Cisco Secure Firewall ASA の新機能（リリース別）

初版：2005 年 5 月 31 日

最終更新：2024 年 5 月 27 日

Cisco Secure Firewall ASA の新機能

このドキュメントでは、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。

バージョン 9.20 の新機能

ASA 9.20(2)/ASDM 7.20(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。
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。 • 4215：15M → **40M** • 4225：30M → **80M** • 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	

機能	説明
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。 新しい/変更されたコマンド： 新しい/変更された画面：
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。 新規/変更されたコマンド： **health-check chassis-heartbeat-delay-rejoin** 新規/変更された画面：**[設定（Configuration）] > [デバイス管理（Device Management）] > [高可用性と拡張性（High Availability and Scalability）] > [ASAクラスタ（ASA Cluster）] > [自動再参加（Auto 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。 変更されたコマンド：**show failover statistics cp-clients**、**show failover statistics np-clients** *9.18(4)* でも同様です。
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。 変更されたコマンド： **show failover statistics events** *9.18(4)* でも同様です。

ASA 9.20(1)/ASDM 7.20(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	
sysopt connection tcp-max-unprocessed-seg コマンドの ASDM サポート	TCP 未処理セグメントの最大数を 6 ～ 24 に設定できます。デフォルト値は 6 です。SIP 電話機が Call Manager に接続していないことを確認したら、未処理の TCP セグメントの最大数を増やすことができます。 新規/変更された画面：**[設定（Configuration）] > [ファイアウォール（Firewall）] > [高度（Advanced）] > [TCPオプション（TCP Options）]**
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。 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**。
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。 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	

機能	説明
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。 *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。 新規/変更されたコマンド： **clu-keepalive-interval** 新規/変更された画面：**[設定（Configuration）] > [デバイス管理（Device Management）] > [高可用性と拡張性（High Availability and Scalability）] > [ASAクラスタ（ASA Cluster）] > [クラスタの設定（Cluster Configuration）]**
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。 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** 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** 新規/変更された画面：**[設定（Configuration）]>[デバイスの設定（Device Setup）]>[ルーティング（Routing）]>[EIGRPv6]**、**[セットアップ（Setup）]**、**[フィルタルール（Filter Rules）]**、**[インターフェイス（Interface）]**、**[パッシブインターフェイス（Passive Interface）]**、**[再配布（Redistribution）]**、および **[スタティックネイバー(Static Neighbor）]** タブ。

機能	説明
HTTP クライアントによるパスモニタリング	PBR は、特定の宛先 IP のメトリックではなく、アプリケーションドメインの HTTP クライアントを介したパスモニタリングによって収集されたパフォーマンスメトリック（RTT、ジッター、パケット損失、および MOS）を使用できるようになりました。インターフェイスの HTTP ベースのアプリケーションモニタリングオプションは、デフォルトで有効になっています。HTTP ベースのパスモニタリングは、ネットワーク サービス グループのオブジェクトを使用してインターフェイスで設定できます。モニタリング対象のアプリケーションが搭載され、パスを決定するためのインターフェイスの順序付けを行う一致 ACL を使用して、PBR ポリシーを設定できます。 新規/変更された画面：**[設定（Configuration）] > [デバイス設定（Device Setup）] > [インターフェイス設定（Interface Settings）] > [パスモニタリング（Path Monitoring）]**
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。 新規/変更されたコマンド：**default-mcast-group**、**mcast-group**、**peer ip** 新しい/変更された画面： • **[構成（Configuration）] > [デバイスの設定（Device Setup）] > [インターフェイスの設定（Interface Settings）] > [VXLAN]** • **[構成（Configuration）] > [デバイスの設定（Device Setup）] > [インターフェイスの設定（Interface Settings）] > [インターフェイス（Interfaces）] > [追加（Add）] > [VNIインターフェイス（VNI Interface）]**
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。 • DNS • HTTP • ICMP • 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	

機能	説明
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。 新規/変更されたコマンド：**crypto ca trustpointcrl**、**cdp url**、**ocsp url** 新規/変更された画面：**[設定（Configuration）]** > **[サイト間VPN（Site-to-Site VPN）]** > **[証明書管理（Certificate Management）]** > **[CA証明書（CA Certificates）]** > **[追加（Add）]**
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。 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。 新しい/変更されたコマンド： **capture** *capture_name* **switch interface** *interface_name* [**direction** { **both** | **egress** | **ingress** }] 新規/変更された画面：**[ウィザード（Wizards）]** > **[パケット キャプチャ ウィザード（Packet Capture Wizard）]** > **[入力トラフィックセレクタ（Ingress Traffic Selector）]** および **[ウィザード（Wizards）]** > **[パケット キャプチャ ウィザード（Packet Capture Wizard）]** > **[出力トラフィックセレクタ（Egress Traffic Selector）]**
VPN 機能	
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。 • 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。 • 追加の SSL カウンタ。 • 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。 新しい/変更されたコマンド： • **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。 新規/変更されたコマンド： **additional-key-exchange**

機能	説明
SAML を使用した セキュアクライアント 接続認証	DNS ロードバランシングクラスタでは、SAML 認証を ASA で設定するときに、設定が適用されるデバイスに一意に解決されるローカルベース URL を指定できます。 新規/変更された画面：**[設定（Configuration）] > [リモートアクセスVPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [安全なクライアント接続プロファイル（Secure Client Connection Profiles）] > [追加/編集（Add/Edit）] > [ベーシック（Basic）] > [SAMLアイデンティティプロバイダー（SAML Identity Provider）] > [管理（Manage）] > [追加/編集（Add/Edit）]**
ASDM 機能	
Windows 11 のサポート	ASDM は Windows 11 で動作することが確認されています。

バージョン 9.19 の新機能

ASDM 7.19(1.95) の新機能

リリース：**2023年 7 月 5 日**

このリリースに新機能はありません。

ASDM 7.19(1.90) の新機能

リリース日：**2023 年 2 月 16 日**

このリリースに新機能はありません。

ASA 9.19(1)/ASDM 7.19(1) の新機能

リリース日：**2022 年 11 月 29 日**

機能	説明
プラットフォーム機能	
Cisco Secure Firewall 3105	Cisco Secure Firewall 3105 の ASA を導入しました。
Azure ゲートウェイロードバランサを使用した ASA Virtual 自動スケールソリューション	Microsoft Azure にゲートウェイロードバランサを使用して ASA Virtual 自動スケールソリューションを展開できます。詳細については、インターフェイス機能を参照してください。
ファイアウォール機能	

機能	説明
ネットワークサービスグループのサポート	最大 1024 のネットワーク サービス グループを定義でき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	
バイアス言語の除去	「Master」と「Slave」という用語を含むコマンド、コマンド出力、syslog メッセージは、「Control」と「Control」に変更されました。 新規/変更されたコマンド：**cluster control-node**、**enable as-data-node**、**prompt**、**show cluster history**、**show cluster info**
ASA Virtual Amazon Web Services（AWS）クラスタリング	ASA Virtual は AWS で最大 16 ノードの個別インターフェイスのクラスタリングをサポートします。AWS ゲートウェイロードバランサ の有無にかかわらず、クラスタリングを使用できます。 ASDM サポートはありません。
ルーティング機能	
IPv6 の BGP グレースフルリスタート	IPv6 アドレスファミリの BGP グレースフルリスタートサポートを追加しました。 新規/変更されたコマンド：IPv6 ファミリをサポートするために拡張された既存のコマンド：**ha-mode graceful-restart** 新規/変更されたコマンド：**[設定（Configuration）] > [デバイスのセットアップ（Device Setup）] > [ルーティング（Routing）] > [BGP（BGP）] > [IPv6 ファミリ（IPv6 Family）] > [ネイバー（Neighbor）]**
ASDM での BGP トラフィックのループバック インターフェイス サポート	ASDM は、BGP ネイバーシップのソースインターフェイスとしてループバック インターフェイスの設定をサポートするようになりました。ループバック インターフェイスは、パス障害の克服に役立ちます。 新規/変更された画面：**[設定（Configuration）] > [デバイスのセットアップ（Device Setup）] > [ルーティング（Routing）] > [BGP（BGP）] > [IPv4 ファミリ（IPv4 Family）]/[IPv6 ファミリ（IPv6 Family）] > [ネイバー（Neighbor）] > [追加（Add）] > [全般（General）]**
インターフェイス機能	
ASA Virtual で IPv6 をサポート	ASAv は、プライベートおよびパブリック クラウド プラットフォームで IPv6 ネットワークプロトコルをサポートします。 ユーザーは次のことができるようになりました。 • day0 設定で IPv6 管理アドレスを有効にして構成します。 • DHCP および静的な方法を使用して IPv6 アドレスを割り当てます。

機能	説明
Azure ゲートウェイロードバランサの ASA Virtual のペアプロキシ VXLAN	Azure ゲートウェイ ロードバランサ（GWLB）で使用するために、Azure の ASA Virtual のペアプロキシモード VXLAN インターフェイスを構成できます。ASA Virtual は、ペアプロキシの VXLAN セグメントを利用して、単一の NIC に外部インターフェイスと内部インターフェイスを定義します。 新規/変更されたコマンド：**external-port、external-segment-id、internal-port、internal-segment-id、proxy paired** ASDM サポートはありません。
Secure Firewall 3100 固定ポートのデフォルトの前方誤り訂正（FEC）が、25 GB+ SR、CSR、および LR トランシーバの cl74-fc から cl108-rs に変更されました	Secure Firewall 3100 の固定ポートで FEC を Auto に設定すると、25 GB SR、CSR、および LR トランシーバのデフォルトのタイプが cl74-fc ではなく cl108-rs に設定されるようになりました。 新規/変更されたコマンド： **fec** 新規/変更された画面：**[設定（Configuration）] > [デバイスのセットアップ（Device Setup）] > [インターフェイスの設定（Interface Settings）] > [インターフェイス（Interfaces）] > [インターフェイスの編集（Edit Interface）] > [ハードウェアプロパティの構成（Configure Hardware Properties）] > [FEC モード（FEC Mode）]**
ASDM でのループバック インターフェイスのサポート	ASDM は、ループバック インターフェイスをサポートするようになりました。 新規/変更された画面：**[設定（Configuration）] > [デバイスのセットアップ（Device Setup）] > [インターフェイスの設定（Interface Settings）] > [インターフェイス（Interfaces）] > [ループバックインターフェイスの追加（Add Loopback Interface）]**
ライセンス機能	
KVM および VMware 上の ASAv5 の ASA Virtual 永久ライセンス予約のサポート	デフォルトの PLR ソフトウェア利用資格を上書きし、KVM および VMware に 2GB RAM の ASAv を展開するときに Cisco Smart Software Manager（SSM）に ASAv5 PLR ライセンスを発行するように要求する新しいコマンドを利用できます。RAM の設定に合わせてソフトウェア利用資格を ASAv5 からデフォルトの PLR ライセンスに戻すための <*no*> 形式を追加することにより、このコマンドを変更できます。
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	
CiscoSSH スタックのデフォルト化	Cisco SSH スタックがデフォルトで使用されるようになりました。 新規/変更されたコマンド： **ssh stack ciscossh** 新しい/変更された画面： • シングルコンテキストモード：**[Configuration] > [Device Management] > [Management Access] > [ASDM/HTTPS/Telnet/SSH]** • マルチコンテキストモード：**[Configuration] > [Device Management] > [SSH Stack]**
VPN 機能	

機能	説明
VTI 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 VTI の送信元インターフェイスとして設定できるようになりました。静的に設定された IP アドレスの代わりに、ループバック インターフェイスから IP アドレスを継承するサポートも追加されました。ループバック インターフェイスは、パス障害の克服に役立ちます。インターフェイスがダウンした場合、ループバック インターフェイスに割り当てられた IP アドレスを使用してすべてのインターフェイスにアクセスできます。 新規/変更されたコマンド：**tunnel source interface**、**ip unnumbered**、**ipv6 unnumbered** 新規/変更された画面：**[設定（Configuration）] > [デバイスのセットアップ（Device Setup）] > [インターフェイスの設定（Interface Settings）] > [インターフェイス（Interfaces）] > [VTIインターフェイスの追加（Add VTI Interface）] > [詳細（Advanced）]**
ダイナミック仮想トンネルインターフェイス（ダイナミック VTI）のサポート	ダイナミック VTI により ASA が強化されました。ハブの複数のスタティック VTI 構成を単一のダイナミック VTI に置き換えることができます。ハブの構成を変更せずに、新しいスポークをハブに追加できます。ダイナミック VTI はダイナミック（DHCP）スポークをサポートします。 新規/変更されたコマンド：**interface virtual-Template**、**ip unnumbered**、**ipv6 unnumbered**、**tunnel protection ipsec policy** 新規/変更された画面：**[設定（Configuration）] > [デバイスのセットアップ（Device Setup）] > [インターフェイスの設定（Interface Settings）] > [インターフェイス（Interfaces）] > [追加（Add）] > [DVTIインターフェイス（DVTI Interface）] > [詳細（Advanced）]**
EIGRP および OSPF の VTI サポート	EIGRP および OSPFv2/v3 ルーティングが仮想トンネルインターフェイスでサポートされるようになりました。これらのルーティングプロトコルを使用して、ルーティング情報を共有し、ピア間の VTI ベースの VPN トンネルを介してトラフィックフローをルーティングできます。
リモートアクセス VPN の TLS 1.3	TLS 1.3 を使用して、リモートアクセス VPN 接続を暗号化できます。 TLS 1.3 では、次の暗号方式のサポートが追加されています。 • TLS_AES_128_GCM_SHA256 • TLS_CHACHA20_POLY1305_SHA256 • TLS_AES_256_GCM_SHA384 この機能には、Cisco Secure Client バージョン 5.0.01242 以降が必要です。 新規/変更されたコマンド: **sslserver-version**、**sslclient-version** 新規/変更された画面：**[設定（Configuration）] > [デバイス管理（Device Management）] > [詳細（Advanced）] > [SSL設定（SSL Settings）]**

機能	説明
IKEv2 サードパーティクライアントのデュアルスタックサポートが追加されました。	Cisco Secure Firewall ASA は、IKEv2 サードパーティのリモートアクセス VPN クライアントからのデュアルスタック IP 要求をサポートするようになりました。サードパーティのリモートアクセス VPN クライアントが IPv4 アドレスと IPv6 アドレスの両方を要求した場合、ASA は、複数のトラフィックセレクタを使用して両方の IP バージョンアドレスを割り当てることができます。この機能により、サードパーティのリモートアクセス VPN クライアントは、単一の IPsec トンネルを使用して IPv4 および IPv6 データトラフィックを送信できます。 新規/変更されたコマンド：**show crypto ikev2 sa**、**show crypto ipsec sa**、**show vpn-sessiondb ra-ikev2-ipsec**
スタティック VTI インターフェイスのトラフィックセレクタ	スタティック VTI インターフェイスのトラフィックセレクタを割り当てることができるようになりました。 新規/変更されたコマンド：**tunnel protection ipsec policy**

バージョン 9.18 の新機能

ASDM 7.18(1.161) の新機能

リリース：**2023年 7 月 3 日**

このリリースに新機能はありません。

ASA 9.18(4)/ASDM 7.20(1) の新機能

リリース：**2023 年10 月 3 日**

機能	説明
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。 *9.20(1)* でも同様です。

機能	説明
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。 変更されたコマンド：**show failover statistics cp-clients**、**show failover statistics dp-clients** *9.20(2)* でも同様です。
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。 変更されたコマンド： **show failover statistics events** *9.20(2)* でも同様です。
インターフェイス機能	
FXOS local-mgtm **show** コマンドの改善	FXOS local-mgmt のインターフェイス show コマンドに関する追加項目は次のとおりです。 • **show portmanager switch tail-drop-allocated buffers all** コマンドが追加されました。 • **show portmanager switch status** コマンドにイーサネットポート ID が含まれます。 • Cisco Secure Firewall 3100 に、**show portmanager switch default-rule-drop-counter** コマンドが追加されました。 新規/変更された FXOS コマンド：**show portmanager switch tail-drop-allocated buffers all**、**show portmanager switch status**、**show portmanager switch default-rule-drop-counter**
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	

機能	説明
show tech support の改善	次の項目に対して、**show tech support** への出力が追加されました。 • Cisco Secure Firewall 3100 の **show storage detail**、**show slot expand detail**（**show tech support brief** 内） • ASA Virtual のフラッシュ内の dpdk.log からの最近のメッセージ • Firepower 1010 の制御リンク状態 • **show failover** 統計情報 • FXOS local-mgmt **show portmanager switch tail-drop-allocated buffers all** • **show controller** • DPDK mbuf プール統計情報 新規/変更されたコマンド： **show tech support**

ASA 9.18(3)/ASDM 7.19(1.90) の新機能

リリース日：**2023 年 2 月 16 日**

機能	説明
プラットフォーム機能	
Firepower 1010E	Firepower 1010E が導入されました。このモデルは、Power Over Ethernet ポートが搭載されていないことを除き Firepower 1010 と同じです。 7.19(1.90) または 7.18(2.1) での ASDM サポート。ASDM 7.19(1) ではこのモデルをサポートしていません。 *9.18(2.218)* でも同様。このモデルは *9.19(1)* ではサポートされていません。
インターフェイス機能	
Secure Firewall 3100 固定ポートのデフォルトの前方誤り訂正（FEC）が、25 GB+ SR、CSR、および LR トランシーバの cl74-fc から cl108-rs に変更されました	Secure Firewall 3100 の固定ポートで FEC を Auto に設定すると、25 GB SR、CSR、および LR トランシーバのデフォルトのタイプが cl74-fc ではなく cl108-rs に設定されるようになりました。 新規/変更されたコマンド： **fec** 新規/変更された画面：**[設定（Configuration）]** > **[デバイスのセットアップ（Device Setup）]** > **[インターフェイスの設定（Interface Settings）]** > **[インターフェイス（Interfaces）]** > **[インターフェイスの編集（Edit Interface）]** > **[ハードウェアプロパティの構成（Configure Hardware Properties）]** > **[FEC モード（FEC Mode）]** *9.19(1)* および *9.18(2.7)* でも同様。

機能	説明
VPN 機能	
SAML を使用した AnyConnect 接続認証	DNS ロードバランシングクラスタでは、SAML 認証を ASA で設定するときに、設定が適用されるデバイスに一意に解決されるローカルベース URL を指定できます。 新規/変更されたコマンド：**local-base-url***url*

ASA 9.18(2)/ASDM 7.18(1.152) の新機能

リリース日：**2022 年 8 月 10 日**

機能	説明
インターフェイス機能	
BGP および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	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。 • AAA • BGP • SNMP • SSH • Syslog • Telnet 新規/変更されたコマンド：**interface loopback**、**logging host**、**neighbor update-source**、**snmp-server host**、**ssh**、**telnet** ASDM サポートはありません。
ping コマンドの変更	ループバック インターフェイスの ping をサポートするために、**ping** コマンドの動作が変更されました。コマンドでインターフェイスを指定する場合、送信元 IP アドレスは指定されたインターフェイスの IP アドレスと一致しますが、実際の出力インターフェイスは、データルーティングテーブルを使用したルートルックアップによって決定されます。 新規/変更されたコマンド： **ping**

ASDM 7.18(1.152) の新機能

リリース日：**2022 年 8 月 2 日**

このリリースに新機能はありません。

ASA 9.18(1)/ASDM 7.18(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	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。
ファイアウォール機能	
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。	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。 さらに、オブジェクトグループ検索が新規展開のアクセス制御に対してデフォルトで有効になりました。デバイスをアップグレードしても、引き続きこのコマンドは無効になります。有効にする場合（推奨）、手動で行う必要があります。 **注意** ダウングレードすると、**access-group** コマンドはまだ **access-list** コマンドをロードしていないため拒否されます。以前に **forward-reference enable** コマンドを有効にしていた場合でも、このコマンドは現在削除されているため同じ結果となります。ダウングレードする前にすべての **access-group** コマンドを手動でコピーし、ダウングレード後に再入力してください。 **forward-reference enable** コマンドを削除し、新規展開のデフォルト値を変更して **object-group-search access-control** を有効にしました。
ルーティング機能	
PBR のパスモニタリングメトリック。	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ースを 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。 新規/変更されたコマンド：**clear path-monitoring**、**policy-route**、**show path-monitoring** 新規/変更された画面：**[設定（Configuration）] > [デバイス設定（Device Setup）] > [インターフェイス設定（Interface Settings）] > [インターフェイス（Interfaces）]**
インターフェイス機能	

機能	説明
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	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。 新規/変更されたコマンド： **flowcontrol send on** 新規/変更された画面：**[設定（Configuration）]** > **[デバイス設定（Device Setup）]** > **[インターフェイス（Interface）]** > **[全般（General）]**
Secure Firewall 3130 および 3140 のブレークアウトポート	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 ブレー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： **breakout** 新規/変更された画面：**[設定（Configuration）]** > **[デバイス管理（Device Management）]** > **[詳細（Advanced）]** > **[EPM]**
ライセンス機能	
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： **feature carrier** 新規/変更された画面：**[Configuration]** > **[Device Management]** > **[Licensing]** > **[Smart Licensing]**。
証明書の機能	
相互l 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：**ssl-client-certificate** 新規/変更された画面：**[設定（Configuration）]** > **[デバイス管理（Device Management）]** > **[ユーザー/AAA（Users/AAA）]** > > **[AAAサーバーグループ（AAA Server Groups）]**、LDAP を追加または編集。

機能	説明
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 **crypto ca reference-identity** <*name*> 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 reference-identity 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。 reference-identity CLI は、AAA サーバーホスト設定および ddns 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：**ldap-over-ssl**、**ddns update method** 、および **show update method**。 新しい/変更された画面： • **[設定（Configuration）] > [デバイス管理（Device Management）] > [ユーザー/AAA（Users/AAA）]> > [AAAサーバーグループ（AAA Server Groups）] > [認証/認可用のLDAPパラメータ（LDAP Parameters for authentication/authorization）]** • **[設定（Configuration）] > [デバイス管理（Device Management）] > [DNS] > [ダイナミックDNS（Dynamic DNS）] > [メソッドを更新（Update Methods）]**
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	
複数の DNS サーバーグループ	複数の DNS サーバーグループ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 サーバーグループ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 eng.cisco.com サーバー宛てのトラフィックで内部の DNS サーバーを使用する場合は、eng.cisco.com 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 サーバーグループを使用します。たとえば、DefaultDNS 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 サーバーを含めることができます。 新規/変更されたコマンド：**dns-group-map**、**dns-to-domain** 新規/変更された画面：**[設定（Configuration）] > [デバイス管理（Device Management）] > [DNS] > [DNSクライアント（DNS Client）]**
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ギング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、ロギングレートが動的に制限されます。 新規/変更されたコマンド： **logging rate-limit** 新規/変更された画面：**[設定（Configuration）] > [デバイス管理（Device Management）] > [ロギング（Logging）] > [レート制限（Rate Limit）]**

機能	説明
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： **capture real-time** 新規/変更された画面：**[ウィザード（Wizards）]** > **[パケットキャプチャウィザード（Packet Capture Wizard）]** > **[バッファおよびキャプチャ（Buffers & Captures）]**
VPN 機能	
IPsec フローがオフロードされます。	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：**clear flow-offload-ipsec**、**flow-offload-ipsec**、**show flow-offload-ipsec** 新規/変更された画面：**[設定（Configuration）]** > **[ファイアウォール（Firewall）]** > **[高度（Advanced）]** > **[IPsecオフロード（IPsec Offload）]**
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：**authentication saml certificate**、**authentication certificate saml** 、**authentication multiple-certificate saml** 新規/変更された画面：**[設定（Configuration）]** > **[リモートアクセスVPN（Remote Access VPN）]** > **[ネットワーク(クライアント)アクセス（Network (Client) Access）]** > **[IPsec(IKEv1)接続プロファイル（IPsec(IKEv1) Connection Profiles）]** > **[追加/編集（Add/Edit）]** > **[ベーシック（Basic）]**

バージョン 9.17 の新機能

ASDM 7.17(1.155) の新機能

リリース日：**2022 年 6 月 28 日**

このリリースに新機能はありません。

ASDM 7.17(1.152) の新機能

リリース日：**2022 年 2 月 8 日**

このリリースに新機能はありません。

ASA 9.17(1)/ASDM 7.17(1) の新機能

リリース日：**2021 年 12 月 1 日**

機能	説明
プラットフォーム機能	
Cisco Secure Firewall 3100	Cisco Secure Firewall 3110、3120、3130、および 3140 の ASA が導入されました。Cisco Secure Firewall 3100 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。Secure Firewall 3100 25 Gbps 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。 新規/変更されたコマンド： **fec, netmod, speed sfp-detect, raid, show raid, show ssd** 新しい/変更された画面： • **[Configuration] > [Device Management] > [Advanced] > [EPM]** • **[Configuration] > [Device Settings] > [Interfaces] > [Edit Interface] > [Configure Hardware Properties]**
自動スケールに対する ASA 仮想のサポート	ASA 仮想 は、次のパブリッククラウドサービスの自動スケールをサポートするようになりました。 • Google Cloud Platform（GCP） • Oracle Cloud Infrastrucure（OCI） 自動スケーリングは、キャパシティの要件に基づいて ASA 仮想 アプリケーションのインスタンス数を増減します。

機能	説明
AWS の ASA 仮想 での拡張インスタンスのサポート	AWS パブリッククラウド上の ASA 仮想 は、異なる Nitro インスタンスファミリから AWS Nitro システムインスタンスをサポートするようになりました。 AWS 用 ASA 仮想により、次のインスタンスのサポートが追加されています。 • c5a.large、c5a.xlarge、c5a.2xlarge、c5a.4xlarge • c5d.large、c5d.xlarge、c5d.2xlarge、c5d.4xlarge • c5ad.large、c5ad.xlarge、c5ad.2xlarge、c5ad.4xlarge • m5n.large、m5n.xlarge、m5n.2xlarge、m5n.4xlarge • m5zn.large、m5zn.xlarge、m5zn.2xlarge サポートされているインスタンスの詳細なリストについては、『Cisco Adaptive Security Virtual Appliance (ASAv) Data Sheet』を参照してください。
Azure の ASA 仮想 拡張インスタンスのサポート	Azure パブリッククラウド上の ASA 仮想 は、次のインスタンスをサポートするようになりました。 • Standard_D8s_v3 • Standard_D16s_v3 • Standard_F8s_v2 • Standard_F16s_v2 サポートされているインスタンスの詳細なリストについては、『Cisco Adaptive Security Virtual Appliance (ASAv) Data Sheet』を参照してください。
ASA 仮想 の Intel® QuickAssist テクノロジー（QAT）	ASA 仮想 は、 Intel QuickAssist（QAT）8970 PCI アダプタを使用する ASA 仮想 展開にハードウェア暗号化アクセラレーションを提供します。ASA 仮想 を使用した ASAv のハードウェア暗号化アクセラレーションは、VMware ESXi および KVM でのみサポートされます。
OCI 上の ASA 仮想 に対する Single Root I/O Virtualization（SR-IOV）のサポート。	OCI 上の ASA 仮想 に Single Root Input/Output Virtualization（SR-IOV）を実装できるようになりました。SR-IOV により、ASA 仮想 のパフォーマンスを向上させることができます。SR-IOV モードでの vNIC としての Mellanox 5 はサポートされていません。
ファイアウォール機能	
変換後（マップ後）の宛先としての完全修飾ドメイン名（FQDN）オブジェクトの Twice NAT サポート	www.example.com を指定する FQDN ネットワークオブジェクトを、Twice NAT ルールの変換後（マップ後）の宛先アドレスとして使用できます。システムでは、DNS サーバーから返された IP アドレスに基づいてルールが設定されます。

機能	説明
ネットワークサービス オブジェクトと、ポリシーベースのルーティングおよびアクセス制御におけるネットワークサービス オブジェクトの使用	ネットワークサービス オブジェクトを設定し、それらを拡張アクセス コントロール リストで使用して、ポリシーベース ルーティング ルート マップおよびアクセス コントロール グループで使用できます。ネットワークサービス オブジェクトには、IP サブネットまたは DNS ドメイン名の仕様が含まれ、オプションでプロトコルとポートの仕様が含まれます。これらは、基本的にネットワークオブジェクトとサービスオブジェクトを結合します。この機能には、信頼できる DNS サーバーを定義して、DNS ドメイン名解決が信頼できる送信元から IP アドレスを確実に取得できるようにする機能も含まれています。 次のコマンドが追加または変更されました：**access-list extended**、**app-id**、**clear configure object network-service**、**clear configure object-group network-service**、**clear dns ip-cache**、**clear object**、**clear object-group**、**debug network-service**、**description**、**dns trusted-source**、**domain**、**network-service-member**、**network-service reload**、**object-group network-service**、**object network-service**、**policy-route cost**、**set adaptive-interface cost**、**show asp table classify**、**show asp table network-service**、**show dns trusted-source**、**show dns ip-cache**、**show object**、**show object-group**、**show running-config**、**subnet** 次の画面が追加または変更されました。 • **[Configuration]** > **[Device Setup]** > **[Routing]** > **[Route Maps]** の順に移動し、[Add/Edit] ダイアログボックスを追加します。 • **[Configuration]** > **[Device Setup]** > **[Interface Settings]** > **[Interfaces]** の順に移動し、[Add/Edit] ダイアログボックスを追加します。 • **[Configuration]** > **[Firewall]** > **[Objects]** > **[Network Services Objects/Groups]** • **[Configuration]** > **[Device Management]** > **[DNS]** > **[DNS Client]**
ハイ アベイラビリティとスケーラビリティの各機能	
VMware および KVM 用の ASAv30、ASAv50、および ASAv100 クラスタリング	ASA 仮想 クラスタリングを使用すると、最大 16 の ASA 仮想 を単一の論理デバイスとしてグループ化できます。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。ASA 仮想 クラスタリングは、ルーテッド ファイアウォール モードの個別インターフェイスモードをサポートします。 スパンド EtherChannelはサポートされていません。ASA 仮想 は、クラスタ制御リンクに VXLAN 仮想インターフェイス（VNI）を使用します。 新規/変更されたコマンド：**cluster-interface vni**、**nve-only cluster**、**peer-group**、**show cluster info**、**show cluster info instance-type**、**show nve 1** 新しい/変更された画面： • **[Configuration]** > **[Device Setup]** > **[Interface Settings]** > **[Interfaces]** • **[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[ASA Cluster]**

機能	説明
ハイ アベイラビリティ グループまたはクラスタ内のルートのクリア	以前のリリースでは、**clear route** コマンドはユニットのルーティングテーブルのみをクリアしました。現在、ハイアベイラビリティグループまたはクラスタで動作している場合、コマンドはアクティブユニットまたはコントロールユニットでのみ使用でき、グループまたはクラスタ内のすべてのユニットのルーティングテーブルをクリアします。 **clear route** コマンドが変更されました。
インターフェイス機能	
ASA 仮想の Geneve インターフェイスサポート	AWS ゲートウェイロードバランサのシングルアームプロキシをサポートするために、ASAv30、ASAv50、および ASAv100 の Geneve カプセル化サポートが追加されました。 新規/変更されたコマンド：**debug geneve**、**debug nve**、**debug vxlan**、**encapsulation**、**packet-tracer geneve**、**proxy single-arm**、**show asp drop**、**show capture**、**show interface**、**show nve** 新しい/変更された画面： • **[Configuration]** > **[Device Setup]** > **[Interface Settings]** > **[Interfaces]** > **[Add]** > **[VNI Interface]** • **[Configuration]** > **[Device Setup]** > **[Interface Settings]** > **[VXLAN]**
Secure Firewall 3100 の自動ネゴシエーションは、1 ギガビット以上のインターフェイスで有効または無効にすることができます。	Secure Firewall 3100 の自動ネゴシエーションは、1 ギガビット以上のインターフェイスで有効または無効にすることができます。他のモデルの SFP ポートの場合、**no speed nonegotiate** オプションは速度を 1000 Mbps に設定します。新しいコマンドは、自動ネゴシエーションと速度を個別に設定できることを意味します。 新規/変更されたコマンド：**negotiate-auto** 新規/変更された画面： **[Configuration]** > **[Device Setup]** > **[Interface Settings]** > **[Interfaces]** > **[Advanced]**
管理およびトラブルシューティングの機能	
起動時間と tmatch コンパイルステータス。	**show version** コマンドには、システムの起動（ブート）にかかった時間に関する情報が含まれるようになりました。設定が大きいほど、システムの起動に時間がかかることに注意してください。 新しい **show asp rule-engine** コマンドは、tmatch コンパイルのステータスを表示します。Tmatch コンパイルは、アクセスグループ、NAT テーブル、およびその他のいくつかの項目として使用されるアクセスリストに使用されます。これは、非常に大きな ACL と NAT テーブルがある場合には、CPU リソースを消費し、進行中のパフォーマンスに影響を与える可能性がある内部プロセスです。コンパイル時間は、アクセスリスト、NAT テーブルなどのサイズによって異なります。

機能	説明
show access-list element-count 出力の拡張と **show tech-support** コンテンツの強化	**show access-list element-count** の出力は、次のように拡張されています。 • マルチコンテキストモードのシステムコンテキストで使用すると、出力には、すべてのコンテキストのすべてのアクセスリストの要素数が表示されます。 • オブジェクトグループ検索を有効にして使用すると、出力には要素数のオブジェクトグループの数に関する詳細が含まれます。 さらに、**show tech-support** 出力には **show access-list element-count** と **show asp rule-engine** の出力が含まれます。
CiscoSSH スタック	ASA は、SSH 接続に独自の SSH スタックを使用します。代わりに、OpenSSH に基づく CiscoSSH スタックを使用するように選択できるようになりました。デフォルトスタックは引き続き ASA スタックです。Cisco SSH は次をサポートします。 • FIPS の準拠性 • シスコおよびオープンソースコミュニティからの更新を含む定期的な更新 CiscoSSH スタックは次をサポートしないことに注意してください。 • VPN を介した別のインターフェイスへの SSH（管理アクセス） • EdDSA キーペア • FIPS モードの RSA キーペア これらの機能が必要な場合は、引き続き ASA SSH スタックを使用する必要があります。 CiscoSSH スタックでは、SCP 機能に若干の変更があります。ASA **copy** コマンドを使用して SCP サーバとの間でファイルをコピーするには、**ssh** コマンドを使用して、ASA で SCP サーバサブネット/ホストの SSH アクセスを有効にする必要があります。 新規/変更されたコマンド： **ssh stack ciscossh** 新しい/変更された画面： • シングルコンテキストモード：**[Configuration]** > **[Device Management]** > **[Management Access]** > **[ASDM/HTTPS/Telnet/SSH]** • マルチコンテキストモード：**[Configuration]** > **[Device Management]** > **[SSH Stack]**
パケットトレーサでの PCAP サポート	パケットトレーサツールで PCAP ファイルを再生し、トレース結果を取得できます。**pcap** および **force** は、パケットトレーサでの PCAP の使用をサポートするための 2 つの新しいキーワードです。 新規/変更されたコマンド：**packet-tracer input** および**show packet-tracer**

機能	説明
より強力なローカルユーザーと有効なパスワード要件	ローカルユーザーと有効なパスワードについて、次のパスワード要件が追加されました。 • パスワードの長さ：8 文字以上。以前は、最小値が 3 文字でした。 • 繰り返し文字と連続文字：3 つ以上の連続した ASCII 文字または繰り返しの ASCII 文字は許可されません。たとえば、次のパスワードは拒否されます。 • **abc**user1 • user**543** • user**aaaa** • user2**666** 新規/変更されたコマンド：**enable password**、**username** 新規/変更された画面： • **[Configuration]** > **[Device Management]** > **[Users/AAA]** > **[User Accounts]** • **[Configuration]** > **[Device Setup]** > **[Device Name/Password]**
ローカルユーザーのロックアウトの変更	設定可能な回数のログイン試行に失敗すると、ASA はローカルユーザーをロックアウトする場合があります。この機能は、特権レベル 15 のユーザーには適用されませんでした。また、管理者がアカウントのロックを解除するまで、ユーザーは無期限にロックアウトされます。管理者がその前に **clear aaa local user lockout** コマンドを使用しない限り、ユーザーは 10 分後にロック解除されるようになりました。特権レベル 15 のユーザーも、ロックアウト設定が適用されるようになりました。 新規/変更されたコマンド：**aaa local authentication attempts max-fail** 、**show aaa local user**
SSH および Telnet パスワード変更プロンプト	ローカルユーザーが SSH または Telnet を使用して ASA に初めてログインすると、パスワードを変更するように求められます。また、管理者がパスワードを変更した後、最初のログインに対してもプロンプトが表示されます。ただし、ASA がリロードすると、最初のログインであっても、ユーザーにプロンプトは表示されません。 VPN などのローカル ユーザー データベースを使用するサービスは、SSH または Telnet ログイン中に変更された場合、新しいパスワードも使用する必要があることに注意してください。 新規/変更されたコマンド： **show aaa local user**
モニタリング機能	
SNMP は、ネットワークオブジェクトの形式で複数のホストをグループ化するときに IPv6 をサポートするようになりました	**snmp-server** コマンドの **host-group** コマンドは、IPv6 ホスト、範囲、およびサブネットオブジェクトをサポートするようになりました。 新規/変更されたコマンド： **snmp-server host-group**

機能	説明
VPN 機能	
IKEv2 のローカルトンネル ID のサポート	IKEv2 のローカルトンネルID設定のサポートが追加されました。 新規/変更されたコマンド： **set ikev2 local-identity**
DAP 制約による SAML 属性のサポート	DAP ポリシーの選択に使用できる SAML アサーション属性のサポートが追加されました。また、*cisco_group_policy* 属性でグループポリシーを指定する機能も導入されています。
IDP 設定の複数の SAML トラストポイント	この機能は、同じエンティティ ID の複数のアプリケーションをサポートするアプリケーションの SAML IDP 設定ごとに、複数の IDP トラストポイントの追加をサポートします。 新規/変更されたコマンド： **saml idp-trustpoint <trustpoint-name>**
セキュアクライアント VPN SAML 外部ブラウザ	VPN SAML 外部ブラウザを設定して、パスワードなしの認証、WebAuthN、FIDO2、SSO、U2F、Cookie の永続性による SAML エクスペリエンスの向上など、追加の認証の選択肢を有効にできるようになりました。リモートアクセス VPN 接続プロファイルのプライマリ認証方式として SAML を使用する場合は、セキュアクライアントクライアントが セキュアクライアント 組み込みブラウザではなく、クライアントのローカルブラウザを使用して Web 認証を実行するように選択できます。このオプションは、VPN 認証と他の企業ログインの間のシングルサインオン（SSO）を有効にします。また、生体認証や Yubikeys など、埋め込みブラウザでは実行できない Web 認証方法をサポートする場合は、このオプションを選択します。 新規/変更されたコマンド： **external-browser** 新規/変更された画面： **[Remote Access VPN connection profile wizard]** > **[SAML Login Experience]**
SAML を使用した VPN ロードバランシング	ASA は、SAML 認証を使用した VPN ロードバランシングをサポートするようになりました。

バージョン 9.16 の新機能

ASA 9.16(4) の新機能

リリース日：2022 年 10 月 13 日

このリリースに新機能はありません。

ASA 9.16(3) の新機能

リリース日：2022 年 4 月 6 日

このリリースに新機能はありません。

ASA 9.16(2) の新機能

リリース：2021 年 8 月 18 日

このリリースに新機能はありません。

ASDM 7.16(1.150) の新機能

リリース：2021 年 6 月 15 日

このリリースに新機能はありません。

ASA 9.16(1)/ASDM 7.16(1) の新機能

リリース日：2021 年 5 月 26 日

機能	説明
ファイアウォール機能	
システム定義の NAT ルールの新しいセクション 0。	新しいセクション 0 が NAT ルールテーブルに追加されました。このセクションは、システムの使用に限定されます。システムが正常に機能するために必要なすべての NAT ルールがこのセクションに追加され、これらのルールは作成したルールよりも優先されます。以前は、システム定義のルールがセクション 1 に追加され、ユーザー定義のルールがシステムの適切な機能を妨げる可能性がありました。セクション 0 のルールを追加、編集、または削除することはできませんが、**show nat detail** コマンド出力に表示されます。
デフォルトの SIP インスペクション ポリシー マップは、非 SIP トラフィックをドロップします。	SIP インスペクションされるトラフィックでは、現在、デフォルトでは非 SIP トラフィックがドロップされます。以前のデフォルトでは、SIP のインスペクション対象ポートで非 SIP トラフィックが許可されていました。 デフォルトの SIP ポリシーマップが変更され、**no traffic-non-sip** コマンドが追加されました。

機能	説明
GTP インスペクションでドロップされる IMSI プレフィックスを指定する機能です。	GTP インスペクションでは、許可する Mobile Country Code/Mobile Network Code（MCC/MNC）の組み合わせを識別するために、IMSI プレフィックスフィルタリングを設定できます。ドロップする MCC/MNC の組み合わせに対して IMSI フィルタリングを実行できるようになりました。これにより、望ましくない組み合わせをリストにして、デフォルトで他のすべての組み合わせを許可することができます。 **drop mcc** コマンドが追加されました。 次の画面が変更されました：GTP インスペクションマップの [IMSI Prefix Filtering] タブに [Drop] オプションが追加されました。
初期接続の最大セグメントサイズ（MSS）を設定します。	サービスポリシーを設定して、初期接続制限に達したときに初期接続の SYN cookie を生成するためのサーバーの最大セグメントサイズ（MSS）を設定できます。これは、最大初期接続数も設定するサービスポリシーの場合に意味があります。 新規/変更されたコマンド：**set connection syn-cookie-mss** 新規/変更された画面：[Add/Edit Service Policy] ウィザードの **[Connection Settings]**
多対 1 および 1 対多接続の CPU 使用率とパフォーマンスが向上しました。	ダイナミック NAT / PAT およびスキャン脅威検出とホスト統計情報を含む接続を除き、システムは接続の作成時に、ローカルホストオブジェクトを作成せず、ロックすることもなくなりました。これにより、多数の接続を同じサーバー（ロードバランサや Web サーバーなど）に対して確立する場合や、1 つのエンドポイントが多数のリモートホストに接続する場合に、パフォーマンスと CPU 使用率が向上します。 次のコマンドが変更されました：**clear local-host**（廃止）、 **show local-host**
プラットフォーム機能	
VMware ESXi 7.0 用の ASA 仮想サポート	ASA 仮想 仮想プラットフォームは、VMware ESXi 7.0 で動作するホストをサポートしています。vi.ovf および esxi.ovf ファイルに新しい VMware ハードウェアバージョンが追加され、ESXi 7.0 で ASA 仮想 の最適なパフォーマンスと使いやすさを実現しました。 変更されたコマンドはありません。 変更された画面はありません。
ASA 仮想 の Intel® QuickAssist テクノロジー（QAT）	ASA 仮想 は、 Intel QuickAssist（QAT）8970 PCI アダプタを使用する ASA 仮想 展開にハードウェア暗号化アクセラレーションを提供します。ASA 仮想 を使用した ASAv のハードウェア暗号化アクセラレーションは、VMware ESXi および KVM でのみサポートされます。 変更されたコマンドはありません。 変更された画面はありません。

機能	説明
OpenStack の ASA 仮想	ASA 仮想 仮想プラットフォームに OpenStack のサポートが追加されました。 変更されたコマンドはありません。 変更された画面はありません。
ハイ アベイラビリティとスケーラビリティの各機能	
Firepower 4100/9300 でのクラスタリングの PAT ポートブロック割り当てが改善されました	PAT ポートブロック割り当ての改善により、制御ユニットはノードに参加するためにポートを確保し、未使用のポートを積極的に再利用できるようになります。割り当てを最適化するために、**cluster-member-limit** コマンドを使用して、クラスタ内に配置する予定の最大ノードを設定できます。これにより、制御ユニットは計画されたノード数にポートブロックを割り当てることができ、使用する予定のない追加のノード用にポートを予約する必要がなくなります。デフォルトは 16 ノードです。また、syslog 747046 を監視して、新しいノードに使用できるポートが十分にあることを確認することもできます。 新規/変更されたコマンド：**cluster-member-limit**、**show nat pool cluster** [**summary**]、**show nat pool ip detail** 新規/変更された画面：**[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[ASA Cluster]** > **[Cluster Configuration]** > **[Cluster Member Limit]** フィールド
show cluster history コマンドの改善	**show cluster history** コマンドの出力が追加されました。 新規/変更されたコマンド： **show cluster history brief**、**show cluster history latest**、**show cluster history reverse**、**show cluster history time**
Firepower 1140 の最大コンテキスト数が 5 から 10 に増加	Firepower 1140 は、最大 10 のコンテキストをサポートするようになりました。
証明書の機能	
認定のための Enrollment over Secure Transport（EST）	ASA は、Enrollment over Secure Transport（EST）を使用した証明書の登録をサポートしています。ただし、EST 登録は、RSA キーおよび ECDSA キーとのみ使用するように設定できます。EST 登録用に設定されたトラストポイント用に EdDSA キーペアを使用することはできません。 新規/変更されたコマンド：**enrollment protocol**、**crypto ca authenticate**、および**crypto ca enroll** 新規/変更された画面：**[Configuration]** > **[Device Management]** > **[Certificate Management]** > **[Identity Certificate]** > **[Advanced]**.

機能	説明
新しい EdDSA キーのサポート	新しいキーオプション EdDSA が、既存の RSA および ECDSA オプションに追加されました。 新規/変更されたコマンド：**crypto key generate**、**crypto key zeroize**、**show crypto key mypubkey** 新規/変更された画面：**[Configuration]** > **[Device Management]** > **[Certificate Management]** > **[Identity Certificate]** > **[Add Identity Certificates]** > **[Add Key Pair]**
証明書キーの制限を上書きするコマンド	認定に SHA1with RSA 暗号化アルゴリズムを使用するためのサポート、および RSA キーサイズが 2048 未満の証明書のサポートが削除されました。**crypto ca permit-weak-crypto** コマンドを使用して、これらの制限を上書きできます。 新規/変更されたコマンド： **crypto ca permit-weak-crypto** 新規/変更された画面：**[Configuration]** > **[Device Management]** > **[Certificate Management]** > **[Identity Certificate]**、**[Configuration]** > **[Remote Access VPN]** > **[Certificate Management]** > **[Identity Certificate]**、および**[Configuration]** > **[Remote Access VPN]** > **[Certificate Management]** > **[Code Signer]**
管理およびトラブルシューティングの機能	

機能	説明
SSH セキュリティの改善	SSH が次の SSH セキュリティの改善をサポートするようになりました。 • ホストキーの形式：**crypto key generate** {**eddsa** | **ecdsa**}。RSA に加えて、EdDSA および ECDSA ホストキーのサポートが追加されました。ASA は、存在する場合、EdDSA、ECDSA、RSA の順にキーの使用を試みます。**ssh key-exchange hostkey rsa** コマンドで RSA キーを使用するように ASA を明示的に設定する場合は、2048 ビット以上のキーを生成する必要があります。アップグレードの互換性のために、ASA はデフォルトのホストキー設定が使用されている場合にのみ、より小さい RSA ホストキーを使用します。RSA のサポートは今後のリリースで削除されます。 • キー交換アルゴリズム：**ssh key-exchange group** {**ecdh-sha2-nistp256** | **curve25519-sha256**} • 暗号化アルゴリズム：**ssh cipher encryption chacha20-poly1305@openssh.com** • SSH バージョン 1 はサポートされなくなりました。**ssh version** コマンドは削除されました。 新規/変更されたコマンド：**crypto key generate eddsa**、**crypto key zeroize eddsa** 、**show crypto key mypubkey**、**ssh cipher encryption chacha20-poly1305@openssh.com**、**ssh key-exchange group** {**ecdh-sha2-nistp256** | **curve25519-sha256**}、**ssh key-exchange hostkey**、**ssh version** 新しい/変更された画面： • **[Configuration]** > **[Device Management]** > **[Management Access]** > **[ASDM/HTTPS/Telnet/SSH]** • **[Configuration]** > **[Device Management]** > **[Certificate Management]** > **[Identity Certificates]** • **[Configuration]** > **[Device Management]** > **[Advanced]** > **[SSH Ciphers]**
モニタリング機能	
SNMPv3 認証	ユーザー認証に SHA-224 および SHA-384 を使用できるようになりました。ユーザー認証に MD5 を使用できなくなりました。 暗号化に DES を使用できなくなりました。 新規/変更されたコマンド：**snmp-server user** 新規/変更された画面：**[構成（Configuration）]** > **[デバイス管理（Device Management）]** > **[管理アクセス（Management Access）]** > **[SNMP]**
VPN 機能	

機能	説明
スタティック VTI での IPv6 のサポート	ASA は、仮想トンネルインターフェイス（VTI）の設定で IPv6 アドレスをサポートしています。 VTI トンネル送信元インターフェイスには、トンネルエンドポイントとして使用するように設定できる IPv6 アドレスを設定できます。トンネル送信元インターフェイスに複数の IPv6 アドレスがある場合は、使用するアドレスを指定できます。指定しない場合は、リストの最初の IPv6 グローバルアドレスがデフォルトで使用されます。 トンネルモードは、IPv4 または IPv6 のいずれかです。ただし、トンネルをアクティブにするには、VTI で設定されている IP アドレスタイプと同じである必要があります。IPv6 アドレスは、VTI のトンネル送信元インターフェイスまたはトンネル宛先インターフェイスに割り当てることができます。 新規/変更されたコマンド：**tunnel source interface**、**tunnel destination**、**tunnel mode**
デバイスあたり 1024 個の VTI インターフェイスのサポート	デバイスに設定できる VTI の最大数が、100 個から 1024 個に増加しました。 プラットフォームが 1024 個を超えるインターフェイスをサポートしている場合でも、VTI の数はそのプラットフォームで設定可能な VLAN の数に制限されます。たとえば、ASA 5510 は 100 個の VLAN をサポートしているため、トンネル数は 100 から設定された物理インターフェイスの数を引いた数になります。 新規/変更されたコマンド：なし 新規/変更された画面：なし
SSL の DH グループ 15 のサポート	SSL 暗号化の DH グループ 15 のサポートが追加されました。 新規/変更されたコマンド： **ssl dh-group group15**
IPsec 暗号化の DH グループ 31 のサポート	IPsec 暗号化の DH グループ 31 のサポートが追加されました。 新規/変更されたコマンド： **set pfs**
IKEv2 キューの SA を制限するサポート	SA-INIT パケットのキュー数を制限するサポートが追加されました。 新規/変更されたコマンド： **crypto ikev2 limit queue sa_init**
IPsec 統計情報をクリアするオプション	IPsec 統計情報をクリアおよびリセットするための CLI が導入されました。 新規/変更されたコマンド：**clear crypto ipsec stats** および**clear ipsec stats**

バージョン 9.15 の新機能

ASDM 7.15(1.150) の新機能

リリース日：**2021** 年 **2** 月 **8** 日

このリリースに新機能はありません。

ASA 9.15(1)/ASDM 7.15(1) の新機能

リリース：**2020** 年 **11** 月 **2** 日

機能	説明
プラットフォーム機能	
パブリッククラウド向け ASAv	次のパブリッククラウドサービスに ASAv を導入しました。 • Oracle Cloud Infrastrucure（OCI） • Google Cloud Platform（GCP） 変更されたコマンドはありません。 変更された画面はありません。
自動スケールに対する ASAv のサポート	ASAv は、次のパブリッククラウドサービスの自動スケールをサポートするようになりました。 • Amazon Web Services（AWS） • Miscrosoft Azure 自動スケーリングは、キャパシティの要件に基づいて ASAv アプリケーションのインスタンス数を増減します。 変更されたコマンドはありません。 変更された画面はありません。
ASAv for Microsoft Azure の Accelerated Networking に対するサポート（SR-IOV）	Microsoft Azure パブリッククラウド上の ASAv は、Azure の Accelerated Networking（AN）をサポートするようになりました。これにより、VM に対するシングルルート I/O の仮想化（SR-IOV）が可能になり、ネットワーキングのパフォーマンスが大幅に向上しています。 変更されたコマンドはありません。 変更された画面はありません。
ファイアウォール機能	

機能	説明
クラスタリングでの PAT アドレス割り当ての変更。PAT プールの **flat** オプションがデフォルトで有効になり、設定できなくなりました。	PAT アドレスがクラスタのメンバーに配布される方法が変更されます。以前は、アドレスはクラスタのメンバーに配布されていたため、PAT プールにはクラスタメンバーごとに少なくとも 1 つのアドレスが必要でした。マスターは各 PAT プールアドレスを等しいサイズのポートブロックに分割し、それらをクラスタメンバーに配布するようになりました。各メンバーには、同じ PAT アドレスのポートブロックがあります。したがって、通常 PAT に必要な接続量に応じて、PAT プールのサイズを 1 つの IP アドレスにまで減らすことができます。ポートブロックは、1024 ～ 65535 の範囲で 512 ポートのブロック単位で割り当てられます。オプションで、PAT プールルールを設定するときに、このブロック割り当てに予約ポート 1 ー 1023 を含めることができます。たとえば、単一ノードでは PAT プール IP アドレスあたり 65535 個の接続すべてを処理するのに対し、4 ノードクラスタでは、各ノードは 32 個のブロックを取得し、PAT プール IP アドレスあたり 16384 個の接続を処理できます。 この変更の一環として、スタンドアロンまたはクラスタ内での動作に関わりなく、すべてのシステムの PAT プールは、フラットなポート範囲 1023 ー 65535 を使用できるようになりました。以前は、**flat** オプションを PAT プールルールに含めることで、フラットな範囲をオプションで使用できました。**flat** キーワードはサポートされなくなりました。PAT プールは常にフラットになります。**include-reserve** キーワードは、以前は **flat** のサブキーワードでしたが、PAT プール構成内の独立したキーワードになりました。このオプションを使用すると、PAT プール内に 1 ー 1023 のポート範囲を含めることができます。 ポートブロック割り当てを設定する（**block-allocation** PAT プールオプション）と、デフォルトの 512 ポートブロックではなく、独自のブロック割り当てサイズが使用されます。また、クラスタ内のシステムの PAT プールに拡張 PAT を設定することはできません。 新規/変更されたコマンド：**nat**、**show nat pool** 新規/変更された画面：[NAT PAT Pool configuration]
新規インストールでは、デフォルトで XDMCP インスペクションが無効になっています。	以前は、すべてのトラフィックに対して XDMCP インスペクションがデフォルトで有効になっていました。新しいシステムと再イメージ化されたシステムを含む新規インストールでは、XDMCP はデフォルトで無効になっています。このインスペクションが必要な場合は、有効にしてください。アップグレードでは、デフォルトのインスペクション設定を使用して XDMCP インスペクションを有効にしただけでも、XDMCP インスペクションの現在の設定は保持されます。
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
フェールオーバー遅延の無効化	ブリッジグループまたは IPv6 DAD を使用する場合、フェールオーバーが発生すると、新しいアクティブユニットは、スタンバイユニットがネットワーキングタスクを完了してスタンバイ状態に移行するまで、最大3000ミリ秒待機します。その後、アクティブユニットはトラフィックの受け渡しを開始できます。この遅延を回避するために、待機時間を無効にすると、スタンバイユニットが移行する前にアクティブユニットがトラフィックの受け渡しを開始します。 新規/変更されたコマンド： **failover wait-disable** 新規または変更された画面：**[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[Failover]** > **[Enable switchover waiting for peer state]**
ルーティング機能	
マルチキャスト IGMP インターフェイスの状態制限の 500 から 5000 への引き上げ	マルチキャスト IGMP インターフェイスの状態制限が 500 から 5000 に引き上げられました。 新規/変更されたコマンド： **igmp limit** ASDM サポートはありません。 *9.12(4)* でも同様です。
インターフェイス機能	
シングルコンテキストモード用の一意の MAC アドレスの生成に関する ASDM のサポート	ASDM でシングルコンテキストモードの VLAN サブインターフェイス用に一意の MAC アドレスを生成することを有効にできるようになりました。通常、サブインターフェイスはメイン インターフェイスと同じ MAC アドレスを共有します。IPv6 リンクローカル アドレスは MAC アドレスに基づいて生成されるため、この機能により一意の IPv6 リンクローカル アドレスが許可されます。ASA 9.8(3)、9.8(4)、および 9.9(2) で CLI のサポートが追加された。 新規/変更された画面：**[Configuration]** > **[Device Setup]** > **[Interface Settings]** > **[Interfaces]**
DDNS の Web 更新方式のサポート	DDNS の Web 更新方式を使用するようにインターフェイスを設定できるようになりました。 新規/変更されたコマンド： **show ddns update interface**、**show ddns update method**、**web update-url**、**web update-type** 新規/変更された画面：**[Configuration]** > **[Device Management]** > **[DNS]** > **[Dynamic DNS]**
証明書の機能	

機能	説明
スタティック CRL 分散ポイント URL をサポートするための match certificate コマンドの変更	静的 CDP URL コンフィギュレーション コマンドでは、CDP を検証中のチェーン内の各証明書に一意にマッピングできます。ただし、このようなマッピングは各証明書で 1 つだけサポートされていました。今回の変更で、静的に設定された CDP を認証用の証明書チェーンにマッピングできるようになりました。 新規/変更されたコマンド：**match certificate override cdp**、
管理およびトラブルシューティングの機能	
SDI AAA サーバーグループで使用するノードシークレットファイルの RSA Authentication Manager からの手動インポート。	SDI AAA サーバーグループで使用するために RSA Authentication Manager からエクスポートしたノードシークレットファイルをインポートできます。 次のコマンドが追加されました。**aaa sdi import-node-secret**、**clear aaa sdi node-secret**、**show aaa sdi node-secrets**。 次の画面が追加されました。**[Configuration]** > **[Device Management]** > **[Users/AAA]** > **[AAA SDI]**。
show fragment コマンドの出力の拡張	**show fragment** コマンドの出力が拡張され、IP フラグメント関連のドロップとエラーカウンタが含まれるようになりました。 変更されたコマンドはありません。 変更された画面はありません
show tech-support コマンドの出力の拡張	**show tech-support** コマンドの出力が拡張され、暗号アクセラレータに設定されたバイアスが含まれるようになりました。バイアス値は ssl、ipsec、または balanced になります。 変更されたコマンドはありません。 変更された画面はありません
モニタリング機能	
cplane キープアライブ ホールドタイム値の設定のサポート	高い CPU 使用率によって通信が遅延するため、キープアライブイベントへの応答が ASA に到達できず、カード障害によるフェールオーバーが発生します。キープアライブタイムアウト期間と最大キープアライブカウンタ値を設定して、十分な時間と再試行が行われるようにできます。 新規/変更されたコマンド： **service-module** 次の画面を追加しました。**[Configuration]** > **[Device Management]** > **[Service Module Settings]**
VPN 機能	

機能	説明
ネゴシエーション中のSAの絶対値としての最大数設定に対するサポート	ネゴシエーション中の SA の最大数を絶対値として 15000 まで、または最大デバイスキャパシティから得られる最大値を設定できるようになりました（以前はパーセンテージのみが許可されていました）。 新規/変更されたコマンド： **crypto ikev2 limit max-in-negotiation-sa value** ASDM サポートはありません。 *9.12(4)* でも同様です。
WebVPN ハンドラのクロスサイト リクエスト フォージェリ（CSRF）の脆弱性の防止	ASA は、WebVPN ハンドラの CSRF 攻撃に対する保護を提供します。CSRF 攻撃が検出されると、警告メッセージでユーザーに通知します。この機能は、デフォルトで有効にされています。
Kerberos Constrained Delegation（KCD）のケルベロスサーバーの検証	KCD 用に設定されている場合、ASA は Kerberos キーを取得するために、設定されたサーバーとの AD ドメイン参加を開始します。これらのキーは、ASA がクライアントレス SSL VPN ユーザーに代わってサービスチケットを要求するために必要です。必要に応じて、ドメイン参加時にサーバーのアイデンティティを検証するように ASA を設定できます。 **kcd-server** コマンドを変更し、**validate-server-certificate** キーワードを追加しました。 次の画面を変更しました。 **[Configuration]** > **[Remote Access VPN]** > **[Clientless SSL VPN Access]** > **[Advanced]** > **[Microsoft KCD Server]**

バージョン 9.14 の新機能

ASA 9.14(4)/ASDM 7.17(1) の新機能

リリース日：2022 年 2 月 2 日

このリリースに新機能はありません。

ASA 9.14(3)/ASDM 7.15(1.150) の新機能

リリース：2021 年 6 月 15 日

このリリースに新機能はありません。

ASA 9.14(2) の新機能

リリース：**2020 年 11 月 9 日**

機能	説明
SNMP 機能	
サイト間 VPN 経由の SNMP ポーリング	サイト間 VPN 経由のセキュアな SNMP ポーリングの場合、VPN 設定の一部として外部インターフェイスの IP アドレスを暗号マップアクセスリストに含めます。

ASA 9.14(1.30) の新機能

リリース：**2020 年 9 月 23 日**

機能	説明
ライセンシング機能	
ASAv100 永続ライセンス予約	ASAv100 で製品 ID L-ASAV100SR-K9= を使用した永続ライセンス予約がサポートされるようになりました。**注**：すべてのアカウントが永続ライセンス予約について承認されているわけではありません。

ASDM 7.14(1.48) の新機能

リリース日：**2020 年 4 月 30 日**

機能	説明
プラットフォーム機能	
ASA 9.12 以前について、ASA 5512-X、5515-X、5585-X、および ASASM に対するサポートが復活	この ASDM リリースでは、9.12 以前を実行している場合、ASA 5512-X、5515-X、5585-X、および ASASM に対するサポートが復活しました。これらのモデルの最終 ASA バージョンは 9.12 です。元の 7.13(1) リリースと 7.14(1) リリースでは、これらのモデルでの後方互換性がブロックされていましたが、このバージョンでは互換性が復活しています。

ASA 仮想 9.14(1.6) の新機能

リリース日：**2020 年 4 月 30 日**

（注） このリリースは、ASA 仮想 でのみサポートされています。

機能	説明
プラットフォーム機能	
ASAv100 プラットフォーム	ASA 仮想 仮想プラットフォームに、20 Gbps のファイアウォール スループット レベルを提供するハイエンド パフォーマンス モデルの ASAv100 が追加されました。ASAv100 はサブスクリプションベースのライセンスで、期間は 1 年、3 年、または 5 年です。 ASAv100 は、VMware ESXi および KVM でのみサポートされます。

ASA 9.14(1)/ASDM 7.14(1) の新機能

リリース日：**2020 年 4 月 6 日**

機能	説明
プラットフォーム機能	
Firepower 4112 用の ASA	Firepower 4112 用の ASA を導入しました。 変更されたコマンドはありません。 変更された画面はありません。 （注） FXOS 2.8(1) が必要です。
ファイアウォール機能	
show access-list の出力でポート番号を表示できる。	**show access-list** コマンドに数値キーワードが追加されました。これを使用すると、アクセス制御エントリの名前ではなくポート番号を表示できます。たとえば、www の代わりに 80 を表示できます。
object-group icmp-type コマンドが非推奨になった。	**object-group icmp-type** コマンドは、このリリースでも引き続きサポートされますが、推奨されず、将来のリリースで削除される可能性があります。すべての ICMP タイプのオブジェクトをサービス オブジェクト グループに変更し（**object-group service**）、オブジェクト内で **service icmp** を指定してください。

機能	説明
Kerberos キー発行局（KDC）認証。	Kerberos キー配布局（KDC）からキータブファイルをインポートできます。システムは、Kerberos サーバーを使用してユーザーを認証する前にサーバーがスプーフィングされていないことを認証できます。KDC 認証を実行するには、Kerberos KDC で**ホスト/*ASA_hostname***サービスプリンシパル名（SPN）を設定してから、その SPN のキータブをエクスポートする必要があります。その後に、キータブを ASA にアップロードし、KDC を検証するように Kerberos AAA サーバーグループを設定する必要があります。 新規/変更されたコマンド：**aaa kerberos import-keytab**、**clear aaa kerberos keytab**、**show aaa kerberos keytab**、**validate-kdc** 新規/変更された画面：**[構成（Configuration）] > [デバイス管理（Device Management）] > [ユーザー/AAA（Users/AAA）] > [AAA Kerberos]**、**[構成（Configuration）] > [デバイス管理（Device Management）] > [ユーザー/AAA（Users/AAA）] > [AAAサーバーグループ（AAA Server Groups）]**Kerberos サーバーグループの [追加/編集（Add/Edit）] ダイアログボックス。
ハイ アベイラビリティとスケーラビリティの各機能	
データユニットとの設定の並列同期	制御ユニットでは、デフォルトで設定変更がデータユニットと同時に同期化されるようになりました。以前は、順番に同期が行われていました。 新規/変更されたコマンド： **config-replicate-parallel** 新規/変更された画面：**[Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster] > [Cluster Configuration] > [Enable parallel configuration replicate]** チェックボックス
クラスタへの参加失敗や削除のメッセージが、以下に追加されました。 **show cluster history**	クラスタユニットがクラスタへの参加に失敗した場合や、クラスタを離脱した場合の新しいメッセージが、 **show cluster history** コマンドに追加されました。 新規/変更されたコマンド： **show cluster history** 変更された画面はありません。
インターフェイス機能	
Firepower 1000 および 2100 の 1GB ファイバインターフェイスで速度の自動ネゴシエーションを無効にできる	自動ネゴシエーションを無効にするように Firepower 1100 または 2100 SFP インターフェイスを設定できるようになりました。10GB インターフェイスの場合、自動ネゴシエーションなしで速度を 1GB に設定できます。速度が 10 GB に設定されているインターフェイスの自動ネゴシエーションは無効にできません。 新規/変更されたコマンド： **speed nonegotiate** 新規/変更された画面：**[構成（Configuration）] > [デバイスの設定（Device Settings）] > [インターフェイス（Interfaces）] > [インターフェイスの編集（Edit Interface）] > [ハードウェアプロパティの構成（Configure Hardware Properties）] > [速度（Speed）]**
管理およびトラブルシューティングの機能	

機能	説明
新しい **connection-data-rate** コマンド	この **connection-data-rate** コマンドは、ASA での個別接続のデータレートの概要を提供するために導入されました。このコマンドを有効にすると、フローごとのデータレートが既存の接続情報とともに提供されます。この情報は、高いデータレートの望ましくない接続を識別してブロックし、最適な CPU 使用率を確保するために役立ちます。 新規/変更されたコマンド：**conn data-rate**、**show conn data-rate**、**show conn detail**、**clear conn data-rate** 変更された画面はありません。
HTTPS アイドルタイムアウトの設定	ASDM、WebVPN、および他のクライアントを含む、ASA へのすべての HTTPS 接続のアイドルタイムアウトを設定できるようになりました。これまでは、**http server idle-timeout** コマンドを使用して ASDM アイドルタイムアウトを設定することしかできませんでした。両方のタイムアウトを設定した場合は、新しいコマンドによる設定が優先されます。 新規/変更されたコマンド： **http connection idle-timeout** 新規/変更された画面：**[構成（Configuration）] > [デバイス管理（Device Management）] > [管理アクセス（Management Access）] > [ASDM/HTTPS/Telnet/SSH] > [HTTP設定（HTTP Settings）] > [接続アイドルタイムアウト（Connection Idle Timeout）]** チェックボックス。
NTPv4 のサポート	ASA が NTPv4 をサポートするようになりました。 変更されたコマンドはありません。 変更された画面はありません。
新しい **clear logging counter** コマンド	**show logging** コマンドは、ASA で設定された各ロギングカテゴリについてログに記録されたメッセージの統計を提供します。**clear logging counter** コマンドは、ログに記録されたカウンタと統計をクリアするために導入されました。 新規/変更されたコマンド： **clear logging counter** 変更された画面はありません。
アプライアンスモードの Firepower 1000 および 2100 での FXOS のデバッグコマンドの変更	**debug fxos_parser** コマンドは簡素化され、FXOS に関して一般に使用されるトラブルシューティングメッセージを提供するようになりました。その他の FXOS デバッグコマンドは、**debug menu fxos_parser** コマンドの下に移動されました。 新規/変更されたコマンド：**debug fxos_parser**、**debug menu fxos_parser** 変更された画面はありません。

機能	説明
show tech-support コマンドの拡張	**show ssl objects** コマンドと **show ssl errors** コマンドが **show tech-support** コマンドの出力に追加されました。 新規/変更されたコマンド： **show tech-support** 変更された画面はありません。 *9.12(4)* でも同様です。
モニタリング機能	
Net-SNMP バージョン 5.8 のサポート	ASA は Net-SNMP（IPv4 と IPv6 の両方を使用して SNMP v1、SNMP v2c、および SNMP v3 を実装するために使用されるアプリケーションスイート）を使用しています。 変更されたコマンドはありません。 新規/変更された画面：**[構成（Configuration）] > [デバイス管理（Device Management）] > [管理アクセス（Management Access）] > [SNMP]**
SNMP の MIB および OID	ASA は、CISCO-REMOTE-ACCESS-MONITOR-MIB のサポートを拡張し、SNMP を介して RADIUS からの認証の拒否/失敗を追跡します。この機能により、次の 3 つの SNMP OID が実装されます。 • crasNumTotalFailures（失敗の総数） • crasNumSetupFailInsufResources（AAA およびその他の内部エラー） • crasNumAbortedSessions（中断されたセッション）オブジェクト ASA は、Advanced Encryption Standard（AES）暗号アルゴリズムのサポートを提供します。この機能により、次の SNMP OID が実装されます。 • usmAesCfb128Protocol • usmNoPrivProtocol
SNMPv3 認証	ユーザー認証に SHA-256 HMAC を使用できるようになりました。 新規/変更されたコマンド：**snmp-server user** 新規/変更された画面：**[構成（Configuration）] > [デバイス管理（Device Management）] > [管理アクセス（Management Access）] > [SNMP]**
debug telemetry 表示されていません。	**debug telemetry** コマンドを使用すると、テレメトリに関連するデバッグメッセージが表示されます。このデバッグは、テレメトリレポートの生成時にエラーの原因を特定するために役立ちます。 新規/変更されたコマンド：**debug telemetry**、**show debug telemetry** 変更された画面はありません。

機能	説明
VPN 機能	
VTI での DHCP リレーサーバーのサポート	DHCP リレーサーバーを設定して、VTI トンネルインターフェイスを介して DHCP メッセージを転送できるようになりました。 新規/変更されたコマンド：**dhcprelay server** 新規/変更された画面：**[構成（Configuration）] > [デバイス管理（Device Management）] > [DHCP] > [DHCPリレー（DHCP Relay）]**
複数ピアクリプトマップの IKEv2 サポート	複数ピアクリプトマップで IKEv2 を設定できるようになりました。トンネル内のピアがダウンすると、IKEv2 はリスト内の次のピアで SA の確立を試みます。 変更されたコマンドはありません。 新規/変更された画面：**[構成（Configuration）] > [サイト間VPN（Site-to-Site VPN）] > [詳細設定（Advanced）] > [クリプトマップ（Crypto Maps）] > [IPsecルールの作成/編集（Create / Edit IPsec Rule）] > [トンネルポリシー（クリプトマップ）- 基本（Tunnel Policy (Crypto Map) - Basic）]**
複数証明書認証のユーザー名オプション	複数証明書認証で、1 つの証明書（マシン証明書）または 2 つ目の証明書（ユーザー証明書）のどちらからの属性を AAA 認証に使用するのかを指定できるようになりました。 新規/変更されたコマンド：**username-from-certificate-choice**、**secondary-username-from-certificate-choice** 新規/変更された画面： • **[接続プロファイル（Connection Profile）] > [詳細設定（Advanced）] > [認証（Authentication）]** • **[接続プロファイル（Connection Profile）] > [詳細設定（Advanced）] > [セカンダリ認証（Secondary Authentication）]**

バージョン 9.13 の新機能

ASDM 7.13(1.101) の新機能

リリース日：**2020 年 5 月 7 日**

機能	説明
プラットフォーム機能	

機能	説明
ASA 9.12 以前について、ASA 5512-X、5515-X、5585-X、および ASASM に対するサポートが復活	この ASDM リリースでは、9.12 以前を実行している場合、ASA 5512-X、5515-X、5585-X、および ASASM に対するサポートが復活しました。これらのモデルの最終 ASA バージョンは 9.12 です。元の 7.13(1) リリースと 7.14(1) リリースでは、これらのモデルでの後方互換性がブロックされていましたが、このバージョンでは互換性が復活しています。

ASA 9.13(1)/ASDM 7.13(1）の新機能

リリース：**2019 年 9 月 25 日**

機能	説明
プラットフォーム機能	
Firepower 1010 用の ASA	Firepower 1010 用の ASA を導入しました。このデスクトップモデルには、組み込みハードウェアスイッチと Power on Ethernet+（PoE+）のサポートが含まれています。 新規/変更されたコマンド：**boot system**、**clock timezone**、**connect fxos admin**、**forward interface**、**interface vlan**、**power inline**、**show counters**、**show environment**、**show interface**、**show inventory**、**show power inline**、**show switch mac-address-table**、**show switch vlan**、**switchport**、**switchport access vlan**、**switchport mode**、**switchport trunk allowed vlan** 新しい/変更された画面： • **[Configuration]** > **[Device Setup]** > **[Interface Settings]** > **[Interfaces]** > **[Edit]** > **[Switch Port]** • **[Configuration]** > **[Device Setup]** > **[Interface Settings]** > **[Interfaces]** > **[Edit]** > **[Power Over Ethernet]** • **[Configuration]** > **[Device Setup]** > **[Interface Settings]** > **[Interfaces]** > **[Add VLAN Interface]** • **[Configuration]** > **[Device Management]** > **[System Image/Configuration]** > **[Boot Image/Configuration]** • **[Configuration]** > **[Device Setup]** > **[System Time]** > **[Clock]** • **[Monitoring]** > **[Interfaces]** > **[L2 Switching]** • **[Monitoring]** > **[Interfaces]** > **[Power Over Ethernet]**

機能	説明
Firepower 1120、1140、および 1150 用の ASA	Firepower 1120、1140、および 1150 用の ASA を導入しました。 新規/変更されたコマンド：**boot system**、**clock timezone**、**connect fxos admin**、**show counters**、**show environment**、**show interface**、**show inventory** 新しい/変更された画面： • **[Configuration]** > **[Device Management]** > **[System Image/Configuration]** > **[Boot Image/Configuration]** • **[Configuration]** > **[Device Setup]** > **[System Time]** > **[Clock]**
Firepower 2100 アプライアンス モード	Firepower 2100 は、Firepower eXtensible Operating System（FXOS）という基礎となるオペレーティング システムを実行します。Firepower 2100 は、次のモードで実行できます。 • アプライアンス モード（現在はデフォルト）：アプライアンス モードでは、ASA のすべての設定を行うことができます。FXOS CLI からは、高度なトラブルシューティング コマンドのみ使用できます。 • プラットフォーム モード：プラットフォーム モードでは、FXOS で、基本的な動作パラメータとハードウェア インターフェイスの設定を行う必要があります。これらの設定には、インターフェイスの有効化、EtherChannels の確立、NTP、イメージ管理などが含まれます。シャーシマネージャ Web インターフェイスまたは FXOS CLI を使用できます。その後、ASDM または ASA CLI を使用して ASA オペレーティング システムにセキュリティ ポリシーを設定できます。 9.13(1）にアップグレードしている場合、モードはプラットフォーム モードのままになります。 新規/変更されたコマンド：**boot system**、**clock timezone**、**connect fxos admin**、**fxos mode appliance**、**show counters**、**show environment**、**show fxos mode**、**show interface**、**show inventory** 新しい/変更された画面： • **[Configuration]** > **[Device Management]** > **[System Image/Configuration]** > **[Boot Image/Configuration]** • **[Configuration]** > **[Device Setup]** > **[System Time]** > **[Clock]**
DHCP の予約	ASA DHCP サーバーが DHCP の予約をサポートするようになりました。クライアントの MAC アドレスに基づいて、定義されたアドレスプールから DHCP クライアントにスタティック IP アドレスを割り当てることができます。 新規/変更されたコマンド： **dhcpd reserve-address** 変更された画面はありません。

機能	説明
ASA 仮想 最小メモリ要件	ASA 仮想 の最小メモリ要件は 2GB です。現在の ASA 仮想 が 2GB 未満のメモリで動作している場合、ASA 仮想 VM のメモリを増やすことなく、以前のバージョンから 9.13(1)にアップグレードすることはできません。また、バージョン 9.13(1) を使用して新しい ASA 仮想 VM を再展開することもできます。 変更されたコマンドはありません。 変更された画面はありません。
ASA 仮想 MSLA サポート	ASA 仮想 は、シスコのマネージド サービス ライセンス契約（MSLA）プログラムをサポートしています。このプログラムは、マネージド ソフトウェア サービスをサードパーティに提供するシスコのお客様およびパートナー向けに設計された、ソフトウェアのライセンスおよび消費のフレームワークです。 MSLA はスマートライセンスの新しい形式で、ライセンス スマート エージェントは時間単位でライセンス権限付与の使用状況を追跡します。 新規/変更されたコマンド：**license smart**、**mode**、**utility**、**custom-id**、**custom-info**、**privacy**、**transport type**、**transport url**、**transport proxy** 新規/変更された画面：**[Configuration]** > **[Device Management]** > **[Licensing]** > **[Smart Licensing]**。
ASA 仮想 柔軟なライセンス	すべての ASA 仮想 ライセンスは、サポートされているすべての ASA 仮想 vCPU/メモリ構成で使用できるようになりました。セキュアクライアント および TLS プロキシのセッション制限は、モデルタイプに関連付けられたプラットフォーム制限ではなく、インストールされた ASA 仮想 プラットフォームの権限付与によって決まります。 新規/変更されたコマンド： **show version**、**show vm**、**show cpu**、**show license features** 新規/変更された画面：**[Configuration]** > **[Device Management]** > **[Licensing]** > **[Smart Licensing]**。
AWS の ASA 仮想 での C5 インスタンスのサポート。C4、C3、および M4 インスタンスの拡張サポート	AWS パブリッククラウド上の ASA 仮想 は、C5 インスタンスをサポートするようになりました（c5.large、c5.xlarge、および c5.2xlarge）。 さらに、C4 インスタンス（c4.2xlarge および c4.4xlarge）、C3 インスタンス（c3.2xlarge、c3.4xlarge、および c3.8xlarge）および M4 インスタンス（m4.2xlarge および m4.4xlarge）のサポートが拡張されました。 変更されたコマンドはありません。 変更された画面はありません。

機能	説明
より多くの Azure 仮想マシンサイズをサポートする Microsoft Azure の ASA 仮想	Microsoft Azure パブリッククラウドの ASA 仮想 は、より多くの Linux 仮想マシンサイズをサポートするようになりました。 • Standard_D4、Standard_D4_v2 • Standard_D8_v3 • Standard_DS3、Standard_DS3_v2 • Standard_DS4、Standard_DS4_v2 • Standard_F4、Standard_F4s • Standard_F8、Standard_F8s 以前のリリースでは、Standard_D3 と Standard_D3_v2 のサイズのみがサポートされていました。 変更されたコマンドはありません。 変更された画面はありません。
DPDK の ASA 仮想 拡張サポート	ASA 仮想 は、Data Plane Development Kit（DPDK）の拡張機能をサポートして、複数の NIC キューのサポートを有効にします。これにより、マルチコア CPU はネットワーク インターフェイスに同時に効率よくサービスを提供できるようになります。 これは、Microsoft Azure と Hyper-v を除くすべての ASA 仮想 ハイパーバイザに適用されます。 （注） DPDK のサポートは、リリース ASA 9.10 (1)/ASDM 7.13(1) で導入されました。 変更されたコマンドはありません。 変更された画面はありません。
VMware ESXi 6.7 用の ASA 仮想 サポート	ASA 仮想 仮想プラットフォームは、VMware ESXi 6.7 で動作するホストをサポートしています。*vi.ovf* および *esxi.ovf* ファイルに新しい VMware ハードウェア バージョンが追加され、ESXi 6.7 で ASA 仮想 の最適なパフォーマンスと使いやすさを実現しました。 変更されたコマンドはありません。 変更された画面はありません。
ISA 3000 の VLAN 数の増加	Security Plus ライセンスが有効な ISA 3000 について、最大 VLAN 数が 25 から 100 に増えました。
ファイアウォール機能	

機能	説明
モバイル端末の場所のロギング（GTP インスペクション）	GTP インスペクションを設定すると、モバイル端末の初期の場所とそれ以降の場所の変更をログに記録できます。場所の変更を追跡すると、不正なローミング請求を識別するのに役立つ場合があります。 新規/変更されたコマンド：**location-logging** 新規/変更された画面：**[Configuration]** > **[Firewall]** > **[Objects]** > **[Inspect Maps]** > **[GTP]**。
GTPv2 および GTPv1 リリース 15 がサポートされています。	システムで GTPv2 3GPP 29.274 V15.5.0 がサポートされるようになりました。GTPv1 の場合、3GPP 29.060 V15.2.0 までサポートしています。新しいサポートでは、2 件のメッセージおよび 53 件の情報要素の認識が追加されています。 変更されたコマンドはありません。 変更された画面はありません。
アドレスとポート変換のマッピング（MAP-T）	アドレスとポートのマッピング (MAP) は、主にサービスプロバイダー (SP) ネットワークで使用する機能です。サービス プロバイダーは、IPv6 専用ネットワーク、MAP ドメインを稼働でき、同時に、IPv4 専用のサブスクライバをサポートし、パブリック インターネット上の IPv4 専用サイトとの通信ニーズに対応します。MAP は、RFC7597、RFC7598、および RFC7599 で定義されています。 新規/変更されたコマンド：**basic-mapping-rule**、**default-mapping-rule**、**ipv4-prefix**、**ipv6-prefix**、**map-domain**、**share-ratio**、**show map-domain**、**start-port** 新規/変更されたコマンド：**[Configuration]** > **[Device Setup]** > **cgnat map**、**[Monitoring]** > **[Properties]** > **[Map Domains]**
グループごとの AAA サーバーグループとサーバーの制限が増えました。	より多くの AAA サーバー グループを設定できます。シングルコンテキストモードでは、200 個の AAA サーバーグループを設定できます（以前の制限は 100）。マルチコンテキストモードでは、8 個設定できます（以前の制限は 4）。 さらに、マルチコンテキストモードでは、グループごとに 8 台のサーバーを設定できます（以前の制限はグループごとに 4 台のサーバー）。シングル コンテキストモードのグループごとの制限の 16 は変更されていません。 これらの新しい制限を受け入れるために、次のコマンドが変更されました。**aaa-server**、**aaa-server host** これらの新しい制限を受け入れるために、AAA 画面が変更されました。
SCCP（Skinny）インスペクションでは、TLS プロキシが廃止されました。	**tls-proxy** キーワード、および SCCP/Skinny 暗号化インスペクションのサポートは廃止されました。このキーワードは今後のリリースで **inspect skinny** コマンドから削除される予定です。
VPN 機能	

機能	説明
クライアントとしての WebVPN の HSTS サポート	http-headers と呼ばれる WebVPN モードの新しい CLI モードが追加され、WebVPN は、HTTP 参照を HSTS であるホストの HTTPS 参照に変換できるようになりました。ASA からブラウザへの WebVPN 接続用にこのヘッダーを送信する場合、ユーザー エージェントがリソースの埋め込みを許可するかどうかを設定します。 http-headers は次のように設定することも選択できます。**x-content-type-options**、**x-xss-protection**、**hsts-client**（クライアントとしての WebVPN の HSTS サポート）、**hsts-server**、または **content-security-policy**。 新規/変更されたコマンド：**webvpn**、**show webvpn hsts host (name <hostname&s{253}> | all)**、および **clear webvpn hsts host (name <hostname&s{253}> | all)**。 新規/変更された画面：**[Configuration]** > **[Remote Access VPN]** > **[Clientless SSL VPN Access]** > **[Advanced]** > **[Proxies]**。
キー交換用に追加された Diffie-Hellman グループ 15 および 16	Diffie-Hellman グループ 15 および 16 のサポートを追加するために、これらの新しい制限を受け入れるようにいくつかの **crypto** コマンドが変更されました。 **crypto ikev2 policy <index> group <number>** および **crypto map <map-name> <map-index> set pfs <group>.**
show asp table vpn-context 出力の機能強化	デバッグ機能を強化するために、次の VPN コンテキスト カウンタが出力に追加されました。 Lock Err、No SA、IP Ver Err、および Tun Down。 新しい/変更されたコマンド：**show asp table vpn-context**（出力のみ）。
リモートアクセス VPN の最大セッション制限に達した場合の即時セッション確立	ユーザーが最大セッション（ログイン）制限に達すると、システムはユーザーの最も古いセッションを削除し、削除が完了するのを待ってから新しいセッションを確立します。これにより、最初の試行でユーザーが正常に接続できなくなる可能性があります。この遅延を削除し、削除の完了を待たずにシステムに新しい接続を確立させることができます。 新規/変更されたコマンド：**vpn-simultaneous-login-delete-no-delay** 新規/変更された画面：**[Configuration]** > **[Remote Access VPN]** > **[Network (Client) Access]** > **[Group Policies]**、[Add/Edit] ダイアログボックス、**[General]**タブ
ハイ アベイラビリティとスケーラビリティの各機能	
デッド接続検出（DCD）の発信側および応答側の情報、およびクラスタ内の DCD のサポート。	デッド接続検出（DCD）を有効にした場合は、**show conn detail** コマンドを使用して発信側と応答側に関する情報を取得できます。デッド接続検出を使用すると、非アクティブな接続を維持できます。**show conn** の出力は、エンドポイントがプローブされた頻度が示されます。さらに、DCD がクラスタでサポートされるようになりました。 新しい/変更されたコマンド：**show conn**（出力のみ） 変更された画面はありません。

機能	説明
クラスタのトラフィック負荷のモニター	クラスタ メンバのトラフィック負荷をモニターできるようになりました。これには、合計接続数、CPU とメモリの使用率、バッファ ドロップなどが含まれます。負荷が高すぎる場合、残りのユニットが負荷を処理できる場合は、ユニットのクラスタリングを手動で無効にするか、外部スイッチのロードバランシングを調整するかを選択できます。この機能は、デフォルトでイネーブルにされています。 新規/変更されたコマンド：**debug cluster load-monitor**、**load-monitor**、**show cluster info load-monitor** 新しい/変更された画面： • **[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[ASA Cluster]** > **[Cluster Configuration]** > **[Enable Cluster Load Monitor]** チェックボックス • **[Monitoring]** > **[ASA Cluster]** > **[Cluster Load-Monitoring]**
クラスタ結合の高速化	データユニットが制御ユニットと同じ設定の場合、設定の同期をスキップし、結合を高速化します。この機能は、デフォルトでイネーブルにされています。この機能はユニットごとに設定され、制御ユニットからデータユニットには複製されません。 （注） 一部の設定コマンドは、クラスタ結合の高速化と互換性がありません。これらのコマンドがユニットに存在する場合、クラスタ結合の高速化が有効になっていても、設定の同期は常に発生します。クラスタ結合の高速化を動作させるには、互換性のない設定を削除する必要があります。**show cluster info unit-join-acceleration incompatible-config** を使用して、互換性のない設定を表示します。 新規/変更されたコマンド：**unit join-acceleration**、**show cluster info unit-join-acceleration incompatible-config** 新規/変更された画面：**[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[ASA Cluster]** > **[Cluster Configuration]** > **[Enable config sync accelleration]** チェックボックス
ルーティング機能	
SMTP 設定の機能強化	必要に応じて、プライマリおよびバックアップインターフェイス名を指定してSMTPサーバーを設定することで、ロギングに使用するルーティングテーブル（管理ルーティング テーブルまたはデータ ルーティング テーブル）を識別するためにASAを有効にできます。インターフェイスが指定されていない場合、ASAは管理ルーティングテーブルルックアップを参照し、適切なルートエントリが存在しない場合は、データ ルーティング テーブルを参照します。 新規/変更されたコマンド： **smtp-server [primary-interface][backup-interface]**

機能	説明
NSF 待機タイマーを設定するためのサポート	OSPF ルータは、すべてのネイバーがパケットに含まれているか不明な場合、Hello パケットにアタッチされている EO-TLV に RS ビットを設定することが期待されています。また、隣接関係（アジャセンシー）を維持するためにはルータの再起動が必要です。ただし、RS ビット値は RouterDeadInterval 秒より長くすることはできません。**timers nsf wait** コマンドは、Hello パケットの RS ビットを RouterDeadInterval 秒未満に設定するために導入されました。 新規/変更されたコマンド： **timers nsf wait**
TFTP ブロックサイズを設定するためのサポート	TFTP ファイル転送用に固定された一般的なブロックサイズは 512 オクテットです。新しいコマンド **tftp blocksize** は、より大きなブロックサイズを設定するために導入されました。これにより、TFTP ファイル転送速度が向上します。513 ～ 8192 オクテットのブロックサイズを設定できます。新しいデフォルトのブロックサイズは 1456 オクテットです。このコマンドの **no** 形式を使用すると、ブロックサイズが古いデフォルト値（512 オクテット）にリセットされます。**timers nsf wait** コマンドは、Hello パケットの RS ビットを RouterDeadInterval 秒未満に設定するために導入されました。 新規/変更されたコマンド： **tftp blocksize**
証明書の機能	
FIPS ステータスを表示するためのサポート	**show running-configuration fips** コマンドは、FIPS が有効になっているときにのみ、FIPS のステータスを表示していました。動作状態を確認するために、**show fips** コマンドが導入されました。このコマンドは、ユーザーが無効状態または有効状態になっている FIPS を有効または無効にしたときに、FIPS のステータスを表示します。このコマンドは、有効化または無効化アクションの後にデバイスを再起動するためのステータスも表示します。 新規/変更されたコマンド： **show fips**
CRL キャッシュサイズの拡張	大規模な CRL ダウンロードの失敗を防ぐため、キャッシュサイズを拡張し、また、個別の CRL 内のエントリ数の制限を取り除きました。 • マルチ コンテキスト モードの場合、コンテキストごとの合計 CRL キャッシュサイズが 16 MB に増加しました。 • シングル コンテキスト モードの場合、合計 CRL キャッシュサイズが 128 MB に増加しました。

機能	説明
CRL 分散ポイント コマンドの変更	スタティック CDP URL コンフィギュレーション コマンドが削除され、match certificate コマンドに移行しました。 新規/変更されたコマンド：**crypto-ca-trustpoint crl** と **crl url** はその他の関連ロジックで削除され、**match-certificate override-cdp** が導入されました。 新規/変更された画面：**[Configuration]** > **[Device Management]** > **[Certificate Management]** > **[CA Certificates]** スタティック CDP URL は 9.13(1)12 で match certificate コマンドに再導入されました。
管理およびトラブルシューティングの機能	
Firepower 1000、 Firepower 2100 アプライアンス モードがライセンス評価モードの場合の管理アクセス	ASA には、管理アクセスのみを対象にした 3DES 機能がデフォルトで含まれているので、Smart Software Manager に接続でき、すぐに ASDM を使用することもできます。後に ASA で SSH アクセスを設定する場合は、SSH および SCP を使用することもできます。高度な暗号化を必要とするその他の機能（VPN など）では、最初に Smart Software Manager に登録する必要がある高度暗号化が有効になっている必要があります。 （注） 登録する前に高度な暗号化を使用できる機能の設定を試みると（脆弱な暗号化のみ設定している場合でも）、HTTPS 接続はそのインターフェイスでドロップされ、再接続できません。このルールの例外は、管理 1/1 などの管理専用インターフェイスに接続されている場合です。SSH は影響を受けません。HTTPS 接続が失われた場合は、コンソール ポートに接続して ASA を再設定するか、管理専用インターフェイスに接続するか、または高度暗号化機能用に設定されていないインターフェイスに接続することができます。 変更されたコマンドはありません。 変更された画面はありません。

機能	説明
追加の NTP 認証アルゴリズム	以前は、NTP 認証では MD5 だけがサポートされていました。ASA は、次のアルゴリズムをサポートするようになりました。 • MD5 • SHA-1 • SHA-256 • SHA-512 • AES-CMAC 新規/変更されたコマンド： **ntp authentication-key** 新しい/変更された画面： **[Configuration]** > **[Device Setup]** > **[System Time]** > **[NTP]** > **[Add]** ボタン > **[Add NTP Server Configuration]** ダイアログボックス > **[Key Algorithm]** ドロップダウンリスト
Firepower 4100/9300 の ASA Security Service Exchange（SSE）テレメトリ サポート	ネットワークで Cisco Success Network を有効にすると、デバイスの使用状況に関する情報と統計情報がシスコに提供され、テクニカルサポートの最適化に使用されます。ASA デバイスで収集されるテレメトリ データには、CPU、メモリ、ディスク、または帯域幅の使用状況、ライセンスの使用状況、設定されている機能リスト、クラスタ/フェールオーバー情報などが含まれます。 新規/変更されたコマンド：**service telemetry** および **show telemetry** 新しい/変更された画面： • **[Configuration]** > **[Device Management]** > **[Telemetry]** • **[Monitoring]** > **[Properties]** > **[Telemetry]**
事前定義されたリストに応じて最も高いセキュリティから最も低いセキュリティへという順序で SSH 暗号化の暗号を表示	事前定義されたリストに応じて、SSH暗号化の暗号が最も高いセキュリティから最も低いセキュリティへという順序（中または高）で表示されるようになりました。以前のリリースでは、最も低いものから最も高いものへの順序でリストされており、セキュリティが高い暗号よりも低い暗号が先に表示されていました。 新規/変更されたコマンド： **ssh cipher encryption** 新しい/変更された画面： **[Configuration]** > **[Device Management]** > **[Advanced]** > **[SSH Ciphers]**
show tech-support に追加の出力が含まれている	**show tech-support** の出力が強化され、次の出力が表示されるようになりました。 **show flow-offload info detail** **show flow-offload statistics** **show asp table socket** 新しい/変更されたコマンド：**show tech-support**（出力のみ）

機能	説明
ドロップ ロケーション情報を含む **show-capture asp_drop** 出力の機能強化	ASP ドロップ カウンタを使用したトラブルシューティングでは、同じ理由による ASP ドロップがさまざまな場所で使用されている場合は特に、ドロップの正確な位置は不明です。この情報は、ドロップの根本原因を特定する上で重要です。この拡張機能を使用すると、ビルド ターゲット、ASA リリース番号、ハードウェア モデル、および ASLR メモリ テキスト領域などの ASP ドロップの詳細が表示されます（ドロップの位置のデコードが容易になります）。 新規/変更されたコマンド： **show-capture asp_drop**
変更内容 **debug crypto ca**	**debug crypto ca transactions** および **debug crypto ca messages** オプションは、すべての該当するコンテンツを **debug crypto ca** コマンド自体に提供するために統合されています。また、使用可能なデバッグ レベルの数が 14 に削減されました。 新規/変更されたコマンド： **debug crypto ca**
Firepower 1000 および2100 の FXOS 機能	
安全消去	安全消去機能は、SSD 自体で特別なツールを使用してもデータを回復できないように、SSD 上のすべてのデータを消去します。デバイスを使用停止する場合は、FXOS で安全に消去する必要があります。 新規/変更された FXOS コマンド：**erase secure**（local-mgmt） サポートされているモデル：Firepower 1000 および 2100
設定可能な HTTPS プロトコル	FXOS HTTPS アクセス用の SSL/TLS のバージョンを設定できます。 新規/変更された FXOS コマンド： **set https access-protocols** サポートされているモデル：プラットフォーム モードの Firepower 2100
IPSec およびキーリングの FQDN の適用	FXOS では、ピアの FQDN がそのピアによって提示された x.509 証明書の DNS 名と一致する必要があるように、FQDN の適用を設定できます。IPSec の場合、9.13(1) より前に作成された接続を除き、適用はデフォルトで有効になっています。古い接続への適用は手動で有効にする必要があります。キーリングの場合、すべてのホスト名が FQDN である必要があり、ワイルドカードは使用できません。 新規/変更された FXOS コマンド：**set dns**、**set e-mail**、**set fqdn-enforce**、**set ip**、**set ipv6**、**set remote-address**、**set remote-ike-id** 削除されたコマンド：**fi-a-ip**、**fi-a-ipv6**、**fi-b-ip**、**fi-b-ipv6** サポートされているモデル：プラットフォーム モードの Firepower 2100

機能	説明
新しいIPSec暗号とアルゴリズム	FXOS 管理トラフィックを暗号化する IPSec トンネルを設定するために、次の IKE および ESP 暗号とアルゴリズムが追加されました。 • 暗号：aes192。既存の暗号には、aes128、aes256、aes128gcm16 などがあります。 • 疑似乱数関数（PRF)（IKE のみ）：prfsha384、prfsha512、prfsha256。既存の PRF：prfsha1。 • 整合性アルゴリズム：sha256、sha384、sha512、sha1_160。既存のアルゴリズム：sha1。 • Diffie-Hellman グループ：curve25519、ecp256、ecp384、ecp521、modp3072、modp4096。既存のグループ：modp2048。 変更された FXOS コマンドはありません。 サポートされているモデル：プラットフォーム モードの Firepower 2100
SSH 認証の機能拡張	FXOS では、次の SSH サーバー暗号化アルゴリズムが追加されました。 • aes128-gcm@openssh.com • aes256-gcm@openssh.com • chacha20-poly@openssh.com FXOS では、次の SSH サーバーキー交換方式が追加されました。 • diffie-hellman-group14-sha256 • curve25519-sha256 • curve25519-sha256@libssh.org • ecdh-sha2-nistp256 • ecdh-sha2-nistp384 • ecdh-sha2-nistp521 新規/変更された FXOS コマンド：**set ssh-server encrypt-algorithm**、**set ssh-server kex-algorithm** サポートされているモデル：プラットフォーム モードの Firepower 2100
X.509 証明書の EDCS キー	FXOS 証明書に EDCS キーを使用できるようになりました。以前は、RSA キーだけがサポートされていました。 新規/変更された FXOS コマンド：**set elliptic-curve**、**set keypair-type** サポートされているモデル：プラットフォーム モードの Firepower 2100

機能	説明
ユーザー パスワードの改善	次のような FXOS パスワードセキュリティの改善が追加されました。 • ユーザー パスワードには最大 127 文字を使用できます。古い制限は 80 文字でした。 • デフォルトでは、強力なパスワード チェックが有効になっています。 • 管理者パスワードの設定を求めるプロンプトが表示されます。 • パスワードの有効期限切れ。 • パスワード再利用の制限。 • **set change-during-interval** コマンドを削除し、**set change-interval**、**set no-change-interval**、および **set history-count** コマンドの **disabled** オプションを追加しました。 新規/変更された FXOS コマンド：**set change-during-interval**、**set expiration-grace-period**、**set expiration-warning-period**、**set history-count**、**set no-change-interval**、**set password**、**set password-expiration**、**set password-reuse-interval** 新規/変更された [Firepower Chassis Manager] 画面： • [System] > [User Management] > [Local Users] > > • [System] > [User Management] > [Settings] > > サポートされているモデル：プラットフォーム モードの Firepower 2100

バージョン 9.12 の新機能

ASA 9.12(4) の新機能

リリース日：**2020 年 5 月 26 日**

機能	説明
ルーティング機能	
マルチキャスト IGMP インターフェイスの状態制限の 500 から 5000 への引き上げ	マルチキャスト IGMP インターフェイスの状態制限が 500 から 5000 に引き上げられました。 新規/変更されたコマンド： **igmp limit** ASDM サポートはありません。
トラブルシューティング機能	

機能	説明
show tech-support コマンドの拡張	**show ssl objects** コマンドと **show ssl errors** コマンドが **show tech-support** コマンドの出力に追加されました。 新規/変更されたコマンド： **show tech-support** 変更された画面はありません。
VPN 機能	
ネゴシエーション中のSAの絶対値としての最大数設定に対するサポート	ネゴシエーション中の SA の最大数を絶対値として 15000 まで、または最大デバイスキャパシティから得られる最大値を設定できるようになりました（以前はパーセンテージのみが許可されていました）。 新規/変更されたコマンド： **crypto ikev2 limit max-in-negotiation-sa value** ASDM サポートはありません。

ASA 9.12(3) の新機能

リリース日：**2019 年 11 月 25 日**

このリリースに新機能はありません。

ASA 9.12(2)/ASDM 7.12(2) の新機能

リリース日：**2019 年 5 月 30 日**

機能	説明
プラットフォーム機能	
Firepower 9300 SM-56 のサポート	セキュリティ モジュール、SM-56 を導入しました。 FXOS 2.6.1.157 が必要です。 変更されたコマンドはありません。 変更された画面はありません。
管理機能	
SSH キー交換モードの設定は、管理コンテキストに限定されています。	管理コンテキストではSSHキー交換を設定する必要があります。この設定は、他のすべてのコンテキストによって継承されます。 新規/変更されたコマンド： **ssh key-exchange** 新規/変更された画面：**[Configuration] > [Device Management] > [Management Access] > [ASDM/HTTPS/Telnet/SSH] > [SSH Settings] > [DH Key Exchange]**

機能	説明
ASDM 機能	
ASDM の OpenJRE バージョン	OracleJRE ではなく、OpenJRE 1.8.x を使用する ASDM のバージョンをインストールできます。OpenJRE バージョンのファイル名は、**asdm-openjre-***version***.bin** です。
[Tools] > **[Preferences]** オプションで ASA FirePOWER モジュールのローカル管理ファイル フォルダを指定	ASA FirePOWER モジュールのローカル管理ファイルをインストールする場所を指定できるようになりました。設定された場所に対して読み取り/書き込み権限を持っている必要があります。 新規/変更された画面： **[Tools]** > **[Preferences]** > **SFR Location ウィザード**領域

ASA 9.12(1)/ASDM 7.12(1) の新機能

リリース：**2019 年 3 月 13 日**

機能	説明
プラットフォーム機能	
Firepower 4115、4125、および 4145 向け ASA	Firepower 4115、4125、および 4145 が導入されました。 FXOS 2.6.1 が必要です。 変更されたコマンドはありません。 変更された画面はありません。
ASA および脅威に対する防御を同じ Firepower 9300 の別のモジュールでサポート	ASA および 脅威に対する防御 論理デバイスを同じ Firepower 9300 上で展開できるようになりました。 FXOS 2.6.1 が必要です。 変更されたコマンドはありません。 変更された画面はありません。
Firepower 9300 SM-40 および SM-48 のサポート	2 つのセキュリティ モジュール、SM-40 および SM-48 が導入されました。 FXOS 2.6.1 が必要です。 変更されたコマンドはありません。 変更された画面はありません。
ファイアウォール機能	

機能	説明
GTPv1 リリース 10.12 のサポート	システムで GTPv1 リリース 10.12 がサポートされるようになりました。以前は、リリース 6.1 がサポートされていました。新しいサポートでは、25 件の GTPv1 メッセージおよび 66 件の情報要素の認識が追加されています。 さらに、動作の変更もあります。不明なメッセージ ID が許可されるようになりました。以前は、不明なメッセージはドロップされ、ログに記録されていました。 変更されたコマンドはありません。 変更された画面はありません。
Cisco Umbrella の強化	Cisco Umbrella をバイパスする必要があるローカル ドメイン名を特定できるようになりました。これらのドメインの DNS 要求は、Umbrella を処理せず DNS サーバーに直接送信されます。また、DNS 要求の解決に使用する Umbrella サーバーも特定できるようになりました。さらに、Umbrella サーバーを使用できない場合は、DNS 要求がブロックされないように、Umbrella インスペクション ポリシーをフェールオープンに定義することができます。 新規/変更されたコマンド：**local-domain-bypass**、**resolver**、**umbrella fail-open** 新規/変更された画面：**[Configuration]** > **[Firewall]** > **[Objects]** > **[Umbrella]**、**[Configuration]** > **[Firewall]** > **[Objects]** > **[Inspect Maps]** > **[DNS]**
オブジェクト グループの検索しきい値がデフォルトで無効になりました。	これまではオブジェクト グループの検索が有効になると、この機能によりしきい値が適用され、パフォーマンスの低下を防止していました。そのしきい値が、デフォルトで無効になりました。しきい値は、**object-group-search threshold** コマンドを使用して有効にできます。 新規/変更されたコマンド：**object-group-search threshold** 次の画面が変更されました：**[Configuration]** > **[Access Rules]** > **Advanced**
NAT のポート ブロック割り当てに対する暫定ログ	NAT のポート ブロックの割り当てを有効にすると、ポート ブロックの作成および削除中にシステムで syslog メッセージが生成されます。暫定ログの記録を有効にすると、指定した間隔でメッセージ 305017 が生成されます。メッセージは、その時点で割り当てられているすべてのアクティブ ポートブロックをレポートします（プロトコル（ICMP、TCP、UDP）、送信元および宛先インターフェイス、IP アドレス、ポート ブロックを含む）。 新規/変更されたコマンド：**xlate block-allocation pba-interim-logging** *seconds* 新規/変更された画面：**[Configuration]** > **[Firewall]** > **[Advanced]** > **[PAT Port Block Allocation]**
VPN 機能	

機能	説明
debug aaa の新しい **condition** オプション	**condition** オプションが **debug aaa** コマンドに追加されました。このオプションを使用すると、グループ名、ユーザー名またはピア IP アドレスに基づいて VPN デバッグをフィルタ処理できます。 新規/変更されたコマンド： **debug aaa condition** 変更された画面はありません。
IKEv2 での RSA SHA-1 のサポート	IKEv2 の RSA SHA-1 ハッシュ アルゴリズムを使用して署名を生成できるようになりました。 新規/変更されたコマンド： **rsa-sig-sha1** 新しい/変更された画面：
DES と3DES の両方の暗号化ライセンス、および使用可能な暗号のデフォルトの SSL 設定を表示します。	3DES 暗号化ライセンスの有無にかかわらず、デフォルトの SSL 設定を表示できるようになりました。さらに、デバイスでサポートされているすべての暗号を表示することもできます。 新規/変更されたコマンド： **show ssl information** 変更された画面はありません。
webVPN HSTS へのサブドメインの追加	ドメイン所有者は、Web ブラウザの HSTS プリロードリストに含める必要があるドメインを送信できます。 新規/変更されたコマンド： **hostname(config-webvpn) includesubdomains** 新しい/変更された画面： **[Configuration]** > **[Remote Access VPN]** > **[Clientless SSL VPN Access]** > **[Advanced]** > **[Proxies]** > [Enable HSTS Subdomains] フィールド
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
サイトごとのクラスタリング用 Gratuitous ARP	ASA では、Gratuitous ARP（GARP）パケットを生成してスイッチング インフラストラクチャを常に最新の状態に保つようになりました。各サイトの優先順位値が最も高いメンバによって、グローバル MAC/IP アドレスの GARP トラフィックが定期的に生成されます。クラスタから送信されたサイトごとの MAC および IP アドレスとパケットがサイト固有の MAC アドレスおよび IP アドレスを使用するのに対し、クラスタで受信したパケットは、グローバル MAC アドレスおよび IP アドレスを使用します。トラフィックがグローバル MAC アドレスから定期的に生成されない場合、グローバル MAC アドレスのスイッチで MAC アドレスのタイムアウトが発生する可能性があります。タイムアウト後にグローバル MAC アドレスへのトラフィックがスイッチングインフラストラクチャ全体にわたりフラッディングされ、これによりパフォーマンスおよびセキュリティ上の問題が発生することがあります。各スパンド EtherChannel のユニットおよびサイト MAC アドレスごとにサイト ID を設定すると、GARP がデフォルトで有効になります。 新規/変更されたコマンド： **site-periodic-garp interval** 新規/変更された画面：**[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[ASA Cluster]** > **[Cluster Configuration]** > **[Site Periodic GARP]** フィールド
マルチコンテキストモードの HTTPS リソース管理	リソースクラスの非 ASDM HTTPS セッションの最大数を設定できるようになりました。デフォルトでは、制限はコンテキストあたり最大 6 に設定でき、すべてのコンテキスト全体では最大 100 の HTTPS セッションを使用できます。 新規/変更されたコマンド： **limit-resource http** ASDM サポートはありません。
ルーティング機能	
認証のための OSPF キー チェーンのサポート	OSPF は、MD5 キーを使用してネイバーおよびルートアップデートを認証します。ASA では、MD5 ダイジェストの生成に使用されるキーには関連付けられている有効期間がありませんでした。したがって、キーを定期的に変更するにはユーザーによる介入が必要でした。この制限を打破するために、OSPFv2 は循環キーを使用した MD5 認証をサポートしています。 キー チェーンのキーの承認と送信の有効期間に基づいて、OSPF 認証でキーおよびフォームの隣接関係を承認または拒否します。 新規/変更されたコマンド：**accept-lifetime**、**area virtual-link authentication**、**cryptographic-algorithm**、**key**、**key chain**、**key-string**、**ospf authentication**、**send-lifetime** 新しい/変更された画面： • **[Configuration]** > **[Device Setup]** > **[Key Chain]** • **[Configuration]** > **[Device Setup]** > **[Routing]** > **[OSPF]** > **[Setup]** > **[Authentication]** • **[Configuration]** > **[Device Setup]** > **[Routing]** > **[OSPF]** > **[Setup]** > **[Virtual Link]**

機能	説明
証明書の機能	
登録用 URL のローカル CA を設定可能な FQDN	ASA の構成済み FQDN を使用する代わりに設定可能な登録用 URL の FQDN を作成するため、新しい CLI オプションが導入されました。この新しいオプションは、**crypto ca server** の **smpt** モードに追加されます。 新規/変更されたコマンド： **fqdn**
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	
enable ログイン時にパスワードの変更が必要になりました	デフォルトの **enable** のパスワードは空白です。ASA で特権 EXEC モードへのアクセスを試行する場合に、パスワードを 3 文字以上の値に変更することが必須となりました。空白のままにすることはできません。**no enable password** コマンドは現在サポートされていません。 CLI で **aaa authorization exec auto-enable** を有効にすると、**enable** コマンド、**login** コマンド（特権レベル 2 以上のユーザー）、または SSH/Telnet セッションを使用して特権 EXEC モードにアクセスできます。これらの方法ではすべて、イネーブルパスワードを設定する必要があります。 このパスワード変更の要件は、ASDM のログインには適用されません。ASDM のデフォルトでは、ユーザー名を使用せず **enable** パスワードを使用してログインすることができます。 新規/変更されたコマンド： **enable password** 変更された画面はありません。
管理セッションの設定可能な制限	集約、ユーザー単位、およびプロトコル単位の管理セッションの最大数を設定できます。これまでは、セッションの集約数しか設定できませんでした。この機能がコンソール セッションに影響を与えることはありません。マルチ コンテキスト モードでは HTTPS セッションの数を設定することはできず、最大セッション数は 5 で固定されています。また、**quota management-session** コマンドはシステム コンフィギュレーションでは受け入れられず、代わりにコンテキスト コンフィギュレーションで使用できるようになっています。集約セッションの最大数が 15 になりました。0（無制限）または 16 以上に設定してアップグレードすると、値は 15 に変更されます。 新規/変更されたコマンド：**quota management-session**、**show quota management-session** 新規/変更された画面：**[Configuration]** > **[Device Management]** > **[Management Access]** > **[Management Session Quota]**

機能	説明
管理権限レベルの変更通知	有効なアクセス（**aaa authentication enable console**）を認証するか、または特権 EXEC への直接アクセス（**aaa authorization exec auto-enable**）を許可すると、前回のログイン以降に割り当てられたアクセス レベルが変更された場合に ASA からユーザーへ通知されるようになりました。 新規/変更されたコマンド： **show aaa login-history** 新しい/変更された画面： [Status] バー > [Login History] アイコン
IPv6 での NTP サポート	NTP サーバーに IPv6 アドレスを指定できるようになりました。 新規/変更されたコマンド： **ntp server** 新規/変更された画面：**[Configuration]** > **[Device Setup]** > **[System Time]** > **[NTP]** > **[Add]** ボタン > [Add NTP Server Configuration] ダイアログ ボックス
SSH によるセキュリティの強化	次の SSH セキュリティの改善を参照してください。 • Diffie-Hellman Group 14 SHA256 キー交換のサポート。この設定がデフォルトになりました。以前のデフォルトは Group 1 SHA1 でした。 • HMAC-SHA256 整合性暗号のサポート。デフォルトは、高セキュリティの暗号セット（hmac-sha2-256 のみ）になりました。以前のデフォルトは中程度のセットでした。 新規/変更されたコマンド：**ssh cipher integrity** 、**ssh key-exchange group dh-group14-sha256** 新規/変更された画面： • **[Configuration]** > **[Device Management]** > **[Management Access]** > **[ASDM/HTTPS/Telnet/SSH]** • **[Configuration]** > **[Device Management]** > **[Advanced]** > **[SSH Ciphers]**
非ブラウザベースの HTTPS クライアントによる ASA へのアクセスの許可	非ブラウザベースの HTTPS クライアントが ASA 上の HTTPS サービスにアクセスできるようにすることができます。デフォルトでは、ASDM、CSM、および REST API が許可されています。 新規/変更されたコマンド： **http server basic-auth-client** 新規/変更された画面： **[Configuration]** > **[Device Management]** > **[Management Access]** > **[HTTP Non-Browser Client Support]**

機能	説明
クラスタ制御リンク上でのみのコントロール プレーン パケットのキャプチャ	クラスタ制御リンク（およびデータ プレーン パケットなし）でのみコントロール プレーンパケットをキャプチャできるようになりました。このオプションは、マルチコンテキスト モードのシステムで、ACL を使用してトラフィックを照合できない場合に役立ちます。 新規/変更されたコマンド： **capture interface cluster cp-cluster** 新規/変更された画面： **[Wizards]** > **[Packet Capture Wizard]** > **[Cluster Option]**
debug conn コマンド	接続処理を記録する 2 つの履歴メカニズムを提供するために **debug conn** コマンドが追加されました。1 つ目の履歴リストはスレッドの操作を記録するスレッドごとのリストです。2 つ目の履歴リストは conn グループに操作を記録するリストです。接続が有効になっている場合、接続のロック、ロック解除、削除などの処理イベントが 2 つの履歴リストに記録されます。問題が発生すると、これら 2 つのリストを使用して不正なロジックを判断する処理で確認することができます。 新規/変更されたコマンド： **debug conn**
show tech-support に追加の出力が含まれている	**show tech-support** の出力が拡張され、次の出力が表示されるようになりました。 • **show ipv6 interface** • **show aaa-server** • **show fragment** 新規/変更されたコマンド： **show tech-support**
SNMP ウォーク操作中の空きメモリおよび使用済みメモリの統計情報の結果の有効化および無効化の ASDM サポート	CPU リソースが過剰に使用されないようにするには、SNMP ウォーク操作によって収集された空きメモリと使用済みメモリの統計情報のクエリを有効または無効にすることができます。 新規または変更された画面：**[Configuration]** > **[Device Management]** > **[Management Access]** > **[SNMP]**
マルチコンテキスト モードのシステムの ASDM [Home] ペインに設定可能なグラフ更新間隔	マルチコンテキスト モードのシステムでは、[Home] ペインのグラフの更新間隔の時間を設定できるようになりました。 新規/変更された画面： **[Tools]** > **[Preferences]** > **[Graph User time interval in System Context]**

バージョン 9.10 の新機能

ASA 9.10(1)/ASDM 7.10(1) の新機能

リリース日：**2018 年 10 月 25 日**

機能	説明
プラットフォーム機能	
ASA 仮想 用の ASAv VHD カスタムイメージ	シスコが提供する圧縮 VHD イメージを使用して、Azure に独自のカスタム ASA 仮想 イメージを作成できるようになりました。VHD イメージを使用して展開するには、Azure ストレージ アカウントに VHD イメージをアップロードする必要があります。次に、アップロードしたディスクイメージおよび Azure Resource Manager テンプレートを使用して、管理対象イメージを作成できます。Azureテンプレートは、リソースの説明とパラメータの定義が含まれている JSON ファイルです。
Azure 用 ASA 仮想	ASA 仮想 は Azure 中国市場で入手できます。
DPDK の ASA 仮想 サポート	DPDK（データプレーン開発キット）は、ポーリングモードドライバを使用して ASA 仮想 のデータプレーンに統合されています。
FirePOWER モジュール バージョン 6.3 の ISA 3000 サポート	以前サポート対象だったバージョンは FirePOWER 5.4 でした。
ファイアウォール機能	
Cisco Umbrella サポート	Cisco Umbrella で定義されている エンタープライズ セキュリティ ポリシーをユーザー接続に適用できるように DNS 要求を Cisco Umbrella へリダイレクトするようにデバイスを設定できます。FQDN に基づいて接続を許可またはブロックできます。または、疑わしい FQDN の場合は Cisco Umbrella インテリジェント プロキシにユーザーをリダイレクトして URL フィルタリングを実行できます。Umbrella の設定は、DNS インスペクション ポリシーに含まれています。 新規/変更されたコマンド：**umbrella**、**umbrella-global**、**token**、**public-key**、**timeout edns**、**dnscrypt**、**show service-policy inspect dns detail** 新しい/変更された画面： **[Configuration]** > **[Firewall]** > **[Objects]** > **[Umbrella]**、**[Configuration]** > **[Firewall]** > **[Objects]** > **[Inspect Maps]** > **[DNS]**

機能	説明
MSISDNおよび選択モードのフィルタリング、アンチリプレイ、およびユーザー スプーフィング保護に対する GTP インスペクションの機能拡張	モバイル ステーション国際サブスクライバ電話番号（MSISDN）または選択モードに基づいて PDP コンテキストの作成メッセージをドロップするように GTP インスペクションを設定できるようになりました。また、アンチリプレイとユーザー スプーフィング保護も実装できます。 新規/変更されたコマンド：**anti-replay**、**gtp-u-header-check**、**match msisdn**、**match selection-mode** 新規/変更された画面： **[Configuration]** > **[Firewall]** > **[Objects]** > **[Inspection Maps]** > **[GTP]** > **[Add/Edit]** ダイアログボックス
TCP ステート バイパスのデフォルトのアイドル タイムアウト	TCP ステート バイパス接続のデフォルトのアイドル タイムアウトは 1 時間ではなく、2 分になりました。
カットスルー プロキシ ログイン ページからのログアウト ボタンの削除をサポート	ユーザー ID 情報（AAA 認証 リスナー）を取得するようにカットスルー プロキシを設定している場合、ページからログアウト ボタンを削除できるようになりました。これは、ユーザーが NAT デバイスの背後から接続し、IP アドレスで識別できない場合に便利です。1 人のユーザーがログアウトすると、その IP アドレスのすべてのユーザーがログアウトされます。 新規/変更されたコマンド：**aaa authentication listener no-logout-button** ASDM サポートはありません。 *9.8(3)* でも同様。
Trustsec SXP 接続の設定可能な削除ホールド ダウン タイマー	デフォルトの SXP 接続ホールド ダウン タイマーは 120 秒です。このタイマーを 120 ～ 64000 秒に設定できるようになりました。 新規/変更されたコマンド：**cts sxp delete-hold-down period**、**show cts sxp connection brief**、**show cts sxp connections** ASDM サポートはありません。 *9.8(3)* でも同様。
トランスペアレント モードでの NAT'ed フローのオフロードをサポート	フロー オフロード（**flow-offload enable** および **set connection advanced-options flow-offload** コマンド）を使用している場合、トランスペアレント モードで NAT を必要とするフローをオフロードされたフローに含めることができるようになりました。

機能	説明
Firepower Firepower 4100/9300 ASA 論理デバイスのトランスペアレントモード展開のサポート	Firepower 4100/9300 で ASA を展開するときに、トランスペアレントまたはルーテッド モードを指定できるようになりました。 新規/変更された FXOS コマンド：**enter bootstrap-key FIREWALL_MODE**、**set value routed**、**set value transparent** 新規/変更された [Firepower Chassis Manager] 画面： **[Logical Devices] > [Add Device] > [Settings]** 新規/変更されたオプション：[Firewall Mode] ドロップダウン リスト
VPN 機能	
従来の SAML 認証のサポート	CSCvg65072 の修正とともに ASA を展開すると、SAML のデフォルト動作で、AnyConnect 4.4 または 4.5 ではサポートされていない組み込みブラウザが使用されます。そのため、引き続き AnyConnect 4.4 または 4.5 を使用するには、従来の外部ブラウザで SAML 認証方式を有効にする必要があります。セキュリティ上の制限があるため、このオプションは、AnyConnect 4.6（またはそれ以降）に移行するための一時的な計画の一環としてのみ使用してください。このオプションは近い将来に廃止されます。 新規/変更されたコマンド： **saml external-browser** 新しい/変更された画面： **[設定（Configuration）] > [リモートアクセスVPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）]**> [Secure Client AnyConnect接続プロファイル（Secure Client Connection Profiles）] ページ > [接続プロファイル（Connection Profiles）] 領域 > [追加（Add）] ボタン > [Secure Client 接続プロファイルの追加（Add Secure Client AnyConnect Connection Profile）] ダイアログボックス **[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Connection Profiles] >** ページ > [Connection Profiles] 領域 > [Add] ボタン > [Add Clientless SSL VPN Connection Profile] ダイアログボックス 新規および変更されたオプション：[SAML External Browser] チェックボックス *9.8(3)* でも同様。

機能	説明
セキュアクライアント VPN リモートアクセス接続のための DTLS 1.2 サポート	DTLS 1.2（RFC-6347 で規定）では、現在サポートされている DTLS 1.0（バージョン番号 1.1 は DTLS には使用されません）に加えて、 Cisco Secure クライアントの AnyConnect VPN モジュールもサポートされるようになりました。これは、5506-X、5508-X、および 5516-X を除くすべての ASA モデルに適用され、ASA がクライアントではなく、サーバーとしてのみ機能している場合に適用されます。DTLS 1.2 は、現在のすべての TLS/DTLS 暗号方式と大きな Cookie サイズに加えて、追加の暗号方式をサポートしています。 新規/変更されたコマンド：**show run ssl**、**show vpn-sessiondb detail anyconnectssl cipher**、**ssl server-version** 新規/変更された画面：**[Configuration]** > **[Remote Access VPN]** > **[Advanced]** > **[SSL Settings]**
ハイ アベイラビリティとスケーラビリティの各機能	
Firepower 4100/9300 のクラスタ制御リンクのカスタマイズ可能な IP アドレス	クラスタ制御リンクのデフォルトでは 127.2.0.0/16 ネットワークが使用されます。これで FXOS でクラスタを展開するときにネットワークを設定できます。シャーシは、シャーシ ID およびスロット ID（127.2.*chassis_id*.*slot_id*）に基づいて、各ユニットのクラスタ制御リンク インターフェイス IP アドレスを自動生成します。ただし、一部のネットワーク展開では、127.2.0.0/16 トラフィックはパスできません。そのため、ループバック（127.0.0.0/8）およびマルチキャスト（224.0.0.0/4）アドレスを除き、FXOS にクラスタ制御リンクのカスタム /16 サブネットを作成できるようになりました。 新規/変更された FXOS コマンド： **set cluster-control-link network** 新規/変更された [Firepower Chassis Manager] 画面： **[Logical Devices]** > **[Add Device]** > **[Cluster Information]** 新規/変更されたオプション：[CCL Subnet IP] フィールド
Firepower 9300 シャーシごとのクラスタ ユニットのパラレル参加	Firepower 9300 の場合、この機能により、シャーシ内のセキュリティ モジュールがクラスタに同時に参加し、トラフィックがモジュール間で均等に分散されるようになります。他のモジュールよりもかなり前に参加したモジュールは、他のモジュールがまだ負荷を共有できないため、必要以上のトラフィックを受信することがあります。 新規/変更されたコマンド： **unit parallel-join** 新しい/変更された画面： **[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[ASA Cluster]** 新規/変更されたオプション：[Parallel Join of Units Per Chassis] エリア

機能	説明
クラスタ インターフェイス デバウンス時間は、ダウン状態から稼働状態に変更するインターフェイスに適用されるようになりました。	インターフェイスのステータス更新が発生すると、ASA はインターフェイスを障害としてマークし、クラスタからユニットを削除するまで **health-check monitor-interface debounce-time** コマンドまたは ASDM **[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[ASA Cluster]** 画面で指定されたミリ秒数待機します。この機能は、ダウン状態から稼働状態に変更するインターフェイスに適用されるようになりました。たとえば、ダウン状態から稼働状態に移行している EtherChannel の場合（スイッチがリロードされた、またはスイッチが有効になっている EtherChannel など）、デバウンス時間を長くすることで、他のクラスタ ユニットの方がポートのバンドルが速いという理由だけで、クラスタ ユニット上でインターフェイスがエラー表示されるのを防ぐことができます。 変更されたコマンドはありません。 変更された画面はありません。
Microsoft Azure Government クラウドでの ASA 仮想のアクティブ/バックアップの高可用性	アクティブな ASA 仮想 の障害が Microsoft Azure パブリッククラウドのバックアップ ASA 仮想 へのシステムの自動フェールオーバーをトリガーするのを許可する、ステートレスなアクティブ/バックアップソリューションが、Azure Government クラウドで使用できるようになりました。 新規または変更されたコマンド：**failover cloud** 新規または変更された画面：**[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[Failover]** **[Monitoring]** > **[Properties]** > **[Failover]** > **[Status]** **[Monitoring]** > **[Properties]** > **[Failover]** > **[History]**
インターフェイス機能	
Firepower 2100/4100/9300 のスーパーバイザの関連付けを表示するための **show interface ip brief** および **show ipv6 interface** の出力の強化	Firepower 2100/4100/9300 の場合、コマンドの出力は、インターフェイスのスーパーバイザの関連付けステータスを表示するために強化されています。 新規/変更されたコマンド：**show interface ip brief**、**show ipv6 interface**
Firepower 2100 では、**set lacp-mode** コマンドが **set port-channel-mode** に変更されています。	**set lacp-mode** コマンドは、Firepower 4100/9300 でのコマンドの使用方法に合わせるために **set port-channel-mode** に変更されています。 新規/変更された FXOS コマンド： **set port-channel-mode**
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	

機能	説明
Firepower 2100 の NTP 認証のサポート	FXOS で SHA1 NTP サーバー認証を設定できるようになりました。 新規/変更された FXOS コマンド：**enable ntp-authentication**、**set ntp-sha1-key-id**、**set ntp-sha1-key-string** 新規/変更された [Firepower Chassis Manager] 画面： **[Platform Settings]** > **[NTP]** 新規/変更されたオプション：[NTP Server Authentication: Enable] チェックボックス、[Authentication Key] フィールド、[Authentication Value] フィールド
ACL を使用せず IPv6 トラフィックを一致させるためのパケットキャプチャのサポート	**capture** コマンドの **match** キーワードを使用する場合、**any** キーワードは IPv4 トラフィックのみ照合します。IPv4 または IPv6 トラフィックをキャプチャするために、**any4** と **any6** キーワードを指定できるようになりました。**any** キーワードでは、引き続き IPv4 トラフィックのみ照合されます。 新規/変更されたコマンド：**capture match** ASDM サポートはありません。
Firepower 2100 の FXOS に対する SSH の公開キー認証のサポート	SSH キーを設定し、パスワード認証の代わりに公開キー認証を使用したり、両方の認証を使用したりできます。 新規/変更された FXOS コマンド：**set sshkey** Firepower Chassis Manager のサポートはありません。
GRE および IPinIP カプセル化のサポート	内部インターフェイス上でパケット キャプチャを実行するときに、ICMP、UDP、TCP などでの GRE および IPinIP カプセル化を表示するコマンドの出力が強化されています。 新規/変更されたコマンド：**show capture**
アプリケーションのキャッシュの割り当てを制限するメモリしきい値を有効にするためのサポート	デバイスの管理性と安定性を維持するためのメモリの予約ができるように、特定のメモリしきい値に達するアプリケーション キャッシュの割り当てを制限することができます。 新規/変更されたコマンド：**memory threshold enable**、**show run memory threshold**、**clear conf memory threshold**
RFC 5424 ロギングのタイムスタンプのサポート	RFC 5424 形式に従ってロギング タイムスタンプを有効にできます。 新規/変更されたコマンド：**logging timestamp**
TCB-IPS のメモリ使用量を表示するためのサポート	TCB-IPS でのアプリケーション レベルのメモリ キャッシュを表示します。 新規/変更されたコマンド：**show memory app-cache**

機能	説明
SNMP ウォーク操作中の空きメモリおよび使用済みメモリの統計情報の結果を有効または無効にするためのサポート	CPU リソースが過剰に使用されないようにするには、SNMP ウォーク操作によって収集された空きメモリと使用済みメモリの統計情報のクエリを有効または無効にすることができます。 新規/変更されたコマンド：**snmp-server enable oid** ASDM サポートはありません。

バージョン 9.9 の新機能

ASDM 7.9(2.152) の新機能

リリース日：**2018 年 5 月 9 日**

機能	説明
VPN 機能	
従来の SAML 認証のサポート	CSCvg65072 の修正とともに ASA を展開すると、SAML のデフォルト動作で、AnyConnect 4.4 または 4.5 ではサポートされていない組み込みブラウザが使用されます。そのため、引き続き AnyConnect 4.4 または 4.5 を使用するには、従来の外部ブラウザで SAML 認証方式を有効にする必要があります。セキュリティ上の制限があるため、このオプションは、AnyConnect 4.6 に移行するための一時的な計画の一環としてのみ使用してください。このオプションは近い将来に廃止されます。 新しい/変更された画面： **[設定（Configuration）] > [リモートアクセスVPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）]**セキュアクライアント**[接続プロファイル（Connection Profiles）]** ページ > **[接続プロファイル（Connection Profiles）]** 領域 > **[追加（Add）]** ボタン > **[追加（Add）]** セキュアクライアント**[接続プロファイル（Connection Profile）]** ダイアログ **[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Connection Profiles] >** ページ > [Connection Profiles] 領域 > [Add] ボタン > [Add Clientless SSL VPN Connection Profile] ダイアログボックス 新規および変更されたオプション：[SAML External Browser] チェックボックス

ASA 9.9(2)/ASDM 7.9(2) の新機能

リリース：**2018年3月26日**

機能	説明
プラットフォーム機能	
VMware ESXi 6.5 用の ASA 仮想 サポート	ASA 仮想プラットフォームは、VMware ESXi 6.5 で動作するホストをサポートしています。*vi.ovf* および *esxi.ovf* ファイルに新しい VMware ハードウェアバージョンが追加され、ESXi 6.5 で ASA 仮想 の最適なパフォーマンスと使いやすさを実現しました。 変更されたコマンドはありません。 変更された画面はありません。
VMXNET3 インターフェイス用の ASA 仮想 サポート	ASA 仮想プラットフォームは、VMware ハイパーバイザ上の VMXNET3 インターフェイスをサポートしています。 変更されたコマンドはありません。 変更された画面はありません。
初回起動時の仮想シリアル コンソール用の ASA 仮想 サポート	ASA 仮想 にアクセスして設定するために、仮想 VGA コンソールではなく初回起動時に仮想シリアルコンソールを使用するように ASA 仮想 を設定できるようになりました。 新規または変更されたコマンド：**console serial**
Microsoft Azure 上での高可用性のために複数の Azure サブスクリプションでユーザー定義ルートを更新する ASA 仮想 サポート	Azure 高可用性構成で ASA 仮想 を構成して、複数の Azure サブスクリプションでユーザー定義ルートを更新できるようになりました。 新規または変更されたコマンド：**failover cloud route-table** 新規または変更された画面：**[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[Failover]** > **[Route-Table]**
VPN 機能	
IKEv2 プロトコルに拡張されたリモートアクセス VPN マルチコンテキスト サポート	セキュアクライアント やサードパーティ製標準ベース IPSec IKEv2 VPN クライアントがマルチコンテキストモードで稼働する ASA へのリモートアクセス VPN セッションを確立できるように ASA を設定することをサポートします。
RADIUS サーバーへの IPv6 接続	ASA 9.9.2 では、外部 AAA RADIUS サーバーへの IPv6 接続がサポートされるようになりました。

機能	説明
BVI サポートのための Easy VPN 拡張	Easy VPN は、ブリッジ型仮想インターフェイス（BVI）を内部セキュア インターフェイスとしてサポートするように拡張され、インターフェイスを内部セキュアインターフェイスとして使用するように直接設定できるようになりました。それ以外の場合は、ASA がセキュリティ レベルを使用して、その内部セキュアインターフェイスを選択します。 また、VPN **管理アクセス**がその BVI で有効になっている場合、**telnet**、**http**、**ssh** などの管理サービスを BVI で設定できるようになりました。非 VPN 管理アクセスの場合は、ブリッジ グループ メンバ インターフェイスでこれらのサービスの設定を続行する必要があります。 新規または変更されたコマンド：**vpnclient secure interface** [*interface-name*]、**https**、**telnet**、**ssh**、**management-access**
分散型 VPN セッションの改善	• 分散型 S2S VPN のアクティブ セッションとバックアップ セッションのバランスをとるアクティブセッションの再配布ロジックが改善されました。また、管理者が入力した単一の **cluster redistribute vpn-sessiondb** コマンドに対し、バランシング プロセスをバックグラウンドで最大 8 回繰り返すことができます。 • クラスタ全体のダイナミック リバース ルート インジェクション（RRI）の処理が改善されました。
ハイ アベイラビリティとスケーラビリティの各機能	
内部障害発生後に自動的にクラスタに再参加する	以前は、多くのエラー状態によりクラスタ ユニットがクラスタから削除されていました。この問題を解決した後、手動でクラスタに再参加する必要がありました。現在は、ユニットはデフォルトで 5 分、10 分、および 20 分の間隔でクラスタに自動的に再参加を試行します。これらの値は設定できます。内部の障害には、アプリケーション同期のタイムアウト、矛盾したアプリケーション ステータスなどがあります。 新規または変更されたコマンド：**health-check system auto-rejoin**、**show cluster info auto-join** 新規または変更された画面：**[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[ASA Cluster]** > **[Auto Rejoin]**

機能	説明
ASA 5000-X シリーズに対してインターフェイスを障害としてマークするために設定可能なデバウンス時間	ASA がインターフェイスを障害が発生していると見なし、ASA 5500-X シリーズ上のクラスタからユニットが削除されるまでのデバウンス時間を設定できるようになりました。この機能により、インターフェイスの障害をより迅速に検出できます。デバウンス時間を短くすると、誤検出の可能性が高くなることに注意してください。インターフェイスのステータス更新が発生すると、ASA はインターフェイスを障害としてマークし、クラスタからユニットを削除するまで指定されたミリ秒数待機します。デフォルトのデバウンス時間は 500 ms で、有効な値の範囲は 300 ms ～ 9 秒です。この機能は以前は Firepower 4100/9300 で使用できました。 新規または変更されたコマンド：**health-check monitor-interface debounce-time** 新規または変更された画面：**[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[ASA Cluster]**
クラスタの信頼性の高いトランスポート プロトコル メッセージのトランスポートに関連する統計情報の表示	ユニットごとのクラスタの信頼性の高いトランスポート バッファ使用率を確認して、バッファがコントロール プレーンでいっぱいになったときにパケット ドロップの問題を特定できるようになりました。 新規または変更されたコマンド：**show cluster info transport cp detail**
ピア ユニットからのフェールオーバー履歴の表示	ピア ユニットから、**details** キーワードを使用して、フェールオーバー履歴を表示できるようになりました。これには、フェールオーバー状態の変更と状態変更の理由が含まれます。 新規または変更されたコマンド：**show failover**
インターフェイス機能	
シングル コンテキスト モード用の一意の MAC アドレス生成	シングル コンテキスト モードで VLAN サブインターフェイスの一意の MAC アドレス生成を有効にできるようになりました。通常、サブインターフェイスはメインインターフェイスと同じ MAC アドレスを共有します。IPv6 リンクローカル アドレスは MAC アドレスに基づいて生成されるため、この機能により一意の IPv6 リンクローカル アドレスが許可されます。 新規または変更されたコマンド：**mac-address auto** ASDM サポートはありません。 *9.8(3)* と *9.8(4)* も同様です。
管理機能	
RSA キー ペアによる 3072 ビット キーのサポート	モジュラス サイズを 3072 に設定できるようになりました。 新規または変更されたコマンド：**crypto key generate rsa modulus** 新規または変更された画面：**[Configuration]** > **[Device Management]** > **[Certificate Management]** > **[Identity Certificates]**

機能	説明
FXOS ブートストラップ設定によるイネーブル パスワードの設定	Firepower 4100/9300 に ASA を展開すると、ブートストラップ設定のパスワード設定により、イネーブル パスワードと管理者ユーザー パスワードが設定されるようになりました。FXOS バージョン 2.3.1 が必要です。
モニタリング機能とトラブルシューティング機能	
SNMP IPv6 のサポート	ASA は、IPv6 経由での SNMP サーバーとの通信、IPv6 経由でのクエリとトラップの実行許可、既存の MIB に対する IPv6 アドレスのサポートなど、SNMP over IPv6 をサポートするようになりました。RFC 8096 で説明されているように、次の新しい SNMP IPv6 MIB オブジェクトが追加されました。 • ipv6InterfaceTable（OID：1.3.6.1.2.1.4.30）：インターフェイスごとの IPv6 固有の情報が含まれています。 • ipAddressPrefixTable（OID：1.3.6.1.2.1.4.32）：このエンティティによって学習されたすべてのプレフィックスが含まれています。 • ipAddressTable（OID：1.3.6.1.2.1.4.34）：エンティティのインターフェイスに関連するアドレッシング情報が含まれています。 • ipNetToPhysicalTable（OID：1.3.6.1.2.1.4.35）：IP アドレスから物理アドレスへのマッピングが含まれています。 新規または変更されたコマンド：**snmp-server host** （注） **snmp-server host-group** コマンドは IPv6 をサポートしていません。 新規または変更された画面：**[Configuration]** > **[Device Management]** > **[Management Access]** > **[SNMP]**
単一ユーザー セッションのトラブルシューティングのための条件付きデバッグ	条件付きデバッグ機能は、設定されたフィルタ条件に基づく特定の ASA VPN セッションのログを確認することを支援するようになりました。IPv4 および IPv6 サブネットの「any, any」のサポートが提供されます。

ASDM 7.9(1.151) の新機能

リリース：2018 年 2 月 14 日

このリリースに新機能はありません。

ASA 9.9(1)/ASDM 7.9(1) の新機能

リリース：**2017年12月4日**

機能	説明
ファイアウォール機能	
Ethertype アクセス コントロール リストの変更	EtherType アクセス コントロール リストは、Ethernet II IPX（EII IPX）をサポートするようになりました。さらに、DSAP キーワードに新しいキーワードが追加され、共通 DSAP 値（BPDU（0x42）、IPX（0xE0）、Raw IPX（0xFF）、および ISIS（0xFE））をサポートします。その結果、BPDU または ISIS キーワードを使用する既存の EtherType アクセス コントロール エントリは自動的に DSAP 仕様を使用するように変換され、IPX のルールは 3 つのルール（DSAP IPX、DSAP Raw IPX、および EII IPX）に変換されます。さらに、IPX を EtherType 値として使用するパケットキャプチャは廃止されました。これは、IPX が 3 つの個別の EtherType に対応するためです。 新規/変更されたコマンド：**access-list ethertype** キーワード **eii-ipx** および **dsap** {**bpdu** | **ipx** | **isis** | **raw-ipx**}が追加されました。**capture ethernet-typeipx** キーワードはサポートされなくなりました。 新規または変更された画面：**[Configuration]** > **[Firewall]** > **[Ethertype Rules]**
VPN 機能	

機能	説明
Firepower 9300 上のクラスタリングによる分散型サイト間 VPN	Firepower 9300 上の ASA クラスタは、分散モードでサイト間 VPN をサポートします。分散モードでは、（集中モードなどの）制御ユニットだけでなく、ASA クラスタのメンバー間で多数のサイト間 IPsec IKEv2 VPN 接続を分散させることができます。これにより、集中型 VPN の機能を超えて VPN サポートが大幅に拡張され、高可用性が実現します。分散型 S2S VPN は、それぞれ最大 3 つのモジュールを含む最大 2 つのシャーシのクラスタ（合計 6 つのクラスタ メンバー）上で動作し、各モジュールは最大約 36,000 のアクティブ セッション（合計 72,000)に対し、最大 6,000 のアクティブ セッション（合計 12,000）をサポートします。 新規または変更されたコマンド：**cluster redistribute vpn-sessiondb**、**show cluster vpn-sessiondb**、**vpn mode**、**show cluster resource usage**、**show vpn-sessiondb**、**show connection detail**、**show crypto ikev2** 新規または変更された画面： **[Monitoring] > [ASA Cluster] > [ASA Cluster] > [VPN Cluster Summary]** **[Monitoring] > [VPN] > [VPN Statistics] > [Sessions]** **[Configuration] > [Device Management] > [High Availablility and Scalability] > [ASA Cluster]** **[Wizards] > [Site-to-Site]** **[Monitoring] > [VPN] > [VPN Statistics] > [Sessions]** **[Monitoring] > [ASA Cluster] > [ASA Cluster] > [VPN Cluster Summary]** **[Monitoring] > [ASA Cluster] > [ASA Cluster] > [System Resource Graphs] > [CPU/Memory]** **[Monitoring] > [Logging] > [Real-Time Log Viewer]**
ハイ アベイラビリティとスケーラビリティの各機能	
Microsoft Azure での ASA 仮想のアクティブ/バックアップの高可用性	アクティブな ASA 仮想 の障害が Microsoft Azure パブリッククラウドのバックアップ ASA 仮想 へのシステムの自動フェールオーバーをトリガーするのを許可する、ステートレスなアクティブ/バックアップソリューション。 新規または変更されたコマンド：**failover cloud** 新規または変更された画面：**[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[Failover]** **[Monitoring]** > **[Properties]** > **[Failover]** > **[Status]** **[Monitoring]** > **[Properties]** > **[Failover]** > **[History]** バージョン *9.8(1.200)* でも同様です。

機能	説明
Firepowerシャーシのシャーシヘルス チェックの障害検出の向上	シャーシヘルスチェックの保留時間をより低い値（100 ms）に設定できるようになりました。以前の最小値は 300 ms でした。 新規または変更されたコマンド：**app-agent heartbeat interval** ASDM サポートはありません。
クラスタリングのサイト間冗長性	サイト間の冗長性により、トラフィックフローのバックアップオーナーは常にオーナーとは別のサイトに置かれます。この機能によって、サイトの障害から保護されます。 新規または変更されたコマンド：**site-redundancy**、**show asp cluster counter change**、**show asp table cluster chash-table**、**show conn flag** 新規または変更された画面：**[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[ASA Cluster]**
動作と一致する**cluster remove unit**コマンドの動作**no enable**	**cluster remove unit** コマンドは、**no enable** コマンドと同様に、クラスタリングまたはリロードを手動で再度有効にするまで、クラスタからユニットを削除するようになりました。以前は、FXOS からブートストラップ設定を再展開すると、クラスタリングが再度有効になりました。無効化されたステータスは、ブートストラップ設定の再展開の場合でも維持されるようになりました。ただし、ASA をリロードすると、クラスタリングが再度有効になります。 新規または変更されたコマンド：cluster remove unit 新規または変更された画面：**[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[ASA Cluster]**
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 バージョン 1 の廃止	SSH バージョン 1 は廃止され、今後のリリースで削除される予定です。デフォルト設定が SSH v1 と v2 の両方から SSH v2 のみに変更されました。 新規/変更されたコマンド： **ssh version** 新しい/変更された画面： • **[Configuration]** > **[Device Management]** > **[Management Access]** > **[ASDM/HTTPS/Telnet/SSH]**

機能	説明
強化されたパケット トレーサおよびパケット キャプチャ機能	パケット トレーサは次の機能で強化されました。 • パケットがクラスタ ユニット間を通過するときにパケットを追跡します。 • シミュレートされたパケットが ASA から出られるようにします。 • シミュレートされたパケットのセキュリティ チェックをバイパスします。 • シミュレートされたパケットを IPsec/SSL で復号化されたパケットとして扱います。 パケット キャプチャは次の機能で強化されました。 • パケットを復号化した後にキャプチャします。 • トレースをキャプチャし、永続リストに保持します。 新規または変更されたコマンド：**cluster exec capture test trace include-decrypted**、**cluster exec capture test trace persist**、**cluster exec clear packet-tracer**、**cluster exec show packet-tracer id**、**cluster exec show packet-tracer origin**、**packet-tracer persist**、**packet-tracer transmit**、**packet-tracer decrypted**、**packet-tracer bypass-checks** 新規または変更された画面： **[Tools] > [Packet Tracer]** 次のオプションをサポートする [Cluster Capture] フィールドを追加しました：[decrypted]、[persist]、[bypass-checks]、[transmit] [All Sessions] ドロップダウンリストの下の [Filter By] ビューに 2 つの新しいオプションを追加しました：[Origin] および [Origin-ID] **[Monitoring] > [VPN] > [VPN Statistics] > [Packet Tracer and Capture]** [Packet Capture Wizard] 画面に [ICMP Capture] フィールドを追加しました：**[Wizards] > [Packet Capture Wizard]** ICMP キャプチャをサポートする 2 つのオプション、**include-decrypted** および **persist** を追加しました。

バージョン 9.8 の新機能

ASA 9.8(4) の新機能

リリース日：**2019 年 4 月 24 日**

機能	説明
VPN 機能	
webVPN HSTS へのサブドメインの追加	ドメイン所有者は、Web ブラウザの HSTS プリロードリストに含める必要があるドメインを送信できます。 新規/変更されたコマンド： **hostname(config-webvpn) includesubdomains** 新しい/変更された画面： **[Configuration]** > **[Remote Access VPN]** > **[Clientless SSL VPN Access]** > **[Advanced]** > **[Proxies]** > [Enable HSTS Subdomains] フィールド *9.12(1)* でも同様です。
管理機能	
非ブラウザベースの HTTPS クライアントによる ASA へのアクセスの許可	非ブラウザベースの HTTPS クライアントが ASA 上の HTTPS サービスにアクセスできるようにすることができます。デフォルトでは、ASDM、CSM、および REST API が許可されています。多くの専門クライアント（python ライブラリ、curl、wget など）は、クロスサイト要求の偽造（CSRF）トークンベースの認証をサポートしていないため、これらのクライアントが ASA 基本認証方式を使用することを明確に許可する必要があります。セキュリティ上の理由から、必要なクライアントのみを許可する必要があります。 新規/変更されたコマンド： **http server basic-auth-client** 新規/変更された画面： **[Configuration]** > **[Device Management]** > **[Management Access]** > **[HTTP Non-Browser Client Support]** *9.12(1)* でも同様です。
show tech-support に追加の出力が含まれている	**show tech-support** の出力が拡張され、次の出力が表示されるようになりました。 • **show ipv6 interface** • **show aaa-server** • **show fragment** 新規/変更されたコマンド： **show tech-support** *9.12(1)* でも同様です。

機能	説明
SNMP ウォーク操作中の空きメモリおよび使用済みメモリの統計情報の結果を有効または無効にするためのサポート	CPU リソースが過剰に使用されないようにするには、SNMP ウォーク操作によって収集された空きメモリと使用済みメモリの統計情報のクエリを有効または無効にすることができます。 新規/変更されたコマンド：**snmp-server enable oid** 新規または変更された画面：**[Configuration]** > **[Device Management]** > **[Management Access]** > **[SNMP]** *9.10(1)* でも同様です。

ASA 9.8(3)/ASDM 7.9(2.152) の新機能

リリース日：**2018 年 7 月 2 日**

機能	説明
プラットフォーム機能	
Firepower 2100 アクティブ LED はスタンバイ モードのときにオレンジ色に点灯するようになりました。	以前は、スタンバイ モード時にはアクティブ LED は点灯していませんでした。
ファイアウォール機能	
カットスルー プロキシ ログイン ページからのログアウト ボタンの削除をサポート。	ユーザー ID 情報（AAA 認証 リスナー）を取得するようにカットスルー プロキシを設定している場合、ページからログアウト ボタンを削除できるようになりました。これは、ユーザーが NAT デバイスの背後から接続し、IP アドレスで識別できない場合に便利です。1 人のユーザーがログアウトすると、その IP アドレスのすべてのユーザーがログアウトされます。 新規/変更されたコマンド：**aaa authentication listener no-logout-button**。 ASDM サポートはありません。
Trustsec SXP 接続の設定可能な削除ホールド ダウン タイマー	デフォルトの SXP 接続ホールド ダウン タイマーは 120 秒です。このタイマーを 120 ～ 64000 秒に設定できるようになりました。 新規/変更されたコマンド：**cts sxp delete-hold-down period**、**show cts sxp connection brief**、**show cts sxp connections** ASDM サポートはありません。
VPN 機能	

機能	説明
従来の SAML 認証のサポート	CSCvg65072 の修正とともに ASA を展開すると、SAML のデフォルト動作で、AnyConnect 4.4 または 4.5 ではサポートされていない組み込みブラウザが使用されます。そのため、引き続き AnyConnect 4.4 または 4.5 を使用するには、従来の外部ブラウザで SAML 認証方式を有効にする必要があります。セキュリティ上の制限があるため、このオプションは、AnyConnect 4.6 に移行するための一時的な計画の一環としてのみ使用してください。このオプションは近い将来に廃止されます。 新規/変更されたコマンド： **saml external-browser** 新しい/変更された画面： **[設定（Configuration）]** > **[リモートアクセスVPN（Remote Access VPN）]** > **[ネットワーク（クライアント）アクセス（Network (Client) Access）]**セキュアクライアント**[接続プロファイル（Connection Profiles）]** ページ > **[接続プロファイル（Connection Profiles）]** 領域 > **[追加（Add）]** ボタン > **[追加（Add）]** セキュアクライアント**[接続プロファイル（Connection Profile）]** ダイアログ **[Configuration]** > **[Remote Access VPN]** > **[Clientless SSL VPN Access]** > **[Connection Profiles]** > ページ > [Connection Profiles] 領域 > [Add] ボタン > [Add Clientless SSL VPN Connection Profile] ダイアログボックス 新規および変更されたオプション：[SAML External Browser] チェックボックス
インターフェイス機能	
シングル コンテキスト モード用の一意の MAC アドレス生成	シングル コンテキスト モードで VLAN サブインターフェイスの一意の MAC アドレス生成を有効にできるようになりました。通常、サブインターフェイスはメインインターフェイスと同じ MAC アドレスを共有します。IPv6 リンクローカル アドレスは MAC アドレスに基づいて生成されるため、この機能により一意の IPv6 リンクローカル アドレスが許可されます。 新規または変更されたコマンド：**mac-address auto** ASDM サポートはありません。 *9.9 (2)* 以降でも同様です。

ASDM 7.8(2.151) の新機能

リリース：**2017年10月12日**

機能	説明
ファイアウォール機能	

機能	説明
Ethertype アクセス コントロール リストの変更	EtherType アクセス コントロール リストは、Ethernet II IPX（EII IPX）をサポートするようになりました。さらに、DSAP キーワードに新しいキーワードが追加され、共通 DSAP 値（BPDU（0x42）、IPX（0xE0）、Raw IPX（0xFF）、および ISIS（0xFE））をサポートします。その結果、BPDU または ISIS キーワードを使用する既存の EtherType アクセス コントロール エントリは自動的に DSAP 仕様を使用するように変換され、IPX のルールは 3 つのルール（DSAP IPX、DSAP Raw IPX、および EII IPX）に変換されます。さらに、IPX を EtherType 値として使用するパケット キャプチャは廃止されました。これは、IPX が 3 つの個別の EtherType に対応するためです。 この機能は、9.8(2.9)およびその他の暫定リリースでサポートされています。詳細については、CSCvf57908 を参照してください。 次のコマンドが変更されました：**access-list ethertype** キーワード **eii-ipx** および **dsap** {**bpdu** | **ipx** | **isis** | **raw-ipx**}が追加されました。**capture ethernet-typeipx** キーワードはサポートされなくなりました。 次の画面が変更されました：**[Configuration]** > **[Firewall]** > **[Ethertype Rules]**.

ASA 9.8(2)/ASDM 7.8(2) の新機能

リリース：**2017年8月28日**

機能	説明
プラットフォーム機能	

機能	説明
FirePOWER 2100 シリーズ用の ASA	FirePOWER 2110、2120、2130、2140 用の ASA を導入しました。FirePOWER 4100 および 9300 と同様に、FirePOWER 2100 は基盤の FXOS オペレーティング システムを実行してから、ASA オペレーティング システムをアプリケーションとして実行します。FirePOWER 2100 実装では、FirePOWER 4100 および 9300 よりも緊密に FXOS を ASA と連携させます（軽量な FXOS 機能、単一デバイス イメージ バンドル、ASA および FXOS の両方に対する簡単な管理アクセス）。 FXOS には、EtherChannel の作成、NTP サービス、ハードウェアのモニタリング、およびその他の基本機能を含む、インターフェイスの構成ハードウェア設定があります。この構成では、Firepower Chassis Manager または FXOS CLI を使用できます。ASA には、（FirePOWER 4100 および 9300 とは異なり）スマート ライセンスを含む、その他すべての機能があります。ASA および FXOS はそれぞれ、管理 1/1 インターフェイスでの独自の IP アドレスを持っています。ユーザーは、任意のデータ インターフェイスから ASA および FXOS インスタンス両方の管理を設定できます。 次のコマンドが導入されました。**connect fxos**、**fxos https**、**fxos snmp**、**fxos ssh**、**ip-client** 次の画面が導入されました。 **[Configuration] > [Device Management] > [Management Access] > [FXOS Remote Management]**
国防総省（DoD）統合機能認定製品リスト	ASA は、統合機能認定製品リスト（UC APL）の要件に準拠するように更新されました。このリリースでは、**fips enable** コマンドを入力すると、ASA がリロードされます。フェールオーバーを有効にする前に、両方のフェールオーバー ピアが同じ FIPS モードになっている必要があります。 **fips enable** コマンドが変更されました。
Amazon Web Services M4 インスタンスサポートの ASA 仮想	ASA 仮想 を M4 インスタンスとして展開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。 変更された画面はありません。
ASAv5 1.5 GB RAM 機能	バージョン 9.7(1) 以降、ASAv5 では、セキュアクライアント の有効化や ASA 仮想 へのファイルのダウンロードなど、特定の機能が失敗した場合にメモリが枯渇することがあります。1.5 GB の RAM を ASAv5 に割り当てられるようになりました（1 GB から増加しました）。 変更されたコマンドはありません。 変更された画面はありません。
VPN 機能	

機能	説明
HTTP Strict Transport Security（HSTS）ヘッダーのサポート	HSTS は、クライアントレス SSL VPN でのプロトコル ダウングレード攻撃や Cookie ハイジャックから Web サイトを保護します。これにより Web サーバーは、Web ブラウザ（またはその他の準拠しているユーザー エージェント）が Web サーバーと通信するにはセキュア HTTPS 接続を使用する必要があり、非セキュアな HTTP プロトコルを使用して通信することはできないことを宣言できます。HSTS は IETF 標準化過程プロトコルであり、RFC 6797 で指定されます。 次のコマンドが導入されました。**hsts enable, hsts max-age** *age_in_seconds* 次の画面が変更されました：[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Advanced] > [Proxies]
インターフェイス機能	
ASAv50 の VLAN サポート	ASAv50 では、SR-IOV インターフェイスの ixgbe-vf vNIC で VLAN がサポートされるようになりました。 変更されたコマンドはありません。 変更された画面はありません。

ASA 9.8(1.200) の新機能

リリース：**2017年7月30日**

（注） このリリースは、Microsoft Azure の ASA 仮想 でのみサポートされます。これらの機能は、バージョン 9.8(2) ではサポートされていません。

機能	説明
ハイ アベイラビリティとスケーラビリティの各機能	
Microsoft Azure での ASA 仮想のアクティブ/バックアップの高可用性	アクティブな ASA 仮想 の障害が Microsoft Azure パブリッククラウドのバックアップ ASA 仮想 へのシステムの自動フェールオーバーをトリガーするのを許可する、ステートレスなアクティブ/バックアップソリューション。 次のコマンドが導入されました。**failover cloud** ASDM サポートはありません。

ASDM 7.8(1.150) の新機能

リリース：2017年6月20日

このリリースに新機能はありません。

ASA 9.8(1)/ASDM 7.8(1) の新機能

リリース：2017年5月15日

機能	説明
プラットフォーム機能	
ASAv50 プラットフォーム	ASA 仮想プラットフォームに、10 Gbps のファイアウォール スループット レベルを提供するハイエンド パフォーマンス ASAv50 プラットフォームが追加されました。ASAv50 には ixgbe-vf vNIC が必要です。これは VMware および KVM でのみサポートされます。
ASA 仮想プラットフォームの SR-IOV	ASA 仮想プラットフォームでは、Single Root I/O Virtualization（SR-IOV）インターフェイスがサポートされます。これにより、複数の VM でホスト内の 1 つの PCIe ネットワークアダプタを共有できるようになります。ASA 仮想 SR-IOV サポートは、VMware、KVM、および AWS でのみ使用可能です。
自動 ASP ロードバランシングが ASA 仮想 でサポートされるようになりました。	以前は、ASP ロード バランシングは手動でのみ有効または無効にできました。 次のコマンドを変更しました。**asp load-balance per-packet-auto** 次の画面が変更されました。[Configuration] > [Device Management] > [Advanced] > [ASP Load Balancing]。
ファイアウォール機能	
TLS プロキシ サーバーの SSL 暗号スイートの設定サポート	ASA が TLS プロキシ サーバーとして動作している場合は、SSL 暗号スイートを設定できるようになりました。以前は、**[Configuration]** > **[Device Management]** > **[Advanced]** > **[SSL Settings]** > **[Encryption]** ページで **ssl cipher** コマンドを使用した ASA のグローバル設定のみが可能でした。 次のコマンドが導入されました。 **server cipher-suite** 次の画面が変更されました。**[Configuration]** > **[Firewall]** > **[Unified Communications]** > **[TLS Proxy]**、追加/編集ダイアログ ボックス、[Server Configuration] ページ。

機能	説明
ICMP エラーのグローバル タイムアウト	ASA が ICMP エコー応答パケットを受信してから ICMP 接続を削除するまでのアイドル時間を設定できるようになりました。このタイムアウトが無効（デフォルト）で、ICMP インスペクションが有効に設定されている場合、ASA はエコー応答を受信するとすぐに ICMP 接続を削除します。したがって、終了しているその接続に対して生成されたすべての ICMP エラーは破棄されます。このタイムアウトは ICMP 接続の削除を遅らせるので、重要な ICMP エラーを受信することが可能になります。 次のコマンドが追加されました。 **timeout icmp-error** **[Configuration]** > **[Firewall]** > **[Advanced]** > **[Global Timeouts]** の画面が変更されました。
ハイ アベイラビリティとスケーラビリティの各機能	
改善されたクラスタ ユニットのヘルス チェック障害検出	ユニット ヘルスチェックの保留時間をより低めの値に設定できます（最小値は .3 秒）以前の最小値は .8 秒でした。この機能は、ユニット ヘルス チェック メッセージング スキームを、コントロール プレーンのキープアライブからデータ プレーンのハートビートに変更します。ハートビートを使用すると、コントロールプレーン CPU のホッギングやスケジューリングの遅延の影響を受けないため、クラスタリングの信頼性と応答性が向上します。保留時間を短く設定すると、クラスタ制御リンクのメッセージング アクティビティが増加することに注意してください。保留時間を短く設定する前にネットワークを分析することをお勧めします。たとえば、ある保留時間間隔の間に 3 つのハートビート メッセージが存在するため、クラスタ制御リンクを介してあるユニットから別のユニットへの ping が保留時間/3 以内に戻ることを確認します。保留時間を 0.3 ～ 0.7 に設定した後に ASA ソフトウェアをダウングレードした場合、新しい設定がサポートされていないので、この設定はデフォルトの 3 秒に戻ります。 次のコマンドを変更しました。**health-check holdtime**、**show asp drop cluster counter**、**show cluster info health details** 次の画面を変更しました。**[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[ASA Cluster]**
に対してインターフェイスを障害としてマークするために設定可能なデバウンス時間 Firepower 4100/9300 シャーシ	ASA がインターフェイスを障害が発生していると見なし、クラスタからユニットが削除されるまでのデバウンス時間を設定できるようになりました。この機能により、インターフェイスの障害をより迅速に検出できます。デバウンス時間を短くすると、誤検出の可能性が高くなることに注意してください。インターフェイスのステータス更新が発生すると、ASA はインターフェイスを障害としてマークし、クラスタからユニットを削除するまで指定されたミリ秒数待機します。デフォルトのデバウンス時間は 500 ms で、有効な値の範囲は 300 ms ～ 9 秒です。 新規または変更されたコマンド：**health-check monitor-interface debounce-time** 新規または変更された画面：**[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[ASA Cluster]**

機能	説明
VPN 機能	
VTI での IKEv2、証明書ベース認証、および ACL のサポート	仮想トンネル インターフェイス（VTI）は、BGP（静的 VTI）をサポートするようになりました。スタンドアロン モードとハイ アベイラビリティ モードで、IKEv2 を使用できます。IPsec プロファイルにトラストポイントを設定することにより、証明書ベースの認証を使用できます。また、入力トラフィックをフィルタリングする access-group コマンドを使用して、VTI 上でアクセス リストを適用することもできます。 IPsec プロファイルのコンフィギュレーション モードに次のコマンドが導入されました。**set trustpoint** 次の画面で、証明書ベース認証のトラストポイントを選択するオプションが導入されました。 **[Configuration] > [Site-to-Site VPN] > [Advanced] > [IPsec Proposals (Transform Sets)] > [IPsec Profile] > [Add]**
モバイル IKEv2（MobIKE）はデフォルトで有効になっています	リモート アクセス クライアントとして動作するモバイル デバイスは、移動中にトランスペアレント IP アドレスを変更する必要があります。ASA で MobIKE をサポートすることにより、現在の SA を削除せずに現在の IKE セキュリティ アソシエーション（SA）を更新することが可能になります。MobIKE は [always on] に設定されます。 次のコマンドが導入されました。**ikev2 mobike-rrc**。リターン ルータビリティのチェックを有効または無効にするために使用されます。
SAML 2.0 SSO の更新	SAML 要求におけるシグネチャのデフォルト署名メソッドが SHA1 から SHA2 に変更され、ユーザーが rsa-sha1、rsa-sha256、rsa-sha384、rsa-sha512 の中から署名メソッドを選択して設定できるようになりました。 webvpn モードでの **saml idp signature** コマンドが変更されました。このコマンドには *value* を設定できます。デフォルトは [disabled] のままです。 次の画面が変更されました。**[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Advanced] > [Single Sign On Servers] > [Add]**。
tunnelgroup webvpn-attributesの変更	**pre-fill-username** および **secondary-pre-fill-username** の値を **ssl-client** から **client** に変更しました。 webvpn モードでの次のコマンドが変更されました：**pre-fill-username** および **secondary-pre-fill-username** は **client** 値を設定できます。
AAA 機能	

機能	説明
ログイン履歴	デフォルトでは、ログイン履歴は90日間保存されます。この機能を無効にするか、期間を最大365日まで変更できます。1つ以上の管理メソッド（SSH、ASDM、Telnetなど）でローカルAAA認証を有効にしている場合、この機能はローカルデータベースのユーザー名にのみ適用されます。 次のコマンドが導入されました。**aaa authentication login-history**、**show aaa login-history** 次の画面が導入されました。**[Configuration]** > **[Device Management]** > **[Users/AAA]** > **[Login History]**
パスワードの再利用とユーザー名と一致するパスワードの使用を禁止するパスワード ポリシーの適用	最大 7 世代にわたるパスワードの再利用と、ユーザー名と一致するパスワードの使用を禁止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。**password-history**、**password-policy reuse-interval**、**password-policy username-check** 次の画面が変更されました。**[Configuration]** > **[Device Management]** > **[Users/AAA]** > **[Password Policy]**
SSH公開キー認証を使用するユーザーの認証とパスワードを使用するユーザー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 ユーザー 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。ユーザーに対して **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ー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ー名にのみ適用されます。また、任意の AAA サーバー タイプ （**aaa authentication ssh console radius_1** など）を使用できます。たとえば、一部のユーザーはローカル データベースを使用して公開キー認証を使用し、他のユーザーは 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。 変更された画面はありません。 バージョン *9.6(3)* でも同様です。
モニタリング機能とトラブルシューティング機能	
ASA クラッシュ発生時に実行中のパケット キャプチャの保存	以前は、ASA がクラッシュするとアクティブなパケット キャプチャは失われました。現在は、クラッシュが発生すると、パケット キャプチャは disk 0 に以下のファイル名で保存されます。[*context_name***.**]*capture_name*.**pcap**。 変更されたコマンドはありません。 変更された画面はありません。

バージョン 9.7 の新機能

ASDM 7.7(1.151) の新機能

リリース：2017年4月28日

（注） ASDM 7.7(1.150) は、バグ CSCvd90344 に基づき Cisco.com から削除されました。

機能	説明
管理機能	
ASDM アップグレード ツールの新しいバックグラウンド サービス	ASDM は、[Tools] > [Check for ASA/ASDM Upgrades] の新しいバックグラウンド サービスです。Cisco は、前のバージョンの ASDM で使用されていた古いサービスを将来廃止する予定です。

ASA 9.7(1.4)/ASDM 7.7(1) の新機能

リリース：2017年4月4日

（注） バージョン 9.7(1) は、バグ CSCvd78303 に基づき Cisco.com から削除されました。

機能	説明
プラットフォーム機能	

機能	説明
Integrated Routing and Bridging（IRB; 統合ルーティングおよびブリッジング）を使用した ASA 5506-X シリーズ用の新しいデフォルト設定	新しいデフォルト設定が ASA 5506-X シリーズに使用されます。統合ブリッジングおよびルーティング機能は、外部レイヤ 2 スイッチの使用に代わる手段を提供します。ハードウェア スイッチを含む ASA 5505 を交換するユーザーの場合、この機能を使用することにより、追加のハードウェア使用せずに ASA 5505 を ASA 5506-X やその他の ASA モデルに置き換えることができます。 新しいデフォルト設定には次の内容が含まれます。 • GigabitEthernet 1/1、DHCP からの IP アドレスの外部インターフェイス • GigabitEthernet ½（inside1）から 1/8（inside7）、IP アドレス 192.168.1.1 が指定された内部ブリッジグループ BVI 1 • 内部 --> 外部へのトラフィック フロー • 内部 --> メンバー インターフェイス用内部トラフィック フロー • （ASA 5506W-X）GigabitEthernet 1/9、IP アドレス 192.168.10.1 の Wi-Fi インターフェイス • （ASA 5506W-X） WiFi<--> 内部のトラフィック フロー、WiFi --> 外部へのトラフィック フロー • 内部および WiFi 上のクライアントに対する DHCP。アクセス ポイント自体とそのすべてのクライアントが ASA を DHCP サーバーとして使用します。 • 管理 1/1 インターフェイスが稼働しているが、そうでない場合は未設定。ASA FirePOWER モジュールは、このインターフェイスを使用して ASA 内部ネットワークに接続し、内部インターフェイスをインターネットへのゲートウェイとして使用できます。 • ASDM アクセス：内部ホストと Wi-Fi ホストが許可されます。 • NAT：内部、WiFi、および管理から外部へのすべてのトラフィックのインターフェイス PAT。 アップグレードする場合、**configure factory-default** コマンドを使用して設定を消去しデフォルトを適用するか、必要に応じて BVI とブリッジ グループのメンバーを手動で設定することができます。内部ブリッジグループの通信を簡単に許可するには、**same-security-traffic permit inter-interface** コマンドを有効にする必要があります（このコマンドは、ASA 5506W-X のデフォルト設定にすでに存在します）。

機能	説明
ISA 3000 でのアラーム ポートのサポート	ISA 3000 は、2 つのアラーム入力インターフェイスと 1 つのアラーム出力インターフェイスをサポートします。ドアセンサーなどの外部センサーは、アラーム入力に接続できます。ブザーなどの外部デバイスは、アラーム出力インターフェイスに接続できます。トリガーされたアラームは、2 つの LED、syslog、SNMP トラップを経由し、アラーム出力インターフェイスに接続されたデバイスを介して伝えられます。ユーザーは、外部アラームの説明を設定できます。また、外部アラームと内部アラームの重大度とトリガーも指定できます。すべてのアラームは、リレー、モニタリング、およびロギングに設定できます。 次のコマンドが導入されました。**alarm contact description**、**alarm contact severity**、**alarm contact trigger**、**alarm facility input-alarm**、**alarm facility power-supply rps**、**alarm facility temperature**、**alarm facility temperature high**、**alarm facility temperature low**、**clear configure alarm**、**clear facility-alarm output**、**show alarm settings**、**show environment alarm-contact**。 次の画面が導入されました。 **[Configuration] > [Device Management] > [Alarm Port] > [Alarm Contact]** **[Configuration] > [Device Management] > [Alarm Port] > [Redundant Power Supply]** **[Configuration] > [Device Management] > [Alarm Port] > [Temperature]** **[Monitoring] > [Properties] > [Alarm] > [Alarm Settings]** **[Monitoring] > [Properties] > [Alarm] > [Alarm Contact]** **[Monitoring] > [Properties] > [Alarm] > [Facility Alarm Status]**
ASAv10 での Microsoft Azure Security Center のサポート	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。Microsoft Azure Security Center は、非常にセキュアなパブリック クラウドインフラストラクチャの導入を簡素化する、Azure 上の Microsoft オーケストレーションおよび管理レイヤです。ASA 仮想 を Azure Security Center に統合することにより、Azure環境を保護するファイアウォールオプションとして ASA 仮想 を提供できます。

機能	説明
ISA 3000 用の Precision Time Protocol（PTP）	ISA 3000 は PTP（ネットワークに分散したノードの時刻同期プロトコル）をサポートします。PTP は、そのハードウェア タイムスタンプ機能により、NTP などの他の時刻同期プロトコルより高い精度を実現します。ISA 3000 は、ワンステップのエンドツーエンド トランスペアレント クロックに加えて、PTP 転送モードもサポートします。インスペクションのために PTP トラフィックが ASA FirePOWER モジュールに送信されることのないようにするため、デフォルト設定に次のコマンドが追加されました。既存の導入がある場合は、次のコマンドを手動で追加する必要があります。 `object-group service bypass_sfr_inspect` `  service-object udp destination range 319 320` `access-list sfrAccessList extended deny object-group bypass_sfr_inspect any any` 次のコマンドが導入されました。 **debug ptp**、**ptp domain**、**ptp mode e2etransparent**、**ptp enable**、**show ptp clock**、**show ptp internal-info**、**show ptp port** 次の画面が導入されました。 **[Configuration]** > **[Device Management]** > **[PTP]** **[Monitoring]** > **[Properties]** > **[PTP]**
ISA 3000 の自動バックアップと復元	バックアップ コマンドと復元コマンドのプリセット パラメータを使用して、自動バックアップ機能や自動復元機能を有効にできます。これらの機能は、外部メディアからの初期設定、デバイス交換、作動可能状態へのロールバックなどで使用されます。 次のコマンドが導入されました。**backup-package location**、**backup-package auto**、**show backup-package status**、**show backup-package summary** 次の画面が導入されました。**[Configuration]** > **[Device Management]** > **[Auto Backup & Restore Configuration]**
ファイアウォール機能	
SCTP マルチストリーミングの並べ替えとリアセンブル、およびフラグメンテーションのサポート。SCTP エンドポイントに複数の IP アドレスが設定された SCTP マルチホーミングのサポート。	このシステムは、SCTP マルチストリーミングの並べ替え、リアセンブル、およびフラグメンテーションを完全にサポートしており、これにより SCTP トラフィックに対する Diameter および M3UA インスペクションの有効性が改善されています。このシステムは、各エンドポイントに複数の IP アドレスが設定された SCTP マルチホーミングもサポートしています。マルチホーミングでは、セカンデリ アドレスに必要なピンホールをシステムが開くので、セカンデリ アドレスを許可するためのアクセス ルールをユーザーが設定する必要はありません。SCTP エンドポイントは、それぞれ 3 つの IP アドレスに制限する必要があります。 **show sctp detail** コマンドの出力が変更されました。 変更された画面はありません。

機能	説明
M3UAインスペクションの改善。	M3UAインスペクションは、ステートフルフェールオーバー、半分散クラスタリング、およびマルチホーミングをサポートするようになりました。また、アプリケーションサーバープロセス（ASP）の状態の厳密な検証や、さまざまなメッセージの検証も設定できます。ASP状態の厳密な検証は、ステートフルフェールオーバーとクラスタリングに必要です。 次のコマンドが追加または変更されました。**clear service-policy inspect m3ua session** [**assocID** *id*]、**match port sctp**、**message-tag-validation**、**show service-policy inspect m3ua drop**、**show service-policy inspect m3ua endpoint**、**show service-policy inspect m3ua session**、**show service-policy inspect m3ua table**、**strict-asp-state**、**timeout session**。 次の画面が変更されました。**[Configuration]** > **[Firewall]** > **[Objects]** > **[Inspection Maps]** > **[M3UA]** [Add/Edit] ダイアログボックス。
TLSプロキシでのTLSv1.2、およびCisco Unified Communications Manager 10.5.2のサポート。	暗号化SIP用のTLSプロキシでのTLSv1.2、またはCisco Unified Communications Manager 10.5.2でのSCCPインスペクションを使用できるようになりました。TLSプロキシは、**client cipher-suite**コマンドの一部として追加されたTLSv1.2暗号スイートをサポートします。 次のコマンドが変更されました。 **client cipher-suite** 変更された画面はありません。

機能	説明
Integrated Routing and Bridging（IRB）	Integrated Routing and Bridging（統合ルーティングおよびブリッジング）は、ブリッジグループとルーテッド インターフェイス間をルーティングする機能を提供します。ブリッジグループとは、ASAがルートの代わりにブリッジするインターフェイスのグループのことです。ASA は、ASA がファイアウォールとして機能し続ける点で本来のブリッジとは異なります。つまり、インターフェイス間のアクセス制御が実行され、通常のファイアウォール検査もすべて実行されます。以前は、トランスペアレント ファイアウォール モードでのみブリッジグループの設定が可能だったため、ブリッジグループ間でのルーティングはできませんでした。この機能を使用すると、ルーテッド ファイアウォール モードのブリッジ グループの設定と、ブリッジグループ間およびブリッジグループとルーテッドインターフェイス間のルーティングを実行できます。ブリッジ グループは、ブリッジ仮想インターフェイス（BVI）を使用して、ブリッジ グループのゲートウェイとして機能することによってルーティングに参加します。そのブリッジグループに指定する ASA 上に別のインターフェイスが存在する場合、Integrated Routing and Bridging（IRB）は外部レイヤ 2 スイッチの使用に代わる手段を提供します。ルーテッド モードでは、BVI は名前付きインターフェイスとなり、アクセス ルールや DHCP サーバーなどの一部の機能に、メンバー インターフェイスとは個別に参加できます。 トランスペアレント モードでサポートされるマルチ コンテキスト モードや ASA クラスタリングの各機能は、ルーテッドモードではサポートされません。マルチキャスト ルーティングとダイナミック ルーティングの機能も、BVI ではサポートされません。 次のコマンドが変更されました。**access-group**、**access-list ethertype**、**arp-inspection**、**dhcpd**、**mac-address-table static**、**mac-address-table aging-time**、**mac-learn**、**route**、**show arp-inspection**、**show bridge-group**、**show mac-address-table**、**show mac-learn** 次の画面が変更されました。 **[Configuration]** > **[Device Setup]** > **[Interface Settings]** > **[Interfaces]** **[Configuration]** > **[Device Setup]** > **[Routing]** > **[Static Routes]** **[Configuration]** > **[Device Management]** > **[DHCP]** > **[DHCP Server]** **[Configuration]** > **[Firewall]** > **[Access Rules]** **[Configuration]** > **[Firewall]** > **[EtherType Rules]**
VM 属性	ネットワーク オブジェクトを定義することにより、VMware vCenter で管理している VMware ESXi 環境の 1 つ以上の仮想マシン（VM）に関連付けられている属性に従ってトラフィックをフィルタリングできます。アクセス コントロール リスト（ACL）を定義して、1 つ以上の属性を共有する VM のグループからのトラフィックにポリシーを指定することができます。 **show attribute** コマンドが追加されました。 次の画面が追加されました。 **[Configuration]** > **[Firewall]** > **[VM Atttribute Agent]**

機能	説明
内部ゲートウェイ プロトコルの古いルートのタイムアウト	OSPF などの内部ゲートウェイ プロトコルの古いルートを削除するためのタイムアウトを設定できるようになりました。 **timeout igp stale-route** コマンドが追加されました。 **[Configuration]** > **[Firewall]** > **[Advanced]** > **[Global Timeouts]** の画面が変更されました。
オブジェクト グループ検索に関するネットワーク オブジェクトの制限。	**object-group-search access-control** コマンドを使用してオブジェクト グループ検索を有効にすることで、アクセス ルールの検索に必要なメモリを抑えることができます。オブジェクト グループ検索を有効にした場合、ネットワーク オブジェクトまたはサービス オブジェクトは拡張されませんが、それらのグループの定義に基づいて一致するアクセス ルールが検索されます。 このリリース以降、以下の制限が適用されます。接続ごとに、送信元と宛先の両方の IP アドレスがネットワーク オブジェクトと照合されます。発信元アドレスに一致するオブジェクトの数が、宛先アドレスと一致する数の 1 万倍を超えると接続が切断されます。 このチェックは、パフォーマンスの低下を防止します。一致件数が膨大になることを防ぐためにルールを設定します。
ルーティング機能	
31 ビット サブネットマスク	ルーテッドインターフェイスに関しては、ポイントツーポイント接続向けの31 ビットのサブネットに IP アドレスを設定できます。31 ビット サブネットには 2 つのアドレスのみが含まれます。通常、サブネットの最初と最後のアドレスはネットワーク用とブロードキャスト用に予約されており、2 アドレス サブネットは使用できません。ただし、ポイントツーポイント接続があり、ネットワーク アドレスやブロードキャスト アドレスが不要な場合は、IPv4 形式でアドレスを保持するのに 31 サブネット ビットが役立ちます。たとえば、2 つの ASA 間のフェールオーバー リンクに必要なアドレスは 2 つだけです。リンクの一方の側から送信されるパケットはすべてもう一方の側で受信され、ブロードキャスティングは必要ありません。また、SNMP や Syslog を実行する管理ステーションを直接接続することもできます。この機能は、ブリッジグループ用の BVI、またはマルチキャストルーティングではサポートされていません。 次のコマンドが変更されました。**ip address**、**http**、**logging host**、**snmp-server host**、**ssh** 次の画面が変更されました。 **[Configuration]** > **[Device Setup]** > **[Interface Settings]** > **[Interfaces]** > **[Add Interface]** > **[General]**
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
Firepower 4100/9300 シャーシ 上の ASA のサイト間クラスタリングの改善	ASA クラスタを展開すると、それぞれの Firepower 4100/9300 シャーシのサイト ID を設定できます。以前は ASA アプリケーション内でサイト ID を設定する必要がありました。この新しい機能は、初期導入を簡単にします。ASA 構成内でサイト ID を設定できなくなったことに注意してください。また、サイト間クラスタリングとの互換性を高めるために、安定性とパフォーマンスに関する複数の改善が含まれる ASA 9.7(1) および FXOS 2.1.1 にアップグレードすることを推奨します。 次のコマンドが変更されました。**site-id** 次の画面が変更されました。**[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[ASA Cluster]** > **[Cluster Configuration]**
ディレクタ ローカリゼーション：データセンターのサイト間クラスタリングの改善	データ センターのパフォーマンスを向上し、サイト間クラスタリングのトラフィックを維持するために、ディレクタ ローカリゼーションを有効にできます。通常、新しい接続は特定のサイト内のクラスタ メンバーによってロード バランスされ、所有されています。しかし、ASA は任意のサイトのメンバーにディレクタ ロールを割り当てます。ディレクタ ローカリゼーションにより、所有者と同じサイトのローカル ディレクタ、どのサイトにも存在可能なグローバル ディレクタという追加のディレクタ ロールが有効になります。所有者とディレクタが同一サイトに存在すると、パフォーマンスが向上します。また、元の所有者が失敗した場合、ローカルなディレクタは同じサイトで新しい接続の所有者を選択します。グローバルなディレクタは、クラスタ メンバーが別のサイトで所有される接続のパケットを受信する場合に使用されます。 次のコマンドが導入または変更されました。**director-localization**、**show asp table cluster chash**、**show conn**、**show conn detail** 次の画面を変更しました。**[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[ASA Cluster]** > **[Cluster Configuration]**
高速検出の設定が可能な、フェールオーバーのポーリングをモニタリングするインターフェイス リンク ステート	デフォルトでは、フェールオーバーペアの ASA は、500 ミリ秒ごとにインターフェイスのリンク ステートをチェックします。ポーリングの間隔を 300 ミリ秒から 799 ミリ秒の間で設定できるようになりました。たとえば、ポーリング時間を 300 ミリ秒に設定すると、ASA はインターフェイス障害やトリガーのフェールオーバーをより迅速に検出できます。 次のコマンドが導入されました。**failover polltime link-state** 次の画面が変更されました。**[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[Failover]** > **[Criteria]**

機能	説明
FirePOWER 9300 および 4100 でのアクティブ/スタンバイ フェールオーバー ヘルス モニタリングで、双方向フォワーディング検出（BFD）がサポートされました。	FirePOWER 9300 および 4100 上のアクティブ/スタンバイ ペアの 2 つのユニット間のフェールオーバーヘルスチェックに対して、双方向フォワーディング検出（BFD）を有効にできるようになりました。ヘルス チェックに BFD を使用すると、デフォルトのヘルスチェックより信頼性が高まり、CPU の使用を抑えることができます。 次のコマンドが導入されました。**failover health-check bfd** 次の画面が変更されました。**[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[Failover]** > **[Setup]**
VPN 機能	
IKEv2 静的暗号マップ用ダイナミック RRI	**crypto map** に **dynamic** が指定されている場合、IPSec セキュリティ アソシエーション（SA）の確立に成功すると、ダイナミック リバース ルート インジェクションが発生します。ルートは、ネゴシエートされたセレクタの情報に基づいて追加されます。IPsec SA's が削除されると、このルートは削除されます。ダイナミック RRI は、IKEv2 ベースの静的暗号マップでのみサポートされます。 次のコマンドが変更されました。**crypto map set reverse-route**。 次の画面が変更されました。[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Advanced] > [IPsec] > [Crypto Maps] > [Add/Edit] > [Tunnel Policy (Crypto Maps) - Advanced]
ASA VPN モジュールの仮想トンネル インターフェイス（VTI）のサポート	ASA VPN モジュールが、仮想トンネル インターフェイス（VTI）と呼ばれる新しい論理インターフェイスによって強化されており、ピアへの VPN トンネルを表すために使用されます。これは、トンネルの各終端に接続されている IPsec プロファイルを利用したルート ベースの VPN をサポートします。VTI を使用することにより、静的暗号マップのアクセス リストを設定してインターフェイスにマッピングすることが不要になります。 次のコマンドが導入されました。**crypto ipsec profile**、**interface tunnel**、**responder-only**、**set ikev1 transform-set**、**set pfs**、**set security-association lifetime**、**tunnel destination**、**tunnel mode ipsec**、**tunnel protection ipsec profile**、**tunnel source interface**。 次の画面が導入されました。 **[Configuration]** > **[Site-to-Site VPN]** > **[Advanced]** > **[IPsec Proposals (Transform Sets)]** > **[IPsec Profile]** **[Configuration]** > **[Site-to-Site VPN]** > **[Advanced]** > **[IPsec Proposals (Transform Sets)]** > **[IPsec Profile]** > **[Add]** > **[Add IPsec Profile]** **[Configuration]** > **[Device Setup]** > **[Interface Settings]** > **[Interfaces]** > **[Add]** > **[VTI Interface]** **[Configuration]** > **[Device Setup]** > **[Interface Settings]** > **[Interfaces]** > **[Add]** > **[VTI Interface]** > **[General]** **[Configuration]** > **[Device Setup]** > **[Interface Settings]** > **[Interfaces]** > **[Add]** > **[VTI Interface]** > **[Advanced]**

機能	説明
セキュアクライアント 用 SAML 2.0 ベースの SSO	SAML 2.0 ベースのサービス プロバイダー IdP が、プライベート ネットワークでサポートされます。ユーザーとサービス間のゲートウェイとしてASAを使用すると、IdP の認証は制限付きの名前非表示 webvpn セッションで処理され、IdP とユーザー間のすべてのトラフィックは変換されます。 次のコマンドが追加されました。**saml idp** 次のコマンドが変更されました。**debug webvpn saml**、**show saml metadata** 次の画面が変更されました。**[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Advanced] > [Single Sign On Servers] > [Add SSO Server]**.
CMPv2	ワイヤレス LTE ネットワークのセキュリティ ゲートウェイ デバイスとして配置できるように、ASA が証明書の管理プロトコル（CMPv2）を使用した特定の管理機能をサポートするようになりました。 次のコマンドが変更されました。**enrollment url**、**keypair**、**auto-update**、**crypto-ca-trustpoint**、**show crypto ca server certificates**、**show crypto key**、**show tech-support** 次の画面が変更されました。**[Configuration] > [Remote Access VPN] > [Certificate Management] > [Identity Certificates] > [Add an Identity Certificate]**
マルチ証明書認証	セキュアクライアント SSL クライアントプロトコルと IKEv2 クライアントプロトコルを使用して、セッションごとに複数の認証を検証できるようになりました。マルチ証明書認証のプロトコル交換を定義し、これを両方のセッションタイプで利用できるように、集約認証プロトコルが拡張されました。 次のコマンドが変更されました。**authentication {[aaa] [certificate | multiple-certificate] | saml}** 次の画面が変更されました。 **[設定（Configuration）] > [リモートアクセスVPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [ダイナミックアクセスポリシー（Dynamic Access Policies）] > [Edit（編集）] > [Secure Client] > [接続プロファイル（Connection Profile）]** **[設定（Configuration）] > [リモートアクセスVPN（Remote Access VPN）] > [ネットワーククライアントアクセス（Network Client Access）] > [Secure Client] [接続プロファイル（Connection Profiles）] > [編集（Edit）] [Secure Client] [接続プロファイル（Connection Profiles）]**
スプリット トンネリング ルーティングの制限の引き上げ	AC-SSL および AC-IKEv2 のスプリット トンネリング ルートの制限は、200 から 1200 に引き上げられました。IKEv1 の制限は 200 で変わりません。

機能	説明
Chrome のスマート トンネル サポート	Mac デバイスや Windows デバイスの Chrome ブラウザでスマート トンネルをサポートするための新しいメソッドが作成されました。Chrome Smart Tunnel Extension は、Netscape プラグイン アプリケーション プログラム インターフェイス（NPAPI）に代わるものです。NPAPI は、Chrome ではサポートされなくなりました。この拡張プログラムをインストールしていない Chrome でスマート トンネルに対応したブックマークをクリックすると、ユーザーは拡張プログラムを取得できるように Chrome ウェブストアにリダイレクトされます。Chrome を新規インストールする場合、ユーザーは拡張プログラムを取得できるように Chrome ウェブストアに移動されます。この拡張プログラムは、スマート トンネルの実行に必要なバイナリを ASA からダウンロードします。通常のブックマーク、およびスマート トンネルを使用する際のアプリケーション設定は、この新しい拡張プログラムのインストール プロセス以外は変更されません。
クライアントレス SSL VPN：すべての Web インターフェイスのセッション情報	すべての Web インターフェイスが、ログインに使用されたユーザー名などの現在のセッションの詳細と、現在割り当てられているユーザー権限を表示するようになりました。これは、ユーザーが現在のユーザー セッションを知るのに役立ち、ユーザー セキュリティの向上につながります。
クライアントレス SSL VPN：Web アプリケーション セッションのクッキーすべての検証	すべての Web アプリケーションは、セキュリティ関連のクッキーすべてを検証してはじめて、アクセス権を付与するようになります。要求があるごとに、認証トークンまたはセッション ID を持つ各クッキーが検証され、その後にユーザー セッションへのアクセスが付与されます。同じ要求に複数のセッション Cookie が含まれている場合、その接続は破棄されます。検証に失敗したクッキーは無効なクッキーとして扱われ、そのイベントは監査ログに追加されます。
セキュアクライアント：最大接続時間アラート間隔が、Cisco Secure Client の AnyConnect VPN モジュール の接続に関するグループポリシーでサポートされるようになりました。	このアラート間隔は、最大接続時間に達する前に、終了を警告するメッセージをユーザーに表示する間隔を指定します。有効な時間間隔は 1 ～ 30 分です。デフォルトは 30 分です。以前は、クライアントレス接続とサイト間 VPN 接続でサポートされていました。 次のコマンドを接続に使用できるようになりました。 セキュアクライアント **vpn-session-timeout alert-interval** 次の画面が変更されました。[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] > [Add/Edit] > [General] > [More Options]。[Maximum Connect Time Alert Interval] フィールドが追加されました。
AAA 機能	
AAA 用 LDAP サーバーおよび TACACS+ サーバーの IPv6 アドレスのサポート	AAA に使用する LDAP サーバーおよび TACACS+ サーバーで IPv4 アドレスか IPv6 アドレスのいずれかを使用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。**aaa-server host**、**test aaa-server** 次の画面が変更されました。**[Configuration]** > **[Device Management]** > **[Users/AAA]** > **[AAA Server Groups]** > **[Add AAA Server Group]**

機能	説明
管理機能	
すべてのローカル **username** および **enable** パスワードに対する PBKDF2 ハッシュ	長さ制限内のすべてのローカル **username** および **enable** パスワードは、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。以前は、32 文字以下のパスワードが MD5 ベースのハッシュ メソッドを使用していました。既存のパスワードでは、ユーザーが新しいパスワードを入力しない限り、MD5 ベースのハッシュが引き続き使用されます。ダウングレードのガイドラインについては、『一般操作構成ガイド』の「ソフトウェアおよびコンフィギュレーション」の章を参照してください。 次のコマンドが変更されました。**enable password**、**username** 次の画面が変更されました。 **[Configuration]** > **[Device Setup]** > **[Device Name/Password]** > **[Enable Password]** **[Configuration]** > **[Device Management]** > **[Users/AAA]** > **[User Accounts]** > **[Add/Edit User Account]** > **[Identity]**
ライセンシング機能	
Firepower 4100/9300 シャーシ 上のフェールオーバー ペアのライセンス変更	アクティブなユニットのみがライセンス権限を要求します。以前は、両方のユニットがライセンスの権限付与を要求していました。FXOS 2.1.1 でサポートされます。
モニタリング機能とトラブルシューティング機能	
トレースルート用の IPv6 アドレスのサポート	**traceroute** コマンドが変更され、IPv6 アドレスも受け入れられるようになりました。 次のコマンドが変更されました。**traceroute** 次の画面が変更されました。**[Tools]** > **[Traceroute]**
ブリッジ グループ メンバー インターフェイス用のパケット トレーサのサポート	ブリッジ グループ メンバー インターフェイスにパケット トレーサを使用できるようになりました。 **packet-tracer** コマンドに次の 2 つのオプションが追加されました。**vlan-id** および **dmac** パケット トレーサの画面に [VLAN ID] および [Destination MAC Address] フィールドが追加されました。**[Tools]** > **[Packet Tracer]**
syslog サーバーの IPv6 アドレスのサポート	syslog サーバーに IPv6 アドレスを設定して、TCP や UDP 経由で syslog を記録または送信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。**logging host**、**show running config**、**show logging** 次の画面が変更されました。**[Configuration]** > **[Device Management]** > **[Logging]** > **[Syslog Servers]** > **[Add Syslog Server]**

機能	説明
SNMP の MIB および OID	ASA は、ISA 3000 の Precision Time Protocol（PTP）の一部として、エンドツーエンド トランスペアレント クロック モードに対応する SNMP MIB オブジェクトをサポートするようになりました。次の SNMP MIB オブジェクトがサポートされます。 • ciscoPtpMIBSystemInfo • cPtpClockDefaultDSTable • cPtpClockTransDefaultDSTable • cPtpClockPortTransDSTable
手動によるパケット キャプチャの停止と開始	キャプチャを手動で停止および開始できるようになりました。 追加/変更されたコマンド： **capture stop** 追加/変更された画面：**[Wizards]** > **[Packet Capture Wizard]** > **[Run Captures]** 追加/変更されたオプション：[Start] ボタン、[Stop] ボタン

バージョン 9.6 の新機能

ASA 9.6(4)/ASDM 7.9(1) 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)/ASDM 7.7(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	

機能	説明
SSH公開キー認証を使用するユーザーの認証とパスワードを使用するユーザーの認証を区別します。	9.6(2) より前のリリースでは、ローカルユーザーデータベース（**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。ユーザーに対して **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ー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ー名にのみ適用されます。また、任意の AAA サーバー タイプ（**aaa authentication ssh console radius_1** など）を使用できます。たとえば、一部のユーザー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、他のユーザーは 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。 変更された画面はありません。 バージョン *9.8(1)* でも同様です。

ASDM 7.6(2.150) の新機能

リリース：2016年10月12日

このリリースに新機能はありません。

ASA 9.6(2)/ASDM 7.6(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。 追加または変更された画面はありません。

機能	説明
ASA 仮想 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、ASA 仮想 の Virtio 仮想インターフェイスを追加または削除できます。ASA 仮想 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。ASA 仮想 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 ASA 仮想 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。
ASA 仮想 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	ASA 仮想 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 ASA 仮想 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 ASA 仮想 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**
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 サーバー 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 サーバーの接続とスマート 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ー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	

機能	説明
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** 次のページが変更されました。**[Configuration]** > **[Firewall]** > **[Objects]** > **[Inspection Maps]** > **[DNS]** > [Add/Edit] ダイアログボックス
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** 次のページが追加または変更されました。**[Configuration]** > **[Firewall]** > **[Objects]** > **[Inspection Maps]** > **[M3UA]**、サービス ポリシー ルールの場合は **[Rule Action]** > **[Protocol Inspection]** タブ
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** 次のタブにオプションが追加されました。[Add/Edit Service Policy] ダイアログボックスの [Rule Actions] > [Protocol Inspection]
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	サーバー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 サーバーが 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 サーバー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** 次の画面が変更されました。**[Configuration]** > **[Device Management]** > **[Cloud Web Security]**

機能	説明
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** 次の画面が変更されました。**[Configuration]** > **[Firewall]** > **[Advanced]** > **[Global Timeouts]** 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** 次の画面が変更されました。**[Configuration]** > **[Firewall]** > **[Objects]** > **[TCP Maps]** > [Add/Edit] ダイアログボックス
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。 変更された画面はありません。
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。

機能	説明
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** 次の画面が変更されました。**[Configuration]** > **[Device Management]** > **[Advanced]** > **[ARP]** > **[ARP Static Table]**
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** 次の画面が変更されました。**[Configuration]** > **[Firewall]** > **[EtherType Rules]**。
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/ユーザー名	セキュアクライアント 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ー名取得機能の 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。 変更された画面はありません。
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：該当ユーザーのみに関連付けられ、該当ユーザー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、あらゆるユーザー 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** 次の画面が変更されました。**[Configuration]** > **[Context Management]** > **[Resource Class]** > **[Add Resource Class]** **[Configuration]** > **[Context Management]** > **[Security Contexts]**
マルチコンテキストモードでのセキュアクライアント プロファイルのサポート	マルチコンテキストモードでの セキュアクライアント プロファイルのサポート ASDM を使用して新しいプロファイルを追加するには、Secure Client 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 セキュアクライアント 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 セキュアクライアント 接続のステートフル フェールオーバーがサポートされるようになりました。 変更されたコマンドはありません。 変更された画面はありません。
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。 変更された画面はありません。
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。 変更された画面はありません。
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。 変更された画面はありません。
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、Secure Client 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。 次の画面が変更されました。**[設定（Configuration）] > [リモートアクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [**セキュアクライアント**プロファイル（Profile）]**
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** 次の画面が変更されました。**[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Advanced] > [IPsec] > [IPsec Proposals (Transform Sets)] > [IKEv2 proposals] > [Add/Edit]**

機能	説明
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** 次の画面に [Enable IPsec Inner Routing Lookup] チェックボックスが追加されました。**[Configuration]** > **[Remote Access VPN]** > **[Network (Client) Access]** > **[Advanced]** > **[IPsec]** > **[Crypto Maps]**
証明書とセキュアな接続の機能	
ASA クライアントによるサーバー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ー証明書は、[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	サーバーが認証のために 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 サーバーへ接続します。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 サーバーモード 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ユーザー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** 次の画面を変更しました。**[Configuration]** > **[Device Management]** > **[Management Access]** > **[ASDM/HTTPS/Telnet/SSH]**

機能	説明
セキュアな syslog サーバーの接続とスマート 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ー 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 サーバーとスマート ライセンス サーバーへの 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** 次の画面が変更されました。 **[Configuration] > [Remote Access VPN] > [Advanced]** **[Configuration] > [Device Management] > [Logging] > [Syslog Servers] > [Add/Edit]** **[Configuration] > [Device Management] > [Smart Call Home]**
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 ユーザー 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。ユーザー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ー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** 次の画面が変更されました。 **[Configuration] > [Device Management] > [Management Access] > [ASDM/HTTPS/Telnet/SSH]** **[Configuration] > [Device Management] > [Users/AAA] > [User Accounts] > [Add/Edit User Account]**
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** 次の画面が変更されました。**[Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] > [Advanced]**
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** 次の画面が追加または変更されました。 **[Configuration]** > **[Device Setup]** > **[Routing]** > **[BFD]** > **[Template]** **[Configuration]** > **[Device Setup]** > **[Routing]** > **[BFD]** > **[Interface]** **[Configuration]** > **[Device Setup]** > **[Routing]** > **[BFD]** > **[Map]** **[Configuration]** > **[Device Setup]** > **[Routing]** > **[BGP]** > **[IPv6 Family]** > **[Neighbors]**

機能	説明
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 サーバーから 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 サーバー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 サーバー：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** 次の画面が追加または変更されました。 **[Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] > [Add Interface] > [IPv6]** **[Configuration] > [Device Management] > [DHCP] > [DHCP Pool]** **[Configuration] > [Device Setup] > [Routing] > [BGP] > [IPv6 Family] > [Networks]** **[Monitoring] > [interfaces] > [DHCP]**
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の セキュアクライアント からのダイナミック ACL における同期時間の改善	フェールオーバーペアで セキュアクライアント を使用するとき、関連付けられているダイナミック ACL（dACL）における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。 変更された画面はありません。
ライセンシング機能	

機能	説明
ASA 仮想 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、ASA 仮想 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 ASA 仮想 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永続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** ASDM サポートはありません。 バージョン *9.5(2.200)* でも同様です。
ASA 仮想 のサテライトサーバーのサポート	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 サテライトサーバー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。 変更された画面はありません。
ASA 仮想 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。 変更された画面はありません。
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
ASA 仮想 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、ASA 仮想 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、[Configuration] > [Device Management] > [Licensing] > [Smart Licensing] ページで [Force registration] オプションを指定して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** 変更された画面はありません。 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** 変更された画面はありません。
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** 変更された画面はありません。
NetFlow経由の接続ごとのトラッキング パケット数の追跡	NetFlow ユーザー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。 変更された画面はありません。

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 ユーザーは、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。ユーザーがネイティブ engineID を指定しない場合、**show running config** 出力に engineID がユーザーごとに 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** ASDM サポートはありません。 バージョン *9.4(3)* でも同様です。

ASA 9.6(1)/ASDM 7.6(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。 追加または変更された画面はありません。
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。 追加または変更された画面はありません。

機能	説明
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**。 ASDM サポートはありません。
ファイアウォール機能	
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**。 次の画面が追加または変更されました。 **[Configuration] > [Firewall] > [Objects] > [Inspect Maps] > [Diameter]** **[Configuration] > [Firewall] > [Service Policy]** の [Add/Edit] ウィザードの **[Rule Actions] > [Protocol Inspection]** タブ
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。 追加または変更された画面はありません。
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**。 H.323 インスペクション ポリシー マップの [Call Attributes] タブにオプションが追加されました。
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**。 **[Configuration] > [Firewall] > [Identity By TrustSec]** と [SGT Map Setup] ダイアログ ボックスが変更されました。

機能	説明
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。 追加または変更された画面はありません。
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、セキュア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** 追加または変更された画面はありません。
設定可能な SSH 暗号機能と HMAC アルゴリズム	ユーザーは 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**。 次の画面が導入されました。**[Configuration]** > **[Device Management]** > **[Advanced]** > **[SSH Ciphers]** *9.1(7)* 、*9.4(3)* および *9.5(3)* でも使用可能です。

機能	説明
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** 次の画面に機能が追加されました。**[Configuration]** > **[Device Management]** > **[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ーについて、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.** 次の画面が導入されました。 **[Configuration] > [Device Setup] > [Routing] > [ISIS]** **[Monitoring] > [Routing] > [ISIS]**
ハイ アベイラビリティとスケーラビリティの各機能	
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** 次の画面を変更しました。**[Configuration]** > **[Device Setup]** > **[Interface Settings]** > **[Interfaces]** > **[Add/Edit EtherChannel Interface]** > **[Advanced]**

機能	説明
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** 次の画面が変更されました。 **[Configuration]** > **[Device Setup]** > **[Device Name/Password]** > **[Enable Password]** **[Configuration]** > **[Device Management]** > **[Users/AAA]** > **[User Accounts]** > **[Add/Edit User Account]** > **[Identity]**
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 4GB 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。 追加または変更された画面はありません。 *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。

バージョン 9.5 の新機能

ASA 9.5(3.9)/ASDM 7.6(2) の新機能

リリース：**2017年4月11日**

（注） バージョン 9.5(3) は、バグ CSCvd78303 に基づき Cisco.com から削除されました。

機能	説明
リモート アクセス機能	

機能	説明
設定可能な SSH 暗号機能と HMAC アルゴリズム	ユーザーは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**。 次の画面が導入されました。**[Configuration]** > **[Device Management]** > **[Advanced]** > **[SSH Ciphers]** *9.1(7)* および *9.4(3)* でも使用可能です。

ASA 仮想 9.5(2.200)/ASDM 7.5(2.153) の新機能

リリース：**2016年1月28日**

（注） このリリースは、ASA 仮想 のみをサポートします。

機能	説明
プラットフォーム機能	
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。ASA 仮想 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 ASA 仮想 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。
ライセンシング機能	

機能	説明
ASA 仮想 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、ASA 仮想 用に永続ライセンスを要求できます。 （注） すべてのアカウントが永続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** ASDM サポートはありません。
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、ASA 仮想 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、[Configuration] > [Device Management] > [Licensing] > [Smart Licensing] ページで [Force registration] オプションを指定して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** 変更された画面はありません。

ASA 9.5(2.1)/ASDM 7.5(2) の新機能

リリース：**2015年12月14日**

（注） このリリースは、Firepower 9300 の ASA のみをサポートします。

機能	説明
プラットフォーム機能	

機能	説明
Firepower 9300 での ASA の VPN サポート	FXOS 1.1.3 では、VPN 機能を設定できるようになりました。
ファイアウォール機能	
Firepower 9300 での ASA のフローのオフロード	ASA からオフロードし、（Firepower 9300 上の）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。これにより、データセンターのより大きなデータ フローのパフォーマンスが向上します。 FXOS 1.1.3 も必要です。 次のコマンドが追加または変更されました。**clear flow-offload**、**flow-offload enable**、**set-connection advanced-options flow-offload**、**show conn detail**、**show flow-offload**。 次の画面が追加または変更されました：**[Configuration]** > **[Firewall]** > **[Advanced]** > **[Offload Engine]**、**[Configuration]** > **[Firewall]** > **[Service Policy Rules]** の下でルールを追加または編集する場合の **[Rule Actions]** > **[Connection Settings]** タブ。
ハイ アベイラビリティ機能	
Firepower 9300 での 6 モジュールのシャーシ間クラスタリング と ASA のサイト間クラスタリング	FXOS 1.1.3 では、シャーシ間、さらにサイト間クラスタリングを有効にできます。最大 6 つのシャーシに最大 6 つのモジュールを含めることができます。 変更されたコマンドはありません。 変更された画面はありません。
ライセンシング機能	
Firepower 9300 の ASA に高度暗号化（3DES）ライセンスを自動的に適用	通常の Cisco Smart Software Manager（SSM）ユーザーの場合、FirePOWER 9300 で登録トークンを適用すると、対象となるお客様には強力な暗号化ライセンスが自動的に有効になります。 （注） スマート ソフトウェア マネージャ サテライトが導入されている場合、ASDM や他の高度暗号機能を使用するには、ASA の展開後に ASA CLI を使用して、高度暗号化ライセンスを有効にする必要があります。 この機能には、FXOS 1.1.3 が必要です。 サテライト以外の構成では、次のコマンドが除去されました。**feature strong-encryption** 次の画面が変更されました。**[Configuration]** > **[Device Management]** > **[Licensing]** > **[Smart License]**

ASA 9.5(2)/ASDM 7.5(2) の新機能

リリース：**2015年11月30日**

機能	説明
プラットフォーム機能	
Cisco ISA 3000 サポート	Cisco ISA 3000 は、DIN レールにマウントされた高耐久型の産業用セキュリティ アプライアンスです。ギガビットイーサネットと専用管理ポートを備えた、低消費電型ファンレス デバイスです。このモデルには ASA Firepower モジュールが事前にインストールされています。このモデルの特別な機能として、カスタマイズされたトランスペアレントモードのデフォルト設定と、電源喪失時もトラフィックがアプライアンスを通過することを可能にするハードウェア バイパス機能があります。 次のコマンドが導入されました。**hardware-bypass**、**hardware-bypass manual**、**hardware-bypass boot-delay** 次の画面が変更されました。**[Configuration]** > **[Device Management]** > **[Hardware Bypass]** バージョン *9.4(1.225)* でも同様です。
ファイアウォール機能	
DCERPC インスペクションの改善および UUID フィルタリング	DCERPC インスペクションは、OxidResolver ServerAlive2 opnum5 メッセージに対して NAT をサポートするようになりました。また、DCERPC メッセージの汎用一意識別子（UUID）でフィルタリングし、特定のメッセージ タイプをリセットするかログに記録できるようになりました。UUID フィルタリング用の新しい DCERPC インスペクション クラス マップがあります。 次のコマンドが導入されました。**match** [**not**] **uuid**。次のコマンドが変更されました。**class-map type inspect**。 **[Configuration]** > **[Firewall]** > **[Objects]** > **[Class Maps]** > **[DCERPC]** の画面が追加されました。 次の画面が変更されました。**[Configuration]** > **[Firewall]** > **[Objects]** > **[Inspect Maps]** > **[DCERPC]**。

機能	説明
Diameter インスペクション	Diameter トラフィックを検査できるようになりました。Diameter インスペクションには キャリア ライセンスが必要です。 次のコマンドが導入または変更されました。**class-map type inspect diameter**、**diameter**、**inspect diameter**、**match application-id**、**match avp**、**match command-code**、**policy-map type inspect diameter**、**show conn detail**、**show diameter**、**show service-policy inspect diameter**、**unsupported** 次の画面が追加または変更されました。 **[Configuration]** > **[Firewall]** > **[Objects]** > **[Inspect Maps]** > **[Diameter]** と **[Diameter AVP]** **[Configuration]** > **[Firewall]** > **[Service Policy]** の [Add/Edit] ウィザードの **[Rule Actions]** > **[Protocol Inspection]** タブ
SCTP インスペクションとアクセス制御	サービス オブジェクト、アクセス コントロール リスト（ACL）とアクセス ルールにて SCTP プロトコルとポートの仕様を使用して、SCTP トラフィックを検査できるようになりました。SCTP インスペクションには キャリア ライセンスが必要です。 次のコマンドが導入されました。**access-list extended** 、**clear conn protocol sctp**、**inspect sctp**、**match ppid**、**nat static** (object)、**policy-map type inspect sctp**、**service-object**、**service**、**set connection advanced-options sctp-state-bypass**、**show conn protocol sctp**、**show local-host connection sctp**、**show service-policy inspect sctp**、**timeout sctp** 次の画面が追加または変更されました。 **[Configuration]** > **[Firewall]** > **[Access Rules]** の [Add/Edit] ダイアログ **[Configuration]** > **[Firewall]** > **[Advanced]** > **[ACL Manager]** の [Add/Edit] ダイアログ **[Configuration]** > **[Firewall]** > **[Advanced]** > **[Global Timeouts]** **[Configuration]** > **[Firewall]** > **[NAT]** の [Add/Edit static network object NAT rule] 、[Advanced NAT Settings] ダイアログボックス **[Configuration]** > **[Firewall]** > **[Objects]** > **[Service Objects/Groups]** の [Add/Edit] ダイアログ **[Configuration]** > **[Firewall]** > **[Objects]** > **[Inspect Maps]** > **[SCTP]** **[Configuration]** > **[Firewall]** > **[Service Policy]** の [Add/Edit] ウィサードの **[Rule Actions]** > **[Protocol Inspection]** と [Connection Settings] タブ

機能	説明
キャリア グレード NAT の強化は、フェールオーバーおよび ASA クラスタリングでサポートされます。	キャリア グレードまたは大規模 PAT では、NAT に 1 度に 1 つのポート変換を割り当てさせるのではなく、各ホストにポートのブロックを割り当てることができます（RFC 6888 を参照してください）。この機能は、フェールオーバーおよび ASA クラスタの導入でサポートされます。 次のコマンドが変更されました。**show local-host** 変更された画面はありません。
ASA FirePOWER 6.0 でのアクティブ認証向けキャプティブ ポータル。	キャプティブ ポータル機能では、ASA FirePOWER 6.0 で始まるアイデンティティ ポリシーを使用してアクティブ認証を有効にする必要があります。 次のコマンドが導入または変更されました。**captive-portal**、**clear configure captive-portal**、**show running-config captive-portal**。
ハイ アベイラビリティ機能	
サイト間フロー モビリティの LISP インスペクション	Cisco Locator/ID Separation Protocol（LISP）のアーキテクチャは、デバイス ID をその場所から 2 つの異なるナンバリング スペースに分離し、サーバーの移行をクライアントに対して透過的にします。ASA は、場所変更の LISP トラフィックを検査し、その情報をシームレスなクラスタリング運用に活用できます。ASA クラスタ メンバーは、最初のホップ ルータと出力トンネル ルータまたは入力トンネル ルータの間の LISP トラフィックを検査し、フロー オーナーの所在場所を新規サイトに変更します。 次のコマンドが導入または変更されました。**allowed-eid**、**clear cluster info flow-mobility counters**、**clear lisp eid**、**cluster flow-mobility lisp**、**debug cluster flow-mobility**、**debug lisp eid-notify-intercept**、**flow-mobility lisp**、**inspect lisp**、**policy-map type inspect lisp**、**site-id**、**show asp table classify domain inspect-lisp**、**show cluster info flow-mobility counters**、**show conn**、**show lisp eid**、**show service-policy**、**validate-key** 次の画面が導入または変更されました。 **[Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster] > [Cluster Configuration]** **[Configuration] > [Firewall] > [Objects] > [Inspect Maps] > [LISP]** **[Configuration] > [Firewall] > [Service Policy Rules] > [Protocol Inspection]** **[Configuration] > [Firewall] > [Service Policy Rules] > [Cluster]** **[Monitoring] > [Routing] > [LISP-EID Table]**
ASA 5516-X でのクラスタリングのサポート	ASA 5516-X が 2 ユニット クラスタをサポートするようになりました。基本ライセンスでは、2 ユニットのクラスタリングがデフォルトで有効化されています。 変更されたコマンドはありません。 変更された画面はありません。

機能	説明
クラスタリング トレース エントリの設定可能なレベル	デフォルトで、すべてのレベルクラスタリングイベントは、多くの下位レベルのイベント以外に、トレースバッファに含まれます。より上位レベルのイベントへのトレースを制限するために、クラスタの最小トレース レベルを設定できます。 次のコマンドが導入されました。**trace-level** 変更された画面はありません。
インターフェイス機能	
セカンデリ VLAN のプライマリ VLAN へのマッピングのサポート	サブ インターフェイスで、1 つ以上のセカンデリ VLAN を設定できるようになりました。ASA はセカンダリ VLAN でトラフィックを受信すると、そのトラフィックをプライマリ VLAN にマップします。 次のコマンドを導入または変更しました。**vlan secondary**、**show vlan mapping** 次の画面が変更されました。**[Configuration]** > **[Device Setup]** > **[Interface Settings]** > **[Interfaces]** **[Configuration]** > **[Device Setup]** > **[Interface Settings]** > **[Interfaces]** > **[Add Interface]** > **[General]**
ルーティング機能	
マルチキャスト ルーティングの PIM ブートストラップ ルータ（BSR）のサポート	ASA は、現在、異なるグループにマルチキャスト トラフィックをルーティングするためにスタティック RP を設定できるようサポートしています。複数の RP が存在する可能性のある大規模で複雑なネットワークについては、ASA では RP のモビリティに対応できるよう、PIM BSR を使用したダイナミック RP の選択をサポートします。 次のコマンドが導入されました。**clear pim group-map**、**debug pim bsr**、**pim bsr-border**、**pim bsr-candidate**、**show pim bsr-router**、**show pim group-map rp-timers** 次の画面が導入されました。**[Configuration]** > **[Device Setup]** > **[Routing]** > **[Multicast]** > **[PIM]** > **[Bootstrap Router]**
リモート アクセス機能	

機能	説明
マルチ コンテキスト モードでのリモートアクセスVPNサポート	次のリモート アクセス機能をマルチ コンテキスト モードで使用できるようになりました。 • AnyConnect 3.x 以降（SSL VPN のみ、IKEv2 はサポートしません） • 中央集中型 セキュアクライアント のイメージの設定 • セキュアクライアント のイメージのアップグレード • セキュアクライアント 接続のコンテキストリソース管理 （注） マルチコンテキストモードでは Secure Client Premier ライセンスが必要です。デフォルトやレガシーのライセンスは使用できません。 次のコマンドが導入されました。**limit-resource vpn anyconnect**、**limit-resource vpn burst anyconnect** 次の画面が変更されました。**[Configuration]** > **[Context Management]** > **[Resource Class]** > **[Add Resource Class]**
クライアントレス SSL VPN で SAML 2.0ベースのシングル サインオン（SSO）機能を提供	ASA は、SAML のサービス プロバイダーとして機能します。
クライアントレス SSL VPN の条件付きデバッグ	フィルタ条件設定に基づき、フィルタリングによりログをデバッグし、より深く分析できます。 debug コマンドに次の追加が導入されました。 • [no] debug webvpn condition user <user name> • [no] debug webvpn condition group <group name> • [no] debug webvpn condition p-ipaddress <ipv4> [subnet<mask>] • [no] debug webvpn condition p-ipaddress <ipv6> [prefix<prefix>] • debug webvpn condition reset • show debug webvpn condition • show webvpn debug-condition

機能	説明
クライアントレス SSL VPN キャッシュはデフォルトでは無効	クライアントレス SSL VPN のキャッシュはデフォルトで無効になりました。クライアントレス SSL VPN キャッシュを無効にすることで安定性が改善します。キャッシュを有効にするには手動で有効にする必要があります。 `webvpn` `  cache` `  no disable` 次のコマンドが変更されました。**cache** 次の画面が変更されました。**[Configuration]** > **[Remote Access VPN]** > **[Clientless SSL VPN Access]** > **[Advanced]** > **[Content Cache]**
ライセンシング機能	
サーバー証明書の発行階層が変更された場合の Smart Call Home/スマート ライセンス証明書の検証	スマート ライセンスでは、Smart Call Home インフラストラクチャが使用されます。ASA はバックグラウンドで Smart Call Home 匿名レポートを最初に設定するときに、Call Home サーバー証明書を発行した CA の証明書を含むトラストポイントを自動的に作成します。ASA はサーバー証明書の発行階層が変更された場合の証明書の検証をサポートします。トラストプールバンドルの定期的な自動更新を有効にできます。 次のコマンドが導入されました。**auto-import** 次の画面が変更されました。**[Configuration]** > **[Remote Access VPN]** > **[Certificate Management]** > **[Trusted Certificate Pool]** > **[Edit Policy]**
新しいキャリア ライセンス	新しいキャリア ライセンスは既存の GTP/GPRS ライセンスを置き換え、SCTP と Diameter インスペクションもサポートします。Firepower 9300 上の ASA の場合、**feature mobile-sp** コマンドは **feature carrier** コマンドに自動的に移行します。 次のコマンドが導入または変更されました。**feature carrier**、**show activation-key**、**show license**、**show tech-support**、**show version** 次の画面が変更されました。**[Configuration]** > **[Device Management]** > **[Licensing]** > **[Smart License]**
モニタリング機能	

機能	説明
SNMP engineID の同期	HA 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 ユーザーは、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。ユーザーがネイティブ engineID を指定しない場合、**show running config** 出力に engineID がユーザーごとに 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**、**no snmp-server user** 追加または変更された画面はありません。 *9.4(3)* でも使用可能です。
show tech support の強化	**show tech support** コマンドは現在次のとおりです。 • **dir all-filesystems** の出力が含まれます。この出力は次の場合に役立つことがあります。 • SSL VPN コンフィギュレーション：必要なリソースが ASA にあるかどうかを確認します。 • クラッシュ：クラッシュ ファイルの日付のタイムスタンプと存在を確認します。 • **show kernel cgroup-controller detail** の出力の削除：このコマンド出力は **show tech-support detail** の出力内に残されます。 次のコマンドが変更されました。**show tech support** 追加または変更された画面はありません。 *9.1(7)* および *9.4(3)* でも使用可能です。
デバッグ ロギング トレースの永続化	以前は、デバッグを syslog サーバーへリダイレクトするために **logging debug-trace** が有効になっている場合、（ネットワークの接続性またはタイムアウトにより）SSH 接続が切断されるとデバッグは削除されました。しかし、**logging** コマンドが有効である限りデバッグを永続的に保持されるようになりました。 **logging debug-trace** コマンドが変更されました。 変更された画面はありません。

ASA 9.5(1.5)/ASDM 7.5(1.112) の新機能

リリース：**2015年11月11日**

機能	説明
プラットフォーム機能	
ASA FirePOWER 6.0 のサポート	ASA FirePOWER モジュール向けのソフトウェア バージョン 6.0 は、以前からサポートされているすべてのデバイス モデルでサポートされます。
5512-X ～ 5585-X 向けの ASDM を介した ASA FirePOWER モジュール管理サポート	モジュールでバージョン 6.0 の実行時、Management Center（旧称：FireSIGHT Management Center）の代わりに ASDM を使用して、ASA FirePOWER モジュールを管理できます。6.0 を実行している場合は、ASDM で 5506-X、5506H-X 5506W-X、5508-X および 5516-X のモジュールも管理できます。 新しい画面またはコマンドは追加されていません。

ASDM 7.5(1.90) の新機能

リリース：**2015年10月14日**

機能	説明
リモート アクセス機能	
AnyConnect バージョン 4.2 のサポート	ASDM は、AnyConnect 4.2 およびネットワーク可視性モジュール（NVM）をサポートしています。NVM は、キャパシティとサービスの計画、監査、コンプライアンス、およびセキュリティ分析に関して、企業内管理者の実行能力を向上させます。NVM（ネットワーク可視性モジュール）は、エンドポイントのテレメトリを収集して、フロー データとファイル レピュテーションを syslog に記録し、さらに、ファイルの分析と UI インターフェイスの提供を行うコレクタ（サードパーティ ベンダー）にもフロー レコードをエクスポートします。 次の画面が変更されました。[設定（Configuration）]>[リモートアクセスVPN（Remote Access VPN）]>[ネットワーク（クライアント）アクセス（Network (Client) Access）]>[セキュアクライアント プロファイル（Profile）]（[ネットワーク可視性サービス プロファイル（Network Visibility Service Profile）] という新しいプロファイル）

ASA 仮想 9.5(1.200)/ASDM 7.5(1) の新機能

リリース：**2015年8月31日**

（注） このリリースは、ASA 仮想 のみをサポートします。

機能	説明
プラットフォーム機能	
Microsoft Hyper-V スーパーバイザ サポート	ASA 仮想 のハイパーバイザ ポートフォリオを拡張します。
ASAv5 低容量メモリ サポート	ASAv5 は 1 GB RAM のみでも実行できるようになりました。以前は 2 GB を必要としていました。導入済みの ASAv5 では、ライセンスにより許容される以上のメモリを使用していることを示すエラーが発生するため、割り当て済みメモリを 1 GB に減らす必要があります。

ASA 9.5(1)/ASDM 7.5(1) の新機能

リリース：**2015年8月12日**

（注） このバージョンは Firepower 9300 ASA セキュリティ モジュールまたは ISA 3000 をサポートしません。

機能	説明
ファイアウォール機能	
GTPv2 インスペクションと GTPv0/1 インスペクションの改善	GTP インスペクションは GTPv2 を処理できるようになりました。また、すべてのバージョンの GTP インスペクションで IPv6 アドレスがサポートされるようになりました。 次のコマンドが変更されました。**clear service-policy inspect gtp statistics**、**clear service-policy inspect gtp pdpmcb**、**clear service-policy inspect gtp request**、**match message id**、**show service-policy inspect gtp pdpmcb**、**show service-policy inspect gtp request**、**show service-policy inspect gtp statistics**、**timeout endpoint** 次のコマンドが非推奨になりました。**timeout gsn** 次の画面が変更されました。[Configuration] > [Firewall] > [Objects] > [Inspect Maps] > [GTP]。

機能	説明
IP オプション インスペクションの改善	IP オプション インスペクションは、すべての有効な IP オプションをサポートするようになりました。まだ定義されていないオプションを含む、標準または試行的なオプションを許可、クリア、またはドロップするようにインスペクションを調整できます。また、IP オプション インスペクション マップで明示的に定義されていないオプションのデフォルトの動作を設定できます。 次のコマンドを導入しました。 **basic-security, commercial-security, default, exp-flow-control, exp-measure, extended-security, imi-traffic-description, quick-start, record-route, timestamp** 次の画面が変更されました。[Configuration] > [Firewall] > [Objects] > [Inspect Maps] > [IP Options]。
キャリア グレード NAT の拡張	キャリア グレードまたは大規模 PAT では、NAT に 1 度に 1 つのポート変換を割り当てさせるのではなく、各ホストにポートのブロックを割り当てることができます（RFC 6888 を参照してください）。 次のコマンドが導入されました。**xlate block-allocation size**、**xlate block-allocation maximum-per-host**。**block-allocation** キーワードが **nat** コマンドに追加されました。 次の画面が導入されました。[Configuration] > [Firewall] > [Advanced] > [PAT Port Block Allocation]。 [Enable Block Allocation] オブジェクト NAT および Twice NAT ダイアログボックスが追加されました。
ハイ アベイラビリティ機能	
ルーテッド ファイアウォール モードのスパンド EtherChannel でのサイト間クラスタリング	ルーテッドモードでは、スパンド EtherChannel サイト間クラスタリングを使用することができます。MAC アドレスのフラッピングを防ぐには、各インターフェイスのサイト別の MAC アドレスがサイトのユニット上で共有できるように、各クラスタ メンバーのサイト ID を設定します。 次のコマンドを導入または変更しました。**site-id**、**mac-address site-id**、**show cluster info**、**show interface** 次の画面が変更されました。 [Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster] > [Cluster Configuration]
インターフェイスまたはクラスタ制御リンクが失敗した場合の auto-rejoin 動作の ASA クラスタのカスタマイズ	インターフェイスまたはクラスタ制御リンクが失敗した場合、auto-rejoin 動作をカスタマイズできます。 次のコマンドが導入されました。**health-check auto-rejoin** 次の画面が導入されました。 [Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster] > [Auto Rejoin]
ASA クラスタは、GTPv1 と GTPv2 をサポートします	ASA クラスタは、GTPv1 および GTPv2 インスペクションをサポートします。 変更されたコマンドはありません。 変更された画面はありません。

機能	説明
TCP 接続のクラスタ複製遅延	この機能で、ディレクタ/バックアップ フロー作成の遅延による存続期間が短いフローに関連する「不要な作業」を排除できます。 次のコマンドを導入しました。**cluster replication delay** 次の画面を導入しました。**[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[ASA Cluster Replication]** バージョン *9.4(1.152)* の *Firepower 9300 ASA* セキュリティ モジュールにも使用できます。
ASA クラスタリングのハードウェア モジュールのヘルス モニタリングの無効化	クラスタリング使用時、ASA はデフォルトで、設置されているハードウェア モジュール（ASA FirePOWER モジュールなど）のヘルス モニタリングを行います。特定のハードウェア モジュールの障害によってフェールオーバーをトリガーすることが望ましくない場合は、モジュールのモニタリングをディセーブルにできます。 次のコマンドを変更しました。**health-check monitor-interface service-module** 次の画面が変更されました。[Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster] > [Cluster Interface Health Monitoring]
ASA 5506H のフェールオーバー リンクとして、管理 1/1 インターフェイスを使用できるようになりました。	管理 1/1 インターフェイスは、ASA 5506H に限りフェールオーバー リンクとして設定できるようになりました。この機能により、デバイスの他のインターフェイスをデータ インターフェイスとして使用できます。この機能を使用した場合、ASA FirePOWER モジュールは使用できません。このモジュールでは管理 1/1 インターフェイスを通常の管理インターフェイスとして維持することが必須です。 次のコマンドが変更されました。**failover lan interface**、**failover link** 次の画面が変更されました。[Configuration] > [Device Management] > [High Availability and Scalability] > [Failover] > [Setup]
ルーティング機能	
ポリシーベース ルーティングの IPv6 サポート	ポリシーベース ルーティングで IPv6 アドレスがサポートされました。 次のコマンドが導入されました。**set ipv6 next-hop**、**set default ipv6-next hop**、**set ipv6 dscp** 次の画面が変更されました。 **[Configuration] > [Device Setup] > [Routing] > [Route Maps] > [Add Route Map] > [Policy Based Routing] [Configuration] > [Device Setup] > [Routing] > [Route Maps] > [Add Route Maps] > [Match Clause]**
ポリシーベース ルーティングの VXLAN サポート	VNI インターフェイスでポリシーベース ルーティングを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。 次の画面が変更されました。[Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] > [Add/Edit Interface] > [General]。

機能	説明
アイデンティティ ファイアウォールと Cisco TrustSec でのポリシーベース ルーティングのサポート	アイデンティティ ファイアウォールと Cisco TrustSec を設定し、ポリシーベース ルーティングのルートマップでアイデンティティ ファイアウォールと Cisco TrustSec ACL を使用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。 次の画面が変更されました。**[Configuration] > [Device Setup] > [Routing] > [Route Maps] > [Add Route Maps] > [Match Clause]**
管理専用インターフェイス用の個別のルーティング テーブル	データ トラフィックから管理トラフィックを区別して分離するため、ASA は管理専用インターフェイス用の個別のルーティング テーブルをサポートしました。 次のコマンドが導入または変更されました。**backup、clear ipv6 route management-only、clear route management-only、configure http、configure net、copy、enrollment source、name-server、restore、show asp table route-management-only、show ipv6 route management-only show route management-only** 変更された画面はありません。
Protocol Independent Multicast Source-Specific Multicast（PIM-SSM）パススルーのサポート	ASA では、最後のホップ ルータである場合を除いて、マルチキャスト ルーティングが有効になっているときに PIM-SSM パケットが通過できるようになりました。この機能により、さまざまな攻撃から保護すると同時に、マルチキャスト グループをより柔軟に選択できるようになりました。ホストは、明示的に要求された送信元からのトラフィックのみを受信します。 変更されたコマンドはありません。 変更された画面はありません。
リモート アクセス機能	
IPv6 VLAN マッピング	ASA VPN コードは IPv6 の機能を完全にサポートするよう強化されました。管理者による設定の変更は不要です。
クライアントレス SSL VPN の SharePoint 2013 サポート	SharePoint のこの新バージョンが新たにサポートされ、事前定義されているアプリケーションテンプレートが追加されました。 次の画面が変更されました。[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Portal] > [Bookmarks] > [Add Bookmark List] > [Select Bookmark Type] > [Predefined application templates]
クライアントレス VPN のダイナミック ブックマーク	ブックマークを使用する際のマクロのリストに CSCO_WEBVPN_DYNAMIC_URL と CSCO_WEBVPN_MACROLIST が追加されました。これらのマクロは、管理者が複数のブックマーク リンクを生成できる単一のブックマークをクライアントレス ユーザーのポータル上で設定し、ブックマークを静的に設定して LDAP 属性マップが提供する任意のサイズのリストを利用できるようにします。 次の画面が変更されました。[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Portal] > [Bookmarks]。

機能	説明
VPN バナーの長さの増加	VPN リモート クライアント ポータルでのログイン後に表示される全体的なバナーの長さが、500 ～ 4000 文字に増加しました。 次のコマンドが変更されました。**banner**（グループ ポリシー） 次の画面が変更されました。**[Configuration] > [Remote Access VPN] > .... [Add/Edit Internal Group Policy] > [General Parameters] > [Banner]**。
ASA 5506-X、5506W-X、5506H-X および 5508-X の Cisco Easy VPN クライアント	このリリースは、ASA 5506-X シリーズでの Cisco Easy VPN の使用をサポートし、かつ ASA 5508-X 用の Cisco Easy VPN をサポートします。ASA は、VPN ヘッドエンドに接続すると VPN ハードウェア クライアントとして機能します。ASA の背後にある Easy VPN ポート上のデバイス（コンピュータ、プリンタなど）は、VPN 経由で通信できます。個別に VPN クライアントを実行する必要はありません。ASA インターフェイス 1 つのみで Easy VPN ポートとして機能できます。このポートに複数のデバイスを接続するには、レイヤ 2 スイッチをこのポート上に配置してから、このスイッチにデバイスを接続します。 次のコマンドが導入されました。**vpnclient enable**、**vpnclient server**、**vpnclient mode**、**vpnclient username**、**vpnclient ipsec-over-tcp**、**vpnclient management**、**vpnclient vpngroup**、**vpnclient trustpoint**、**vpnclient nem-st-autoconnect**、**vpnclient mac-exempt** 次の画面が導入されました。[Configuration] > [VPN] > [Easy VPN Remote]
モニタリング機能	
syslog メッセージ内の無効なユーザー名の表示	失敗したログイン試行の syslog メッセージに無効なユーザー名を表示できるようになりました。デフォルト設定では、ユーザー名が無効な場合、または有効かどうか不明な場合、ユーザー名は非表示です。たとえば、ユーザーが誤ってユーザー名の代わりにパスワードを入力した場合、結果として生成される syslog メッセージで「ユーザー名」を隠すのが安全です。ログインに関するトラブルシューティングに役立てるために、無効なユーザー名を表示することもできます。 次のコマンドが導入されました。 **no logging hide username** 次の画面が変更されました。[Configuration] > [Device Management] > [Logging] > [Syslog Setup]。 この機能は、*9.2(4)* と *9.3(3)*でも使用できます。
REST API の機能	
REST API バージョン 1.2.1	REST API バージョン 1.2.1 のサポートが追加されました。

バージョン 9.4 の新機能

ASA 9.4(4.5)/ASDM 7.6(2) の新機能

リリース：**2017年4月3日**

（注） バージョン 9.4(4) は、バグ CSCvd78303 のため、Cisco.com から削除されました。

このリリースに新機能はありません。

ASA 9.4(3)/ASDM 7.6(1) の新機能

リリース：**2016年4月25日**

機能	説明
ファイアウォール機能	
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** 次の画面が変更されました。**[Configuration]** > **[Firewall]** > **[Advanced]** > **[Global Timeouts]**
リモート アクセス機能	
設定可能な SSH 暗号機能と HMAC アルゴリズム	ユーザーは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。 次のコマンドが導入されました。**ssh cipher encryption**、**ssh cipher integrity**。 次の画面が導入されました。**[Configuration]** > **[Device Management]** > **[Advanced]** > **[SSH Ciphers]** *9.1(7)* でも使用可能です。

機能	説明
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** 次の画面に機能が追加されました。**[Configuration]** > **[Device Management]** > **[HTTP Redirect]** *9.1(7)* でも使用可能です。
モニタリング機能	
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 ユーザーは、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。ユーザーがネイティブ engineID を指定しない場合、**show running config** 出力に engineID がユーザーごとに 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** ASDM サポートはありません。
show tech support の強化	**show tech support** コマンドは現在次のとおりです。 • **dir all-filesystems** の出力が含まれます。この出力は次の場合に役立つことがあります。 • SSL VPN コンフィギュレーション：必要なリソースが ASA にあるかどうかを確認します。 • クラッシュ：クラッシュ ファイルの日付のタイムスタンプと存在を確認します。 • **show kernel cgroup-controller detail** の出力の削除：このコマンド出力は **show tech-support detail** の出力内に残されます。 次のコマンドが変更されました。**show tech support** 追加または変更された画面はありません。 *9.1(7)* でも使用可能です。

機能	説明
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4GB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。 追加または変更された画面はありません。 *9.1(7)* でも使用可能です。

ASA 9.4(2.145)/ASDM 7.5(1) の新機能

リリース：**2015年11月13日**

このリリースに新機能はありません。

（注） このリリースは Firepower 9300 ASA セキュリティ モジュールのみをサポートします。

ASA 9.4(2)/ASDM 7.5(1) の新機能

リリース：**2015年9月24日**

このリリースに新機能はありません。

（注） ASAv 9.4(1.200) の各機能はこのリリースには含まれません。

（注） このバージョンは ISA 3000 をサポートしません。

ASA 9.4(1.225)/ASDM 7.5(1) の新機能

リリース：**2015年9月17日**

（注） このリリースは Cisco ISA 3000 のみをサポートします。

機能	説明
プラットフォーム機能	
Cisco ISA 3000 サポート	Cisco ISA 3000 は、DIN レールにマウントされた高耐久型の産業用セキュリティ アプライアンスです。ギガビットイーサネットと専用管理ポートを備えた、低消費電型ファンレス デバイスです。このモデルには ASA Firepower モジュールが事前にインストールされています。このモデルの特別な機能として、カスタマイズされたトランスペアレントモードのデフォルト設定と、電源喪失時もトラフィックがアプライアンスを通過することを可能にするハードウェア バイパス機能があります。 次のコマンドが導入されました。**hardware-bypass**、**hardware-bypass manual**、**hardware-bypass boot-delay**、**show hardware-bypass** 次の画面が導入されました。**[Configuration]** > **[Device Management]** > **[Hardware Bypass]** **hardware-bypass boot-delay** コマンドは ASDM 7.5(1) では使用できません。 この機能は、バージョン *9.5(1)* では使用できません。

ASA 9.4(1.152)/ASDM 7.4(3) の新機能

リリース：**2015年7月13日**

（注） このリリースは、Firepower 9300 の ASA のみをサポートします。

機能	説明
プラットフォーム機能	
Firepower 9300 の ASA セキュリティ モジュール	Firepower 9300 の ASA セキュリティ モジュールに ASA を導入しました。 （注） シャーシマネージャ 1.1.1 は Firepower 9300 の ASA セキュリティモジュールの VPN 機能（サイト間またはリモートアクセス）を一切サポートしません。
ハイ アベイラビリティ機能	

機能	説明
Firepower 9300 用シャーシ内 ASA クラスタリング	FirePOWER 9300 シャーシ内では、最大 3 つのセキュリティ モジュールをクラスタ化できます。シャーシ内のすべてのモジュールは、クラスタに属している必要があります。 次のコマンドを導入しました。**cluster replication delay**、**debug service-module**、**management-only individual**、**show cluster chassis** 次の画面を導入しました。**[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[ASA Cluster Replication]**
ライセンシング機能	
Firepower 9300 の ASA のシスコ スマート ソフトウェア ライセンシング	FirePOWER 9300 に ASA のシスコ スマート ソフトウェア ライセンシングが導入されました。 次のコマンドが導入されました。**feature strong-encryption**、**feature mobile-sp**、**feature context** 次の画面が変更されました。**[Configuration]** > **[Device Management]** > **[Licensing]** > **[Smart License]**

ASA 仮想 9.4(1.200)/ASDM 7.4(2) の新機能

リリース：**2015年5月12日**

（注） このリリースは、ASA 仮想 のみをサポートします。

機能	説明
プラットフォーム機能	
VMware 上の ASA 仮想 では vCenter サポートは不要になりました。	vCenter なしで、vSphere クライアントまたは OVFTool のデイゼロ設定を使用して ASA 仮想 を VMware 上にインストールできるようになりました。
Amazon Web Services（AWS）の ASA 仮想	Amazon Web Services（AWS）とデイゼロ設定で ASA 仮想 を使用できるようになりました。 （注） Amazon Web Services は ASAv10 と ASAv30 のモデルのみをサポートします。

ASDM 7.4(2) の新機能

リリース：**2015年5月6日**

機能	説明
リモート アクセス機能	
AnyConnect バージョン 4.1 のサポート	ASDM は AnyConnect バージョン 4.1 をサポートするようになりました。 次の画面が変更されました。[設定（Configuration）]>[リモートアクセスVPN（Remote Access VPN）]>[ネットワーク（クライアント）アクセス（Network (Client) Access）]>[セキュアクライアント プロファイル（Profile）]（[AMP イネーブラサービスプロファイル（AMP Enabler Service Profile）] という新しいプロファイル）

ASA 9.4(1)/ASDM 7.4(1) の新機能

リリース：**2015年3月30日**

機能	説明
プラットフォーム機能	
ASA 5506W-X、ASA 5506H-X、ASA 5508-X、ASA 5516-X	ワイヤレス アクセス ポイントを内蔵した ASA 5506W-X、強化された ASA 5506H-X、ASA 5508-X、ASA 5516-X の各モデルが導入されました。 **hw-module module wlan recover image**、**hw-module module wlan recover image** の各コマンドが導入されました。 変更された ASDM 画面はありません。
認定機能	
国防総省（DoD）統一機能規則（UCR）2013 証明書	ASA は、DoD UCR 2013 規則を遵守するように更新されています。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。 • 定期的な証明書認証 • 証明書有効期限のアラート • 基本制約 CA フラグの適用 • 証明書コンフィギュレーションの ASDM ユーザー名 • ASDM 管理認証 • IKEv2 無効セレクタの通知設定 • 16 進数の IKEv2 事前共有キー

機能	説明
FIPS 140-2 認証のコンプライアンス更新	ASA で FIPS モードを有効にすると、ASA が FIPS 140-2 に準拠するように追加制限が設定されます。次の制限があります。 • RSA および DH キー サイズの制限：RSA および DH キー 2K（2048 ビット）以上のみが許可されます。DH の場合、これはグループ 1（768 ビット）、2（1024 ビット）、5（1536 ビット）が許可されないことを意味します。 （注） キー サイズの制限により、FIPS での IKEv1 の使用が無効になります。 • デジタル署名のハッシュ アルゴリズムの制限：SHA 256 以上のみが許可されます。 • SSH 暗号の制限：許可された暗号は aes128-cbc または aes256-cbc です。MAC は SHA1 です。 ASA の FIPS 認証ステータスを表示するには、次の URL を参照してください。 http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140InProcess.pdf この PDF は毎週更新されます。 詳細については、Computer Security Division Computer Security Resource Center のサイトを参照してください。 http://csrc.nist.gov/groups/STM/cmvp/inprocess.html **fips enable** コマンドが変更されました。
ファイアウォール機能	
複数のコアを搭載した ASA での SIP インスペクションのパフォーマンスが向上。	複数のコアで ASA を通過する SIP シグナリングチングが複数存在する場合の SIP インスペクション パフォーマンスが向上しました。ただし、TLS、電話、または IME プロキシを使用する場合、パフォーマンスの向上は見られません。 変更されたコマンドはありません。 変更された画面はありません。
電話プロキシおよび UC-IME プロキシに対する SIP インスペクションのサポートが削除されました。	SIP インスペクションを設定する際、電話プロキシまたは UC-IME プロキシは使用できなくなります。暗号化されたトラフィックを検査するには、TLS プロキシを使用します。 **phone-proxy**、**uc-ime** の各コマンドが削除されました。**inspect sip** コマンドから **phone-proxy** キーワードと **uc-ime** キーワードが削除されました。 [Select SIP Inspect Map] サービス ポリシー ダイアログボックスから [Phone Proxy] と [UC-IME Proxy] が削除されました。

機能	説明
ISystemMapper UUID メッセージ RemoteGetClassObject opnum3 の DCERPC インスペクションのサポート。	ASA は、リリース 8.3 で EPM 以外の DCERPC メッセージのサポートを開始し、ISystemMapper UUID メッセージ RemoteCreateInstance opnum4 をサポートしています。この変更により、RemoteGetClassObject opnum3 メッセージまでサポートが拡張されます。 変更されたコマンドはありません。 変更された画面はありません。
コンテキストごとに無制限の SNMP サーバー トラップ ホスト	ASA では、コンテキストごとに SNMP サーバーのトラップ ホスト数の制限がありません。**show snmp-server host** コマンドの出力には ASA をポーリングしているアクティブなホストと、静的に設定されたホストのみが表示されます。 **show snmp-server host** コマンドが変更されました。 変更された画面はありません。
VXLAN パケットインスペクション	ASA は、標準形式に準拠するために VXLAN ヘッダーを検査できます。 **inspect vxlan** コマンドが導入されました。 次の画面が変更されました。[Configuration] > [Firewall] > [Service Policy Rules] > [Add Service Policy Rule] > [Rule Actions] > [Protocol Inspection]
IPv6 の DHCP モニタリング	IPv6 の DHCP 統計情報および DHCP バインディングをモニターできます。 次の画面が導入されました。 [Monitoring] > [Interfaces] > [DHCP] > [IPV6 DHCP Statistics Monitoring] > [Interfaces] > [DHCP] > [IPV6 DHCP Binding]
ESMTP インスペクションの TLS セッションでのデフォルトの動作が変更されました。	ESMTP インスペクションのデフォルトが、検査されない、TLS セッションを許可するように変更されました。ただし、このデフォルトは新しい、または再イメージングされたシステムに適用されます。**no allow-tls** を含むシステムをアップグレードする場合、このコマンドは変更されません。 デフォルトの動作の変更は、古いバージョンでも行われました：8.4（7.25）、8.5（1.23）、8.6（1.16）、8.7（1.15）、9.0（4.28）、9.1（6.1）、9.2（3.2）、9.3（1.2）、9.3（2.2）。
ハイ アベイラビリティ機能	
スタンバイ ASA での syslog 生成のブロック	スタンバイ装置で特定の syslog の生成をブロックできます。 **no logging message** *syslog-id* **standby** コマンドが導入されました。 変更された画面はありません。

機能	説明
インターフェイスごとに ASA クラスタのヘルス モニタリングをイネーブルまたはディセーブル	ヘルスモニタリングは、インターフェイスごとにイネーブルまたはディセーブルにすることができます。デフォルトでは、ポートチャネル、冗長、および単一のすべての物理インターフェイスでヘルスモニタリングがイネーブルになっています。ヘルス モニタリングは VLAN サブインターフェイス、または VNI や BVI などの仮想インターフェイスでは実行されません。クラスタ制御リンクのモニタリングは設定できません。このリンクは常にモニターされています。たとえば、管理インターフェイスなど、必須以外のインターフェイスのヘルスモニタリングをディセーブルにすることができます。 **health-check monitor-interface** コマンドが導入されました。 次の画面が変更されました。[Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster] > [Cluster Interface Health Monitoring]
DHCP リレーの ASA クラスタリングのサポート	ASA クラスタで DHCP リレーを設定できます。クライアントの DHCP 要求は、クライアントの MAC アドレスのハッシュを使用してクラスタ メンバにロードバランスされます。DHCP クライアントおよびサーバー機能はサポートされていません。 **debug cluster dhcp-relay** コマンドが導入されました。 変更された画面はありません。
ASA クラスタリングでの SIP インスペクションのサポート	ASA クラスタで SIP インスペクションを設定できます。制御フローは、任意のユニットで作成できますが（ロード バランシングのため）、その子データ フローは同じユニットに存在する必要があります。TLS プロキシ設定はサポートされていません。 **show cluster service-policy** コマンドが導入されました。 変更された画面はありません。
ルーティング機能	

機能	説明
ポリシーベースルーティング	ポリシーベース ルーティング（PBR）は、ACL を使用して指定された QoS でトラフィックが特定のパスを経由するために使用するメカニズムです。ACL では、パケットのレイヤ 3 および レイヤ4 ヘッダーの内容に基づいてトラフィックを分類できます。このソリューションにより、管理者は区別されたトラフィックに QoS を提供し、低帯域幅、低コストの永続パス、高帯域幅、高コストのスイッチドパスの間でインタラクティブ トラフィックとバッチ トラフィックを分散でき、インターネット サービス プロバイダーとその他の組織は明確に定義されたインターネット接続を介して一連のさまざまなユーザーから送信されるトラフィックをルーティングできます。 **set ip next-hop verify-availability、set ip next-hop、set ip next-hop recursive、set interface、set ip default next-hop、set default interface、set ip df、set ip dscp、policy-route route-map、show policy-route、debug policy-route** の各コマンドが導入されました。 次の画面が導入または変更されました。 **[Configuration] > [Device Setup] > [Routing] > [Route Maps] > [Policy Based Routing] [Configuration] > [Device Setup] > [Routing] > [Interface Settings] > [Interfaces]**
インターフェイス機能	
VXLAN のサポート	VXLAN のサポートが追加されました（VXLAN トンネル エンドポイント（VTEP）のサポートを含む）。ASA またはセキュリティ コンテキストごとに 1 つの VTEP 送信元インターフェイスを定義できます。 次のコマンドが導入されました。**debug vxlan、default-mcast-group、encapsulation vxlan、inspect vxlan、interface vni、mcast-group、nve、nve-only、peer ip、segment-id、show arp vtep-mapping、show interface vni、show mac-address-table vtep-mapping、show nve、show vni vlan-mapping、source-interface、vtep-nve、vxlan port** 次の画面が導入されました。 **[Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] > [Add] > [VNI Interface] [Configuration] > [Device Setup] > [Interface Settings] > [VXLAN]**
モニタリング機能	
EEM のメモリ トラッキング	メモリの割り当てとメモリの使用状況をログに記録してメモリ ロギングのラップ イベントに応答するための新しいデバッグ機能が追加されました。 次のコマンドが導入または変更されました。**memory logging、show memory logging、show memory logging include、event memory-logging-wrap** 次の画面が変更されました。[Configuration] > [Device Management] > [Advanced] > [Embedded Event Manager] > [Add Event Manager Applet] > [Add Event Manager Applet Event]

機能	説明
トラブルシューティングのクラッシュ	**show tech-support** コマンドの出力と **show crashinfo** コマンドの出力には、生成された syslog の最新 50 行が含まれます。これらの結果を表示できるようにするには、**logging buffer** コマンドをイネーブルにする必要があります。
リモート アクセス機能	
ECDHE-ECDSA 暗号のサポート	TLSv1.2 では、次の暗号のサポートが追加されています。 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • DHE-RSA-AES256-GCM-SHA384 • AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • DHE-RSA-AES128-GCM-SHA256 • RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 （注） 優先度が最も高いのは ECDSA 暗号方式と DHE 暗号方式です。 **ssl ecdh-group** コマンドが導入されました。 次の画面が変更されました。[Configuration] > [Remote Access VPN] > [Advanced] > [SSL Settings]。

機能	説明
クライアントレス SSL VPN セッション Cookie アクセスの制限	クライアントレス SSL VPN セッション Cookie が JavaScript などのクライアント側のスクリプトを介してサードパーティからアクセスされないようにすることができます。 （注） この機能は、Cisco TAC から使用を推奨された場合のみ使用してください。このコマンドをイネーブルにすると、次のクライアントレス SSL VPN 機能が警告なしで動作しなくなるため、セキュリティ上のリスクが発生します。 • Java プラグイン • Java リライタ • ポートフォワーディング。 • ファイルブラウザ • デスクトップ アプリケーション（Microsoft Office アプリケーションなど）を必要とする Sharepoint 機能 • セキュアクライアントWeb 起動 • Citrix Receiver、XenDesktop、および Xenon • その他の非ブラウザ ベース アプリケーションおよびブラウザプラグインベースのアプリケーション **http-only-cookie** コマンドが導入されました。 次の画面が変更されました。[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Advanced] > [HTTP Cookie]。 この機能は、*9.2(3)* にもあります。
セキュリティ グループ タギングを使用した仮想デスクトップのアクセス制御	ASA では、内部アプリケーションおよび Web サイトへのクライアントレス SSL リモートアクセス用にセキュリティ グループ タギングベースのポリシー制御をサポートしています。この機能では、配信コントローラおよび ASA のコンテンツ変換エンジンとして XenDesktop による Citrix の仮想デスクトップ インフラストラクチャ（VDI）を使用します。 詳細については、次の Citrix 製品のマニュアルを参照してください。 • XenDesktop および XenApp のポリシー：http://support.citrix.com/proddocs/topic/infocenter/ic-how-to-use.html • XenDesktop 7 でのポリシーの管理：http://support.citrix.com/proddocs/topic/xendesktop-7/cds-policies-wrapper-rho.html • XenDesktop 7 のポリシー用のグループ ポリシー エディタの使用：http://support.citrix.com/proddocs/topic/xendesktop-7/cds-policies-use-gpmc.html

機能	説明
クライアントレスSSL VPN に OWA 2013 機能のサポートを追加	クライアントレス SSL VPN では、以下を除き、OWA 2013 の新機能をサポートしています。 • タブレットおよびスマートフォンのサポート • オフライン モード • Active Directory Federation Services（AD FS）2.0. ASA および AD FS 2.0 は、暗号化プロトコルをネゴシエートできません。 変更されたコマンドはありません。 変更された画面はありません。
クライアントレスSSL VPN に Citrix XenDesktop 7.5 および StoreFront 2.5 のサポートを追加	クライアントレス SSL VPN では、XenDesktop 7.5 および StoreFront 2.5 のアクセスをサポートしています。 XenDesktop 7.5 の機能の完全なリストと詳細については、http://support.citrix.com/proddocs/topic/xenapp-xendesktop-75/cds-75-about-whats-new.html を参照してください。 StoreFront 2.5 の機能の完全なリストと詳細については、http://support.citrix.com/proddocs/topic/dws-storefront-25/dws-about.html を参照してください。 変更されたコマンドはありません。 変更された画面はありません。
定期的な証明書認証	定期的な証明書認証を有効にすると、ASA は、VPN クライアントから受信した証明書チェーンを保存し、それらを定期的に再認証します。 **periodic-authentication certificate**、**revocation-check, show vpn-sessiondb** の各コマンドが導入または変更されました。 次の画面が変更されました。 **[Configuration] > [Device Management] > [Certificate Management] > [Identity Certificates] [Configuration] > [Device Management] > [Certificate Management] > [CA Certificates]**

機能	説明
証明書有効期限のアラート	ASA は、トラスト ポイントですべての CA および ID の証明書の有効期限について 24 時間ごとにチェックします。証明書の有効期限がまもなく切れる場合は、syslog がアラートとして発行されます。リマインダおよび繰り返しの間隔を設定できます。デフォルトでは、リマインダは有効期限の 60 日前に開始し、7 日ごとに繰り返されます。 **crypto ca alerts expiration** コマンドが導入または変更されました。 次の画面が変更されました。 **[Configuration] > [Device Management] > [Certificate Management] > [Identity Certificates] [Configuration] > [Device Management] > [Certificate Management] > [CA Certificates]**
基本制約 CA フラグの適用	デフォルトでは、CA フラグのない証明書を CA 証明書として ASA にインストールできなくなりました。基本制約拡張は、証明書のサブジェクトが CA で、この証明書を含む有効な認証パスの最大深さかどうかを示すものです。必要に応じて、これらの証明書のインストールを許可するように ASA を設定できます。 **ca-check** コマンドが導入されました。 次の画面が変更されました。[Configuration] > [Device Management] > [Certificate Management] > [CA Certificates]
IKEv2 無効セレクタの通知設定	現在、ASA が SA 上で着信パケットを受信し、そのパケットのヘッダー フィールドが SA 用のセレクタに適合しなかった場合、ASA はそのパケットを廃棄します。ピアへの IKEv2 通知の送信をイネーブルまたはディセーブルにすることができます。この通知の送信はデフォルトで無効になっています。 （注） この機能は、セキュアクライアント 3.1.06060 以降でサポートされています。 **crypto ikev2 notify invalid-selectors** コマンドが導入されました。
16 進数の IKEv2 事前共有キー	16 進数の IKEv2 事前共有キーを設定できます。 **ikev2 local-authentication pre-shared-key hex**、**ikev2 remote-authentication pre-shared-key hex** の各コマンドが導入されました。
管理機能	
ASDM 管理認証	HTTP アクセスと Telnet および SSH アクセス別に管理認証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。 **aaa authorization http console** 次の画面が変更されました。**[Configuration] > [Device Management] > [Users/AAA] > [AAA Access] > [Authorization]**

機能	説明
証明書コンフィギュレーションの ASDM ユーザー名	ASDM の証明書認証（**http authentication-certificate**）を有効にすると、ASDM が証明書からユーザー名を抽出する方法を設定できます。また、ログインプロンプトでユーザー名を事前に入力して表示できます。 次のコマンドが導入されました。**http username-from-certificate** 次の画面が導入されました。**[Configuration] > [Device Management] > [Management Access] > [HTTP Certificate Rule]**
CLI で **?** の入力時にヘルプを有効または無効にするための **terminal interactive** コマンド	通常、ASA CLI で **?** を入力すると、コマンドヘルプが表示されます。コマンド内にテキストとして **?** を入力できるようにするには（たとえば、URL の一部として ? を含めるには）、**no terminal interactive** コマンドを使用してインタラクティブなヘルプを無効にします。 次のコマンドが導入されました。terminal interactive
REST API の機能	
REST API バージョン 1.1	REST API バージョン 1.1 のサポートが追加されました。
トークンベース認証が（既存の基本認証に加えて）サポートされるようになりました。	クライアントは特定の URL にログイン要求を送信でき、成功すると、（応答ヘッダーに）トークンが返されます。クライアントはさらなる API コールを送信するために、（特別な要求ヘッダー内で）このトークンを使用します。トークンは明示的に無効にするまで、またはアイドル/セッション タイムアウトに到達するまで有効です。
マルチ コンテキスト モードの限定的なサポート	REST API エージェントをマルチ コンテキスト モードで有効にできるようになりました。CLI コマンドはシステム コンテキスト モードでのみ発行できます（シングル コンテキスト モードと同じコマンド）。 次のようにパススルー CLI の API コマンドを使用して、コンテキストを設定できます。 `https://<asa_admin_context_ip>/api/cli?context=<context_name>` **context** パラメータがない場合、要求は **admin** コンテキストに向けられたものとみなされます。

機能	説明
高度な（粒状の）インスペクション	次のプロトコルの詳細なインスペクションをサポートします。 • DNS over UDP • HTTP • ICMP • ICMP ERROR • RTSP • SIP • FTP • DCERPC • IP オプション • NetBIOS Name Server over IP • SQL*Net

バージョン 9.3 の新機能

ASA 9.3(3)/ASDM 7.4(1) の新機能

リリース：**2015年4月22日**

機能	説明
プラットフォーム機能	
syslog メッセージ内の無効なユーザー名の表示	失敗したログイン試行の syslog メッセージに無効なユーザー名を表示できるようになりました。デフォルト設定では、ユーザー名が無効な場合、または有効かどうか不明な場合、ユーザー名は非表示です。たとえば、ユーザーが誤ってユーザー名の代わりにパスワードを入力した場合、結果として生成される syslog メッセージで「ユーザー名」を隠すのが安全です。ログインに関するトラブルシューティングに役立てるために、無効なユーザー名を表示することもできます。 次のコマンドが導入されました。**no logging hide username** この機能は、ASDM ではサポートされていません。 この機能は、*9.4(1)* では使用できません。

ASA 9.3(2)/ASDM 7.3(3) の新機能

リリース：**2015年2月2日**

機能	説明
プラットフォーム機能	
ASA 5506-X の ASA FirePOWER ソフトウェア モジュール	ASA FirePOWER は ASDM を使用する ASA 5506-X 上で構成できます。の FireSIGHT Management Center は不要です。ただし、ASDM の代わり使用することもできます。 次の画面が導入されました。 **[Home] > [ASA FirePOWER Dashboard]** **[Home] > [ASA FirePOWER Reporting]** **[Configuration] > [ASA FirePOWER Configuration]** **[Monitoring] > [ASA FirePOWER Monitoring]**

ASA 9.3(2.200)/ASDM 7.3(2) の新機能

リリース：**2014年12月18日**

（注） このリリースは、ASAv のみをサポートします。

機能	説明
プラットフォーム機能	
KVM と Virtio がある ASAv	カーネルベース仮想マシン（KVM）および Virtio 仮想インターフェイドライバを使用して ASAv を展開できます。

ASA 9.3(2)/ASDM 7.3(2) の新機能

リリース：**2014年12月18日**

機能	説明
プラットフォーム機能	
ASA 5506-X	ASA 5506-X を導入しました。 次のコマンドを導入または変更しました。**service sw-reset-button**、**upgr rommon**、**show environment temperature accelerator**

機能	説明
ASA 5506-X の ASA FirePOWER ソフトウェア モジュール	ASA FirePOWER は ASDM を使用する ASA 5506-X 上で構成できます。別の FireSIGHT Management Center は不要です。ただし、ASDM の代わりに使用することもできます。**注**：この機能には ASA 7.3(3) が必要です。 次の画面が導入されました。 **[Home] > [ASA FirePOWER Dashboard]** **[Home] > [ASA FirePOWER Reporting]** **[Configuration] > [ASA FirePOWER Configuration]** **[Monitoring] > [ASA FirePOWER Monitoring]**
トラフィック リダイレクション インターフェイスを使用した ASA FirePOWER パッシブ モニタ専用モード	サービス ポリシーを使用する代わりに、トラフィックをモジュールに送信するようにトラフィック転送インターフェイスを設定できるようになりました。このモードでは、モジュールも ASA もトラフィックに影響を与えません。 **traffic-forward sfr monitor-only** コマンドを完全にサポートしています。これは、CLI でのみ設定できます。
ASA 5585-X での混在レベルの SSP	ASA 5585-X で次の混在レベルの SSP を使用できるようになりました。 • ASA SSP-10/ASA FirePOWER SSP-40 • ASA SSP-20/ASA FirePOWER SSP-60 要件：スロット 0 で ASA SSP、スロット 1 で ASA FirePOWER SSP
ASA REST API 1.0.1	ASA の主要な機能の設定および管理をサポートするために REST API が追加されました。 次のコマンドを導入または変更しました。**rest-api image**、**rest-api agent**、**show rest-api agent**、**debug rest-api**、**show version**
ASA イメージの署名と検証のサポート	ASAイメージは、デジタル署名を使用して署名されるようになりました。デジタル署名は、ASA が起動した後に検証されます。 次のコマンドが導入されました。**copy /noverify**、**verify /image-signature**、**show software authenticity keys**、**show software authenticity file**、**show software authenticity running**、**show software authenticity development**、**software authenticity development**、**software authenticity key add special**、**software authenticity key revoke special** この機能は、ASDM ではサポートされていません。

機能	説明
加速セキュリティ パス ロード バランシング	加速セキュリティ パス（ASP）ロード バランシング メカニズムを利用すると、複数の CPU コアでインターフェイス受信リングからパケットを信して個別に処理できるため、パケット損失が減少し、スループットが善します。 次のコマンドが導入されました。**asp load-balance per-packet-auto** 次の画面が導入されました。[Configuration] > [Device Management] > [Advanced] > [ASP Load Balancing]
ファイアウォール機能	
ACL およびオブジェクトを編集するためのコンフィギュレーション セッション アクセス ルール内でのオブジェクトおよび ACL の前方参照	独立したコンフィギュレーション セッションで ACL およびオブジェクを編集できるようになりました。オブジェクトおよび ACL を前方参照ることも可能です。つまり、まだ存在していないオブジェクトや ACL 対するルールおよびアクセス グループを設定することができます。 次のコマンドが導入されました。**clear configuration session**、**clear sessio** **configure session**、**forward-reference**、**show configuration session** この機能は、ASDM ではサポートされていません。
信頼検証サービス、NAT66、CUCM 10.5(1)、および Model 8831 Phone に対する SIP のサポート	SIP インスペクションで信頼検証サービス用サーバを設定できるようりました。NAT66 も使用できます。SIP インスペクションは CUCM 10. でテスト済みです。 次のコマンドが導入されました。**trust-verification-server** 次の画面が導入されました。[Configuration] > [Firewall] > [Objects] > [Inspection Maps] > [SIP] > [Add/Edit SIP Inspect Map] > [Details] > [TVS Ser
CUCM 10.5(1) に対する Unified Communications のサポート	SIP および SCCP インスペクションのテストと検証が Cisco Unified Communications Manager 10.5(1) を使用して実施されました。
リモート アクセス機能	
Citrix VDI に対するブラウザのサポート	Citrix VDI にアクセスするための HTML 5 ベースのブラウザ ソリューンがサポートされるようになり、デスクトップ上の Citrix Receiver クアントが不要になりました。
Mac OSX 10.9 用のクライアントレス SSL VPN	Mac OSX 10.9 でサポートされているすべてのブラウザでクライアントス SSL VPN 機能（リライタ、スマート トンネル、プラグインなど）がポートされるようになりました。

機能	説明
標準ベースでサードパーティの IKEv2 リモート アクセス クライアントとの相互運用性	AnyConnect に加え、標準ベースでサードパーティの IKEv2 リモート アクセス クライアントを介した VPN 接続がサポートされるようになりました。認証では、事前共有キー、証明書、拡張認証プロトコル（EAP）を介したユーザー認証などがサポートされます。 次のコマンドを導入または変更しました。**ikev2 remote-authentication**、**ikev2 local-authentication**、**clear vpn-sessiondb**、**show vpn-sessiondb**、**vpn-sessiondb logoff** 次の画面が導入または変更されました。 [Wizards] > [IPsec IKEv2 Remote Access Wizard] **[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [IPsec (IKEv2) Connection Profiles]** **[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [IPsec (IKEv2) Connection Profiles] > [Add/Edit] > [Advanced] > [IPsec]** **[Monitoring] > [VPN] > [VPN Statistics] > [Sessions]**
Transport Layer Security（TLS）バージョン 1.2 のサポート	TLS バージョン 1.2 がサポートされ、ASDM、クライアントレス SSVPN、および AnyConnect VPN でメッセージを安全に伝送できるようになりました。 次のコマンドを導入または変更しました。**ssl client-version**、**ssl server-version**、**ssl cipher**、**ssl trust-point**、**ssl dh-group**、**show ssl**、**show ssl cipher**、**show vpn-sessiondb** 次のコマンドが非推奨になりました。**ssl encryption** 次の画面が変更されました。 **[Configuration] > [Device Management] > [Advanced] > [SSL Settings]** **[Configuration] > [Remote Access VPN] > [Advanced] > [SSL Settings]**
TLS バージョン 1.2 に対する AnyConnect 4.0 のサポート	AnyConnect 4.0 で TLS バージョン 1.2 がサポートされるようになりました。また、4 つの暗号スイート（DHE-RSA-AES256-SHA256、DHE-RSA-AES128-SHA256、AES256-SHA256、および AES128-SHA256）が追加されました。
ライセンシング機能	

機能	説明
ASAv のシスコ スマート ソフトウェア ライセンシング	Smart Software Licensing では、ライセンスのプールを購入して管理するとができます。PAK ライセンスとは異なり、スマート ライセンスは特のシリアル番号に関連付けられません。各ユニットのライセンス キー管理しなくても、簡単に ASAv を導入したり導入を終了したりできますスマート ソフトウェア ライセンスを利用すれば、ライセンスの使用状と要件をひと目で確認することもできます。 **clear configure license**、**debug license agent**、**feature tier**、**http-proxy**、**lic smart**、**license smart deregister**、**license smart register**、**license smart rene show license**、**show running-config license**、**throughput level** 各コマンド導入されました。 次の画面が導入または変更されました。 **[Configuration] > [Device Management] > [Licensing] > [Smart License]** **[Configuration] > [Device Management] > [Smart Call-Home]** **[Monitoring] > [Properties] > [Smart License]**
ハイ アベイラビリティ機能	
フェールオーバー ペアのスタンバイ装置またはスタンバイ コンテキストのコンフィギュレーション変更のロック	通常のコンフィギュレーションの同期を除いてスタンバイ装置上で変更できないように、スタンバイ装置（アクティブ/スタンバイ フェールオバー）またはスタンバイ コンテキスト（アクティブ/アクティブ フェオーバー）のコンフィギュレーション変更をロックできるようになりた。 **failover standby config-lock** コマンドが導入されました。 次の画面が変更になりました。[Configuration] > [Device Management] > [H Availability and Scalability] > [Failover] > [Setup]
内部ネットワーク間に ASA クラスタ ファイアウォールを備えたトランスペアレント モードの ASA クラスタリング サイト間導入	各サイトの内部ネットワークとゲートウェイ ルータ間にトランスペアント モードのクラスタを導入し（AKA イーストウェスト挿入）、サ間に内部 VLAN を拡張できます。オーバーレイ トランスポート仮想化（OTV）の使用を推奨しますが、ゲートウェイ ルータの重複する MAC ドレスおよび IP アドレスがサイト間で漏えいしないようにする任意の法を使用できます。HSRP などの First Hop Redundancy Protocol（FHRP）使用して、同じ仮想 MAC アドレスおよび IP アドレスをゲートウェイタに提供します。
インターフェイス機能	

機能	説明
トラフィック ゾーン	インターフェイスをトラフィック ゾーンにグループ化することで、トラフィックのロードバランシング（等コストマルチパス（ECMP）ルーティングを使用）、ルートの冗長性、および複数のインターフェイス間での非対称ルーティングを実現できます。 （注） 名前付きゾーンにはセキュリティポリシーを適用できません。セキュリティポリシーはインターフェイスに基づきます。ゾーン内のインターフェイスが同じアクセス ルール、NAT、およびサービス ポリシーを使用して設定されていれば、ロードバランシングおよび非対称ルーティングは正しく動作します。 **zone、zone-member、show running-config zone、clear configure zone、show zone、show asp table zone、show nameif zone、show conn long、show local-host zone、show route zone、show asp table routing、clear conn zone、clear local-host zone** の各コマンドが導入または変更されました。 次の画面が導入または変更されました。 **[Configuration] > [Device Setup] > [Interface Parameters] > [Zones]** **[Configuration] > [Device Setup] > [Interface Parameters] > [Interfaces]**
ルーティング機能	
IPv6 に対する BGP のサポート	IPv6 のサポートが追加されました。 次のコマンドを導入または変更しました。**address-family ipv6、bgp router-id、ipv6 prefix-list、ipv6 prefix-list description、ipv6 prefix-list sequence-number、match ipv6 next-hop、match ipv6 route-source、match ipv6- address prefix-list、set ipv6-address prefix -list、set ipv6 next-hop、set ipv6 next-hop peer-address** 次の画面が導入されました。[Configuration] > [Device Setup] > [Routing] > [BGP] > [IPv6 Family]
モニタリング機能	

機能	説明
SNMP の MIB およびトラップ	新しい ASA 5506-X をサポートするように CISCO-PRODUCTS-MIB お CISCO-ENTITY-VENDORTYPE-OID-MIB が更新されました。 SNMP の sysObjectID OID および entPhysicalVendorType OID に、新しい 品として ASA 5506-X が追加されました。 ASA で CISCO-CONFIG-MAN-MIB がサポートされるようになりまし 以下が可能です。 • 特定のコンフィギュレーションについて入力されたコマンドを確 る。 • 実行コンフィギュレーションに変更が発生したときに NMS に通 る。 • 実行コンフィギュレーションが最後に変更または保存されたとき イム スタンプを追跡する。 • 端末の詳細やコマンドのソースなど、コマンドに対するその他の を追跡する。 次のコマンドが変更されました。**snmp-server enable traps** 次の画面が変更されました。[Configuration] > [Device Management] > [Management Access] > [SNMP] > [Configure Traps] > [SNMP Trap Configurat
トラブルシューティングに使用するルートのサマリー情報の表示	**show route-summary** コマンドの出力が **show tech-support detail** コマン に追加されました。
管理機能	
システムのバックアップと復元	CLI を使用した、包括的なシステムのバックアップと復元がサポート るようになりました。 **backup** および **restore** コマンドが導入されました。 変更された画面はありません。この機能はすでに ASDM で利用可能で

ASA 9.3(1)/ASDM 7.3(1) の新機能

リリース：2014年7月24日

（注） このリリース以降、ASA 5505 はサポートされません。ASA バージョン 9.2 は、ASA 5505 の最終リリースです。

機能	説明
ファイアウォール機能	
IPv6 に対する SIP、SCCP、および TLS プロキシのサポート	SIP、SCCP、および TLS プロキシ（SIP または SCCP を使用） いる場合、IPv6 トラフィックを検査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。 変更された ASDM 画面はありません。
Cisco Unified Communications Manager 8.6 のサポート	ASA と Cisco Unified Communications Manager バージョン 8.6 か れるようになりました（SCCPv21 のサポートを含む）。 変更されたコマンドはありません。 変更された ASDM 画面はありません。
アクセス グループおよび NAT に関するルールエンジンのトランザクション コミット モデル	イネーブルの場合、ルールの編集の完了後、ルールの更新が す。ルールの照合パフォーマンスへの影響はありません。 **asp rule-engine transactional-commit**、**show running-config asp** **transactional-commit**、**clear configure asp rule-engine transacti** の各コマンドが導入されました。 次の画面が導入されました。[Configuration] > [Device Manager [Advanced] > [Rule Engine]。
リモート アクセス機能	
クライアントレス SSL VPN に対する XenDesktop 7 のサポート	クライアントレス SSL VPN に対する XenDesktop 7 のサポート ました。自動サインオンを含むブックマークを作成する場合に ング ページの URL またはコントロール ID を指定できるよう た。 変更されたコマンドはありません。 次の画面が変更されました。[Configuration] > [Remote Access [Clientless SSL VPN Access] > [Portal] > [Bookmarks]。

機能	説明
AnyConnect カスタム属性の強化	カスタム属性では、ASA に組み込まれていない AnyConne アップグレードなど）が定義および設定されます。カスタ 強化され、複数の値やより大きな値を設定できるようにな は、カスタム属性のタイプ、名前、および値の指定が必要 す。また、カスタム属性をダイナミック アクセス ポリシー プ ポリシーに追加できるようになりました。9.3.x にアッ と、以前に定義したカスタム属性がこの強化された設定フ 新されます。 **anyconnect-custom-attr**、**anyconnect-custom-data**、および **an** の各コマンドが導入または変更されました。 次の画面が導入または変更されました。 **[Configuration] > [Remote Access VPN] > [Network (Client)** **[Advanced] > [AnyConnect Custom Attributes]** **[Configuration] > [Remote Access VPN] > [Network (Client)** **[Advanced] > [AnyConnect Custom Attribute Names]** **[Configuration] > [Remote Access VPN] > [Network (Client) A** **Policies] > [Add/Edit] > [Advanced] > [AnyConnect Client] >** **Attributes]** **[Configuration] > [Remote Access VPN] > [Network (Client)** **[Dynamic Access Policies] > [Add/Edit] > [AnyConnect Custo**
デスクトップ プラットフォームの AnyConnect Identity Extension（ACIDex）	ACIDex（AnyConnect エンドポイント属性または Mobile Po れる）は、AnyConnect VPN クライアントがポスチャ情報を 際に使用する方法です。ダイナミック アクセス ポリシーで の認証にこれらのエンドポイント属性が使用されます。 現在、AnyConnect VPN クライアントには、デスクトップ グ システム（Windows、Mac OS X、および Linux）のプラ 別機能が搭載されているほか、DAP で使用可能な MAC ア が用意されています。 変更されたコマンドはありません。 次の画面が変更されました。 [Configuration] > [Remote Acc [Dynamic Access Policies] > [Add/Edit] > [Add/Edit (endpoint a [Endpoint Attribute Type] では [AnyConnect] を選択します。[プダウン リストにはオペレーティング システムが追加さ た、[MAC Address] が [Mac Address Pool] に変更されまし

機能	説明
VPN に対する TrustSec SGT の割り当て	リモート ユーザーが接続するときに、TrustSec セキュリティグ（SGT）を ASA の SGT-IP テーブルに追加できるようにな 新しい **security-group-tag value** コマンドが導入されました。 次の画面が導入または変更されました。 **[Configuration] > [Remote Access VPN] > [AAA/Local Users] > [> [Edit User] > [VPN Policy]** **[Configuration] > [Remote Access VPN] > [Network (Client) Acce Policies] > [Add a Policy]**
ハイ アベイラビリティ機能	
クラスタリング内のモジュールのヘルス モニタリングに対するサポートの強化	クラスタリング内のモジュールのヘルス モニタリングに対すサポートが強化されました。 **show cluster info health** コマンドが変更されました。 変更された ASDM 画面はありません。
ハードウェア モジュールのヘルス モニタリングの無効化	ASA はデフォルトで、インストール済みハードウェア モジュFirePOWER モジュールなど）のヘルス モニタリングを行いまハードウェア モジュールの障害によってフェールオーバーをることが望ましくない場合は、モジュールのモニタリングをにできます。 **monitor-interface service-module** コマンドが変更されました。 次の画面が変更になりました。[Configuration] > [Device Manage Availability and Scalability] > [Failover] > [Interfaces]
プラットフォーム機能	

機能	説明
ASP ロード バランシング	**asp load-balance per-packet** コマンドの新しい **auto** オプシ と、ASA の各インターフェイス受信リングで、ASP ロー のオン/オフをパケットごとに柔軟に切り替えることができ 動メカニズムにより、非対称トラフィックが導入されてい 出し、次の問題を回避することができます。 • フロー上での突発的なトラフィックの増加によって発 ラン • 特定のインターフェイス受信リングをオーバーサブス ルク フローによるオーバーラン • 1 つのコアでは耐えられないような、かなり大きな負 るインターフェイス受信リングで発生するオーバーラ **asp load-balance per-packet auto**、**show asp load-balance pe** **asp load-balance per-packet history**、および **clear asp load-** の各コマンドが導入または変更されました。 変更された ASDM 画面はありません。
SNMP MIB	CISCO-REMOTE-ACCESS-MONITOR-MIB が ASASM をサ になりました。
インターフェイス機能	
トランスペアレント モードのブリッジ グループの最大数が 250 に増加	ブリッジグループの最大数が8個から250個に増えました。 ドでは最大 250 個、マルチ モードではコンテキストあたり リッジグループを設定でき、各ブリッジグループには最大 フェイスを追加できます。 **interface bvi** および **bridge-group** コマンドが変更されまし 次の画面が変更されました。 **[Configuration] > [Device Setup] > [Interfaces]** **[Configuration] > [Device Setup] > [Interfaces] > [Add/Edit I** **Interface]** **[Configuration] > [Device Setup] > [Interfaces] > [Add/Edit I**
ルーティング機能	
ASA クラスタリングに対する BGP のサポート	ASA クラスタリングに対する BGP のサポートが追加され 次の新しいコマンドが導入されました。bgp router-id cluste 次の画面が変更されました。[Configuration] > [Device Setup [BGP] > [IPv4 Family] > [General]

機能	説明
ノンストップ フォワーディングに対する BGP のサポート	ノンストップ フォワーディングに対する BGP のサポートが追加された。 次の新しいコマンドが導入されました。bgp graceful-restart、neighbor graceful-restart 次の画面が変更されました。 **[Configuration] > [Device Setup] > [Routing] > [BGP] > [General]** **[Configuration] > [Device Setup] > [Routing] > [BGP] > [IPv4 Family] > [Neighbor]** **[Monitoring] > [Routing] > [BGP Neighbors]**
アドバタイズされたマップに対する BGP のサポート	アドバタイズされたマップに対する BGPv4 のサポートが追加さ 次の新しいコマンドが導入されました。neighbor advertise-map 次の画面が変更されました。[Configuration] > [Device Setup] > [BGP] > [IPv4 Family] > [Neighbor] > [Add BGP Neighbor] > [Rou
ノンストップ フォワーディング（NSF）に対する OSPF のサポート	NSF に対する OSPFv2 および OSPFv3 のサポートが追加されま 次のコマンドが追加されました。capability、nsf cisco、nsf cisco ietf、nsf ietf helper、nsf ietf helper strict-lsa-checking、graceful-restart helper、graceful-restart helper strict-lsa-checking 次の画面が追加されました。 **[Configuration] > [Device Setup] > [Routing] > [OSPF] > [Setup] > Properties]** **[Configuration] > [Device Setup] > [Routing] > [OSPFv3] > [Setup] > Properties]**
AAA 機能	

機能	説明
レイヤ 2 セキュリティ グループのタグ インポジション	セキュリティ グループ タギングをイーサネット タギング使用して、ポリシーを適用できるようになりました。SGT タギング（レイヤ 2 SGT インポジションとも呼ばれる）を ASA でシスコ独自のイーサネット フレーミング（イーサ 0x8909）を使用して、ギガビットイーサネットインターフ リティ グループ タグを送受信できます。これにより、送信 ティ グループ タグをプレーン テキストのイーサネット フ きます。 **cts manual**、**policy static sgt**、**propagate sgt**、**cts role-based cts sgt-map**、**packet-tracer**、**capture**、**show capture**、**show asp table classify**、**show running-config all**、**clear configure a memory** の各コマンドが導入または変更されました。 次の画面が変更されました。 **[Configuration] > [Device Setup] > [Interfaces] > [Add Interfa** **[Configuration] > [Device Setup] > [Interfaces] > [Add Redu > [Advanced]** **[Configuration] > [Device Setup] > [Add Ethernet Interface]** **[Wizards] > [Packet Capture Wizard]** **[Tools] > [Packet Tracer]**
AAA の Windows NT ドメイン認証の削除	リモート アクセス VPN ユーザーに対する NTLM のサポー した。 次のコマンドが非推奨になりました。aaa-server protocol nt 次の画面が変更されました。[Configuration] > [Remote Acc [AAA/Local Users] > [AAA Server Groups] > [Add AAA Serve
ASDM Identity Certificate Wizard	最新バージョンの Java を使用している場合、ASDM ラン 頼できる証明書が必要になります。証明書の要件は、自己 証明書をインストールすることによって簡単に満たすこと [ASDM Identity Certificate Wizard] を使用すると、自己署名 書を簡単に作成できます。最初に ASDM を起動したとき 明書がない場合、Java Web Start を使用して ASDM を起動 れます。この新しいウィザードは自動的に開始されます。 成したら、Java コントロール パネルに登録する必要があり ついては、https://www.cisco.com/go/asdm-certificate を参照し 次の画面が追加されました。[Wizards] > [ASDM Identity Cert
モニタリング機能	

機能	説明
物理インターフェイスの集約トラフィックのモニタリング	**show traffic** コマンドの出力が更新され、物理インターフェイ約トラフィックが含まれるようになりました。この機能をイネるには、最初に **sysopt traffic detailed-statistics** コマンドを入力あります。
show tech support の強化	**show tech-support** コマンドに **show resource usage count all 1** れるようになりました。これには、xlate、conn、inspect、sysl する情報が含まれます。この情報は、パフォーマンスに関する するために役立ちます。 次のコマンドが変更されました。**show tech support** 追加または変更された画面はありません。
ASDM は、ボットネット トラフィック フィルタ レポートを PDF ではなく HTML として保存することができます。	ASDM はボットネット トラフィック フィルタ レポートを PD として保存できなくなりました。それは代わりに HTML とし ます。 次の画面が変更されました。[Monitoring] > [Botnet Traffic Filte

バージョン 9.2 の新機能

ASA 9.2(4)/ASDM 7.4(3) の新機能

リリース：**2015年7月16日**

機能	説明
プラットフォーム機能	
syslog メッセージ内の無効なユーザー名の表示	失敗したログイン試行の syslog メッセージに無効なユーザー名 るようになりました。デフォルト設定では、ユーザー名が無効 たは有効かどうか不明な場合、ユーザー名は非表示です。たと ザーが誤ってユーザー名の代わりにパスワードを入力した場合 て生成される syslog メッセージで「ユーザー名」を隠すのが安 グインに関するトラブルシューティングに役立てるために、 ザー名を表示することもできます。 次のコマンドが導入されました。**no logging hide username** 次の画面が変更されました。[Configuration] > [Device Manager [Logging] > [Syslog Setup]。
DHCP 機能	

機能	説明
DHCP リレー サーバは、応答用の DHCP サーバ識別子を確認します。	ASA DHCP リレーサーバが不適切な DHCP サーバから応答 応答を処理する前に、その応答が適切なサーバからのもの 認するようになりました。
モニタリング機能	
Xlate カウントへのポーリング可能にする NAT-MIB cnatAddrBindNumberOfEntries および cnatAddrBindSessionCount OID。	SNMP の xlate_count および max_xlate_count に、NAT-MIB cnatAddrBindNumberOfEntries および cnatAddrBindSessionC ポートされるようになりました。 このデータは、**show xlate count** コマンドと同等です。 変更された ASDM 画面はありません。 *8.4(5)* および *9.1(5)* でも使用可能です。

ASA 9.2(3)/ASDM 7.3(1.101) の新機能

リリース：**2014年12月15日**

機能	説明
リモート アクセス機能	

機能	説明
クライアントレス SSL VPN セッション Cookie アクセスの制限	クライアントレス SSL VPN セッション Cookie が JavaScript な アント側のスクリプトを介してサードパーティからアクセス にすることができます。 （注） この機能は、Cisco TAC から使用を推奨された場合 てください。このコマンドをイネーブルにすると、 イアントレス SSL VPN 機能が警告なしで動作しな め、セキュリティ上のリスクが発生します。 • Java プラグイン • Java リライタ • ポートフォワーディング。 • ファイルブラウザ • デスクトップ アプリケーション（Microsoft O ケーションなど）を必要とする Sharepoint 機能 • AnyConnect Web 起動 • Citrix Receiver、XenDesktop、および Xenon • その他の非ブラウザ ベース アプリケーション ウザプラグインベースのアプリケーション 次のコマンドが導入されました。**http-only-cookie** 次の画面が変更されました。[Configuration] > [Remote Access [Clientless SSL VPN Access] > [Advanced] > [HTTP Cookie]

ASA 9.2(2.4)/ASDM 7.2(2) の新機能

リリース：**2014年8月12日**

（注） バージョン 9.2(2) はビルドの問題により Cisco.com から削除されました。バージョン 9.2(2.4) またはそれ以降にアップグレードしてください。

機能	説明
プラットフォーム機能	

機能	説明
ASA 5585-X（すべてのモデル）で適合する ASA FirePOWER SSP ハードウェア モジュールをサポート。 ASA 5512-X ～ ASA 5555-X で ASA FirePOWER ソフトウェア モジュールをサポート。	ASA FirePOWER モジュールは、次世代 IPS（NGIPS）、アの可視性とコントロール（AVC）、URL フィルタリング、ア保護（AMP）などの次世代ファイアウォール サービスこのモジュールは、シングルまたはマルチ コンテキスト モドまたはトランスペアレント モードで使用できます。 **capture interface asa_dataplane**、**debug sfr**、**hw-module mo hw-module module 1 reset**、**hw-module module 1 shutdown**、**host ip**、**session do get-config**、**session do password-reset**、**s show asp table classify domain sfr**、**show capture**、**show con sfr**、**show service-policy**、**sw-module sfr** の各コマンドが導れました。 次の画面が導入されました。 **[Home] > [ASA FirePOWER Status]** **[Wizards] > [Startup Wizard] > [ASA FirePOWER Basic Co** **[Configuration] > [Firewall > Service Policy Rules] > [Add Ser > [Rule Actions] > [ASA FirePOWER Inspection]**
リモート アクセス機能	
クライアントレス SSL VPN のための Windows 8.1 および Windows 7 上での Internet Explorer 11 ブラウザのサポート	クライアントレス SSL VPN のための Windows 7 および Wi Internet Explorer 11 のサポートを追加しました。 変更されたコマンドはありません。 変更された画面はありません。

ASA 9.2(1)/ASDM 7.2(1) の新機能

リリース：**2014年4月24日**

（注） このリリース以降、ASA 5510、ASA 5520、ASA 5540、ASA 5550、ASA 5580 はサポートされていません。ASA バージョン 9.1 は、これらのモデルの最終リリースです。

機能	説明
プラットフォーム機能	
Cisco 適応セキュリティ仮想アプライアンス（ASAv）は、新しいプラットフォームとして ASA シリーズに追加されました。	ASAv は、仮想化環境に包括的なファイアウォール機能を センター トラフィックとマルチテナント環境のセキュリテ す。ASAv は、VMware vSphere 上で稼働します。ASDM ま 用して、ASAv を管理およびモニタすることができます。

機能	説明
ルーティング機能	
BGP のサポート	ボーダー ゲートウェイ プロトコル（BGP）をサポートするよ した。BGP は相互自律システム ルーティング プロトコルです インターネットのルーティング情報を交換するために、イン サービス プロバイダー（ISP）間で使用されるプロトコルです 次のコマンドが導入されました。**router bgp**、**bgp maxas-limi** **log-neighbor-changes**、**bgp transport path-mtu-discovery**、**bgp** **fast-external-fallover**、**bgp enforce-first-as**、**bgp asnotation dot**、 **bgp default local-preference**、**bgp always-compare-med**、**bgp b** **compare-routerid**、**bgp deterministic-med**、**bgp bestpath med** **missing-as-worst**、**policy-list**、**match as-path**、**match communi** **metric**、**match tag**、**as-path access-list**、**community-list**、**addr** **ipv4**、**bgp router-id**、**distance bgp**、**table-map**、**bgp suppress-i** **redistribute-internal**、**bgp scan-time**、**bgp nexthop**、**aggregate** **neighbor**、**bgp inject-map**、**show bgp**、**show bgp cidr-only**、**sh** **community**、**show bgp all neighbors**、**show bgp community**、**sh** **community-list**、**show bgp filter-list**、**show bgp injected-paths**、 **ipv4 unicast**、**show bgp neighbors**、**show bgp paths**、**show bgp** **pending-prefixes**、**show bgp prefix-list**、**show bgp regexp**、**sho** **replication**、**show bgp rib-failure**、**show bgp route-map**、**show** **summary**、**show bgp system-config**、**show bgp update-group**、 **network**、**maximum-path**、**network** 次のコマンドが変更されました。**show route**、**show route sum** **running-config router**、**clear config router**、**clear route all**、**tim** **arrival**、**timers pacing**、**timers throttle**、**redistribute bgp**。 次の画面が導入されました。 **[Configuration] > [Device Setup] > [Routing] > [BGP]** **[Monitoring] > [Routing] > [BGP Neighbors]**、**[Monitoring] > [** **[BGP Routes]** 次の画面が変更されました。 **[設定（Configuration） > [デバイスの設定（Device Setup）] >** **グ（Routing）] > [スタティックルート（Static Routes）] > [追** **> [スタティックルートを追加（Add Static Route）]** **[Configuration] > [Device Setup] > [Routing] > [Route Maps] > [** **Route Map]**

機能	説明
Null0 インターフェイス用のスタティックルート	トラフィックを Null0 インターフェイスへ送信すると、指ワーク宛のパケットはドロップします。この機能は、BGP Triggered Black Hole (RTBH) の設定に役立ちます。 **route** コマンドが変更されました。 次の画面が変更されました。[Configuration] > [Device Setup [Static Routes] > [Add] > [Add Static Route]
Fast Hello に対する OSPF サポート	OSPF は、Fast Hello パケット機能をサポートしているため ワークでのコンバージェンスが高速なコンフィギュレーシ す。 次のコマンドが変更されました。**ospf dead-interval** 次の画面が変更されました。[Configuration] > [Device Setup [OSPF] > [Interface] > [Edit OSPF Interface Advanced Propertie
新規 OSPF タイマー	新しい OSPF タイマーを追加し、古いタイマーを廃止しま 次のコマンドが導入されました。**timers lsa arrival**、**timers throttle** 次のコマンドが削除されました。**timers spf**、**timers lsa-gro** 次の画面が変更されました。[Configuration] > [Device Setup [OSPF] > [Setup] > [Edit OSPF Process Advanced Properties]
ACL を使用する OSPF ルート フィルタリング	ACL を使用したルート フィルタリングがサポートされる た。 次のコマンドが導入されました。**distribute-list** 次の画面が追加されました。[Configuration] > [Device Setup [OSPF] > [Filtering Rules] > [Add Filter Rules]
OSPF モニタリングの強化	OSPF モニタリングの詳細情報が追加されました。 次のコマンドが変更されました。**show ospf events**、**show o ospf statistics**、**show ospf border-routers [detail]**、**show ospf**
OSPF 再配布 BGP	OSPF 再配布機能が追加されました。 次のコマンドが追加されました。**redistribute bgp** 次の画面が追加されました。[Configuration] > [Device Setup [OSPF] > [Redistribution]
EIGRP の [Auto- Summary]	EIGRP の [Auto-Summary] フィールドはデフォルトでディ ました。 次の画面が変更されました。[Configuration] > [Device Setup [EIGRP] > [Setup] > [Edit EIGRP Process Advanced Properties]

機能	説明
ハイ アベイラビリティ機能	
トランスペアレント モードでの異なる地理的位置にあるクラスタ メンバのサポート（サイト間）	トランスペアレント ファイアウォール モードでスパンドEther ドを使用すると、クラスタ メンバを異なる地理的な場所に配 うになりました。ルーテッド ファイアウォール モードのスパ EtherChannel での Inter-Site クラスタリングはサポートされま 変更されたコマンドはありません。 変更された ASDM 画面はありません。
クラスタリングに対するスタティック LACP ポート プライオリティのサポート	一部のスイッチは、LACP でのダイナミック ポート プライオ ポートしていません（アクティブおよびスタンバイ リンク）。 ク ポート プライオリティをディセーブルにすることで、スパ EtherChannel との互換性を高めることができるようになりまし 意事項にも従う必要があります。 • クラスタ制御リンク パスのネットワーク エレメントでは クサムを検証しないようにする必要があります。クラスタ 経由でリダイレクトされたトラフィックには、正しい L4 ムが設定されていません。L4 チェックサムを検証するス り、トラフィックがドロップされる可能性があります。 • ポートチャネル バンドルのダウンタイムは、設定されて アライブ インターバルを超えてはなりません。 **clacp static-port-priority** コマンドが導入されました。 次の画面が変更されました。[Configuration] > [Device Manager Availability and Scalability] > [ASA Cluster]

機能	説明
クラスタリングのためのスパンド EtherChannel での 32 個のアクティブ リンクのサポート	ASA EtherChannels は最大 16 個のアクティブ リンクをサポ なりました。スパンド EtherChannel ではその機能が拡張さ 台のスイッチで使用し、ダイナミック ポート プライオリテ ブルにした場合、クラスタ全体で最大 32 個のアクティブ トします。スイッチは、16 のアクティブ リンクを持つ Eth ポートする必要があります（Cisco Nexus 7000 の F2 シリー ト イーサネット モジュールなど）。 8 個のアクティブ リンクをサポートする VSS または vPC の 合は、スパンド EtherChannel に 16 個のアクティブ リンク （各スイッチに接続された 8 個）。従来は、VSS/vPC で使 あっても、スパンド EtherChannel は 8 個のアクティブ リン タンバイ リンクしかサポートしませんでした。 （注） スパンド EtherChannel で 8 個より多くのアクテ 使用する場合は、スタンバイ リンクも使用でき 32 個のアクティブ リンクをサポートするには、 ンクの使用を可能にする cLACP ダイナミック オリティをディセーブルにする必要があります **clacp static-port-priority** コマンドが導入されました。 次の画面が変更されました。[Configuration] > [Device Mana Availability and Scalability] > [ASA Cluster]
ASA 5585-X の 16 のクラスタ メンバのサポート	ASA 5585-X が 16 ユニット クラスタをサポートするように 変更されたコマンドはありません。 変更された ASDM 画面はありません。
Cisco Nexus 9300 でのクラスタリングのサポート	ASA では、Cisco Nexus 9300 への接続時にクラスタリング す。
リモート アクセス機能	

機能	説明
ISE 許可の変更	ISE Change of Authorization（CoA）機能は、認証、認可、およ ティング（AAA）セッションの属性を、セッション確立後に変 のメカニズムを提供します。AAA のユーザーまたはユーザー ポリシーを変更すると、ISE から ASA へ CoA パケットを直接 証を再初期化し、新しいポリシーを適用できます。インライン 実施ポイント（IPEP）で、ASA と確立された各 VPN セッショ ス コントロール リスト（ACL）を適用する必要がなくなりま エンド ユーザーが VPN 接続を要求すると、ASA はユーザーに 認証を実行し、ネットワークへの制限付きアクセスを提供する ACL を受領します。アカウンティング開始メッセージが ISE に セッションが登録されます。ポスチャ アセスメントが NAC コ と ISE 間で直接行われます。このプロセスは、ASA に透過的で CoA の「ポリシー プッシュ」を介して ASA にポリシーの更新 す。これにより、ネットワーク アクセス権限を高める新しいユ が識別されます。後続の CoA 更新を介し、接続のライフタイ のポリシー評価が ASA に透過的に行われる場合があります。 次のコマンドが導入されました。**dynamic-authorization**、**auth** **debug radius dynamic-authorization** 次のコマンドが変更されました。**without-csd** [**anyconnect**]、 **interim-accounting-update** [**periodic** [*interval*]] 次のコマンドが削除されました。**nac-policy**、**eou**、**nac-setting** 次の画面が変更されました。[Configuration] > [Remote Access V [AAA/Local Users] > [AAA Server Groups] > [Add/Edit AAA Serv
クライアントレス リライタ HTTP 1.1 圧縮処理の改善	クライアントが圧縮コンテンツをサポートしておりコンテンツ られない場合に、サーバから圧縮コンテンツが受け入れられる ライタが変更されました。コンテンツを書き換える必要があり 縮されていると識別される場合、コンテンツは圧縮解除され、 れ、クライアントがサポートしている場合には再圧縮します。 導入または変更されたコマンドはありません。 導入または変更された ASDM 画面はありません。
OpenSSL のアップグレード	ASA 上の OpenSSL のバージョンは、バージョン 1.0.1e に更新 （注） ハートビート オプションは無効になったため、AS Heartbleed バグに対しては脆弱でありません。 導入または変更されたコマンドはありません。 導入または変更された ASDM 画面はありません。
インターフェイス機能	

機能	説明
EtherChannel あたり 16 個のアクティブ リンクのサポート	EtherChannel あたり最大で 16 個のアクティブ リンクを設定 なりました。これまでは、8 個のアクティブ リンクと 8 個 リンクが設定できました。スイッチは、16 個のアクティブ ト可能である必要があります（たとえば、Cisco Nexus 7000 10 ギガビット イーサネット モジュール）。 （注） 旧バージョンの ASA からアップグレードする場 得るために、アクティブなインターフェイスの 設定します（**lacp max-bundle** コマンド）。 次のコマンドが変更されました。**lacp max-bundle** および **p** **min-bundle**。 次の画面が変更されました。[Configuration] > [Device Setup [Add/Edit EtherChannel Interface] > [Advanced]。
最大 MTU が 9198 バイトになりました	ASA で使用できる最大の MTU は 9198 バイトです（CLI の 用のモデルの正確な最大値を確認してください）。この値 ヘッダーは含まれません。以前は、ASA で 65535 バイトの 定できましたが、これは不正確であり、問題が発生する可 た。9198 よりも大きいサイズに MTU を設定している場合 レード時に MTU のサイズが自動的に削減されます。場合 の MTU の変更により MTU の不一致が発生する可能性があ している機器が新しい MTU 値を使用するように設定され 認してください。 次のコマンドが変更されました。**mtu** 次の画面が変更されました。[Configuration] > [Device Setup Settings] > [Interfaces] > [Edit Interface] > [Advanced] バージョン *9.1(6)* でも同様です。
モニタリング機能	

機能	説明
Embedded Event Manager（EEM）	EEM 機能を利用することで、問題をデバッグし、トラブルシグに対して汎用ロギングを提供できます。EEM は、EEM シションを実行してイベントに応答します。2 つの構成要素があつは EEM がトリガーするイベントであり、もう 1 つはアクするイベント マネージャ アプレットです。複数のイベントをマネージャ アプレットに追加でき、イベント マネージャ アそれがトリガーとなって、設定されているアクションが起動 次のコマンドを導入または変更しました。**event manager appl description**、**event syslog id**、**event none**、**event timer**、**event c action cli command**、**output**、**show running-config event manag manager run**、**show event manager**、**show counters protocol ee configure event manager**、**debug event manager**、**debug menu** 次の画面が導入されました。[Configuration] > [Device Manager [Advanced] > [Embedded Event Manager]、[Monitoring] > [Proper Applets]。
SNMP のホスト、ホスト グループ、ユーザー リスト	最大 4000 個までホストを追加できるようになりました。サポアクティブなポーリング先の数は 128 個です。ホスト グルー加する個々のホストを示すためにネットワーク オブジェクトます。1 つのホストに複数のユーザーを関連付けることがで **snmp-server host-group**、**snmp-server user-list**、**show running- snmp-server**、**clear configure snmp-server** の各コマンドが導入されました。 次の画面が変更されました。[Configuration] > [Device Manager [Management Access] > [SNMP]。
SNMP メッセージのサイズ	SNMP で送信できるメッセージのサイズが 1472 バイトまでに拡
SNMP の MIB および OID	ASA は、cpmCPUTotal5minRev OID をサポートするようにな SNMP の sysObjectID OID および entPhysicalVendorType OID に品として ASAv が追加されました。 新しい ASAv プラットフォームをサポートするよう、CISCO-PRODUCTS-MIB および CISCO-ENTITY-VENDORTYP が更新されました。
管理機能	

機能	説明
改善されたワンタイム パスワード認証	十分な認可特権を持つ管理者は、認証クレデンシャルを一権 EXEC モードに移行できます。**auto-enable** オプションが**exec** コマンドに追加されました。 次のコマンドが変更されました。**aaa authorization exec**。 次の画面が変更されました。[Configuration] > [Device Mana[Users/AAA] > [AAA Access] > [Authorization]。
デフォルトでイネーブルになっている Auto Update サーバ証明書の検証	Auto Update Server 証明書の確認がデフォルトでイネーブル新しい設定では、証明書の確認を明示的にディセーブルにます。証明書の確認をイネーブルにしていなかった場合にスからアップグレードしようとすると、証明書の確認はイく、次の警告が表示されます。 `WARNING: The certificate provided by the auto-update s be verified.` `In order to verify this certificate please use the ver option.` コンフィギュレーションの移行では、検証を行わないようされます。次のコマンドを使用します。 **auto-update server no-verification** 次のコマンドが変更されました。**auto-update server** [**verif no-verification**] 次の画面が変更されました。[Configuration] > [Device Mana[System/Image Configuration] > [Auto Update] > [Add Auto Up

バージョン 9.1 の新機能

ASA 9.1(7.4)/ASDM 7.5(2.153) の新機能

リリース：**2016 年 2 月 19 日**

（注） バージョン 9.1(7) はビルドの問題により Cisco.com から削除されました。バージョン 9.1(7.4) またはそれ以降にアップグレードしてください。

機能	説明
リモート アクセス機能	

機能	説明
クライアントレス SSL VPN セッション Cookie アクセスの制限	クライアントレス SSL VPN セッション Cookie が JavaScript などのクラのスクリプトを介してサードパーティからアクセスされないようにする ます。 （注） この機能は、Cisco TAC から使用を推奨された場合のみ使用 い。このコマンドをイネーブルにすると、次のクライアント VPN 機能が警告なしで動作しなくなるため、セキュリティ が発生します。 • Java プラグイン • Java リライタ • ポートフォワーディング。 • ファイルブラウザ • デスクトップ アプリケーション（Microsoft Office アプリケーション 要とする Sharepoint 機能 • AnyConnect Web 起動 • Citrix Receiver、XenDesktop、および Xenon • その他の非ブラウザ ベース アプリケーションおよびブラウザプラ スのアプリケーション **http-only-cookie** コマンドが導入されました。 次の画面が変更されました。[Configuration] > [Remote Access VPN] > [C VPN Access] > [Advanced] > [HTTP Cookie]。 この機能は、*9.2(3)* と *9.4(1)*でも使用できます。
設定可能な SSH 暗号機能と HMAC アルゴリズム	ユーザーは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 換アルゴリズムに対して HMAC と暗号化を設定できます。 次のコマンドが導入されました。**ssh cipher encryption** および **ssh ciphe** ASDM サポートはありません。

機能	説明
クライアントレス SSL VPN キャッシュはデフォルトでは無効	クライアントレス SSL VPN のキャッシュはデフォルトで無効になり イアントレス SSL VPN キャッシュを無効にすることで安定性が改善 シュを有効にするには手動で有効にする必要があります。 **webvpn** **cache** **no disable** 次のコマンドが変更されました。**cache** 次の画面が変更されました。[Configuration] > [Remote Access VPN] > VPN Access] > [Advanced] > [Content Cache] *9.5(2)* 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 HT 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 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** 次の画面に機能が追加されました。[Configuration] > [Device Manage Redirect]
管理機能	
show tech support の強化	**show tech support** コマンドは現在次のとおりです。 • **dir all-filesystems** の出力が含まれます。この出力は次の場合に行 ります。 • SSL VPN コンフィギュレーション：必要なリソースが ASA かを確認します。 • クラッシュ：クラッシュ ファイルの日付のタイムスタンプ ます。 • **show resource usage count all 1** の出力が含まれます。これには、 inspect、syslog などに関する情報が含まれます。この情報は、ハ に関する問題を診断するために役立ちます。 • **show kernel cgroup-controller detail** の出力の削除：このコマン **tech-support detail** の出力内に残されます。 次のコマンドが変更されました。**show tech support** 追加または変更された画面はありません。

機能	説明
CISCO-ENHANCED-MEMPOOL-MIB の cempMemPoolTable のサポート	CISCO-ENHANCED-MEMPOOL-MIB の cempMemPoolTable がサポートさ 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 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 て、プラットフォーム上の4GB以上のメモリのレポーティン トします。 追加または変更されたコマンドはありません。 追加または変更された画面はありません。

ASA 9.1(6)/ASDM 7.1(7) の新機能

リリース：**2015年3月2日**

機能	説明
インターフェイス機能	
最大 MTU が 9198 バイトになりました	ASA で使用できる最大の MTU は 9198 バイトです（CLI のヘルプでご使 の正確な最大値を確認してください）。この値にはレイヤ 2 ヘッダーは ん。以前は、ASA で 65535 バイトの最大 MTU を指定できましたが、こ であり、問題が発生する可能性がありました。9198 よりも大きいサイズ 設定している場合は、アップグレード時にMTUのサイズが自動的に削減 場合によっては、このMTUの変更によりMTUの不一致が発生する可能 す。接続している機器が新しい MTU 値を使用するように設定されてい 認してください。 次のコマンドが変更されました。**mtu** 次の画面が変更されました。[Configuration] > [Device Setup] > [Interface [Interfaces] > [Edit Interface] > [Advanced]

ASA 9.1(5)/ASDM 7.1(6) の新機能

リリース：**2014年3月31日**

機能	説明
管理機能	

機能	説明
セキュア コピー クライアント	SCP サーバとの間でファイルを転送するため、ASA は Secure Copy（SCP をサポートするようになりました。 **ssh pubkey-chain**、**server (ssh pubkey-chain)**、**key-string**、**key-hash**、**ssh st** の各コマンドが導入されました。 **copy scp** コマンドが変更されました。 次の画面が変更されました。 [Tools] > [File Management] > [File Transfer] > [Between Remote Server and Flash > [Device Management] > [Management Access] > [File Access] > [Secure Copy
改善されたワンタイム パスワード認証	十分な認可特権を持つ管理者は、認証クレデンシャルを一度入力すると特 ドに移行できます。**auto-enable** オプションが **aaa authorization exec** コマ ました。 次のコマンドが変更されました。**aaa authorization exec**。 次の画面が変更されました。[Configuration] > [Device Management] > [User Access] > [Authorization]。
ファイアウォール機能	
アクセス グループに関するルールエンジンのトランザクション コミット モデル	イネーブルの場合、ルールの編集の完了後、ルールの更新が適用されます 合パフォーマンスへの影響はありません。 次のコマンドが導入されました。**asp rule-engine transactional-commit**、**sho** **asp rule-engine transactional-commit**、**clear configure asp rule-engine trans** 次の画面が導入されました。[Configuration] > [Device Management] > [Adv Engine]。
モニタリング機能	
SNMP のホスト、ホスト グループ、ユーザー リスト	最大 4000 個までホストを追加できるようになりました。サポートされる ポーリング先の数は 128 個です。ホスト グループとして追加する個々の めにネットワーク オブジェクトを指定できます。1 つのホストに複数のオ 付けることができます。 **snmp-server host-group**、**snmp-server user-list**、**show running-config snmp** **configure snmp-server** の各コマンドが導入または変更されました。 次の画面が変更されました。[Configuration] > [Device Management] > [Man > [SNMP]

機能	説明
Xlate カウントへのポーリング可能にする NAT-MIB cnatAddrBindNumberOfEntries および cnatAddrBindSessionCount OID。	SNMP の xlate_count および max_xlate_count に、NAT-MIB cnatAddrBindNumb および cnatAddrBindSessionCount OID がサポートされるようになりました。 このデータは、**show xlate count** コマンドと同等です。 変更された ASDM 画面はありません。 *8.4(5)* でも使用可能です。
リモート アクセス機能	
AnyConnect DTLS の単一セッションにおけるパフォーマンスの向上	ストリーミング メディアなどの UDP トラフィックは、AnyConnect DTLS 接続信時に多数のパケットがドロップすることに影響を受けていました。たとえり、ストリーミング ビデオの再生画質が悪かったり、ストリーミングが完全りすることがありました。この理由は、フロー制御キューが比較的小さかっります。 DTLS フロー制御キュー サイズを増やし、これを埋め合わせるために管理者サイズを減らしました。TLS セッションでは、この変更に対応するために暗ドの優先順位が高に変更されました。DTLS と TLS の両方のセッションで、はパケットがドロップした場合でも持続するようになりました。これにより トリームは閉じられなくなり、ドロップするパケットの数は他の接続方法となります。 変更されたコマンドはありません。 変更された ASDM 画面はありません。

機能	説明
Webtype ACL の機能拡張	URL 正規化を導入しました。URL 正規化は、パス正規化、ケース正規化 化を含む追加のセキュリティ機能です。ACE とポータルアドレスバーに は、比較前に正規化されます。webvpn トラフィック フィルタリングに関 ためです。 たとえば、https://calo.cisco.com/checkout/Devices をブックマークすると、 の下の https://calo.cisco.com/checkout/Devices/* は一致しているように見え URL 正規化が導入されているので、ブックマーク URL と Web タイプ AC 前に正規化されます。この例では、https://calo.cisco.com/checkout/Devices https://calo.cisco.com/checkout/Devices に正規化され、https://calo.cisco.com/ch は同じままであるため、その 2 つは一致しません。 要件を満たすため、次の設定が必要です。 • URL（https://calo.cisco.com/checkout/Devices）のブックマークを許可 の URL を許可するように ACL を設定します。 • Devices フォルダ内で URL を許可するには、https://calo.cisco.com/che を許可するように ACL を設定します。 変更されたコマンドはありません。 変更された ASDM 画面はありません。

ASA 9.1(4)/ASDM 7.1(5) の新機能

リリース：**2013年12月9日**

機能	説明
リモート アクセス機能	
HTML5 Websocket のプロキシ化	HTML5 Websocket は、クライアントとサーバとの間の持続的接続を提供 アントレス SSL VPN 接続の確立中に、ハンドシェイクはサーバに HTTP 要求として表示されます。ASA プロキシはこの要求をバックエンドにプ ンドシェイクが完了した後にリレーを提供するようになりました。ゲー は現在サポートされていません。 変更されたコマンドはありません。 変更された ASDM 画面はありません。

機能	説明
IKEv2 用の内部 IPv6	IPv6 トラフィックは、IPsec/IKEv2 トンネル経由でトンネルできるようになり れにより ASA から AnyConnect VPN への接続は完全に IPv6 準拠になります。 IPv4 と IPv6 の両方のトラフィックがトンネル化されており、クライアントと ドの両方が GRE をサポートしている場合に使用されます。単一トラフィック 合、または GRE がクライアントあるいはヘッドエンドによってサポートされ 合は、ストレート IPsec を使用します。 （注） この機能は AnyConnect クライアント バージョン 3.1.05 以降が必 **show ipsec sa** および **show vpn-sessiondb detail anyconnect** コマンドの出力は、 れた IPv6 アドレスを反映し、IKEv2 デュアル トラフィックの実行時に GRE ト モードのセキュリティ アソシエーションを示すように更新されました。 **vpn-filter** コマンドを IPv4 および IPv6 ACL に使用することが必要になりまし れた **ipv6-vpn-filter** コマンドが IPv6 ACL を設定するために使用された場合、 します。 変更された ASDM 画面はありません。
Citrix サーバ モバイルを実行しているモバイルデバイスには、追加の接続オプションがあります。	ASA 経由で Citrix サーバに接続するモバイル デバイスのサポートには、トン プの選択、および承認のための RSA Securid が含まれるようになりました。モ ザーに別のトンネル グループを選択することを許可すると、管理者は異なる 使用できます。 Citrix Receiver ユーザーがトンネルグループを選択しないときに VDI 接続用の のトンネルグループを設定するために、**application-type** コマンドが導入され 定のグループ ポリシーまたはユーザー用の VDI 設定を無効にするために、**no** ンが **vdi** コマンドに追加されました。 次の画面が変更されました。[Configuration] > [Remote Access VPN] > [Clientli Access] > [VDI Access]
スプリットトンネリングによる除外 ACL のサポート	VPN トラフィックのスプリットトンネリングは拡張され、除外および組み込 ACL をサポートするようになりました。除外 ACL は以前は無視されていま （注） この機能は AnyConnect クライアント バージョン 3.1.03103 以降が 変更されたコマンドはありません。 変更された ASDM 画面はありません。
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
ASA 5500-X でのクラスタリングのサポート	ASA 5512-X、ASA 5515-X、ASA 5525-X、ASA 5545-X および ASA 5555- クラスタをサポートするようになりました。2ユニットのクラスタリング ンスではデフォルトでイネーブルになります。ASA 5512-X では Security が必要です。 変更されたコマンドはありません。 変更された ASDM 画面はありません。
ヘルス チェック モニタリングの VSS および vPC によるサポートの強化	クラスタ制御リンクが EtherChannel として設定されていて（推奨）、VS アに接続されている場合、ヘルス チェック モニタリングによって安定性 できます。一部のスイッチ（Nexus 5000 など）では、VSS/vPC の 1 つのユ トダウンまたは起動すると、そのスイッチに接続されている EtherChanne ターフェイスが ASA に対してアップと認識される場合がありますが、ス ラフィックが渡されていません。ASA holdtime timeout を低い値（0.8 秒な た場合、ASA が誤ってクラスタから削除される可能性があり、ASA はキ メッセージをこれらのいずれかの EtherChannel インターフェイスに送信し ヘルス チェック機能をイネーブルにすると、ASA はクラスタ制御リンク EtherChannel インターフェイスでキープアライブ メッセージをフラッデ なくとも 1 台のスイッチがそれを受信できることを確認します。 **health-check** [**vss-enabled**] コマンドが変更されました。 次の画面が変更されました。[Configuration] > [Device Management] > [High Scalability] > [ASA Cluster]
異なる地理的位置にあるクラスタ メンバのサポート（サイト間）。個別インターフェイス モードのみ	個別インターフェイス モードを使用すると、クラスタ メンバを異なる地 置できるようになりました。サイト間のガイドラインについては、設定ガ てください。 変更されたコマンドはありません。 変更された ASDM 画面はありません。
Cisco Nexus 5000 と Cisco Catalyst 3750-X を使用するクラスタリングのサポート	ASA では、Cisco Nexus 5000 および Cisco Catalyst 3750-X への接続時にク サポートします。 **health-check** [**vss-enabled**] コマンドが変更されました。 次の画面が変更されました。[Configuration] > [Device Management] > [High Scalability] > [ASA Cluster]
基本的な操作機能	

機能	説明
DHCP 再バインド機能	DHCP 再バインド フェーズに、クライアントはトンネル グループ リスト内の サーバへの再バインドを試行するようになりました。このリリース以前には スの更新に失敗した場合、クライアントは代替サーバへ再バインドしません 次のコマンドが導入されました。**show ip address dhcp lease proxy**、**show ip a** **lease summary**、および **show ip address dhcp lease server** 次の画面が導入されました。[Monitoring] > [Interfaces] > [DHCP]> [DHCP Lease
トラブルシューティング機能	
crashinfo ダンプには AK47 フレームワーク情報が含まれる	アプリケーション カーネル層 4 ～ 7（AK47）フレームワーク関連情報は、c プから入手できます。新しいオプション **ak47** が **debug menu** コマンドに追加 フレームワークの問題のデバッグに役立てることができます。crashinfo ダン ムワーク関連情報は次のとおりです。 • AK47 インスタンスの作成。 • AK47 インスタンスの破棄。 • メモリ マネージャ フレームでの crashinfo の生成。 • ファイバ スタック オーバーフロー後の crashinfo の生成。 • ローカル変数オーバーフロー後の crashinfo の生成。 • 例外が発生した後の crashinfo の生成。

ASA 9.1(3)/ASDM 7.1(4) の新機能

リリース：2013年9月18日

機能	説明
モジュール機能	
マルチ コンテキスト モードでの ASA CX モジュールのサポート	ASA でコンテキストごとに ASA CX サービス ポリシーを設定できます。 （注） コンテキストごとに ASA サービス ポリシーを設定できますが、 設定されている）ASA CX モジュール自体はシングル コンテキス デバイスです。つまり、ASA から着信するコンテキスト固有のト は共通の ASA CX ポリシーと照合されます。 ASA CX 9.2(1) 以降が必要です。 変更されたコマンドはありません。 変更された ASDM 画面はありません。

機能	説明
ASA CX SSP-40 および -60 用の ASA 5585-X（SSP-40 および -60 搭載）サポート	ASA CX SSP-40 および -60 モジュールは、SSP-40 および -60 搭載の ASA するレベルで使用できます。 ASA CX 9.2(1) 以降が必要です。 変更されたコマンドはありません。 変更された画面はありません。
ASA CX バックプレーンでキャプチャされたパケットのフィルタリング	**match** または **access-list** キーワードを **capture interface asa_dataplane** コマ用して、ASA CX バックプレーンでキャプチャされたパケットをフィルタ ようになりました。ASA CX モジュールに固有の制御トラフィックは、a match フィルタリングの影響を受けません。ASA はすべての制御トラフ チャします。マルチ コンテキスト モードでは、コンテキストごとにパケ を設定します。マルチ コンテキスト モードのすべての制御トラフィック はシステム実行スペースだけであることに注意してください。access list 使用して制御トラフィックのみのフィルタリングを行うことができない オプションはシステム実行スペースでは使用できません。 ASA CX 9.2(1) 以降が必要です。 **capture interface asa_dataplane** コマンドが変更されました。 新しいオプションとして、[Use backplane channel] が [Packet Capture Wizar Traffic Selector] 画面と [Egress Selector] 画面に追加されました。これによ クプレーン上でキャプチャされたパケットのフィルタリングが可能にな
モニタリング機能	
メモリの上位 10 ユーザーの表示機能	上位割り当て済み bin サイズと割り当て済みの bin サイズごとの上位 10 P とができます。以前は、この情報を見るためには、複数のコマンド（**sho** コマンドと **show memory binsize** コマンド）の入力が必要でした。新しい り、メモリの問題の迅速な分析が可能です。 次のコマンドが導入されました。**show memory top-usage** 変更された ASDM 画面はありません。 *8.4(6)* でも使用可能です。

機能	説明
Smart Call Home	ASA クラスタリングをサポートする新しいタイプの Smart Call Home メッセー ました。 Smart Call Home クラスタリング メッセージは、次の 3 種類のイベントに対し されます。 • ユニットがクラスタに参加したとき • ユニットがクラスタから脱退したとき • クラスタ ユニットがクラスタ マスターになったとき 送信される各メッセージには次の情報が含まれています。 • アクティブ クラスタのメンバ数 • クラスタ マスターでの **show cluster info** コマンドおよび **show cluster his** ドの出力 次のコマンドが変更されました。**show call-home**、**show running-config call-h** 変更された ASDM 画面はありません。 *9.0(3)* でも使用可能です。
リモート アクセス機能	
user-storage value コマンドのパスワードの **show** コマンドでの暗号化	**show running-config** コマンドを入力すると、**user-storage value** コマンドのパ 暗号化されます。 次のコマンドが変更されました。**user-storage value** 次の画面が変更されました。[Configuration] > [Remote Access VPN] > [Clientle Access] > [Group Policies] > [More Options] > [Session Settings] *8.4(6)* でも使用可能です。

ASA 9.1(2)/ASDM 7.1(3) の新機能

リリース：2013年5月14日

（注） 8.4(6) で追加された機能は、この表で明示されていない限り、9.1(2) には含まれていません。

機能	説明
認定機能	

機能	説明
FIPS 認定および Common Criteria 認定	FIPS 140-2 非専有セキュリティ ポリシーは、Cisco ASA シリーズのレベル 証の一部として更新されました。このシリーズには、Cisco ASA 5505、A 5520、ASA 5540、ASA 5550、ASA 5580、ASA 5512-X、ASA 5515-X、AS 5545-X、ASA 5555-X、ASA 5585-X、および ASA サービス モジュールが Common Criteria Evaluation Assurance Level 4（EAL4）が更新されました。 Cisco ASA および VPN プラットフォーム ソリューションの特定の Target （TOE）の基準が提供されます。
暗号化機能	
フェールオーバー リンクおよびステート リンクの通信を暗号化する IPsec LAN-to-LAN トンネルのサポート	フェールオーバー キーに独自の暗号化を使用する代わりに（**failover key** フェールオーバー リンクおよびステート リンクの暗号化に IPsec LAN-to が使用できるようになりました。 （注） フェールオーバー LAN-to-LAN トンネルは、IPsec（その他の V スには適用されません。 **failover ipsec pre-shared-key**、**show vpn-sessiondb** の各コマンドが導入ま した。 次の画面が変更されました。[Configuration] > [Device Management] > [Hig [Failover] > [Setup]。

機能	説明
SSL 暗号化用の追加のエフェメラル Diffie-Hellman 暗号	ASA で次のエフェメラル Diffie-Hellman（DHE）SSL 暗号スイートがサポート になりました。 • DHE-AES128-SHA1 • DHE-AES256-SHA1 これらの暗号スイートは、RFC 3268『*Advanced Encryption Standard (AES) Cip* *Transport Layer Security (TLS)*』で指定されています。 DHE では完全転送秘密が提供されるため、クライアントでサポートされてい は推奨される暗号です。次の制限事項を確認してください。 • DHE は SSL 3.0 接続ではサポートされないため、SSL サーバの TLS 1.0 も にしてください。 `!! set server version` `ciscoasa(config)# ssl server-version tlsv1 sslv3` `!! set client version` `ciscoasa(config) # ssl client-version any` • 一部の一般的なアプリケーションで DHE はサポートされないため、SSL トとサーバの両方に共通の暗号スイートを使用できるように、他の SSL を少なくとも 1 つ含めます。 • 一部のクライアントで DHE はサポートされない場合があります。AnyC よび 3.0、Cisco Secure Desktop、Internet Explorer 9.0 などです。 **ssl encryption** コマンドが変更されました。 次の画面が変更されました。[Configuration] > [Device Management] > [Advanc Settings] *8.4(4.1)* でも使用可能です。
管理機能	

機能	説明
ローカルデータベースを使用する場合の管理者パスワードポリシーのサポート	ローカル データベースを使用して CLI または ASDM アクセスの認証を設 指定期間を過ぎるとユーザーにパスワードの変更を要求し、パスワードの 変更文字数などのパスワード標準に従うことを要求するパスワード ポリ ます。 次のコマンドが導入されました。**change-password**、**password-policy lifeti** **password-policy minimum changes**、**password-policy minimum-length**、**pa** **minimum-lowercase**、**password-policy minimum-uppercase**、**password-pol** **minimum-numeric**、**password-policy minimum-special**、**password-policy auth** **clear configure password-policy**、**show running-config password-policy** 次の画面が導入されました。[Configuration] > [Device Management] > [Users/A Policy] *8.4(4.1)* でも使用可能です。
SSH 公開キー認証のサポート	ASA への SSH 接続の公開キー認証は、ユーザー単位で有効にできるよう 公開キー ファイル（PKF）でフォーマットされたキーまたは Base64 キー す。PKF キーは、4096 ビットまで使用できます。ASA がサポートする B 大 2048 ビット）では大きすぎるキーについては、PKF 形式を使用します 次のコマンドが導入されました。**ssh authenticaion**。 次の画面が導入されました。 [Configuration] > [Device Management] > [Users/AAA] > [User Accounts] > [Ed > [Public Key Authentication] および [Configuration] > [Device Management] > [User Accounts] > [Edit User Account] > [Public Key Using PKF] *8.4(4.1)* でも使用可能。*PKF* キー形式は *9.1(2)* でのみサポートされます。
SSH の AES-CTR 暗号化	ASA での SSH サーバーの実装が、AES-CTR モードの暗号化をサポートで ました。
SSH キー再生成間隔の改善	SSH 接続は、接続時間 60 分間またはデータ トラフィック 1 GB ごとに再 次のコマンドが導入されました。**show ssh sessions detail**。
SSH キー交換の Diffie-Hellman グループ 14 のサポート	SSH キー交換に Diffie-Hellman グループ 14 が追加されました。これまで だけがサポートされていました。 次のコマンドが導入されました。**ssh key-exchange**。 次の画面が変更されました。[Configuration] > [Device Management] > [Man > [ASDM/HTTPS/Telnet/SSH] *8.4(4.1)* でも使用可能です。

機能	説明
管理セッションの最大数のサポート	同時 ASDM、SSH、Telnet セッションの最大数を設定できます。 次のコマンドが導入されました。**quota management-session**、**show running-c management-session**、**show quota management-session**。 次の画面が導入されました。[Configuration] > [Device Management] > [Manage > [Management Session Quota] *8.4(4.1)* でも使用可能です。
ASDM のプリログイン バナーのサポート	管理者は、ユーザーが管理アクセスのために ASDM にログインする前に表示 セージを定義できます。このカスタマイズ可能コンテンツはプリログイン バ れ、特別な要件や重要な情報をユーザーに通知することができます。
デフォルトの Telnet パスワードが削除されました	ASA への管理アクセスのセキュリティ向上のために、Telnet のデフォルト ロ ワードが削除されました。Telnet を使用してログインする前に、パスワードを する必要があります。**注**：ログイン パスワードが使用されるのは、Telnet コ（**aaa authentication telnet console** コマンド）を設定しない場合の Telnet に対 す。 以前はパスワードをクリアすると、ASA がデフォルト「cisco」を復元してい ではパスワードをクリアすると、パスワードは削除されるようになりました ログイン パスワードは、スイッチから ASASM への Telnet セッションでも使 （**session** コマンドを参照）。最初 ASASM のアクセスでは、ログイン パスワ するまで、**service-module session** コマンドを使用します。 **passwd** コマンドが変更されました。 変更された ASDM 画面はありません。 *9.0(2)* でも使用可能です。
プラットフォーム機能	
電源投入時自己診断テスト（POST）のサポート	ASA は、FIPS 140-2 準拠モードで実行されていない場合でも、起動時の電源 診断テストを実行します。 AES-GCM/GMAC アルゴリズム、ECDSA アルゴリズム、PRNG、Determinist Generator Validation System（DRBGVS）の変更に対応するために、POST が追 た。
疑似乱数生成（PRNG）の改善	X9.31 の実装がアップグレードされ、シングルコアの ASA での Network Dev Profile（NDPP）に対応するために、3DES 暗号化の代わりに AES-256 の暗号 るようになりました。

機能	説明
イメージ検証のサポート	SHA-512 イメージ整合性チェックのサポートが追加されました。 次のコマンドが変更されました。**verify** 変更された ASDM 画面はありません。 *8.4(4.1)* でも使用可能です。
ASA サービス モジュール上でプライベート VLAN のサポート	ASASM では、プライベート VLAN を使用できます。ASASM にプライマ り当てると、ASASM は自動的にセカンダリ VLAN トラフィックを処理し 能は、ASASM 上での設定は必要ありません。詳細については、スイッチ レーション ガイドを参照してください。
CPU プロファイルの拡張機能	**cpu profile activate** コマンドが、以下をサポートするようになりました。 • トリガーされるまでのプロファイラの開始の遅延（グローバルまたは CPU%） • シングル スレッドのサンプリング 次のコマンドが変更されました。**cpu profile activate** [*n-samples*] [**sample-p** *process-name*] [**trigger cpu-usage** *cpu%* [*process-name*] 変更された ASDM 画面はありません。 *8.4(6)* でも使用可能です。
DHCP 機能	
インターフェイスごとの DHCP リレー サーバ（IPv4 のみ）	DHCP リレー サーバーをインターフェイスごとに設定できるようになり インターフェイスに届いた要求は、そのインターフェイス用に指定され してのみリレーされます。インターフェイス単位の DHCP リレーでは、 されません。 **dhcprelay server**（インターフェイス設定モード）、**clear configure dhcpr** **running-config dhcprelay** の各コマンドが導入または変更されました。 次の画面が変更されました。[Configuration] > [Device Management] > [DHCP

機能	説明
DHCP の信頼できるインターフェイス	DHCP Option 82 を維持するために、インターフェイスを信頼できるインターして設定できるようになりました。DHCP Option 82 は、DHCP スヌーピングソース ガードのために、ダウンストリームのスイッチおよびルータによってす。通常、ASA DHCP リレー エージェントが Option 82 をすでに設定した Dトを受信しても、giaddr フィールド（サーバーにパケットを転送する前に、ジェントによって設定された DHCP リレー エージェント アドレスを指定すド）が 0 に設定されている場合は、ASA はそのパケットをデフォルトで削除ンターフェイスを信頼できるインターフェイスとして指定することで、Optiしたままパケットを転送できます。 次のコマンドを導入または変更しました。**dhcprelay information trusted**、**dhinformarion trust-all**、**show running-config dhcprelay** 次の画面が変更されました。[Configuration] > [Device Management] > [DHCP] > [
モジュール機能	
ASA 5585-X のネットワークモジュール サポート	ASA 5585-X が、スロット 1 でネットワーク モジュール上の追加インターフポートするようになりました。次のオプション ネットワーク モジュールのつをインストールできます。 • ASA 4 ポート 10G ネットワーク モジュール • ASA 8 ポート 10G ネットワーク モジュール • ASA 20 ポート 1G ネットワーク モジュール *8.4(4.1)* でも使用可能です。
ASA 5585-X DC 電源サポート	ASA 5585-X DC 電源のサポートが追加されました。 *8.4(5)* でも使用可能です。
デモンストレーション用 ASA CX モニタリング専用モードのサポート	デモンストレーション目的でのみ、サービス ポリシー用のモニタリング専用ネーブルにすることができ、元のトラフィックに影響を与えずに、トラフィを ASA CX モジュールに転送することができます。 デモンストレーション用のもう 1 つのオプションは、サービス ポリシーの作フィック転送をモニタ専用モードで設定することです。トラフィック転送イイスは、ASA をバイパスすることにより、すべてのトラフィックを ASA CXに直接送信します。 次のコマンドを導入または変更しました。**cxsc** {**fail-close** | **fail-open**} **monitor** **traffic-forward cxsc monitor-only** 次の画面が変更されました。[Configuration] > [Firewall] > [Service Policy Rules] >Policy Rule] > [Rule Actions] > [ASA CX Inspection] トラフィック転送機能は CLI のみでサポートされます。

機能	説明
ASA CX モジュールおよび NAT 64 のサポート	ASA CX モジュールとともに NAT 64 を使用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。 変更された ASDM 画面はありません。
NetFlow 機能	
NetFlow フロー更新イベントおよび NetFlow テンプレートの拡張セットのサポート	フロー更新イベントに加え、NetFlowテンプレートが存在するようになり より NAT で IP バージョンに変更があるフローと、NAT 後に IPv6 のまま ローを追跡できます。 IPv6 変換のサポートのため、2 つの新しいフィールドが追加されました。 いくつかの NetFlow フィールド ID が、IPFIX の同等のものに変更されま 詳細については、『*Cisco ASA Implementation Note for NetFlow Collectors*』 さい。
ファイアウォール機能	
EtherType ACL による IS-IS トラフィック（トランスペアレントファイアウォールモード）のサポート	トランスペアレント ファイアウォール モードでは、ASA が EtherType AC IS-IS トラフィックを渡すことができるようになりました。 **access-list ethertype** {**permit** | **deny**} **is-is** コマンドが変更されました。 次の画面が変更されました。[Configuration] > [Device Management] > [Mar > [EtherType Rules] *8.4(5)* でも使用可能です。
ハーフクローズタイムアウト最小値を 30 秒に削減	グローバルタイムアウトおよび接続タイムアウトの両方のハーフクロー トの最小値は、より優れた DoS 保護を提供するために 5 分から 30 秒に短 **set connection timeout half-closed**、**timeout half-closed** の各コマンドが変更 次の画面が変更されました。 **[Configuration] > [Firewall] > [Service Policy Rules] > [Connection Settings]** **[Configuration] > [Firewall] > [Advanced] > [Global Timeouts]**。
リモート アクセス機能	

機能	説明
IKE セキュリティとパフォーマンスの改善	IKE v2 に加えて IKE v1 に対して、IPSec-IKE セキュリティ アソシエーション限できます。 次のコマンドが変更されました。**crypto ikev1 limit** 次の画面が変更されました。[Configuration] > [Site-to-Site VPN] > [Advanced] > [I
	IKE v2 ナンスのサイズが 64 バイトに増加しました。 ASDM 画面または CLI に変更はありません。
	サイト間 IKE v2 では、新しいアルゴリズムは、子の IPsec SA によって使用さアルゴリズムが親の IKE より強力でないことを保障します。強力アルゴリズベルに下げられます。 この新しいアルゴリズムはデフォルトでイネーブルです。この機能をディセないことを推奨します。 次のコマンドが導入されました。**crypto ipsec ikev2 sa-strength-enforcement** 変更された ASDM 画面はありません。
	サイト間の場合は、IPSec データ ベースの再調整をディセーブルにできます 次のコマンドが変更されました。**crypto ipsec security-association** 次の画面が変更されました。[Configuration] > [Site-to-Site] > [IKE Parameter]
ホスト スキャンおよびASA相互運用性の改善	ホスト スキャンおよび ASA のプロセスが改善され、クライアントから ASA属性が転送できます。つまり、クライアントとのVPN接続を確立し、ダイナセス ポリシーを適用するために、ASA はより長い時間を割くことができます *8.4(5)* でも使用可能です。

機能	説明
クライアントレス SSL VPN：Windows 8 のサポート	このリリースでは、Windows 8 x86（32 ビット）および Windows 8 x64（6 レーティング システムのサポートが追加されました。 Windows 8 では次のブラウザのみがサポートされます。 • Internet Explorer 10（デスクトップのみ） • Firefox（すべての Windows 8 バージョンをサポート） • Chrome（すべての Windows 8 バージョンをサポート） 次の制限事項を確認してください。 • Internet Explorer 10 • Modern（別名 Metro）ブラウザはサポートされません。 • 拡張保護モードをイネーブルにする場合は、信頼できるゾーンに ることを推奨します。 • 拡張保護モードがイネーブルの場合は、スマート トンネルおよ サポートされません。 • Windows 8 PC への Java Remote Desktop Protocol (RDP) プラグイン接続 されません。 *9.0(2)* でも使用可能です。
Cisco Secure Desktop：Windows 8 のサポート	CSD 3.6.6215 がアップデートされ、プリログイン ポリシーのオペレーテ のチェックで Windows 8 が選択できるようになりました。 次の制限事項を確認してください。 • Secure Desktop（Vault）は Windows 8 ではサポートされません。 *9.0(2)* でも使用可能です。
Dynamic Access Policies：Windows 8 のサポート	ASDM がアップデートされ、DAP オペレーティング システム属性で Win きるようになりました。 *9.0(2)* でも使用可能です。
モニタリング機能	

機能	説明
NSEL	フロートラフィックの定期的なバイトカウンタを提供するために flow-updat 導入されました。flow-update イベントが NetFlow コレクタに送信される時間 できます。flow-update レコードを送信するコレクタをフィルタリングできま 次のコマンドを導入または変更しました。**flow-export active refresh-interval**、 **event-type** 次の画面が変更されました。 [Configuration] > [Device Management] > [Logging] > [NetFlow] **[Configuration] > [Firewall] > [Service Policy Rules] > [Add Service Policy Rule** **Rule Actions] > [NetFlow] > [Add Flow Event]** *8.4(5)* でも使用可能です。

ASA 9.1(1)/ASDM 7.1(1) の新機能

リリース：**2012年12月3日**

（注） 8.4（4.x）、8.4（5）、8.4（6）、9.0（2）にない機能は、9.0（1）機能テーブルにない限り 9.1（1）にもありません。

機能	説明
モジュール機能	
ASA 5512-X ～ ASA 5555-X に対する ASA CX SSP のサポート	ASA 5512-X、ASA 5515-X、ASA 5525-X、ASA 5545-X、および に対する ASA CX SSP ソフトウェア モジュールのサポートが した。ASA CX ソフトウェア モジュールには、ASA 上に Cisc ステート ドライブ（SSD）が必要です。SSD の詳細について 5500-X のハードウェア ガイドを参照してください。 **session cxsc**、**show module cxsc**、**sw-module cxsc** の各コマンド ました。 変更された画面はありません。

バージョン 9.0 の新機能

ASA 9.0(4)/ASDM 7.1(4) の新機能

ASA 9.0(4)/ASDM 7.1(4) には新機能はありませんでした。

ASA 9.0(3)/ASDM 7.1(3) の新機能

リリース：**2013年7月22日**

（注） 8.4（4.x）、8.4（5）、8.4（6）にない機能は、9.0（1）機能テーブルにない限り 9.0（3）にもありません。

機能	説明
モニタリング機能	
Smart Call Home	ASA クラスタリングをサポートする新しいタイプの Smart セージを追加しました。 Smart Call Home クラスタリング メッセージは、次の 3 種類 対してのみ送信されます。 • ユニットがクラスタに参加したとき • ユニットがクラスタから脱退したとき • クラスタ ユニットがクラスタ マスターになったとき 送信される各メッセージには次の情報が含まれています。 • アクティブ クラスタのメンバ数 • クラスタ マスターでの **show cluster info** コマンドおよ **history** コマンドの出力

ASA 9.0(2)/ASDM 7.1(2) の新機能

リリース日：**2013 年 2 月 25 日**

（注） 8.4（4.x）、8.4（5）、8.4（6）にない機能は、9.0（1）機能テーブルにない限り 9.0（2）にもありません。

機能	説明
リモート アクセス機能	

機能	説明
クライアントレス SSL VPN：Windows 8 のサポート	このリリースでは、Windows 8 x86（32 ビット）および Windo ビット）オペレーティング システムのサポートが追加されま Windows 8 では次のブラウザのみがサポートされます。 • Internet Explorer 10（デスクトップのみ） • Firefox（すべての Windows 8 バージョンをサポート） • Chrome（すべての Windows 8 バージョンをサポート） 次の制限事項を確認してください。 • Internet Explorer 10 • Modern（別名 Metro）ブラウザはサポートされませ • 拡張保護モードをイネーブルにする場合は、信頼でき ASA を追加することを推奨します。 • 拡張保護モードがイネーブルの場合は、スマート ト びポート転送はサポートされません。 • Windows 8 PC への Java Remote Desktop Protocol (RDP) プラ は、サポートされません。
管理機能	
デフォルトの Telnet パスワードが削除されました	ASA への管理アクセスのセキュリティ向上のために、Telnet の ログインパスワードが削除されました。Telnet を使用してログ に、パスワードを手動で設定する必要があります。**注**：ログイ ドが使用されるのは、Telnet ユーザー認証（**aaa authentication** コマンド）を設定しない場合の Telnet に対してのみです。 以前はパスワードをクリアすると、ASA がデフォルト「cisco ていました。今ではパスワードをクリアすると、パスワードは ようになりました。 ログイン パスワードは、スイッチから ASASM への Telnet セ も使用されます（**session** コマンドを参照）。最初 ASASM の は、ログインパスワードを設定するまで、**service-module sess** を使用します。 **passwd** コマンドが変更されました。 変更された ASDM 画面はありません。

ASA 9.0(1)/ASDM 7.0(1) の新機能

リリース：**2012年10月29日**

（注） 8.4(4.x)、8.4(5)、および8.4(6) で追加された機能は、この表で明示されていない限り、9.0(1) には含まれていません。

機能	説明
ファイアウォール機能	

機能	説明
Cisco TrustSec の統合	Cisco TrustSec は、既存の ID 認証インフラストラクチャを基盤 セス コントロール ソリューションです。ネットワーク デバイ タ機密性保持を目的としており、セキュリティ アクセス サー のプラットフォーム上で統合します。Cisco TrustSec ソリューシ 実行デバイスはユーザー属性とエンドポイント属性の組み合わ て、ロールベースおよびアイデンティティベースのアクセス ルを決定します。 このリリースでは、ASA に Cisco TrustSec が統合されており、 ティ グループに基づいてポリシーが適用されます。Cisco Trus ン内のアクセス ポリシーは、トポロジには依存しません。ネ IP アドレスではなく、送信元および宛先のデバイスのロールに ます。 ASA は、セキュリティ グループに基づくその他のタイプのポ プリケーション インスペクションなど）に対しても Cisco Trust ションを活用できます。たとえば、設定するクラスマップの中 リティ グループに基づくアクセス ポリシーを入れることがで 次のコマンドが導入または変更されました。**access-list extend** **enable**、 **cts server-group**、**cts sxp default**、**cts sxp retry period** **reconcile period**、**cts sxp connection peer**、**cts import-pac**、**cts** **environment-data**、**object-group security**、**security-group**、**sho** **running-config cts**、**show running-config object-group**、**clear co** **clear configure object-group**、**show cts**、**show object-group**、**sh** **security-group**、**clear cts**、**debug cts** 次の MIB が導入されました：CISCO-TRUSTSEC-SXP-MIB 次の画面が導入または変更されました。 **[Configuration] > [Firewall] > [Identity by TrustSec]** **[Configuration] > [Firewall] > [Objects] > [Security Groups Obj** **[Configuration] > [Firewall] > [Access Rules] > [Add Access Rul** **[Monitoring] > [Properties] > [Identity by TrustSec] > [PAC]** **[Monitoring] > [Properties] > [Identity by TrustSec] > [Environm** **[Monitoring] > [Properties] > [Identity by TrustSec] > [SXP Con** **[Monitoring] > [Properties] > [Identity by TrustSec] > [IP Mapp** **[Monitoring] > [Properties] > [Connections]** **[Tools] > [Packet Tracer]**

機能	説明
Cisco クラウド Web セキュリティ（ScanSafe）	Cisco クラウド Web セキュリティは、Web トラフィックに ツスキャンなどのマルウェア防御サービスを実行します。 アイデンティティに基づいて Web トラフィックのリダイレ 行うこともできます。 （注） クライアントレス SSL VPN は、クラウド Web セ はサポートされません。クライアントレス SSL V クについては、クラウド Web セキュリティの A ポリシーの対象外となっていることを確認して **class-map type inspect scansafe**、**default user group**、**http**[**s**]（ **inspect scansafe**、**license**、**match user group**、**policy-map ty** **scansafe**、**retry-count**、**scansafe**、**scansafe general-options**、 | **backup**}、**show conn scansafe**、**show scansafe server**、**show** **statistics**、**user-identity monitor**、**whitelist** の各コマンドが導 されました。 次の画面が導入または変更されました。 **[Configuration] > [Device Management] > [Cloud Web Secur** **[Configuration] > [Firewall] > [Objects] > [Class Maps] > [Clou** **[Configuration] > [Firewall] > [Objects] > [Class Maps] > [Clou** **> [Add/Edit]** **[Configuration] > [Firewall] > [Objects] > [Inspect Maps] > [** **Security]** **[Configuration] > [Firewall] > [Objects] > [Inspect Maps] > [** **Security] > [Add/Edit]** **[Configuration] > [Firewall] > [Objects] > [Inspect Maps] >[C** **Security] > [Add/Edit] > [Manage Cloud Web Security Class** **[Configuration] > [Firewall] > [Identity Options][Configurat** **> [Service Policy Rules]** **[Monitoring] > [Properties] > [Cloud Web Security]**
ICMP コードによって ICMP トラフィックをフィルタリングするための拡張 ACL とオブジェクト機能拡張	ICMP コードに基づいて ICMP トラフィックの許可または うになりました。 次のコマンドを導入または変更しました。**access-list exten** **service-object**、**service** 次の画面が導入または変更されました。 **[Configuration] > [Firewall] > [Objects] > [Service Objects/G** **[Configuration] > [Firewall] > [Access Rule]**
ASASM でのユニファイド コミュニケーションのサポート	ASASM は、すべてのユニファイドコミュニケーション機 るようになりました。

機能	説明
逆引き DNS ルックアップ用の NAT のサポート	NAT ルールがイネーブルにされた DNS インスペクションを使 NAT、IPv6 NAT、および NAT64 を使用する場合、NAT は逆引 クアップ用の DNS PTR レコードの変換をサポートするようにな
Per-Session PAT	Per-session PAT 機能によって PAT のスケーラビリティが向上 ラスタリングの場合に各メンバ ユニットに独自の PAT 接続を ようになります。Multi-Session PAT 接続は、マスター ユニッ てマスターユニットを所有者とする必要があります。Per-Sess ションの終了時に、ASA からリセットが送信され、即座に xl れます。このリセットによって、エンド ノードは即座に接続 TIME_WAIT 状態を回避します。対照的に、Multi-Session PAT タイムアウトが使用されます（デフォルトでは 30 秒）。「ヒ ラン」トラフィック、たとえば HTTP や HTTPS の場合は、Pe 能によって、1 アドレスでサポートされる接続率が大幅に増加 あります。Per-session 機能を使用しない場合は、特定の IP プロ する 1 アドレスの最大接続率は約 2000/秒です。Per-session 機 る場合は、特定の IP プロトコルに対する 1 アドレスの接続率 均ライフタイムです。 デフォルトでは、すべての TCP トラフィックおよび UDP DNS クが、Per-session PAT xlate を使用します。Multi-Session PAT の 活用できるトラフィック、たとえば H.323、SIP、Skinny に対し PAT をディセーブルにするには、Per-session 拒否ルールを作成 次のコマンドが導入されました。**xlate per-session**、**clear conf** **show running-config xlate** 次の画面が導入されました。[Configuration] > [Firewall] > [Adv [Per-Session NAT Rules]

機能	説明
間接接続されたサブネットの ARP キャッシュの追加	ASA ARP キャッシュには、直接接続されたサブネットかけがデフォルトで含まれています。また、ARPキャッシュたサブネットを含めることができるようになりました。セスクを認識していない場合は、この機能をイネーブルにすません。この機能は、ASAに対するサービス拒否（DoS）場合があります。任意のインターフェイスのユーザが大量送信して、偽エントリでASA ARPテーブルがあふれる可能 次の機能を使用する場合は、この機能を使用する必要があます。 • セカンデリ サブネット。 • トラフィック転送の隣接ルートのプロキシ ARP。 **arp permit-nonconnected** コマンドが導入されました。 次の画面が変更されました。[Configuration] > [Device Mana[Advanced]> [ARP] > [ARP Static Table]。 *8.4(5)* でも使用可能です。
ダイナミック ACL からピンホール メカニズムへの SunRPC の変更	これまでは、Sun RPCインスペクションは発信アクセス リしません。これは、インスペクション エンジンでセカンダイナミック アクセス リストが使用されるためです。 このリリースでは、ASA でダイナミック アクセス リスト入力方向のみでサポートされ、ダイナミック ポート宛ての クは ASA によってドロップされます。したがって、Sun Rションは、ピンホール メカニズムを設定して出力トラフィトします。Sun RPCインスペクションは、このピンホール用して発信ダイナミック アクセス リストをサポートしま *8.4(4.1)* でも使用可能です。

機能	説明
インスペクション リセット アクションの変更	これまでは、インスペクション エンジン ルールに従って ASA ケットがドロップされると、ドロップされたパケットのソー に RST が 1 つのみ送信されました。この動作により、リソー 発生する可能性があります。 このリリースでは、リセットアクションを使用するようにイン ン エンジンを設定し、パケットによってリセットがトリガー 次の条件で ASA によって TCP リセットが送信されます。 • **service resetoutbound** コマンドがイネーブルの場合、ASA セットを内部ホストに送信します。（**service resetoutbou** は、デフォルトでイネーブルです）。 • **service resetinbound** コマンドがイネーブルの場合、ASA に トを外部ホストに送信します。（**service resetinbound** コマ フォルトではディセーブルです）。 詳細については、ASA コマンド リファレンスの **service** コマン てください。 この動作によって、リセット アクションが ASA および内部サ をリセットすることが確実になります。したがって、DoS 攻撃 す。外部ホストの場合、ASA はリセットをデフォルトで送信 リセットによって情報が公開されません。 *8.4(4.1)* でも使用可能です。
サービス ポリシー ルールの最大接続数の引き上げ	サービス ポリシー ルールの最大接続数が 65535 から 2000000 られました。 **set connection conn-max**、**set connection embryonic-conn-max**、**s** **per-client-embryonic-max**、**set connection per-client-max** の各コ 更されました。 次の画面が変更されました。[Configuration] > [Firewall] > [Serv Rules] > [Connection Settings] *8.4(5)* でも使用可能です。
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
ASA 5580 および 5585-X の ASA クラスタリング	

機能	説明
	ASA クラスタリングを利用すると、複数の ASA をグループ化 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 ての利便性（管理、ネットワークへの統合）を備える一方で、 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。ASA リングは、ASA 5580 および ASA 5585-X でサポートされます。 スタ内のすべてのユニットが同一モデル、同一ハードウェア仕 とが必要です。クラスタリングがイネーブルのときにサポート 能のリストについては、コンフィギュレーション ガイドを参 さい。 次のコマンドを導入または変更しました。**channel-group**、**cla** **system-mac**、**clear cluster info**、**clear configure cluster**、**cluster c** **group**、**cluster interface-mode**、**cluster-interface**、**conn-rebalan** **console-replicate**、**cluster master unit**、**cluster remove unit**、**del** **debug lacp cluster**、**enable**（クラスタ グループ）、**health-che** **address**、**ipv6 address**、**key**（クラスタ グループ）、**local-unit**、 （インターフェイス）、**mac-address pool**、**mtu cluster**、**port-** **span-cluster**、**priority**（クラスタ グループ）、**prompt cluster-** **asp cluster counter**、**show asp table cluster chash-table**、**show cl** **cluster info**、**show cluster user-identity**、**show lacp cluster**、**sho** **running-config cluster** 次の画面が導入または変更されました。 [Home] > [Device Dashboard] [Home] > [Cluster Dashboard][Home] > [Cluster Firewall Dashboar **[Configuration] > [Device Management] > [Advanced] > [Addre** **[MAC Address Pools]** **[Configuration] > [Device Management] > [High Availability and** **> [ASA Cluster]** **Configuration > Device Management > Logging > Syslog Setup >** **[Configuration] > [Device Setup] > [Interfaces]> [Add/Edit Inter** **[Advanced]** **[Configuration] > [Device Setup] > [Interfaces]> [Add/Edit Interf** **[Configuration] > [Device Setup] > [Interfaces] > [Add/Edit Ethe** **Interface] > [Advanced]** **[Configuration] > [Firewall] > [Advanced] > [Per-Session NAT R** **[Monitoring] > [ASA Cluster][Monitoring] > [Properties] > [Syste** **Graphs] > [Cluster Control Link]** **[Tools] > [Preferences] > [General]** **[Tools] > [System Reload]** **[Tools] > [Upgrade Software from Local Computer]**

機能	説明
	[Wizards] > [High Availability and Scalability Wizard] **[Wizards] > [Packet Capture Wizard]** **[Wizards] > [Startup Wizard]**
クラスタリングに対する OSPF、EIGRP、マルチキャスト	OSPFv2 および OSPFv3 の場合は、バルク同期、ルート同期 ンド EtherChannel がクラスタリング環境でサポートされま EIGRP の場合は、バルク同期、ルート同期、およびスパン がクラスタリング環境でサポートされます。 マルチキャスト ルーティングは、クラスタリングをサポー **show route cluster**、**debug route cluster**、**show mfib cluster**、 **cluster** の各コマンドが導入または変更されました。
クラスタリングのパケット キャプチャ	クラスタ全体のトラブルシューティングをサポートするに **capture** コマンドを使用してマスター ユニット上でのクラ フィックのキャプチャをイネーブルにします。これで、ク てのスレーブ ユニットでも自動的にイネーブルになりま キーワードは新しいキーワードであり、**capture** コマンド ラスタ全体のキャプチャがイネーブルになります。 **capture**、**show capture** の各コマンドが変更されました。 次の画面が変更されました。[Wizards] > [Packet Capture Wi
クラスタリングに対するロギング	クラスタ内の各ユニットは、syslog メッセージを個別に生成 **device-id** コマンドを使用すると、同一または異なるデバイ syslog メッセージを生成することができ、クラスタ内の同 ユニットからのメッセージのように見せることができます **logging device-id** コマンドが変更されました。 次の画面が変更されました。[Configuration] > [Logging] > [[Advanced] > [Advanced Syslog Configuration]
Cisco Nexus 7000 と Cisco Catalyst 6500 を使用するクラスタリングのサポート	ASA は、Cisco Nexus 7000 および Cisco Catalyst 6500（Super および 720-10GE）に接続するときにクラスタリングをサ

機能	説明
バルク同期中の接続複製レートの設定	ステートフル フェールオーバーを使用するときに、ASA で接 バイ装置に複製されるレートを設定できるようになりました。 では、接続は 15 秒間隔でスタンバイ装置に複製されます。た ク同期が発生すると（たとえば、フェールオーバーを最初に したときなど）、1 秒あたりの最大接続数の制限のために、大 同期するのに 15 秒では不十分な場合があります。たとえば、 大接続数を 800 万とします。800 万の接続を 15 秒間で複製す とは、1 秒あたり約 53.3 万の接続を作成するということです。 秒あたりに許可される最大接続数は 30 万です。複製レートが の最大接続数以下になるように指定できるようになり、同期期 の接続が同期されるまで調整されます。 **failover replication rate** *rate* コマンドが導入されました。 *8.4(4.1)* および *8.5(1.7)* でも使用可能です。
IPv6 の機能	
ASA の外部インターフェイスでの IPv6 サポート（VPN 機能用）。	このリリースの ASA では、外部インターフェイスへの IPv6 VP および IKEv2/IPsec プロトコルを使用）のサポートが追加され このリリースの ASA では、内部インターフェイスでの IPv6 VPN ク（SSL プロトコルを使用）がこれまでと同様にサポートされ リリースは、内部インターフェイス上での IKEv2/IPsec プロト しません。
IPv6 のためのリモート アクセス VPN のサポート：IPv6 アドレス割り当てポリシー	AnyConnect クライアントに IPv4 アドレスと IPv6 アドレスの一 方を割り当てるように ASA を設定できます。このようにする 上で内部的なアドレス プールを作成するか、ASA 上のローカ に専用アドレスを割り当てます。 エンドポイントに両方のタイプのアドレスを割り当てるには、 ントのオペレーティング システムの中でデュアル スタック プ 実装されている必要があります。 クライアントへの IPv6 アドレスの割り当ては、SSL プロトコ サポートされます。この機能は、IKEv2/IPsec プロトコルに対し トされません。 **ipv6-vpn-addr-assign**、**vpn-framed-ipv6-address** の各コマンドが した。 次の画面が変更されました。 **[Configuration] > [Remote Access VPN] > [Network (Client) Acces Assignment] > [Assignment Policy]** **[Configuration] > [Remote Access VPN] > [AAA/Local Users] > [> [(Edit local user account)] > [VPN Policy]**

機能	説明
IPv6 のためのリモート アクセス VPN のサポート：IPv6 アドレスを使用する DNS サーバのグループ ポリシーへの割り当て	DNS サーバを、ASA のネットワーク（クライアント）アクプ ポリシー内で定義できます。最大 4 個の DNS サーバ ア個の IPv4 アドレスと最大 2 個の IPv6 アドレス）を指定で IPv6 アドレスを持つ DNS サーバに VPN クライアントから は、SSL プロトコルを使用するようにクライアントが設定です。この機能は、IKEv2/IPsec プロトコルを使用するよクライアントではサポートされていません。 **dns-server value** コマンドが変更されました。 次の画面が変更されました。[Configuration] > [Remote Access (Client) Access] > [Group Policies] > [(Edit group policy)] > [Se
IPv6 のためのリモート アクセス VPN のサポート：スプリット トンネリング	スプリット トンネリングを使用すると、一部のネットワークを VPN トンネルを介して（暗号化あり）ルーティング ネットワーク トラフィックを VPN トンネルの外部で（「つまりクリア テキストとして）ルーティングすることがで ネットワーク トラフィックに対してスプリット トンネリるようになりました。このようにするには、IPv6 ポリシー中で統合アクセス コントロール ルールを指定します。 IPv6 スプリット トンネリングは、Smart Call Home 機能に るテレメトリ データで報告されます。IPv4 または IPv6 のリット トンネリングが有効になっている場合、Smart Call のスプリット トンネリングは「有効」と報告されます。タの場合、VPN セッション データベースは、通常はセッ 告される IPv6 データを表示します。 SSL プロトコルを使用するように設定された VPN クライ「トンネル」について、IPv6 トラフィックを含めるか除外 きます。この機能は、IKEv2/IPsec プロトコルに対しては せん。 **ipv6-split-tunnel-policy** コマンドが導入されました。 次の画面が変更されました。[Configuration] > [Remote Access (Client) Access] > [Group Policies] > [(Edit group policy)] > [A Tunneling]

機能	説明
IPv6 のためのリモート アクセス VPN のサポート：AnyConnect クライアントのファイアウォール ルール	クライアント ファイアウォール用のアクセス コントロール ルと IPv6 の両方のアドレスのアクセス リスト エントリをサポー IPv6 アドレスが含まれている ACL は、SSL プロトコルを使用設定されたクライアントに適用できます。この機能は、IKEvトコルに対してはサポートされません。 **anyconnect firewall-rule** コマンドが変更されました。 次の画面が変更されました。[Configuration] > [Remote Access VP(Client) Access] > [Group Policies] > [(Edit group policy)] > [Adva[AnyConnect Client] > [Client Firewall]
IPv6 のためのリモート アクセス VPN のサポート：クライアント プロトコル バイパス	クライアント プロトコル バイパス機能を使用すると、ASA がフィックだけを予期しているときの IPv4 トラフィックの管理トラフィックだけを予期しているときの IPv6 トラフィックの設定することができます。 AnyConnect クライアントが ASA に VPN 接続するときに、AS IPv6 の一方または両方のアドレスを割り当てます。ASA が A続に IPv4 アドレスまたは IPv6 アドレスだけを割り当てた場合IP アドレスを割り当てなかったネットワーク トラフィックにライアント プロトコル バイパスによってそのトラフィックをせるか、または ASA をバイパスしてクライアントからの暗号まり「クリア テキスト」としての送信を許可するかを設定でなりました。 たとえば、IPv4 アドレスのみ AnyConnect 接続に割り当てられイントがデュアル スタックされていると想定してください。ポイントが IPv6 アドレスへの到達を試みたときに、クライアス プロトコル機能がディセーブルの場合は、IPv6 トラフィップされますが、クライアント バイパス プロトコルがイネーブルIPv6 トラフィックはクライアントからクリア テキストとしてす。 この機能は、クライアントが SSL と IKEv2/IPsec プロトコルの用するように設定されていても使用できます。 **client-bypass-protocol** コマンドが導入されました。 次の画面が変更されました。[Configuration] > [Remote Access VP(Client) Access] > [Group Policies] > [(Group Policy) Advanced] > Client] > [Client Bypass Protocol]

機能	説明
IPv6 のためのリモート アクセス VPN のサポート：IPv6 インターフェイス ID とプレフィックス	ローカル VPN ユーザーに対して専用の IPv6 アドレスを指 なりました。 この機能の利点を活用できるのは、ユーザーが SSL プロト るように設定されている場合です。この機能は、IKEv2/IP に対してはサポートされません。 **vpn-framed-ipv6-address** コマンドが導入されました。 次の画面が変更されました。[Configuration] > [Remote Acce [AAA/Local Users] > [Local Users] > [(Edit User)] > [VPN Poli
IPv6 のためのリモート アクセス VPN のサポート：ASA FQDN の AnyConnect クライアントへの送信	AnyConnect クライアントに ASA の FQDN を返すことがで は、ロード バランシングおよびセッション ローミングに行 この機能は、クライアントが SSL と IKEv2/IPsec プロトコ 用するように設定されていても使用できます。 **gateway-fqdn** コマンドが導入されました。 次の画面が変更されました。[Configuration] > [Remote Access (Client) Access] > [Group Policies] > [(Edit group policy)] > [A [AnyConnect]
IPv6 のためのリモート アクセス VPN のサポート：ASA VPN ロード バランシング	IPv6 アドレスを持つクライアントは、AnyConnect 接続を行 クラスタのパブリック向け IPv6 アドレスを経由すること を経由することもできます。同様に、IPv6 アドレスを持つ は、AnyConnect VPN 接続を行うときに、ASA クラスタの IPv4 アドレスを経由することも、GSS サーバを経由するこ どちらのタイプの接続も ASA クラスタ内でロード バラン す。 IPv6 アドレスを持つクライアントが ASA のパブリック向 に接続できるようにするには、IPv6 から IPv4 へのネット 変換を実行できるデバイスがネットワーク上に存在する必 この機能は、クライアントが SSL と IKEv2/IPsec プロトコ 用するように設定されていても使用できます。 **show run vpn load-balancing** コマンドが変更されました。 次の画面が変更されました。[Configuration] > [Remote Acce Balancing]

機能	説明
IPv6 のためのリモート アクセス VPN のサポート：動的アクセス ポリシーが IPv6 属性をサポート	ASA 9.0 以降を ASDM 6.8 以降とともに使用するときに、次のナミック アクセス ポリシー（DAP）の一部として指定できるました。 • IPv6 アドレス（Cisco AAA 属性として） • IPv6 TCP および UDP ポート（デバイスのエンドポイントとして） • ネットワーク ACL フィルタ（クライアント） この機能は、クライアントが SSL と IKEv2/IPsec プロトコルの用するように設定されていても使用できます。 次の画面が変更されました。 **[Configuration] > [Remote Access VPN] > [Network (Client) Ac [Dynamic Access Policies] > [Add] > [Cisco AAA attribute]** **[Configuration] > [Remote Access VPN] > [Network (Client) Ac [Dynamic Access Policies] > [Add] > [Device] > [Add Endpoint A** **[Configuration] > [Remote Access VPN] > [Network (Client) Ac [Dynamic Access Policies] > [Network ACL Filters (client)]** **[Configuration] > [Remote Access VPN] > [Network (Client) Ac [Dynamic Access Policies] > [Webtype ACL Filters (clientless)]**
IPv6 のためのリモート アクセス VPN のサポート：セッション管理	セッション管理の出力の Public/Assigned アドレス フィールドレスが表示されるのは、AnyConnect 接続、サイトツーサイトおよびクライアントレス SSL VPN 接続の場合です。新しいフワードを追加して出力をフィルタリングし、IPv6（外部またはだけを表示することができます。IPv6 ユーザー フィルタに対ありません。 この機能を使用できるのは、クライアントが SSL プロトコルように設定されている場合です。この機能では、IKEv2/IPsec はサポートされません。 **show vpn-sessiondb** コマンドが変更されました。 次の画面が変更されました。[Monitoring] > [VPN] > [VPN Stat [Sessions]

機能	説明
IPv6 用の NAT のサポート	NAT が IPv6 トラフィックをサポートするようになり、IPv の変換（NAT64）もサポートされます。IPv4 と IPv6 の間の ンスペアレント モードではサポートされません。 **nat**（グローバルおよびオブジェクト ネットワーク コンフ ン モード）、**show conn**、**show nat**、**show nat pool**、**show x** ドが変更されました。 次の画面が変更されました。 **[Configuration] > [Firewall] > [Objects] > [Network Objects/** **[Configuration] > [Firewall] > [NAT Rules]**
DHCPv6 リレー	DHCP リレーが IPv6 に対してサポートされます。 **ipv6 dhcprelay server**、**ipv6 dhcprelay enable**、**ipv6 dhcprela** **config ipv6 dhcprelay**、**ipv6 nd managed-config-flag**、**ipv6 n** **other-config-flag**、**debug ipv6 dhcp**、**debug ipv6 dhcprelay**、 **dhcprelay binding**、**clear ipv6 dhcprelay binding**、**show ipv** **statistics**、**clear ipv6 dhcprelay statistics** の各コマンドが導入 次の画面が変更されました。[Configuration] > [Device Manag > [DHCP Relay]

機能	説明
OSPFv3	

機能	説明
	OSPFv3 ルーティングが IPv6 に対してサポートされます。OSPFv3に関する次の追加のガイドラインと制限事項に注意 クラスタ • OSPFv2 および OSPFv3 は、クラスタリングをサポー • クラスタリングが設定されているときは、OSPFv3 暗されません。クラスタリング環境で OSPFv3 暗号化を ると、エラー メッセージが表示されます。 • 個々のインターフェイスを使用するときに、必ずマス レーブ ユニットを OSPFv2 または OSPFv3 のネイバー す。 • 個々のインターフェイスを使用するときに、OSPFv2 できるのは、マスター ユニットの共有インターフェイ コンテキスト間のみです。スタティック ネイバーの設 されるのは、ポイントツーポイント リンク上のみです 1 つのインターフェイス上では 1 つのネイバー ステー 許可されます。 その他 • OSPFv2 および OSPFv3 は 1 つのインターフェイス上 タンスをサポートしています。 • ESP および AH プロトコルが OSPFv3 認証に対してサ す。 • OSPFv3 は非ペイロード暗号化をサポートします。 **ipv6 ospf cost**、**ipv6 ospf database-filter all out**、**ipv6 ospf d** **ipv6 ospf hello-interval**、**ipv6 ospf mtu-ignore**、**ipv6 ospf neig** **network**、**ipv6 ospf priority**、**ipv6 ospf retransmit-interval**、 **transmit-delay**、**ipv6 router ospf**、**ipv6 router ospf area**、**ip** **default**、**ipv6 router ospf default-information**、**ipv6 router o** **ipv6 router ospf exit**、**ipv6 router ospf ignore**、**ipv6 router o** **log-adjacency-changes**、**ipv6 router ospf no**、**ipv6 router osp** **ipv6 router ospf router-id**、**ipv6 router ospf summary-prefix** **ospf timers**、**area range**、**area virtual-link**、**default**、**defaul** **originate**、**distance**、**ignore lsa mospf**、**log-adjacency-changes** **router-id**、**summary-prefix**、**timers lsa arrival**、**timers paci** **pacing lsa-group**、**timers pacing retransmission**、**show ipv6** **ospf border-routers**、**show ipv6 ospf database-filter**、**show i** **flood-list**、**show ipv6 ospf interface**、**show ipv6 ospf neighbo** **ospf request-list**、**show ipv6 ospf retransmission-list**、**show i** **summary-prefix**、**show ipv6 ospf virtual-links**、**show ospf**、

機能	説明
	router、**clear ipv6 ospf**、**clear configure ipv6 router**、**debug osp** マンドが導入または変更されました。 次の画面が導入されました。 **[Configuration] > [Device Setup] > [Routing] > [OSPFv3] > [Set** **[Configuration] > [Device Setup] > [Routing] > [OSPFv3] > [Int** **[Configuration] > [Device Setup] > [Routing] > [OSPFv3] > [Red** **[Configuration] > [Device Setup] > [Routing] > [OSPFv3] > [Sum** **[Configuration] > [Device Setup] > [Routing] > [OSPFv3] > [Vir** **[Monitoring] > [Routing] > [OSPFv3 LSAs]** **[Monitoring] > [Routing] > [OSPFv3 Neighbors]**
IPv4 および IPv6 の統合 ACL	ACL で IPv4 および IPv6 アドレスがサポートされるようになり 信元および宛先に対して IPv4 および IPv6 アドレスの組み合わ きます。IPv6 固有の ACL は非推奨です。既存の IPv6 ACL は 移行されます。 IPv6 アドレスが含まれている ACL は、SSL プロトコルを使用 設定されたクライアントに適用できます。この機能は、IKEv トコルに対してはサポートされません。 次のコマンドが変更されました。**access-list extended**、**access-** **ipv6 access-list**、**ipv6 access-list webtype**、**ipv6-vpn-filter** の各コ 除されました。 次の画面が変更されました。 **[Configuration] > [Firewall] > [Access Rules]** **[Configuration] > [Remote Access VPN] > [Network（Client）Acc** **Policies] > [General] > [More Options]**
IPv4 および IPv6 の混合オブジェクト グループ	以前は、ネットワーク オブジェクト グループに含まれている て IPv4 アドレスであるか、すべて IPv6 アドレスでなければな した。現在では、ネットワーク オブジェクト グループが、IP 両方のアドレスの混合をサポートするようになりました。 （注） 混合オブジェクト グループを NAT に使用すること ん。 次のコマンドが変更されました。**object-group network-** 次の画面が変更されました。[Configuration] > [Firewall] > [Object Objects/Groups]

機能	説明
ネットワーク オブジェクトの IPv6 アドレスの範囲	ネットワーク オブジェクトの IPv6 アドレス範囲を設定でました。 次のコマンドが変更されました。**range-** 次の画面が変更されました。[Configuration] > [Firewall] > [Ob Objects/Groups]
IPv6 および NAT64 のインスペクションのサポート	IPv6 トラフィックの DNS インスペクションがサポートさました。 また、次のインスペクションについて、IPv4 と IPv6 の間トされます。 • DNS • FTP • HTTP • ICMP また、サポートされていないインスペクションが IPv6 トラ信してドロップしたときに syslog メッセージ（767001）をに、サービス ポリシーを設定できます。 **service-policy fail-close** コマンドが変更されました。 次の画面が変更されました。[Configuration] > [Firewall] > [Rules] > [Add Service Policy Rule Wizard - Service Policy]
リモート アクセス機能	
クライアントレス SSL VPN：追加サポート	次のブラウザ、オペレーティング システム、Web テクノロアプリケーションのサポートが追加されました。 **インターネット ブラウザのサポート**：Microsoft Internet Exp 4、5、6、7、および 8 **オペレーティング システムのサポート**：Mac OS X 10.7 **Web テクノロジーのサポート**：HTML 5 **アプリケーションのサポート**：SharePoint 2010
クライアントレス SSL VPN：リライタ エンジンの品質向上	クライアントレス SSL VPN リライタ エンジンの品質と有上しました。その結果、クライアントレス SSL VPN ユーザザー エクスペリエンスも向上が期待できます。 この機能に関して、追加または変更されたコマンドはあり この機能に関して、追加または変更された ASDM 画面はあ *8.4(4.1)* でも使用可能です。

機能	説明
クライアントレス SSL VPN：Citrix Mobile Receiver	これは、モバイル デバイス上で実行される Citrix Receiver アプ ンから XenApp および XenDesktop VDI サーバへの、ASA 経由 リモート アクセスを実現するための機能です。 ASA が Citrix Receiver と Citrix サーバとの間のプロキシとなる ユーザーが Citrix 仮想化リソースへの接続を試みるときに、C のアドレスとクレデンシャルの代わりに、ユーザーは ASA の アドレスとクレデンシャルを入力します。 **vdi** コマンドが変更されました。 次の画面が変更されました。[Configuration] > [Remote Access V [Clientless SSL VPN Access] > [Group Policy] > [Edit] > [More Op Access] > [Add VDI Server]
クライアントレス SSL VPN：拡張自動サインオン	この機能は、認証にダイナミック パラメータを必要とする Web ションのサポートを強化します。 次の画面が変更されました。[Configuration] > [Remote Access V [Clientless SSL VPN Access] > [Portal] > [Bookmarks]
クライアントレス SSL VPN：クライアントレス Java リライタ プロキシ サポート	この機能は、クライアントレス Java プラグインのためのプロ トを行います（クライアント マシンのブラウザでプロキシが いるとき）。 この機能に関して、追加または変更されたコマンドはありま この機能に関して、追加または変更された ASDM 画面はあり
クライアントレス SSL VPN：Remote File Explorer	Remote File Explorer は、企業ネットワークを Web ブラウザか するための機能です。ユーザーが Cisco SSL VPN ポータル ペー File System] アイコンをクリックすると、アプレットがユーザ で起動され、リモート ファイル システムがツリーとフォルダ されます。 この機能に関して、追加または変更されたコマンドはありま この機能に関して、追加または変更された ASDM 画面はあり
クライアントレス SSL VPN：サーバ証明書の検証	この機能は、クライアントレス SSL VPN のサポートを拡張しま ト HTTPS サイトの SSL サーバ証明書を、信頼済み CA 証明書 比較して検証することができます。 次のコマンドが変更されました。ssl-server-check、crypto、cry trustpool、crl、certificate、revocation-check 次の画面が変更されました。[Configuration] > [Remote Access V [Certificate Management] > [Trusted Certificate Pool]

機能	説明
AnyConnect のパフォーマンスの向上	この機能は、マルチコア プラットフォームでの AnyConne ラフィックのスループット パフォーマンスを高めます。こ データパスを高速化し、AnyConnect、スマート トンネル、 フォワーディングに関して、ユーザーが認識可能なパフォ 実現します。 **crypto engine accelerator-bias**、**show crypto accelerator** の各 更されました。 次の画面が変更されました。[Configuration] > [Remote Acce [Advanced] > [Crypto Engine]
カスタム属性	カスタム属性は、まだ ASDM に追加されていない AnyCon し、設定します。カスタム属性をグループ ポリシーに追加 の値を定義します。 AnyConnect 3.1 については、カスタム属性は、AnyConnect I をサポートするために使用できます。 カスタム属性の利点は、AnyConnect クライアントが IKEv2 どちらのプロトコルを使用するように設定されていても活 **anyconnect-custom-attr** コマンドが追加されました。 新しい画面が追加されました。[Configuration] > [Remote A [Network (Client) Access] > [Advanced] > [AnyConnect Custom

機能	説明
次世代暗号化	

機能	説明
	National Standards Association（NSA）は、暗号化強度に関 格に従うためにデバイスがサポートする必要がある、一連 リズムを定めています。RFC 6379 で Suite B 暗号化スイー います。NSA Suite B として定義されるアルゴリズムのセ 1 つの標準になりつつあるため、AnyConnect IPSec VPN（ よび公開キーインフラストラクチャ（PKI）サブシステム るようになりました。次世代暗号化（NGE）には、このセ なスーパーセットが含まれており、IPsec V3 VPN のための ズムが追加されるほか、IKEv2 に対する Diffie-Hellman グ 24、および DTLS と IKEv2 に対する RSA 証明書（4096 ビ 加されています。 次の機能は、Suite B のアルゴリズムをサポートするため れました。 • AES-GCM/GMAC のサポート（128、192、256 ビット • IKEv2 ペイロード暗号化と認証 • ESP パケット暗号化と認証 • マルチコア プラットフォームでのみサポートされ ウェア • SHA-2 サポート（256、384、512 ビット ハッシュ） • ESP パケット認証 • マルチコア プラットフォームでのみサポートされ ウェアおよびソフトウェア • ECDH サポート（グループ 19、20、および 21） • IKEv2 キー交換 • IKEv2 PFS • 単一またはマルチコアのプラットフォームでのみ ソフトウェア • ECDSA サポート（256、384、521 ビット楕円曲線） • IKEv2 ユーザー認証 • PKI 証明書登録 • PKI 証明書の生成および検証 • 単一またはマルチコアのプラットフォームでのみ ソフトウェア

機能	説明
	新しい暗号化アルゴリズムが IPsecV3 に対して追加されまし （注） Suite B のアルゴリズムをサポートするには、AnyC Premium ライセンスが IKEv2 リモート アクセス接 ですが、他の接続または目的（たとえば PKI）のた B を使用する場合は、制限はありません。IPsecV3 ンスに関する制限はありません。 **crypto ikev2 policy**、**crypto ipsec ikev2 ipsec-proposal**、**crypto ke crypto key zeroize**、**show crypto key mypubkey**、**show vpn-sessi** マンドが導入または変更されました。 次の画面が導入または変更されました。 **[Monitor] > [VPN] > [Sessions]** **[Monitor] > [VPN] > [Encryption Statistics]** **[Configuration] > [Site-to-Site VPN] > [Certificate Management Certificates]** **[Configuration] > [Site-to-Site VPN] > [Advanced] > [System Op** **[Configuration] > [Remote Access VPN] > [Network (Client) Ac [Advanced] > [IPsec] > [Crypto Maps]**
ASASM での VPN のサポート	ASASM は、すべての VPN 機能をサポートするようになりま
マルチ コンテキスト モード機能	
マルチ コンテキスト モードのサイトツーサイト VPN	サイトツーサイト VPN トンネルが、マルチ コンテキスト モー トされるようになりました。
サイトツーサイト VPN トンネルのための新しいリソース タイプ	新しいリソース タイプ vpn other と vpn burst other が作成され は、各コンテキストでのサイトツーサイト VPN トンネルの最 するためです。 **limit-resource**、**show resource types**、**show resource usage**、**sh allocation** の各コマンドが変更されました。 次の画面が変更されました。[Configuration] > [Context Manage [Resource Class] > [Add Resource Class]
セキュリティ コンテキストでのダイナミック ルーティング	EIGRP と OSPFv2 ダイナミック ルーティング プロトコルが、 テキスト モードでサポートされるようになりました。OSPFv3 びマルチキャスト ルーティングはサポートされません。

機能	説明
ルーティング テーブル エントリのための新しいリソース タイプ	新規リソース クラス routes が作成されました。これは、各のルーティング テーブル エントリの最大数を設定するため **limit-resource**、**show resource types**、**show resource usage**、**allocation** の各コマンドが変更されました。 次の画面が変更されました。[Configuration] > [Context Man [Resource Class] > [Add Resource Class]
マルチ コンテキスト モードのファイアウォール モードの混合がサポートされます。	セキュリティ コンテキスごとに個別のファイアウォール モきます。したがってその一部をトランスペアレント モード の他をルーテッド モードで実行することができます。 **firewall transparent** コマンドが変更されました。 ASDM ではファイアウォール モードを設定できません。コ インターフェイスを使用する必要があります。 バージョン *8.5(1)* でも使用可能です。
モジュール機能	
Cisco 7600 スイッチでの ASA サービス モジュールのサポート	Cisco 7600 シリーズは、ASASM をサポートするようになり のハードウェアとソフトウェアの要件については、次の U ください。 http://www.cisco.com/en/US/docs/security/asa/compatibility/asa

機能	説明
ASA CX SSP-10 と -20 に対する ASA 5585-X サポート	ASA CX モジュールを使用すると、特定の状況の完全なコンテ づいてセキュリティを強制することができます。このコンテキ ユーザーのアイデンティティ（誰が）、ユーザーがアクセスを アプリケーションまたはWebサイト（何を）、アクセス試行の こで）、アクセス試行の時間（いつ）、およびアクセスに使用 デバイスのプロパティ（どのように）が含まれます。ASA CX を使用すると、フローの完全なコンテキストを抽出して、細分 シーを適用することができます。たとえば、Facebook へのアク するが Facebook でのゲームへのアクセスは禁止する、あるい 密データベースへのアクセスを財務担当者に許可するが他の社 するといったことが可能です。 **capture**、**cxsc**、**cxsc auth-proxy**、**debug cxsc**、**hw-module mod** **password-reset**、**hw-module module reload**、**hw-module modul** **hw-module module shutdown**、**session do setup host ip**、**session do** **session do password-reset**、**show asp table classify domain cxsc**、 **table classify domain cxsc-auth-proxy**、**show capture**、**show con** **module**、**show service-policy** の各コマンドが導入または変更さ 次の画面が導入されました。 **[Home] > [ASA CX Status]** **[Wizards] > [Startup Wizard] > [ASA CX Basic Configuration]** **[Configuration] > [Firewall > Service Policy Rules] > [Add Service** **> [Rule Actions] > [ASA CX Inspection]** *8.4(4.1)* でも使用可能です。
SSP-10 および SSP-20 に対する ASA 5585-X デュアル SSP サポート（SSP-40 および SSP-60 に加えて）、デュアル SSP に対する VPN サポート	ASA 5585-X は、すべての SSP モデルでデュアル SSP をサポー になりました（同一シャーシ内で同じレベルの SSP を 2 つ使用て デュアル SSP を使用するときに VPN がサポートされるようにな 変更されたコマンドはありません。 変更された画面はありません。

バージョン 8.7 の新機能

ASA 8.7(1.1)/ASDM 6.7(1) の新機能

リリース：**2012年10月16日**

（注） バージョン 8.7(1) はビルドの問題により Cisco.com から削除されました。バージョン 8.7(1.1) またはそれ以降にアップグレードしてください。

機能	説明
プラットフォーム機能	
ASA 1000V のサポート	Nexus 1000V スイッチと ASA 1000V のサポートが導入されました。
ASA 1000V のクローニング	VM のクローニングを使用して、現在の配置に ASA 1000V のインスタン加できます。
管理機能	
ASDM モード	ASA 用の単一 GUI ベースのデバイス マネージャである Adaptive Security（ASDM）を使用して、ASA 1000V を設定、管理、およびモニタできま
VNMC モード	複数のテナント用の GUI ベースのマルチデバイス マネージャである Cisc Management Center（VNMC）を使用して、ASA 1000V を設定および管理
XML API	Cisco VNMC によって提供されるアプリケーション プログラムのインタ る XML API を使用して、ASA 1000V を設定および管理できます。この機 ドだけで使用できます。
ファイアウォール機能	
Cisco VNMC のアクセスと設定	Cisco VNMC のアクセスと設定では、セキュリティ プロファイルを作成 ます。ASDM で [Configuration] > [Device Setup] > [Interfaces] ペインを使用 へのアクセスを設定できます。Cisco VNMC にアクセスするには、ログイ とパスワード、ホスト名、および共有秘密を入力します。その後、セキュ イルおよびセキュリティプロファイルインターフェイスを設定します。 は、CLI を使用して、セキュリティ プロファイルを設定します。

機能	説明
セキュリティプロファイルとセキュリティプロファイル インターフェイス	セキュリティ プロファイルは、Cisco VNMC で設定され、Cisco Nexus 1000V 当てられたエッジ セキュリティ プロファイルに対応するインターフェイスで ラフィックのポリシーは、これらのインターフェイスと外部インターフェイ てられます。[Configuration] > [Device Setup] > [Interfaces] ペインを使用してセ プロファイルを追加できます。名前を追加し、サービス インターフェイスを とにより、セキュリティ プロファイルを作成します。ASDM は、Cisco VNM セキュリティ プロファイルを生成し、セキュリティ プロファイル ID を割り 自動的に一意のインターフェイスの名前を生成します。インターフェイス名 リティ ポリシー コンフィギュレーションで使用されます。 次のコマンドを導入または変更しました。**interface security-profile**、**security mtu**、**vpath path-mtu**、**clear interface security-profile**、**clear configure interfa security-profile**、**show interface security-profile**、**show running-config interfac security-profile**、**show interface ip brief**、**show running-config mtu**、**show vsn show vsn security-profile** 次の画面が導入または変更されました。 **[Configuration] > [Device Setup] > [Interfaces] [Configuration] > [Device Setup] > [Add Security Profile] [Monitoring] > [Interfaces] > [Security Profiles]**
サービスインターフェイス	サービスインターフェイスは、セキュリティ プロファイルインターフェイス られたイーサネット インターフェイスです。内部インターフェイスであるこ サービス インターフェイスを 1 つだけ設定できます。 コマンド **service-interface security-profile all** が導入されました。 次の画面が変更されました。[Configuration] > [Device Setup] > [Interfaces]
VNMC ポリシー エージェント	VNMC ポリシー エージェントは ASDM および VNMC モードの両方でポリシ ネーブルにします。HTTPS 経由で Cisco VNMC から XML ベースの要求を受 1000V 設定に変換する Web サーバが含まれます。 次のコマンドが導入されました。**vnmc policy-agent**、**login**、**shared-secret**、**r host**、**vnmc org**、**show vnmc policy-agent**、**show running-config vnmc policy-a configure vnmc policy-agent** 次の画面が変更されました。[Configuration] > [Device Setup] > [Interfaces]

バージョン 8.6 の新機能

ASA 8.6(1)/ASDM 6.6(1) の新機能

リリース：**2012 年 2 月 28 日**

（注） この ASA ソフトウェア バージョンは、ASA 5512-X、ASA 5515-X、ASA 5525-X、ASA 5545-X、および ASA 5555-X でのみサポートされます。

バージョン 8.6(1) には、8.4(2) のすべての機能と、この表に表示されている機能が含まれています。

8.4(3) で追加された機能は、この表で明示されていない限り、8.6(1) には含まれていません。

機能	説明
ハードウェアの機能	
ASA 5512-X ～ ASA 5555-X のサポート	ASA 5512-X、ASA 5515-X、ASA 5525-X、ASA 5545-X、および ASA 555 が導入されました。
IPS 機能	
ASA 5512-X ～ ASA 5555-X に対する IPS SSP のサポート	ASA 5512-X、ASA 5515-X、ASA 5525-X、ASA 5545-X、および ASA 5555 SSP ソフトウェア モジュールのサポートが導入されました。 **session**、**show module**、**sw-module** の各コマンドが導入または変更されま 変更された画面はありません。
リモート アクセス機能	
ブラウザでのクライアントレス SSL VPN のサポート	ASA は、Microsoft Internet Explorer 9 および Firefox 4 を使用してクライア VPN をサポートするようになりました。 バージョン *8.4(3)* でも使用可能です。

機能	説明
DTLS および TLS における圧縮	スループットを向上させるため、シスコは AnyConnect 3.0 以降で DTLS と T サポートするようになりました。各トンネリング メソッドは個別に圧縮を構 優先設定は SSL と DTLS の両方の圧縮を LZS とすることです。この機能は、 クライアントからの移行を強化します。 （注） 高圧縮データを渡す高速リモート アクセス接続でデータ圧縮を使 は、ASA にかなりの処理能力が要求されます。ASA で他の活動や クがあると、プラットフォームでサポートできるセッションの数に 次のコマンドを導入または変更しました。**anyconnect dtls compression** [**lzs** | **n** **anyconnect ssl compression** [**deflate** | **lzs** | **none**] 次の画面が変更されました。[Configuration] > [Remote Access VPN] > [Clientle Access] > [Group Policies] > [Edit] > [Edit Internal Group Policy] > [Advanced] > [Client] > [SSL Compression] バージョン *8.4(3)* でも使用可能です。
クライアントレス SSL VPN セッションタイムアウトアラート	ユーザーの VPN セッションが、無活動またはセッションタイムアウトにより とをユーザーに警告するカスタム メッセージを作成できます。 次のコマンドが導入されました。**vpn-session-timeout alert-interval**、**vpn-idle** **alert-interval** 次の画面が導入されました。 [Remote Access VPN] > [Configuration] > [Clientless SSL VPN Access] > [Portal] [Customizations] > [Add/Edit] > [Timeout Alerts] [Remote Access VPN] > [Configu [Clientless SSL VPN Access] > [Group Policies] > [Add/Edit General] バージョン *8.4(3)* でも使用可能です。
マルチ コンテキスト モード機能	

機能	説明
MAC アドレス プレフィックスの自動生成	マルチ コンテキスト モードで、ASA が MAC アドレス自動生成のコンフ ンを変換し、デフォルトのプレフィックスを使用できるようになりまし ンターフェイスの MAC アドレスの最後の 2 バイトに基づいてプレフィッ します。この変換は、リロード時または MAC アドレス生成を再度イネー 自動的に行われます。生成のプレフィックス方式は、セグメント上で一意 スがより適切に保証されるなど、多くの利点をもたらします。**show runn** **mac-address** コマンドを入力して、自動生成されたプレフィックスを表示 フィックスを変更する場合、カスタム プレフィックスによって機能を再 MAC アドレス生成の従来の方法は使用できなくなります。 （注） フェールオーバー ペアのヒットレス アップグレードを維持す は、フェールオーバーが有効である場合、既存のコンフィギ MAC アドレス メソッドをリロード時に変換しません。ただし フィックス方式に手動で変更することを強く推奨します。ア に、MAC アドレス生成のプレフィックス方式を使用するには、 プレフィックスを使用する MAC アドレス生成を再びイネーブ **mac-address auto** コマンドが変更されました。 次の画面が変更されました。[Configuration] > [Context Management] > [Sec
AAA 機能	
属性あたりの最大 LDAP 値が増加	単一の属性に対して ASA が受け取ることができる値の最大数は、1000（ ら 5000 に増やされました。許可される範囲は 500 ～ 5000 です。設定され た応答メッセージを受信した場合、ASA は認証を拒否します。ASA が、 を持つ単一の属性を検出した場合、ASA は情報 syslog 109036 を生成しま を超える場合、ASA はエラー レベル syslog 109037 を生成します。 次のコマンドが導入されました。**ldap-max-value-range** *number*（このコマ ホスト設定モードで入力します）。 ASDM ではこのコマンドはサポートされません。コマンドライン ツール ンドを入力してください。 バージョン *8.4(3)* でも使用可能です。
LDAP 検索結果の下位範囲のサポート	サーバ設定に応じて、LDAP 検索が多数の値を持つ属性という結果になる ブ範囲を返し、ASA が残りの値範囲に対して追加のクエリを開始するこ とがあります。ASA は残りの範囲に対して複数のクエリを行い、応答を 配列に結合するようになりました。 バージョン *8.4(3)* でも使用可能です。
トラブルシューティング機能	

機能	説明
show asp table classifier および **show asp table filter** コマンドの正規表現照合	出力をフィルタするために、**show asp table classifier** と **show asp table filter** コ規表現を使用して入力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。**show asp table classifier match** *regex*、**show a match** *regex* ASDM ではこのコマンドはサポートされません。コマンドライン ツールを使ンドを入力してください。 バージョン *8.4(3)* でも使用可能です。

バージョン 8.5 の新機能

ASA 8.5(1.7)/ASDM 6.5(1.101) の新機能

リリース：**2012年3月5日**

（注） 解決される特定の問題がある場合にだけ、Cisco.com にポストされた ASA 暫定リリースにアップグレードすることを推奨します。実稼働環境で暫定リリースを実行する場合は、暫定リリースでは対象のテストだけが実行されることに注意してください。暫定リリースは、TAC Web サイトによって十分にサポートされ、通常、次のメンテナンス リリースが使用可能になるまでの期間だけダウンロード サイトに残されます。暫定リリースを実行することを選択した場合、使用可能になったときに、完全にテストされたメンテナンス リリース、または機能リリースにアップグレードすることを強く推奨します。

次のメンテナンスまたは機能リリースの時点で暫定リリース機能についてマニュアルを作成します。各 ASA 暫定リリースの解決済みの警告のリストについては、Cisco.com のソフトウェア ダウンロード サイトから入手可能な暫定リリース ノートを参照してください。

表 1 : ASA 暫定バージョン 8.5(1.7)/ASDM バージョン 6.5(1.101)

機能	説明
ハードウェアの機能	
Catalyst 6500 スーパーバイザ 2T のサポート	ASA は、現在、Catalyst 6500 スーパーバイザ 2T と相互運用できます。ハードフトウェアの互換性については、次の URL を参照してください。 http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrx.html （注） ASA の FPD イメージのアップグレードが必要なことがあります。ノートのアップグレードの手順を参照してください。
マルチ コンテキスト機能	

機能	説明
MAC アドレス プレフィックスの自動生成の ASDM サポート	ASDM は、プレフィックスを指定していない場合に自動生成されたプレ用されることを表示するようになりました。 次の画面が変更されました。[Configuration] > [Context Management] > [Sec
フェールオーバー機能	
バルク同期中の接続複製レートの設定	ステートフル フェールオーバーを使用するときに、ASA で接続がスタンされるレートを設定できるようになりました。デフォルトでは、接続はンバイ装置に複製されます。ただし、バルク同期が発生すると（たとえばバーを最初にイネーブルにしたときなど）、1 秒あたりの最大接続数の制量の接続を同期するのに 15 秒では不十分な場合があります。たとえば、続数を 800 万とします。800 万の接続を 15 秒間で複製するということは53.3 万の接続を作成するということです。しかし、1 秒あたりに許可され30 万です。複製レートが 1 秒あたりの最大接続数以下になるように指定り、同期期間はすべての接続が同期されるまで調整されます。 **failover replication rate** *rate* コマンドが導入されました。 次の画面が変更されました。[Configuration] > [Device Management] > [High [Failover]

ASA 8.5(1.6)/ASDM 6.5(1) の新機能

リリース：**2012年1月27日**

（注） 解決される特定の問題がある場合にだけ、Cisco.com にポストされた ASA 暫定リリースにアップグレードすることを推奨します。実稼働環境で暫定リリースを実行する場合は、暫定リリースでは対象のテストだけが実行されることに注意してください。暫定リリースは、TAC Web サイトによって十分にサポートされ、通常、次のメンテナンス リリースが使用可能になるまでの期間だけダウンロードサイトに残されます。暫定リリースを実行することを選択した場合、使用可能になったときに、完全にテストされたメンテナンス リリース、または機能リリースにアップグレードすることを強く推奨します。

次のメンテナンスまたは機能リリースの時点で暫定リリース機能についてマニュアルを作成します。各 ASA 暫定リリースの解決済みの警告のリストについては、Cisco.com のソフトウェア ダウンロード サイトから入手可能な暫定リリース ノートを参照してください。

表 *2 : ASA* 暫定バージョン *8.5(1.6)/ASDM* バージョン *6.5(1)*

機能	説明
マルチ コンテキスト機能	

機能	説明
MAC アドレス プレフィックスの自動生成	マルチ コンテキスト モードで、ASA が MAC アドレス自動生成のコンフィギ ンを変換し、デフォルトのプレフィックスを使用できるようになりました。A クプレーンのMACアドレスの最後の2バイトに基づいてプレフィックスを自 す。この変換は、リロード時またはMACアドレス生成を再度イネーブルにす 的に行われます。生成のプレフィックス方式は、セグメント上で一意のMAC より適切に保証されるなど、多くの利点をもたらします。**show running-config** コマンドを入力して、自動生成されたプレフィックスを表示できます。プレ を変更する場合、カスタムプレフィックスによって機能を再設定できます。 ス生成の従来の方法は使用できなくなります。 （注） フェールオーバー ペアのヒットレス アップグレードを維持するた は、フェールオーバーが有効である場合、既存のコンフィギュレ MACアドレスメソッドをリロード時に変換しません。ただし、フ バーを使用するときは、プレフィックスによる生成方式に手動で とを強く推奨します。プレフィックスメソッドを使用しない場合 ロット番号にインストールされた ASASM では、フェールオーバ た場合に MAC アドレスの変更が行われ、トラフィックの中断が とがあります。アップグレード後に、MACアドレス生成のプレフ 式を使用するには、デフォルトのプレフィックスを使用する MA 生成を再びイネーブルにします。 **mac-address auto** コマンドが変更されました。 ASDM は変更されませんでした。

ASA 8.5(1)/ASDM 6.5(1) の新機能

リリース：2011年7月8日

この ASA および ASDM ソフトウェア バージョンは ASASM 上でのみサポートされます。

バージョン 8.5(1) には、8.4(1) のすべての機能と、この表に表示されている機能が含まれています。ただし、次の機能はペイロード暗号化なしのソフトウェアではサポートされず、このリリースは、ペイロード暗号化機能なしのリリースとしてだけ使用できます。

- VPN
- ユニファイド コミュニケーション

8.4(2) で追加された機能は、この表で明示されていない限り、8.5(1) には含まれていません。

表 3 : ASA バージョン 8.5(1)/ASDM バージョン 6.5(1) の新機能

機能	説明
ハードウェアの機能	

機能	説明
ASA サービス モジュールのサポート	Cisco Catalyst 6500 E スイッチに ASASM のサポートが導入されました。
ファイアウォール機能	
マルチ コンテキスト モードのファイアウォール モードの混合がサポートされます。	セキュリティ コンテキスごとに個別のファイアウォール モードを設定でがってその一部をトランスペアレント モードで実行し、その他をルーテ行することができます。 **firewall transparent** コマンドが変更されました。 ASDM ではファイアウォール モードを設定できません。コマンドラインスを使用する必要があります。
インターフェイス機能	
MACアドレスの自動生成がマルチ コンテキスト モードで、デフォルトでイネーブルになる	MAC アドレスの自動生成は、マルチ コンテキスト モードで、デフォルになりました。 **mac address auto** コマンドが変更されました。 次の画面が変更されました。[System] > [Configuration] > [Context Managen Contexts]
NAT の機能	

機能	説明
アイデンティティ NAT の設定が可能なプロキシ ARP およびルート ルックアップ	アイデンティティ NAT の以前のリリースでは、プロキシ ARP はディセーブ 出力インターフェイスの決定には常にルート ルックアップが使用されてい らを設定することはできませんでした。8.4(2) 以降、アイデンティティ NAT ト動作は他のスタティック NAT コンフィギュレーションの動作に一致する れました。これにより、デフォルトでプロキシ ARP はイネーブルにされ、N ギュレーションにより出力インターフェイスが決定されるようになりました ている場合）。これらの設定をそのまま残すこともできますし、個別にイネ はディセーブルにすることもできます。通常のスタティック NAT のプロキシ セーブルにすることもできるようになっています。 8.3 よりも前の設定の場合、8.4(2) 以降への NAT 免除ルール（**nat 0 access-lis** の移行には、プロキシ ARP をディセーブルにするキーワード **no-proxy-arp** お ルックアップを使用するキーワード **route-lookup** があります。8.3(2) および 行に使用された **unidirectional** キーワードは、移行に使用されなくなりまし 8.3(2)、8.4(1) から 8.4(2) にアップグレードすると、既存機能を保持するため アイデンティティ NAT コンフィギュレーションに **no-proxy-arp** キーワードと キーワードが含まれるようになっています。**unidirectional** キーワードは削除 **nat static** [**no-proxy-arp**] [**route-lookup**]（オブジェクト ネットワーク）、およ **static** [**no-proxy-arp**] [**route-lookup**]（グローバル）コマンドが変更されまし 次の画面が変更されました。 [Configuration] > [Firewall] > [NAT Rules] > [Add/Edit Network Object] > [Advanc Settings] [Configuration] > [Firewall] > [NAT Rules] > [Add/Edit NAT Rule] バージョン *8.4(2)* でも使用可能です。
PAT プールおよびラウンドロビン アドレス割り当て	1 つのアドレスの代わりに、PAT アドレスのプールを指定できるようになり た、オプションで、PAT アドレスのすべてのポートを使用してからプール内 レスを使用するのではなく、PAT アドレスのラウンドロビン割り当てをイネ ることもできます。これらの機能は、1 つの PAT アドレスで多数の接続を行 合にそれが DoS 攻撃の対象となることを防止するのに役立ちます。またこの機 多数の PAT アドレスを簡単に設定できます。 （注） 現在の 8.5(1) では、PAT プール機能をダイナミック NAT または PA ルバック方式として使用することはできません。PAT プールは、 ク PAT のプライマリ方式（CSCtq20634）としてのみ設定できます **nat dynamic** [**pat-pool** *mapped_object* [**round-robin**]]（オブジェクト ネットワー び **nat source dynamic** [**pat-pool** *mapped_object* [**round-robin**]]（グローバル）コ 更されました。 次の画面が変更されました。 [Configuration] > [Firewall] > [NAT Rules] > [Add/Edit Network Object] [Configuratio > [NAT Rules] > [Add/Edit NAT Rule] バージョン *8.4(2)* でも使用可能です。

機能	説明
スイッチ統合機能	
自動ステート	スイッチのスーパーバイザ エンジンは、ASA VLAN に関連付けられてい フェイスのステータスに関して、自動ステート メッセージを ASASM に たとえば、VLANに関連付けられているすべての物理インターフェイスが 自動ステートメッセージにより、VLANがダウンしていることがASAに ASA では、この情報を受けて、VLAN をダウンとして宣言し、いずれの が発生しているかを判別するために通常必要となるインターフェイス モ トをバイパスできます。自動ステートメッセージングにより、ASA がリ するのに要する時間が大幅に短縮されます（自動ステートがサポートさ の最長 45 秒と比較すると、数ミリ秒も短縮されます）。 （注） スイッチで自動ステートメッセージングがサポートされるの 1 つの ASA を搭載した場合だけです。 次の Cisco IOS コマンドを参照してください。**firewall autostate**。
仮想スイッチングシステム	ASASM は、スイッチに設定された場合に VSS をサポートします。ASA ません。

バージョン 8.4 の新機能

ASA 8.4(7)/ASDM 7.1(3) の新機能

リリース：**2013年9月3日**

ASA 8.4(7)/ASDM 7.1(3) には新機能はありませんでした。

ASA 8.4(6)/ASDM 7.1(2.102) の新機能

リリース：**2013年4月29日**

機能	説明
モニタリング機能	

機能	説明
メモリの上位10ユーザーの表示機能	上位割り当て済み bin サイズと割り当て済みの bin サイズごとの上位 10 PC を とができます。以前は、この情報を見るためには、複数のコマンド（**show m** コマンドと **show memory binsize** コマンド）の入力が必要でした。新しいコ り、メモリの問題の迅速な分析が可能です。 次のコマンドが導入されました。**show memory top-usage** ASDM の変更はありません。 この機能は、*8.5*（*1*）、*8.6*（*1*）、*8.7*（*1*）、*9.0*（*1*）、*9.1*（*1*）では、利用で
CPUプロファイルの拡張機能	**cpu profile activate** コマンドが、以下をサポートするようになりました。 • トリガーされるまでのプロファイラの開始の遅延（グローバルまたは特 CPU%） • シングル スレッドのサンプリング 次のコマンドが変更されました。**cpu profile activate** [*n-samples*] [**sample-proc** *process-name*] [**trigger cpu-usage** *cpu%* [*process-name*] ASDM の変更はありません。 この機能は、*8.5*（*1*）、*8.6*（*1*）、*8.7*（*1*）、*9.0*（*1*）、*9.1*（*1*）では、利用で
リモート アクセス機能	
user-storage value コマンドのパスワードの **show** コマンドでの暗号化	**show running-config** コマンドを入力すると、**user-storage value** コマンドのパ 暗号化されます。 次のコマンドが変更されました。**user-storage value** 次の画面が変更されました。[Configuration] > [Remote Access VPN] > [Clientle Access] > [Group Policies] > [More Options] > [Session Settings] この機能は、*8.5*（*1*）、*8.6*（*1*）、*8.7*（*1*）、*9.0*（*1*）、*9.1*（*1*）では、利用で

ASA 8.4(5)/ASDM 7.0(2) の新機能

リリース：2012年10月31日

機能	説明
ファイアウォール機能	

機能	説明
EtherType ACL による IS-IS トラフィック（トランスペアレントファイアウォールモード）のサポート	トランスペアレント ファイアウォール モードでは、ASA が EtherType AC IS-IS トラフィックを渡すことができるようになりました。 **access-list ethertype** {**permit** | **deny**} **is-is** コマンドが変更されました。 次の画面が変更されました。[Configuration] > [Device Management] > [Mar > [EtherType Rules] この機能は、*8.5*（*1*）、*8.6*（*1*）、*8.7*（*1*）、*9.0*（*1*）、*9.1*（*1*）では、利
間接接続されたサブネットの ARP キャッシュの追加	ASA ARP キャッシュには、直接接続されたサブネットからのエントリだ で含まれています。また、ARP キャッシュに間接接続されたサブネット できるようになりました。セキュリティ リスクを認識していない場合は ネーブルにすることは推奨しません。この機能は、ASA に対するサービ 攻撃を助長する場合があります。任意のインターフェイスのユーザが大量 送信して、偽エントリで ASA ARP テーブルがあふれる可能性があります 次の機能を使用する場合は、この機能を使用する必要がある可能性があり • セカンデリ サブネット。 • トラフィック転送の隣接ルートのプロキシ ARP。 **arp permit-nonconnected** コマンドが導入されました。 次の画面が変更されました。[Configuration] > [Device Management] > [Adv [ARP Static Table] この機能は、*8.5(1)*、*8.6(1)*、または *8.7(1)* では使用できません。
サービス ポリシー ルールの最大接続数の引き上げ	サービス ポリシー ルールの最大接続数が 65535 から 2000000 に引き上げ **set connection conn-max**、**set connection embryonic-conn-max**、**set connect per-client-embryonic-max**、**set connection per-client-max** の各コマンドが変 次の画面が変更されました。[Configuration] > [Firewall] > [Service Policy Rul Settings] この機能は、*8.5(1)*、*8.6(1)*、または *8.7(1)* では使用できません。
リモート アクセス機能	
ホストスキャンおよびASA相互運用性の改善	ホスト スキャンおよび ASA のプロセスが改善され、クライアントから A 属性が転送できます。つまり、クライアントとの VPN 接続を確立し、ダ セス ポリシーを適用するために、ASA はより長い時間を割くことができ この機能は、*8.5*（*1*）、*8.6*（*1*）、*8.7*（*1*）、*9.0*（*1*）、*9.1*（*1*）では、利

機能	説明
Cisco Secure Desktop：Windows 8 のサポート	CSD 3.6.6215 がアップデートされ、プリログイン ポリシーのオペレーティン のチェックで Windows 8 が選択できるようになりました。 次の制限事項を確認してください。 • Secure Desktop（Vault）は Windows 8 ではサポートされません。
Dynamic Access Policies：Windows 8 のサポート	ASDM がアップデートされ、DAP オペレーティング システム属性で Window きるようになりました。
モニタリング機能	
Xlate カウントへのポーリング可能にする NAT-MIB cnatAddrBindNumberOfEntries および cnatAddrBindSessionCount OID。	SNMP の xlate_count および max_xlate_count に、NAT-MIB cnatAddrBindNumb および cnatAddrBindSessionCount OID がサポートされるようになりました。 このデータは、**show xlate count** コマンドと同等です。 この機能は、*8.5（1）*、*8.6（1）*、*8.7（1）*、*9.0（1）*、*9.1（1）*では、利用
NSEL	フロートラフィックの定期的なバイトカウンタを提供するために flow-updat 導入されました。flow-update イベントが NetFlow コレクタに送信される時間 できます。flow-update レコードを送信するコレクタをフィルタリングできま 次のコマンドが導入されました。**flow-export active refresh-interval** 次のコマンドが変更されました。**flow-export event-type** 次の画面が変更されました。 [Configuration] > [Device Management] > [Logging] > [NetFlow] **[Configuration] > [Firewall] > [Service Policy Rules] > [Add Service Policy Rule Rule Actions] > [NetFlow] > [Add Flow Event]** この機能は、*8.5（1）*、*8.6（1）*、*8.7（1）*、*9.0（1）*、*9.1（1）*では、利用
ハードウェアの機能	
ASA 5585-X DC 電源サポート	ASA 5585-X DC 電源のサポートが追加されました。 この機能は、*8.5（1）*、*8.6（1）*、*8.7（1）*、*9.0（1）*、*9.1（1）*では、利用

ASA 8.4(4.5)/ASDM 6.4(9.103) の新機能

リリース：**2012年8月13日**

（注） バージョン 8.4(4.3) はビルドの問題により Cisco.com から削除されました。バージョン 8.4(4.5) またはそれ以降にアップグレードしてください。

解決される特定の問題がある場合にだけ、Cisco.com にポストされた暫定リリースにアップグレードすることを推奨します。実稼働環境で暫定リリースを実行する場合は、暫定リリースでは対象のテストだけが実行されることに注意してください。暫定リリースは、TAC Web サイトによって十分にサポートされ、次のメンテナンス リリースが使用可能になるまでの期間だけダウンロードサイトに残されます。暫定リリースを実行することを選択した場合、使用可能になったときに、完全にテストされたメンテナンス リリース、または機能リリースにアップグレードすることを強く推奨します。次のメンテナンスまたは機能リリースの時点で暫定リリース機能についてマニュアルを作成します。各暫定リリースの解決済みの警告のリストについては、Cisco.comのソフトウェア ダウンロードサイトから入手可能な暫定リリース ノートを参照してください。

機能	説明
ファイアウォール機能	
間接接続されたサブネットの ARP キャッシュの追加	ASA ARP キャッシュには、直接接続されたサブネットからのエントリだで含まれています。また、ARP キャッシュに間接接続されたサブネットできるようになりました。セキュリティ リスクを認識していない場合はネーブルにすることは推奨しません。この機能は、ASA に対するサービ攻撃を助長する場合があります。任意のインターフェイスのユーザが大量送信して、偽エントリで ASA ARP テーブルがあふれる可能性があります 次の機能を使用する場合は、この機能を使用する必要がある可能性があり • セカンデリ サブネット。 • トラフィック転送の隣接ルートのプロキシ ARP。 **arp permit-nonconnected** コマンドが導入されました。 次の画面が変更されました。[Configuration] > [Device Management] > [Adv [ARP Static Table] この機能は、*8.5(1)*、*8.6(1)*、または *8.7(1)* では使用できません。
モニタリング機能	

機能	説明
Xlate カウントへのポーリング可能にする NAT-MIB cnatAddrBindNumberOfEntries および cnatAddrBindSessionCount OID。	SNMP の xlate_count および max_xlate_count に、NAT-MIB cnatAddrBindNumb および cnatAddrBindSessionCount OID がサポートされるようになりました。 このデータは、**show xlate count** コマンドと同等です。 この機能は、*8.5（1）*、*8.6（1）*、*8.7（1）*、*9.0（1）*、*9.1（1）*では、利用

ASA 8.4(4.1)/ASDM 6.4(9) の新機能

リリース：2012年6月18日

（注） バージョン 8.4(4) はビルドの問題により Cisco.com から削除されました。バージョン 8.4(4.1) またはそれ以降にアップグレードしてください。

機能	説明
認定機能	
FIPS 認定および Common Criteria 認定	Cisco ASA 5500 シリーズのレベル 2 FIPS 140-2 検証の一部として、FIPS 140-2 リティ ポリシーが更新されました。Cisco ASA 5505、ASA 5510、ASA 5520、 ASA 5550、ASA 5580、および ASA 5585-X が対象です。 Common Criteria Evaluation Assurance Level 4（EAL4）が更新されました。こ Cisco ASA および VPN プラットフォーム ソリューションの特定の Target Of （TOE）の基準が提供されます。 この機能は、*8.5（1）*、*8.6（1）*、*8.7（1）*、*9.0（1）*、*9.0(2)*、*9.1(1)* では、 せん。
ローカルデータベースを使用する場合の管理者パスワードポリシーのサポート	ローカル データベースを使用して CLI または ASDM アクセスの認証を設定す 指定期間を過ぎるとユーザーにパスワードの変更を要求し、パスワードの最 変更文字数などのパスワード標準に従うことを要求するパスワード ポリシー ます。 次のコマンドを導入または変更しました。**change-password**、**password-polic** **password-policy minimum changes**、**password-policy minimum-length**、**passw** **minimum-lowercase**、**password-policy minimum-uppercase**、**password-policy** **minimum-numeric**、**password-policy minimum-special**、**password-policy authenti** **clear configure password-policy**、**show running-config password-policy** 次の画面が導入されました。[Configuration] > [Device Management] > [Users/AAA Policy] この機能は、*8.5（1）*、*8.6（1）*、*8.7（1）*、*9.0（1）*、*9.0(2)*、*9.1(1)* では、 せん。

機能	説明
SSH 公開キー認証のサポート	ASA への SSH 接続の公開キー認証は、最大 2048 ビットの Base64 キーをザー単位で有効に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。**ssh authenticaion**。 次の画面が導入されました。[Configuration] > [Device Management] > [User Accounts] > [Edit User Account] > [Public Key Authentication] この機能は、*8.5（1）*、*8.6（1）*、*8.7（1）*、*9.0（1）*、*9.0(2)*、*9.1(1)* でせん。
SSH キー交換の Diffie-Hellman グループ 14 のサポート	SSH キー交換に Diffie-Hellman グループ 14 が追加されました。これまでだけがサポートされていました。 次のコマンドが導入されました。**ssh key-exchange**。 次の画面が変更されました。[Configuration] > [Device Management] > [Man > [ASDM/HTTPS/Telnet/SSH] この機能は、*8.5（1）*、*8.6（1）*、*8.7（1）*、*9.0（1）*、*9.0(2)*、*9.1(1)* でせん。
管理セッションの最大数のサポート	同時 ASDM、SSH、Telnet セッションの最大数を設定できます。 次のコマンドが導入されました。**quota management-session**、**show runni management-session**、**show quota management-session**。 次の画面が導入されました。[Configuration] > [Device Management] > [Man > [Management Session Quota] この機能は、*8.5（1）*、*8.6（1）*、*8.7（1）*、*9.0（1）*、*9.0(2)*、*9.1(1)* でせん。

機能	説明
SSL 暗号化用の追加のエフェメラル Diffie-Hellman 暗号	ASA で次のエフェメラル Diffie-Hellman（DHE）SSL 暗号スイートがサポート になりました。 • DHE-AES128-SHA1 • DHE-AES256-SHA1 これらの暗号スイートは、RFC 3268『*Advanced Encryption Standard (AES) Cip* *Transport Layer Security (TLS)*』で指定されています。 DHE では完全転送秘密が提供されるため、クライアントでサポートされてい は推奨される暗号です。次の制限事項を確認してください。 • DHE は SSL 3.0 接続ではサポートされないため、SSL サーバの TLS 1.0 も にしてください。 `!! set server version` `ciscoasa(config)# ssl server-version tlsv1 sslv3` `!! set client version` `ciscoasa(config) # ssl client-version any` • 一部の一般的なアプリケーションで DHE はサポートされないため、SSL トとサーバの両方に共通の暗号スイートを使用できるように、他の SSL を少なくとも 1 つ含めます。 • 一部のクライアントで DHE はサポートされない場合があります。AnyC よび 3.0、Cisco Secure Desktop、Internet Explorer 9.0 などです。 **ssl encryption** コマンドが変更されました。 次の画面が変更されました。[Configuration] > [Device Management] > [Advanc Settings] この機能は、*8.5（1）*、*8.6（1）*、*8.7（1）*、*9.0（1）*、*9.0(2)*、*9.1(1)* では、 せん。
イメージ検証	SHA-512 イメージ整合性チェックのサポートが追加されました。 次のコマンドが変更されました。**verify** この機能は、*8.5（1）*、*8.6（1）*、*8.7（1）*、*9.0（1）*、*9.0(2)*、*9.1(1)* では、 せん。

機能	説明
疑似乱数生成の向上	エントロピー追加のためのハードウェアベースのノイズが、ソフトウェア 生成プロセスに追加されました。この変更により、疑似乱数生成（PRNG ムになり、攻撃者が繰り返し可能なパターンを入手したり、暗号化およ 使用される次の乱数を推測したりすることがより困難になります。PRNG に、次の 2 つの変更が行われました。 • ソフトウェアベースの RNG のパラメータの 1 つとして使用するラン に、最新のハードウェアベースの RNG を使用します。 • ハードウェアベースの RNG を使用できない場合は、ソフトウェアベ に追加のハードウェア ノイズ ソースを使用します。使用しているモ 次のハードウェア センサーが使用されます。 • ASA 5505：電圧センサー。 • ASA 5510 および 5550：ファン スピード センサー。 • ASA 5520、5540、および 5580：温度センサー。 • ASA 5585-X：ファン スピード センサー。 次のコマンドが導入されました。**show debug menu cts** [**128** | **129**] この機能は、*8.5（1）*、*8.6（1）*、*8.7（1）*、*9.0（1）*、*9.0(2)*、*9.1(1)* で せん。
リモート アクセス機能	
クライアントレス SSL VPN：リライタ エンジンの品質向上	クライアントレス SSL VPN リライタ エンジンの品質と有効性が大きく向 の結果、クライアントレス SSL VPN ユーザーのエンドユーザー エクスペ が期待できます。 この機能に関して、追加または変更されたコマンドはありません。 この機能に関して、追加または変更された ASDM 画面はありません。 この機能は、*8.5(1)*、*8.6(1)*、または *8.7(1)* では使用できません。
フェールオーバー機能	

機能	説明
バルク同期中の接続複製レートの設定	ステートフル フェールオーバーを使用するときに、ASA で接続がスタンバイされるレートを設定できるようになりました。デフォルトでは、接続は 15 秒ンバイ装置に複製されます。ただし、バルク同期が発生すると（たとえば、フバーを最初にイネーブルにしたときなど）、1 秒あたりの最大接続数の制限の量の接続を同期するのに 15 秒では不十分な場合があります。たとえば、ASA続数を 800 万とします。800 万の接続を 15 秒間で複製するということは、1 53.3 万の接続を作成するということです。ただし、1 秒あたりに許可される最30 万です。複製レートが 1 秒あたりの最大接続数以下になるように指定でき り、同期期間はすべての接続が同期されるまで調整されます。 **failover replication rate** *rate* コマンドが導入されました。 この機能は、*8.6(1)* または *8.7(1)* では使用できません。この機能は、*8.5(1.7)* す。
アプリケーション インスペクション機能	
ダイナミック ACL からピンホール メカニズムへの SunRPC の変更	これまでは、Sun RPC インスペクションは発信アクセス リストをサポートしれは、インスペクションエンジンでセカンダリ接続でなくダイナミック アクが使用されるためです。 このリリースでは、ASA でダイナミック アクセス リストを設定すると、入方サポートされ、ダイナミック ポート宛ての出トラフィックは ASA によって ます。したがって、Sun RPC インスペクションは、ピンホール メカニズムを力トラフィックをサポートします。Sun RPC インスペクションは、このピンニズムを使用して発信ダイナミック アクセス リストをサポートします。 この機能は、*8.5(1)*、*8.6(1)*、または *8.7(1)* では使用できません。

機能	説明
インスペクションリセットアクションの変更	これまでは、インスペクションエンジンルールに従ってASAによってパプされると、ドロップされたパケットのソースデバイスにRSTが1つのた。この動作により、リソースの問題が発生する可能性があります。 このリリースでは、リセットアクションを使用するようにインスペクシ設定し、パケットによってリセットがトリガーされると、次の条件でASリセットが送信されます。 • **service resetoutbound** コマンドがイネーブルの場合、ASA は TCP リストに送信します。（**service resetoutbound** コマンドは、デフォルトです）。 • **service resetinbound** コマンドがイネーブルの場合、ASA は TCP リセトに送信します。（**service resetinbound** コマンドは、デフォルトでです）。 詳細については、ASA コマンド リファレンスの **service** コマンドを参照し この動作によって、リセットアクションがASAおよび内部サーバの接続ことが確実になります。したがって、DoS 攻撃を防ぎます。外部ホストのリセットをデフォルトで送信せず、TCP リセットによって情報が公開さ この機能は、*8.5(1)*、*8.6(1)*、または *8.7(1)* では使用できません。
モジュール機能	
ASA CX SSP-10 と -20 に対する ASA 5585-X サポート	ASA CX モジュールを使用すると、特定の状況の完全なコンテキストに基リティを強制することができます。このコンテキストには、ユーザーのア（誰が）、ユーザーがアクセスを試みているアプリケーションまたは We を）、アクセス試行の発生元（どこで）、アクセス試行の時間（いつ）、スに使用されているデバイスのプロパティ（どのように）が含まれます。ジュールを使用すると、フローの完全なコンテキストを抽出して、細分化を適用することができます。たとえば、Facebook へのアクセスを許可するのゲームへのアクセスは禁止する、あるいは企業の機密データベースへの務担当者に許可するが他の社員には禁止するといったことが可能です。 **capture**、**cxsc**、**cxsc auth-proxy**、**debug cxsc**、**hw-module module password-re module reload**、**hw-module module reset**、**hw-module module shutdown**、**s host ip**、**session do get-config**、**session do password-reset**、**show asp table c cxsc**、**show asp table classify domain cxsc-auth-proxy**、**show capture**、**show module**、**show service-policy** の各コマンドが導入または変更されました。 次の画面が導入されました。 **[Home] > [ASA CX Status][Wizards] > [Startup Wizard] > [ASA CX Basic C** **[Configuration] > [Firewall > Service Policy Rules] > [Add Service Policy Rule] > [ASA CX Inspection]**

機能	説明
ASA 5585-X のネットワーク モジュール サポート	ASA 5585-X が、スロット 1 でネットワーク モジュール上の追加インターフ ポートするようになりました。次のオプション ネットワーク モジュールの つをインストールできます。 • ASA 4 ポート 10G ネットワーク モジュール • ASA 8 ポート 10G ネットワーク モジュール • ASA 20 ポート 1G ネットワーク モジュール この機能は、*9.0(1)*、*9.0(2)*、または *9.1(1)* では使用できません。

ASA 8.4(3)/ASDM 6.4(7) の新機能

リリース：**2012** 年 **1** 月 **9** 日

機能	説明
NAT の機能	
ラウンドロビン PAT プール割り当てで、既存のホストの同じ IP アドレスを使用する	ラウンドロビン割り当てで PAT プールを使用するときに、ホストに既存の接 合、そのホストからの後続の接続では、ポートが使用可能であれば同じ PAT が使用されます。 変更されたコマンドはありません。 変更された画面はありません。 この機能は、*8.5(1)* または *8.6(1)* では使用できません。
PAT プールの PAT ポートのフラットな範囲	使用できる場合、実際の送信元ポート番号がマッピング ポートに対して使用 ただし、実際のポートが使用できない場合は、デフォルトで、マッピング ポ のポート番号と同じポート範囲（0 ～ 511、512 ～ 1023、および 1024 ～ 6553 されます。そのため、1024 よりも下のポートには、小さい PAT プールのみか 下位ポート範囲を使用するトラフィックが数多くある場合は、PAT プールを きに、サイズが異なる 3 つの層の代わりにフラットなポート範囲を使用する できます。1024 ～ 65535 または 1 ～ 65535 です。 次のコマンドが変更されました。**nat dynamic** [**pat-pool** *mapped_object* [**flat** [**inclu** （オブジェクト ネットワーク設定モード）および **nat source dynamic** [**pat-po** *mapped_object* [**flat** [**include-reserve**]]]（グローバル設定モード） 次の画面が変更されました。 **[Configuration] > [Firewall] > [NAT Rules] > [Add/Edit Network Object]** **[Configuration] > [Firewall] > [NAT Rules] > [Add/Edit NAT Rule]** この機能は、*8.5(1)* または *8.6(1)* では使用できません。

機能	説明
PAT プールの拡張 PAT	各 PAT IP アドレスでは、最大 65535 個のポートを使用できます。65535 個 換が不十分な場合は、PAT プールに対して拡張 PAT をイネーブルにする す。拡張 PAT では、変換情報の宛先アドレスとポートを含め、IP アドレ く、サービスごとに 65535 個のポートが使用されます。 次のコマンドが変更されました。**nat dynamic** [**pat-pool** *mapped_object* [**ex** ジェクト ネットワーク設定モード）および **nat source dynamic** [**pat-pool** * [**extended**]]（グローバル設定モード） 次の画面が変更されました。 **[Configuration] > [Firewall] > [NAT Rules] > [Add/Edit Network Object]** **[Configuration] > [Firewall] > [NAT Rules] > [Add/Edit NAT Rule]** この機能は、*8.5(1)* または *8.6(1)* では使用できません。
PAT xlate に対する設定可能なタイムアウト	PAT xlate がタイムアウトし（デフォルトでは 30 秒後）、ASA が新しい変 を再使用すると、一部のアップストリーム ルータは、前の接続がアップ イスで依然として開いている可能性があるため、この新しい接続を拒否で ます。PAT xlate のタイムアウトを、30 秒～ 5 分の範囲内の値に設定でき した。 **timeout pat-xlate** コマンドが導入されました。 次の画面が変更されました。[Configuration] > [Firewall] > [Advanced] > [Gl この機能は、*8.5(1)* または *8.6(1)* では使用できません。

機能	説明
VPN ピアのローカル IP アドレスを変換してピアの実際の IP アドレスに戻す自動 NAT ルール	まれに、内部ネットワークで、割り当てられたローカル IP アドレスではなく の実際の IP アドレスを使用する場合があります。VPN では通常、内部ネッ クセスするために、割り当てられたローカル IP アドレスがピアに指定され し、内部サーバーおよびネットワーク セキュリティがピアの実際の IP アド 場合などに、ローカル IP アドレスを変換してピアの実際のパブリック IP ア 場合があります。 この機能は、トンネル グループごとに 1 つのインターフェイスでイネーブル ができます。VPN セッションが確立または切断されると、オブジェクト NA 的に追加および削除されます。ルールは **show nat** コマンドを使用して表示 （注） ルーティングの問題のため、この機能が必要でない場合は、この は推奨しません。ご使用のネットワークとの機能の互換性を確認 Cisco TAC にお問い合わせください。次の制限事項を確認してく • Cisco IPsec および AnyConnect クライアントのみがサポート • NAT ポリシーおよび VPN ポリシーが適用されるように、パ アドレスへのリターン トラフィックは ASA にルーティング があります。 • ロードバランシングはサポートされません（ルーティングの め）。 • ローミング（パブリック IP 変更）はサポートされません。 **nat-assigned-to-public-ip** *interface* コマンド（トンネル グループ一般属性コン ション モード）が導入されました。 ASDM ではこのコマンドはサポートされません。コマンドライン ツールを ンドを入力してください。
リモート アクセス機能	
ブラウザでのクライアントレス SSL VPN のサポート	ASA は、Microsoft Internet Explorer 9 および Firefox 4 を使用してクライアン VPN をサポートするようになりました。

機能	説明
DTLS および TLS における圧縮	スループットを向上させるため、シスコは AnyConnect 3.0 以降で DTLS サポートするようになりました。各トンネリング メソッドは個別に圧縮優先設定は SSL と DTLS の両方の圧縮を LZS とすることです。この機能クライアントからの移行を強化します。 （注） 高圧縮データを渡す高速リモート アクセス接続でデータ圧縮は、ASA にかなりの処理能力が要求されます。ASA で他の活動クがあると、プラットフォームでサポートできるセッションの 次のコマンドを導入または変更しました。**anyconnect dtls compression** [**lz** **anyconnect ssl compression** [**deflate** | **lzs** | **none**] 次の画面が変更されました。[Configuration] > [Remote Access VPN] > [Clie Access] > [Group Policies] > [Edit] > [Edit Internal Group Policy] > [Advanced] Client] > [SSL Compression]
クライアントレス SSL VPN セッション タイムアウト アラート	ユーザーの VPN セッションが、無活動またはセッション タイムアウトに とをユーザーに警告するカスタム メッセージを作成できます。 次のコマンドが導入されました。**vpn-session-timeout alert-interval**、**vpn- alert-interval** 次の画面が導入されました。 **[Remote Access VPN] > [Configuration] > [Clientless SSL VPN Access] > [P [Customizations] > [Add/Edit] > [Timeout Alerts]** **[Remote Access VPN] > [Configuration] > [Clientless SSL VPN Access] > [G [Add/Edit General]**
AAA 機能	
属性あたりの最大 LDAP 値が増加	単一の属性に対して ASA が受け取ることができる値の最大数は、1000（ら 5000 に増やされました。許可される範囲は 500 ～ 5000 です。設定さ た応答メッセージを受信した場合、ASA は認証を拒否します。ASA が、 を持つ単一の属性を検出した場合、ASA は情報 syslog 109036 を生成しま を超える場合、ASA はエラー レベル syslog 109037 を生成します。 次のコマンドが導入されました。**ldap-max-value-range** *number*（このコマ ホスト設定モードで入力します）。 ASDM ではこのコマンドはサポートされません。コマンドライン ツール ンドを入力してください。
LDAP 検索結果の下位範囲のサポート	サーバ設定に応じて、LDAP 検索が多数の値を持つ属性という結果になる ブ範囲を返し、ASA が残りの値範囲に対して追加のクエリを開始するこ とがあります。ASA は残りの範囲に対して複数のクエリを行い、応答を 配列に結合するようになりました。

機能	説明
ASA からの RADIUS アクセス要求パケットおよびアカウンティング要求パケットでの主なベンダー固有属性（VSA）の送信	4 つの新しい VSA：Tunnel Group Name（146）および Client Type（150）は、RADIUS アクセス要求パケットで送信されます。Session Type（151）および Se（152）は、ASA からの RADIUS アカウンティング要求パケットで送信され すべての属性が、すべてのアカウンティング要求パケットタイプ（開始、中間ト、および終了）に送信されます。RADIUS サーバー（ACS や ISE など）にやポリシー属性を強制適用したり、アカウンティングや課金のためにそれら用したりできます。
トラブルシューティング機能	
show asp table classifier および **show asp table filter** コマンドの正規表現照合	出力をフィルタするために、**show asp table classifier** と **show asp table filter** コ規表現を使用して入力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。**show asp table classifier match** *regex*、**show a match** *regex* ASDM ではこのコマンドはサポートされません。コマンドライン ツールを使ンドを入力してください。

ASA 8.4(2.8)/ASDM 6.4(5.106) の新機能

リリース：**2011年8月31日**

（注） 解決される特定の問題がある場合にだけ、Cisco.com にポストされた ASA 暫定リリースにアップグレードすることを推奨します。実稼働環境で暫定リリースを実行する場合は、暫定リリースでは対象のテストだけが実行されることに注意してください。暫定リリースは、TAC Web サイトによって十分にサポートされ、通常、次のメンテナンス リリースが使用可能になるまでの期間だけダウンロードサイトに残されます。暫定リリースを実行することを選択した場合、使用可能になったときに、完全にテストされたメンテナンス リリース、または機能リリースにアップグレードすることを強く推奨します。

次のメンテナンスまたは機能リリースの時点で暫定リリース機能についてマニュアルを作成します。各 ASA 暫定リリースの解決済みの警告のリストについては、Cisco.com のソフトウェア ダウンロード サイトから入手可能な暫定リリース ノートを参照してください。

機能	説明
リモート アクセス機能	
ブラウザでのクライアントレス SSL VPN のサポート	ASA は、Microsoft Internet Explorer 9 および Firefox 4 を使用してクライアン VPN をサポートするようになりました。 バージョン *8.2(5.13)* および *8.3.2(25)* でも使用可能です。

機能	説明
DTLS および TLS における圧縮	スループットを向上させるため、シスコは AnyConnect 3.0 以降で DTLS サポートするようになりました。各トンネリング メソッドは個別に圧縮優先設定は SSL と DTLS の両方の圧縮を LZS とすることです。この機能クライアントからの移行を強化します。 （注） 高圧縮データを渡す高速リモート アクセス接続でデータ圧縮は、ASA にかなりの処理能力が要求されます。ASA で他の活クがあると、プラットフォームでサポートできるセッションの 次のコマンドを導入または変更しました。**anyconnect dtls compression** [**lz** **anyconnect ssl compression** [**deflate** | **lzs** | **none**] 次の画面が変更されました。[Configuration] > [Remote Access VPN] > [Clie Access] > [Group Policies] > [Edit] > [Edit Internal Group Policy] > [Advanced] Client] > [SSL Compression] バージョン *8.2(5.13)* および *8.3.2(25)* でも使用可能です。
クライアントレス SSL VPN セッション タイムアウト アラート	ユーザーの VPN セッションが、無活動またはセッション タイムアウトに とをユーザーに警告するカスタム メッセージを作成できます。 次のコマンドが導入されました。**vpn-session-timeout alert-interval**、**vpn- alert-interval** 次の画面が導入されました。 **[Remote Access VPN] > [Configuration] > [Clientless SSL VPN Access] > [P [Customizations] > [Add/Edit] > [Timeout Alerts]** **[Remote Access VPN] > [Configuration] > [Clientless SSL VPN Access] > [G [Add/Edit General]**
AAA 機能	
属性あたりの最大 LDAP 値が増加	単一の属性に対して ASA が受け取ることができる値の最大数は、1000（ら 5000 に増やされました。許可される範囲は 500 ～ 5000 です。設定さ た応答メッセージを受信した場合、ASA は認証を拒否します。ASA が、 を持つ単一の属性を検出した場合、ASA は情報 syslog 109036 を生成しま を超える場合、ASA はエラー レベル syslog 109037 を生成します。 次のコマンドが導入されました。**ldap-max-value-range** *number*（このコマ ホスト設定モードで入力します）。 ASDM ではこのコマンドはサポートされません。コマンドライン ツール ンドを入力してください。
LDAP 検索結果の下位範囲のサポート	サーバ設定に応じて、LDAP 検索が多数の値を持つ属性という結果になる ブ範囲を返し、ASA が残りの値範囲に対して追加のクエリを開始するこ とがあります。ASA は残りの範囲に対して複数のクエリを行い、応答を 配列に結合するようになりました。

機能	説明
トラブルシューティング機能	
show asp table classifier および **show asp table filter** コマンドの正規表現照合	出力をフィルタするために、**show asp table classifier** と **show asp table filter** コ規表現を使用して入力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。**show asp table classifier match** *regex*、**show a match** *regex* ASDM ではこのコマンドはサポートされません。コマンドライン ツールを使ンドを入力してください。 バージョン *8.2(5.13)* および *8.3.2(25)* でも使用可能です。

ASA 8.4(2)/ASDM 6.4(5) の新機能

リリース：**2011** 年 **6** 月 **20** 日

機能	説明
ファイアウォール機能	

機能	説明
アイデンティティ ファイアウォール	通常、ファイアウォールはユーザー アイデンティティを認識せず、したンティティに基づいてセキュリティ ポリシーを適用できません。 ASA のアイデンティティ ファイアウォールでは、ユーザーのアイデンテたより細かなアクセス コントロールが実現されます。送信元 IP アドレスザー名とユーザー グループ名に基づいて、アクセスルールとセキュリテ定できます。ASA は、IP アドレスと Windows Active Directory のログイン に基づいてセキュリティポリシーを適用し、ネットワーク IP アドレスでグされたユーザー名を使用してイベントを報告します。 アイデンティティ ファイアウォールは、実際のアイデンティティ マッピ外部 Active Directory（AD）エージェントとの連携により、Microsoft Activ合されます。ASA は Windows Active Directory をソースとして使用して、レスについて最新のユーザー アイデンティティ情報を取得します。 企業では、ユーザーによっては、Web ポータル（カットスルー プロキシ VPN を使用した認証など、通常とは異なる認証メカニズムを使用してネグオンする場合があります。これらの認証方式がアイデンティティに基づリシーと連携できるようにアイデンティティ ファイアウォールを設定すす。 次のコマンドを導入または変更しました。**user-identity enable**、**user-iden default-domain**、**user-identity domain**、**user-identity logout-probe**、**user-id inactive-user-timer**、**user-identity poll-import-user-group-timer**、**user-iden netbios-response-fail**、**user-identity user-not-found**、**user-identity action ad user-identity action mac-address-mismatch**、**user-identity action domain-co user-identity ad-agent active-user-database**、**user-identity ad-agent hello-time ad-agent aaa-server**、**user-identity update import-user**、**user-identity static ad-agent-mode**、**dns domain-lookup**、**dns poll-timer**、**dns expire-entry-time user**、**show user-identity**、**show dns**、**clear configure user-identity**、**clear d user-identity**、**test aaa-server ad-agent** 次の画面が導入されました。 **[Configuration] > [Firewall] > [Identity Options]**。**[設定（Configuration）] ル（Firewall）] > [オブジェクト（Objects）] > [ローカルユーザーグルー Groups）]** **[Monitoring] > [Properties] > [Identity]** 次の画面が変更されました。 **[Configuration] > [Device Management] > [Users/AAA] > [AAA Server Grou Server Group]**

機能	説明
アイデンティティ NAT の設定が可能なプロキシ ARP およびルート ルックアップ	アイデンティティ NAT の以前のリリースでは、プロキシ ARP はディセーブ 出力インターフェイスの決定には常にルート ルックアップが使用されてい らを設定することはできませんでした。8.4(2) 以降、アイデンティティ NAT ト動作は他のスタティック NAT コンフィギュレーションの動作に一致する れました。これにより、デフォルトでプロキシ ARP はイネーブルにされ、N ギュレーションにより出力インターフェイスが決定されるようになりました ている場合）。これらの設定をそのまま残すこともできますし、個別にイネ はディセーブルにすることもできます。通常のスタティック NAT のプロキシ セーブルにすることもできるようになっています。 8.3 よりも前の設定の場合、8.4(2) 以降への NAT 免除ルール（**nat 0 access-lis** の移行には、プロキシ ARP をディセーブルにするキーワード **no-proxy-arp** お ルックアップを使用するキーワード **route-lookup** があります。8.3(2) および 行に使用された **unidirectional** キーワードは、移行に使用されなくなりまし 8.3(2)、8.4(1) から 8.4(2) にアップグレードすると、既存機能を保持するため アイデンティティ NAT コンフィギュレーションに **no-proxy-arp** キーワードと キーワードが含まれるようになっています。**unidirectional** キーワードは削除 **nat static** [**no-proxy-arp**] [**route-lookup**]（オブジェクト ネットワーク）、およ **static** [**no-proxy-arp**] [**route-lookup**]（グローバル）コマンドが変更されまし 次の画面が変更されました。 **[Configuration] > [Firewall] > [NAT Rules] > [Add/Edit Network Object] > [Ad** **Settings]** **[Configuration] > [Firewall] > [NAT Rules] > [Add/Edit NAT Rule]**
PAT プールおよびラウンドロビン アドレス割り当て	1 つのアドレスの代わりに、PAT アドレスのプールを指定できるようになり た、オプションで、PAT アドレスのすべてのポートを使用してからプール内 レスを使用するのではなく、PAT アドレスのラウンドロビン割り当てをイネ ることもできます。これらの機能は、1 つの PAT アドレスで多数の接続を行 合にそれが DoS 攻撃の対象となることを防止するのに役立ちます。またこの機 多数の PAT アドレスを簡単に設定できます。 （注） 現在の 8.4(2) では、PAT プール機能をダイナミック NAT または P ルバック方式として使用することはできません。PAT プールは、 ク PAT のプライマリ方式（CSCtq20634）としてのみ設定できます **nat dynamic** [**pat-pool** *mapped_object* [**round-robin**]]（オブジェクト ネットワー び **nat source dynamic** [**pat-pool** *mapped_object* [**round-robin**]]（グローバル）コ 更されました。 次の画面が変更されました。 **[Configuration] > [Firewall] > [NAT Rules] > [Add/Edit Network Object]** **[Configuration] > [Firewall] > [NAT Rules] > [Add/Edit NAT Rule]**

機能	説明
IPv6 インスペクション	サービス ポリシーを設定して IPv6 インスペクションを設定し、拡張ヘッ IPv6 トラフィックを選択的にブロックできます。IPv6 パケットに対して リティ チェックが実行されます。ASA は、ルータ ヘッダーとノー ネクス ブロックする一方で、常に、ホップバイホップと宛先オプション タイプ を通過させます。 デフォルトの IPv6 インスペクションをイネーブルにするか、IPv6 インス スタマイズできます。IPv6 インスペクションのポリシー マップを定義す て、IPv6 パケット内で見つかった次のタイプの拡張ヘッダーに基づいて 選択的にドロップするように ASA を設定できます。 • ホップバイホップ オプション • ルーティング（タイプ 0） • フラグメント • 宛先オプション • 認証 • カプセル化セキュリティ ペイロード 次のコマンドが変更されました。**policy-map type inspect ipv6、verify-hea header、match header routing-type、match header routing-address count gt count gt** 次の画面が導入されました。[Configuration] > [Firewall] > [Objects] > [Inspe
リモート アクセス機能	
ポータル アクセス ルール	この拡張機能により、カスタマーは、HTTP ヘッダー内に存在するデータ ライアントレス SSL VPN セッションを許可または拒否するグローバルな ス SSL VPN アクセス ポリシーを設定することができます。拒否された場 コードがクライアントに返されます。この拒否は、ユーザー認証の前に行 処理リソースの使用が最小限に抑えられます。 次のコマンドが変更されました。**webvpn portal-access-rule** 次の画面が変更されました。[Configuration] > [Remote Access VPN] > [Clie Access] > [Portal] > [Portal Access Rules] バージョン *8.2(5)* でも使用可能です。
Microsoft Outlook Web App 2010 のクライアントレス サポート	ASA 8.4(2) クライアントレス SSL VPN コア リライタは、Microsoft Outloo をサポートするようになりました。

機能	説明
IPsec IKEv2 整合性および PRF のセキュア ハッシュ アルゴリズム SHA-2 サポート	このリリースでは、ASA への IPsec/IKEv2 AnyConnect セキュア モビリティ ク接続の暗号化ハッシュ セキュリティの向上のために、セキュア ハッシュ ア SHA-2 がサポートされます。米国政府の要請に基づき、SHA-2 には 256、38 512 ビットのダイジェストを生成するハッシュ機能が実装されています。 次のコマンドが変更されました。**integrity**、**prf, show crypto ikev2 sa detail**、**vpn-sessiondb detail remote** 次の画面が変更されました。[Configuration] > [Remote Access VPN] > [Networ Access] > [Advanced] > [IPsec] > [IKE Policies] > [Add/Edit IKEv2 Policy (Propos
IPsec IKEv2 でのデジタル署名のセキュア ハッシュ アルゴリズム SHA-2 サポート	このリリースでは、デジタル証明書を使用する IPsec IKEv2 VPN 接続の認証 SHA-2 準拠の署名アルゴリズムの使用がサポートされます。ハッシュ サイ SHA-256、SHA-384、および SHA-512 があります。 IPsec IKEv2 接続の SHA-2 デジタル署名が、AnyConnect セキュア モビリティ ト バージョン 3.0.1 以降でサポートされます。
AnyConnect 用のスプリット トンネル DNS ポリシー	このリリースには、スプリット トンネルを介して DNS アドレスを解決する AnyConnect セキュア モビリティ クライアントにプッシュダウンされた新しい 含まれています。このポリシーは、SSL プロトコルまたは IPsec/IKEv2 プロ する VPN 接続に適用され、AnyConnect クライアントに対して VPN トンネ すべての DNS アドレスを解決するように指示します。DNS 解決に失敗すると は未解決のまま残ります。AnyConnect Client は、パブリック DNS サーバー経 スを解決しようとはしません。 デフォルトでは、この機能はディセーブルになっています。クライアントは トトンネル ポリシーに従ってトンネル経由で DNS クエリーを送信します。ポ すべてのネットワークをトンネリング、ネットワーク リストで指定された ネ をトンネリング、またはネットワーク リストで指定されたネットワークを除 次のコマンドが導入されました。split-tunnel-all-dns 次の画面が変更されました。[Configuration] > [Remote Access VPN] > [Networ Access] > [Group Policies] > [Add/Edit Group Policy] > [Advanced] > [Split Tunnel All DNS Lookups Through Tunnel] チェックボックスを参照）。 バージョン *8.2(5)* でも使用可能です。

機能	説明
Mobile Posture （以前の名称は AnyConnect Identification Extensions for Mobile Device Detection）	モバイル デバイスへの VPN 接続の許可または拒否、グループ単位でのモ ス アクセスのイネーブル化またはディセーブル化、およびモバイル デバ データに基づいた接続モバイル デバイスに関する情報の収集を実行する 定できるようになりました。AnyConnect for iPhone/iPad/iPod バージョン 2 AnyConnect for Android バージョン 2.4.x の各モバイル プラットフォーム ポートされています。 ライセンス要件 リモート アクセス コントロールを適用し、モバイル デバイスからポスチ 集するには、AnyConnect Mobile ライセンスと、AnyConnect Essentials また Premium ライセンスのいずれかが ASA にインストールされている必要が ストールするライセンスに基づいて次の機能を受け取ります。 • **AnyConnect Premium ライセンス機能** AnyConnect Premium ライセンスをインストールする企業は、DAP 属性お エンドポイント属性に基づいてサポートされているモバイル デバイスの 適用できます。これには、モバイル デバイスからのリモート アクセスの が含まれます。 • **AnyConnect Essentials ライセンス機能** AnyConnect Essentials ライセンスをインストールする企業は、次の操作を • モバイル デバイス アクセスをグループ単位でイネーブルまたはディ す。この機能を、ASDM を使用して設定します。 • CLI または ASDM を使用して接続モバイル デバイスに関する情報を だし、DAP ポリシーを適用したり、これらのモバイル デバイスへの スを拒否/許可したりする機能はありません）。 次の画面が変更されました。[Configuration] > [Remote Access VPN] > [Net Access] > [Dynamic Access Policies] > [Add/Edit Endpoint Attributes] > [Endpo Type:AnyConnect] バージョン *8.2(5)* でも使用可能です。

機能	説明
SSL SHA-2 デジタル署名	デジタル証明書を使用する SSL VPN 接続の認証における SHA-2 準拠の署名ア を使用できるようになりました。SHA-2 のサポートには、SHA-256、SHA-3 SHA-512 の 3 つすべてのハッシュ サイズが含まれます。SHA-2 には AnyCon 降（2.5(2) 以降を推奨）が必要です。このリリースは、他の使用または製品 をサポートしません。 注意：SHA-2 接続のフェールオーバーをサポートするためには、スタンバイ イメージを実行している必要があります。 次のコマンドが変更されました。**show crypto ca certificate**（[Signature Algori ルドは、署名の生成時に使用されるダイジェスト アルゴリズムを識別します 変更された画面はありません。 バージョン *8.2(5)* でも使用可能です。
SHA2 証明書署名による Microsoft Windows 7 と Android ネイティブ VPN クライアントのサポート	ASA は、L2TP/IPsec プロトコルを使用する場合、Microsoft Windows 7 および イティブ VPN クライアント用の SHA2 証明書署名サポートをサポートします 変更されたコマンドはありません。 変更された画面はありません。 バージョン *8.2(5)* でも使用可能です。
group-url 属性をオーバーライドするための証明書のマッピングの有効化/無効化	この機能は、接続プロファイルの選択プロセス中に、接続プロファイルのプ スを変更します。デフォルトでは、接続プロファイルで指定された証明書の 値とエンドポイントで使用される証明書のフィールド値が ASA によって照合 した場合は、そのプロファイルが VPN 接続に割り当てられます。このオプシ により、エンドポイントが要求したグループ URL を指定する接続プロファイ プリファレンスが変更されます。この新しいオプションにより、管理者は A ウェアの数多くの旧リリースによって使用されるグループ URL プリファレン きます。 次のコマンドが導入されました。**tunnel-group-preference**。 次の画面が変更されました。 **[Configuration] > [Remote Access VPN] > [Clientless SSL VPN] > [Connection** **[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [AnyConnec Profiles]** バージョン *8.2(5)* でも使用可能です。
ASA 5585-X の機能	

機能	説明
SSP-40 および SSP-60 対応のデュアル SSP のサポート	SSP-40 および SSP-60 の場合、同じシャーシでレベルが同じ 2 つの SSP を レベルが混在した SSP はサポートされていません（たとえば、SSP-40 と 合わせはサポートされていません）。各 SSP は個別のコンフィギュレー 理を持つ独立したデバイスとして動作します。必要に応じて 2 つの SSP バー ペアとして使用できます。 （注） 2 個の SSP をシャーシで使用する場合、VPN はサポートされ し、VPN がディセーブルになっていないことに注意してくだ **show module**、**show inventory**、**show environment** の各コマンドが変更さ 変更された画面はありません。
IPS SSP-10、-20、-40、および -60 のサポート	ASA 5585-X 用の IPS SSP-10、-20、-40、および -60 のサポートを導入しま は対応するレベルの SSP がある場合にのみインストールできます（たと IPS SSP-10）。 バージョン *8.2(5)* でも使用可能です。
CSC SSM の機能	
CSC SSM サポート	CSC SSM について、次の機能のサポートが追加されました。 • HTTPS トラフィック リダイレクション：受信 HTTPS 接続の URL フ WRS クエリー。 • 受信および送信 SMTP、POP3 電子メールのグローバル認定のホワイ • 製品ライセンス更新の電子メール通知。 変更されたコマンドはありません。 次の画面が変更されました。 **[Configuration] > [Trend Micro Content Security] > [Mail] > [SMTP]** **[Configuration] > [Trend Micro Content Security] > [Mail] > [POP3]** **[Configuration] > [Trend Micro Content Security] > [Host/Notification Setti** **[Configuration] > [Trend Micro Content Security] > [CSC Setup] > [Host C**
モニタリング機能	

機能	説明
Smart Call-Home Anonymous Reporting	顧客は Anonymous Reporting をイネーブルにして、ASA プラットフォームを とができるようになりました。Anonymous Reporting により、エラーおよびイ る最小限の情報をデバイスからシスコに安全に送信できます。 次のコマンドが導入されました。**call-home reporting anonymous**、**call-home t** **anonymous** 次の画面が変更されました。[Configuration] > [Device Monitoring] > [Smart Ca バージョン *8.2(5)* でも使用可能です。
IF-MIB ifAlias OID のサポート	ASA は、ifAlias OID をサポートするようになりました。IF-MIB をブラウズす OID はインターフェイスの記述に設定済みの値に設定されます。 バージョン *8.2(5)* でも使用可能です。
インターフェイス機能	
1 ギガビット イーサネット インターフェイスでのフロー制御のポーズフレームのサポート	1 ギガビット イーサネット インターフェイスでのフロー制御用の停止（XOF を有効化できるようになりました。サポートは以前は 8.2(2) の 10 ギガビット ト インターフェイス用に追加されていました。 **flowcontrol** コマンドが変更されました。 次の画面が変更されました。 （シングル モード）[Configuration] > [Device Setup] > [Interfaces] > [Add/Edit I [General] （マルチ モード、システム）[Configuration] > [Interfaces] > [Add/Edit Interface バージョン *8.2(5)* でも使用可能です。
管理機能	
SSH セキュリティの向上：SSH のデフォルトのユーザー名はサポートされない	8.4(2) 以降、**pix** または **asa** ユーザー名とログイン パスワードで SSH を使用 接続することができなくなりました。SSH を使用するには、**aaa authenticatio** **LOCAL** コマンド（CLI）または [Configuration] > [Device Management] > [Use [AAA Access] > [Authentication (ASDM)] を使用して AAA 認証を設定してから ユーザーを定義する必要があります。定義するには、**username** コマンド（C するか、[Configuration] > [Device Management] > [Users/AAA] > [User Accounts 選択します。ローカル データベースの代わりに AAA サーバーを認証に使用 ローカル認証もバックアップの手段として設定しておくことをお勧めします
ユニファイド コミュニケーション機能	

機能	説明
ASA Tandberg と H.323 インスペクションとの相互運用性	H.323 インスペクションは、双方向ビデオ セッションの双方向信号をサ になりました。この機能拡張により、一方向のビデオ会議での H.323 イン が Tandberg ビデオ電話によってサポートされます。双方向信号をサポート 電話はビデオ モードを切り替えることができます（H.263 ビデオ セッショ 高解像度ビデオの圧縮標準である H.264 を使用してセッションを再オー 変更されたコマンドはありません。 変更された画面はありません。 バージョン *8.2(5)* でも使用可能です。
ルーティング機能	
バックアップ スタティック ルートを使用する接続のタイムアウト	同じネットワークへの複数のスタティック ルートが存在しており、それ が異なる場合は、ASA は接続確立時点でメトリックが最良のルートを使 適切なルートが使用可能になった場合は、このタイムアウトによって接 ので、その適切なルートを使用して接続を再確立できます。デフォルト はタイムアウトしません）。この機能を使用するには、タイムアウトを します。 **timeout floating-conn** コマンドが変更されました。 次の画面が変更されました。[Configuration] > [Firewall] > [Advanced] > [G バージョン *8.2(5)* でも使用可能です。
ASDM 機能	
Migrate Network Object Group Members	8.3 以降に移行する場合、ASA は名前付きネットワーク オブジェクトを の機能のインライン IP アドレスを置き換えます。名前付きオブジェクトに はコンフィギュレーションで使用されているすべての IP アドレスに対し ジェクトを自動的に作成します。これらの自動作成されるオブジェクト よってのみ識別され、名前がなく、プラットフォーム設定に名前付きオ ては存在しません。 移行の一部として名前付きオブジェクトを ASA が作成する場合、合致す ASDM 専用オブジェクトは、名前付きオブジェクトに置換されます。唯一 トワーク オブジェクト グループの非名前付きオブジェクトです。ネット クト グループ内にある IP アドレスの名前付きオブジェクトを ASA が作 ASDM は非名前付きオブジェクトを維持したまま、重複したオブジェク 成します。これらのオブジェクトをマージするには、[Tools] > [Migrate N Group Members] を選択します。 次の画面が導入されました。[Tools] > [Migrate Network Object Group Mem 詳細については、「*Cisco ASA 5500 Migration to Version 8.3 and Later*」を参 い。

ASA 8.4(1.11)/ASDM 6.4(2) の新機能

リリース：**2011年5月20日**

（注） 解決される特定の問題がある場合にだけ、Cisco.com にポストされた暫定リリースにアップグレードすることを推奨します。実稼働環境で暫定リリースを実行する場合は、暫定リリースでは対象のテストだけが実行されることに注意してください。暫定リリースは、TAC Web サイトによって十分にサポートされ、次のメンテナンスリリースが使用可能になるまでの期間だけダウンロードサイトに残されます。暫定リリースを実行することを選択した場合、使用可能になったときに、完全にテストされたメンテナンス リリース、または機能リリースにアップグレードすることを強く推奨します。次のメンテナンスまたは機能リリースの時点で暫定リリース機能についてマニュアルを作成します。各暫定リリースの解決済みの警告のリストについては、Cisco.comのソフトウェアダウンロードサイトから入手可能な暫定リリースノートを参照してください。

機能	説明
ファイアウォール機能	
PAT プールおよびラウンドロビン アドレス割り当て	1 つのアドレスの代わりに、PAT アドレスのプールを指定できるようになり た、オプションで、PAT アドレスのすべてのポートを使用してからプール内 レスを使用するのではなく、PAT アドレスのラウンドロビン割り当てをイネ ることもできます。これらの機能は、1 つの PAT アドレスで多数の接続を行 合にそれがDoS攻撃の対象となることを防止するのに役立ちます。またこの機 多数の PAT アドレスを簡単に設定できます。 （注） 現在の 8.4(1.11) では、PAT プール機能をダイナミック NAT また フォールバック方式として使用することはできません。PAT プー ナミック PAT のプライマリ方式（CSCtq20634）としてのみ設定で **nat dynamic** [**pat-pool** *mapped_object* [**round-robin**]]（オブジェクト ネットワー び **nat source dynamic** [**pat-pool** *mapped_object* [**round-robin**]]（グローバル）コ 更されました。 次の画面が変更されました。 **[Configuration] > [Firewall] > [NAT Rules] > [Add/Edit Network Object] [Conf** **[Firewall] > [NAT Rules] > [Add/Edit NAT Rule]**

ASA 8.4(1)/ASDM 6.4(1) の新機能

リリース：**2011 年 1 月 31 日**

機能	説明
ハードウェアの機能	
ASA 5585-X のサポート	セキュリティ サービス プロセッサ（SSP）-10、-20、-40、および -60 を搭 5585-X のサポートが導入されました。 （注） このサポートは 8.2(3) と 8.2(4) で追加されていました。8.3(x) 5585-X はサポートされていません。
輸出用のペイロード暗号化なしハードウェア	ASA 5585-X のペイロード暗号化なしモデルを購入いただけます。輸出先 は、Cisco ASA 5500 シリーズでペイロード暗号化をイネーブルにできませ トウェアは、ペイロード暗号化なしモデルを検出し、次の機能をディセー • ユニファイド コミュニケーション • VPN このモデルでも管理接続用に高度暗号化（3DES/AES）ライセンスをイン す。たとえば、ASDM HTTPS/SSL、SSHv2、Telnet、および SNMPv3 を使 ボットネット トラフィック フィルタ（SSL を使用）用のダイナミック デ ウンロードすることもできます。
リモート アクセス機能	
Android プラットフォーム上の L2TP/IPsec サポート	L2TP/IPsec プロトコルとネイティブ Android VPN クライアントを使用する モバイル デバイスと ASA 5500 シリーズ デバイスとの間の VPN 接続をサ になりました。モバイル デバイスで Android 2.1 以降のオペレーティング されている必要があります。 バージョン *8.2(5)* でも使用可能です。
AnyConnect パスワードの UTF-8 文字サポート	ASA 8.4(1) で使用される AnyConnect 3.0 で、RADIUS/MSCHAP および LI を使用して送信されるパスワードの UTF-8 文字がサポートされます。

機能	説明
IKEv2 による IPsec VPN 接続	インターネット キー交換バージョン 2（IKEv2）は、インターネット プロトリティ（IPsec）トンネルの確立および制御に使用される最新のキー交換プロASA で、すべてのクライアント オペレーティング システムについて、AnyCoア モビリティ クライアント バージョン 3.0(1) での IKEv2 を使用する IPsec れるようになりました。 ASA 上で、グループ ポリシーでユーザーに対して IPsec 接続をイネーブルにAnyConnect クライアントでは、クライアント プロファイルのサーバ リストにASA についてプライマリ プロトコル（IPsec または SSL）を指定します。 AnyConnect Essentials ライセンスおよび AnyConnect Premium ライセンスに Iした IPsec リモート アクセス VPN が追加されました。 Other VPN ライセンス（以前の IPsec VPN）にはサイトツーサイト セッションました。Other VPN ライセンスは基本ライセンスに含まれています。 次のコマンドが変更されました。**vpn-tunnel-protocol**、**crypto ikev2 policy**、**enable**、**crypto ipsec ikev2**、**crypto dynamic-map**、**crypto map** 次の画面が変更されました。 **[Configure] > [Site-to-Site VPN] > [Connection Profiles]** **[Configure] > [Remote Access] > [Network (Client) Access] > [AnyConnect Connec** **[Network (Client) Access] > [Advanced] > [IPsec] > [IKE Parameters] > [IKE P** **[Network (Client) Access] > [Advanced] > [IPsec] > [IKE Parameters] > [IKE P** **[Network (Client) Access] > [Advanced] > [IPsec] > [IKE Parameters] > [IKE P**
SSL SHA-2 デジタル署名	このリリースは、デジタル証明書を使用する SSL VPN 接続の認証における S署名アルゴリズムをサポートします。SHA-2 のサポートには、SHA-256、SHびび SHA-512 の 3 つすべてのハッシュ サイズが含まれます。SHA-2 には AnyC以降（2.5.2 以降を推奨）が必要です。このリリースは、他の使用または製品をサポートしません。この機能にはコンフィギュレーションの変更はありま **注意**：SHA-2 接続のフェールオーバーをサポートするためには、スタンバイイメージを実行している必要があります。この機能をサポートするために、**ca certificate** コマンドに署名の生成に使用されるダイジェスト アルゴリズム[Signature Algorithm] フィールドを追加しました。

機能	説明
SCEP プロキシ	SCEP プロキシは、AnyConnect セキュア モビリティ クライアントに自動 パーティ証明書登録のサポートを提供します。この機能を使用して、エン 続を認可するデバイス証明書のゼロタッチでのセキュアな展開による An ポート、非企業資産によるアクセスを防止するポリシーの適用、および企 を実行します。この機能には、AnyConnect Premium ライセンスが必要で ライセンスでは使用できません。 次のコマンドが導入または変更されました。**crypto ikev2 enable**、**scep-enr** **scep-forwarding-url**、**debug crypto ca scep-proxy**、**secondary-username-fr** **secondary-pre-fill-username**
ホストスキャンパッケージのサポート	この機能により、ASA がホストスキャンパッケージをインストールまた ドして、ホスト スキャンをイネーブルまたはディセーブルにするために が提供されます。このパッケージは、スタンドアロンのホスト スキャン ASA が AnyConnect 次世代パッケージから抽出するパッケージです。 AnyConnect の以前のリリースでは、エンドポイントのポスチャは Cisco S （CSD）によって決定されました。ホスト スキャンは、CSD にバンドル くの機能の 1 つでした。ホスト スキャンが CSD のバンドルから除外され AnyConnect 管理者は、CSD の他の機能とは別にホスト スキャンを自由に ストールできます。 次のコマンドが導入されました。**csd hostscan image path**

機能	説明
Kerberos Constrained Delegation（KCD）	このリリースでは、KCD のプロトコル移行および制約付き委任の拡張機能が装されます。KCD により、クライアントレス SSL VPN（WebVPN ともいう）は Kerberos で保護された Web サービスへの SSO アクセスが可能になります。なサービスやアプリケーションの例として、Outlook Web Access（OWA）、およびインターネット インフォメーション サービス（IIS）があります。 プロトコル移行の実装により、ASA はリモート アクセス ユーザーに代わっサービス チケットを取得できるため、ユーザーに Kerberos による KDC へのしません。代わりに、ユーザーはクライアントレス SSL VPN（WebVPN ともでサポートされている認証メカニズムのいずれか（デジタル証明書やスマーど）を使用して、ASA に対して認証します。ユーザー認証が完了すると、Aザーの代わりに代替チケットを要求して取得します。代替チケットは、ASAス チケットです。ASA は次に、代替チケットを使用して、リモート アクセの他のサービス チケットを取得できます。 制約付き委任は、委任に対して信頼されたサービス（ASA など）が使用できるクリソースをドメイン管理者が制限する方法を提供します。このタスクを実行アカウントを設定し、そのアカウントの下でサービスが実行されて、特定のタ上で実行されているサービスの特定のインスタンスへの委任に対して信頼にします。 次のコマンドが変更されました。**kcd-server**、**clear aaa**、**show aaa**、**test aaa-authentication** 次の画面が変更されました。[Configuration] > [Remote Access VPN] > [Clientless Access] > [Advanced] > [Microsoft KCD Server]
ブラウザでのクライアントレス SSL VPN のサポート	ASA で、Apple Safari 5 によるクライアントレス SSL VPN がサポートされるよした。

機能	説明
クライアントレス VPN 自動サインオンの機能拡張	スマート トンネルによって、Internet Explorer だけでなく Firefox での HTT サインオンがサポートされるようになりました。Internet Explorer を使用 に、管理者は Firefox ブラウザがクレデンシャルを自動的に送信するホス す。認証方式によっては、管理者が ASA において（[Add Smart Tunnel Aut ウィンドウで）、ウェブアプリケーションの設定と一致するレルムの文字 ことが必要となる場合があります。スマート トンネルでの自動サインオ 換を含むブックマークを使用できるようになりました。 POST プラグインは廃止されました。以前の POST プラグインは、管理者 マクロを含むブックマークを指定し、POST 要求のポストの前にロードす ページを受信できるようにするために作成されました。POST プラグイン は、前もって取得されたクッキーおよびその他のヘッダー項目の存在を必 の通過が許可されました。管理者は、ブックマークの作成時に事前ロー して、同じ機能を実現できるようになりました。POSTプラグインと同様 前ロード ページの URL と POST 要求の送信先 URL を指定します。 デフォルトの事前設定された SSL VPN ポータルを独自のポータルで置き きるようになりました。これを実行するには、管理者は外部ポータルと します。グループ ポリシー ホームページと異なり、外部ポータルでは、 ジだけでなく（自動サインオン用の）マクロ置換を含むPOST要求がサポ 次のコマンドを導入または変更しました。**smart-tunnel auto-signon** 次の画面が導入または変更されました。 **[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [P** **[Customization]** **[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [P** **[Bookmarks] > [Edit] > [Edit Bookmark]**
スマート トンネル アプリケーションのサポートの拡張	スマート トンネルには、次のアプリケーションのサポートが追加されま • Microsoft Outlook Exchange Server 2010（ネイティブ サポート）。 ユーザーはスマート トンネルを使用して Microsoft Office Outlook を Micro Server に接続できるようになりました。 • Microsoft Sharepoint/Office 2010。 ユーザーは、スマート トンネルを使用して、Microsoft Office 2010 アプリ び Microsoft Sharepoint によるリモート ファイル編集を実行できるように
インターフェイス機能	

機能	説明
EtherChannel サポート（ASA 5510 以降）	最大 48 個の 802.3ad EtherChannel（1 つあたりのアクティブ インターフェイス 定できます。 （注） ASA 5550 上のスロット 1 の統合 4GE SSM を含む 4GE SSM 上のイ イスを EtherChannel の一部として使用することはできません。 **channel-group**、**lacp port-priority**、**interface port-channel**、**lacp max-bundle**、 **min-bundle**、**port-channel load-balance**、**lacp system-priority**、**clear lacp cou** **lacp**、**show port-channel** の各コマンドが導入されました。 次の画面が導入または変更されました。 **[Configuration] > [Device Setup] > [Interfaces]** **[Configuration] > [Device Setup] > [Interfaces] > [Add/Edit EtherChannel Inte** **[Configuration] > [Device Setup] > [Interfaces] > [Add/Edit Interface]** **[Configuration] > [Device Setup] > [EtherChannel]**
トランスペアレントモードのブリッジ グループ	セキュリティ コンテキストのオーバーヘッドを避けたい場合、またはセキュ テキストを最大限に使用したい場合、インターフェイスをブリッジ グループ 化し、各ネットワークに 1 つずつ複数のブリッジ グループを設定できます。 ループのトラフィックは他のブリッジ グループから隔離されます。シングル 最大 8 個、マルチ モードではコンテキストあたり最大 8 個のブリッジ グルー き、各ブリッジ グループには最大 4 個のインターフェイスを追加できます。 （注） ASA 5505 に複数のブリッジ グループを設定できますが、ASA 55 スペアレント モードのデータ インターフェイスは2つという制限 にブリッジ グループを 1 つだけ使用できることを意味します。 **次のコマンドが導入されました。interface bvi、bridge-group、show bridge-g** **次の画面が変更または導入されました。** **[Configuration] > [Device Setup] > [Interfaces]** **[Configuration] > [Device Setup] > [Interfaces] > [Add/Edit Bridge Group Interface][Configuration] > [Device Setup] > [Interfaces] > [Add/Edit Interface]**
拡張性機能	
ASA 5550、5580、および 5585-X でのコンテキストの増加	ASA 5550 および ASA 5585-X（SSP-10）では、コンテキストの最大数が 50 か き上げられました。ASA 5580 および 5585-X（SSP-20）以降では、コンテキス が 50 から 250 に引き上げられました。
ASA 5580 および 5585-X での VLAN 数の増加	ASA 5580 および ASA 5585-X では、VLAN の最大数が 250 から 1024 に引き上 た。

機能	説明
追加のプラットフォームサポート	ASA バージョン 8.4 のサポートされるプラットフォームとして Google Ch れました。32 ビットと 64 ビット両方のプラットフォームが Windows XP 7 と Mac OS X バージョン 6.0 でサポートされます。
ASA 5580 および 5585-X での接続数の増加	ファイアウォール接続の最大数が次のように引き上げられました。 • ASA 5580-20：1,000,000 から 2,000,000 へ。 • ASA 5580-40：2,000,000 から 4,000,000 へ。 • ASA 5585-X with SSP-10：750,000 から 1,000,000 へ。 • ASA 5585-X with SSP-20：1,000,000 から 2,000,000 へ。 • ASA 5585-X with SSP-40：2,000,000 から 4,000,000 へ。 • ASA 5585-X with SSP-60：2,000,000 から 10,000,000 へ。
ASA 5580 での AnyConnect VPN セッション数の増加	AnyConnect VPN セッションの最大数が 5,000 から 10,000 に引き上げられ
ASA 5580 での AnyConnect 以外の VPN セッション数の増加	AnyConnect 以外の VPN セッションの最大数が 5,000 から 10,000 に引き上
ハイ アベイラビリティ機能	
ダイナミック ルーティング プロトコルによるステートフル フェールオーバー	アクティブ装置上のダイナミック ルーティング プロトコル（OSPF や EIG して学習されたルートは、スタンバイ装置の Routing Information Base（R グ情報ベース）テーブルに保存されるようになりました。フェールオー 発生した場合、ルートがわかっているため、セカンダリ アクティブ装置 クは最小限の切断で通過します。ルートは、アクティブ装置上のリンク ンクダウン イベントの場合のみ同期されます。スタンバイ装置上でリン はダウンすると、アクティブ装置から送信されたダイナミック ルートが あります。これは正常な予期された動作です。 次のコマンドが変更されました。**show failover**、**show route**、**show route** 変更された画面はありません。
ユニファイド コミュニケーション機能	

機能	説明
Unified Communication Wizard への電話プロキシの追加	Unified Communications Wizard により、すべての設定が指示され、電話プロキ側面が自動的に設定されます。このウィザードにより、必要な TLS プロキシ作成されます。その後、ウィザードの指示に従って Phone Proxy インスタンス必要な証明書のインポートとインストールを行います。最後に、Phone Proxy クの SIP および SCCP インスペクションが自動的にイネーブルになります。 次の画面が変更されました。 **[Wizards] > [Unified Communications Wizard]** **[Configuration] > [Firewall] > [Unified Communications]**
UC プロトコル インスペクションの機能拡張	SIP インスペクションと SCCP インスペクションの機能拡張により、SCCP v2. SCCP インスペクションにおける GETPORT メッセージのサポート、SIP イン ンにおける INVITE メッセージの SDP フィールドのサポート、SIP 上での QS ングなど、ユニファイド コミュニケーション ソリューションの新機能をサポ す。さらに、Cisco Intercompany Media Engine は Cisco RT Lite 電話とサードパ オ エンドポイント（Tandberg など）もサポートします。 変更されたコマンドはありません。 変更された画面はありません。
インスペクション機能	
DCERPC の機能拡張	DCERPC インスペクションの機能拡張により、RemoteCreateInstance RPC メッ ンスペクションがサポートされます。 変更されたコマンドはありません。 変更された画面はありません。
トラブルシューティングとモニタリングの機能	

機能	説明
SNMP トラップと MIB	以下の追加のキーワードをサポートします。**connection-limit-reached**、**en** **cpu-temperature**、**cpu threshold rising**、**entity fan-failure**、**entity power-su** **ikev2 stop | start**、**interface-threshold**、**memory-threshold**、**nat packet-disc** entPhysicalTable によって、センサー、ファン、電源、および関連コンポ トリがレポートされます。 追加の MIB として、ENTITY-SENSOR-MIB、CISCO-ENTITY-SENSOR-E CISCO-ENTITY-FRU-CONTROL-MIB、CISCO-PROCESS-MIB、 CISCO-ENHANCED-MEMPOOL-MIB、CISCO-L4L7MODULE-RESOURCE NAT-MIB、EVENT-MIB、EXPRESSION-MIB をサポートします。 追加のトラップとして、warmstart、cpmCPURisingThreshold、mteTriggerF cirResourceLimitReached、natPacketDiscard、ciscoEntSensorExtThresholdNoti トします。 **snmp cpu threshold rising**、**snmp interface threshold**、**snmp-server enable** が導入または変更されました。 次の画面が変更されました。[Configuration] > [Device Management] > [Mar > [SNMP]
TCP ping の機能拡張	ICMP エコー要求がブロックされたユーザーは、TCP ping によって TCP で クできます。TCP ping の機能拡張により、ホスト名または IPv4 アドレス る送信元 IP アドレスおよびポートと送信元インターフェイスを指定でき 次のコマンドが変更されました。**ping tcp** 次の画面が変更されました。[Tools] > [Ping]
トップ CPU プロセスの表示	CPU 上で実行されているプロセスをモニタし、特定のプロセスの CPU 使 報を取得できるようになりました。CPU の負荷に関する情報も表示でき ごと、ログ時間の 5 分前、1 分前、および 5 秒前で表示できます。情報は されるため、リアルタイムの統計を確認できます。また、ペインには更新 ため、手動でいつでもデータを更新できます。 次のコマンドが導入されました。**show process cpu-usage sorted** 次の画面が導入されました。[Monitoring] > [Properties] > [CPU - Per Proces
一般的な機能	
パスワード暗号化の可視性	パスワードの暗号化をセキュリティ コンテキストで表示できます。 **show password encryption** コマンドを導入しました。 変更された画面はありません。
ASDM 機能	

機能	説明
ASDM アップグレードの機能拡張	互換性のない ASA ソフトウェア バージョンを持つデバイスに ASDM がロー 合、次のオプションから選択できることがダイアログボックスに表示されま • Cisco.com からイメージ バージョンをアップグレードする。 • ローカル ドライブからイメージ バージョンをアップグレードする。 • 互換性のない ASDM/ASA ペアを継続する（新しい選択肢）。 変更された画面はありません。 この機能は、すべての ASA バージョンと相互運用性があります。
ウィザードへの IKEv2 の実装	IKEv2 のサポートが AnyConnect VPN Wizard（以前の SSL VPN Wizard）、Cl VPN Wizard、および Site-to-Site IPsec VPN Wizard（以前の IPSec VPN Wizard れました。これは、連邦および公共部門の要求に定義された IPsec リモート 件に準拠するためです。新しいサポートによって、セキュリティの強化とと AnyConnect クライアント セッションで使用されるトンネリング プロトコルに 同じエンド ユーザー エクスペリエンスが提供されます。IKEv2 によって、他 の VPN クライアントも ASA に接続できます。 次のウィザードが変更されました。Site-to-Site IPsec VPN Wizard、AnyConnect V Clientless SSL VPN Wizard。
IPS Startup Wizard の機能拡張	ASA 5585-X の IPS SSP では、[IPS Basic Configuration] 画面が Startup Wizard に した。IPS SSP に対するシグニチャ アップデートが、[Auto Update] 画面に追 た。ASA でクロックが設定されるように、[Time Zone and Clock Configuration されました。IPS SSP モジュールはそのクロックを ASA から取得します。 次の画面が導入または変更されました。 [Wizards] > [Startup Wizard] > [IPS Ba Configuration] [Wizards] > [Startup Wizard] > [Auto Update] [Wizards] > [Startup Wi Zone and Clock Configuration]

バージョン 8.3 の新機能

ASA 8.3(2.25)/ASDM 6.4(5.106) の新機能

リリース：**2011年8月31日**

（注） 解決される特定の問題がある場合にだけ、Cisco.com にポストされた ASA 暫定リリースにアップグレードすることを推奨します。実稼働環境で暫定リリースを実行する場合は、暫定リリースでは対象のテストだけが実行されることに注意してください。暫定リリースは、TAC Web サイトによって十分にサポートされ、通常、次のメンテナンス リリースが使用可能になるまでの期間だけダウンロードサイトに残されます。暫定リリースを実行することを選択した場合、使用可能になったときに、完全にテストされたメンテナンス リリース、または機能リリースにアップグレードすることを強く推奨します。

次のメンテナンスまたは機能リリースの時点で暫定リリース機能についてマニュアルを作成します。各 ASA 暫定リリースの解決済みの警告のリストについては、Cisco.com のソフトウェア ダウンロード サイトから入手可能な暫定リリース ノートを参照してください。

機能	説明
リモート アクセス機能	
ブラウザでのクライアントレス SSL VPN のサポート	ASA は、Microsoft Internet Explorer 9 および Firefox 4 を使用してクライア VPN をサポートするようになりました。 バージョン *8.2(5.13)* および *8.4.2(8)* でも使用可能です。
DTLS および TLS における圧縮	スループットを向上させるため、シスコは AnyConnect 3.0 以降で DTLS サポートするようになりました。各トンネリング メソッドは個別に圧縮 優先設定は SSL と DTLS の両方の圧縮を LZS とすることです。この機能 クライアントからの移行を強化します。 （注） 高圧縮データを渡す高速リモート アクセス接続でデータ圧縮 は、ASA にかなりの処理能力が要求されます。ASA で他の活動 クがあると、プラットフォームでサポートできるセッションの 次のコマンドを導入または変更しました。**anyconnect dtls compression** [**lz** **anyconnect ssl compression** [**deflate** | **lzs** | **none**] 次の画面が変更されました。[Configuration] > [Remote Access VPN] > [Clie Access] > [Group Policies] > [Edit] > [Edit Internal Group Policy] > [Advanced] Client] > [SSL Compression] バージョン *8.2(5.13)* および *8.4.2(8)* でも使用可能です。
トラブルシューティング機能	

機能	説明
show asp table classifier および **show asp table filter** コマンドの正規表現照合	出力をフィルタするために、**show asp table classifier** と **show asp table filter** コ 規表現を使用して入力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。**show asp table classifier match** *regex*、**show a** **match** *regex* ASDM ではこのコマンドはサポートされません。コマンドライン ツールを使 ンドを入力してください。 バージョン *8.2(5.13)* および *8.4.2(8)* でも使用可能です。

ASA 8.3(2)/ASDM 6.3(2) の新機能

リリース：**2010年8月2日**

機能	説明
モニタリング機能	
拡張ロギングと接続ブロック	TCP を使用するように syslog サーバーを設定すると、syslog サーバーを使用 合、ASA はサーバーが再び使用可能になるまで syslog メッセージを生成する をブロックします（たとえば、VPN、ファイアウォール、カットスループロ この機能は、ASA のロギング キューがいっぱいのときにも新しい接続をブロ うに拡張されました。接続は、ロギング キューがクリアされると再開されま この機能は、Common Criteria EAL4+ への準拠のために追加されました。必要 り、syslog メッセージを送信できない場合でも新しい接続を許可することを指 新しい接続を許可するには、UDP を使用するように syslog サーバを設定する **logging permit-hostdown** コマンドを使用します。[Configuration] > [Device Ma [Logging] > [Syslog Servers] ペインで [Allow user traffic to pass when TCP syslog s チェックボックスをオンにします。 次のコマンドが変更されました。**show logging** 次の syslog メッセージが導入されました。414005、414006、414007、および 変更された ASDM 画面はありませんでした。

機能	説明
syslog メッセージのフィルタリングとソート	次のサポートが追加されました。 • さまざまなカラムに対応する複数のテキスト文字列に基づく syslog メルタリング。 • カスタム フィルタの作成。 • メッセージのカラムによるソート。詳細については、『ASDM 構成してください。 次の画面が変更されました。 **[Monitoring] > [Logging] > [Real-Time Log Viewer] > [View]** **[Monitoring] > [Logging] > [Log Buffer Viewer] > [View]** この機能は、すべての *ASA* バージョンと相互運用性があります。
CSC SSM の syslog メッセージのクリア	[Latest CSC Security Events] ペインで syslog メッセージをクリアするため加されました。 次の画面が変更されました。[Home] > [Content Security] この機能は、すべての *ASA* バージョンと相互運用性があります。
リモート アクセス機能	
2048 ビット RSA 証明書と Diffie-Hellman Group 5（DH5）のパフォーマンスの改善	（ASA 5510、ASA 5520、ASA 5540、および ASA 5550 のみ）2048 ビット DH5 キーなどの大規模なモジュラス演算には、ソフトウェアの代わりに理を有効にすることを強くお勧めします。サイズが大きいキーにソフト用し続ける場合は、IPsec と SSL VPN 接続の低速セッション確立により、スが大幅に低下することがあります。また、ソフトウェアからハードウ移行時に発生する可能性がある一時的なパケット損失を最小限に抑える が低い期間またはメンテナンス期間にまずハードウェア処理を有効にす ます。 （注） SSL VPN を使用する ASA 5540 と ASA 5550 の場合、特定の負 サイズが大きいキーのソフトウェア処理を使用し続けることが セッションが非常にゆっくりと追加され、ASA がフルで稼働 データ スループットへの悪影響はセッションの確立の積極的 くなります。 次のコマンドが導入または変更されました。**crypto engine large-mod-accel crypto engine**、**show running-config crypto engine**、および **show running-c** ASDM で、コマンドライン インターフェイス ツールを使用して、**crypto large-mod-accel** コマンドを入力します。 バージョン *8.2(3)* でも使用可能です。

機能	説明
Microsoft Internet Explorer プロキシのロックダウン制御	この機能をイネーブルにすると AnyConnect VPN セッションの間 Microsoft Int の接続タブが非表示になります。この機能をディセーブルにすると、[Conne の表示は変更されません。このタブのデフォルト設定は、ユーザーのレジス 応じて表示または非表示になります。 次のコマンドが導入されました。**msie-proxy lockdown** ASDM で、コマンドライン インターフェイス ツールを使用して、このコマン ます。 バージョン *8.2(3)* でも使用可能です。
セカンダリ パスワードの強化	すべての認証のために共通セカンダリ パスワードの SSL VPN サポートを設定 ライマリ パスワードをセカンダリ パスワードとして使用できるようになり 次のコマンドが変更されました。**secondary-pre-fill-username** [**use-primary-p** **use-common-password**]] 次の画面が変更されました。[Configuration] > [Remote Access VPN] > [Clientles > [Connection Profiles] > [Add/Edit Clientless SSL VPN Connection Profile] > [Ad [Secondary Authentication]
一般的な機能	

機能	説明
輸出用のペイロード暗号化なしイメージ	輸出先の国によっては、Cisco ASA 5500 シリーズでペイロード暗号化をイきません。バージョン 8.3(2) の場合、次のモデルにペイロード暗号化なし（asa832-npe-k8.bin）をインストールできるようになりました。 • ASA 5505 • ASA 5510 • ASA 5520 • ASA 5540 • ASA 5550 ペイロード暗号化なしイメージで無効にする機能には、次のものが含まれ • ユニファイド コミュニケーション。 • VPN のための強力な暗号化（DES 暗号化は引き続き VPN に利用可能 • VPN ロード バランシング（CLI GUI がまだ存在していることに注意ただし機能はしません）。 • ボットネット トラフィック ファイラの動的データベースのダウンロラック リストとホワイト リストは引き続きサポートされます。CLI していることに注意してください。ただし機能はしません）。 • SSL、SSHv2、SNMPv3 などの強力な暗号を必要とする管理プロトコ本の暗号化（DES）を使って SSL または SNMPv3 を使用できます。および SNMPv1 と v2 は引き続き使用できます。 強力な暗号化（3DES/AES）ライセンスをインストールしようとすると、されます。 `WARNING: Strong encryption types have been disabled in this image; the VPN-3DES-AES license option has been ignored.`

ASA 8.3(1)/ASDM 6.3(1) の新機能

リリース：**2010年3月8日**

機能	説明
リモート アクセス機能	

機能	説明
スマート トンネルの拡張機能	ログオフの拡張機能：すべてのブラウザ ウィンドウが閉じると、スマート ログオフできるようになりました（親アフィニティ）。あるいは、システム 知アイコンを右クリックすると、ログアウトを確認できます。 トンネル ポリシー：管理者は、VPN ゲートウェイを通過する接続と通過しな 定できます。管理者が許可すれば、エンドユーザーはスマート トンネルを使 リソースにアクセス中、直接インターネットをブラウズできます。 トンネリングするアプリケーションのコンフィギュレーションの簡素化：ス ネルが必要な場合、スマート トンネルにアクセスしてから特定の Web ページ するというプロセスのリストを設定する必要はありません。ブックマークま ドアロン アプリケーションの [enable smart tunnel] チェックボックスを使用す セスを簡単に設定できます。 グループ ポリシー ホーム ページ：管理者はスマート トンネル経由で接続で ASDM のチェックボックスを使用して、グループ ポリシーでホーム ページを ようになりました。 **smart-tunnel network** および **smart-tunnel tunnel-policy** コマンドが導入され 次の画面が変更されました。[Configuration] > [Remote Access VPN] > [AAA/L [Local Users] > [Edit] > [VPN Policy] > [Clientless SSL VPN]

機能	説明
ブラウザベース VPN で新しくサポートされるプラットフォーム	リリース 8.3(1) では、新しくサポートされる次のプラットフォームから、ス（クライアントレス）の VPN アクセスが可能です。 • Windows 7 x86（32 ビット）および x64（64 ビット）、Internet Explo Firefox 3.x 経由 • Windows Vista x64、Internet Explorer 7.x/8.x または Firefox 3.x 経由。 • Windows XP x64、Internet Explorer 6.x/7.x/8.x および Firefox 3.x 経由 • Mac OS 10.6.x 32 および 64 ビット、Safari 4.x および Firefox 3.x 経由 Firefox 2.x は、今後テストは実施されませんが、ほとんどの場合動作する す。 リリース 8.3(1) では、Mac OS 10.5 の 64 ビット アプリケーションに対し、スのサポートが導入されます。 リリース 8.3(1) は、ブラウザベースの VPN アクセスでサポートされるす トおよび 64 ビット Windows OS、Mac OS 10.5（Intel プロセッサで稼働中 および Mac OS 10.6.x 上で、スマート トンネル アクセスをサポートする。 た。ASA は、64 ビット OS 上でのポート転送をサポートしません。 ブラウザベースの VPN アクセスでは、Windows 7、Vista、および Internet Web フォルダはサポートされません。 RDP プラグインの ActiveX バージョンは、64 ビット ブラウザに使用でき （注） Windows 2000 および Mac OS X 10.4 のブラウザベース アクセス 対象外となりました。

機能	説明
IKEv1 LAN-to-LAN VPN 接続用の IPv6 サポート	IPv4 アドレッシングと IPv6 アドレッシングが混在した、またはすべて IPv6 ングの LAN-to-LAN 接続については、両方のピアが Cisco ASA 5500 シリーズ 合、および両方の内部ネットワークのアドレッシング方式が一致している場 IPv4 または両方が IPv6 の場合）は、ASA で VPN トンネルがサポートされま 具体的には、両方のピアが Cisco ASA 5500 シリーズ ASA の場合、次のトポロ トされます。 • ASA の内部ネットワークが IPv4 で、外部ネットワークが IPv6（内部イン ス上のアドレスが IPv4 で、外部インターフェイス上のアドレスが IPv6） • ASA の内部ネットワークが IPv6 で、外部ネットワークが IPv4（内部イン ス上のアドレスが IPv6 で、外部インターフェイス上のアドレスが IPv4） • ASA の内部ネットワークが IPv6 で、外部ネットワークが IPv6（内部およ ターフェイス上のアドレスが IPv6） （注） 現在 Cisco ASA 5500 シリーズは、CSCtd38078 の不具合より、I 接続の ピア デバイスとしての Cisco IOS デバイスに接続でき **isakmp enable**、**crypto map**、**crypto dynamic-map**、**tunnel-group**、**ipv6-vpn-f** **vpn-sessiondb**、**show crypto isakmp sa**、**show crypto ipsec sa**、**show crypto debug** **show debug crypto**、**show vpn-sessiondb**、**debug crypto condition**、**debug mem** マンドが変更または導入されました。 次の画面が変更または導入されました。 **[Wizards] > [IPsec VPN Wizard] >** **[Configuration] > [Site-to-Site VPN] > [Connection Profiles][Configuration] > [S** **VPN] > [Connection Profiles] > [Basic] > [Add IPsec Site-to-Site Connection Pro** **[Configuration] > [Site-to-Site VPN] > [Group Policies]** **[Configuration] > [Site-to-Site VPN] > [Group Policies] > [Edit Internal Group** **[Configuration] > [Site-to-Site VPN] > [Advanced] > [Crypto Maps]** **[Configuration] > [Site-to-Site VPN] > [Advanced] > [Crypto Maps] > [Add] > [** **Rule]** **[Configuration] > [Site-to-Site VPN] > [Advanced] > [ACL Manager]**

機能	説明
AnyConnect プロファイル エディタ用プラグイン	AnyConnect プロファイル エディタは、AnyConnect 2.5 またはそれ以降の ロファイル（クライアント機能を制御する設定が含まれる XML ファイル めに使用できる、便利な GUI ベースの設定ツールです。以前はプロファ ロファイル ファイル内の XML タグを編集して手動で変更することしか た。AnyConnect プロファイル エディタは、ASDM イメージとともにパッ いる anyconnectprof.sgz という名前のプラグイン バイナリ ファイルで、A シュ メモリのルート ディレクトリ disk0:/ にインストールされます。この いクライアントのリリースで利用できる新しい AnyConnect 機能と互換性 を更新できます。
SSL VPN ポータル カスタマイズ エディタ	ASDM の新しい [Edit Customization Object] ウィンドウを使用して、クライ ユーザーに表示される画面をブランド変更してカスタマイズできます。企 キスト メッセージ、および一般的なレイアウトを含む、ログオン、ポー グアウト画面をカスタマイズできます。以前は、ASA ソフトウェア イメ イズ機能が埋め込まれていました。ASDM に移行することで、この機能の 幅に使いやすくなります。 次の画面が変更されました。[Configuration] > [Remote Access VPN] > [Clie Access] > [Portal] > [Customization]
リモート アクセス VPN の使いやすさの向上	ASDM は、クライアントレス SSL VPN、AnyConnect SSL VPN リモート は ASDM アシスタントを使用する IPsec リモート アクセスを設定するた のガイドを提供しています。ASDM アシスタントは VPN ウィザードより り、利用開始のみを目的として設計されています。 次の画面が変更されました。[Configuration] > [Remote Access VPN] > [Introd Assistant]
ファイアウォール機能	
インターフェイスに依存しないアクセス ポリシー	1 つのインターフェイスに適用される規則のほか、グローバルに適用され を設定できるようになりました。コンフィギュレーションでグローバル シーとインターフェイス固有のアクセス ポリシーの両方が指定されている バル ポリシーの前にインターフェイス固有のポリシーがは評価されます。 **access-group global** コマンドが変更されました。 次の画面が変更されました。[Configuration] > [Firewall] > [Access Rules]

機能	説明
ネットワークおよびサービス オブジェクト	名前付きのネットワーク オブジェクトを作成し、ホスト、サブネット、また ス範囲の代わりにコンフィギュレーションで使用できるようになりました。 付きのサービス オブジェクトを作成し、プロトコルおよびポートの代わりに レーションで使用できるようになりました。オブジェクトの定義は、コンフ ションの他の部分を変更せずに、1 箇所だけを変更することができます。この は、次の機能でネットワークおよびサービス オブジェクトがサポートされま • NAT • アクセス リスト ルール • ネットワーク オブジェクト グループ （注） 以前のリリースでは、ASDM はネットワーク オブジェクトを 用するだけでした。この機能は、ネットワーク オブジェクト フォームのサポートを導入します。 **object network**、**object service**、**show running-config object**、**clear configure o** **access-list extended**、**object-group network** の各コマンドが変更または導入さ 次の画面が変更または導入されました。 **[Configuration] > [Firewall] > [Objects] > [Network Objects/Groups]** **[Configuration] > [Firewall] > [Objects] > [Service Objects/Groups]** **[Configuration] > [Firewall] > [NAT Rules]**、**[Configuration] > [Firewall] > [Ac**
オブジェクト グループ拡張規則の削減	パケット分類のパフォーマンスは十分なレベルで維持しつつ、ネットワーク ト グループの拡張は大幅に削減されました。 **show object-group**、**clear object-group**、**show access-list** の各コマンドが変更さ 次の画面が変更されました。[Configuration] > [Firewall] > [Access Rules] > [Ac
NAT の簡素化	NAT コンフィギュレーションは全面的に再設計され、柔軟性と使いやすさが た。自動 NAT を使用して NAT を設定すると、ネットワーク オブジェクトの として NAT を設定でき、手動 NAT を使用すると、より高度な NAT オプショ きるようになりました。 **nat**（グローバルおよびオブジェクト ネットワーク コンフィギュレーション **show nat**、**show nat pool**、**show xlate**、**show running-config nat** の各コマンド は変更されました。 **global**、**static**、**nat-control**、**alias** の各コマンドは削除されました。 次の画面が変更または導入されました。 **[Configuration] > [Firewall] > [Objects] > [Network Objects/Group] [Configura** **[Firewall] > [NAT Rules]**

機能	説明
アクセス リストでの変換後のアドレスに代わる実際の IP アドレスの使用	NAT を使用する場合、多数の機能を実現するために、アクセス リストで レスを使用する必要はなくなりました。次の機能を設定する場合は、常に ない実際のアドレスを使用します。実際のアドレスを使用するというこ フィギュレーションが変更された場合にアクセス リストを変更する必要 味します。 アクセス リストを使用する次のコマンドと機能では、今後は実際の IP ア れます。8.3 へのアップグレードを行うと、特に指定のない限り、これら IP アドレスを使用するよう自動的に移行されます。 • **access-group コマンド** アクセス ルール • モジュラ ポリシー フレームワーク **match access-list** コマンド サービス ル • ボットネット トラフィック フィルタの **dynamic-filter enable classify-** • AAA **aaa ... match** コマンド ルール • WCCP **wccp redirect-list group-list** コマンドのリダイレクト。 （注） WCCP は 8.3 へのアップグレード時に自動的に移行されま
脅威検出の拡張機能	高度な統計情報を収集するレート間隔の数値をカスタマイズできるよう デフォルトのレート数は、3 から 1 に変更されました。基本的な統計情報 報、およびスキャン脅威検出用に、メモリの使用方法が改善されました。 **threat-detection statistics port number-of-rates**、**threat-detection statistics p** **number-of-rates**、**show threat-detection memory** の各コマンドが変更され 次の画面が変更されました。[Configuration] > [Firewall] > [Threat Detection
ユニファイド コミュニケーション機能	
SCCP v19 のサポート	Cisco Phone Proxy 機能の IP フォン サポートが拡張され、サポート対象 IP に SCCP プロトコルのバージョン 19 のサポートが追加されました。

機能	説明
Cisco Intercompany Media Engine Proxy	Cisco Intercompany Media Engine（UC-IME）では、企業は VoIP テクノロジー現された高度な機能を使用して、インターネット上でオンデマンドの相互通す。Cisco Intercompany Media Engine では、ピアツーピア、セキュリティ、お ロトコルを使用してビジネス間にダイナミック SIP トランクを作成すること なる企業内の Cisco Unified Communications Manager クラスタの間で企業間フェ ンを実現できます。企業の集合は、最終的にそれらの間にクラスタ間トラン る 1 つの大きなビジネスであるかのように連携します。 **uc-ime**、**fallback hold-down**、**fallback monitoring**、**fallback sensitivity-file**、**ma listening-interface**、**media-termination**、**ticket epoch**、**ucm address**、**clear config debug uc-ime**、**show running-config uc-ime**、**inspect sip** の各コマンドが変更ま れました。 次の画面が変更または導入されました。 [Wizards] > [Unified Communications Wizard] > [Cisco Intercompany Media Engin Proxy][Configuration] > [Firewall] > [Unified Communications]、および [UC-IME リック [Configuration] > [Firewall] > [Service Policy Rules] > [Add/Edit Service P [Rule Actions] > [Select SIP Inspection Map]
IME 向けの SIP インスペクション サポート	SIP インスペクションが拡張され、新しい Cisco Intercompany Media Engine（ Proxy のサポートが追加されました。 **inspect sip** コマンドが変更されました。 次の画面が変更されました。[Configuration] > [Firewall] > [Service Policy Rules Service Policy Rule] > [Rule Actions] > [Select SIP Inspection Map]
Unified Communication Wizard	Unified Communications Wizard は、設定全体を手引きし、Cisco Mobility Adva シ、Cisco Presence Federation プロキシ、Cisco Intercompany Media Engine プロ な面を自動的に設定します。さらに、Unified Communications Wizard はプロキ 要な面を自動的に設定します。 次の画面が変更されました。 **[Wizards] > [Unified Communications Wizard]** **[Configuration] > [Firewall] > [Unified Communications]**
ユニファイドコミュニケーション機能の強化されたナビゲーション	[Phone Proxy]、[TLS Proxy]、[CTL File]、および [CTL Provider] ページなどの ド コミュニケーション プロキシ機能は、左側のナビゲーション パネルの [C ゴリの下から、新しい [Unified Communications] カテゴリに移動しました。さ 新しいカテゴリには、新しい Unified Communication Wizard と [UC-IME Proxy まれています。 この機能は、すべての *ASA* バージョンと相互運用性があります。
ルーティング機能	

機能	説明
ルート マップ サポート	ASDM により、スタティック ルートとダイナミック ルートのサポートが た。 次の画面が変更されました。[Configuration] > [Device Setup] > [Routing] > この機能は、すべての *ASA* バージョンと相互運用性があります。
モニタリング機能	
アクセスリストのヒット数のタイムスタンプ	指定されたアクセス リストについて、ハッシュ値とヒット数とともにタ 表示されます。 **show access-list** コマンドが変更されました。 次の画面が変更されました。[Configuration] > [Firewall] > [Access Rules] （ は、[Hit] 列のセル上にマウスを置くと表示されます）。
ASDM のハイ パフォーマンス モニタリング	ASDM のハイ パフォーマンス モニタリングをイネーブルにすると、ASA れたホストの上位 200 を表示できるようになりました。ホストの各エン トの IP アドレスと、ホストによって開始された接続の数が含まれ、この 秒ごとにアップデートされます。 **hpm topn enable**、**clear configure hpm**、および **show running-config hpm** 導入されました。 次の画面が導入されました。[Home] > [Firewall Dashboard] > [Top 200 Hos
ライセンシング機能	
同一でないフェールオーバー ライセンス	フェールオーバー ライセンスが各ユニット上で同一である必要がなくな のユニットで使用するライセンスは、プライマリ ユニットおよびセカン らの結合されたライセンスです。 （注） ASA 5505 および 5510 ASA では、両方の装置に Security Plus 要です。基本ライセンスはフェールオーバーをサポートしない イセンスのみを保持するスタンバイ装置ではフェールオーバー にできません。 **show activation-key** および **show version** の各コマンドが変更されました。 次の画面が変更されました。[Configuration] > [Device Management] > [Licens Key]

機能	説明
スタック可能な時間ベースライセンス	時間ベース ライセンスがスタッカブルになりました。多くの場合、時間ベースは更新の必要があり、旧ライセンスから新しいライセンスへシームレスに要があります。時間ベース ライセンスだけで使用される機能では、新しいラ適用される前に、ライセンスの有効期限が切れてしまわないことが特に重要では時間ベース ライセンスをスタックできるので、ライセンスの有効期限が新しいライセンスを早めにインストールしたために時間が無駄になったりすりません。数値ティアを持つライセンスの場合、スタックできるのは容量がンスだけです。たとえば、SSL VPN セッション数が 1000 である 2 つの ライタック可能です。ライセンスの状態を表示できます。これには show activatioドを [Configuration] > [Device Management] > [Licensing] > [Activation Key] で
Intercompany Media Engine ライセンス	IME ライセンスが導入されました。
稼働時間に基づいた時間ベース ライセンス	時間ベースライセンスでは、ASA の合計稼働時間に応じてカウントダウンしテム クロックはライセンスには影響しません。
複数の時間ベースライセンスの同時アクティブ化	時間ベース ライセンスを複数インストールできるようになり、同時に機能こアクティブなライセンスを保持できるようになりました。 **show activation-key** および **show version** の各コマンドが変更されました。 次の画面が変更されました。[Configuration] > [Device Management] > [Licensing Key]
時間ベースライセンスのアクティブ化と非アクティブ化の個別化	コマンドを使用して、時間ベース ライセンスをアクティブ化または非アクテるようになりました。 **activation-key** [**activate** | **deactivate**] コマンドが変更されました。 次の画面が変更されました。[Configuration] > [Device Management] > [Licensing Key]
一般的な機能	
マスター パスフレーズ	マスターパスフレーズ機能を利用すると、プレーンテキストパスワードを暗形式で安全に保存できます。この機能では、マスター キーを使用して、機能ことなく、すべてのパスワードを例外なく暗号化またはマスクできます。パ復元機能は、マスター パスフレーズをサポートします。 **key config-key password-encryption** および **password encryption aes** の各コマンれました。 次の画面が導入されました。 **[Configuration] > [Device Management] > [Advanced] > [Master Passphrase] [C > [Device Management] > [Device Administration] > [Master Passphrase]**
ASDM 機能	

機能	説明
Upgrade Software from Cisco.com Wizard	Upgrade Software from Cisco.com Wizard は変更され、ASDM と ASA をより ンに自動的にアップグレードできるようになりました。注意点として、 ングル モードでのみ使用できます。システム実行スペースでは複数のコ ドで使用できます。コンテキストでは使用できません。 次の画面が変更されました。[Tools] > [Check for ASA/ASDM Updates] この機能は、すべての *ASA* バージョンと相互運用性があります。
バックアップ/復元の機能拡張	[Backup Configurations] ペインが並べ替えられ、グループ編成が変更され より、バックアップするファイルをより簡単に選択できます。[Backup Pr 追加され、バックアップの進行状況を視覚的に測定できるようになりまし プまたは復元を使用するときにパフォーマンスが大幅に向上しているこ す。 次の画面が変更されました。[Tools] > [Backup Configurations] または [Too Configurations] この機能は、すべての *ASA* バージョンと相互運用性があります。

バージョン 8.2 の新機能

ASA 8.2(5.13)/ASDM 6.4(4.106) の新機能

リリース：**2011年9月18日**

（注） 解決される特定の問題がある場合にだけ、Cisco.com にポストされた ASA 暫定リリースにアップグレードすることを推奨します。実稼働環境で暫定リリースを実行する場合は、暫定リリースでは対象のテストだけが実行されることに注意してください。暫定リリースは、TAC Web サイトによって十分にサポートされ、通常、次のメンテナンス リリースが使用可能になるまでの期間だけダウンロードサイトに残されます。暫定リリースを実行することを選択した場合、使用可能になったときに、完全にテストされたメンテナンス リリース、または機能リリースにアップグレードすることを強く推奨します。

次のメンテナンスまたは機能リリースの時点で暫定リリース機能についてマニュアルを作成します。各 ASA 暫定リリースの解決済みの警告のリストについては、Cisco.com のソフトウェア ダウンロード サイトから入手可能な暫定リリース ノートを参照してください。

機能	説明
リモート アクセス機能	

機能	説明
ブラウザでのクライアントレス SSL VPN のサポート	ASA は、Microsoft Internet Explorer 9 および Firefox 4 を使用してクライアン VPN をサポートするようになりました。 バージョン *8.3(2.25)* および *8.4.2(8)* でも使用可能です。
DTLS および TLS における圧縮	スループットを向上させるため、シスコは AnyConnect 3.0 以降で DTLS と T サポートするようになりました。各トンネリング メソッドは個別に圧縮を構 優先設定は SSL と DTLS の両方の圧縮を LZS とすることです。この機能は、 クライアントからの移行を強化します。 （注） 高圧縮データを渡す高速リモート アクセス接続でデータ圧縮を使 は、ASA にかなりの処理能力が要求されます。ASA で他の活動や クがあると、プラットフォームでサポートできるセッションの数は 次のコマンドを導入または変更しました。**anyconnect dtls compression** [**lzs** | **n** **anyconnect ssl compression** [**deflate** | **lzs** | **none**] 次の画面が変更されました。[Configuration] > [Remote Access VPN] > [Clientle Access] > [Group Policies] > [Edit] > [Edit Internal Group Policy] > [Advanced] > [Client] > [SSL Compression] バージョン *8.3(2.25)* およびバージョン *8.4.2(8)* でも使用可能です。
トラブルシューティング機能	
show asp table classifier および **show asp table filter** コマンドの正規表現照合	出力をフィルタするために、**show asp table classifier** と **show asp table filter** コ 規表現を使用して入力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。**show asp table classifier match** *regex*、**show a** **match** *regex* ASDM ではこのコマンドはサポートされません。コマンドライン ツールを使 ンドを入力してください。 バージョン *8.3(2.25)* およびバージョン *8.4.2(8)* でも使用可能です。

ASA 8.2(5)/ASDM 6.4(3) の新機能

リリース：**2011 年 5 月 23 日**

機能	説明
モニタリング機能	

機能	説明
Smart Call-Home Anonymous Reporting	顧客は Anonymous Reporting をイネーブルにして、ASA プラットフォームを できるようになりました。Anonymous Reporting により、エラーおよびヘルス の情報をデバイスからシスコに安全に送信できます。 次のコマンドが導入されました。**call-home reporting anonymous**、**call-home** **anonymous** 次の画面が変更されました。[Configuration] > [Device Monitoring] > [Smart Cal バージョン *8.4(2)* でも使用可能です。
IF-MIB ifAlias OID のサポート	ASA は、ifAlias OID をサポートするようになりました。IF-MIB をブラウズ OID はインターフェイスの記述に設定済みの値に設定されます。 バージョン *8.4(2)* でも使用可能です。
リモート アクセス機能	
ポータル アクセス ルール	この拡張機能により、カスタマーは、HTTP ヘッダー内に存在するデータに イアントレス SSL VPN セッションを許可または拒否するグローバルなクライ VPN アクセス ポリシーを設定することができます。拒否された場合は、エラ ライアントに返されます。この拒否は、ユーザー認証の前に行われるため、 使用が最小限に抑えられます。 次のコマンドが変更されました。**portal-access-rule** 次の画面が変更されました。[Configuration] > [Remote Access VPN] > [Clientless > [Portal] > [Portal Access Rules] バージョン *8.4(2)* でも使用可能です。

機能	説明
Mobile Posture （以前の名称は AnyConnect Identification Extensions for Mobile Device Detection）	モバイル デバイスへの VPN 接続の許可または拒否、グループ単位でのモバイル クセスのイネーブル化またはディセーブル化、およびモバイルデバイスのポスチ 基づいた接続モバイル デバイスに関する情報の収集を実行するように ASA を設 うになりました。AnyConnect for iPhone/iPad/iPod バージョン 2.5.x および AnyConne バージョン 2.4.x の各モバイルプラットフォームでこの機能がサポートされてい でこれらの属性を設定するために CSD をイネーブルにする必要はありません。 ライセンス要件 リモート アクセス コントロールを適用し、モバイル デバイスからポスチャ デー るには、AnyConnect Mobile ライセンスと、AnyConnect Essentials または AnyCon ライセンスのいずれかが ASA にインストールされている必要があります。イン ライセンスに基づいて次の機能を受け取ります。 • **AnyConnect Premium ライセンス機能** AnyConnect Premium ライセンスをインストールする企業は、DAP 属性および他の ドポイント属性に基づいてサポートされているモバイル デバイスの DAP ポリシ きます。これには、モバイルデバイスからのリモートアクセスの許可または拒否 す。 • **AnyConnect Essentials ライセンス機能** AnyConnect Essentials ライセンスをインストールする企業は、次の操作を実行で • ASDM を使用してグループ単位でのモバイルデバイス アクセスをイネーブル セーブルにして、この機能を設定します。 • CLI または ASDM を使用して接続モバイル デバイスに関する情報を表示し し、DAP ポリシーを適用したり、これらのモバイル デバイスへのリモート 拒否/許可したりする機能はありません）。 次の画面が変更されました。[Configuration] > [Remote Access VPN] > [Network (C > [Dynamic Access Policies] > [Add/Edit Endpoint Attributes] > [Endpoint Attribute Type バージョン *8.4(2)* でも使用可能です。

機能	説明
AnyConnect 用のスプリット トンネル DNS ポリシー	このリリースには、スプリット トンネルを介して DNS アドレスを解決するた セキュア モビリティ クライアントにプッシュダウンされた新しいポリシーが す。このポリシーは、SSL プロトコルまたは IPsec/IKEv2 プロトコルを使用す 適用され、AnyConnect クライアントに対して VPN トンネルを経由するすべて スを解決するように指示します。DNS 解決に失敗すると、アドレスは未解決 す。AnyConnect Client は、パブリック DNS サーバー経由でアドレスを解決し ん。 デフォルトでは、この機能はディセーブルになっています。クライアントは ンネル ポリシーに従ってトンネル経由で DNS クエリーを送信します。ポリシ のネットワークをトンネリング、ネットワーク リストで指定されたネットワ ング、またはネットワーク リストで指定されたネットワークを除外です。 次のコマンドが導入されました。**split-tunnel-all-dns** 次の画面が変更されました。[Configuration] > [Remote Access VPN] > [Network > [Group Policies] > [Add/Edit Group Policy] > [Advanced] > [Split Tunneling]（[S Lookups Through Tunnel] チェックボックスを参照）。 バージョン *8.4(2)* でも使用可能です。
SSL SHA-2 デジタル署名	デジタル証明書を使用する SSL VPN 接続の認証における SHA-2 準拠の署名ア 使用できるようになりました。SHA-2 のサポートには、SHA-256、SHA-384、 の 3 つすべてのハッシュ サイズが含まれます。SHA-2 には AnyConnect 2.5(1) 降を推奨）が必要です。このリリースは、他の使用または製品では SHA-2 を ん。 注意：SHA-2 接続のフェールオーバーをサポートするためには、スタンバイ メージを実行している必要があります。 次のコマンドが変更されました。**show crypto ca certificate**（[Signature Algorit は、署名の生成時に使用されるダイジェスト アルゴリズムを識別します）。 変更された画面はありません。 バージョン *8.4(2)* でも使用可能です。
L2TP/IPsec による Android のサポート	L2TP/IPsec プロトコルとネイティブ Android VPN クライアントを使用する場 バイル デバイスと ASA 5500 シリーズ デバイスとの間の VPN 接続をサポー りました。モバイル デバイスで Android 2.1 以降のオペレーティング システ いる必要があります。 変更されたコマンドはありません。 変更された画面はありません。 バージョン *8.4(1)* でも使用可能です。

機能	説明
SHA2 証明書署名による Microsoft Windows 7 と Android ネイティブ VPN クライアントのサポート	ASA は、L2TP/IPsec プロトコルを使用する場合、Microsoft Windows 7 および An ティブ VPN クライアント用の SHA2 証明書署名サポートをサポートします。 変更されたコマンドはありません。 変更された画面はありません。 バージョン *8.4(2)* でも使用可能です。
group-url 属性をオーバーライドするための証明書のマッピングの有効化/無効化	この機能は、接続プロファイルの選択プロセス中に、接続プロファイルのプリフ 変更します。デフォルトでは、接続プロファイルで指定された証明書のフィール ドポイントで使用される証明書のフィールド値が ASA によって照合され、一致し そのプロファイルが VPN 接続に割り当てられます。このオプションの機能により イントが要求したグループ URL を指定する接続プロファイルに対するプリファレ されます。この新しいオプションにより、管理者は ASA ソフトウェアの数多くの によって使用されるグループ URL プリファレンスを利用できます。 次のコマンドが導入されました。**tunnel-group-preference**。 次の画面が変更されました。 **[Configuration] > [Remote Access VPN] > [Clientless SSL VPN] > [Connection Prof** **[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [AnyConnec Profiles]** バージョン *8.4(2)* でも使用可能です。
インターフェイス機能	
1 ギガビット イーサネット インターフェイスでのフロー制御のポーズ フレームのサポート	1 ギガビット イーサネット インターフェイスでのフロー制御用の停止（XOFF） 有効化できるようになりました。サポートは以前は 8.2(2) の 10 ギガビット イー ンターフェイス用に追加されていました。 **flowcontrol** コマンドが変更されました。 次の画面が変更されました。 （シングル モード）[Configuration] > [Device Setup] > [Interfaces] > [Add/Edit Interfac （マルチ モード、システム）[Configuration] > [Interfaces] > [Add/Edit Interface] バージョン *8.4(2)* でも使用可能です。
ユニファイド コミュニケーション機能	

機能	説明
ASA Tandberg と H.323 インスペクションとの相互運用性	H.323 インスペクションは、双方向ビデオ セッションの双方向信号をサポーりました。この機能拡張により、一方向のビデオ会議での H.323 インスペクシビデオ電話によってサポートされます。双方向信号をサポートすると、Tandオ モードを切り替えることができます（H.263 ビデオ セッションの側を閉じオの圧縮標準である H.264 を使用してセッションを再オープンします）。 変更されたコマンドはありません。 変更された画面はありません。 バージョン *8.4(2)* でも使用可能です。
ルーティング機能	
バックアップ スタティック ルートを使用する接続のタイムアウト	同じネットワークへの複数のスタティック ルートが存在しており、それぞれなる場合は、ASA は接続確立時点でメトリックが最良のルートを使用しますルートが使用可能になった場合は、このタイムアウトによって接続が閉じら適切なルートを使用して接続を再確立できます。デフォルトは 0 です（接続しません）。この機能を使用するには、タイムアウトを新しい値に変更しま **timeout floating-conn** コマンドが変更されました。 次の画面が変更されました。[Configuration] > [Firewall] > [Advanced] > [Global バージョン *8.4(2)* でも使用可能です。

ASA 8.2(4.4)/ASDM 6.3(5) の新機能

リリース：**2011年3月4日**

（注） 解決される特定の問題がある場合にだけ、Cisco.com にポストされた暫定リリースにアップグレードすることを推奨します。実稼働環境で暫定リリースを実行する場合は、暫定リリースでは対象のテストだけが実行されることに注意してください。暫定リリースは、TAC Web サイトによって十分にサポートされ、次のメンテナンス リリースが使用可能になるまでの期間だけダウンロードサイトに残されます。暫定リリースを実行することを選択した場合、使用可能になったときに、完全にテストされたメンテナンス リリース、または機能リリースにアップグレードすることを強く推奨します。次のメンテナンスまたは機能リリースの時点で暫定リリース機能についてマニュアルを作成します。各暫定リリースの解決済みの警告のリストについては、Cisco.com のソフトウェア ダウンロード サイトから入手可能な *Cisco ASA* 暫定リリースノートを参照してください。

機能	説明
ハードウェアの機能	

機能	説明
ASA 5585-X 対応の IPS SSP-10、-20、-40、および -60 のサポート	ASA 5585-X 用の IPS SSP-10、-20、-40、および -60 のサポートを導入しました。対応するレベルの SSP がある場合にのみインストールできます（たとえば SSP-SSP-10）。
リモート アクセス機能	
Outlook Web Access 2010 のクライアントレス SSL VPN サポート	デフォルトでは、クライアント SSL VPN は Outlook Web Access（OWA）2010 ト用のコンテンツ変換（リライト）サポートを提供するようになりました。 変更されたコマンドはありません。 変更された画面はありません。

ASA 8.2(4.1)/ASDM 6.3(5) の新機能

リリース：2011年1月18日

（注） 解決される特定の問題がある場合にだけ、Cisco.com にポストされた暫定リリースにアップグレードすることを推奨します。実稼働環境で暫定リリースを実行する場合は、暫定リリースでは対象のテストだけが実行されることに注意してください。暫定リリースは、TAC Web サイトによって十分にサポートされ、次のメンテナンスリリースが使用可能になるまでの期間だけダウンロードサイトに残されます。暫定リリースを実行することを選択した場合、使用可能になったときに、完全にテストされたメンテナンス リリース、または機能リリースにアップグレードすることを強く推奨します。次のメンテナンスまたは機能リリースの時点で暫定リリース機能についてマニュアルを作成します。各暫定リリースの解決済みの警告のリストについては、Cisco.com のソフトウェア ダウンロード サイトから入手可能な *Cisco ASA* 暫定リリースノートを参照してください。

機能	説明
リモート アクセス機能	
SSL SHA-2 デジタル署名	このリリースは、デジタル証明書を使用する SSL VPN 接続の認証における SHA 名アルゴリズムをサポートします。SHA-2 のサポートには、SHA-256、SHA-384 SHA-512 の 3 つすべてのハッシュ サイズが含まれます。SHA-2 には AnyConnec（2.5.2以降を推奨）が必要です。このリリースは、他の使用または製品では SH トしません。この機能にはコンフィギュレーションの変更はありません。注意 : のフェールオーバーをサポートするためには、スタンバイ ASA も同じイメージを る必要があります。この機能をサポートするために、**show crypto ca certificate** コ名の生成に使用されるダイジェスト アルゴリズムを指定する [Signature Algorithm ドを追加しました。

ASA 8.2(4)/ASDM 6.3(5) の新機能

リリース：**2010年12月15日**

機能	説明
ハードウェアの機能	
Cisco ASA 5585-X（SSP-10 および SSP-40 搭載）サポート	セキュリティ サービス プロセッサ（SSP）-10 および -40 を搭載した ASA 558 が導入されました。 （注） ASA 5585-X はバージョン 8.3(x) ではサポートされていません。

ASA 8.2(3.9)/ASDM 6.3(4) の新機能

リリース：**2010年11月2日**

（注） 解決される特定の問題がある場合にだけ、Cisco.com にポストされた暫定リリースにアップグレードすることを推奨します。実稼働環境で暫定リリースを実行する場合は、暫定リリースでは対象のテストだけが実行されることに注意してください。暫定リリースは、TAC Web サイトによって十分にサポートされ、次のメンテナンス リリースが使用可能になるまでの期間だけダウンロードサイトに残されます。暫定リリースを実行することを選択した場合、使用可能になったときに、完全にテストされたメンテナンス リリース、または機能リリースにアップグレードすることを強く推奨します。次のメンテナンスまたは機能リリースの時点で暫定リリース機能についてマニュアルを作成します。各暫定リリースの解決済みの警告のリストについては、Cisco.com のソフトウェア ダウンロード サイトから入手可能な *Cisco ASA* 暫定リリース ノートを参照してください。

機能	説明
リモート アクセス機能	
SSL SHA-2 デジタル署名	このリリースは、デジタル証明書を使用する SSL VPN 接続の認証における S 名アルゴリズムをサポートします。SHA-2 のサポートには、SHA-256、SHA- SHA-512 の 3 つすべてのハッシュ サイズが含まれます。SHA-2 には AnyCon （2.5.2 以降を推奨）が必要です。このリリースは、他の使用または製品では トしません。この機能にはコンフィギュレーションの変更はありません。注 のフェールオーバーをサポートするためには、スタンバイ ASA も同じイメー る必要があります。この機能をサポートするために、**show crypto ca certifica** 名の生成に使用されるダイジェスト アルゴリズムを指定する [Signature Algor ドを追加しました。

ASA 8.2(3)/ASDM 6.3(3) と 6.3(4) の新機能

リリース：**2010年8月9日**

（注） ASDM 6.3(4) には新しい機能は含まれていません。それには ASA 5585-X のサポートに必要な警告の修正が含まれています。

機能	説明
ハードウェアの機能	
Cisco ASA 5585-X（SSP-20 および SSP-60 搭載）サポート	セキュリティ サービス プロセッサ（SSP）-20 および -60 を搭載した ASA 5585-X が導入されました。 （注） ASA 5585-X はバージョン 8.3(x) ではサポートされていません。 ASA 5585-X には、ASDM の 6.3(4) が必要です。
リモート アクセス機能	
2048 ビット RSA 証明書と Diffie-Hellman Group 5（DH5）のパフォーマンスの改善	（ASA 5510、ASA 5520、ASA 5540、および ASA 5550 のみ）2048 ビット証明書キーなどの大規模なモジュラス演算には、ソフトウェアの代わりにハードウェアにすることを強くお勧めします。サイズが大きいキーにソフトウェア処理を使用合は、IPsec と SSL VPN 接続の低速セッション確立により、パフォーマンスが大ることがあります。また、ソフトウェアからハードウェアへの処理の移行時に発性がある一時的なパケット損失を最小限に抑えるために、使用率が低い期間またンス期間にまずハードウェア処理を有効にすることを推奨します。 （注） SSL VPN を使用する ASA 5540 と ASA 5550 の場合、特定の負荷条件ズが大きいキーのソフトウェア処理を使用し続けることができます。ションが非常にゆっくりと追加され、ASA がフルで稼働している場合スループットへの悪影響はセッションの確立の積極的な影響より大きす。 ASA 5580/5585-X プラットフォームには、この機能がすでに統合されしたがって、crypto engine コマンドは、これらのプラットフォームにません。 次のコマンドが導入または変更されました。**crypto engine large-mod-accel**、**clea crypto engine**、**show running-config crypto engine**、および **show running-config cr** ASDM で、コマンドライン インターフェイス ツールを使用して、**crypto engine lar** コマンドを入力します。 バージョン *8.3(2)* でも使用可能です。

機能	説明
Microsoft Internet Explorerプロキシのロックダウン制御	この機能をイネーブルにすると AnyConnect VPN セッションの間 Microsoft Int 接続タブが非表示になります。この機能をディセーブルにすると、[Connectio は変更されません。このタブのデフォルト設定は、ユーザーのレジストリ設 または非表示になります。 次のコマンドが導入されました。**msie-proxy lockdown** ASDM で、コマンドライン インターフェイス ツールを使用して、このコマン す。
信頼できるネットワーク検出の一時停止と再開	この機能により、AnyConnect クライアントはセッション情報と cookie を保持 ンがアイドル タイマーの設定時間を超えない限り、ユーザーが退社しても接 に復元することができます。この機能には、TND の一時停止と再開をサポー AnyConnect リリースが必要です。

ASA 8.2(2)/ASDM 6.2(5) の新機能

リリース：**2010年1月11日**

機能	説明
リモート アクセス機能	
VPN セッションのレジューム待機のスケーラブル ソリューション	管理者は、アクティブ状態のユーザー数をトレースし、統計情報を確認でき した。ライセンス キャパシティに到達せず、新規ユーザーがログインできる 間非アクティブなセッションはアイドルとマークされます（さらに自動的に す）。 次の画面が変更されました。[Monitoring] > [VPN] > [VPN Statistics] > [Sessions バージョン *8.0(5)* でも使用可能です。
アプリケーション インスペクション機能	

機能	説明
IP オプションのインスペクション	特定の IP オプションを持つどの IP パケットに ASA の通過を許可できるかを設定 になりました。IP パケットの IP オプションをクリアして、ASA の通過を許可す きます。以前は、すべての IP オプションは、いくつかの特別な場合を除いて、デ は拒否されていました。 （注） このインスペクションはデフォルトでイネーブルになっています。次 がデフォルトのグローバル サービス ポリシーに追加されました。**inspe** したがって、ASA がルーテッド モードの場合、その ASA はパケット Alert オプション（option 20）が含まれた RSVP トラフィックを許可し 次のコマンドが導入されました。**policy-map type inspect ip-options**、**inspect ip-opt** **nop** 次の画面が導入されました。 **[Configuration] > [Firewall] > [Objects] > [Inspect Maps] > [IP-Options]** **[Configuration] > [Firewall] > [Service Policy] > [Add/Edit Service Policy Rule] > [P** **> [Protocol Inspection]**
H.323 エンドポイント間のコール設定のイネーブル化	Gatekeeper がネットワーク内にある場合は、H.323 エンドポイント間のコール セ をイネーブルにできます。ASA には、RegistrationRequest/RegistrationConfirm（R メッセージに基づいてコールのピンホールを開くオプションが含まれています。 これらの RRQ/RCF メッセージはゲートキーパーとの間で送信されるため、コー ポイント IP アドレスは不明であり、ASA は送信元 IP アドレス/ポート 0/0 を通し ルを開けます。デフォルトでは、このオプションは無効になっています。 次のコマンドが導入されました。**ras-rcf-pinholes enable**（**policy-map type inspect parameters** コマンドの下） 次の画面が変更されました。[Configuration] > [Firewall] > [Objects] > [Inspect Maps [Details] > [State Checking] バージョン *8.0(5)* でも使用可能です。
ユニファイド コミュニケーション機能	
モビリティ プロキシ アプリケーションでの Unified Communications Proxy ライセンス不要化	モビリティ プロキシに UC Proxy ライセンスが必要なくなりました。
インターフェイス機能	

機能	説明
マルチ コンテキスト モードでは、自動生成 MAC アドレスでユーザー設定可能プレフィックスやその他の拡張を使用	MAC アドレス形式は、プレフィックスの使用、固定開始値（A2）の使用、オーバー ペアでプライマリ装置とセカンダリ装置の MAC アドレスに対しての使用が可能になるように変更されました。 MAC アドレスは現在、リロード間で持続されるようになっています。 コマンドパーサーは現在、自動生成がイネーブルになっているかどうかをチMAC アドレスを手動でも割り当てることができるようにする場合は、A2 をアドレスは開始できません。 コマンド **mac-address auto prefix** *prefix* が変更されました。 次の画面が変更されました。[Configuration] > [Context Management] > [Security バージョン *8.0(5)* でも使用可能です。
ASA 5580 10 ギガビット イーサネット インターフェイスでのフロー制御のポーズ フレームのサポート	フロー制御のポーズ（XOFF）フレームをイネーブルにできるようになりまし **flowcontrol** コマンドが導入されました。 次の画面が変更されました。 （シングル モード）[Configuration] > [Device Setup] > [Interfaces] > [Add/Edit Inte （マルチモード、システム）**[設定（Configuration）] > [インターフェイス（ [インターフェイスを追加または編集（Add/Edit Interface）]**
ファイアウォール機能	
ボットネット トラフィック フィルタの機能拡張	ボットネットトラフィックフィルタでは、脅威レベルに基づいた、ブラックれているトラフィックの自動ブロッキングがサポートされるようになりましよびレポートで、マルウェアサイトのカテゴリおよび脅威レベルも表示でき は、感染したホストを表示するように拡張されました。上位ホストに対する間タイムアウトが削除され、タイムアウトがなくなりました。 **dynamic-filter ambiguous-is-black**、**dynamic-filter drop blacklist**、**show dynamic- show dynamic-filter reports infected-hosts**、および **show dynamic-filter reports** 導入または変更されました。 次の画面が導入または変更されました。 **[Configuration] > [Firewall] > [Botnet Traffic Filter] > [Traffic Settings] [Monito Traffic Filter] > [Infected Hosts]**
すべてのプロトコルの接続タイムアウト	アイドルタイムアウトは、TCP だけでなく、すべてのプロトコルに適用する ました。 次のコマンドが変更されました。**set connection timeout** 次の画面が変更されました。[Configuration] > [Firewall] > [Service Policies] > [[Connection Settings]
ルーティング機能	

機能	説明
ルーティング問題を解決するための DHCP RFC 互換性（rfc3011、rfc3527）	この拡張では、DHCP RFCs 3011（IPv4 サブネット選択オプション）および 3527 エージェント情報オプションのリンク選択サブオプション）の ASA サポートが導 た。VPN クライアント用に設定された DHCP サーバごとに、ASA を設定して [Sub オプションまたは [Link Selection] オプションを送信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。**dhcp-server** [**subnet-selection** | **link-selection]** 次の画面が変更されました。[Remote Access VPN] > [Network Access] > [IPsec conne > [Add/Edit] バージョン *8.0(5)* でも使用可能です。
ハイ アベイラビリティ機能	
フェールオーバー コンフィギュレーションでの IPv6 サポート	IPv6 はフェールオーバー設定をサポートするようになりました。アクティブとス IPv6 アドレスをインターフェイスに割り当て、フェールオーバーとステートフル オーバー インターフェイスに IPv6 アドレスを使用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。**failover interface ip**、**ipv6 address** 次の画面が変更されました。 **[Configuration] > [Device Management] > [High Availability] > [Failover] > [Setup]** **[Configuration] > [Device Management] > [High Availability] > [Failover] > [Interfa** **[Configuration] > [Device Management] > [High Availability] > [HA/Scalability Wiz**
スイッチオーバー イベント中のインターフェイスのアップまたはダウン時に通知なし	通常動作時のリンク アップおよびリンク ダウン遷移と、フェールオーバー中の プ/ダウン遷移を区別するために、フェールオーバー中にリンク アップトラップま ダウン トラップは送信されません。また、フェールオーバー中のリンク アップお 遷移に関する syslog メッセージも送信されません。 バージョン *8.0(5)* でも使用可能です。
AAA 機能	
100 AAA サーバ グループ	最大で 100 の AAA サーバ グループを設定できるようになりました。以前の制限 バ グループでした。 次のコマンドが変更されました。**aaa-server** 次の画面が変更されました。[Configuration] > [Device Management] > [Users/AAA] > Groups]
モニタリング機能	

機能	説明
Smart Call Home	Smart Call Home は、ASA に関する予防的診断およびリアルタイム アラートを トワークの可用性および運用効率を向上させます。顧客と TAC エンジニアは れたときに問題を迅速に解決するために必要なものを入手できます。 （注） Smart Call Home サーバ バージョン 3.0(1) には、ASA の限定サポー 詳細については、「Important Notes」を参照してください。 次のコマンドが導入されました。**call-home**、**call-home send alert-group**、**call** **call-home send**、**service call-home**、**show call-home**、**show call-home registered** 次の画面が導入されました。[Configuration] > [Device Management] > [Smart C

ASA 8.2(1)/ASDM 6.2(1) の新機能

リリース：**2009年5月6日**

Hi

機能	説明
リモート アクセス機能	
ASDM 認証のワンタイム パスワード サポート	ASDM では現在、RSA SecurID（SDI）でサポートされているワンタイム パス を使用して管理者認証がサポートされています。この機能は、スタティック 証している管理者に関するセキュリティ上の問題に対処します。 ASDM ユーザー向けの新しいセッション コントロールには、セッション時間 を制限する機能が搭載されています。ASDM 管理者が使用するパスワードが なると、ASDM により管理者の再認証を求めるプロンプトが表示されます。 **http server idle-timeout** および **http server session-timeout** というコマンドが導 **http server idle-timeout** のデフォルト値は 20 分で、1440 分まで増やすことが ASDM で [Configuration] > [Device Management] > [Management Access] > [ASDM/HTTPD/Telnet/SSH] を参照してください。
Secure Desktop のカスタマイズ	ASDM を使用して、Secure Desktop バックグラウンド（ロック アイコン）と ラー、および Desktop、Cache Cleaner、Keystroke Logger、Close Secure Deskto ウのダイアログ バナーなど、リモート ユーザーに表示される Secure Desktop スタマイズできます。 ASDM で [Configuration] > [CSD Manager] > [Secure Desktop Manager] を参照し

機能	説明
証明書からのユーザー名事前入力	ユーザー名事前入力機能により、ユーザー名およびパスワード認証をする場合に ら抽出されたユーザー名の使用がイネーブルになります。この機能がイネーブル グイン画面でユーザー名が「あらかじめ入力されて」おり、ユーザーはパスワー け求められます。この機能を使用するには、**pre-fill username** コマンドおよび **username-from-certificate** コマンドの両方をトンネルグループ コンフィギュレー ドで設定する必要があります。 ユーザー名事前入力機能は、ユーザ名が 2 つ必要な場合に、二重認証のユーザー 明書からプライマリ ユーザー名とセカンダリ ユーザー名を抽出する機能をサポー ため、二重認証機能はユーザー名事前入力機能と互換性があります。二重認証の ザー名事前入力機能を設定する場合、管理者は次の新しいトンネルグループ汎用属 ギュレーション モード コマンドを使用します。 • **secondary-pre-fill-username**：クライアントレスまたは AnyConnect クライア ユーザー名抽出をイネーブルにします。 • **secondary-username-from-certificate**：ユーザー名として使用するため、証明 つかの標準 DN フィールドを抽出できるようにします。 ASDM で、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [An Clienltess SSL VPN Connection Profiles] > [Advanced] を参照してください。設定は [Authentication]、[Secondary Authentication]、および [Authorization] の各ペインに表 ます。

機能	説明
二重認証	二重認証機能では、Payment Card Industry Standards Council Data Security Stand ネットワークへのリモート アクセスに対して 2 つの要素からなる認証を実行 能では、ユーザーはログイン ページで異なる 2 組のログイン クレデンシャル があります。たとえば、プライマリ認証をワンタイム パスワード、セカンダ ン（Active Directory）クレデンシャルとする場合が考えられます。いずれかの ると、接続が拒否されます。 AnyConnect VPN クライアントおよびクライアントレス SSL VPN の両方で二 トされています。AnyConnect クライアントでは、Windows コンピュータ（サ Windows Mobile 装置および Start Before Logon など）、Mac コンピュータ、お ピュータで二重認証がサポートされています。IPsec VPN クライアント、SVC カットスループロキシ認証、ハードウェア クライアント認証、および管理認 はサポートされていません。 二重認証には、次の新しいトンネルグループ汎用属性コンフィギュレーショ ドが必要です。 • **secondary-authentication-server-group**：SDI サーバ グループになること ンダリ AAA サーバ グループを指定します。 • **secondary-username-from-certificate**：ユーザー名として使用するため、 つかの標準 DN フィールドを抽出できるようにします。 • **secondary-pre-fill-username**：クライアントレス接続または AnyConnect ク 続において、ユーザー名抽出をイネーブルにします。 • **authentication-attr-from-server**：どの認証サーバ認可属性が接続に適用さ ます。 • **authenticated-session-username**：どの認証ユーザー名がセッションに関連 るかを指定します。 （注） RSA/SDI 認証サーバ タイプは、セカンダリ ユーザー名および レデンシャルとして使用できません。これはプライマリ認証に ます。 ASDM で、[Configuration] > [Remote Access VPN] > [Network (Client) Access or VPN] > [AnyConnect Connection Profiles] > [Add/Edit] > [Advanced] > [Secondary を参照してください。

機能	説明
AnyConnect Essentials	AnyConnect Essentials は、別途ライセンス付与される SSL VPN クライアントです で設定され、以下を除く AnyConnect の全機能を提供します。 • CSD を使用できない（HostScan/Vault/Cache Cleaner を含む） • クライアントレス SSL VPN 非対応 • Windows Mobile サポートがオプション AnyConnect Essentials クライアントは、Microsoft Windows Vista、Windows Mobile XP、Windows 2000、Linux、または Macintosh OS X を実行しているリモート エン に Cisco SSL VPN Client の利点をもたらします。 AnyConnect Essentials を設定する場合、管理者は次のコマンドを使用します。 **anyconnect-essentials**：AnyConnect Essentials 機能をイネーブルにします。この機 コマンドの **no** 形式を使用して）ディセーブルになった場合、SSL プレミアム ラ 使用されます。この機能は、デフォルトでイネーブルにされています。 （注） このライセンスは、共有されている SSL VPN プレミアム ライセンス 用できません。 ASDM で、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Ac [AnyConnect Essentials License] を参照してください。このペインを表示するため AnyConnect Essentials ライセンスをインストールする必要があります。
接続プロファイル単位の Cisco Secure Desktop のディセーブル	Cisco Secure Desktop は、イネーブルになっている場合、自動的にすべてのコン 行され、ASA への SSL VPN 接続を行います。この新機能により、接続プロファ あるユーザーが Cisco Secure Desktop を実行しないようにできます。この機能に のセッションのエンドポイント属性が検出されなくなるため、ダイナミック ア シー（DAP）コンフィギュレーションを調整しなければならない場合があります CLI：[**no**] **without-csd** コマンド （注） ASDM の「接続プロファイル」は CLI で「トンネル グループ」とも ます。また、**group-url** コマンドはこの機能に必要です。SSL VPN セ 接続エイリアスが使用されている場合、この機能は有効になりません ASDM で、[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > Profiles] > [Add or Edit] > [Advanced, Clientless SSL VPN Configuration] または [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [AnyConnect C Profiles] > [Add or Edit] > [Advanced] > [SSL VPN] を参照してください。

機能	説明
接続プロファイルごとの証明書認証	以前のバージョンは、ASAインターフェイスごとに証明書認証をサポートし 明書が必要ない場合でもユーザーは証明書を要求されていました。この新機 ザーは、接続プロファイルコンフィギュレーションで証明書が必要な場合だ されます。この機能は自動的に実行されるため、**ssl certificate authentication** なくなりましたが、ASA では下位互換性を考え、このコマンドは保持されて ASDM で、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > Connection Profiles] > [Add/Edit] > [Basic] または [Configuration] > [Remote Access VPN] > [Clientless SSL VPN] > [Connection Prof > [Basic] を参照してください。
証明書マッピング向け EKU 拡張機能	この機能では、クライアント証明書の Extended Key Usage 拡張機能を確認し 使用してクライアントでどの接続プロファイルを使用するべきか判断する、 作成する機能が追加されています。クライアントがそのプロファイルに一致 フォルトグループが使用されます。証明書が有効かどうか、また接続プロフ 定により、接続結果が異なります。 **extended-key-usage** というコマンドが導入されました。 ASDM で、[IPSec Certificate to Connection Maps] > [Rules] ペイン、または [Cer VPN Connections Profile Maps] ペインを使用してください。
Win 2007 Server の SSL VPN SharePoint サポート	クライアントレス SSL VPN セッションでは現在 Microsoft Office SharePoint Se ポートされています。
SSL VPN セッションの共有ライセンス	多数の SSL VPN セッションに対する共有ライセンスを購入し、ASA の 1 つを ス サーバ、残りをクライアントに設定することで、ASA のグループ間で必要 ションを共有できます。 **license-server** コマンド（各種）、**show shared licens** 入されました。 （注） このライセンスは、AnyConnect Essentials ライセンスと同時には使 ASDM で、[Configuration] > [Device Management] > [Licensing] > [Shared SSL V 参照してください。[Monitoring] > [VPN] > [Clientless SSL VPN] > [Shared Licen ください。
更新された VPN ウィザード	VPN ウィザード（[Wizards] > [IPSec VPN Wizard] を選択してアクセス可能） た。IPsec 暗号化と認証（以前の手順 11 の 9）を選択する手順は、ウィザー 定のデフォルト値を生成するようになったために削除されました。さらに、I プション）を選択する手順には、Perfect Forward Secrecy（PFS）を有効にして Group を設定するための新しいフィールドが含まれるようになりました。
ファイアウォール機能	

機能	説明
TCP ステート バイパス	アップストリーム ルータに非対称ルーティングが設定されており、トラフィッ ASA を通過することがある場合は、特定のトラフィックに対して TCP ステート 設定できます。**set connection advanced tcp-state-bypass** コマンドが導入されまし ASDM で、[Configuration] > [Firewall] > [Service Policy Rules] > [Rule Actions] > [C Settings] を参照してください。
Phone Proxy で使用されるメディア終端インスタンスのインターフェイス単位の IP アドレス	バージョン 8.0（4）では、ASA にグローバル メディア終端アドレス（MTA）を ました。バージョン 8.2 では、インターフェイス別に MTA を設定できるように （最低MTA数は2個）。この機能拡張の結果、旧型CLIは廃止されました。必要 引き続き古いコンフィギュレーションを使用できます。ただし、コンフィギュレ 変更する必要がある場合、新しいコンフィギュレーション方式だけが受け付けら いコンフィギュレーションは復元できません。 ASDM で、[Configuration] > [Firewall] > [Advanced] > [Encrypted Traffic Inspection] Termination Address] を参照してください。
Phone Proxy の CTL ファイルの表示	Cisco Phone Proxy 機能には、Phone Proxy で使用される CTL ファイルを表示する コマンドが含まれています。**show ctl-file** コマンドを使用すると、電話プロキシ スの設定時のデバッグに役立ちます。 このコマンドは ASDM ではサポートされていません。
Phone Proxy データベースからのセキュアフォン エントリのクリア	Cisco Phone Proxy 機能には、Phone Proxy データベースのセキュアフォン エントリ る **clear phone-proxy secure-phones** コマンドが含まれています。セキュア IP 電話 時に必ず CTL ファイルが要求されるため、Phone Proxy により IP 電話をセキュア るデータベースが作成されます。セキュア フォンデータベースのエントリは、設 定タイムアウト後に（**timeout secure-phones** コマンドを介して）削除されます。 **clear phone-proxy secure-phones** コマンドを使用して、設定したタイムアウトを待 Proxy データベースをクリアできます。 このコマンドは ASDM ではサポートされていません。
H.323 アプリケーション インスペクションでの H.239 メッセージ サポート	このリリースでは、ASA では H.323 アプリケーション インスペクションの一部 規格がサポートされています。H.239 は、H.300 シリーズ エンドポイントが 1 回 追加ビデオ チャネルを開くことができる機能を提供する規格です。コールで、エ ト（ビデオ電話など）はビデオ用チャネルとデータ プレゼンテーション用チャネ ます。H.239 ネゴシエーションは H.245 チャネルで発生します。ASA により、追 チャネルのピンホールが開きます。エンドポイントは、オープン論理チャネル メ （OLC）を使用して新しいチャネルの作成を通知します。メッセージ拡張は H.2 ン 13 の一部です。テレプレゼンテーション セッションの復号化と符号化は、デ イネーブルにされています。H.239 の符号化と復号化は ASN.1 コーダによって実行 ASDM で、[Configuration] > [Firewall] > [Service Policy Rules] > [Add Service Policy > [Rule Actions] > [Protocol Inspection] > [H.323 H.225] を参照してください。[Con リックし、H.323 Inspect Map を選択します。

機能	説明
エンドポイントから OLCAck が送信されない場合の H.323 エンドポイントの処理	H.323 アプリケーション インスペクションが、一般的な H.323 エンドポイントう機能拡張されました。機能拡張は、H.239 プロトコル識別情報を持つ extende OLC を使用しているエンドポイントに影響を与えます。ピアから OLC メッ H.323 エンドポイントから OLCAck が送信されない場合でも、ASA により O 案情報がメディア アレイに登録され、（extendedVideoCapability）メディア ホールが開きます。 ASDM で、[Configuration] > [Firewall] > [Service Policy Rules] > [Add Service Po > [Rule Actions] > [Protocol Inspection] > [H.323 H.225] を参照してください。
トランスペアレント ファイアウォール モードの IPv6	トランスペアレント ファイアウォール モードは現在 IPv6 ルーティングに参 このリリース以前は、ASA はトランスペアレント モードでは IPv6 トラフィ んでした。現在では、IPv6 管理アドレスをトランスペアレント モードで設定 ス リストを作成し、ASA により IPv6 パケットが認識され、渡されるなど、 能を設定できます。 特に指定がない限り、すべての IPv6 機能がサポートされています。 ASDM で、[Configuration] > [Device Management] > [Management Access] > [Ma Address] を参照してください。
Botnet Traffic Filter	マルウェアとは、知らないうちにホストにインストールされている悪意のあ です。個人情報（パスワード、クレジット カード番号、キー ストローク、ま タ）の送信などのネットワーク アクティビティを試みるマルウェアは、マル 不正な IP アドレスへの接続を開始したときにボットネット トラフィック フ 検出できます。Botnet Traffic Filter は、悪意のある既知のドメイン名および I む動的データベースと、着信接続および発信接続とを照合して、疑わしいア すべてログに記録します。また、ローカルの「ブラックリスト」または「ホ に IP アドレスやドメイン名を入力して、スタティック データベースでダイ ベースを補完できます。 （注） この機能には、ボットネット トラフィック フィルタ ライセンス 細については、次のライセンス マニュアルを参照してください。 http://www.cisco.com/en/US/docs/security/asa/asa82/license/license82.h **dynamic-filter** コマンド（各種）および **inspect dns dynamic-filter-snoop** キー れました。 ASDM で、[Configuration] > [Firewall] > [Botnet Traffic Filter] を参照してくだ
ASA 5505 の AIP SSC カード	AIP SSC で ASA 5505 ASA の IPS が提供されます。AIP SSM では仮想センサ れていない点に注意してください。**allow-ssc-mgmt**、**hw-module module ip**、お **module allow-ip** コマンドが導入されました。 ASDM で、[Configuration] > [Device Setup] > [SSC Setup] および [Configuration] してください。

機能	説明
IPS の IPv6 サポート	トラフィック クラスで **match any** コマンドを使用し、ポリシー マップで **ips** コマ されている場合に、IPv6 トラフィックを AIP SSM または SSC に送信できるよう た。 ASDM で、[Configuration] > [Firewall] > [Service Policy Rules] を参照してくださ
管理機能	
SNMP バージョン 3 および暗号化	このリリースでは、DES 暗号化、3DES 暗号化、または AES 暗号化、およびサポ いるセキュリティ モデルの中でも最もセキュアな形式である SNMP バージョン 3 しています。このバージョンにより、User-based Security Model（USM）を使用し を設定できます。 次のコマンドが導入されました。 • **show snmp engineid** • **show snmp group** • **show snmp-server group** • **show snmp-server user** • **snmp-server group** • **snmp-server user** 次のコマンドが変更されました。 • **snmp-server host** ASDM で、[Configuration] > [Device Management] > [Management Access] > [SNMP ください。
NetFlow	この機能は、ASA 5580 用にバージョン 8.1(1) で導入されました。この機能はこの によって他のプラットフォームに導入されます。新しい NetFlow 機能では ASA の 能を拡張し、NetFlow プロトコルを介したフローベースのイベントをロギングし ASDM では、**[Configuration] > [Device Management] > [Logging] > [Netflow]** を参 さい。
ルーティング機能	
マルチキャスト NAT	ASA で、グループ アドレスのマルチキャスト NAT がサポートされるようにな
トラブルシューティング機能	

機能	説明
コアダンプ機能	コアダンプは、プログラムが異常終了したときの実行中プログラムのスナップ コアダンプは、エラーを診断またはデバッグし、後でまたはサイト外で分析す シュを保存する場合に使用します。Cisco TAC では、ユーザーがコアダンプ ルにして、ASA でのアプリケーションまたはシステムのクラッシュをトラブ グする必要がある場合があります。 コアダンプをイネーブルにする方法について、**coredump enable** コマンドを参 い。
ASDM 機能	
IPv6 用の ASDM のサポート	特に指定がない限り、すべての IPv6 機能がサポートされています。
公開サーバ コンフィギュレーションのサポート	ASDM を使用して公開サーバを設定できます。これにより、外部インターフ るサーバおよびサービスを定義できます。 ASDM で、[Configuration] > [Firewall] > [Public Servers] を参照してください。

バージョン 8.1 の新機能

ASA 8.1(2)/ASDM 6.1(5) の新機能

リリース：**2008年10月10日**

機能	説明
リモート アクセス機能	

機能	説明
IE 用スマート トンネルを使用した自動サインオン	この機能を使用すると、WININET 接続のためのログイン クレデンシャルの代替ります。Internet Explorer を含め、ほとんどの Microsoft 製アプリケーションは W用しています。Mozilla Firefox は WININET を使用していないため、この機能でサません。また、HTTP ベースの認証もサポートされるため、フォームベースの認能とともに使用できません。 クレデンシャルは、サービスではなく宛先ホストに静的に関連付けられるため、デンシャルが正しくない場合、実行時に動的に修正できません。また、宛先ホけられていることから、そのホスト上の一部のサービスへのアクセスを拒否する場合、自動サインオンがイネーブルになっているホストのサポートは望ましくなります。 スマート トンネル用のグループ自動サインオンを設定するには、自動サインオンローバル リストを作成し、次にリストをグループ ポリシーまたはユーザー名にす。この機能はダイナミック アクセス ポリシーでサポートされません。 ASDM では、[Configuration] > [Firewall] > [Advanced] > [ACL Manager] を参照して
Entrust 証明書のプロビジョニング	ASDM 6.1.3（バージョン 8.0x と 8.1x を実行するセキュリティ アプライアンスをバージョン）には、Entrust Web サイトへのリンクが含まれていて、お使いの AS（テスト用）または割引が適用された永続 SSL ID 証明書を申請できます。 ASDM では、[Configuration] > [Remote Access VPN] > [Certificate Management] > [Certificates] > [Enroll ASA SSL VPN head-end with Entrust] を参照してください。
IKE キー再生成時のユーザー再認証の時間延長	フェーズ 1 SA キーの再生成時に、リモート ユーザーに対しクレデンシャルを入により多くの時間を与えるようにセキュリティ アプライアンスを設定できます。reauthenticate-on-rekey が IKE トンネルで設定され、フェーズ 1 キー再生成が発生キュリティ アプライアンスでユーザーに対して認証のためのプロンプトが表示ンシャルを入力するための時間は約 2 分しかありませんでした。その 2 分間のうちがクレデンシャルを入力しないと、トンネルは終了していました。この新機能をにすると、トンネルがドロップされるまでにクレデンシャルを入力する時間はよます。合計時間は、キーの再生成が実際に行われる、確立しようとしている新し1 SA と、期限切れになっている古いフェーズ 1 SA の間の差です。デフォルトのキーの再生成時間が設定された状態で、差はおよそ 3 時間（つまりキーの再生成15% です）。 ASDM で、[Configuration] > [Device Management] > [Certificate Management] > [Identit を参照してください。

機能	説明
永続的 IPSec トンネル フロー	永続的 IPSec トンネル フロー機能をイネーブルにすると、セキュリティ アプトンネルがドロップして回復した後、ステートフル（TCP）トンネル フローます。他のすべてのフローは、トンネルがドロップしたときにドロップされルが設定されたときに再確立する必要があります。TCP フローを維持するこいアプリケーションや影響を受けやすいアプリケーションは、トンネルが短ても動作し続けることができます。この機能では、IPsec LAN-to-LAN トンネドウェア クライアントからのネットワーク拡張モード トンネルをサポートしたは AnyConnect/SSL VPN リモート アクセス トンネルはサポートしていませ**connection preserve-vpn-flows** コマンドを参照してください。このオプションで無効です。 ASDM で、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [IPsec] > [System Options] を参照してください。永続的 IPSec トンネル フローするには、[Preserve stateful VPN flows when the tunnel drops for Network Extensi チェックボックスをオンにしてください。
アクティブ ディレクトリ グループの表示	アクティブ ディレクトリ グループの一覧を表示するために、CLI コマンド **s**が追加されました。ASDM ダイナミック アクセス ポリシーでは、管理者がこ使用することで、VPN ポリシーを定義するために使用できる MS AD グループできます。 ASDM で、[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access Access Policies] > [Add/Edit DAP] > [Add/Edit AAA Attribute] を参照してくださ
Mac OS 上でのスマート トンネル	スマート トンネルで Mac OS がサポートされるようになりました。 ASDM で、[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access [Smart Tunnels] を参照してください。
ファイアウォール機能	
NetFlow フィルタリング	トラフィックとイベント タイプに基づいて NetFlow イベントをフィルタリンまざまなコレクタにレコードを送信できます。たとえば、すべての flow-crea るコレクタに記録し、flow-denied イベントを別のコレクタに記録できます。**event-type** コマンドを参照してください。 ASDM では、[Configuration] > [Firewall] > [Security Policy] > [Service Policy Rul Service Policy Rule] > [Rule Actions] > [NetFlow] を参照してください。

機能	説明
NetFlow の遅延フロー作成イベント	存続期間が短いフローでは、NetFlow 収集装置はフロー作成とティアダウンとい ベントを認識する場合とは異なり、単一イベントを処理することによるメリットが フロー作成イベントを送信するまでの遅延を設定できるようになりました。タイ 切れになる前にフローが切断された場合は、フローティアダウンイベントのみが す。**flow-export delay flow-create** コマンドを参照してください。 （注） ティアダウンイベントには、フローに関するあらゆる情報が含まれま 紛失はありません。 ASDM では、[Configuration] > [Device Management] > [Logging] > [NetFlow] を参照 い。
QoS トラフィック シェーピング	ASA などの、ファスト イーサネットを使用してパケットを高速に送信するデバ し、そのデバイスがケーブル モデムなどの低速デバイスに接続されている場合、 デムがボトルネックとなり、ケーブル モデムでパケットが頻繁にドロップされま 度が異なるネットワークを管理するため、固定の低速でパケットを転送するよう ティ アプライアンスを設定できます。**shape** コマンドを参照してください。 また、**crypto ipsec security-association replay** コマンドも参照してください。この は、IPSec アンチ リプレイ ウィンドウ サイズを設定できます。プライオリティ グには、パケットの並べ替えという副作用があります。IPSec パケットの場合、 撃防止ウィンドウ内にない異常なパケットに対しては、警告 syslog メッセージが す。これらの警告は、プライオリティ キューイングでは誤報となります。この新 ドは、誤報の可能性を防ぎます。 ASDM で、[Configuration] > [Firewall] > [Security Policy] > [Service Policy Rules] > [Service Policy Rule] > [Rule Actions] > [QoS] を参照してください。トラフィック シ でサポートされているトラフィック クラスは、すべてのトラフィックに一致する だけであることに注意してください。

機能	説明
TCP 正規化の機能拡張	特定のパケットタイプに対し、TCP正規化のアクションを設定できるように 前は、これらの種類のパケットに対するデフォルトのアクションは、パケッ ることでした。パケットを許可するように TCP ノーマライザを設定できるよ た。 • TCP の無効な ACK のチェック（**invalid-ack** コマンド） • ウィンドウを超えた TCP パケット シーケンスのチェック（**seq-past-win** • データ チェックを使用した TCP SYN-ACK（**synack-data** コマンド） TCP アウトオブオーダー パケット バッファ タイムアウトを設定することもて コマンドの **timeout** キーワード）。以前は、タイムアウトは 4 秒でした。タ の値に設定できるようになりました。 MSS を超えたパケットのデフォルト アクションが、ドロップから許可に変更 （**exceed-mss** コマンド）。 次の設定できないアクションが、次のパケットタイプに対してドロップから れました。 • Bad option length in TCP • TCP Window scale on non-SYN • Bad TCP window scale value • Bad TCP SACK ALLOW option ASDM で、[Configuration] > [Firewall] > [Objects] > [TCP Maps] を参照してくた
TCP 代行受信の統計情報	TCP 代行受信する統計情報の収集を、**threat-detection statistics tcp-intercept** してイネーブルにし、**show threat-detection statistics** コマンドを使用して表示 ASDM では、[Configuration] > [Firewall] > [Threat Detection] を参照してくださ
脅威検出排除タイムアウト	脅威検出の排除タイムアウトを、**threat-detection scanning-threat shun duratio** 用して設定できるようになりました。 ASDM では、[Configuration] > [Firewall] > [Threat Detection] を参照してくださ
脅威を検知したときのホスト統計情報の微調整	**threat-detection statistics host number-of-rate** コマンドを使用して、ホスト統計 を減らすことができるようになりました。これにより、この機能によるシス 軽減します。 ASDM では、[Configuration] > [Firewall] > [Threat Detection] を参照してくださ
プラットフォーム機能	
VLAN 数の増加	ASA 5580 上でサポートされる VLAN 数が 100 から 250 に増加されました。

機能	説明
名前のないインターフェイスに対するSNMP のサポート	以前の SNMP では、**nameif** コマンドを使用して設定されたインターフェイスに関けが提供されていました。たとえば、SNMP は、名前が付けられているインターIF MIB および IP MIB に関してだけトラップを送信し walk を実行していました。張され、すべての物理インターフェイスと論理インターフェイスに関する情報をうになりました。**nameif** コマンドは SNMP を使用してインターフェイスを表示すになりました。

ASA 8.1(1)/ASDM 6.1(1) の新機能

リリース：**2008年3月1日**

機能	説明
Cisco ASA 5580 の導入	2 つのモデルで Cisco ASA 5580 が導入されました。 • ASA 5580-20 では、5 ギガビット/秒の TCP トラフィックを提供し、フォーマンスはさらに向上しています。システムの多くの機能がマ応になったことで、このような高スループットが実現しました。さあたり 60,000 を超える TCP 接続が可能であり、最大で 100 万接続します。 • ASA 5580-40 では、10 ギガビット/秒の TCP トラフィックを提供し、と同様に UDP のパフォーマンスはさらに向上しています。ASA 55秒あたり 120,000 を超える TCP 接続が可能であり、最大で 200 万接トします。 ASDM では、[Home] > [System Resource Status]、および [Home] > [Device > [Environment Status] を参照してください。
NetFlow	新しい NetFlow 機能では ASA のロギング機能を拡張し、NetFlow プロたフローベースのイベントをロギングします。この機能と新しい CLI コ細については、『*Cisco ASA 5580 Adaptive Security Appliance Command Line Guide*』を参照してください。 ASDM では、[Configuration] > [Device Management] > [Logging] > [Netflo てください。

機能	説明
ジャンボ フレーム サポート	Cisco ASA 5580 では、ジャンボ フレームをサポートするには **jumbo-f** コマンドを入力します。ジャンボ フレームとは、標準の最大フレー 1518 バイト（レイヤ 2 ヘッダーおよび FCS を含む）を超えるイーサ トのことであり、最大は 9216 バイトになります。イーサネット フ るためのメモリ容量を増やすことにより、すべてのインターフェイ ンボ フレームのサポートをイネーブルにできます。ジャンボ フレー メモリを割り当てると、アクセス リストなどのその他の機能の最大 れる場合があります。 ASDM で、[Configuration] > [Device Setup] > [Interfaces] > [Add/Edit In [Advanced] を確認してください。
マルチコア ASA のパケットごとのロード バランシング	マルチコア ASA の場合、デフォルトの動作は、1 コアのみが一度に フェイス受信リングからパケットを受け取ることを許可するという **load-balance per-packet** コマンドは、この動作を変更して、複数のコ フェイス受信リングから複数のパケットを受け取り、それらを独立 とを許可します。デフォルトの動作は、パケットがすべてのインタ グで一律に受信されるというシナリオ向けに最適化されています。 次のコマンドが導入されました。**asp load-balance per-packet**、**show**
SIP プロビジョナル メディアのタイムアウト	SIP 暫定メディアのタイムアウトを、timeout sip-provisional-media コ て設定できるようになりました。 ASDM で、[Configuration] > [Firewall] > [Advanced] > [Global Timeout ださい。
アクティベーション キーの詳細	**show activation key detail** コマンドを使用することで、永続的および ティベーション キーとそれらで有効な機能を確認できます（事前に れているすべての一時キーとそれらの有効期限日を含む）。 ASDM のシングル コンテキスト モードでは、[Configuration] > [Dev > [System Image/Configuration] > [Activation Key] を参照してください。 チ コンテキスト モードでは、[System] > [Configuration] > [Device Ma [Activation Key] を参照してください。
新しい ASDM オンライン ヘルプ エンジン	ASDM は、オンライン ヘルプの新しい外観をサポートするようにな ライン ヘルプは、左側のブックマーク ペインからユーザーがトピッ を維持したまま、右側のペインで主題項目を参照できるようになり
ASDM CPU コア使用率グラフ	単一または複数モードで、CPU コア使用率グラフにより、ASDM ホ らコア CPU 使用率の状態を表示できます。
ASDM のインテリジェント プラットフォーム管理インターフェイス（IPMI）	インテリジェント プラットフォーム管理インターフェイス（IPMI） 加されました。これによりユーザーは、電源、冷却ファン、プロセ の温度の各状態に関する情報を ASDM ホーム ページから確認できる した。

機能	説明
ASDM アシスタント	ASDM アシスタントは、[View] メニューから利用できるようになりまし [Tools] メニュー）。GUI が変更され、[Search] 機構は簡素化されました
ASDM バックアップと復元の機能強化	バックアップと復元の機能強化により、ローカルマシンに設定をバック 必要に応じてサーバにそれらを戻して復元できます。さらに、この機能 関連のファイルをバックアップします。この機能は、[Tools] > [Backup C および [Tools] > [Restore Configuration] にあります。 バージョン *8.0* でもサポートされます。
ASDM ログ ビューア	ログ ビューア拡張機能により、syslog メッセージから解析されたソース ポート情報が表示されます。この情報は、[Monitoring] > [Logging] > [Re Viewer] および [Log Buffer] ページで表示されます。 バージョン *8.0* でもサポートされます。
ASDM での拡張 VPN 検索	キーワードまたはコマンドの入力中に、インテリジェントなヒントを提 コマンドベース検索機能が追加されました。この検索拡張機能は、[Use [Connection Profiles]、[Group Policies] ページにのみ存在します。 バージョン *8.0* でもサポートされます。

バージョン 8.0 の新機能

ASA 8.0(5)/ASDM 6.2(3) の新機能

リリース：**2009年11月3日**

（注） バージョン 8.0(5) は PIX セキュリティ アプライアンスでサポートされていません。

機能	説明
リモート アクセス機能	
VPN セッションのレジューム待機のスケーラブル ソリューション	管理者は、アクティブ状態のユーザー数をトレースし、統計情報を確認できるよ した。ライセンス キャパシティに到達せず、新規ユーザーがログインできるよう 間非アクティブなセッションはアイドルとマークされます（さらに自動的にログ す）。 ASDM 画面が変更されました。[Monitoring] > [VPN] > [VPN Statistics] > [Sessions バージョン *8.2(2)* でも使用可能です。
アプリケーション インスペクション機能	

機能	説明
H.323エンドポイント間のコール設定のイネーブル化	Gatekeeper がネットワーク内にある場合は、H.323 エンドポイント間のコール をイネーブルにできます。ASA には、RegistrationRequest/RegistrationConfirm メッセージに基づいてコールのピンホールを開くオプションが含まれていま これらの RRQ/RCF メッセージはゲートキーパーとの間で送受信されるため、 ポイントの IP アドレスは不明で、セキュリティ アプライアンスが発信元 IP 0/0 を通じてピンホールを開きます。デフォルトでは、このオプションは無効 す。 次のコマンドが導入されました。**ras-rcf-pinholes enable** H.323 インスペクシ マップの作成時にパラメータ コンフィギュレーション モードの間このコマン す。 ASDM 画面が変更されました。[Configuration] > [Firewall] > [Objects] > [Inspect > [Details] > [State Checking] バージョン *8.2(2)* でも使用可能です。
インターフェイス機能	
マルチ コンテキスト モードでは、自動生成 MAC アドレスでユーザー設定可能プレフィックスやその他の拡張を使用	MAC アドレス形式は、プレフィックスの使用、固定開始値（A2）の使用、お オーバー ペアでプライマリ装置とセカンダリ装置の MAC アドレスに対して の使用が可能になるように変更されました。 MAC アドレスは現在、リロード間で持続されるようになっています。 コマンドパーサーは現在、自動生成がイネーブルになっているかどうかをチ MAC アドレスを手動でも割り当てることができるようにする場合は、A2 を アドレスは開始できません。 コマンド **mac-address auto prefix** *prefix* が変更されました。 ASDM 画面が変更されました。[Configuration] > [Context Management] > [Secu バージョン *8.2(2)* でも使用可能です。
ハイ アベイラビリティ機能	
スイッチオーバー イベント中のインターフェイスのアップまたはダウン時に通知なし	通常動作時のリンク アップおよびリンク ダウン遷移と、フェールオーバー中 プ/ダウン遷移を区別するために、フェールオーバー中にリンク アップトラッ ダウントラップは送信されません。また、フェールオーバー中のリンク アッ 遷移に関する syslog メッセージも送信されません。 バージョン *8.2(2)* でも使用可能です。
ルーティング機能	

機能	説明
ルーティング問題を解決するための DHCP RFC 互換性（rfc3011、rfc3527）	この拡張では、DHCP RFCs 3011（IPv4 サブネット選択オプション）および 3527 エージェント情報オプションのリンク選択サブオプション）の ASA サポートが導 た。**dhcp-server** コマンドを使用して設定した各 DHCP サーバに対して、**subnet-** プションおよび **link-selection** オプションを送信するか、いずれも送信しないよ 設定できるようになりました。 次の ASDM 画面が変更されました。[Remote Access VPN] > [Network Access] > [IPs profiles] > [Add/Edit] バージョン *8.2(2)* でも使用可能です。
SSM 機能	
ASDM の CSC 6.3 サポート	ASDM は、メイン ホーム ページ上の [Plus License] リストに [Web Reputation]、[Policies]、および [User ID Settings] を表示します。CSC 6.3 セキュリティ イベン 含まれています。これは新しい Web レピュテーション イベントおよびユーザー の識別などです。

ASA 8.0(4)/ASDM 6.1(3) の新機能

リリース：**2008年8月11日**

機能	説明
ユニファイド コミュニケーション機能[1]	
電話プロキシ	フォン プロキシ機能がサポートされています。ASA フォン プロキシは、Metreos Phone Proxy と同様の機能をサポートしており、SIP インスペクションと強化さ ティが追加でサポートされています。ASA フォン プロキシの主な機能は次のと • 電話機に対しシグナリングとメディアの暗号化を強制する、セキュア リモ • 証明書に基づくリモート IP 電話の認証 • IP 電話からの TLS シグナリングを終端し、Cisco Unified Mobility Advantage TCP および TLS を開始 • SRTP を終端し、着信側への RTP/SRTP を開始 ASDM で、[Configuration] > [Firewall] > [Advanced] > [Encrypted Traffic Inspection] > [を参照してください。

機能	説明
モビリティ プロキシ	Cisco Unified Mobility Advantage クライアントとサーバの間のセキュア接続（ キシ）がサポートされます。 Cisco Unified Mobility Advantage ソリューションには、Cisco Unified Mobile Co Cisco Unified Mobility Advantage サーバが含まれています。Cisco Unified Mobi は、モバイルハンドセット用の使いやすいソフトウェア アプリケーションで プライズ通信アプリケーションとサービスを携帯電話やスマート フォンに拡 リティ ソリューションを使用することで、通信が円滑になり、企業全体でリ ボレーションが可能になります。 このソリューションの ASA は、MMP（旧称 OLWP）プロトコルを検査しま Cisco Unified Mobile Communicator と Cisco Unified Mobility Advantage の間の独 です。ASA は TLS プロキシとしても機能し、Cisco Unified Mobile Communicato Mobility Advantage の間で TLS シグナリングを終端および発信します。 ASDM で、[Configuration] > [Firewall] > [Advanced] > [Encrypted Traffic Inspectio を参照してください。
プレゼンス フェデレーション プロキシ	Cisco Unified Presence サーバと Cisco/Microsoft Presence サーバの間のセキュア ス フェデレーション プロキシ）がサポートされます。Presence ソリューショ と、企業は Cisco Unified Presence クライアントを企業ネットワークに安全に接 なる企業のプレゼンス サーバ間でプレゼンス情報を共有したりできます。 ASA は、インターネットおよび企業内通信のためのプレゼンスを可能にする す。SSL 対応の Cisco Unified Presence クライアントは、プレゼンス サーバへ 立できます。ASA では、サードパーティ製プレゼンス サーバと Cisco Unified の間の通信を含め、サーバ間通信のための SSL 通信が可能です。複数の企業 報を共有し、IM アプリケーションを使用できます。ASA は、サーバ間の SI 検査します。 ASDM で、[Configuration] > [Firewall] > [Service Policy Rules] > [Add/Edit Servic [Rule Actions] > [Protocol Inspection] または [Configuration] > [Firewall] > [Advanc Traffic Inspection] > [TLS Proxy] > [Add] > [Client Configuration] を参照してくだ
リモート アクセス機能	

機能	説明
IE1 用スマート トンネルを使用した自動サインオン 1	この機能を使用すると、WININET 接続のためのログイン クレデンシャルの代替 ります。Internet Explorer を含め、ほとんどの Microsoft 製アプリケーションは W 用しています。Mozilla Firefox は WININET を使用していないため、この機能でサ ません。また、HTTP ベースの認証もサポートされるため、フォームベースの認 能とともに使用できません。 クレデンシャルは、サービスではなく宛先ホストに静的に関連付けられるため、 デンシャルが正しくない場合、実行時に動的に修正できません。また、宛先ホス けられていることから、そのホスト上の一部のサービスへのアクセスを拒否する 場合、自動サインオンがイネーブルになっているホストのサポートは望ましくな ります。 スマート トンネル用のグループ自動サインオンを設定するには、自動サインオン ローバル リストを作成し、次にリストをグループ ポリシーまたはユーザー名に す。この機能はダイナミック アクセス ポリシーでサポートされません。 ASDM で、[Firewall] > [Advanced] > [ACL Manager] を参照してください。
Entrust 証明書のプロビジョニング 1	ASDM には、ASA の一時的（テスト用）または割引価格の永続的な SSL 身元証 込むための、Entrust Web サイトへのリンクが含まれています。 ASDM で、[Configuration] > [Remote Access VPN] > [Certificate Management] > [Identit を参照してください。[Enroll ASA SSL VPN head-end with Entrust] をクリックしま
IKE キー再生成時のユーザー再認証の時間延長	フェーズ 1 SA キーの再生成時に、リモート ユーザーに対しクレデンシャルを入 により多くの時間を与えるようにセキュリティ アプライアンスを設定できます。 reauthenticate-on-rekey が IKE トンネルで設定され、フェーズ 1 キー再生成が発生 キュリティ アプライアンスでユーザーに対して認証のためのプロンプトが表示さ ンシャルを入力するための時間は約2分しかありませんでした。その2分間のうち がクレデンシャルを入力しないと、トンネルは終了していました。この新機能を にすると、トンネルがドロップされるまでにクレデンシャルを入力する時間はよ ます。合計時間は、キーの再生成が実際に行われる、確立しようとしている新し 1 SA と、期限切れになっている古いフェーズ 1 SA の間の差です。デフォルトの キーの再生成時間が設定された状態で、差はおよそ 3 時間（つまりキーの再生成 15% です）。 ASDM で、[Configuration] > [Device Management] > [Certificate Management] > [Identit を参照してください。

機能	説明
永続的 IPSec トンネル フロー	永続的 IPSec トンネル フロー機能をイネーブルにすると、セキュリティ アプ トンネルがドロップして回復した後、ステートフル（TCP）トンネル フロー ます。他のすべてのフローは、トンネルがドロップしたときにドロップされ ルが設定されたときに再確立する必要があります。TCP フローを維持するこ いアプリケーションや影響を受けやすいアプリケーションは、トンネルが短 ても動作し続けることができます。この機能は、IPSec の LAN 間トンネルと クライアントからのネットワーク拡張モード トンネルをサポートしています AnyConnect/SSL VPN リモート アクセス トンネルはサポートしていません。 **connection preserve-vpn-flows** コマンドを参照してください。このオプション で無効です。 ASDM で、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [IPsec] > [System Options] を参照してください。永続的 IPSec トンネル フロー するには、[Preserve stateful VPN flows when the tunnel drops for Network Extensi チェックボックスをオンにしてください。
アクティブ ディレクトリ グループの表示	アクティブ ディレクトリ グループの一覧を表示するために、CLI コマンド **sh** が追加されました。ASDM ダイナミック アクセス ポリシーでは、管理者がこ 使用することで、VPN ポリシーを定義するために使用できる MS AD グルー できます。 ASDM で、[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access Access Policies] > [Add/Edit DAP] > [Add/Edit AAA Attribute] を参照してくださ
Mac OS1 上でのスマート トンネル [1]	スマート トンネルで Mac OS がサポートされるようになりました。 ASDM で、[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access [Smart Tunnels] を参照してください。
ローカル アドレス プールの編集	アドレス プールは、目的の接続に影響を与えることなく編集できます。アド ありプールから排除されていない場合、接続は影響を受けません。ただし、 スがプールから除去されている場合、接続はダウンします。 バージョン *7.0(8)* および *7.2(4)* でも使用可能です。
ファイアウォール機能	

機能	説明
QoS トラフィック シェーピング	ASA などの、ファスト イーサネットを使用してパケットを高速に送信するデバ し、そのデバイスがケーブル モデムなどの低速デバイスに接続されている場合、 デムがボトルネックとなり、ケーブル モデムでパケットが頻繁にドロップされま 度が異なるネットワークを管理するため、固定の低速でパケットを転送するよう ティ アプライアンスを設定できます。**shape** コマンドを参照してください。また、 **security-association replay** コマンドも参照してください。このコマンドでは、IPS プレイ ウィンドウ サイズを設定できます。プライオリティ キューイングには、 並べ替えという副作用があります。IPSec パケットの場合、リプレイ攻撃防止ウ にない異常なパケットに対しては、警告 syslog メッセージが生成されます。これ プライオリティ キューイングでは誤報となります。この新しいコマンドは、誤報 防ぎます。 ASDM で、[Configuration] > [Firewall] > [Security Policy] > [Service Policy Rules] > [Service Policy Rule] > [Rule Actions] > [QoS] を参照してください。トラフィック シ でサポートされているトラフィック クラスは、すべてのトラフィックに一致する だけであることに注意してください。 バージョン *7.2(4)* でも使用可能です。

機能	説明
TCP 正規化の機能拡張	特定のパケットタイプに対し、TCP正規化のアクションを設定できるように 前は、これらの種類のパケットに対するデフォルトのアクションは、パケッ ることでした。パケットを許可するように TCP ノーマライザを設定できるよ た。 • TCP の無効な ACK のチェック（**invalid-ack** コマンド） • ウィンドウを超えた TCP パケット シーケンスのチェック（**seq-past-win** • データ チェックを使用した TCP SYN-ACK（**synack-data** コマンド） TCP アウトオブオーダー パケット バッファ タイムアウトを設定することもて コマンドの **timeout** キーワード）。以前は、タイムアウトは 4 秒でした。タ の値に設定できるようになりました。 MSS を超えたパケットのデフォルト アクションが、ドロップから許可に変更 （**exceed-mss** コマンド）。 次の設定できないアクションが、次のパケットタイプに対してドロップから れました。 • Bad option length in TCP • TCP Window scale on non-SYN • Bad TCP window scale value • Bad TCP SACK ALLOW option ASDM で、[Configuration] > [Firewall] > [Objects] > [TCP Maps] を参照してくた バージョン *7.2(4)* でも使用可能です。
TCP 代行受信の統計情報	TCP 代行受信する統計情報の収集を、**threat-detection statistics tcp-intercept** してイネーブルにし、**show threat-detection statistics** コマンドを使用して表示 ASDM 6.1(5) 以降で、[Configuration] > [Firewall] > [Threat Detection] を参照し のコマンドは、ASDM 6.1(3) ではサポートされていませんでした。
脅威検出排除タイムアウト	脅威検出の排除タイムアウトを、**threat-detection scanning-threat shun duratio** 用して設定できるようになりました。 ASDM 6.1(5) 以降で、[Configuration] > [Firewall] > [Threat Detection] を参照し のコマンドは、ASDM 6.1(3) ではサポートされていませんでした。
SIP プロビジョナル メディアのタイムアウト	SIP 暫定メディアのタイムアウトを、**timeout sip-provisional-media** コマンド できるようになりました。 ASDM で、[Configuration] > [Firewall] > [Advanced] > [Global Timeouts] を参照 バージョン *7.2(4)* でも使用可能です。

機能	説明
clear conn コマンド	**clear conn** コマンドは、接続を削除するために追加されました。 バージョン *7.0(8)* および *7.2(4)* でも使用可能です。
フラグメントの完全リアセンブル	**fragment** コマンドは **reassembly full** キーワードで拡張され、デバイス経由でルーれるフラグメントの完全リアセンブルが可能になりました。デバイスで終端するトは、常に完全にリアセンブルされます。 バージョン *7.0(8)* および *7.2(4)* でも使用可能です。
Ethertype ACL MAC の機能強化	EtherType ACL は、非標準 MAC を許可するように強化されています。既存のデルールが保持され、新しいルールを追加する必要はありません。 バージョン *7.0(8)* および *7.2(4)* でも使用可能です。
トラブルシューティングとモニタリングの機能	
capture コマンドの強化	**capture type asp-drop** *drop_code* コマンドは、**all** を *drop_code* として受け入れるので、セキュリティチェックが原因でドロップされたものを含め、ASA がドロてのパケットをキャプチャできるようになりました。 バージョン *7.0(8)* および *7.2(4)* でも使用可能です。
show asp drop コマンドの強化	カウンタが最後にクリアされた時間を示すタイムスタンプが出力に含まれるよた（**clear asp drop** コマンドを参照）。また、説明の横にドロップ理由のキーワれるため、そのキーワードを使用して簡単に **capture asp-drop** コマンドを使用 バージョン *7.0(8)* および *8.0(4)* でも使用可能です。
clear asp table コマンド	**clear asp table** コマンドが、show asp table コマンドによるヒット出力をクリアするされました。 バージョン *7.0(8)* および *7.2(4)* でも使用可能です。
show asp table classify hits コマンドの強化	**hits** オプションが **show asp table classify** コマンドに追加され、asp テーブル カウアされた最終時刻を示すタイムスタンプが表示されるようになりました。ゼロとhits 値があるルールも表示されます。これによりユーザーはどのルールがヒットばやく参照できます。特に単純な設定であると **show asp table classify** コマンド百ものエントリが存在するようになるため便利です。 バージョン *7.0(8)* および *8.0(4)* でも使用可能です。
MIB の機能拡張	CISCO-REMOTE-ACCESS-MONITOR-MIB はより完全に実装されます。 *8.0(4)* でも使用可能です。
show perfmon コマンド	次の速度出力が追加されました。[TCP Intercept Connections Established]、[TCP In Attempts]、[TCP Embryonic Connections Timeout]、および [Valid Connections Rate in T バージョン *7.0(8)* および *7.2(4)* でも使用可能です。

機能	説明
memory tracking コマンド	次の新しいコマンドが、このリリースで導入されました。 • **memory tracking enable**：このコマンドにより、ヒープ メモリ要求のト 効になります。 • **no memory tracking enable**：このコマンドは、ヒープ メモリ要求の追跡 在収集したすべての情報をクリーンアップし、ツール自体によって使用 ヒープ メモリをシステムに返します。 • **clear memory tracking**：このコマンドは現在収集したすべての情報を消 れ以降もメモリ要求の追跡は継続します。 • **show memory tracking**：このコマンドは、ツールの追跡対象である現在 いるメモリを、最上位呼び出し元関数アドレス別に示します。 • **show memory tracking address**：このコマンドは、メモリの各部分に分割 てられているメモリを示しています。この出力は、ツールの追跡対象で てられている各メモリのサイズ、位置、および最上位呼び出し元関数を一 • **show memory tracking dump**：このコマンドは、指定されたメモリ アド 位置、呼び出しスタックの一部、およびメモリ ダンプを表示します。 • **show memory tracking detail**：このコマンドは、ツールの内部動作への洞 使用されるさまざまな内部の詳細を示しています。 バージョン *7.0(8)* および *7.2(4)* でも使用可能です。
ルーティング機能	

機能	説明
IPv6 マルチキャスト リスナー ディスカバリ プロトコル v2 サポート	ASA は、マルチキャスト リスナー ディスカバリ プロトコル（MLD）バージョン トするようになりました。これにより直接接続リンク上のマルチキャストアドレ の存在を検出し、特にどのマルチキャストアドレスがそれらの隣接ノードの対象 検出します。ASA はマルチキャスト アドレス リスナーまたはホストにはなりま チキャスト ルータにはならず、マルチキャスト リスナー クエリに応答し、マル リスナー レポートのみを送信します。 次のコマンドがこの機能をサポートしています。 • **clear ipv6 mld traffic**：clear ipv6 mld traffic コマンドを使用すると、すべての スト リスナー検出トラフィック カウンタをリセットできます。 • **show ipv6 mld traffic**：show ipv6 mld コマンドを使用すると、すべてのマルチ スナー検出トラフィック カウンタを表示できます。 • **debug ipv6 mld**：debug ipv6 コマンドのこの機能拡張により、ユーザーは M ル アクティビティが正常に機能しているかどうかを確認するための MLD 用 メッセージを表示できます。 • **show debug ipv6 mld**：show debug ipv6 コマンドのこの機能拡張により、ユー ipv6 mld が有効になっているか無効になっているかを表示できます。 バージョン *7.2(4)* でも使用可能です。
プラットフォーム機能	
ASA 5505 に対するネイティブ VLAN サポート	**switchport trunk native vlan** コマンドを使用して、ネイティブ VLAN を ASA 550 ポートに含めることができるようになりました。 ASDM で、[Configuration] > [Device Setup] > [Interfaces] > [Switch Ports] > [Edit] ダ 参照してください。 バージョン *7.2(4)* でも使用可能です。
名前のないインターフェイスに対する SNMP のサポート	以前の SNMP では、**nameif** コマンドを使用して設定されたインターフェイスに関 けが提供されていました。たとえば、SNMP は、名前が付けられているインター IF MIB および IP MIB に関してだけトラップを送信し walk を実行していました。 には名前のないスイッチポートと名前付きの VLAN インターフェイスがあるため 物理インターフェイスと論理インターフェイスに関する情報を表示するように S されました。SNMP を使用してインターフェイスを表示するために **nameif** コマン くなりました。これらの変更は、ASA 5505 だけでなく、すべてのモデルに影響
フェールオーバー機能	
failover timeout コマンド	**failover timeout** コマンドに、静的固定機能とともに使用されるフェールオーバー が不要になりました。 バージョン *7.0(8)* および *7.2(4)* でも使用可能です。

機能	説明
ASDM 機能	
DNS パネルの簡素化	ASDM GUI 上の DNS パネルは、使いやすさのために変更されています。[Co [Device Management] > [DNS] を参照してください。
[File Transfer] ダイアログ ボックスの再設計	[File Transfer] ダイアログ ボックスでは、ファイルをドラッグアンドドロップ ダイアログ ボックスにアクセスするには、[Tools] > [File Management] と進み Transfer] をクリックします。
ACL ヒット カウンタのクリア	ACL ヒット カウンタをクリアできる機能が追加されました。[Firewall] > [Ad Manager] パネルを参照してください。
ACL の名前変更	ASDM から ACL を名前変更する機能を追加しました。 [Firewall] > [Advanced] > [ACL Manager] パネルを参照してください。
1 つのパネルへの ASDM/HTTPS、SSH、Telnet の組み合わせ	ASDM では、ASDM、HTTPS、SSH、Telnet が 1 つのパネルに統合されていま > [Properties] > [Device Access] > [ASDM/HTTPS/Telnet/SSH Sessions] パネルを い。
ACL マネージャでのすべての標準 ACL の表示	すべての標準 ACL を ACL マネージャで表示できるようにする機能が追加さ [Firewall] > [Advanced] > [ACL Manager] パネルを参照してください。

[1] （1）この機能は、PIX セキュリティ アプライアンスではサポートされていません。

ASA 8.0(3)/ASDM 6.0(3) の新機能

リリース：**2007年11月7日**

機能	説明
VPN 機能	
AnyConnect RSA SoftID API の統合	AnyConnect VPN クライアントに対し、ユーザー トークン コードを SoftID を使用した直接通信のサポートを提供します。また、接続プ ンネル グループ）に対し、SoftID メッセージ サポートを指定する機 プロキシを通じて受信した SDI メッセージに一致する SDI メッセー ティ アプライアンス上で設定するための機能も提供します。この機 と、リモート クライアント ユーザーに対して、認証に必要なアクシ 切なプロンプトが表示され、AnyConnect クライアントが認証に対し ることが保証されます。

機能	説明
IP アドレス再利用の遅延	IPアドレスがIPアドレスプールに返された後、IPアドレスの再利用を遅 遅延を増やすことで、IPアドレスがプールに返されてすぐに再割り当て に、セキュリティアプライアンスで発生する可能性がある問題を避ける ます。 ASDM で、[Configure] > [Remote Access VPN] > [Network (Client) Access] Assignment] > [Assignment Policy] を参照してください。
クライアントレス SSL VPN キャッシング静的コンテンツの機能拡張	クライアント SSL VPN キャッシュ コマンドには次の 2 つの変更があり **cache-compressed** コマンドが非推奨になりました。 新しい **cache-static-content** コマンドは、すべての静的コンテンツをキャ ように ASA を設定します。これはつまり、SSL VPN の書き換えが行わ てのキャッシュ可能 Web オブジェクトのことです。これには、画像や ルなどのコンテンツが含まれています。 コマンドの構文は次のとおりです。**cache-static-content** {**enable** | **disable** トでは、静的コンテンツ キャッシングが無効になっています。 例： `hostname (config) # webvpn` `hostname (config-webvpn) # cache` `hostname (config-webvpn-cache) # cache-static-content enable` hostname (config-webvpn-cache) # ASDM で、[Configuration] > [Remote Access VPN] > [Clientless SSL VPN [Advanced] > [Content Cache] を参照してください。 バージョン *7.2(3)* でも使用可能です。
スマート カードの取り外し切断	この機能により、セントラルサイトの管理者は、スマートカードを取り アクティブなトンネルを削除するためのリモートクライアントポリシー ます。Cisco VPN リモート アクセス ソフトウェア クライアント（IPSec 方）は、デフォルトでは、ユーザーが認証に使用されるスマートカード ときに既存の VPN トンネルを切断します。次の CLI コマンドは、スマ が取り外されたときに既存の VPN トンネルを切断します。 **smartcard-removal-disconnect** {**enable** | **disable**}。このオプションは、デ 有効です。 ASDM で、[Configuration] > [Remote Access VPN] > [Network (Client) Acc Policies] > [Add/Edit Internal/External Group Policies] > [More Options] を参 さい。 バージョン *7.2(3)* でも使用可能です。

機能	説明
WebVPN ロード バランシング	適応型セキュリティ アプライアンスは、ロード バランシングのため用をサポートするようになりました。FQDN を使用して WebVPN ロングを実行するには、ロード バランシング用に FQDN の使用を有効 **redirect-fqdn enable** コマンドを入力する必要があります。DNS サーフェイス外の各適応型セキュリティアプライアンスのエントリを（は）追加します。それぞれの適応型セキュリティ アプライアンスのスに、ルックアップ用にそのアドレスに関連付けられたDNSエントいる必要があります。これらのDNSエントリに対しては、逆ルックブルにする必要があります。**dns domain-lookup inside** コマンドを使セキュリティ アプライアンスでDNSルックアップをイネーブルにし部分には、DNSサーバへのルートを持つ任意のインターフェイスを後に、適応型セキュリティ アプライアンス上の DNS サーバの IP アる必要があります。次に示すのは、この拡張機能に関連付けられてです。**redirect-fqdn** {**enable** | **disable**}。 ASDM で、[Configuration] > [VPN] > [Load Balancing] を参照してくた バージョン *7.2(3)* でも使用可能です。
アプリケーション インスペクション機能	
WAAS と ASA の相互運用性	ポリシーマップ クラス設定モードでWAASインスペクションを有効 **inspect waas** コマンドが追加されました。この CLI は、機能の設定で限にするために、モジュラ ポリシー フレームワークに統合されていwaasコマンドは、デフォルトのインスペクション クラスおよびカスプの下に設定できます。このインスペクション サービスは、デフォルトではありません。 キーワード オプション waas は、WAAS 統計を表示するために、**sho inspect** コマンドに追加されました。 `show service-policy inspect waas` 新しいシステム ログ メッセージは、接続で WAAS 最適化が検出さされます。WAAS最適化接続では、すべてのL7検査サービス（IPS パスされます。 システム ログの番号と形式： %ASA-6-428001：WAAS confirmed from in_interface:src_ip_addr/src_po out_interface:dest_ip_addr/dest_port, inspection services bypassed on this c WAAS接続で、新しい接続フラグ「W」が追加されました。**show co** ドは、新しいフラグを反映するように更新されています。 ASDM で、[Configuration] > [Firewall] > [Service Policy Rules] > [Add/E Rule] > [Rule Actions] > [Protocol Inspection] を参照してください。 バージョン *7.2(3)* でも使用可能です。

機能	説明
DNS ガードの機能拡張	DNS ガードをイネーブルまたはディセーブルにするためのオプションが した。この機能をイネーブルにすると、1 つの DNS 要求に対して 1 つの だけが許可されます。 ASDM で、[Configuration] > [Firewall] > [Objects] > [Inspect maps] > [DNS ください。 バージョン *7.2(3)* でも使用可能です。
ESMTP over TLS のサポート	この拡張機能は、esmtp ポリシー マップに構成パラメータ **allow-tls** [**act** 加します。デフォルトでは、このパラメータはイネーブルになってい にすると、ESMTP インスペクションは 250-STARTTLS エコー応答をサ スクすることも、クライアントから STARTTLS コマンドをマスクするこ せん。サーバが 220 応答コードで応答したら、ESMTP インスペクション がオフになります。そのセッションの ESMTP トラフィックは検査され す。**allow-tls action log** パラメータが設定されていると、ESMTP セッシ が開始されたときに、syslog メッセージ ASA-6-108007 が生成されます `policy-map type inspect esmtp esmtp_map` `parameters` `allow-tls [action log]` **allow-tls** パラメータに関連付けられたカウンタを表示するための新しい service-policy inspect esmtp コマンドに追加されました。これは **allow-tls** マップで設定されている場合にのみ存在します。デフォルトでは、この はイネーブルになっていません。 `show service-policy inspect esmtp` `allow-tls, count 0, log 0` この拡張機能は、**allow-tls** パラメータの新しいシステム ログ メッセージ す。これは esmtp セッションでサーバがクライアントの STARTTLS コマ て 220 応答コードで応答したことを示します。ESMTP インスペクション では、この接続のトラフィックは検査されなくなりました。 システム ログの番号と形式： %ASA-6-108007: TLS started on ESMTP session between client <client-side interface-name>:<client IP address>/<client port> and server <server-side interface-name>:<server IP address>/<server port> ASDM で、[Configuration] > [Firewall] > [Objects] > [Inspect Map] > [ESMT てください。 バージョン *7.2(3)* でも使用可能です。
ハイ アベイラビリティ機能	

機能	説明
データプレーン キープアライブ メカニズムの追加	ASA を構成して、AIP SSM がアップグレードされた場合に、フェー生させないようにできます。以前のリリースでは、AIP SSM がある フェールオーバーで構成されている場合に AIP SSM ソフトウェアが AIP SSM はソフトウェアの更新を有効にするためにリブートまたは するので、ASA はフェールオーバーをトリガーします。 バージョン *7.0(7)* および *7.2(3)* でも使用可能です。
完全修飾ドメイン名（FQDN）のサポートの機能拡張	**redirect-fqdn** コマンドに、完全修飾ドメイン名（FQDN）または IP ロードバランシング クラスタ内のクライアントに送信するためのオ されました。 ASDM で、[Configuration] > [Device Management] >[High Availability] Balancing] または [Configuration] > [Remote Access VPN] > [Load Balar てください。
DHCP 機能	
DHCP クライアント ID の拡張機能	**ip address dhcp** コマンドを使用してインターフェイスの DHCP クラ ネーブルにすると、一部の ISP でオプション 61 がインターフェイス であると見なされます。MAC アドレスが DHCP 要求パケットに含ま 合、IP アドレスは割り当てられません。この新しいコマンドを使用 ン 61 用にインターフェイス MAC アドレスを含めます。このコマン 場合は、クライアント ID は次のようになります。cisco-<MAC>-<interf 次のコマンドが導入されました。**dhcp-client client-id interface** *interf* 次の画面が変更されました。[Configuration] > [Device Management] > [Server]。次に [Advanced] をクリックします。 バージョン *7.2(3)* でも使用可能です。
DHCP クライアント ブロードキャスト フラグ	**ip address dhcp** コマンドを使用してインターフェイスの DHCP クラ ネーブルにすると、DHCP クライアントが検出を送信して IP アドレ きに、このコマンドを使用して、DHCP パケット ヘッダーでブロー グを 1 に設定できます。DHCP サーバはこのブロードキャスト フラ し、フラグが 1 に設定されている場合は応答パケットをブロードキ **no dhcp-client broadcast-flag** コマンドを入力すると、ブロードキャス に設定され、DHCP サーバは応答パケットを提供された IP アドレス にユニキャストします。 DHCP クライアントは、DHCP サーバからブロードキャスト オファ ト オファーの両方を受信できます。 次のコマンドが導入されました。**dhcp-client broadcast-flag** 次の画面が変更されました。[Configuration] > [Device Management] > [Server]。次に [Advanced] をクリックします。

機能	説明
プラットフォーム機能	
ASA 5510 Security Plus ライセンスにより、ポート 0 と 1 のギガビット イーサネットが可能になります。	ASA 5510 ASA は、ポート 0 と 1 の GE（ギガビット イーサネット）を Security Plus ライセンスを持つようになりました。ライセンスを Base か Plus にアップグレードした場合、外部 Ethernet 0/0 および Ethernet 0/1 の の FE（ファスト イーサネット）の 100 Mbps から GE の 1000 Mbps に地 インターフェイス名は Ethernet 0/0 および Ethernet 0/1 のままです。**speed** 使用してインターフェイスの速度を変更します。また、**show interface** コ 用して各インターフェイスの現在の設定速度を確認します。 バージョン *7.2(3)* でも使用可能です。
ASA 5505 の増加した VLAN の範囲	ASA 5505 ASA は 1 ～ 4090 の範囲の VLAN ID をサポートするようにな 当初は 1 ～ 1001 の VLAN ID のみがサポートされていました。 バージョン *7.2(3)* でも使用可能です。
トラブルシューティング機能	
capture コマンドの強化	capture コマンドの拡張により、ユーザーはトラフィックをキャプチャし イムで表示することができます。コマンドライン オプションを指定して クセス リストを設定する必要なくトラフィックをフィルタすることもで の拡張機能では、**real-time** と 5 タプルの **match** オプションが追加され **capture** *cap_name* [**real-time**] [**dump**] [**detail** [**trace**] [**match** *prot* {**host** *ip* | *i* [{**eq** | **lt** | **gt**} *port*] {**host** *ip* | *ip mask* | **any**} [{**eq** | **lt** | **gt**} *port*]] バージョン *7.2(3)* でも使用可能です。
ASDM 機能	
ASDM バナー拡張機能	適応型セキュリティ アプライアンス ソフトウェアは、ASDM バナーを ています。設定した場合、ASDM を起動すると、このバナー テキストが は切断のためのオプションとともに、ダイアログボックスに表示されます オプションを選択すると、バナーが閉じて通常どおりログインが完了し [Disconnect] オプションを選択するとバナーが閉じて接続が終了します。 張は顧客に、接続の前に、書面によるポリシー条件の受け入れを求めま 次に示すのは、この拡張機能に関連付けられている新しい CLI です。 **banner** {**exec** | **login** | **motd** | **asdm**} *text* **show banner** [**exec** | **login** | **motd** | **asdm**] **clear banner** ASDM で、[Configuration] > [Properties] > [Device Administration] > [Bann てください。 バージョン *7.2(3)* でも使用可能です。

機能	説明
ASDM のローカリゼーションの機能拡張	ASDM は AnyConnect ローカリゼーションをサポートするように機能た。[Configuration] > [Remote Access VPN] > [Network (Client) Access] Customization] を参照するか、または [Configuration] > [RemoteAccess Access] > [AnyConnect Customization] および [Configuration] > [RemoteAc Localization] > [MST Translation] **パネル**を参照してください。
時間ベース ライセンスの機能拡張	[Home] ページで、[Device Dashboard] タブの [License] タブには、時センスの有効期限が切れるまでの日数が示されています（該当する
Network Objects	ファイアウォール規則で使用できる真のネットワーク オブジェクトうになりました。オブジェクトには名前を付けることができ、オブすると、その変更はオブジェクトが使用される場所ではどこでも継た、ルールを作成すると、ルールで指定したネットワークは自動的オブジェクト リストに追加され、どこでもそれらを再利用できます エントリも名前を付けて編集できます。[Configuration] > [Firewall] > [Network Objects/Groups] を参照してください。
クライアント ソフトウェアの場所の機能強化	クライアント ソフトウェアの場所のリストに、Linux または Mac のクライアント更新を許可するためのサポートが追加されました。[Co Access VPN] > [Language Localization] を参照してください。 バージョン *7.2(3)* でも使用可能です。
CSC イベントと統計レポートの機能拡張	Cisco Content Security and Control（CSC）6.2 ソフトウェアを使用す新しい Damage Cleanup Services（DCS）機能用のイベントと統計を提 はクライアントおよびサーバからマルウェアを削除して、システム モリを修復します。

ASA 8.0(2)/ASDM 6.0(2) の新機能

リリース：2007年6月18日

（注） 8.0(1)/6.0(1) リリースはありませんでした。

機能	説明
ルーティング機能	
EIGRP ルーティング	ASA は、EIGRP ルーティングまたは EIGRP スタブ ルーティン ています。
ハイ アベイラビリティ機能	

機能	説明
フェールオーバー ペアでのリモート コマンド実行	フェールオーバー ペアのピア ユニット上で、直接ピアに接続しな ンドを実行できます。これは、Active/Standby フェールオーバーと フェールオーバーの両方で実行可能です。
CSM コンフィギュレーションのロール バックのサポート	フェールオーバー構成において、Cisco Security Manager コンフィギ ンのロールバック機能のサポートが追加されています。
フェールオーバー ペアの Auto Update のサポート	Auto Update サーバを使用して、フェールオーバー ペアのプラット メージとコンフィギュレーションを更新できます。
SIP シグナリングのステートフル フェールオーバー	SIP メディアとシグナリング接続がスタンバイ ユニットに複製され
冗長インターフェイス	論理冗長インターフェイスは、アクティブとスタンバイの物理イン スからなるペアです。アクティブインターフェイスで障害が発生す ンバイ インターフェイスがアクティブになって、トラフィックを通 ます。冗長インターフェイスを設定して ASA の信頼性を高めるこ す。この機能は、デバイスレベルのフェールオーバーとは別個のも 必要な場合はフェールオーバーとともに冗長インターフェイスも設 す。最大 8 個の冗長インターフェイス ペアを設定できます。
モジュール機能	
AIP SSM を使用した仮想 IPS センサー	IPS ソフトウェアのバージョン 6.0 以降を実行している AIP SSM で 仮想センサーを実行できます。つまり、AIP SSM に複数のセキュ シーを設定することができます。各コンテキストまたはシングルモ セキュリティ アプライアンスを 1 つまたは複数の仮想センサーに り、複数のセキュリティ コンテキストを同じ仮想センサーに割り当 できます。仮想センターの詳細（サポートされている最大センサー ついては、IPS のマニュアルを参照してください。
パスワードのリセット	SSM ハードウェア モジュールのパスワードをリセットできます。
VPN 認証機能[2]	
証明書とユーザー名およびパスワード ログインの組み合わせ	管理者が SSL VPN 接続にログインするには、証明書に加えてユー スワードが必要です。
内部ドメイン ユーザー名とパスワード	ワンタイム パスワードなど、ドメイン ユーザー名とパスワード以 ンシャルを使用してログインするユーザーに対し、内部リソースへ のためのパスワードを提供します。これは、ユーザーがログインす 力するパスワードとは別のパスワードです。
汎用 LDAP サポート	これには、OpenLDAP と Novell LDAP が含まれます。認証と認可で LDAP サポートが拡張されます。

機能	説明
オンスクリーン キーボード	ASA には、ログイン ページと、内部リソースに対する以降の認 のオンスクリーン キーボード オプションがあります。これは、 理的なキーボード上の文字を入力するのではなく、マウスを使 リーンキーボード上の文字をクリックするようにユーザーに要 ソフトウェアベースのキーストローク ロガーに対するさらなる す。
RSA Access Manager で確認される SAML SSO	ASA は、RSA Access Manager（Cleartrust および Federated Identi 使用した、シングル サインオン（SSO）のための Security Asse Language（SAML）プロトコルをサポートしています。
NTLMv2	バージョン 8.0(2) では、Windows ベースのクライアントに対し のサポートが追加されています。
証明書の機能	
ローカル認証局（CA）	ブラウザベースおよびクライアントベースの SSL VPN 接続で使 ASA 上の認証局を提供します。
OCSP CRL	SSL VPN の OCSP 失効チェック機能を提供します。
Cisco Secure Desktop の機能	
ホスト スキャン	Cisco AnyConnect またはクライアントレス SSL VPN 接続の完了 リモート コンピュータは、アンチウイルス アプリケーション ウェア アプリケーション、ファイアウォール、オペレーティン および関連する更新の大幅に拡張されたコレクションをスキャ た、任意のレジストリ エントリ、ファイル名、およびプロセス キャン対象にすることもできます。スキャン結果を ASA に送信 は、ユーザー ログイン クレデンシャルとコンピュータ スキャ 使用して、ダイナミック アクセス ポリシー（DAP）を割り当て Advanced Endpoint Assessment ライセンスを使用すると、バージ すように非準拠コンピュータのアップデートを試行する機能を Scan を拡張できます。 シスコは、Host Scan でサポートされるアプリケーションとバー に、Cisco Secure Desktop とは異なるパッケージで、タイムリー を提供できます。

機能	説明
単純化されたログイン前評価と定期的なチェック	Cisco Secure Desktop では、離れた場所にある Microsoft Windows コ に対するログイン前チェックと定期的なチェックを簡単に設定でき Secure Desktop では、チェックの単純化されたグラフィカルなビュ て、エンドポイント チェック条件の追加、変更、削除、条件の設 す。このグラフィカル ビューを使用してチェックのシーケンスの設 クの分岐へのリンク、ログインの拒否、エンドポイント プロファイ てを行う際、Cisco Secure Desktop Manager は変更内容を XML ファ します。返された結果と、接続タイプや複数のグループ設定など、 データ タイプを使用して、DAP を生成しセッションに適用するよ を設定できます。
VPN アクセス ポリシー機能	
ダイナミック アクセス ポリシー（DAP）	VPN ゲートウェイは動的な環境で動作します。個々の VPN 接続に 変更されるイントラネット設定、組織内の各ユーザーが持つさまざ ル、および設定とセキュリティ レベルが異なるリモート アクセス のログインなど、複数の変数が影響する可能性があります。VPN 環 ザー認可のタスクは、スタティックな設定のネットワークでの認可 もかなり複雑です。 ASA ではダイナミック アクセス ポリシー（DAP）によって、これ まな変数に対処する認可機能を設定できます。ダイナミック アクセ は、特定のユーザー トンネルまたはユーザー セッションに関連付 アクセス コントロール属性を設定して作成します。これらの属性に のグループ メンバーシップやエンドポイント セキュリティの問題 す。つまり、ASA では、定義したポリシーに基づき、特定のセッシ クセス権が特定のユーザーに付与されます。セキュリティ アプライ ユーザーが接続するときに、1 つまたは複数の DAP レコードから属 たは集約して、DAP を生成します。DAP レコードは、リモート ラ ンドポイント セキュリティ情報および認証されたユーザーの AAA 基づいて選択されます。選択された DAP レコードは、ユーザー ド はセッションに適用されます。
管理者の区別	同じデータベース（RADIUS または LDAP）下で、通常のリモート ユーザーと管理ユーザを区別できます。TELNET や SSH など、さ 法を使用したコンソールへのアクセスを作成し、管理者に限定する ます。これは、IETF RADIUS サービス タイプ属性に基づいていま
プラットフォームの機能拡張	
リモート アクセス VPN 接続のための VLAN のサポート	グループ レベルまたはユーザー レベルでクライアント トラフィッ ング（タギング）をサポートします。この機能は、IPSec および S ベースの接続だけでなく、クライアントレスとも互換性があります

機能	説明
ASA 5510 の VPN ロード バランシング	ロード バランシング サポートが、Security Plus ライセンスを持応型セキュリティ アプライアンスに拡張されています。
暗号化条件付きデバッグ	ピア IP アドレス、暗号化エンジンの接続 ID、セキュリティ パデックス（SPI）などの事前に定義された暗号化条件に基づいてをデバッグできます。デバッグ メッセージを特定の IPSec 操作バッグ出力の量を減らすことで、多数のトンネルがある ASA をブルシューティングできます。
ブラウザベースの SSL VPN 機能	
拡張されたポータル設計	バージョン 8.0(2) には、よりわかりやすく構成され視覚的に魅されたエンド ユーザー インターフェイスが含まれています。
カスタマイゼーション	ユーザーに見えるすべての内容を、管理者が定義してカスタマ
FTP のサポート	CIFS（Windows ベース）に加え、FTP 経由でファイルにアクセ
プラグイン アプレット	バージョン 8.0(2) では、事前にインストールされたクライアンションを必要としない、TCP ベースのアプリケーションをサポムワークが追加されています。Java アプレットを使用して、ブSSL VPN ポータルからこれらのアプリケーションにアクセスでTELNET、SSH、RDP、および VNC がサポートされています。
スマート トンネル	スマート トンネルは、ASA をパスウェイとし、ブラウザベースセッションを使用した、アプリケーションとリモート サイト間バージョン 8.0(2) では、スマート トンネル アクセスを許可するンを特定し、アプリケーションのパスと、アクセスを許可する、そのチェックサムの SHA-1 ハッシュを指定できます。Lotおよび Microsoft Outlook Express は、スマート トンネル アクセスプリケーションの例です。 スマート トンネル接続を開始するリモート ホストでは、MicroVista、Windows XP、または Windows 2000 が実行されている必ウザで Java と Microsoft ActiveX のいずれかまたは両方が有効に要があります。
RSS ニュースフィード	管理者はクライアントレス ポータルに RSS ニュースフィード情会社のニュースやその他の情報をユーザーの画面で表示できま
個人用ブックマークのサポート	ユーザーは独自のブックマークを定義できます。これらのブックイル サーバに保存されます。
変換の拡張	Adobe Flash や Java WebStart など、クライアントレス接続上でWeb コンテンツのサポートがいくつか追加されています。
IPv6	パブリック IPv4 接続上で IPv6 リソースへのアクセスが許可さ

機能	説明
Web フォルダ	Windows オペレーティング システムから接続しているブラウザベ VPN ユーザーは、共有ファイル システムを参照し、各種の操作を す。可能な操作は、フォルダの参照、フォルダとファイルのプロパ 照、作成、移動、コピー、ローカル ホストからリモート ホストへ リモート ホストからローカル ホストへのコピー、削除です。Inter には、いつ Web フォルダにアクセスできるかが表示されます。こ にアクセスすると、別のウィンドウが開いて共有フォルダが表示さ フォルダおよびドキュメントのプロパティで許可されている場合、 ここで Web フォルダの機能を実行できます。
Microsoft Sharepoint の機能拡張	Microsoft Sharepoint の Web Access サポートが拡張され、マシン上で Microsoft Office アプリケーションとブラウザが統合され、サーバで いるドキュメントを参照、変更、保存できます。バージョン 8.0(2 Windows Server 2003 の Windows Sharepoint Services 2.0 がサポート す。
HTTP/HTTPS プロキシ サーバ	
PAC サポート	ブラウザにダウンロードするプロキシ自動設定（PAC）ファイルの 定できます。ダウンロードが完了すると、PAC ファイルは JavaScr 用して各 URL のプロキシを識別します。
プロキシ除外リスト	ASA が外部プロキシ サーバに送信できる HTTP 要求から除外する トを設定できます。
VPN ネットワーク アクセス コントロール機能	
SSL VPN トンネルのサポート	ASA では、AnyConnect VPN クライアント セッションを確立するエ トの NAC ポスチャ検証機能が提供されます。
監査サービスのサポート	クライアントがポスチャ検証の要求に応答しない場合は、ASA を設 のクライアントの IP アドレスをオプションの監査サーバに渡すこ す。監査サーバは、ホストのヘルスを評価するために、ホスト IP 使用してホストを直接調べます。たとえば、ホストのウイルス チ トウェアがアクティブかつ最新かどうかを確認するためにホストを ができます。監査サーバは、リモート ホストとの対話を完了すると ホストのヘルスを示すトークンをポスチャ検証サーバに渡します。 ストが正常であることを示すトークンを受信すると、ポスチャ検証 トンネル上のトラフィックに適用するためのネットワーク アクセ を ASA に送信します。
アプリケーション インスペクション機能	
モジュラ ポリシー フレームワーク検査クラス マップ	トラフィックは、検査クラスマップ内の複数の一致コマンドのいず します。以前は、トラフィックがクラス マップに一致するために マップ内のすべての一致コマンドに一致する必要がありました。

機能	説明
暗号化されたストリームの AIC と AIC Arch の変更	TLS への HTTP 検査を提供し、WebVPN HTTP および HTTPS ス AIC/MPF インスペクションが可能です。
SCCP および SIP 用の TLS プロキシ[3]	暗号化されたトラフィックを検査できます。実装には、Cisco C 話する、SSL で暗号化された VoIP シグナリング、つまり Skinn 含まれます。
CCM 用の SIP の機能拡張	シグナリング ピンホールに関して、CCM 5.0 および 6.x との相 しています。
SIP 用の IPv6 のサポート	SIP インスペクション エンジンは IPv6 アドレスをサポートして アドレスは、URL、Via ヘッダー フィールド、SDP フィールド す。
フル RTSP PAT サポート	TCP フラグメント リアセンブリのサポート、RTSP に対するス 析ルーチン、RTSP トラフィックを保護するセキュリティ拡張を
アクセス リスト機能	
拡張されたサービス オブジェクト グループ	TCP サービス、UDP サービス、ICMP タイプ サービス、および ルが混在するサービス オブジェクト グループを設定できます。 特定の ICMP タイプ オブジェクト グループとプロトコル オブジ プが不要になります。拡張されたサービス オブジェクト グル サービスと宛先サービスも指定します。アクセス リスト CLI に サポートするようになりました。
アクセス リストの名前変更機能	アクセス リストの名前を変更できます。
ライブ アクセス リスト ヒット カウント	複数のアクセス リストからの ACE のヒット カウントが含まれ ト カウント値は、トラフィックが特定のアクセス ルールにヒッ 表します。
攻撃防止機能	
適応型セキュリティ アプライアンスへの管理トラフィックの接続制限を設定します。	レイヤ 3/4 管理クラス マップでは、**set connection** コマンドを指
脅威の検出	基本的な脅威検出と脅威検出のスキャンを有効にし、DoS 攻撃 などの攻撃を監視できます。スキャン攻撃に対しては、攻撃元 的に回避できます。また、スキャン脅威統計をイネーブルにし ト、プロトコル、アクセス リストに対する有効なトラフィック フィックの両方を監視できます。
NAT の機能	

機能	説明
トランスペアレント ファイアウォールの NAT サポート	トランスペアレント ファイアウォールの NAT を設定できます。
モニタリング機能	
セキュア ロギング	SSL または TLS と TCP を使用した syslog サーバへのセキュア接続されたシステム ログ メッセージ コンテンツをイネーブルにできまリーズ適応型セキュリティ アプライアンス上ではサポートされま
ASDM 機能	
再設計されたインターフェイス	論理一貫性とナビゲーションの容易さを提供するために、情報を再す。
オンスクリーン ヘルプの拡張	ASDMには、画面上の機能と設定のオプションの説明があります。他の情報源を参照する必要を減らすことができます。
ビジュアル ポリシー エディタ	ビジュアル ポリシー エディタにより、管理者はアクセス コントロシーとポスチャ チェックを設定できます。
ファイアウォール ダッシュボード	ホーム ページから、レート制限を超えるトラフィックと、ホストリスト、ポート、またはプロトコルにより許可またはドロップされたクをモニタすることによって、ネットワークに対する脅威を追跡でなりました。
アクセシビリティ機能	キーボードナビゲーション、グラフィックスの代替テキスト、およたスクリーン リーダー サポートなどの機能が追加されました。
複雑な設定のサポート	変更を適用しなくても、ペイン間を移動できます。これによりそのイスに適用する前に、マルチペイン設定を入力できます。
Device List	ASDMは最近アクセスされたデバイスのリストを維持し、デバイストを切り替えることができます。
SSL VPN 設定ウィザード	新しい SSL VPN 設定ウィザードでは、基本 SSL VPN 接続を設定す順ごとのガイドが示されます。
Startup Wizard の機能拡張	Startup Wizard では、インストールされている CSC SSM にトラフように適応型 ASA を設定できるようになりました。
ASDM アシスタントの機能強化	セキュア音声を設定するアシスタントが追加されました。
Packet Capture Wizard	パケット キャプチャ ウィザードでは、PCAP フォーマットでスニスを取得およびダウンロードすることができます。
サービス ポリシー ルール ウィザード	IPS 仮想化をサポートするように更新されました。
証明書管理の拡張機能	証明書管理 GUI は再編成されて簡素化されました。

[2] （1）クライアントレス SSL VPN 機能は、PIX セキュリティ アプライアンスではサポートされていません。
[3] （2）TLS プロキシは、PIX セキュリティ アプライアンスではサポートされていません。

バージョン 7.2 の新機能

ASA 7.2(5)/ASDM 5.2(5) の新機能

リリース：**2010年5月11日**

ASA 7.2(5)/ASDM 5.2(5) には新機能はありませんでした。

ASA 7.2(4)/ASDM 5.2(4) の新機能

リリース：**2008年4月7日**

機能	説明
リモート アクセス機能	
ローカルアドレス プールの編集	アドレス プールは、目的の接続に影響を与えることなく編集できます。中でありプールから排除されていない場合、接続は影響を受けません。のアドレスがプールから除去されている場合、接続はダウンします。 バージョン *7.0(8)* および *8.0(4)* でも使用可能です。
ルーティング機能	

機能	説明
IPv6 マルチキャスト リスナーディスカバリ プロトコル v2 サポート	ASA は、マルチキャスト リスナー ディスカバリ プロトコル（MLD）バージ ポートするようになりました。これにより直接接続リンク上のマルチキャス リスナーの存在を検出し、特にどのマルチキャスト アドレスがそれらの隣接 象になるかを検出します。ASA はマルチキャスト アドレス リスナーまたはホ りますが、マルチキャスト ルータにはならず、マルチキャスト リスナー ク し、マルチキャスト リスナー レポートのみを送信します。 次のコマンドがこの機能をサポートしています。 • **clear ipv6 mld traffic** clear ipv6 mld traffic コマンドを使用すると、すべてのマルチキャスト リ トラフィック カウンタをリセットできます。 • **show ipv6 mld traffic** show ipv6 mld コマンドを使用すると、すべてのマルチキャスト リスナー フィック カウンタを表示できます。 • **debug ipv6 mld** debug ipv6 コマンドのこの機能拡張により、ユーザーは MLD プロトコル ティが正常に機能しているかどうかを確認するための MLD 用デバッグ を表示できます。 • **show debug ipv6 mld** show debug ipv6 コマンドのこの機能拡張により、ユーザーは debug ipv6 m なっているか無効になっているかを表示できます。 バージョン *8.0(4)* でも使用可能です。
プラットフォーム機能	
ASA 5505 トランク ポート上のネイティブ VLAN サポート	トランク ポート上でネイティブ VLAN を使用できます（**switchport trunk na** マンドを参照してください）。 ASDM で、[Configuration] > [Device Setup] > [Interfaces] > [Switch Ports] > [Edit を参照してください。 バージョン *8.0(4)* でも使用可能です。
接続機能	
clear conn コマンド	**clear conn** コマンドは、接続を削除するために追加されました。 バージョン *7.0(8)* および *8.0(4)* でも使用可能です。

機能	説明
フラグメントの完全リアセンブル	**fragment** コマンドは **reassembly full** キーワードで拡張され、デバイス経由 グされるフラグメントの完全リアセンブルが可能になりました。デバイス ラグメントは、常に完全にリアセンブルされます。 バージョン *7.0(8)* および *8.0(4)* でも使用可能です。
QoS トラフィック シェーピング	ASA などの、ファスト イーサネットを使用してパケットを高速に送信す 在し、そのデバイスがケーブル モデムなどの低速デバイスに接続されて ブル モデムがボトルネックとなり、ケーブル モデムでパケットが頻繁に す。回線速度が異なるネットワークを管理するため、固定の低速でパケ ようにセキュリティ アプライアンスを設定できます。**shape** コマンドを参 い。また、**crypto ipsec security-association replay** コマンドも参照してくだ マンドでは、IPSec アンチ リプレイ ウィンドウ サイズを設定できます。 プライオリティ キューイングには、パケットの並べ替えという副作用があ パケットの場合、リプレイ攻撃防止ウィンドウ内にない異常なパケットに 告 syslog メッセージが生成されます。これらの警告は、プライオリティ は誤報となります。この新しい機能は、誤報の可能性を防ぎます。 ASDM で、[Configuration] > [Firewall] > [Security Policy] > [Service Policy R Service Policy Rule] > [Rule Actions] > [QoS] を参照してください。トラフ ングでサポートされているトラフィック クラスは、すべてのトラフィッ class-default だけであることに注意してください。 バージョン *8.0(4)* でも使用可能です。
ファイアウォール機能	

機能	説明
TCP 正規化の機能拡張	特定のパケットタイプに対し、TCP正規化のアクションを設定できるようにな 以前は、これらの種類のパケットに対するデフォルトのアクションは、パケッ プすることでした。パケットを許可するように TCP ノーマライザを設定でき りました。 • TCP の無効な ACK のチェック（**invalid-ack** コマンド） • ウィンドウを超えた TCP パケット シーケンスのチェック（**seq-past-win** ド） • データ チェックを使用した TCP SYN-ACK（**synack-data** コマンド） TCP アウトオブオーダー パケット バッファ タイムアウトを設定することも （**queue** コマンドの **timeout** キーワード）。以前は、タイムアウトは4秒でし アウトを別の値に設定できるようになりました。 MSS を超えたパケットのデフォルト アクションが、ドロップから許可に変更 （**exceed-mss** コマンド）。 次の設定できないアクションが、次のパケット タイプに対してドロップから 更されました。 • Bad option length in TCP • TCP Window scale on non-SYN • Bad TCP window scale value • Bad TCP SACK ALLOW option ASDM で、[Configuration] > [Global Objects] > [TCP Maps] ペインを参照して バージョン *8.0(4)* でも使用可能です。
SIP プロビジョナル メディアのタイムアウト	SIP 暫定メディアのタイムアウトを、**timeout sip-provisional-media** コマンドを 定できるようになりました。 ASDM で、[Configuration] > [Properties] > [Timeouts] ペインを参照してくださ バージョン *8.0(4)* でも使用可能です。
Ethertype ACL MAC の機能強化	EtherType ACL は、非標準 MAC を許可するように強化されています。既存の のルールが保持され、新しいルールを追加する必要はありません。 バージョン *7.0(8)* および *8.0(4)* でも使用可能です。
トラブルシューティングとモニタリングの機能	

機能	説明
capture コマンドの強化	**capture type asp-drop** *drop_code* コマンドは、**all** を *drop_code* として受け入たので、セキュリティチェックが原因でドロップされたものを含め、AS るすべてのパケットをキャプチャできるようになりました。 バージョン *7.0(8)* および *8.0(4)* でも使用可能です。
MIB の機能拡張	CISCO-REMOTE-ACCESS-MONITOR-MIB はより完全に実装されます。 *8.0(4)* でも使用可能です。
show asp drop コマンドの強化	カウンタが最後にクリアされた時間を示すタイムスタンプが出力に含まれ ました（**clear asp drop** コマンドを参照）。また、説明の横にドロップ理 が表示されるため、そのキーワードを使用して簡単に **capture asp-drop** コ できます。 バージョン *7.0(8)* および *8.0(4)* でも使用可能です。
clear asp table コマンド	**clear asp table** コマンドが、**show asp table** コマンドによるヒット出力をク に追加されました。 バージョン *7.0(8)* および *8.0(4)* でも使用可能です。
show asp table classify hits コマンドの強化	hits オプションが **show asp table classify** コマンドに追加され、asp テーブル リアされた最終時刻を示すタイムスタンプが表示されるようになりまし くない hits 値があるルールも表示されます。これによりユーザーはどのル したかをすばやく参照できます。特に単純な設定であると **show asp table** ドで最終的に何百ものエントリが存在するようになるため便利です。 バージョン *7.0(8)* および *8.0(4)* でも使用可能です。
show perfmon コマンド	次の速度出力が追加されました。[TCP Intercept Connections Established]、 Attempts]、[TCP Embryonic Connections Timeout]、および [Valid Connection Intercept] バージョン *7.0(8)* および *8.0(4)* でも使用可能です。

機能	説明
memory tracking コマンド	次の新しいコマンドが、このリリースで導入されました。 • **memory tracking enable**：このコマンドにより、ヒープ メモリ要求のトラ有効になります。 • **no memory tracking enable**：このコマンドは、ヒープ メモリ要求の追跡を現在収集したすべての情報をクリーンアップし、ツール自体によって使べてのヒープ メモリをシステムに返します。 • **clear memory tracking**：このコマンドは現在収集したすべての情報を消去それ以降もメモリ要求の追跡は継続します。 • **show memory tracking**：このコマンドは、ツールの追跡対象である現在割ているメモリを、最上位呼び出し元関数アドレス別に示します。 • **show memory tracking address**：このコマンドは、メモリの各部分に分割り当てられているメモリを示しています。この出力は、ツールの追跡対在割り当てられている各メモリのサイズ、位置、および最上位呼び出し覧表示します。 • **show memory tracking dump**：このコマンドは、指定されたメモリ アドズ、位置、呼び出しスタックの一部、およびメモリ ダンプを表示します • **show memory tracking detail**：このコマンドは、ツールの内部動作への洞めに使用されるさまざまな内部の詳細を示しています。 バージョン *7.0(8)* および *8.0(4)* でも使用可能です。
フェールオーバー機能	
failover timeout コマンド	**failover timeout** コマンドに、静的固定機能とともに使用されるフェールオーバンスが不要になりました。 バージョン *7.0(8)* および *8.0(4)* でも使用可能です。
ASDM 機能	
Network Objects	ファイアウォール規則で使用できる真のネットワーク オブジェクトを追加でなりました。オブジェクトには名前を付けることができ、オブジェクトを編その変更はオブジェクトが使用される場所ではどこでも継承されます。また作成すると、ルールで指定したネットワークは自動的にネットワーク オブジトに追加され、どこでもそれらを再利用できます。それらの自動エントリも て編集できます。[Configuration] > [Objects] > [Network Objects/Groups] を参照い。
強化された ASDM ルール テーブル	ASDM ルール テーブルは、ポリシーの作成を合理化するように再設計されて

ASA 7.2(3)/ASDM 5.2(3) の新機能

リリース：**2007年8月15日**

機能	説明
リモート アクセス機能	
WebVPN ロードバランシング	適応型セキュリティ アプライアンスは、ロードバランシングのためにFQ ポートするようになりました。FQDN を使用して WebVPN ロードバラン るには、ロード バランシング用に FQDN の使用を有効にし、**redirect-fqd** ドを入力する必要があります。DNS サーバにインターフェイス外の各適応 アプライアンスのエントリを（まだない場合には）追加します。それぞれ リティ アプライアンスの外部 IP アドレスに、ルックアップ用にそのアド られた DNS エントリが設定されている必要があります。これらの DNS エ ては、逆ルックアップもイネーブルにする必要があります。**dns domain-** マンドを使用して、適応型セキュリティ アプライアンスで DNS ルックア ルにします。inside の部分には、DNS サーバへのルートを持つ任意のイン を指定します。最後に、適応型セキュリティ アプライアンス上の DNS サ レスを定義する必要があります。次に示すのは、この拡張機能に関連付け しい CLI です。**redirect-fqdn** {**enable** | **disable**}。 ASDM で、[Configuration] > [VPN] > [Load Balancing] を参照してください バージョン *8.0(3)* でも使用可能です。
クライアントレス SSL VPN キャッシング静的コンテンツの機能拡張	クライアント SSL VPN キャッシュ コマンドには次の 2 つの変更があります **cache-compressed** コマンドが非推奨になりました。 新しい **cache-static-content** コマンドは、すべての静的コンテンツをキャッ に ASA を設定します。これはつまり、SSL VPN の書き換えが行われない シュ可能 Web オブジェクトのことです。これには、画像や PDF ファイル ツが含まれています。 コマンドの構文は次のとおりです。**cache-static-content** {**enable** | **disable**}。 は、静的コンテンツ キャッシングが無効になっています。 例： `hostname (config) # webvpn` `hostname (config-webvpn) # cache` `hostname (config-webvpn-cache) # cache-static-content enable` hostname (config-webvpn-cache) # ASDM で、[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Acce > [Content Cache] を参照してください。 バージョン *8.0(3)* でも使用可能です。

機能	説明
スマートカードの取り外し切断	この機能により、セントラル サイトの管理者は、スマート カードを取り外すティブなトンネルを削除するためのリモート クライアント ポリシーを設定Cisco VPN リモート アクセス ソフトウェア クライアント（IPSec と SSL の両フォルトでは、ユーザーが認証に使用されるスマート カードを取り外すときVPN トンネルを切断します。次の CLI コマンドは、スマート カードが取り外に既存の VPN トンネルを切断します。**smartcard-removal-disconnect** {**enable**このオプションは、デフォルトで有効です。 ASDM で、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [G> [Add/Edit Internal/External Group Policies] > [More Options] を参照してくださ バージョン *8.0(3)* でも使用可能です。
プラットフォーム機能	
ASA 5510 Security Plus ライセンスにより、ポート 0 と 1 のギガビット イーサネットが可能になります。	ASA 5510 ASA は、ポート 0 と 1 の GE（ギガビット イーサネット）を有効にPlus ライセンスを持つようになりました。ライセンスを Base から Security Pグレードした場合、外部 Ethernet 0/0 および Ethernet 0/1 の容量は、元の FEイーサネット）の 100 Mbps から GE の 1000 Mbps に増加します。インターEthernet 0/0 および Ethernet 0/1 のままです。**speed** コマンドを使用してインタの速度を変更します。また、show interface コマンドを使用して各インターフ在の設定速度を確認します。 バージョン *8.0(3)* でも使用可能です。
ASA 5505 の増加した VLAN の範囲	ASA 5505 ASA は 1 ～ 4090 の範囲の VLAN ID をサポートするようになりまし1 ～ 1001 の VLAN ID のみがサポートされていました。 バージョン *8.0(3)* でも使用可能です。
トラブルシューティング機能	
capture コマンドの強化	**capture** コマンドの拡張により、ユーザーはトラフィックをキャプチャし、で表示することができます。コマンドライン オプションを指定して、個別のストを設定する必要なくトラフィックをフィルタすることもできます。この は、**real-time** と 5 タプルの **match** オプションが追加されます。 **capture** *cap_name* [**real-time**] [**dump**] [**detail** [**trace**] [**match** *prot* {**host** *ip* | *ip mas* | **lt** | **gt**} *port*] {**host** *ip* | *ip mask* | **any**} [{**eq** | **lt** | **gt**} *port*]] バージョン *8.0(3)* でも使用可能です。
アプリケーション インスペクション機能	

機能	説明
ESMTP over TLS のサポート	この拡張機能は、esmtp ポリシー マップに構成パラメータ **allow-tls** [**actio** ます。デフォルトでは、このパラメータはイネーブルになっていません。 ESMTP インスペクションは 250-STARTTLS エコー応答をサーバからマス クライアントから **STARTTLS** コマンドをマスクすることもありません。 答コードで応答したら、ESMTP インスペクションはそれ自体がオフにな セッションの ESMTP トラフィックは検査されなくなります。**allow-tls act** タが設定されていると、ESMTP セッションで TLS が開始されたときに、 ジ ASA-6-108007 が生成されます。 `policy-map type inspect esmtp esmtp_map` `parameters` `allow-tls [action log]` **allow-tls** パラメータに関連付けられたカウンタを表示するための新しい行 **service-policy inspect esmtp** コマンドに追加されました。これは **allow-tls** が プで設定されている場合にのみ存在します。デフォルトでは、このパラメ ブルになっていません。 `show service-policy inspect esmtp` `allow-tls, count 0, log 0` この拡張機能は、**allow-tls** パラメータの新しいシステム ログ メッセージ これは esmtp セッションでサーバがクライアントの **STARTTLS** コマンド 答コードで応答したことを示します。ESMTP インスペクション エンジン のトラフィックは検査されなくなりました。 システム ログの番号と形式： %ASA-6-108007: TLS started on ESMTP session between client *<client-side interface-name>:<client IP address>/<client port> and server <server-side interfac IP address>/<server port>* ASDM で、[Configuration] > [Firewall] > [Objects] > [Inspect Map] > [ESMTP ださい。 バージョン *8.0(3)* でも使用可能です。
DNS ガードの機能拡張	DNS ガードをイネーブルまたはディセーブルにするためのオプションが追 この機能をイネーブルにすると、1 つの DNS 要求に対して 1 つの DNS 応 れます。 ASDM で、[Configuration] > [Firewall] > [Objects] > [Inspect maps] > [DNS] さい。 バージョン *8.0(3)* でも使用可能です。

機能	説明
WAAS と ASA の相互運用性	ポリシーマップ クラス設定モードでWAASインスペクションを有効にするた **waas** コマンドが追加されました。この CLI は、機能の設定で柔軟性を最大限 に、モジュラ ポリシー フレームワークに統合されています。 **[no] inspect wa** は、デフォルトのインスペクション クラスおよびカスタム クラスマップの ます。このインスペクション サービスは、デフォルトでイネーブルではあり キーワードオプション waas は、WAAS 統計を表示するために、**show service-** コマンドに追加されました。 `show service-policy inspect waas` 新しいシステム ログ メッセージは、接続で WAAS 最適化が検出された場合 ます。WAAS 最適化接続では、すべての L7 検査サービス（IPS を含む）がバ ます。 システム ログの番号と形式： %ASA-6-428001：WAAS confirmed from in_interface:src_ip_addr/src_port to out_interface:dest_ip_addr/dest_port, inspection services bypassed on this connectio WAAS 接続で、新しい接続フラグ「W」が追加されました。show conn detail コ 新しいフラグを反映するように更新されています。 ASDM で、[Configuration] > [Firewall] > [Service Policy Rules] > [Add/Edit Servic > [Rule Actions] > [Protocol Inspection] を参照してください。 バージョン *8.0(3)* でも使用可能です。
DHCP 機能	
DHCP クライアント ID の拡張機能	**ip address dhcp** コマンドを使用してインターフェイスの DHCP クライアント ルにすると、一部の ISP でオプション 61 がインターフェイス MAC アドレス なされます。MAC アドレスが DHCP 要求パケットに含まれていない場合、IS 割り当てられません。この新しいコマンドを使用して、オプション 61 用にイ イス MAC アドレスを含めます。このコマンドを構成しない場合は、クライ 次のようになります。cisco-<MAC>-<interface>-<hostname> 次のコマンドが導入されました。**dhcp-client client-id interface** *interface_name* 次の画面が変更されました。[Configuration] > [Device Management] > [DHCP] Server]。次に [Advanced] をクリックします。 バージョン *8.0(3)* でも使用可能です。
モジュール機能	

機能	説明
データプレーンキープアライブ メカニズムの追加	ASA を構成して、AIP SSM がアップグレードされた場合に、フェールオせないようにできます。以前のリリースでは、AIP SSM がある 2 つの AS オーバーで構成されている場合に AIP SSM ソフトウェアが更新されると フトウェアの更新を有効にするためにリブートまたは再起動を必要とする フェールオーバーをトリガーします。 バージョン *7.0(7)* および *8.0(3)* でも使用可能です。
ASDM 機能	
ASDM バナー拡張機能	適応型セキュリティ アプライアンス ソフトウェアは、ASDM バナーをサ す。設定した場合、ASDM を起動すると、このバナー テキストが、続行 めのオプションとともに、ダイアログボックスに表示されます。[Continu 選択すると、バナーが閉じて通常どおりログインが完了しますが、[Disco ンを選択するとバナーが閉じて接続が終了します。この機能拡張は顧客に 書面によるポリシー条件の受け入れを求めます。 次に示すのは、この拡張機能に関連付けられている新しい CLI です。 **banner** {**exec** | **login** | **motd** | **asdm**} *text* **show banner** [**exec** | **login** | **motd** | **asdm**] **clear banner** ASDM で、[Configuration] > [Properties] > [Device Administration] > [Banner ださい。 バージョン *8.0(3)* でも使用可能です。
Cisco Content Security and Control（CSC）Damage Cleanup Services（DCS）機能のイベントと統計	Cisco Content Security and Control（CSC）6.2 ソフトウェアを使用すると、 Damage Cleanup Services（DCS）機能用のイベントと統計を提供します。 ントおよびサーバからマルウェアを削除して、システム レジストリとメ す。
クライアント ソフトウェアの場所	クライアント ソフトウェアの場所のリストに、Linux または Mac のシス イアント更新を許可するためのサポートが追加されました。 ASDM で、[Configuration] > [Remote Access VPN] > [Network (Client) Acces > [IPSec] > [Upload Software] > [Client Software] を参照してください。 バージョン *8.0(3)* でも使用可能です。

ASA 7.2(2)/ASDM 5.2(2) の新機能

リリース：**2006年11月22日**

機能	説明
モジュール機能	
SSM でのパスワードのリセット	ユーザー「cisco」の AIP-SSM および CSC-SSM のパスワードは、デフォルト値にリセットして戻すことができます。 次のコマンドが追加されました。**hw-module module password-reset**
AAA 機能	

機能	説明
HTTP（S）認証チャレンジの柔軟設定	新しい **aaa authentication listener** コマンドにより、ASA は Web ページをジョン 7.2(1) で現在使用されているフォームベースのリダイレクト方法を 7.2(2) では、7.2(1) より前に使用可能であった、基本 HTTP 認証を使用す入しました。基本 HTTP および HTTPS 認証では、カスタム ログイン ウされます。次の場合に、基本 HTTP 認証を使用できます。 • 適応型セキュリティ アプライアンスでリスニング ポートを開きたく • ルータ上の NAT を使用し、適応型セキュリティ アプライアンスで損ページ用のトランスレーション ルールを作成しない場合。 • 基本 HTTP 認証の方がネットワークでより効果的に機能する可能性とえば、電子メールに URL が埋め込まれている場合などのように、アプリケーションでは基本認証の方が適していることがあります。 （注） デフォルトでは、**aaa authentication listener** コマンドは設バージョン 7.1 aaa の動作を 7.2(2) のデフォルトにします。ジョン 7.2(1) 設定がバージョン 7.2(2) にアップグレードさ適切な **aaa authentication listener** コマンドが設定に追加さの動作はアップグレードでは変更されません。 基本的な HTTP をサポートするために、**virtual http** コマンドが復元されまカスケード認証要求がある場合に、基本認証とともに必要です。 バージョン 7.2(1) では、基本認証はフォーム ベース認証方法に置き換えの方法では HTTP および HTTPS 接続は ASA によりサポートされる認証レクトされます。認証が成功したら、ブラウザは本来意図されていた UR レクトされます。これは、以下を提供するために実行されました。 • さらにグレースフルなサポート認証チャレンジ処理 • http と https のどちらのユーザーにも同一の認証エクスペリエンス ワーク ユーザーの永続的なログオン/ログオフ URL。この方式では、**aaa** が有効になっている各インターフェイス上の ASA で、開かれているポーする必要がありません。
インターフェイス機能	

機能	説明
VLAN の最大数の増加	ASA 5505 適応型セキュリティ アプライアンス上の Security Plus ライセンスに対 最大数が、5（3 つのフル機能インターフェイス、1 つのフェールオーバー イ イス、1 つのバックアップ インターフェイスに制限されるインターフェイス フル機能インターフェイスに増加されました。また、トランク ポート数も 1 加されました。フル機能のインターフェイスの数が 20 になり、バックアッ ターフェイスを停止するために **backup interface** コマンドを使用する必要がな た。つまり、バックアップ ISP インターフェイス用にフル機能のインターフ 用できるようになりました。backup interface コマンドは、これまでどおり Ea 用に使用できます。 VLAN 制限も増加されました。ASA 5510 適応型セキュリティ アプライアンス ライセンスは 10 から 50 に、Security Plus ライセンスは 25 から 100 に増加さ ASA 5520 適応型セキュリティ アプライアンスでは、100 から 150 に、ASA セキュリティ アプライアンスでは、200 から 250 に増加されました。
ASA 5510 基本ライセンスでの物理インターフェイスの追加	ASA モデル 5510 上で、使用可能な物理インターフェイスの最大数が、3 + 1 （5）に変更されています。
認定機能	
FIPS 140-2	7.2(2) は、FIPS 140 レベル 2 の検証に従っています。
ASDM 機能	
マルチキャスト サポート	次のマルチキャスト コマンドのサポートが追加されました。 • **mfib forwarding** • **multicast boundary** • **pim bidir-neighbor-filter** • **pim neighbor-filter** • **pim old-register-checksum**
ローカル デモ モード	ASDM は、ローカル デモ モードでデバイスに接続されていると機能します。

ASA 7.2(1)/ASDM 5.2(1) の新機能

リリース：**2006年5月31日**

機能	説明
プラットフォーム機能	

機能	説明
ASA 5505 サポート	ASA 5505 は、このリリースで導入されました。ASA 5505 は、小規模オフィス、企業の在宅勤務者向け環境のための新しいモデルであり、内蔵トイーサネット スイッチを備え、Easy VPN、デュアル ISP をサポートし多くの機能があります。 ASA 5505 には、IP フォンなどの Power over Ethernet（PoE）デバイスに使スイッチ ポートがあります。ただしこれらのポートは、その用途のみにません。それらはイーサネット スイッチ ポートとしても使用できます。接続されていない場合、電力はポートに供給されません。
ASA 5550 サポート	ASA 5550 は、ギガビット クラスのセキュリティ サービスを提供し、信頼フォームファクタで大企業およびサービス プロバイダ ネットワーク向けクティブ高可用性を可能にします。イーサネットベースおよびファイバインターフェイス形式でギガビット接続を高密度 VLAN 統合に提供するり、企業はネットワークを多数のハイパフォーマンス ゾーンにセグメンリティを向上させることができます。
Easy VPN 機能（ASA 5505 のみ）	
クライアントモード（ポートアドレス変換とも呼ばれる）およびネットワーク拡張モード	• クライアント モード：ASA 5505 プライベート ネットワーク上のデレスを非表示にします。これにより ASA 5505 プライベート ネットベてのトラフィックは、単一送信元の、割り当てられた IP アドレスル サイト ASA のプライベート ネットワークに着信するようになりル サイトから ASA 5505 プライベート ネットワーク上のデバイスにりアクセスしたりすることはできませんが、割り当てられた IP アドすることはできます。 • ネットワーク拡張モード：ASA の背後のデバイスが、トンネルを介5505 プライベート ネットワーク上のデバイスに直接アクセスするこす。セントラル サイトから ASA 5505 ネットワーク上のデバイスにりアクセスしたりできます。 ASA 5505 にはデフォルト モードはありません。使用するモードを指定すす。
自動トンネル開始	NEM をサポートしますが、クライアント モードはサポートしません。設いるグループ名、ユーザー名、およびパスワードを使用してトンネルを
IKE および IPsec のサポート	ASA 5505 は、事前共有キーおよび証明書（RSA-SIG）をサポートします。有キーに IKE アグレッシブ モードを、RSA-SIG ベースのキー交換には Iドを使用します。Cisco ASA 5505 は、IPsec、IPsec over NAT-T、および IPセッションを開始できます。

機能	説明
セキュア ユニットの認証（SUA）	動的に生成される認証クレデンシャルまたはトンネル開始時に入力する静的 シャルを使用した ASA 5505 認証をサポートします。SUA を有効にすると、 ブラウザまたはインタラクティブ CLI を使用して IKE トンネルを手動でト 要があります。
個別のユーザー認証（IUA）	内部ネットワークでの個々のクライアントの静的およびワンタイム パスワー 効にします。IUA と SUA は相互に独立しています。それらは組み合わせて 機能します。
トークンベース認証	Security Dynamics（SDI）SecurID ワンタイム パスワードをサポートします。
HTTP リダイレクションによる認証	SUA またはユーザー名とパスワードが設定されていない場合または IUA が に、認証されていない HTTP トラフィックをログイン ページにリダイレクト
ロード バランシング	デュアル ISP バックアップで設定されている ASA 5505 は、インターネット 用できる 2 つのイーサネットポートを介して、クラスタベースの VPN ロー グをサポートします。ロードバランシング方式には、着信クライアントの接 「仮想ディレクタ」 IP アドレスが関係しています。仮想ディレクタ IP アド ているサーバはクラスタを形成します。そこでは 1 つのクラスタ メンバがク ターとして機能します。マスターは仮想ディレクタに送信される要求を受け IKE 通知メッセージを使用して、クライアントをクラスタ内の最適なサーバ クトします。現在の ISAKMP セッションが終了して、新しいセッションが最 に対して試行されます。 最適なサーバへの接続が失敗した場合、クライアントは（クラスタの仮想デ アドレスで）プライマリ サーバに再接続し、ロードバランシングの手順を繰り プライマリ サーバへの接続が失敗した場合、クライアントは次の設定済みバ サーバ（別のクラスタのマスターである場合もある）までロールオーバーし
フェールオーバー（バックアップ サーバ リストを使用）	プライマリ サーバに加え、10 台のバックアップ サーバのリストを設定でき 5505 は、プライマリ サーバとのトンネルを確立しようとします。その試行が と、ASA 5505 は、バックアップ サーバ リスト内の順番に従って、他の指定 バとのトンネルを確立しようとします。
デバイス パススルー	IP フォン パススルー機能と LEAP パススルーの両方の機能が含まれます。 プリンタや Cisco IP フォンなどの特定のデバイスは、認証を実行できないた 加できません。デバイス パススルーが有効になっていると、ASA 5505 は、I 場合にこれらのデバイスを認証から除外します。 Easy VPN リモート機能は、MAC アドレスの設定済みリストに基づいて、除 イスを識別します。ワイヤレス アクセス ポイントやワイヤレス ノードなど、 デバイスに関連する問題が存在しています。これらのデバイスは、ワイヤレ ネットワークに参加させるために LEAP/PEAP 認証を必要とします。LEAP/P テージの後になって初めて、ワイヤレス ノードが IUA を実行できるように ASA 5505 も、デバイス パススルーを有効にすると LEAP/PEAP パケットをバ す。これによりワイヤレス ノードが IUA に参加できるようになります。

機能	説明
IKE モード設定	IKE フェーズ I と XAUTH の後に ASA 5505 が要求する属性値を設定でき ル サイトのデバイスは VPN ポリシーをダウンロードし、ASA 5505 はセ 基づいて機能を動的に設定します。SUA、クリア保存パスワード、およ コンセントレータのリストを除いて、動的機能の設定は、トンネルが確立 のみ有効であり続けます。
Remote Management	ASA 5505 の管理を、設定済みの NEM がある外部インターフェイスとのト 暗号化なしの外部インターフェイスに対してサポートします。
Easy VPN ピア名の DNS 解決	ASA 5505 は、Easy VPN ピア名を DNS サーバで解決します。CLI では、 ントの DNS 名を指定できます。
スプリット トンネリング	クライアントは、セントラル サイトへのトンネリングによってアクセス のネットワークのリストに基づいて、トンネル経由で送信するトラフィッ ます。スプリット トンネル ネットワーク リストにリストされている以外 を送信先とするトラフィックは、暗号化されずに送信されます。ゼロ長リ リット トンネリングがなく、すべてのトラフィックがトンネルを経由す す。
プッシュ バナー	IUA を使用して認証しようとする個々のユーザーに対して、HTTP フォー 491 バイト バナー メッセージを設定できます。
アプリケーション インスペクション機能	
拡張 ESMTP インスペクション	この機能により、スパム、フィッシング、不正形式メッセージ攻撃、バッ フローおよびアンダーフロー攻撃などの攻撃を検出できます。また、アプ セキュリティとプロトコル準拠により、正常な ESMTP メッセージだけを 撃の検出や送受信者およびメール中継のブロックも行います。
DCERPC インスペクション	この機能により、DCERPC 検査マップを使用して DCERPC アプリケーシ ションに使用されるデフォルト設定値を変更できます。 DCERPC は、Microsoft 社の分散クライアント/サーバ アプリケーションで プロトコルです。このプロトコルによって、ソフトウェア クライアント プログラムをリモートで実行できるようになります。 通常は、クライアントがウェルノウン ポート番号で接続を受け入れるエ マッパー（EPM）というサーバに、必要なサービスについて動的に割り当 トワーク情報を問い合わせます。次に、クライアントは、サービスを提供 インスタンスへのセカンダリ接続をセットアップします。セキュリティ は、適切なポート番号とネットワーク アドレスへのセカンダリ接続を許 じて NAT または PAT を適用します。

機能	説明
拡張 NetBIOS インスペクション	この機能により、NetBIOS アプリケーション インスペクションに使用される設定値を変更できます。 NetBIOS アプリケーション インスペクションでは、NetBIOS ネーム サービスおよび NetBIOS データグラム サービス パケットに埋め込まれている IP アドレス実行します。また、プロトコル準拠チェックを行って、さまざまなフィールさの整合性を確認します。
拡張 H.323 インスペクション	この機能により、H.323 アプリケーション インスペクションに使用されるデ定値を変更できます。 H.323 インスペクションは RAS、H.225、H.245 をサポートし、埋め込まれたとポートをすべて変換する機能を備えています。ステートのトラッキングとングを実行し、インスペクション機能のアクティベーションをカスケードでき インスペクションは、電話番号のフィルタリング、T.120 のダイナミック制御トンネル機能制御、プロトコルのステート トラッキング、H.323 通話時間制音声とビデオ制御をサポートします。
拡張 DNS インスペクション	この機能により、メッセージが DNS インスペクション ポリシー マップを使メータに違反したときのアクションを指定できます。DNS アプリケーションションは、DNS スプーフィングとキャッシュ ポイズニングを防ぐための DNジ制御をサポートしています。ユーザーが設定可能なルールによって、DNSドメイン名、リソース レコードの TYPE と CLASS に基づいたフィルタリンす。
拡張 FTP インスペクション	この機能により、FTP アプリケーション インスペクションに使用されるデフ値を変更できます。 厳密な FTP インスペクションには、セキュリティと制御を向上させるためのフィルタリングとセキュリティ チェック機能が用意されています。プロトコ性のインスペクションには、パケットの長さのチェック、デリミタとパケッチェック、コマンドのターミネータのチェック、およびコマンドの検証が含 また、ユーザーの値に基づいて FTP 接続をブロックできるので、FTP サイトにド用のファイルを置き、アクセスを特定のユーザーだけに制限できます。フイプ、サーバ名、および他の属性に基づいて、FTP 接続をブロックできますクション時に FTP 接続が拒否されると、システム メッセージのログが作成さ

機能	説明
拡張 HTTP インスペクション	この機能により、HTTP アプリケーション インスペクションに使用され 定値を変更できます。 HTTP アプリケーション インスペクションで HTTP のヘッダーと本文を まざまなデータ チェックができます。これらのチェックで、HTTP 構築、 イプ、トンネルプロトコル、メッセージプロトコルなどがセキュリティ を通過することを防止します。 HTTP アプリケーション インスペクションでトンネル アプリケーション 文字を含む HTTP 要求や応答をブロックして、悪意のあるコンテンツが 達することを防ぎます。HTTP 要求や応答ヘッダーのさまざまな要素のサ のブロッキング、HTTP サーバ ヘッダー タイプのスプーフィングもサポ す。
拡張 Skinny（SCCP）インスペクション	この機能により、SCCP（Skinny）アプリケーション インスペクションに フォルト設定値を変更できます。 Skinny アプリケーション インスペクションでは、パケット データ、ピン 放に埋め込まれている IP アドレスとポート番号を変換します。また、追 準拠チェックと基本的なステート トラッキングも行います。
拡張 SIP インスペクション	この機能により、SIP アプリケーション インスペクションに使用される 値を変更できます。 SIP は、インターネット会議、テレフォニー、イベント通知、およびイン セージングに広く使用されているプロトコルです。テキストベースの性 により、SIP ネットワークは数多くのセキュリティ脅威にさらされます。 SIP アプリケーション インスペクションでは、メッセージ ヘッダーおよ ス変換、ポートの動的開放、および基本的な健全性チェックが行われま ション セキュリティとプロトコル準拠により、正常な SIP メッセージだ ベースの攻撃を検出します。
インスタント メッセージ（IM）インスペクション	この機能により、インスタント メッセージ（IM）アプリケーション イン 使用されるデフォルト設定値を変更できます。 インスタント メッセージ（IM）アプリケーション インスペクションで、 アクセスの使用量を詳細に制御できます。また、機密情報の漏洩やその他 トワークを守ります。正規表現データベースのさまざまな検索パターン スタント メッセージ（IM）プロトコルをフィルタできます。フローが認 は、syslog が生成されます。 スコープを限定するには、アクセス リストから検査するトラフィック ス します。UDP メッセージの場合、対応する UDP ポート番号も設定でき Messenger および MSN Messenger のインスタント メッセージのインスペク トされています。

機能	説明
MPF ベースの正規表現分類マップ	この機能により、モジュラ ポリシー フレームワーク クラス マップで正規表現**match-any** 属性を持つ正規表現のグループを照合することができます。正規マップを使用して、特定のトラフィックの内容を照合できます。たとえば、ト内の URL 文字列の照合が可能です。
Radius アカウンティング インスペクション	この機能により、モバイル課金インフラストラクチャでの過剰請求攻撃からとができます。**policy-map type inspect radius-accounting** コマンドは、このパ導入されました。
H.323 用の GKRCS サポート	ITU-T H.323 勧告には 2 つの制御信号方式が記載されています。それらは Gate Control Signaling（GKRCS）と Direct Call Signalling（DCS）です。DCS は、C トキーパーによってサポートされます。この機能により、Gatekeeper Routed Co（GKRCS）制御信号方式サポートが追加されます。
Skinny ビデオ サポート	この機能により、SCCP バージョン 4.1.2 メッセージ サポートが追加され、**d**が有効である場合に検査機能によって処理されるメッセージ名が印刷されま4.0.1 メッセージがサポートされています。
SIP IP アドレス プライバシー	この機能により、すべてのトランザクション向けにインバウンド SIP パケッまれている外部 IP アドレスを保持することができます。ただし電話の実 IP ア表示にするための REGISTER を除きます（これはプロキシと電話との間で交め）。REGISTER メッセージと REGISTER メッセージへの応答は、そのメッ話とプロキシとの間で交換されるため、この操作からは免除されます。 この機能を有効にすると、SIP ヘッダーの外部 IP アドレスとインバウンド S の SDP データが保持されます。**ip-address-privacy** コマンドを使用してこの機します。
RTP/RTCP インスペクション	この機能は埋め込み IP アドレスに対して NAT を実行し、RTP と RTCP トラピンホールを開きます。Inspects SIP、Skinny、および H.323 で開いたピンホRTP パケットのみが流れるようにします。悪意のあるアプリケーションが UDクを送信して ASA で作成されたピンホールを使用することを防止するためにでは RTP と RTCP トラフィックをモニタし、RTP と RTCP パケットの有効性ます。
リモート アクセスおよびサイト間 VPN 機能	

機能	説明
ネットワークアドミッション コントロール	ネットワークアドミッションコントロール（NAC）は、その状態に基づ できます。このメソッドは、ポスチャ検証（PV）と呼ばれます。PV に パッチでアプリケーションを実行していることの確認と、リモート ホス いるウイルス対策ファイル、パーソナル ファイアウォール ルール、また トウェアが最新であることの確認を含めることができます。 ASA でネットワーク アドミッション コントロールを設定する前に、NA Control Server（ACS）を設定しておく必要があります。 NAC オーセンティケータとして、ASA は次のことを行います。 • IPsec セッションの確立に基づく資格情報の初期交換と、それ以降の 開始します。 • ピアと ACS の間で資格情報の要求と応答をリレーします。 • ACS サーバからの結果に基づいて、IPsec セッションに対してネット ポリシーを適用します。 • ピア オペレーティング システムに基づいて（および必要に応じて AC ローカル例外リストをサポートします。 •（省略可能）クライアントレス ホストの ACS サーバからアクセス します。 ACS クライアントとして、ASA は次のものをサポートします。 • EAP/RADIUS • NAC に必要な RADIUS 属性 ASA 上の NAC は、Cisco IOS レイヤ 3 デバイス（ルータなど）上の NAC す。後者ではルータがルーティングされたトラフィックに基づいて PV を す。NAC で有効にされた ASA は、PV のトリガーとして IPsec VPN セッ ます。NAC で設定された Cisco IOS ルータは、インターセプト ACL を使 ネットワークを宛先としているトラフィックに基づいて PV をトリガーし イスは VPN セッションを開始せずに ASA の背後にあるネットワークに いので、ASA に PV トリガーとしてのインターセプト ACL は必要ありま ピアからのすべての IPsec トラフィックは、ピアのグループに対して設定 トの ACL に従います。 Cisco VPN 3000 Concentrator Series とは異なり、ASA 上の NAC は、ステ ルオーバー、トンネル グループのすべての NAC セッションの初期化、 プ内のすべての NAC セッションの再検証、および各トンネル用に設定さ 証免除リストをサポートします。ASA 上の NAC は、非 VPN トラフィック リティ コンテキスト、および WebVPN をサポートしません。 デフォルトでは、NAC はディセーブルになっています。これはグループ スで有効にすることができます。

機能	説明
L2TP Over IPsec	Layer 2 Tunneling Protocol（L2TP; レイヤ 2 トンネリング プロトコル）は、リイアントがパブリック IP ネットワークを使用して、企業のプライベート ネサーバと安全に通信できるようにする VPN トンネリング プロトコルです。L2タのトンネリングに PPP over UDP（ポート 1701）を使用します。L2TP は、ト/サーバモデルを基本にしています。機能は L2TP ネットワーク サーバ（Lアクセス コンセントレータ（LAC）に分かれています。LNS は、通常、ルーネットワーク ゲートウェイで実行されます。一方、LAC は、ダイヤルアップワーク アクセス サーバ（NAS）や、Microsoft Windows 2000 などの L2TP クラ搭載された PC で実行されます。 L2TP/IPsec は、単一のプラットフォームで IPsec VPN サービスとファイアウビスとともに L2TP VPN ソリューションを展開および管理する機能を提供し リモート アクセスのシナリオで、IPsec を使用する L2TP を設定する最大の利モート ユーザーがゲートウェイや専用回線を使わずにパブリック IP ネットワて VPN にアクセスできることです。これにより、実質的にどの場所からでも用してリモート アクセスが可能になります。この他に、VPN にアクセスするトは Windows 2000 で Microsoft ダイヤルアップ ネットワーク（DUN）を使用よいという利点もあります。Cisco VPN Client ソフトウェアなど、追加のクラフトウェアは必要ありません。
OCSP サポート	Online Certificate Status Protocol（OCSP）は、X.509 デジタル証明書の失効状態ために、CRL への代替を提供します。クライアントに、大規模なことが多い書失効リストのダウンロードを要求するのではなく、OCSP が、特定の証明書会する検証機関に基づいて証明書の状態をローカライズします。
NAT の背後の複数の L2TP Over IPsec クライアント	セキュリティ アプライアンスは、1 つ以上の NAT デバイスの背後にある複数ントにリモート アクセス L2TP-over-IPsec 接続を正常に確立できます。これはover IPsec クライアントがセントラル オフィスと安全に通信する必要がある SOHO/ブランチ オフィス環境での L2TP over IPsec 接続の信頼性を高めます。
Nokia モバイル認証サポート	リモート アクセス用に、ハンドヘルド Nokia 92xx Communicator シリーズ携帯スを使用して VPN を確立できます。これらのデバイスが使用する認証プロトChallenge/Response for Authenticated Cryptographic Keys（CRACK）プロトコル
Zonelabs Integrity Server	Zone Labs Integrity System を展開するネットワーク内の ASA は、リモート Vントに対してセキュリティ ポリシーを適用するように設定できます。この場は、ゾーン ラボ整合性サーバとリモート クライアントとの間のエッジ ゲーす。Zone Labs Integrity サーバとリモート クライアント上の Zone Labs Personより、クライアントがプライベート ネットワーク リソースにアクセスする前トクライアントは一元管理されたセキュリティ ポリシーに確実に準拠しますクライアントとの間でセキュリティ ポリシー情報を渡すように ASA を設定しアント接続を維持するかまたは閉じて、サーバ接続障害を回避します。さらンで、整合性サーバと ASA の両方の SSL 証明書認証を要求するようにしま

機能	説明
ハイブリッド XAUTH	ASA とリモート ユーザーの間の IKE セキュリティを強化するハイブリッ きます。この機能を使用する場合、IKE フェーズ I には 2 つの手順が必要 まず、標準公開キー技法を使用してリモート VPN ユーザーに認証し、一 IKE セキュリティ アソシエーションを確立します。次に、XAUTH 交換が ユーザーを認証します。この拡張認証では、サポートされているいずれか 使用できます。ハイブリッド XAUTH は、ASA 認証にデジタル証明書を ト VPN ユーザー認証に RADIUS、TACACS+、SecurID などのさまざまな ことができます。
IPsec フラグメント化およびリアセンブリ統計	IPsec 関連のフラグメンテーションとリアセンブルの問題のデバッグに役 IPsec フラグメンテーションとリアセンブル統計をモニタできます。新し 処理の前後でのフラグメンテーションと再アセンブリに関する情報を提供
WebVPN 用のインスペクション IPS、CSC、URL のフィルタリング	この機能は、クライアントレス モードとポート転送モードで、WebVPN インスペクション、IPS、およびトレンドマイクロのサポートを追加しま のサポートは以前から存在しています。すべてのモードで、トレンドマ ンジンはトリガーされます（設定されている 場合）。 WebSense と N2H2 のサポートを使用した URL/FTP/HTTPS/Java/Activex フ 追加されました。DNS 検査は DNS 要求に対してトリガーされます。 ポート転送モードで、WebSense と N2H2 サポートを使用したフィルタリ を備えた HTTP、SMTP、FTP、および DNS インスペクションが追加され
ルーティング機能	
アクティブ RIP サポート	ASA は、RIP バージョン 1 および 2 をサポートしています。ASA でイネ とができる RIP ルーティング プロセスは 1 つだけです。RIP ルーティン 効にすると、RIP はすべてのインターフェイス上で有効になります。デフ キュリティ アプライアンスは RIP バージョン 1 アップデートを送信し、 1 およびバージョン 2 アップデートを受け取ります。 インターフェイスで受け入れる RIP のバージョンを指定するには、イン ンフィギュレーション モードで **rip receive version** コマンドを使用します
スタンバイ ISP サポート	この機能によって、プライマリ ISP へのリンクに失敗した場合にリンク を設定できます。プライマリ ルートの可用性の判断と、プライマリ ルー きにセカンダリ ルートを有効にするのにスタティック ルーティングとオ ラッキングを使用します。
PPPoE Client	Point-to-Point Protocol over Ethernet（PPPoE）は、イーサネットと PPP と れられている 2 つの標準を結合して、IP アドレスをクライアント システ 認証方式を提供します。一般的な PPPoE クライアントは、DSL やケーブル のリモート ブロードバンド接続によって ISP に接続されているパーソナル です。ISP は、既存のリモート アクセス インフラストラクチャを使用し バンド アクセスをサポートするためと、顧客の使い勝手向上のために、 ます。

機能	説明
動的 DNS サポート	動的 DNS（DDNS）更新メソッドを作成して、必要な頻度で DNS サーバ上の コード（RR）を更新するように設定できます。 DDNS は DHCP を補完し、ユーザーが動的かつ透過的に再利用可能な IP アド イアントに割り当てることができるようにします。DDNS は、DNS サーバ上 らアドレスへのマッピングと、アドレスから名前へのマッピングを動的に更 します。このバージョンを使用すると、ASA は、DNS レコード更新の IETF 標 トします。
スタティック ルート トラッキング	スタティック ルート トラッキング機能には、スタティック ルートの使用可能 し、プライマリ ルートがダウンした場合のバックアップ ルートをインストー の方式が用意されています。 **clear configure sla、frequency, num-packets、request-data-size、show sla mon** **running-config sla、sla monitor、sla monitor schedule, threshold、timeout、to** の各コマンドが導入されました。 次の画面が導入または変更されました。 **[Configuration] > [Device Setup] > [Routing] > [Static Routes] > [Add Static Ro** **[Configuration] > [Device Setup] > [Routing] > [Static Routes] > [Add Static Ro** **Monitoring Options]**
マルチキャスト ルーティング拡張	マルチキャスト ルーティングの拡張機能では、マルチキャスト境界を定義で れにより同じ IP アドレスを持つ RP があるドメインは、PIM プロセスをより するために PIM ネイバーをフィルタしたり、混合の双方向およびスパースモ トワークをサポートするために PIM bidir ネイバーをフィルタしたりして、相 しないようにします。
拡張 DNS ドメイン名の使用	AAA サーバを設定するとき、また **ping**、**traceroute**、および **copy** コマンドを きにも、www.example.com のような DNS ドメイン名を使用できます。
非暗号化トラフィックのインターフェイス内通信	VPN トラフィックだけでなくすべてのトラフィックが、同じインターフェイ 同じインターフェイスから出ることが許可されるようになりました。
IPv6 アドレスの IPv6 セキュリティ拡張機能	この機能では、直接接続ホストの IPv6 アドレスに対してアドレスのインター 別子部分に Modified EUI-64 形式を使用することを要求するように、セキュリ イアンスを設定できます。
マルチ コンテキスト モード機能	
プライベートと自動 MAC アドレスの割り当ておよび複数コンテキストモードの生成	各インターフェイスに、プライベート MAC アドレス（フェールオーバー用の とスタンバイの両方）を割り当てることができます。複数のコンテキスト モ て、共有コンテキスト インターフェイスの固有の MAC アドレスを自動的に す。これによりコンテキストへのパケットの分類はより信頼性が高くなりま 新しい **mac-address auto** コマンドでは、各共有コンテキスト インターフェイ ベート MAC アドレスを自動的に割り当てることができます。

機能	説明
セキュリティ コンテキストのリソース管理	特定のコンテキストが使用しているリソースが多すぎることが原因で、他のトが接続を拒否されるといった現象が発生した場合は、コンテキストあたの使用量を制限するようにリソース管理を設定できます。
システムからのすべてのコンテキスト構成の保存	**write memory all** コマンドを使用して、システム実行スペースからすべて設定を一度に保存できるようになりました。
ハイ アベイラビリティ機能	
1 秒未満のフェールオーバー	この機能では、1 秒未満の障害を検出して応答するようにフェールオーバす。
構成可能なプロンプト	この機能により、ユーザーは、**show failover** コマンドを入力しなくても、アプライアンスのフェールオーバー ステータスを表示して出力を解析で能によりユーザーは、フェールオーバー ユニットのシャーシ スロット番す。以前は、プロンプトによって、ホスト名、セキュリティ コンテキスモードのみが反映されていました。プロンプト コマンドは、この機能のします。
ファイアウォール機能	
汎用入力レート制限	この機能は、ASA 上、またはファイアウォールの特定のインスペクショのサービス拒否（DoS）攻撃を防止します。7.0 リリースは、出口レートグ）機能をサポートし、このリリースでは、入力レート制限機能は現在のグ機能を拡張します。 **police** コマンドはこの機能のために拡張されています。
通過トラフィックと管理アクセスの認証は VPN クライアントで以前サポートされていたすべてのサーバをサポートする	ファイアウォール認証にはすべてのサーバ タイプを使用できます。ただります。HTTP フォーム プロトコルは、WebVPN ユーザーに対してのみオン認証をサポートし、SDI は HTTP 管理アクセスではサポートされませ
デッド接続検出（DCD）	この機能により、適応型セキュリティ アプライアンスはデッド接続を自期限切れにします。以前のバージョンでは、デッド接続はタイムアウトのタイムアウトが付与されていました。多数のデッド接続がセキュリティスを圧倒していないことを確認するために、手動の介入が必要でした。こまだトラフィックを処理できる接続には干渉することなく、デッド接続的に期限切れにします。set connection timeout および show service-policy サポートを提供します。
WCCP	Web Cache Communication Protocol（WCCP）機能により、WCCP サービスダイレクト Web キャッシュ トラフィックを指定できます。この機能は、のトラフィックを Web キャッシュ エンジンのグループに透過的にリダイソースの使用状況を最適化し、応答時間を短縮します。

機能	説明
フィルタリング機能	
セキュアコンピューティング（N2H2）のための URL フィルタリング拡張機能	この機能により、長い URL、HTTPS、FTP フィルタリングを、Websense（現ダー）および N2H2（Secure Computing によって購入されたベンダー）の両方有効にできます。以前このコードは、このタイプのフィルタリングを提供すWebsense ベンダーのみを有効にしていました。url-block、url-server、および ドが、この機能をサポートします。
管理機能とトラブルシューティング機能	
自動更新	セキュリティアプライアンスは、Auto Update クライアントとして設定されて加え、Auto Update サーバとして設定されるようになりました。既存の client ンド（VPN クライアントの更新にも使用される）は、新しい Auto Update ササポートするように拡張され、クライアントとして設定されているセキュリイアンスを更新するためにセキュリティ アプライアンスが必要とする新しい と引数が含まれます。Auto Update クライアントとして設定されているセキュライアンスでは、引き続き auto-update コマンドを使用して、セキュリティスが Auto Update サーバとの通信に必要なパラメータを設定します。
管理トラフィック用のモジュラ ポリシー フレームワークのサポート	to-the-security-appliance トラフィック用にレイヤ 3/4 クラス マップを定義でりました。これにより管理トラフィックに対して特別なアクションを実行でのバージョンでは、RADIUS アカウンティング トラフィックを検査できます
traceroute	**traceroute** コマンドでは、パケットのルートをその宛先までトレースできま
Packet Tracer	パケット トレーサ ツールにより、動作が期待どおりであるかを確認するため由でパケットの寿命を追跡できます。 **packet-tracer** コマンドは、パケットに関する詳細情報、およびセキュリティンスによるパケットの処理方法を提供します。コンフィギュレーションから が原因でパケットがドロップしたのではない場合、**packet-tracer** コマンドに に関する情報が表示されます。 ASDM の新しい特許出願中のパケット トレーサ ツールにより、アニメーショパケット フロー モデルで、動作が期待どおりであるかどうかを確認するため由でパケットの寿命を簡単に追跡できます。さらに、ネットワーク設計がどであってもトラブルシューティングを簡素化できます。このツールは、送信 IP アドレスなどのパケットの属性に、パケットのさまざまなフェーズおよび視覚的表現を備えます。これにはシングル クリックでアクセスできます。各ついて、パケットがドロップされているかまたは許可されているかを表示し
ASDM 機能	

機能	説明
強化された ASDM ルール テーブル	ASDMルールテーブルは、ポリシーの作成を合理化するように再設計され とより密接にマップする簡素化されたルール作成に加えて、このルールテ パーネッティングや、インターフェイス以外にも関連付けられているオブ プの使用などの、ほとんどの設定シナリオをサポートします。ASDM の ループの使用は、ルールの作成を単純化するために削除されました。以下 ようになりました。 • 1 つのパネルからオブジェクト、オブジェクト グループ、およびルー す。 • インターフェイス、送信元、送信先またはサービスをフィルタしま • 複数の条件を使用して、高度なフィルタリングのルール テーブルで リを実行します。 • リアルタイム ログ ビューアで特定のアクセス ルールのログを表示し • ルールとパケット トレースをシングル クリックで選択します。これ ケット属性が取り込まれます。 • アクセス リストのエントリを簡単に整理し、テーブル内を上下に移 順序を変更できます。 • オブジェクト グループ内の要素を展開して表示します。 • ツールチップを使用してオブジェクトの属性またはグループのメン す。
High Availability and Scalability Wizard	High Availability and Scalability Wizard は、アクティブ/アクティブ、アクテ イ フェールオーバーと VPN ロード バランシングの設定を簡素化するため す。ウィザードもピア デバイスをインテリジェントに設定します。
Syslog の拡張機能	syslog の拡張機能には、次のものが含まれています。 • 送信元 IP、宛先 IP、syslog ID、日付と時刻をさまざまな列に表示す 解析 • 各 syslog の説明と推奨アクションをシングル クリックで表示できる • 重大度レベルに基づく Syslog の色付け • ログ ビューアでのツール ヒントとしての syslog の簡単な説明
NAT ルール	NAT ルールの作成が簡素化されました。
オブジェクト グループ サポート	ネットワーク、サービス、プロトコル、ICMP タイプのオブジェクト グル は完全にサポートするようになりました。
名前付き IP アドレス	IP アドレスに関連する名前を作成する機能が存在するようになりました。

機能	説明
ASDM アシスタント	新しい ASDM アシスタントは、AAA サーバ、ロギング フィルタ、SSL VPN ト、および他の機能を設定するための、タスク志向ガイダンスを提供してい いガイドをアップロードすることもできます。
コンテキスト管理	コンテキスト管理が向上しました。これにはコンテキスト キャッシュや拡張 含まれます。
インスペクション マップ	定義済みの低、中、高のセキュリティ設定により、検査マップの作成と管理 れます。

バージョン 7.1 の新機能

ASA 7.1(2)/ASDM 5.1(2) の新機能

リリース：**2006年3月15日**

ASA 7.1(2)/ASDM 5.1(2) には新機能はありませんでした。

ASA 7.1(1)/ASDM 5.1(1) の新機能

リリース：**2006年2月6日**

機能	説明
プラットフォーム機能	

機能	説明
Content Security and Control（CSC）SSM のサポート	

機能	説明
	シスコの Anti-X ソリューションの不可欠な部分である CSC SSM は、業界最 保護とコンテンツ コントロールをインターネット エッジで提供します。これ 合的なウイルス対策、スパイウェア対策、ファイル ブロック、スパム対策、 グ対策、URL ブロッキングとフィルタリング、およびコンテンツ フィルタリ スが提供されます。CSC SSM サービス モジュールは、次の主要な要素によ り効果的にそのネットワークを保護したり、ネットワークの可用性を向上さ 業員の生産性を向上させたりするのに役立ちます。 • ウイルス対策：トレンドマイクロが提供する市場で主導的なウイルス対 インフラストラクチャにおいて最も有効なポイントであるインターネッ イで、既知および未知のウイルス攻撃から内部ネットワーク リソースを保 境界で電子メールおよび Web トラフィックをクリーンアップすることに ソース集約的なマルウェア感染クリーンアップを不要にして、ビジネス 保します。 • スパイウェア対策：Web トラフィック（HTTP および FTP）や電子メール クによりネットワークにスパイウェアが侵入することをブロックします 高くつくスパイウェア除去プロシージャから IT サポート人員を解放し、 イでスパイウェアをブロックすることにより従業員の生産性を向上させ • スパム対策：非常に低い偽陽性によるスパムの効果的なブロックにより ル通信の有効性が復元され、顧客、ベンダー、およびパートナーとの連 れずに継続します。 • フィッシング対策：ID 盗難保護によりフィッシング攻撃から保護され、 注意により会社または個人情報を開示して金銭的な損失につながるよう 避します。 • TrendLabs による自動更新：ソリューションはウイルス、スパイウェア、 ムの業界で最も大きい、24 時間対応の専門家チームの 1 つにより支援お トされており、ソリューションが最新の保護を提供していることは自動 れます。 • 一元管理：リモートからアクセスできる Web コンソールによる、簡単で 管理と自動更新により、IT サポート コストを削減します。 • Web アクセス、メール（SMTP と POP3）のリアルタイム保護および FT 転送）：企業のメールがすでに保護されている場合でも、多くの従業員 やラップトップからプライベートな Web メールにアクセスし、それがイ トがもたらす脅威の別のエントリ ポイントとなります。同様に、従業員 染された可能性があるファイルのプログラムを直接ダウンロードできま ネット ゲートウェイでのすべての Web トラフィックのリアルタイム保護 の多くの場合に見逃される脆弱性のポイントを大幅に削減できます。 • カテゴリ、スケジューリング、キャッシュを使用する完全な URL フィル 能：URL フィルタリングを使用して、不適切または仕事に無関係な Web アクセスをブロックすることにより、従業員によるインターネット利用

機能	説明
	ます。これにより従業員の生産性は向上し、攻撃的な Web コンテン ことで従業員が法的手段を講じるリスクを制限できます。 • 電子メール コンテンツ フィルタリング：電子メール フィルタリング メールで転送される攻撃的内容に対する法的責任を最小限に抑え、規 アンスを適用し、組織が GLB 法やデータ保護法など法的要件を満た す。
VPN の一般的機能	
Cisco Secure Desktop	Cisco Secure Desktop（CSD）はオプションの Windows ソフトウェア パッ ASA にインストールして、SSL VPN へのアクセスを要求してクライアン のセキュリティを検証し、接続時には安全であることを確認し、切断後に すべてのトレースを削除します。 Microsoft Windows を実行しているリモート PC が ASA に接続した後に、C ストールされ、IP アドレスと特定のファイルの存在、レジストリ キー、 使用して PC の接続元の場所のタイプを特定します。ユーザー認証に続い クセス権を付与するための条件としてオプションの基準を使用します。こ は、PC 上で実行するオペレーティング システム、ウイルス対策ソフトウ ウェア対策ソフトウェア、パーソナル ファイアウォールなどがあります。 PC がネットワークに接続しているときにセキュリティを確保するには、M XP および Windows 2000 クライアント上で稼働する CSD アプリケーショ Desktop により、セッション中にユーザーが実行できる操作を制限します 持つリモート ユーザーの場合、Secure Desktop は 168 ビット Triple Data En （3DES）を使用して、関連があるかまたは SSL VPN セッション中にダウ たデータやファイルを暗号化します。特権が低いリモート ユーザーは、1 （RC4）暗号化アルゴリズムを使用します。セッションを閉じるときに、 はファイルの安全な削除についての米国国防総省（DoD）のセキュリティ て、リモート PC からのすべてのデータを上書きおよび削除します。この により、リモート ユーザーがログアウトするかまたは SSL VPN セッショ トした後に、cookie、ブラウザの履歴、一時ファイル、およびダウンロー ンツは完全に残らなくなります。CSD は、それ自体をクライアント PC か トールします。 Cache Cleaner は、セッションが終了するとクライアント キャッシュを消 Windows XP、Windows 2000、Windows 9x、Linux、および Apple Macintosh ントをサポートします。

機能	説明
CSD ホスト チェックに基づくカスタマイズされたアクセス コントロール	Cisco Secure Desktop がインストールされている適応型セキュリティ アプライ代替グループ ポリシーを指定できます。ASA では、この属性を使用して、次モート CSD クライアントへのアクセス権を制限します。 • VPN 機能ポリシーを「Use Failure Group-Policy」に設定している場合は、を使用します。 • VPN 機能ポリシーを「Use Success Group-Policy, if criteria match」に設定しは、基準が一致しなかったときに、この値を使用します。 この属性は、適用される代替グループ ポリシーの名前を指定します。グルーを選択して、アクセス権限を、デフォルト グループ ポリシーに関連付けらセス権限と区別します。デフォルト値は DfltGrpPolicy です。 （注） VPN 機能ポリシーを「Always use Success Group-Policy」に設定して ASA ではこの属性を使用しません。
SSL VPN Client	SSL VPN クライアントは、ネットワーク管理者がリモート コンピュータに I ライアントをインストールして設定しなくても、リモート ユーザーが IPSec アントの接続性の利点を活用できる VPN トンネリング テクノロジーです。モート コンピュータに既存の SSL 暗号化および ASA の WebVPN ログインお使用します。 SVC セッションを確立するには、リモート ユーザーがブラウザで ASA の W ターフェイスのIPアドレスを入力し、ブラウザはそのインターフェイスに接続ログイン画面を表示します。ユーザーがログインと認証を完了し、ユーザー要としていることを ASA が確認すると、ASA は SVC をリモート コンピュー ロードします。ASA が、SVC を使用するオプションがユーザーにあると確認 ASA は、SVC のインストールをスキップするリンクをユーザー画面に表示 に、SVC をリモート コンピュータにダウンロードします。 ダウンロードが完了すると、SVC はインストールと設定を実行します。接続と（設定に応じて）、SVC はリモート コンピュータに保持されるか、または ンピュータからアンインストールされます。

機能	説明
WebVPN 機能とパフォーマンスの最適化	このバージョンでは、WebVPN パフォーマンスと機能は次のコンポーネされます。 • 複雑な JavaScript、VBScript、および Java が含まれている柔軟なコン成。 • サーバ側とブラウザのキャッシュ • Compression • プロキシ バイパス • アプリケーション プロファイル カスタマイゼーション フレームワー • アプリケーション キープアライブおよびタイムアウトの処理 • 論理（VLAN）インターフェイスのサポート
WebVPN 用の Citrix サポート	WebVPN ユーザーは Citrix MetaFrame サービスにアクセスするために、A使用できるようになりました。この設定では、ASA は Citrix セキュア ゲて機能します。したがって、Citrix セキュア ゲートウェイを使用しないモように Citrix Web Interface ソフトウェアを設定する必要があります。リモが完全修飾ドメイン名（FQDN）を使用して接続する ASA インターフェ明書をインストールします。この機能は、SSL 証明書の共通名（CN）とを指定すると機能しません。リモート ユーザーは、ASA と通信するため を試行します。リモート PC は、DNS または System32\drivers\etc\hosts フトリを使用して、FQDN を解決できる必要があります。最後に、**function** 用して Citrix を有効にします。
WebVPN の PDA サポート	WebVPN は Pocket PC 2003 または Windows Mobile X からアクセスできまザーの場合、これによりプライベート ネットワークへのアクセスはさらす。この機能は設定が不要です。

機能	説明
CIFS ファイル用の文字エンコーディングの WebVPN サポート	WebVPN は、目的の言語での共通インターネット ファイル システム ファイ 表示を保証するために、ポータル ページのオプションの文字エンコーディン トするようになりました。文字エンコードは、日本語のシフト JIS 文字を含む ページで指定された文字セットをサポートします。 http://www.iana.org/assignments/character-sets WebVPN ポータル ページでリモート ユーザーに送信するためにエンコードす トを指定するには、**character-encoding** コマンドを使用します。デフォルトで ト ブラウザに設定されたエンコード タイプが、WebVPN ポータル ページの を決定します。 character-encoding 属性は、デフォルトでは、すべての WebVPN ポータル ペー れるグローバルな設定です。ただし、特定の CIFS サーバから WebVPN ポー のエンコードを指定するには、**file-encoding** コマンドを使用できます。この方 外の文字の符合化が必要な各 CIFS サーバに対し、異なるファイル符号化値を す。 CIFS サーバに適切な文字エンコーディングを、広域的には webvpn character- 性によって、個別的には file-encoding の上書きによってマッピングすること 同様にファイル名やディレクトリ パスを適切にレンダリングすることが必要が CIFS ページの正確な処理と表示が可能になります。 ヒント character-encoding の値および file-encoding の値は、ブラウザによ れるフォント ファミリを排除するものではありません。日本語の 字エンコーディングを使用する場合などは、webvpn カスタマイ コマンド モードで **page style** コマンドを使用してフォント ファミ し、これらの値の 1 つの設定を補足するか、または webvpn カス ション コマンド モードで **no page style** コマンドを入力してフォ リを削除する必要があります。
WebVPN と SSL VPN クライアント接続の圧縮	圧縮により、転送するパケットのサイズは縮小され、特にリモート アクセス るダイヤルアップ モデムやハンドヘルド デバイスなどとの帯域幅に制限があ 合に、通信のパフォーマンスは向上します。 圧縮は、WebVPN と SVC 接続に対してデフォルトでは有効です。ASDM また ンドを使用して圧縮を設定できます。 すべての WebVPN または SVC 接続の圧縮は、グローバル設定モードから **co** マンドで無効にできます。 グループ ポリシーまたはユーザー名 webvpn モードで、WebVPN 接続の場合 コマンドを、SVC 接続の場合は **svc compression** コマンドを使用して、特定の たはユーザーの圧縮を無効にできます。

機能	説明
WebVPN および SVC 接続のアクティブ/スタンバイ ステートフル フェールオーバー	フェールオーバー時には、サービスの継続のため、セカンダリのスタンバアプライアンスとの WebVPN 接続、SVC 接続、IPSec 接続が再確立されブ/スタンバイ フェールオーバーには、各接続に 1 対 1 のアクティブ/スタ必要です。 フェールオーバーに設定されたセキュリティ アプライアンスは、WebVPする認証情報を、スタンバイ セキュリティ アプライアンスと共有しますフェールオーバー後に、WebVPN ユーザーは再認証の必要はありません。 SVC 接続の場合、フェールオーバー後に、SVC は自動的にスタンバイ セライアンスと再接続します。
WebVPN カスタマイゼーション	ユーザーがセキュリティ アプライアンスに接続するときに表示される Wカスタマイズしたり、WebVPN ホーム ページをユーザーごと、グループンネルごとのグループ ベースでカスタマイズしたりできます。ユーザーは、セキュリティ アプライアンスが認証した後に WebVPN のカスタム ホ参照します。 カスケード スタイル シート（CSS）パラメータを使用できます。簡単にするには、ASDM を使用することを推奨します。ASDM には、色見本やプど、スタイルの要素を設定するための便利な機能があります。
自動アプレット ダウンロード	WebVPN を介したリモート アプリケーションを実行するには、ユーザームページの [Start Application Access] をクリックしてポート転送 Java アプロードして開始します。アプリケーション アクセスを簡単にして開始時めに、ユーザーが WebVPN に初めてログインしたときに、自動的にこのレットをダウンロードするように WebVPN を設定できるようになりまし
認証と承認の VPN 機能	
無効にされたアカウントのオーバーライド	AAA サーバからのアカウント無効指示をオーバーライドして、ログオン何らかの方法で許可するように ASA を設定できます。 次のコマンドが導入されました。**override account disabled**
LDAP サポート	セキュリティ アプライアンスを設定して、IPSec VPN ユーザー、SSL VPN WebVPN ユーザーを、LDAP ディレクトリ サーバに対して認証および認きます。認証中、セキュリティ アプライアンスは、VPN ユーザの LDAP イアント プロキシとして機能し、プレーン テキストまたは Simple Authe Security Layer（SASL）プロトコルのいずれかを使って LDAP サーバに対ます。セキュリティ アプライアンスでは、LDAP V3 または V2 準拠のすトリ サーバをサポートします。これはパスワード管理を、Sun Microsyste Directory Server および Microsoft Active Directory サーバ上だけでサポート

機能	説明
パスワード管理	パスワードの期限切れが近づいたときにエンドユーザーに警告するようにA きます。この機能を設定すると、リモート ユーザーがログインするときに、 ユーザーの現在のパスワードの有効期限が近づいていること、または期限が ことを通知します。それから ASA は、ユーザーがパスワードを変更できる。 す。現行のパスワードが失効していない場合、ユーザーはそのパスワードを グインし続けることができます。このコマンドは、このような通知機能をサ RADIUS、RADIUS 対応 NT サーバ、LDAP サーバなどの AAA サーバで有効で または LDAP 認証が設定されていない場合、ASA ではこのコマンドが無視さ このコマンドは、パスワードが失効するまでの日数を変更するものではなく、 ザーに対してパスワード失効の警告を開始してから失効するまでの日数を指 である点に注意してください。デフォルト値は 14 日間です。 LDAP サーバの認証の場合のみ、保留期限についてユーザーに警告を開始す 特定の期限日数を指定できます。 次のコマンドが導入されました。**password management**
シングル サインオン（SSO）	シングル サインオン（SSO）のサポートによって、WebVPN ユーザーはユー スワードを 1 回だけ入力して、複数の保護されているサービスおよび Web サ セスできます。SSO の設定時に次の方法から選択できます。 • Computer Associates eTrust SiteMinder SSO サーバ（以前は Netegrity SiteM 使用の Web サイト セキュリティ インフラストラクチャにすでに SiteMi 込まれている場合には、通常、SiteMinder を使用して SSO を実装するこ ます。 • HTTP Form：SSO 認証を実行するための一般的で標準的な手段であり、 しても使用できます。RADIUS サーバや LDAP サーバなどの他の AAA サ に使用することができます。 • 基本 HTTP 認証と NTLM 認証を使用する SSO：最も単純な 3 つの SSO メ 基本 HTTP または NTLM 認証を使用して、認証用の WebVPN ログイン資 部サーバにパススルーします。このメソッドでは、外部 SSO サーバは必 ん。
トンネル グループおよびグループ ポリシー VPN の機能	
WebVPN トンネル グループのタイプ	このバージョンは、WebVPN トンネル グループを追加します。これにより W の属性を持つトンネル グループを設定できます。この属性には使用する認証 ユーザー GUI に適用する WebVPN カスタマイズ、使用する DNS グループ、 プ名（エイリアス）、グループ URL、CIFS の名前解決に使用する NBNS サー リモート CSD クライアントへのアクセス権を制限するために CSD ユーザに 替グループ ポリシーなどが含まれます。

機能	説明
WebVPN のグループ ベースの DNS 設定	グループ下にある DNS サーバのリストを定義できます。ユーザーに利用 バのリストは、ユーザーが割り当てられているグループに応じて異なり トンネル グループに使用する DNS サーバを指定できます。デフォルト値 です。
WebVPN ユーザーの新しいログイン ページ オプション	ユーザーがログインに使用するトンネル グループを選択できるユーザー を表示するように、WebVPN を設定することもできます。このオプション ログイン ページには、グループを選択するためのドロップ ダウン メニュ 加のフィールドが表示されます。ユーザーは、選択したグループに対して
グループ別名およびグループ URL	1 つ以上の代替名を作成して、1 つ以上のグループ エイリアスを指定する ネル グループを参照できます。ここで指定するグループ エイリアスは、 イン ページにあるドロップダウン リストに表示されます。各グループに スを指定することも、エイリアスを指定しないことも可能です。トンネ 際の名前をこのリストに表示する場合は、その名前をエイリアスとして指 の機能は、同じグループが「Devtest」や「QA」などの複数の通常名で指 合に便利です。 グループの URL を指定すると、ユーザーがログイン時にグループを選択 なります。ユーザーがログインすると、ASA は、tunnel-group-policy テー ザーの着信 URL またはアドレスを検索します。URL が見つかり、さらに になっている場合、ASA は適切なサーバを自動的に選択して、ユーザー名 ドフィールドだけをログイン ウィンドウでユーザに表示します。URL が ループのドロップダウン リストも表示され、ユーザーは選択を行う必要 1 つのグループに対して複数の URL を設定できます。または、URL を設 できます。各 URL は個別に有効または無効にできます。各 URL に別の コマンド）を使用する必要があります。URL 全体を指定する必要があり または HTTPS プロトコルのいずれかを使用できます。 複数のグループに同じ URL を関連付けることはできません。ASA では、 を検証してから、トンネル グループに対する URL を受け入れます。
ASDM 機能	

機能	説明
CSC SSM の管理およびモニタ サポート	ASDM バージョン 5.1 は、トレンドマイクロの HTML ベース設定パネルのシン ASDM の創意工夫とを併せ持つ業界初のソリューションです。これにより、 リシーが確実に適用され、完全なプロビジョニング、設定、CSC SSM によ る豊富な統合脅威管理機能のためのプロセス モニタが簡素化されます。新し ホームページと新しいモニタリング パネルによる、補完的なモニタリング ン ンを提供します。CSC SSM をインストールすると、メインの ASDM ホーム 的に更新され、新しい CSC SSM パネルが表示されます。これは、脅威、電 イルス、ライブ イベント、および重要なモジュール統計（最後にインスト フトウェア/署名の更新、システム リソースなど）の履歴ビューを提供しま モニタリング セクション内では、豊富な分析ツールにより、脅威、ソフトウ リソース グラフなどを詳細に確認できます。Live Security Event Monitor は、 ブルシューティングおよびモニタリング ツールであり、スキャンやブロック メール メッセージ、識別されたウイルス/ワーム、検出された攻撃などをリア 更新します。管理者には、正規表現文字列の一致を使用してメッセージをフ オプションが付与されます。これにより、特定の攻撃のタイプとメッセージ で詳細に分析できます。
Syslog to Access Rule Correlation	この ASDM リリースは、日常的なセキュリティ管理とトラブルシューティン ビティを大幅に強化する、新しい Syslog to Access Rule Correlation を導入して の動的ツールを使用して、セキュリティ管理者は一般的な設定の問題と、ほ ザーおよびネットワーク接続の問題を迅速に解決できます。ユーザーは [Rea Viewer] パネル内の syslog メッセージを選択でき、パネルの上部の [Create] ボ リックするだけで、その特定の syslog のアクセス制御オプションを呼び出す ます。インテリジェントなデフォルト値により、設定プロセスは簡単に済み によりビジネスクリティカルな機能の運用効率と応答時間が改善されます。 Access Rule Correlation ツールは、ユーザー設定のアクセス ルールによって呼 syslog メッセージへの直感的なビューも提供しています。
カスタマイズされた Syslog のカラーリング	ASDM は、syslog レベルに応じて syslog メッセージを色別にグループ化でき ることで、迅速なクリティカル システム メッセージの識別と簡便な syslog モ を実現できます。ユーザーは、デフォルトの色付けオプションを選択するこ しやすいように固有に色付けされた syslog プロファイルを作成することもて
ASDM および WebVPN インターフェイス	ASDM と WebVPN は、同時に同じインターフェイス上で実行できるようにな
ASDM デモ モード	ASDM デモ モード初期サポート。

バージョン 7.0 の新機能

ASA 7.0(8)/ASDM 5.0(8) と ASDM 5.0(9) の新機能

リリース：**2008年6月2日**

（注） ASDM 5.0(9) には新しい機能は含まれていません。警告の修正のみが含まれています。

機能	説明
ファイアウォール機能	
Ethertype ACL MAC の機能強化	EtherType ACL は、非標準 MAC を許可するように強化されています。既のルールが保持され、新しいルールを追加する必要はありません。 バージョン *7.2(4)* および *8.0(4)* でも使用可能です。
リモート アクセス機能	
ローカルアドレス プールの編集	アドレス プールは、目的の接続に影響を与えることなく編集できます。中でありプールから排除されていない場合、接続は影響を受けません。のアドレスがプールから除去されている場合、接続はダウンします。 バージョン *7.2(4)* および *8.0(4)* でも使用可能です。
接続機能	
clear conn コマンド	**clear conn** コマンドは、接続を削除するために追加されました。 バージョン *7.2(4)* および *8.0(4)* でも使用可能です。
フラグメントの完全リアセンブル	**fragment** コマンドは **reassembly full** キーワードで拡張され、デバイス経由グされるフラグメントの完全リアセンブルが可能になりました。デバイラグメントは、常に完全にリアセンブルされます。 バージョン *7.2(4)* および *8.0(4)* でも使用可能です。
トラブルシューティングとモニタリングの機能	
capture コマンドの強化	**capture type asp-drop** *drop_code* コマンドは、**all** を *drop_code* として受け入たので、セキュリティ チェックが原因でドロップされたものを含め、AS るすべてのパケットをキャプチャできるようになりました。 バージョン *7.2(4)* および *8.0(4)* でも使用可能です。

機能	説明
show asp drop コマンドの強化	カウンタが最後にクリアされた時間を示すタイムスタンプが出力に含まれる ました（**clear asp drop** コマンドを参照）。また、説明の横にドロップ理由の が表示されるため、そのキーワードを使用して簡単に **capture asp-drop** コマ できます。 バージョン *7.2(4)* および *8.0(4)* でも使用可能です。
clear asp table コマンド	**clear asp table** コマンドが、**show asp table** コマンドによるヒット出力をクリ に追加されました。 バージョン *7.2(4)* および *8.0(4)* でも使用可能です。
show asp table classify hits コマンドの強化	hits オプションが **show asp table classify** コマンドに追加され、asp テーブル カ リアされた最終時刻を示すタイムスタンプが表示されるようになりました。 くない hits 値があるルールも表示されます。これによりユーザーはどのルー したかをすばやく参照できます。特に単純な設定であると **show asp table cla** ドで最終的に何百ものエントリが存在するようになるため便利です。 バージョン *7.2(4)* および *8.0(4)* でも使用可能です。
show perfmon コマンド	次の速度出力が追加されました。[TCP Intercept Connections Established]、[TC Attempts]、[TCP Embryonic Connections Timeout]、および [Valid Connections R Intercept] バージョン *7.2(4)* および *8.0(4)* でも使用可能です。

機能	説明
memory tracking コマンド	次の新しいコマンドが、このリリースで導入されました。 • **memory tracking enable**：このコマンドにより、ヒープ メモリ要求の 有効になります。 • **no memory tracking enable**：このコマンドは、ヒープ メモリ要求の追 現在収集したすべての情報をクリーンアップし、ツール自体によっ べてのヒープ メモリをシステムに返します。 • **clear memory tracking**：このコマンドは現在収集したすべての情報を それ以降もメモリ要求の追跡は継続します。 • **show memory tracking**：このコマンドは、ツールの追跡対象である現 ているメモリを、最上位呼び出し元関数アドレス別に示します。 • **show memory tracking address**：このコマンドは、メモリの各部分に り当てられているメモリを示しています。この出力は、ツールの追 在割り当てられている各メモリのサイズ、位置、および最上位呼び出 覧表示します。 • **show memory tracking dump**：このコマンドは、指定されたメモリ ア ズ、位置、呼び出しスタックの一部、およびメモリ ダンプを表示し • **show memory tracking detail**：このコマンドは、ツールの内部動作へ めに使用されるさまざまな内部の詳細を示しています。 バージョン *7.2(4)* および *8.0(4)* でも使用可能です。
フェールオーバー機能	
failover timeout コマンド	**failover timeout** コマンドに、静的固定機能とともに使用されるフェールオ ンスが不要になりました。 バージョン *7.2(4)* および *8.0(4)* でも使用可能です。
ユーザービリティ機能	
show access-list の出力	拡張アクセス リストの出力は、読みやすいようにインデントされていま バージョン *7.2(4)* および *8.0(4)* でも使用可能です。

機能	説明
show arp の出力	透過的なファイアウォール モードでは、ARP エントリが静的に設定されたか されたかを把握しておくことが必要な場合があります。ARP インスペクショ ナミック ARP エントリがすでに学習されている場合には、正当なホストから 答をドロップします。ARP インスペクションは静的 ARP エントリでのみ動 show arp コマンドは、各エントリでそれが動的であれば経過時間を示すよう た。ただし静的である場合には示しません。 [Monitoring] > [Interfaces] > [ARP Table] を参照してください。 バージョン *7.2(4)* および *8.0(4)* でも使用可能です。
show conn コマンド	「ローカル」と「外部」ではなく、送信元と宛先の概念を使用するように、 化されました。新しい構文では、送信元アドレスが入力された最初のアドレ が 2 番目のアドレスです。以前の構文では、foreign や port などのキーワード 宛先アドレスおよびポートを設定していました。
ASDM 機能	
フラグメントオプションのサポート	ASDM は、ASDM 経由でルーティングされたパケットを再構成するフラグメ ションをサポートするようになりました。 この機能を設定するには、[Configuration] > [Properties] > [Advanced] > [Fragme てください。

ASA 7.0(7)/ASDM 5.0(7) の新機能

リリース：**2007年7月9日**

機能	説明
モジュール機能	
データプレーンキープアライブ メカニズムの追加	ASA を構成して、AIP SSM がアップグレードされた場合に、フェールオーバ せないようにできます。以前のリリースでは、AIP SSM がある 2 つの ASA オーバーで構成されている場合に AIP SSM ソフトウェアが更新されると、A フトウェアの更新を有効にするためにリブートまたは再起動を必要とするの フェールオーバーをトリガーします。 バージョン *7.2(3)* および *8.0(3)* でも使用可能です。

ASA 7.0(6)/ASDM 5.0(6) の新機能

リリース：**2006年8月22日**

ASA 7.0(6)/ASDM 5.0(6) には新機能はありませんでした。

ASA 7.0(5)/ASDM 5.0(5) の新機能

リリース：**2006年4月14日**

機能	説明
アプリケーション インスペクション機能	
DNS ガードを制御するコマンド	DNS ガード機能を制御できるようになりました。7.0(5) よりも前のリリー インスペクションの設定に関係なく、DNS Guard 機能は常にイネーブルに • ID に一致する DNS 要求がある DNS 応答のステートフル トラッキン • すべての保留中要求への応答時の DNS 接続の切断 このコマンドは、DNS 検査が無効である（**no inspect dns**）インターフェ 効です。DNS インスペクションがイネーブルになっている場合、DNS Gu 実行されます。 次のコマンドが導入されました。**dns guard**
拡張 IPSEC インスペクション	IKE フローの存在に基づいて ESP フローのための特定のピンホールを開 された IPSec 検査機能によって提供されます。この機能は、MPF インフ 内で他の検査とともに設定できます。結果として生じる ESP フローのア ウトは、静的に 10 分で設定されています。許可できる ESP フローの数の ん。 次のコマンドが導入されました。**inspect ipsec-pass-thru**
ファイアウォール機能	
拒否された TCP パケットの RST を無効にするコマンド	TCPパケットが拒否されると、パケットが高セキュリティ インターフェイ リティ インターフェイスに送信されるときに、適応型セキュリティ アプ にリセットを送信します。**service resetinbound** コマンドは、TCP パケッ ら高レベルのセキュリティ インターフェイスへの移動時に拒否されたと 信を有効または無効にするために使用します。**service resetinbound** コマン トが高レベルから低レベルのセキュリティ インターフェイスへの移動時 きの RESET 送信を制御するために使用します。既存の **service resetinbou** 追加のインターフェイス オプションを取るように拡張されました。 次のコマンドが導入されました。**service resetoutbound**、**service resetinbo**
プラットフォーム機能	

機能	説明
接続数と VLAN 数の増加	最大接続数と VLAN が次の数まで増加しました。 • ASA5510 基本ライセンス接続数 32000 -> 50000、VLAN 0 -> 10 • ASA5510 プラス ライセンス接続数 64000 -> 130000、VLAN 10 -> 25 • ASA5520 接続数 130000 -> 280000、VLAN 25 -> 100 • ASA5540 接続数 280000 -> 400000、VLAN 100 -> 200
管理機能	
ローカルデータベースでのパスワードの伸張	ユーザー名と有効化パスワードの長さ制限が、ローカル データベースで 16 やされました。
show interface および **show traffic** コマンドの機能拡張	**show interface** および **show traffic** の両方のコマンドで表示されるトラフィッが、入力、出力、およびドロップで 1 分の速度と 5 分の速度をサポートする ました。速度は、最後の 2 つのサンプリング ポイント間の差分として計算さ 分の速度と 5 分の速度に対して、1 分タイマーと 5 分タイマーがそれぞれの通 常に実行されます。新しい表示の例は次のとおりです。 `1 minute input rate 128 pkts/sec,  15600 bytes/sec` `1 minute output rate 118 pkts/sec,  13646 bytes/sec` `1 minute drop rate 12 pkts/sec` `5 minute input rate 112 pkts/sec,  13504 bytes/sec` `5 minute output rate 101 pkts/sec,  12104 bytes/sec` `5 minute drop rate 4 pkts/sec`

ASA 7.0(4)/ASDM 5.0(4) の新機能

リリース：**2005年10月15日**

（注） 7.0(3)/5.0(3) リリースはありませんでした。

機能	説明
プラットフォーム機能	
4GE SSM のサポート	4GE セキュリティ サービス モジュール（SSM）は、適応型セキュリティア 用のオプション I/O カードです。4GE SSM は、セキュリティ アプライアンス な総数のポートを展開し、イーサネット（RJ-45）または SFP（光ファイバー つの追加ポートを提供します。
VPN 機能	

機能	説明
WebVPN キャプチャ機能	WebVPN キャプチャ機能により、WebVPN 接続では正しく表示されない する情報を記録できます。キャプチャ コマンドで WebVPN キャプチャ機 ます。ただしセキュリティ アプライアンスのパフォーマンスに悪影響が してください。したがって、トラブルシューティングに必要な情報をキ は、必ずこの機能を無効にしてください。
VPN トンネル経由の自動更新	このリリースでは、**auto-update server** コマンドに新しい **source** 引数があ り管理アクセスで使用され **management-access** コマンドで指定された VP のインターフェイスを指定できます。 **auto-update server** *url* [**source** *interface*] [*verify-certificate*]
HTTP プロキシ アプレット	HTTP プロキシは、HTTP と HTTPS の両方の接続をサポートするインタ シです。HTTP プロキシ コードは、すべてのブラウザ HTTP/S 要求を新し にリダイレクトするために、ブラウザのプロキシ設定を動的に変更しま Java アプレットはブラウザのプロキシとして引き継ぐことができます。 HTTP プロキシは、ポートフォワーディング（アプリケーション アクセ 合わせて、または単独で使用できます。 （注） HTTP プロキシ機能は、Internet Explorer を使用する場合にのみ Windows XP を実行しているいくつかの古いコンピュータで、RunOnce レ は、Internet Explorer でプロキシ設定を変更しようとするとポート転送 HT 能がエラーとなるために使用できません。 レジストリは手動変更できます。レジストリを手動で変更するには、次の ます。 **1.** [Start] > [Run] をクリックします。 **2.** 開いたテキスト ボックスに **regedit** と入力し、[OK] をクリックしま **3.** 次のフォルダを開きます。 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\ **4.** CurrentVersion の内部を右クリックし、[New] > [Key] を選択します。 **5.** 新しいキー **RunOnce** に名前を付けます。 **6.** [OK] をクリックします。 このユーザーまたはグループ ポリシーに対してファイル アクセスとファ グ、MAPI プロキシ、HTTP プロキシ、および WebVPN 上での URL 入力 は、WebVPN モードで **functions** コマンドを使用します。

機能	説明
IPSec VPN：カスケード ACL のサポートを追加します。	カスケード ACL とは、拒否 ACE を挿入することで、ACL の評価をバイパスし プセット内の次の ACL の評価を再開するものです。各クリプトマップを別 に関連付けることができるため、拒否 ACE を使用して対応するクリプトマッ 評価から特別なトラフィックを除外し、特別なトラフィックを別のクリプト permit 文と一致させて別のセキュリティを提供または要求できます。暗号 A てられているシーケンス番号によって、クリプトマップセット内の評価の順 ます。
トラブルシューティングとモニタリングの機能	
crashinfo の拡張機能	**crashinfo** コマンドからの出力には、ASA に接続しているすべてのユーザーが とが適切でない機密情報が含まれている場合があります。新しい **crashinfo co** コマンドを使用して、コンソール上に表示される出力を抑制できます。
syslog メッセージのレート制限	ロギング レートの制限により、システム ログ メッセージを生成する速度を す。指定した時間間隔の間に生成されるシステム メッセージの数を制限でき すべてのメッセージ、単一のメッセージ ID、メッセージ ID の範囲、または 度レベルがあるすべてのメッセージのメッセージ生成レートを制限できます ログ メッセージの生成レートを制限するには、**logging rate-limit** コマンドを使
ファイアウォール機能	
モジュラ ポリシー フレームワークを使用した接続タイムアウト	新しい **set connection timeout** コマンドにより、経過したらアイドル状態の T 断される、タイムアウト期間を構成できます。
ダウンロード可能な ACL 拡張機能	RADIUS サーバに送信されたダウンロード可能な ACL 要求が、Message-Aut 性を使用して有効なソースから来たものであることを確認するための新しい されました。 ダウンロード可能な ACL の名前が含まれているユーザー名属性を持つ RADI を受信すると、Cisco Secure ACS は Message-Authenticator 属性をチェックして します。Message-Authenticator 属性の存在により、ダウンロード可能な ACL ワーク アクセスの不正取得に悪用されることが防止されます。Message-Auth とその使用方法は、RFC 2869「RADIUS Extensions」で定義されています。こ http://www.ietf.org で入手できます。

機能	説明
ダウンロード可能なACLでのワイルドカードからネットワーク マスクへの変換	VPN 3000 コンセントレータや Cisco IOS ルータなどの一部の Cisco 製品でクマスクの代わりにワイルドカードを使用して、ダウンロード可能なAC要があります。他方、Cisco ASA 5500 適応型セキュリティ アプライアンスクマスクを使用してダウンロード可能なACLを設定する必要があります能によって、ASA はワイルドカードをネットマスクに内部的に変換できカード ネットマスク表現の変換により、RADIUS サーバ上のダウンローコンフィギュレーションを変更することなく、Cisco VPN 3000 Series Con述されたダウンロード可能な ACL を ASA で使用できます。 ACL ネットマスク変換は、**acl-netmask-convert** コマンドを使用してサーきます。このコマンドは AAA サーバ設定モードで使用できます。
アプリケーション インスペクション機能	
GSN 間での GTP ロード バランシングのサポート	ASA が GTP インスペクションを実行する場合、デフォルトで ASA は、Gされていない GSN からの GTP 応答をドロップします。これは、GSN のドバランシングを使用して、GPRS の効率とスケーラビリティを高めています。GSN プーリングのサポートを有効にするには、**permit response** コます。このコマンドは、GTP 要求がどの GSN に送信されたかにかかわらGSN のセットの中のいずれかからの応答を許可するように ASA を設定し

ASA 7.0(2)/ASDM 5.0(2) の新機能

リリース：**2005年7月22日**

ASA 7.0(2)/ASDM 5.0(2) には新機能はありませんでした。

ASA 7.0(1)/ASDM 5.0(1) の新機能

リリース：**2005年5月31日**

機能	説明
プラットフォーム機能	
ASA 5500 シリーズのサポート	ASA 5500 シリーズのサポートが導入されました。これには ASA 5510、A5540 の各モデルのサポートも含まれています。
ファイアウォール機能	

機能	説明
透過的ファイアウォール（レイヤ 2 ファイアウォール）	この機能により、レイヤ2デバイスに類似したセキュアなブリッジング モー展開して、保護されたネットワーク用の機能豊富なレイヤ2～7ファイアウォリティ サービスを提供できます。これにより企業は、ネットワークの再アドを必要とせずに、既存のネットワーク環境にこのASAを展開できます。ASAれたネットワークの両端のデバイスに対して完全に「非表示」にできますが専用 IP アドレス（別のインターフェイス上でホスト可能）によって管理でき者は、レイヤ2デバイスとプロトコルに対するアクセス コントロール用に、加えて、非 IP（EtherType）ACL を指定できます。 次のコマンドが導入されました。**arp-inspection**、**firewall**、**mac-address-tabl** **mac-learn**
セキュリティ コンテキスト（仮想ファイアウォール）	この機能により、単一のアプライアンスで複数のセキュリティ コンテキスト イアウォール）を作成できるようになりました。各コンテキストはセキュリシー、論理インターフェイス、および管理ドメインの独自のセットを持ちまより企業は、単一の物理アプライアンスに複数のファイアウォールを簡便にら、これらの仮想インスタンスを引き続き個別に管理することもできます。能は、無制限（UR）またはフェールオーバー（FO）ライセンスがある ASA可能です。これはライセンス機能であり、サポートされている複数層のセキンテキスト（2、5、10、20、および 50）があります。 次のコマンドが導入されました。**admin-context**、**context**（および context のド）、**changeto**、および **mode**
アウトバウンド ACL	この機能により、管理者は、アウトバウンド ACL および時間ベース ACL の追加することによって（既存のインバウンドACLサポート上に構築）、アクロール ポリシーを定義する際の柔軟性を向上できます。これらの新機能を使理者は、トラフィックがインターフェイスを出入りするときにアクセス コン適用できるようになりました。時間ベースのアクセス コントロール リストに者は特定の ACL エントリがいつアクティブであるかを定義することによっての使用をより細かく制御できます。新しいコマンドにより、管理者は時間範て、それらの時間範囲を特定の ACL に適用できます。
時間ベース ACL	既存の多用途の **access-list** グローバル設定コマンドは **time-range** コマンドにれました。**time-range** グローバル設定コマンドを使用して定義された、時間リシーを指定します。さらに、**access-group** グローバル設定コマンドは、アクACL を設定するために out キーワードをサポートしています。
ACLエントリの有効化/無効化	この機能は、ACLエントリを削除したり置き換えたりする必要なくACLを微調整できる、便利なトラブルシューティング ツールを提供します。
EtherType アクセス コントロール	この機能には、パケットの EtherType に基づいてパケット フィルタリングおグを実行するための、非常に強力なサポートが含まれています。透過的なファルとして動作するときに、非 IP プロトコルの許可または拒否を非常に柔軟にす。

機能	説明
モジュラ ポリシー フレームワーク	この機能により、非常に柔軟で拡張可能な次世代モジュラ ポリシー フレ入されます。これにより、管理者定義の条件に基づく特定のフローを識別ビスをそのフローに適用する（ファイアウォール/インスペクション ポリシー、QoS ポリシーなど）、フローベースのポリシーを構築できます。ラフィック フローに対するきめ細かい制御と、それらに対して実行され幅に向上します。さらにこの新しいフレームワークにより、インスペクでのフロー固有の設定が可能になります（以前のリリースではグローバル 次のコマンドが導入されました。**class-map**、**policy-map**、および **service-**
TCP セキュリティ エンジン	この機能は、プロトコルとアプリケーション層への攻撃の検出を支援する新しい基礎機能を導入します。TCP ストリームの再アセンブルは、パケケット ストリームに再アセンブルしてそのストリームの分析を実行する一連のパケット全体にわたる攻撃を検出できます。TCP トラフィックの正拡張フラグやオプションのチェック、再送パケットでのデータ改ざんの検トのチェックサム検証などを含む攻撃を検出する追加の手法が提供されま グローバル設定コマンドでの **set connection advanced-options** および **tcp-** 設定コマンドの使用により、広範な TCP セキュリティ ポリシーを設定で
アウトバウンド低遅延キューイング（LLQ）およびポリシング	この機能では、低遅延キューイング（LLQ）およびトラフィック ポリシ（エンドツーエンド ネットワーク QoS ポリシーがある機能のサポート）サービス品質（QoS）要件があるアプリケーションをサポートします。有各インターフェイスはアウトバウンド トラフィック用に 2 つのキューをつは遅延の影響を受けやすいトラフィック用（音声や市場データなど）、延を許容できるトラフィック用（ファイル転送など）です。一連の設定り、キューのパフォーマンスを最適化できます。 QoS 機能は、次のコマンドを使用して管理されます。**police**、**priority**、**p** **queue-limit**、および **tx-ring-limit**
アプリケーション インスペクション機能	
拡張 HTTP インスペクション エンジン	この機能は Web トラフィックのディープ分析を導入しています。これにベースの攻撃からの保護を強化するために、HTTP セッションをきめ細かす。さらに、この新しい HTTP インスペクション エンジンにより、インセージング アプリケーション、ピアツーピア ファイル共有アプリケーシポート 80 または HTTP トランザクションに使用されるポート経由でトンするアプリケーションを管理制御できます。提供される機能には、RFC 準HTTP コマンドの承認と適用、応答検証、多目的インターネット メール拡張タイプの検証とコンテンツ コントロール、Uniform Resource Identifier（U用などがあります。 ユーザーは、**http-map** グローバル設定コマンドを使用し、それをマップ名トするために拡張されている **inspect http** 設定モード コマンドに適用する HTTP インスペクション ポリシーを定義できます。

機能	説明
FTP インスペクション エンジン	この機能には、新しいコマンド フィルタ サポートを提供する FTP インスペ ンジンが含まれています。以前にサポートされていた FTP セキュリティ サー トコル異常検出、プロトコル ステート トラッキング、NAT/PAT サポート、 ポート開放など）に基づいて構築すると、バージョン 7.0 では 9 つの異なる ドの使用を細かく制御でき、ユーザー/グループが FTP セッションで実行でき 制されます。さらにバージョン 7.0 は、FTP サーバ クローキング機能を導入 ASA 経由でアクセスするユーザーから FTP サーバのタイプとバージョンを隠
ESMTP インスペクション エンジン	この機能は、SMTP（ESMTP）プロトコルのサポートを追加した SMTP（RF に基づいて構築されており、RFC 1869 で定義されているさまざまなコマン ています。サポートされているコマンドには、**AUTH**、**DATA**、**EHLO**、**ETR** **HELP**、**MAIL**、**NOOP**、**QUIT**、**RCPT**、**RSET**、**SAML**、**SEND**、**SOML**、お が含まれています（他のすべてのコマンドは、追加のセキュリティ レベルを めに自動的にブロックされます）。 **inspect esmtp** グローバル設定コマンドは、SMTP および ESMTP トラフィック ペクション サービスを提供します。
SunRPC / NIS+ インスペクション エンジン	SunRPC インスペクション エンジンでは、NIS + および SunRPC サービスに対 トが向上しています。固有の拡張として、ポートマッパー v2、RPCBind v3 ての 3 バージョンの検索サービスのサポートが含まれています。 SunRPC / NIS+ インスペクション エンジンを設定するには、**inspect sunrpc** お **sunrpc-server** グローバル設定コマンドを使用します。
ICMP インスペクション エンジン	この機能は、ICMPインスペクションエンジンを導入します。このエンジンに 接続のステートフル トラッキングを提供し、エコー要求と応答とを一致させ ICMP を安全に使用できます。ICMP エラー メッセージには追加の制御を使用 これは確立された接続に対してのみ許可されます。このリリースには、NAT メッセージの機能が導入されました。 **inspect icmp** および **inspect icmp error** コマンドを使用して ICMP インスペク ジンを設定します。

機能	説明
モバイルワイヤレス環境のための GTP インスペクション エンジン	この機能により、GPRS トンネリング プロトコル（GTP）を使用してパケタ サービスを提供する、3G モバイル ワイヤレス環境を保護するための新クション エンジンが導入されます。これらの新しい拡張 GTP インスペクスにより、モバイル サービス プロバイダにはローミング パートナーとのクションが許可され、モバイル管理者には IMSI プレフィックス、APN 個有パラメータに基づく堅牢なフィルタリング機能が提供されます。これに供与される機能です。 ポリシーマップ設定モードの **inspect gtp** コマンドと **gtp-map** グローバル設バージョン 7.0 で導入された新機能です。GTP の詳細および GTP インスシーの設定の詳細な手順については、『CLI Configuration Guide』の「Ma Inspection」を参照してください。**activation-key** exec コマンドを使用してベーション キーをインストールすることが必要になる場合があります。
H.323 インスペクション エンジン	H.323 インスペクション エンジンは、T.38 プロトコルのサポートを追加し Fax over IP（FoIP）のセキュア通信を可能にする ITU 標準です。リアルタアンドフォワードの両方の FAX 方式がサポートされます。H.323 インンジンは、現在サポートされている Direct Call Signaling（DCS）メソット Gatekeeper Routed Call Signaling（GKRCS）をサポートします。ITU 標準に基サポートにより、ASA は H.323 ゲートキーパー間で直接交換されるコーメッセージを処理できます。
H.323 バージョン 3 および 4 のサポート	このリリースは、H.323 バージョン 3 および 4 メッセージ用に NAT と PA し、特に H.323 v3 の機能であるワン コール シグナリング チャネル上でのサポートします。
SIP インスペクション エンジン	この機能は、セッション開始プロトコル（SIP）ベース インスタント メライアント（Microsoft Windows Messenger など）のサポートを追加しますRFC 3428 と RFC 3265 で説明されている機能のサポートが含まれます。
SIP を使用するインスタントメッセージングのためのサポート	フィックスアップ SIP は、Windows Messenger RTC Client バージョン 4.7.0 Windows XP のみで、インスタント メッセージング（IM）チャット機能をようになりました。
構成可能な SIP UDP インスペクション エンジン	これは、非セッション情報プロトコル（SIP）パケットが SIP UDP ポートに削除されるのではなく、ASA を通過するための CLI 対応ソリューショす。
MGCP インスペクション エンジン	この機能には、MGCP プロトコルの NAT と PAT をサポートする MGCP ン エンジンが含まれています。これにより、VoIP プロトコルとして MG 0.1 または 1.0 が組み込まれている分散コール処理環境で、シームレスな合が確保されます。 ポリシー マップ設定モードの **inspect mgcp** コマンドと **mgcp-map** グロードにより、ユーザーは MGCP インスペクション ポリシーを設定できます

機能	説明
RTSP インスペクション エンジン	この機能は、リアルタイム ストリーミング プロトコル（RTSP）の NAT サポ します。これにより Cisco IP/TV、Apple Quicktime、および RealNetworks Rea のストリーミング アプリケーションは、NAT 境界をまたいで透過的に作動で
SNMP インスペクション エンジン	他の新しいインスペクション エンジンと同様に、policy-map 設定モードの in マンドおよび snmp-map グローバル設定コマンドにより、ユーザーは SNMP ション ポリシーを設定できます。
H.323 および SIP インスペクションエンジンのポート アドレス変換（PAT）	このリリースでは、ポート アドレス変換（PAT）のサポートを追加すること 既存の H.323 および SIP インスペクション エンジンのサポートを強化します SIP を使用する PAT のサポートの追加により、顧客は単一のグローバル アド してそのネットワーク アドレス空間を展開できます。
Skinny 用の PAT	この機能により、Cisco IP Phone は、PAT で設定されている場合に ASA を介 CallManager と通信できます。これは、ASA の背後の Skinny IP フォンが VPN 業サイトで CallManager と通話するというリモート アクセス環境で特に重要
ILS インスペクション エンジン	この機能は、ILS および Lightweight Directory Access Protocol（LDAP）の NAT するために、Internet Locator Service（ILS）のフィックスアップを提供します のフィックスアップの追加により、ASA は Microsoft NetMeeting による H.323 の確立をサポートします。Microsoft NetMeeting、SiteServer、および Active D 製品は、ディレクトリ サービスである ILS を活用して、エンドポイントの登 所を提供します。ILS は、LDAP プロトコルをサポートし、LDAPv2 準拠で
構成可能な RAS インスペクション エンジン	この機能には、H.323 RAS（登録、許可、状態）フィックスアップをオフにす ンが含まれており、設定すると、構成内にこのオプションが表示されます。こ 顧客は RAS トラフィックがない場合、RAS メッセージを検査したくない場合 UDP ポート 1718 と 1719 を使用する他のアプリケーションがある場合に、RA スアップをオフにできます。
CTIQBE インスペクション エンジン	TAPI/JTAPI フィックスアップとしても知られているこの機能は、NAT、PAT 方向 NAT をサポートする Computer Telephony Interface Quick Buffer Encoding プロトコル インスペクション モジュールを組み込んでいます。これにより、 SoftPhone や他の Cisco TAPI/JTAPI アプリケーションは、ASA を介したコール プや音声トラフィックのために Cisco CallManager と正常に連携して通信しま このリリースは **inspect ctiqbe 2748** コマンドをサポートします。
MGCP インスペクション エンジン	このリリースでは、Media Gateway Control Protocol（MGCP）1.0 のサポートを ます。これによりコール エージェントと VoIP メディア ゲートウェイとの間 ジは、安全な方法で ASA をパススルーできます。 **inspect mgcp** コマンドを参照してください。

機能	説明
TFTP インスペクション エンジンを設定する機能	TFTP インスペクション エンジンを設定する機能により、TFTP プロトコ TFTP クライアントとサーバ間のファイル転送を許可するように、必要で よび xlate を動的に作成します。具体的には、フィックスアップは TFTP （RRQ）、書き込み要求（WRQ）、およびエラー通知（ERROR）を検査 （注） TFTP フィックスアップはデフォルトでイネーブルになってい ラフィックのリダイレクトにスタティック PAT が使用されて TFTP フィックスアップをイネーブルにする必要があります。
フィルタリング機能	
URL フィルタリング パフォーマンスにおける改善	この機能により、ASA と Websense サーバとの間の通信チャネルの改善に る同時の URL の数は大幅に増えます。 既存の **url-server** グローバル設定コマンドは、**connections** キーワードを 使用されるプール内の TCP 接続の数を指定するようになりました。
URL フィルタリングの機能拡張	このリリースでは、最大 1159 バイトまでの URL の N2H2 URL フィルタ をサポートしています。 Websense の場合、長い URL フィルタリングは、4096 バイトの長さまでの サポートされています。 さらに、このリリースは Web サーバからの応答が N2H2 または Websense グ サービス サーバからの応答よりも速い場合に、その応答をバッファに プションを提供します。このコマンドにより、Web サーバの応答を 2 回 がなくなります。
IPSec VPN 機能	
不完全暗号マップの機能強化	すべてのスタティック クリプト マップでアクセス リストと IPSec ピアを あります。いずれかが欠落している場合、暗号マップは不完全と見なされ ジが出力されます。完全暗号マップに一致しないトラフィックはスキッ ントリが試行されます。フェールオーバー hello パケットは、不完全暗号 からは除外されます。
スポーク間 VPN サポート	この機能により、暗号化されたトラフィックは同じインターフェイスを出 で、スポーク間（およびクライアント間）VPN 通信のサポートが向上し スプリットトンネル リモート アクセス接続は ASA の外部インターフェ るようになりました。これによりリモート アクセス ユーザー VPN トン ターネット宛てトラフィックは、着信と同じインターフェイスから発信 りました（ファイアウォール ルールの適用後）。 **same-security-traffic** コマンドは、スポーク間 VPN サポートを有効にする キーワードを指定して使用すると、トラフィックが同じインターフェイス ことを許可します。

機能	説明
VPN 経由の OSPF ダイナミック ルーティング	OSPF のサポートは、IPSec VPN トンネルを介してネイバーをサポートするよ れています。これにより ASA は、他の OSPF ピアへの VPN トンネルを介し ティング更新をサポートできます。OSPF hello はユニキャストであり、RFC 方法で、識別されたネイバーにトンネルを経て転送するために暗号化されま インターフェイス設定モードの **ospf network point-to-point non-broadcast** コマ 合的な OSPF 動的ルーティング サービスを拡張して、IPSec VPN トンネル経由 をサポートし、VPN 接続ネットワークのためのネットワークの信頼性を向上
リモート管理の機能拡張	この機能により管理者は、リモート ASA の内部インターフェイス IP アドレ て、VPN トンネル経由でファイアウォールをリモート管理できます。実際に は管理アクセスのために、どの ASA インターフェイスでも定義できます。こ 動的 IP アドレスを必要とする ASDM、SSH、Telnet、SNMP などをサポート の機能は、ブロードバンド環境にとって大きなメリットとなります。
X.509 証明書サポート	X.509 証明書のサポートは、ASA で大幅に改善されており、n 層の証明書チ （複数レベルの認証局階層がある環境）のサポート、手動登録（オフライン る環境）、および 4096 ビット RSA キーのサポートを追加します。バージョ Cisco IOS ソフトウェアで導入された新しい認証局である、軽量 X.509 認証局 も含まれています。これは PKI 対応のサイト間 VPN 環境のロールアウトを簡 めに設計されています。
Easy VPN サーバ	このリリースは、Cisco Easy VPN サーバをサポートします。Cisco Easy VPN 既存の VPN ヘッドエンドとシームレスに機能するように設計されています。 Cisco VPN クライアントをサポートし、Cisco Easy VPN サーバで VPN 構成を ことでクライアントの管理オーバーヘッドを最小限に抑えます。Cisco Easy 製品の例としては、Cisco VPN Client v3.x 以上、Cisco VPN 3002 Hardware Cli ります。 （注） ASA はすでにセントラルサイトの VPN デバイスとして機能してお ト アクセス VPN クライアントの終端をサポートします。
Easy VPN サーバのロードバランシング サポート	ASA 5500 ASA は、クラスタベースのコンセントレータ ロード バランシング ます。これは、最も利用されていないコンセントレータへの自動リダイレク VPN 3000 シリーズのコンセントレータ ロード バランシングをサポートしま
バックアップ Easy VPN サーバ情報の動的ダウンロード	ヘッドエンドで定義されているバックアップ コンセントレータのリストの をサポートします。 この機能は次のコマンドをサポートします。vpngroup group_name **backup-se** [*ip2... ip10*]}	**clear-client-cfg**}

機能	説明
Easy VPN インターネット アクセス ポリシー	ASA は、保護されたネットワーク上のユーザーに対してインターネットシーに関して Easy VPN リモート デバイスとして使用される ASA の動作新しい動作は、Easy VPN サーバでスプリット トンネリングが有効な場合す。スプリット トンネリングは、ユーザーが VPN トンネルを使用せずにストセッションでASAを介して接続してインターネットにアクセスできる能です。 Easy VPN リモート デバイスとして使用される ASA は、スプリット トンシーをダウンロードし、Easy VPN サーバに初めて接続するときにそれをシュ メモリに保存します。ポリシーがスプリット トンネリングを有効にで保護されたネットワークに接続しているユーザーは、Easy VPN サーバネルの状態に関係なくインターネットに接続できます。
証明書識別名の確認	この機能により、サイト間でいずれかVPN ピアとして、またはリモートEasy VPN サーバとして機能する適応型セキュリティ アプライアンスは、への証明書の照合を検証できます。
手動トンネル制御ユーザー認証およびトンネル状態用の Easy VPN Web インターフェイス	ユーザーレベルの認証と保護されたユニット認証の導入により、ASA はVPN トンネルまたは非保護ネットワークへのアクセス試行時にユーザーしい Web ページを使用して、資格情報の入力、トンネルの接続と切断、ニタができます。これは Easy VPN サーバ機能にのみ適用されます。
ユーザーレベル認証	ASA の内部ネットワーク上での（IP アドレス ベースの）クライアントのポートします。静的およびワンタイム パスワード（OTP）認証の両方のポートされます。これは Web ベースのインターフェイスにより実行され この機能は **vpn-group-policy** コマンドにサポートを追加します。
セキュア ユニットの認証	この機能により、動的に生成された認証資格情報を使用して、Easy VPN ハードウェア クライアント）デバイスを認証できます。
柔軟な Easy VPN 管理ソリューション	外部インターフェイスを使用したASAの管理には、VPNトンネル経由でのフローは必要ありません。すべてのNMSトラフィックをトンネル経由うに要求したり、このポリシーを微調整したりする柔軟性が得られます。
VPN クライアント セキュリティ ポスチャの適用	この機能により、VPN接続の開始時に、VPNクライアントセキュリティクを実行する機能が導入されました。機能には承認されたホストベースの製品（Cisco Security Agent などの）の適用や、そのバージョン番号、ポリ態（有効/無効）の検証が含まれます。 IKE トンネルのネゴシエーション時にセキュリティ アプライアンスが VPにプッシュするパーソナル ファイアウォール ポリシーを設定するには、シー コンフィギュレーション モードで **client-firewall** コマンドを使用しま
VPN クライアントの更新	クライアントの更新パラメータを設定および変更するには、tunnel-group iンフィギュレーション モードで **client update** コマンドを使用します。

機能	説明
オペレーティングシステムとタイプ別のVPNクライアント ブロック	この機能では、クライアントのタイプ、インストールされているオペレーテムのバージョン、およびVPNクライアント ソフトウェアのバージョンに基が許可されている、さまざまなタイプの VPN クライアント（ソフトウェアト、ルータ、VPN 3002、および PIX）を制限する機能を追加します。非準拠が接続しようとした場合、それらのユーザーは、非準拠ユーザーからの接続可するグループに転送することができます。 ASA を通して IPSec 経由で接続できるリモート アクセス クライアントのタジョンを制限するルールを設定するには、グループ ポリシー コンフィギュモードで **client-access-rule** コマンドを使用します。
Movian VPN クライアント サポート	この機能は、ハンドヘルド（PocketPC および Palm）ベースの Movian VPN のサポートを導入し、ネットワークへのアクセスをモバイル従業員とビジネに安全に拡張します。 Perfect Forward Secrecy をネゴシエートするための Diffie-Hellman Group 7（EC いサポートがバージョン 7.0 に追加されました。このオプションは、Movianアントを対象としたものですが、D-H Group 7（ECC）をサポートする他のクでも使用できます。
VPN NAT 透過機能	この機能は、サイト間とリモート アクセス IPSec ベース VPN のサポートを、ル、ワイヤレス ホット スポット、およびブロードバンド環境などの、NAT を実装するネットワーク環境にまで拡張します。バージョン 7.0 ではさらにと User Datagram Protocol（UDP）NAT トラバーサル方式のサポートも追加さこれは NAT/PAT 境界を経由する安全なトラバーサルのための、IETF UDP ラニズムの既存サポートの補完方式です。 NAT トラバーサル ポリシーを設定するときの追加のオプションについては、ローバル設定コマンドを参照してください。
IKE Syslog サポート	この機能は、IKE syslog サポートの小規模な拡張機能と、スケーラブルな VPシューティングのための限定セットの IKE イベント トレーシング機能を導入れらの拡張機能が追加され、新しい syslog メッセージの生成と改善された IKンドの制御が可能になりました。
Diffie-Hellman（DH）Group 5 のサポート	このリリースは、Group 5 の識別子が付与されている 1536 ビット MODP Groトします。
Advanced Encryption Standard（AES）	この機能は、新しい国際暗号化標準を使用してサイト間およびリモートアク続を保護するためのサポートを追加します。これはさらにサポートされるすモデルに対するソフトウェアベースの AES サポートと、新しい VAC+ カードウェア アクセラレーション AES を提供します。
アドレスプールを使用してネットマスクを割り当てるための新しい機能	この機能により、各アドレス プールのサブネット マスクを定義し、その情報ントに渡すことができるようになりました。

機能	説明
暗号化エンジンの既知解テスト（KAT）	関数KATは、ASA暗号化エンジンのインスタンスをテストするためのもストは、ASA の起動時に毎回、フラッシュ メモリから設定を読み取る前す。KAT は、ASA 上で現行ライセンスの有効な暗号アルゴリズムに対しす。
カスタムバックアップ コンセントレータ タイムアウト	この機能は、VPNヘッドエンドへのASAの接続試行での設定可能なタイします。これにより、リストの次のバックアップ コンセントレータへのに関係する遅延を制御します。 この機能は **vpngroup** コマンドをサポートします。
WebVPN 機能	
Web ブラウザ（WebVPN）経由のリモート アクセス	バージョン 7.0(1) は、単一のルーティング モードで、ASA 5500 シリーズアプライアンス上の WebVPN をサポートします。WebVPN によってユーラウザを使用してセキュリティ アプライアンスへのセキュアなリモートトンネルを確立できます。ソフトウェアまたはハードウェア クライアンせん。WebVPN によって、幅広い Web リソースや、Web 対応アプリケーシーアプリケーションの両方に、HTTPSインターネットサイトに到達でコンピュータから簡単にアクセスできます。WebVPN では、Secure Socketコルとその後継である Transport Layer Security（SSL/TLS1）を使用して、ザーと、セントラル サイトで設定した特定のサポート対象内部リソース接続が提供されます。セキュリティ アプライアンスはプロキシ処理が必し、HTTP ユーザーは認証サブシステムと通信してユーザーを認証しま
CIFS	WebVPNは、共通インターネット ファイル システムをサポートしていまリモート ユーザーは、セントラル サイトで事前に設定されたNT/アクティ リ ファイル サーバおよび共有をブラウズしてアクセスできます。CIFS は実行され、名前解決に DNS と NetBIOS を使用します。
ポート転送	WebVPNポート転送（アプリケーション アクセスとも呼ばれる）により、ザーは SSL VPN 接続を介して TCP アプリケーションを使用できます。

機能	説明
Email	WebVPN は、IMAP4S、POP3S、SMTPS、MAPI、Web メールなどの電子メー るいくつかの方法をサポートします。 • IMAP4S、POP3S、SMTPS WebVPN により、リモート ユーザーは、SSL 接続を介して IMAP4、POP3、 電子メール プロトコルを使用できます。 • MAPI プロキシ WebVPN は MAPI をサポートします。これは MS Outlook Exchange ポート転送 メールへのリモート アクセスです。MS Outlook Exchange はリモート コンピ ンストールされている必要があります。 • Web 電子メール Web 電子メールとは、MS Outlook Web Access for Exchange 2000、Exchange 5 Exchange 2003 のことです。中央サイトに MS Outlook Exchange Server が必要
ルーティング機能	
IPv6 インスペクション、アクセス コントロール、および管理	この機能は、IP バージョン 6（IPv6）インスペクション、アクセス コントロ び管理のサポートを導入します。完全ステートフル インスペクションは、専 ドとデュアル スタック IPv4/IPv6 モードの両方での Through-the-box IPv6 トラ に提供されています。さらに、ASA を純粋な IPv6 環境に展開して、SSHv2、 HTTP、および ICMP を含むプロトコルの、IPv6 to-the-box 管理トラフィック できます。バージョン 7.0 で IPv6 トラフィックをサポートするインスペクシ ンには、HTTP、FTP、SMTP、UDP、TCP、ICMP が含まれます。
DHCP オプション 66 および 150 サポート	この機能は、ASA の内部インターフェイスで DHCP サーバを拡張して、TFT 情報をサービス提供先の DHCP クライアントに提供します。この実装は、DH ン 66 要求に対しては 1 つの TFTP サーバで、DHCP オプション 150 要求には のサーバで応答します。 DHCP オプション 66 および 150 は、IP フォン設定の残りの部分をダウンロー に必要な Cisco CallManager 連絡先情報を提供することによって、Cisco IP Ph SoftPhone のリモート展開を簡略化します。
複数のインターフェイス上の DHCP サーバ サポート	このリリースでは、希望数の統合 Dynamic Host Configuration Protocol（DHCP） 任意のインターフェイス上で設定できます。DHCP クライアントは、外部イ イス上でのみ設定できます。DHCP リレー エージェントは、任意のインター で設定できます。ただし、DHCP サーバと DHCP リレー エージェントは同じ 時に設定できませんが、DHCP クライアントと DHCP リレー エージェントに できます。 次のコマンドが変更されました。**dhcpd address**

機能	説明
マルチキャスト サポート	PIM スパース モードが追加され、PIM-SM を使用してマルチキャスト ツ 接参加できるようになりました。この機能は、IGMP転送とクラスDアク ル ポリシーと ACL のために、既存のマルチキャスト サポートを拡張しま は、マルチキャスト環境における透過モード操作の代替を提供します。 **pim** コマンドと **multicast-routing** コマンドにより、この機能の **show mrib** に加え、新しい機能のサポートが追加されました。
インターフェイス機能	
複数のインターフェイスの一般的なセキュリティ レベル	この機能は、一般的なセキュリティ レベルを共有する複数のインターフ することで、セキュリティ レベルのポリシー構造を拡張します。これに キュリティ ポリシー（たとえば同じ DMZ に接続されている 2 つのポート トワーク内での複数のゾーン/部門など）を持つインターフェイスを許可 キュリティ レベルを共有することで、簡略化されたポリシーの展開が可 同じセキュリティ レベルのインターフェイス間の通信は、各インターフ よって制御されます。 同じセキュリティ レベルで設定されているインターフェイス間でトラフ するには、**same-security-traffic** コマンドと **inter-interface** キーワードを参 い。
show interface コマンド	**show interface** コマンドには表示バッファ カウンタがあります。
専用アウトオブバンド管理インターフェイス	**management-only** 設定コマンドは、インターフェイス設定モードで導入さ への専用アウトオブバンド管理アクセスを有効にします。
GEハードウェア速度設定への変更	ギガビット イーサネット カードは、TBI または GMII モードのハードウ 成できます。TBI モードは、半二重をサポートしません。GMII モードは 重の両方をサポートします。ASA で使用されるすべての i8255x コントロ 構成されており、半二重モードをサポートできないので、半二重設定は削
VLAN ベースの仮想インターフェイス	802.1Q VLAN サポートでは、ASA の柔軟な管理とプロビジョニングが可 能により、物理インターフェイスから IP インターフェイスを分離できま 取り付けられているインターフェイス カードの数には関係なく論理 IP イ を構成することが可能になります）。さらに、IEEE 802.1Q タグを適切に 次のコマンドが導入されました。**vlan**
NAT の機能	

機能	説明
オプションのアドレス変換サービス	この機能では、ネットワーク トラフィックのフローを許可する前に、実施さ ドレス変換ポリシーの以前の要件を除去することによって、ASAの展開を簡素 今では、アドレス変換を必要とするホストとネットワークのみが、構成され 翻訳ポリシーを持つ必要があります。この機能は、新しい設定オプションで 「nat-control」を導入しています。これにより、NAT を増分的に有効にでき バージョン 7.0 では、**nat-control** コマンドを導入しており、ソフトウェアの ジョンからアップグレードする顧客の現在の行動が維持されます。設定が消 る新しいセキュリティ アプライアンスまたはデバイスの場合、トラフィック ティ アプライアンスを通過するには、デフォルトは NAT ポリシーを必要と
ハイ アベイラビリティ機能	
非対称ルーティング サポートを使用したアクティブ/アクティブのフェールオーバー	この機能は、受賞歴がある ASA の高可用性アーキテクチャに基づいて構築さ アクティブ/アクティブ フェールオーバーのサポートを導入します。これによ ライセンス供与された UR または 1 つの UR と 1 つの FO-AA のライセンス保 ASA がフェールオーバー ペアとして動作することができ、両方は非対称ルー ポートで同時にアクティブにトラフィックを渡します。アクティブ/アクティ オーバー機能は、このソフトウェア リリースのセキュリティ コンテキスト機 ます。そこではフェールオーバー ペアの各 ASA が 1 つのコンテキストに対し ブになり、残りに対しては逆対称ペアとしてスタンバイになります。バージ り組んでいる別の主要な顧客課題は、非対称ルーティング サポートです。こ 客は、拡張ルーティング トポロジで有効になります。そこではパケットが I ら入り、別の ISP から出て、それらの環境を保護するために ASA を展開しま ジョン 7.0 で導入された非対称ルーティング サポートを活用します）。 アクティブ/アクティブ機能をサポートするために、**failover active** コマンドに ワードで拡張されており、このソフトウェア リリースはフェールオーバー グ モードを導入します。さらに、インターフェイス設定モードの **asr-group** コマ 対称ルーティングでアクティブ/アクティブ ソリューションを環境に拡張しま
VPN ステートフル フェールオーバー	この機能は、VPN 接続用のステートフル フェールオーバーを導入しており、 るファイアウォール フェールオーバー サービスを補完します。すべてセキュ シエーション（SA）の状態情報と鍵関連情報は、高度な復元力がある VPN ソ ンを提供する、フェールオーバー ペア メンバー間で自動的に同期されます。 デバイスが単一ルーティング モードで動作する場合、VPN ステートフル フ バーは暗黙で有効になります。VPN ステートフル フェールオーバー操作およ 細ビューを含む **show failover** EXEC コマンドに加え、**show isakmp sa**、**show** よび **show vpnd-sessiondb** コマンドには、アクティブとスタンバイの両方のユ けるトンネルに関する情報があります。

機能	説明
フェールオーバーの機能拡張	この機能はフェールオーバー機能を拡張するので、ASA フェールオーババイ ユニットは、仮想 MAC アドレスを使用するように構成できます。オーバー ペアの両方の ASA で同時に障害が発生して、スタンバイ ユニ可能であるというあまり起きることがない状況で、ASA フェールオーバれたデバイスでの潜在的な「古い」ARP エントリの問題を排除します。
show failover コマンド	この新しい機能は、フェールオーバーの最後のオカレンスを表示する **sh**ンドを強化します。
HTTP のフェールオーバーサポート	この機能は **failover replicate http** および **show failover** コマンドをサポートフル フェールオーバー環境での HTTP セッションのステートフル複製が HTTP レプリケーションを有効にすると、**show failover** コマンドは **failov**コマンドを表示します。
ゼロダウンタイム ソフトウェア アップグレード	この機能により、ネットワーク アップタイムやユニット間の接続に影響客はフェールオーバー ペアのソフトウェアのアップグレードを実行でき ン 7.0 は、ASA フェールオーバーのペア間でのバージョン間状態共有機ます。これにより顧客は、（アクティブ/スタンバイ フェールオーバー環がオーバーサブスクライブされていないアクティブ/アクティブ環境（各負荷が 50% 超）の）ペアをフローするトラフィックに影響を与えることンス リリースへのソフトウェア アップグレードを実行できます（バージ7.0(2) にアップグレードするなど）。
一般的な高可用性における機能強化	この機能には、フェールオーバー操作と、フェールオーバー操作におけるフェールオーバーの遷移、スケーラビリティの向上、および一層の堅牢性成に対する、多くの重要な拡張機能が含まれています。 このリリースでは次の新しいコマンドが導入されました。**failover interface polltime**、および **failover reload-standby**
トラブルシューティングとモニタリングの機能	
SNMP サポートの向上	この機能は、SNMPv2c のサポートを追加します。これは、64 ビット カウト イーサネット インターフェイス上のパケット カウンタに役立つ）や、一括転送のサポートなどの新しいサービスを提供します。さらに、バージ SNMPv2 MIB（RFC 1907）、IF-MIB（RFC 1573 と 2233）、および Cisco ニタリング MIB が含まれており、トンネル稼働時間、転送済みバイト/パ VPN フロー統計への完全な可視性を付与します。
SNMP を使用した CPU 使用率モニタリング	この機能は、SNMP による ASA CPU 使用率のモニタリングをサポートし用率情報は、**show cpu** [**usage**] コマンドによって ASA 上で引き続き直接入 SNMP は他のネットワーク管理ソフトウェアとの統合を提供します。
SNMP の機能拡張	ASA プラットフォーム固有のオブジェクト ID のサポートが、**SNMP mib-2.system.sysObjectID** 変数に追加されています。これにより ASA に対サポートが有効になります。

機能	説明
フラッシュ メモリのスタック トレース	この機能により、スタック トレースを非揮発性フラッシュ メモリに格納してトラブルシューティング目的で後から取得できるようにします。
ICMP Ping サービス	この機能は、IPv6アドレスのサポートを含む、ping（ICMPエコー）サービスかの追加機能を導入します。**ping** コマンドも拡張オプションをサポートしてにはデータ パターン、DF ビット、リピート数、データグラム サイズ、間隔、サイズのスイープ範囲などがあります。 既存の **ping** EXEC コマンドは、さまざまなキーワードとパラメータで拡張さネットワーク接続問題のトラブルシューティングに役立ちます。これはさらにドの操作のサポートを提供します。
システム正常性のモニタリングおよび診断サービス	この機能は、システム操作のモニタリングを向上させ、潜在的なネットワークの問題を分離できます。**show resource** および **show counters** コマンドは、アスおよびセキュリティのコンテキストのリソース使用率に関する詳細情報と情報を提供します。CPU 使用率をモニタするために、新しい **show cpu** EXEC と、**show process cpu-hog** EXEC コマンドを使用できます。潜在的なソフトウを分離するために、ソフトウェアは **checkheaps** コマンドと、関連する show ンドを導入しています。最後に、ブロック（パケット）利用についてのより得るために、**show blocks** EXEC コマンドは、システムのブロック キューイン関する広範な分析ツールを提供します。
デバッグ サービス	**debug** コマンドが改善され、それぞれのデバッグをサポートする多くの新機まれました。さらに、デバッグ出力が制限なくすべての仮想端末でサポートになりました。つまり、特定の機能のデバッグ出力を有効にすると、出力を示できます。明らかなこととして、出力はそれが有効とされていたセッショれます。最後に、セキュリティ ポリシーによって許可されておりユーザーが場合には、**logging** コマンドを利用してデバッグ出力を syslog を介して送信できます。
SSL デバッグのサポート	Secure Sockets Layer（SSL）プロトコルのサポートは、**debug** コマンドに追加SSL は、クライアントと ASDM および ASA などのサーバとの間の認証と暗のプロトコルです。

機能	説明
Packet Capture	このリリースでは、パケット キャプチャをサポートしています。ASA パチャは、ASA によって受け入れられたまたはブロックされたすべてのトニッフィングしたり「見たり」する機能を提供します。パケット情報をキら、コンソール上でそれを表示して、TFTP サーバを使用してネットワーイルに転送するか、またはセキュア HTTP を使用して Web ブラウザを介ることを選択できます。ただしASAは、同じネットワークセグメント上係のないトラフィックをキャプチャせず、このパケット キャプチャ機能システム、DNS 名前解決、または無作為検出モードのサポートは含まれ ユーザーは **capture** コマンドを指定して、循環バッファでパケット キャきるようになりました。このキャプチャは、管理者によって停止されるまバッファに書き込み続けます。 ASA は、ISAKMP トラフィックのキャプチャと新しい加速セキュリティよってドロップされたパケットのキャプチャを行う機能をサポートするスの操作を診断するユーザーの能力を向上させる追加サポートを導入しま 既存の **capture** コマンドは新しい **type** キーワードとパラメータによって指ISAKMP、パケット ドロップ、および指定された理由ストリングに一致するロップをキャプチャします。
show tech コマンド	この機能は、追加の診断情報を含めるために、現在の **show tech** コマンドます。
管理機能	
フラッシュ メモリでの複数の設定の保存	このリリースは、管理者がセキュリティ アプライアンスの複数の設定をしいフラッシュ ファイル システムを ASA 上に導入しています。これは、生した場合に設定のロールバックを実行できます。この新しいファイルシイルを管理するためのコマンドが導入されています。 （注） 新しいフラッシュ ファイル システムは、使用できる適切なフスがあれば、設定ファイルだけでなく、複数のシステム イメPIX イメージを格納できます。 **boot config** グローバル設定コマンドでは、起動時に使用すべき設定ファイます。
Secure Asset Recovery	この機能により、**service password recovery** コマンドが ASA 設定にない場データ、証明書、および鍵関連情報を復元できないようにできます（顧客セットを復元できます）。物理的なセキュリティが理想的ではない場合に物が個人の機密性の高い設定データにアクセスすることを防ぐためには、に立ちます。

機能	説明
スケジュールされたシステムのリロード（再起動）	管理者は、特定の時刻または現在時刻からのオフセットのいずれかで、ASA をスケジュールできるようになりました。これにより、ネットワークのダウンスケジュールして、近づいている再起動についてリモートアクセス VPN ユーザーすることがさらに簡単になりました。
コマンドライン インターフェイス（CLI）の利便性	この機能は、改善された使いやすさと共通のユーザー エクスペリエンスのため、コンド補完、オンラインヘルプ、エイリアスなど、多くの人気のある Cisco IOS ソフトウェア コマンドライン サービスを組み込むことによって、CLI「ユーザ エクスペリエンス」を向上させます。
コマンドライン インターフェイス（CLI）アクティベーション キー管理	この機能により、システム モニタ モードを使用したり、新しいイメージのインストールしたりせずに、ASA コマンドライン インターフェイス（CLI）から新しいアクティベーション キーを入力できます。さらに、ASA CLI は、**show version** コマンドを入力すると、現在実行されているアクティベーション キーを表示します。
show version コマンド	**show version** コマンド出力には、Max Physical interfaces と Max interfaces の 2 つのインターフェイス関連行が備えられました。最大インターフェイス数は、物理および仮想インターフェイス数の合計です。
AAA 機能	
AAA 統合	簡易化された VPN ユーザーの認証のための、Kerberos、NT Domain、および RSA SecurID を含む認証サービスとの（別の RADIUS/TACACS+ サーバを必要としない）ネイティブ ン 7.0(1) のネイティブな統合。このリリースでは、ASA への管理アクセスのためのログと、管理セッション中に行われた構成変更すべてをトラッキングするための TACACS+AAA アカウンティング レコードを生成する機能も導入されました。
管理アクセスのための AAA フォールバック	この機能により、認証および承認要求を ASA 上のローカル ユーザー データベースにフォールバックすることができます。要件と設計は、Cisco IOS ソフトウェアおよび ASA の「メソッドリスト」サポートとの将来の互換性に寄与し、ローカル フォールバック メソッドの追加を提供します。
AAA 統合機能拡張	この機能により、簡易化されたユーザーと管理者の認証のための、Kerberos、NT および RSA SecurID を含む認証サービスとの（別の RADIUS/TACACS+ サーバを必要としない）ネイティブな統合が導入されます。この機能では、ASA への管理アクセスのためのトラッキングと、管理セッション中に行われた構成変更すべてをトラッキングするための TACACS+AAA アカウンティング レコードを生成する機能も導入されました。

機能	説明
Secure HyperText Transfer Protocol（HTTPS）認証プロキシ	この機能は、HTTP セッションを安全に認証する ASA の機能を拡張し、H キシのサポートを追加します。HTTP セッションの認証を安全に設定する **authentication secure-http-client** コマンドを使用します。HTTPS セッショ 証を設定するには、**aaa authentication include https** または **aaa authenticat** コマンドを使用します。 このリリースでは、**aaa authentication include tcp/0** コマンドを含む構成に プロキシ機能を継承します。これはデフォルトではバージョン 6.3 以降の グレードにより有効になります。
ダウンロード可能アクセス コントロール リスト（ACL）	この機能は、Access Control Server（ACS）から ASA への ACL のダウンロ トします。これにより AAA サーバ上でユーザごとのアクセス リストを構 ザーごとのアクセス リスト認証を提供し、それを ACS から ASA にダウ ようにします。 この機能は、RADIUS サーバでのみサポートされ、TACACS+ サーバでは せん。
AAA 認証のための新しい Syslog メッセージング	この機能は、サービス ポートを使用する前に、ユーザーに認証を促す新 メッセージを導入します。
per-user-override	この機能により、ユーザーは新しいキーワード per-user-override を **access-** に指定できます。このキーワードを指定すると、ユーザーに関連付けられ ごとのアクセスリスト（AAA 認証でダウンロードされた）の許可/拒否状態 アクセスリストの許可/拒否状態を上書きできます。
ネットワークおよびVPNアクセス用のローカル ユーザー認証データベース	この機能により、ASA ローカル ユーザー名データベースを使用して、ト してカットスルーおよび VPN（xauth を使用する）を実行できます（外部 よる既存の認証に追加する代替として）。 サーバ タグ変数は、値 LOCAL を受け入れて、ローカル データベースを スルー プロキシ認証をサポートするようになりました。
ASDM 機能	
動的ダッシュボード（ASDM ホーム ページ）	• システムと利用可能なリソースをすばやく識別するために、詳細な ライセンス情報を表示します。 • リアルタイムのシステムおよびトラフィックのプロファイルを表示し
Real-time Log Viewer	• リアルタイム syslog メッセージを表示します。 • 拡張フィルタリング機能により、主要なイベントに簡単に焦点を当て ます。

機能	説明
改善された Java Web ベースアーキテクチャ	• 最適化されたアプレット キャッシュ機能により ASDM のロードを加速 • すべての管理およびモニタリング機能に、いつでも、どこでもアクセス す。
ダウンロード可能 ASDM ランチャ（Microsoft Windows 2000 または XP オペレーティング システムのみ）	• ASDM はダウンロードしてご使用の PC 上でローカルに実行できます。 • ASDM ランチャの複数のインスタンスは、同じ管理ワークステーション 複数のセキュリティ アプライアンスに管理アクセスを提供します。 • アプライアンス上にインストールされたバージョンに基づいてソフトウ 的に更新され、ネットワーク全体で一貫性のあるセキュリティ管理が可 す。
複数の言語のオペレーティング システム サポート	英語と日本語の両方のバージョンの Microsoft Windows オペレーティング シ ポートします。

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。