Cisco ASA シリーズ 9.13(x) リリースノート

Cisco ASA シリーズ 9.13(x) リリースノート

このドキュメントには、Cisco ASA ソフトウェアバージョン 9.13(x) のリリース情報が記載されています。

特記事項

- ASA 5512-X、ASA 5515-X、ASA 5585-X、および ASASM 用の ASA 9.13(1) 以降ではサポートされていません。ASA 9.12(x) が最後にサポートされていたバージョンです。ASA 5515-X および ASA 5585-X FirePOWER モジュールについては、サポートされる最後のバージョンは 6.4 です。

  注：ASDM 7.13(1) および ASDM 7.14(1) でも、これらのモデルはサポートされていません。ASDM のサポートを復活させるには、ASDM 7.13(1.101) または 7.14(1.48) にアップグレードする必要があります。

- 9.13(1) 以降では ASAv に 2GB のメモリが必要：9.13(1) 以降の ASAv の最小メモリ要件は 2GB です。現在の ASAv が 2 GB 未満のメモリで動作している場合は、以前のバージョンから 9.13(1) にアップグレードできません。アップグレードする前にメモリサイズを調整する必要があります。バージョン 9.13(1) でサポートされているリソース割り当て（vCPU とメモリ）については、ASAv のスタートアップガイドを参照してください。

- **プラットフォームモードでの 9.13 から 9.12 以前への Firepower 2100 のダウングレードの問題**：プラットフォームモードに変換した 9.13 を新規インストールした Firepower 2100 の場合：9.12 以前にダウングレードすると、FXOS で新しいインターフェイスの設定や、既存のインターフェイスの編集ができなくなります（9.12 以前ではプラットフォームモードのみがサポートされていたことに注意してください）。バージョンを 9.13 に戻すか、または FXOS の erase configuration コマンドを使用して設定をクリアする必要があります。この問題は、元々以前のリリースから 9.13 にアップグレードした場合は発生しません。新しいデバイスや再イメージ化されたデバイスなど、新規インストールのみが影響を受けます。（CSCvr19755）

- 9.13(1) でのクラスタ制御リンク MTU の変更：9.13(1) 以降では、多くのクラスタ制御パケットが以前のリリースよりも大きくなっています。クラスタ制御リンクに推奨されている MTU は常に 1600 以上であり、この値が適切です。ただし、MTU を1600に設定しても接続スイッチの MTU と一致しなかった場合は（スイッチの MTU を1500 のままにしたなど）、ドロップされたクラスタ制御パケットとのこの不一致の影響が現れ始めます。クラスタ制御リンク上のすべてのデバイスが同じ MTU（具体的には 1600 以上）に設定されていることを確認します。

- **ASA 5506-X、5508-X、および 5516-X の ROMMON のバージョン 1.1.15 以降へのアップグレード**：これらの ASA モデルには新しい ROMMON バージョンがあります（2019 年 5 月 15 日）。最新バージョンにアップグレードすることを強くお勧めします。アップグレードするには、『ASA コンフィギュレーション ガイド』の手順を参照してください。

  注意：1.1.15 の ROMMON のアップグレードには、以前の ROMMON バージョンの 2 倍の時間がかかります（約 15 分）。アップグレード中はデバイスの電源を**再投入しないでください**。アップグレードが 30 分以内に完了しないか、または失敗した場合は、シスコ テクニカルサポートに連絡してください。デバイスの電源を再投入したり、リセットしたり**しないでください**。

- **ISA 3000 の ROMMON のバージョン 1.0.5 以降へのアップグレード**：これらの ISA 3000 には新しい ROMMON バージョンがあります（2019 年 5 月 15 日）。最新バージョンにアップグレードすることを強くお勧めします。アップグレードするには、『ASA コンフィギュレーション ガイド』の手順を参照してください。

  注意：1.0.5 の ROMMON のアップグレードには、以前の ROMMON バージョンの 2 倍の時間がかかります（約 15 分）。アップグレード中はデバイスの電源を**再投入しないでください**。アップグレードが 30 分以内に完了しないか、または失敗した場合は、シスコ テクニカルサポートに連絡してください。デバイスの電源を再投入したり、リセットしたり**しないでください**。

- **ASA 5506-X シリーズおよび ASA 5512-X の ASA FirePOWER モジュールについては、9.10(1) 以降ではサポートされない**：ASA 5506-X シリーズおよび 5512-X では、メモリの制約により、9.10(1) 以降で ASA FirePOWER モジュールがサポートされなくなりました。このモジュールの使用を継続するには、9.9(x) 以前の状態のままにしておく必要があります。その他のモジュール タイプは引き続きサポートされます。9.10(1) 以降にアップグレードすると、FirePOWER モジュールにトラフィックを送信するための ASA 設定が消去されます。アップグレード前に設定を必ずバックアップしてください。FirePOWER イメージとその設定は SSD にそのままの状態で保持されます。ダウングレードする場合は、バックアップから ASA 設定をコピーして機能を復元できます。

- **9.13(1) 以降、ASA は、次の認定条件のいずれかが満たされている場合にのみ、LDAP/SSL 接続を確立します。**
  - LDAP サーバー証明書が信頼されていて（トラストポイントまたは ASA トラストプールに存在する）、有効であること。
  - チェーンを発行しているサーバーからの CA 証明書が信頼されていて（トラストポイントまたは ASA トラストプールに存在する）、チェーン内のすべての下位 CA 証明書が完全かつ有効であること。

- **ローカル CA サーバーは 9.13(1) で削除される**：ASA がローカル CA サーバーとして設定されている場合、デジタル証明書の発行、証明書失効リスト（CRL）の発行、および発行された証明書の安全な取り消しが可能です。この機能は古くなったため、**crypto ca server** コマンドは削除されています。

- **CRL 配布ポイントコマンドの削除**：スタティック CDP URL 設定コマンド、つまり **crypto-ca-trustpoint crl** と **crl url** は関連する他のロジックとともに削除されました。CDP URL が match certificate コマンドに移動されました。

（注） CDP URL 設定が拡張され、単一のマップに対して CDP オーバーライドの複数のインスタンスを許可するようになりました（CSCvu05216 を参照）。

- **バイパス証明書の有効性チェックオプションの削除**：CRL または OCSP サーバーとの接続の問題による失効チェックをバイパスするオプションが削除されました。

  次のサブコマンドが削除されています。

  - **revocation-check crl none**
  - **revocation-check ocsp none**
  - **revocation-check crl ocsp none**
  - **revocation-check ocsp crl none**

  したがって、アップグレード後は、trailing none を無視することで、サポートされなくなった revocation-check コマンドは新しい動作に移行します。

（注） これらのコマンドは後で復元されました（CSCtb41710 を参照）。

- **低セキュリティの暗号の廃止**：ASA IKE、IPsec、および SSH モジュールで使用されるいくつかの暗号化方式は、安全ではないと見なされ、廃止されています。これらは、以降のリリースで削除されます。

  IKEv1：次のサブコマンドは廃止されています。

  - **crypto ikev1 policy** *priority*:
    - **hash md5**
    - **encryption 3des**
    - **encryption des**
    - **group 2**
    - **group 5**

  IKEv2：次のサブコマンドは廃止されています。

  - **crypto ikev2 policy** *priority*
    - **integrity md5**
    - **prf md5**

- **group 2**
- **group 5**
- **group 24**
- **encryption 3des**
- **encryption des**（このコマンドは、DES 暗号化ライセンスのみがある場合でも使用できます）
- **encryption null**

IPsec：次のコマンドは廃止されています。

- **crypto ipsec ikev1 transform-set *name* esp-3des esp-des esp-md5-hmac**
- **crypto ipsec ikev2 ipsec-proposal *name***
  - **protocol esp integrity md5**
  - **protocol esp encryption 3des aes-gmac aes-gmac- 192 aes-gmac -256 des**
- **crypto ipsec profile *name***
  - **set pfs group2 group5 group24**

SSH：次のコマンドは廃止されました。

- **ssh cipher integrity custom hmac-sha1-96:hmac-md5: hmac-md5-96**
- **ssh key-exchange group dh-group1-sha1**

SSL：次のコマンドは廃止されました。

- **ssl dh-group group2**
- **ssl dh-group group5**
- **ssl dh-group group24**

暗号マップ：次のコマンドは廃止されました。

- **crypto map *name sequence* set pfs group2**
- **crypto map *name sequence* set pfs group5**
- **crypto map *name sequence* set pfs group24**
- **crypto map *name sequence* set ikev1 phase1-mode aggressive group2**
- **crypto map *name sequence* set ikev1 phase1-mode aggressive group5**

- **crypto map set pfs**、**crypto ipsec profile**、**crypto dynamic-map set pfs**、および **crypto map set ikev1 phase1-mode** を使用する IPsec PFS の **crypto ikev1 policy**、**ssl dh-group**、および **crypto ikev2 policy** の **group** コマンドのデフォルトは、**9.13(1) では、Diffie-Hellman Group 14 になりました。**以前のデフォルトの Diffie-Hellman グループは Group 2 でした。

9.13 (1) 以前のリリースからアップグレードし、古いデフォルト（Diffie-Hellman Group 2）を使用する必要がある場合は、DH グループを **group 2** として手動で設定する必要があります。そうでない場合、トンネルはデフォルトで Group 14 に設定されます。group 2 は今後のリリースで削除されるため、できるだけ早く group 14 にトンネルを移動する必要があります。

システム要件

このセクションでは、このリリースを実行するためのシステム要件を一覧表で示します。

ASA と ASDM の互換性

ASA/ASDM ソフトウェアおよびハードウェアの要件およびモジュールの互換性を含む互換性の詳細については、『Cisco ASA Compatibility』を参照してください。

VPN の互換性

VPN の互換性については、『Supported VPN Platforms, Cisco ASA 5500 Series 』を参照してください。

新機能

このセクションでは、各リリースの新機能を示します。

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

ASA 9.13(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	

機能	説明
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**
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**
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。Firepower Chassis Manager 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**
DHCP の予約	ASA DHCP サーバが 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**

機能	説明
ASAv 最小メモリ要件	ASAv の最小メモリ要件は 2GB です。現在の ASAv が 2GB 未満のメモリで動作している場合、ASAv 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 ASAv 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。
ASAv MSLA サポート	ASAv 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**
ASAv 柔軟なライセンス	すべての ASAv ライセンスは、サポートされているすべての ASAv vCPU/メモリ構成で使用できるようになりました。AnyConnect 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 ASAv 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**
AWS の ASAv 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 ASAv 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。

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 ASAv	Microsoft Azure パブリッククラウドの ASAv 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。
DPDK の ASAv 拡張サポート	ASAv 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 ASAv 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) で導入されました。 変更されたコマンドはありません。
VMware ESXi 6.7 用の ASAv サポート	ASAv 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 ASAv 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。
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	
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**

機能	説明
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。
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**
グループごとの AAA サーバ グループとサーバの制限が増えました。	より多くの AAA サーバ 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）。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**
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	
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)**。
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>.**

機能	説明
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**
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）
クラスタのトラフィック負荷のモニタ	クラスタ メンバのトラフィック負荷をモニタ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**
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**
ルーティング機能	

機能	説明
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]**
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。 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。
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**

機能	説明
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**
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**
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）
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

機能	説明
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
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

機能	説明
SSH 認証の機能拡張	FXOS では、次の SSH サーバ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** 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

ソフトウェアのアップグレード

このセクションには、アップグレードを完了するためのアップグレードパス情報とリンクが記載されています。

ASA のアップグレードパス

現在のバージョンとモデルを表示するには、次のいずれかの方法を使用します。

- ASDM：**[Home]** > **[Device Dashboard]** > **[Device Information]** の順に選択します。
- CLI：**show version** コマンドを使用します。

次の表に、ASA のアップグレードパスを示します。バージョンによっては、新しいバージョンにアップグレードする前に、中間アップグレードが必要な場合があります。推奨バージョンは**太字**で示されています。

（注） 開始バージョンと終了バージョンの間で、各リリースのアップグレードガイドラインを必ず確認してください。場合によっては、アップグレードする前に構成を変更する必要があります。そうしないと、停止が発生する可能性があります。

（注） ASA のセキュリティの問題と、各問題に対する修正を含むリリースについては、ASA Security Advisories を参照してください。

（注） ASA 9.12(x) は ASA 5512-X、5515-X、5585-X、および ASASM 用の最終バージョン、
ASA 9.2(x) は ASA 5505 用の最終バージョン、
ASA 9.1(x) は ASA 5510、5520、5540、5550、および 5580 用の最終バージョンです。

現在のバージョン	暫定アップグレードバージョン	ターゲットバージョン
9.12(x)	—	次のいずれかになります。
9.10(x)	—	次のいずれかになります。 → **9.12(x)**
9.9(x)	—	次のいずれかになります。 → **9.12(x)**
9.8(x)	—	次のいずれかになります。 → **9.12(x)**
9.7(x)	—	次のいずれかになります。 → **9.12(x)** → 9.8(x)
9.6(x)	—	次のいずれかになります。 → **9.12(x)** → 9.8(x)
9.5(x)	—	次のいずれかになります。 → **9.12(x)** → 9.8(x)
9.4(x)	—	次のいずれかになります。 → **9.12(x)** → 9.8(x)

現在のバージョン	暫定アップグレードバージョン	ターゲットバージョン
9.3(x)	—	次のいずれかになります。 → **9.12(x)** → 9.8(x)
9.2(x)	—	次のいずれかになります。 → **9.12(x)** → **9.8(x)**
9.1(2)、9.1(3)、9.1(4)、9.1(5)、9.1(6)、または 9.1(7.4)	—	次のいずれかになります。 → **9.12(x)** → 9.8(x) → 9.1(7.4)
9.1(1)	→ 9.1(2)	次のいずれかになります。 → **9.12(x)** → 9.8(x) → 9.1(7.4)
9.0(2)、9.0(3)、または 9.0(4)	—	次のいずれかになります。 → **9.12(x)** → 9.8(x) → 9.6(x) → 9.1(7.4)
9.0(1)	→ 9.0(4)	次のいずれかになります。 → **9.12(x)** → 9.8(x) → 9.1(7.4)
8.6(1)	→ 9.0(4)	次のいずれかになります。 → **9.12(x)** → 9.8(x) → 9.1(7.4)

現在のバージョン	暫定アップグレードバージョン	ターゲットバージョン
8.5(1)	→ 9.0(4)	次のいずれかになります。 → **9.12(x)** → 9.8(x) → 9.1(7.4)
8.4(5+)	—	次のいずれかになります。 → **9.12(x)** → 9.8(x) → 9.1(7.4) → 9.0(4)
8.4(1) ～ 8.4(4)	→ 9.0(4)	→ **9.12(x)** → 9.8(x) → 9.1(7.4)
8.3(x)	→ 9.0(4)	次のいずれかになります。 → **9.12(x)** → 9.8(x) → 9.1(7.4)
8.2(x) 以前	→ 9.0(4)	次のいずれかになります。 → **9.12(x)** → 9.8(x) → 9.1(7.4)

アップグレードリンク

アップグレードを完了するには、『Cisco ASA Upgrade Guide』を参照してください。

未解決のバグおよび解決済みのバグ

このリリースで未解決のバグおよび解決済みのバグには、Cisco Bug Search Tool を使用してアクセスできます。この Web ベース ツールから、この製品やその他のシスコハードウェアおよびソフトウェア製品でのバグと脆弱性に関する情報を保守するシスコ バグ トラッキング システムにアクセスできます。

（注） Cisco Bug Search Tool にログインしてこのツールを使用するには、Cisco.com アカウントが必要です。アカウントがない場合は、アカウントを登録できます。シスコサポート契約がない場合は、ID でのみバグを探すことができます。検索は実行できません。

Cisco Bug Search Tool の詳細については、Bug Search Tool（BST）ヘルプおよび FAQ を参照してください。

バージョン 9.13(x) で未解決のバグ

次の表に、このリリースノートの発行時点で未解決のバグを示します。

問題 ID 番号	説明
CSCvp95110	APP モードでの ASA のアップグレード後に、プラットフォームとパッケージのバージョンが更新されない
CSCvq02977	HTTPS を介した KP コピーイメージのパフォーマンスが非常に低い
CSCvq15125	SSP FXOS/ASA：ipsec 接続が b/w mio および ASA ゲートウェイで機能しない
CSCvq54299	アクティブユニットとスタンバイユニットの再起動後、40 のコンテキストが設定される代わりに 4 つのコンテキストだけが作成される
CSCvq61523	FP1000：AnyConnect-Parent SSL トンネルで再接続が繰り返される
CSCvq73464	ip-client が有効になっている ASA の IPv6 アドレスが snmptrap ログに表示されない
CSCvr02080	多数のエントリを含む CRL のデコード中に、CERT API プロセスで CPU 占有が観察される
CSCvr19755	FP2100 ASA：ポートチャネルの作成時とインターフェイスの編集時にタイムアウトエラーが発生する
CSCvr19922	クラスタ：特定の状況下で BGP ルートが同期しなくなる場合がある
CSCvr21119	FP1000 ユニットで SSD Secure erase コマンドを発行した際に電源の再投入メッセージが追加される
CSCvr22260	一般的な負荷において ike_mib.c:578 の IkeAddFailEntry で lina がリロードされる
CSCvr23986	負荷が高くなると LINA の mh_magic_verify および SrDoMgmt でアサートがトリガーされる

問題 ID 番号	説明
CSCvr29769	eem を実行している malloc_show_bin_info_pool でセグメント違反とリロードが発生する
CSCvr44123	セッションタイムアウトがデフォルトでない場合、FPR2100 の Chassis Manager または REST API を介してログインできない

バージョン 9.13(1) で解決済みのバグ

次の表に、このリリースノートの発行時点で解決済みのバグを示します。

問題 ID 番号	説明
CSCvi07901	IKEv2 AnyConnect 用の ASA で CISCO-REMOTE-ACCESS-MONITOR-MIB crasIPSecNumSessions がゼロになる
CSCvj99658	レンダリング制御チャネルをテストしている ASA/Lina HA フェールオーバー インターフェイスが応答しない
CSCvn16864	ENH：ASA HTTP WebVPN ポータルに Content-Security-Policy ヘッダーがない
CSCvo05052	vFTD で Snort エンジン検査を通過する ICMP パケットの遅延が変動する
CSCvo80725	「エラー：ip_multicast_ctl によるチャネルの取得に失敗（ERROR: ip_multicast_ctl failed to get channel）」により vFTD 6.4 が OSPF 隣接関係を確立できない
CSCvp09083	ASA が BVI インターフェイス上の DHCP 要求パケットに応答しない
CSCvp23530	write standby または reload 後に、OSPF neighbor コマンドがスタンバイに複製されない
CSCvp38774	WebVPN リライタが Web サイトを正しくロードしない
CSCvp42484	MTU が変更されたときに IS-IS hello パケット長が正しい MTU に更新されない
CSCvp71766	VPN トンネルを介して BVI からソースを取得すると、RADIUS 認証に失敗する
CSCvp73394	フェールオーバー ASA IKEv2 VTI：セカンダリ ASA がスタンバイ IP をトラフィックセレクタとして送信する
CSCvp75965	お客様が FMC で Syslog 設定を指定した後にプライマリ FPR2110 がクラッシュする

問題 ID 番号	説明
CSCvp78171	クラスタ内の ASA がピアユニットとの IPv6 ND テーブルの同期に失敗する
CSCvp91905	ASA が、新しく設定された IPv6 アドレスを現在のリンクローカルアドレスに追加する
CSCvq00560	ASA が、ESP 認証データフィールドサイズ（ICV）に違反するパケットをサイレントドロップする
CSCvq10239	SSL HW アクセラレーションを有効にすると、FTD TCP プロキシが 3 回の再送信後に接続を切断する
CSCvq10500	CLISH と LINA の両方のキャプチャが IPv6 アドレスで機能しない
CSCvq15976	ASA メモリリーク：snp_svc_insert_dtls_session
CSCvq17551	Syslog 711004 のイベントマネージャイベントのトリガーに一貫性がない
CSCvq22358	あるコンテキストのアンチリプレイを無効にすると、他のコンテキストのアンチリプレイも無効になる
CSCvq24494	FP2100 - FP2100 プラットフォームでリング/CPU コアをオーバーサブスクライブするフローによって動作中フローの中断が発生する
CSCvq46737	NAT ポリシー設定で L4 サービスポートによる FTD デバイスの展開に失敗する
CSCvq57591	フェールオーバーリンクで IP 通信のみが中断される場合にデータインターフェイスで LANTEST メッセージが送信されない
CSCvq73595	ユーザー名が 32 文字より長い場合に ASA WebVPN が証明書 UPN からユーザー名を抽出できない
CSCvq76706	「show logging」の出力でメッセージログ統計をクリアする機能
CSCvq84444	静的ルートを設定すると、スタンバイルート ASA で「ルートセッション」の rerr カウンタが増加する

エンドユーザライセンス契約書

エンドユーザライセンス契約書の詳細については、http://www.cisco.com/go/warranty [英語]にアクセスしてください。

関連資料

ASA の詳細については、『Navigating the Cisco ASA Series Documentation』を参照してください。

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。