Cisco ASA シリーズ 9.15(x) リリースノート

Cisco ASA シリーズ 9.15(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 9.15(x) のリリース情報が記載されています。

特記事項

- ASA 9.15(1) 以降では、ASA 5525-X、ASA 5545-X、および ASA 5555-X はサポート対象外：ASA 9.14(x) がサポートされている最後のバージョンです。ASA FirePOWER モジュールについては、6.6 がサポートされている最後のバージョンです。
- **シスコは、ASA バージョン 9.17(1) で有効なクライアントレス SSL VPN の非推奨機能を発表**：9.17(1) より前のリリースでは、限定的なサポートが継続されます。
- Firepower 1010 の場合の無効な VLAN ID による問題発生の可能性：9.15(1) にアップグレードする前に、3968 ー 4047 の範囲内のスイッチポートに VLAN を使用していないことを確認してください。これらの ID は内部使用専用であり、9.15(1) には、これらの ID を使用していないことを確認するチェックが含まれます。たとえば、フェールオーバーペアのアップグレード後にこれらの ID が使用されていた場合、フェールオーバーペアは一時停止状態になります。詳細については、「CSCvw33057」を参照してください。
- **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 Configuration Guide』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。

- SAMLv1 機能の廃止：SAMLv1 のサポートは廃止されました。
- ASA 9.15(1) での低セキュリティ暗号の削除：IKE および IPsecで使用される安全性の低い次の暗号のサポートが廃止されました。
  - Diffie-Hellman グループ：2 および 24
  - 暗号化アルゴリズム：DES、3DES、AES-GMAC、AES-GMAC-192、AES-GMAC-256、NULL、ESP-3DES、ESP-DES、ESP-MD5-HMAC
  - ハッシュアルゴリズム：MD5

（注） 安全性の低い SSH 暗号と SSL 暗号はまだ廃止されていません。

ASA の以前のバージョンからバージョン 9.15(1) にアップグレードする前に、9.15(1) でサポートされている暗号を使用するように VPN 設定を更新する必要があります。そのようにしないと、古い設定が拒否されます。設定が拒否されると、コマンドに応じて次のいずれかのアクションが実行されます。

- コマンドはデフォルトの暗号を使用する。
- コマンドが削除される。

アップグレード前の設定の修正は、クラスタリングまたはフェールオーバーの展開で特に重要です。たとえば、セカンダリユニットが 9.15(1) にアップグレードされ、削除された暗号がプライマリからこのユニットに同期された場合、セカンダリユニットは設定を拒否します。この拒否により、クラスタへの参加の失敗などの予期しない動作が発生する可能性があります。

IKEv1：次のサブコマンドが削除されています。

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

IKEv2：次のサブコマンドが削除されています。

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

- **group 2**
- **group 24**
- **encryption 3des**
- **encryption des**
- **encryption null**

IPsec：次のサブコマンドが削除されています。

- **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 group24**

Crypto Map：次のサブコマンドが削除されています。

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

- CRL 配布ポイント設定の再導入：9.13(1) で削除された静的 CDP URL 設定オプションが **match-certificate** コマンドに再導入されました。
- バイパス証明書の有効性チェックオプションの復元：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復元されました。

  次のサブコマンドが復元されました。

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

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 9.15(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。
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。

機能	説明
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。
ファイアウォール機能	
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**
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** *9.12(4)* でも同様です。
インターフェイス機能	
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**
証明書の機能	
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**。
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。

機能	説明
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。
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**
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** *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。

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 9.14(x) は ASA 5525-X、5545-X、および 5555-X の最終バージョンです。

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
9.14(x)	—	次のいずれかになります。 → 9.15(x)
9.13(x)	—	次のいずれかになります。 → 9.15(x) → 9.14(x)
9.12(x)	—	次のいずれかになります。 → 9.15(x) → 9.14(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
9.10(x)	—	次のいずれかになります。 → 9.15(x) → 9.14(x) → 9.12(x)
9.9(x)	—	次のいずれかになります。 → 9.15(x) → 9.14(x) → 9.12(x)
9.8(x)	—	次のいずれかになります。 → 9.15(x) → 9.14(x) → 9.12(x)
9.7(x)	—	次のいずれかになります。 → 9.15(x) → 9.14(x) → 9.12(x) → 9.8(x)
9.6(x)	—	次のいずれかになります。 → 9.15(x) → 9.14(x) → 9.12(x) → 9.8(x)
9.5(x)	—	次のいずれかになります。 → 9.15(x) → 9.14(x) → 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
9.4(x)	—	次のいずれかになります。 → 9.15(x) → 9.14(x) → 9.12(x) → 9.8(x)
9.3(x)	—	次のいずれかになります。 → 9.15(x) → 9.14(x) → 9.12(x) → 9.8(x)
9.2(x)	—	次のいずれかになります。 → 9.15(x) → 9.14(x) → 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。 → 9.14(x) → **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。 → 9.14(x) → **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
9.0(2)、9.0(3)、または 9.0(4)	—	次のいずれかになります。 → 9.14(x) → **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。 → 9.14(x) → **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。 → 9.14(x) → **9.12(x)** → 9.8(x) → 9.1(7.4)
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)

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
8.3(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、『ASA アップグレード ガイド』を参照してください。

未解決のバグおよび解決されたバグ

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 9.15(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。

不具合 ID 番号	説明
CSCvg69380	ASA：まれに発生した CP 処理での破損によってコンソールロックが発生する
CSCvp69936	ASA：tcp_intercept スレッド名 thread detection でのトレースバック

不具合 ID 番号	説明
CSCvq29993	SSL ポリシーにより 6.4.0-102 2140 で 1550 ブロックと 9472 ブロックが枯渇し、回復しない
CSCvq33761	「no threat-detection statistics tcp-intercept」コマンド実行時の ASA トレースバック
CSCvq36879	DATAPATH での ASA/Lina のトレースバック
CSCvr29769	ASA で EEM を使用すると、リソースが枯渇したときに HA ペアがリロードされることがある
CSCvs84542	スレッド idfw_proc での ASA のトレースバック
CSCvu50049	ASA：アクティブ ASA に設定ファイルをコピーすると、スタンバイ ASA に特定の設定を複製しない
CSCvu71568	2100：着信パケットが「no buffer」によりドロップされ、発信パケットがブロックを枯渇させる
CSCvu73496	Internal1/1 データインターフェイスが、理由やログなしでダウンする。
CSCvu76937	snort CPU が 40% 未満の間に snort-busy カウンタが増加する
CSCvv17509	ASA：DRBG の正常性チェックの失敗による予期しないトレースバックとリロード
CSCvv19521	モニタールールを追加すると、RAVPN と sysopt connection permit-vpn を使用した FTD が動作を停止する
CSCvv30172	リブート後に ADI が断続的に KCD に参加できなくなる
CSCvv30476	clear crypto ipsec sa inactive コマンドでアウトバウンド SA が削除されない
CSCvv32160	フェールオーバー：スタンバイリストがアクセスリストの変更中にクラッシュし、CPU 使用率が高くなる
CSCvv34851	6.7.0-1992：FMC 接続イベントページに SSL 情報が入力されない
CSCvv38481	マルチコンテキストモードでプライマリとセカンダリの ASA ユニット間でのコンテキストの順序付けが適切でない
CSCvv43190	GREヘッダープロトコルフィールドが内部IPヘッダーのプロトコルフィールドと一致しない場合の暗号エンジンエラー
CSCvv50265	DAP：クライアント証明書情報が DAP に渡されない
CSCvv51232	9.14.1.15 でプラットフォームからアプライアンスモードに変更した後、FP 2100 で SNMP トラップが生成されない

不具合 ID 番号	説明
CSCvv65648	ISA-3000 ハードウェアバイパスの動作が write erase 後も変更されない
CSCvv69392	ASA/FTD がスレッド名「IKE Daemon」でトレースバックし、リロードすることがある
CSCvv70984	ブックマーク SSL 暗号設定の変更中の ASA トレースバック
CSCvv71435	ASA 256 ブロックと 1550 ブロックの枯渇により DMA メモリの割り当てが開放されない
CSCvv72466	ASA のアップグレード後、startup-config で OSPF ネットワークコマンドが欠落する
CSCvv73786	IPv6 はサポートされていないため、ASA はフォールバック方式として OCSP に IPv4 を使用する必要があります。
CSCvv76249	ASA が終了した S2S 接続に関連付けられた接続を閉じない
CSCvv78039	静的ルートがスタンバイルートに複製されない
CSCvv82254	crypto_pki traceback で FPR-2110 がトレースバックする
CSCvv82389	それ以上のパケットがない接続の EOF 後に SOF が表示される
CSCvv85029	スレッド名 ace_work で ASA5555 がトレースバックし、リロードする
CSCvv86718	「Address not mapped」、「periodic_handler_internal」で ASA がトレースバックする
CSCvv87232	ASA：igb_saleen_io_sfp_mod_poll_thread プロセスで CPU 専有の値が高くなる
CSCvv88523	アクティブセッションのカウンタが特定の値に達したときに SSL VPN 接続を確立できない
CSCvv94701	ASA が「octnic_hm_thread」でリロードし続け、リロード後は回復するまでに非常に長い時間がかかる
CSCvv95805	ASA5516 9.12.3 がクラッシュし、アクティブユニットに対して再起動する（Octeon クラッシュ）
CSCvv97877	セカンダリユニットがクラスタに参加できない
CSCvv99256	制御ポイントの CPU 使用率が高くなっている大規模なオブジェクトグループの設定により設定の同期が失敗する可能性がある
CSCvw00161	Firepower 2140 での VPN ス レッドによる ASA のトレースバックとリロード

不具合 ID 番号	説明
CSCvw00516	インラインセットを使用すると、Q-in-Q フレーム内のフラグメントが LINA によってドロップされる
CSCvw03373	メモリの破損が原因で、ASA がトレースバックとリロードを頻繁に実行している
CSCvw03628	RFC822Name が空に設定された名前制約により、ASA が CA 証明書をインポートしない
CSCvw06298	コンテキストの共有インターフェイスでの MAC アドレスの重複
CSCvw07407	FTD/HA：「no shutdown」コマンドがスタンバイの実行コンフィギュレーションに表示されない
CSCvw07687	appAgent_hb_receiver_thread での FTD トレースバック
CSCvw08643	AnyConnect IKEv2 セッションで古い VPN コンテキストが表示される
CSCvw08722	9.12(4) へのアップグレード後に AnyConnect のクライアント間通信（Cisco IP 電話のコール）がブロックされる
CSCvw09521	NTP スレッドでトリガーされたウォッチドッグでの ASA のトレースバックとリロード
CSCvw09790	バージョン9.12(3)9 でのスレッド名 Pthread での ASAv のトレースバックとリロード
CSCvw12040	証明書チェーンの検証に失敗したため、ヒープキャッシュメモリが急激に枯渇している
CSCvw14711	IKEv1 フェーズ 2 が暗号 ACL の deny ステートメントを誤ってヒットする
CSCvw16165	ポートチャネルのメンバーがダウンすると、FPR1k ASA がトラフィックの通過を停止する
CSCvw16619	オフロードされた UDP トラフィックが ECMP セットアップでセカンダリルートにフェールオーバーされない
CSCvw16723	クライアントレス VPN のブックマークを使用する場合の Chrome ポップアップでのリダイレクト失敗
CSCvw16858	ASA のメモリ使用率が 100％ のままになる
CSCvw16924	WebVPN：WebVPN ポータルを開けない
CSCvw18086	「Crypto CA」プロセスによる ASA の長時間にわたる CPU 占有
CSCvw18614	LINA プロセスでの ASA トレースバック

不具合 ID 番号	説明
CSCvw19324	IKE デーモンで FP2100 トレースバックが確認される
CSCvw19490	OSPF データベースに RIB の変更が反映されない
CSCvw19686	ASA 5508 でジャンボフレームを有効にすると、DMA メモリ不足の問題が発生する
CSCvw21386	SNMP 機能での ASA のトレースバックとリロード
CSCvw23199	スレッド名 Logger での ASA/FTD のトレースバックとリロード
CSCvw23246	vpn_putuauth：ERR：外部のインターフェイスでの ip x.x.x.x ユーザー xxxxx の uxlate コリジョン
CSCvw24556	フローオフロードが有効になっている場合、FTP ファイル転送（ビッグファイル）が正しく閉じない
CSCvw26171	スレッド名 DATAPATH での ASA のトレースバック
CSCvw26331	スレッド名 ci/console での ASA のトレースバックとリロード
CSCvw27301	EAP を使用した IKEv2 で、MOBIKE ステータスが処理されない
CSCvw28296	H323 インスペクションが、FacilityOpenLocgicalChannel パケットに埋め込まれたメディアサーバー IP のネットワークアドレス変換を実行しない
CSCvw28995	Google Chrome からのみ、WebVPN 経由で SAP ポータルハイパーリンクにアクセスできない
CSCvw33057	ASA WM 1010：FXOS_PARSER_ERROR：cURL がエラーコード 401 invalid ID で返される

バージョン 9.15(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。

不具合 ID 番号	説明
CSCvq98396	ASA：暗号化セッションがスタンバイユニットでリークを処理する
CSCvr77005	インターフェイスが使用可能になると、トラフィックが暗号マップからプライマリインターフェイスにフォールバックしない
CSCvt48260	スタンバイユニットがアクティブユニットを検出すると、fover_parse でトレースバックしてブートループする
CSCvt92077	ASAv での ping の失敗：9.13（CAT9k の再起動後）

不具合 ID 番号	説明
CSCvt97205	ASA 9.14.1 上で SNMPPOLL/SNMPTRAP からリモートエンド（サイト間 VPN）ASA インターフェイスが失敗する
CSCvu33992	トレースバック：ASA が lina_sigcrash+1394 をリロードした
CSCvu89110	ASA：「logging permit-hostdown」が設定され、TCP syslog がダウンしている場合も新しい接続をブロクする
CSCvv10778	9.12.4 へのアップグレード後のスレッド名 DATAPATH（5585）または Lina（2100）のトレースバック
CSCvv25394	アップグレード後、ASA がディスクの名前を交換して disk0 が disk1になり、disk1 が disk0 になった
CSCvv31755	更新の失敗により、アプリケーションとシャーシ間でインターフェイスのステータスが一致しないことがある
CSCvv32333	ASA は現在もマルチモードでの SNMP を介した internal-data0/0 カウンタのポーリングを許可しない
CSCvv37629	不正な SIP パケットにより SIP 接続タイムアウトまで 4k ブロックのホールドアップが発生し、トラフィックの問題を引き起こす可能性がある
CSCvv41453	管理専用ルートテーブルからスタティック IPv6 ルートを削除すると、データトラフィックに影響する
CSCvv49698	ASA Anyconnect url-redirect が IPv6 で機能しない
CSCvv50338	snpi_nat_xlate_destroy+2508 でのトレースバック クラスタ ユニット
CSCvv52591	ctm_hw_malloc_from_pool で DMA メモリリークが発生し、管理接続と VPN 接続が失敗する
CSCvv53696	Anyconnect ユーザーの AAA または CoA タスク中の ASA/FTD トレースバックおよびリロード
CSCvv58332	ASA/FTD が BGP MP_REACH_NLRI 属性のネクストホップバイトを逆順で読み取る
CSCvv62305	フェールオーバーペアに参加しようとした場合の fover_parse での ASA トレースバックとリロード
CSCvv63412	tmatch のコンパイルが進行中のとき、ASA がすべてのトラフィックを理由「No route to host」でドロップする
CSCvv64068	ネットワーク/サービスオブジェクト名の変更後、syslog の ACL のハッシュ値で不一致が発生する

不具合 ID 番号	説明
CSCvv66920	内部フロー：U ターン GRE フローが不正な接続フローの作成をトリガーする
CSCvv69991	FTD が 6.6.1 へのアップグレード後にメンテナンスモードでスタックする
CSCvv87496	「VPN packet redirect on peer」による ASA クラスタメンバー 2048 ブロックの枯渇
CSCvv89355	フェールオーバー後に DHCP プロキシ更新タイマーが起動しない

エンドユーザーライセンス契約書

エンドユーザーライセンス契約書の詳細については、http://www.cisco.com/jp/go/warranty 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。

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。