Cisco ASA シリーズ 9.9(x) リリースノート

Cisco ASA シリーズ 9.9(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 9.9(x) のリリース情報が記載されています。

特記事項

- ASA 5506-X、5508-X、および 5516-X の ROMMON のバージョン 1.1.15 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**。

- AnyConnect 4.4 または 4.5 で SAML 認証を使用しており、ASA バージョン 9.7.1.24、9.8.2.28、または 9.9.2.1（リリース日：2018 年 4 月 18 日）を展開している場合、SAML のデフォルト動作は、AnyConnect 4.4 および 4.5 でサポートされていない組み込みブラウザになります。したがって、AnyConnect 4.4 および 4.5 クライアントが外部（ネイティブ）ブラウザを使用して、SAML で認証するには、トンネル グループ設定で **saml external-browser** コマンドを使用する必要があります。

  （注） **saml external-browser** コマンドは、AnyConnect 4.6 以降にアップグレードするクライアントの移行のために使用されます。セキュリティ上の制限のため、AnyConnect ソフトウェアをアップグレードする際の一時的な移行の一環としてのみこのソリューションを使用してください。今後、このコマンド自体がサポートされなくなります。

- 9.9(2) での大規模な構成における ASA 5506-X のメモリの問題：9.9(2) にアップグレードする場合、大規模な構成の一部がメモリ不足のため拒否され、「エラーが発生しました：ルールをインストールするためのメモリが不足しています（ERROR: Insufficient memory to

install the rules）」のメッセージが表示される場合があります。これを回避する方法の 1 つに、**object-group-search access-control** コマンドを入力して、ACL のメモリ使用量を改善する方法があります。ただし、パフォーマンスに影響する可能性があります。または、9.9(1) にダウングレードすることができます。

- ASA 5506-X、5508-X、および 5516-X 向けの新しい ROMMON バージョン 1.1.12：重要な修正が複数あるため、ROMMON をアップグレードすることを推奨します。https://www.cisco.com/go/asa-firepower-sw を参照し、ご使用のモデル > [ASA Rommon ソフトウェア（ASA Rommon Software）] > [1.1.12] を選択します。詳細については、[ソフトウェアダウンロード（Software Download）] ページの「リリースノート」を参照してください。ROMMON をアップグレードするには、「Upgrade the ROMMON Image (ASA 5506-X, 5508-X, and 5516-X）」を参照してください。Firepower Threat Defense を実行している ASA では、この ROMMON バージョンへのアップグレードはまだサポートされいません。ただし、ASA で正常にアップグレードしてから、Firepower Threat Defense に再イメージ化することができます。

- ASA 9.x で使用する RSA ツールキットのバージョンは、ASA 8.4 で使用されたバージョンとは異なるため、これらの 2 つのバージョン間で PKI の動作に違いが生じます。

  たとえば、9.x ソフトウェアを実行している ASA では、フィールド長が 73 文字までの [Organizational Name Value]（OU）フィールドをもつ証明書のインポートが許可されます。8.4 ソフトウェアを実行している ASA では、60 文字までの OU フィールド名をもつ証明書のインポートが許可されます。この相違のため、ASA 9.x でインポートできる証明書を ASA 8.4 ではインポートできません。ASA 9.x 証明書をバージョン 8.4 を実行している ASA にインポートしようとすると、エラー「ERROR: Import PKCS12 operation failed.」が表示されます。

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 9.9(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 ASAv サポート	ASAv 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 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。
VMXNET3 インターフェイス用の ASAv サポート	ASAv 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。
初回起動時の仮想シリアル コンソール用の ASAv サポート	ASAv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ASAv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定義ルートを更新する ASAv サポート	Azure 高可用性構成で ASAv を構成して、複数の Azure サブスクリプションでユーザ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**
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	AnyConnect 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 を構成することをサポートします。
RADIUS サーバへの IPv6 接続	ASA 9.9.2 では、外部 AAA RADIUS サーバへの 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**
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**

機能	説明
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** *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**
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 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	

機能	説明
SNMP IPv6 のサポート	ASA は、IPv6 経由での SNMP サーバとの通信、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。
単一ユーザ 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。

ASA 9.9(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。

機能	説明
VPN 機能	
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**
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 ASAv のアクティブ/バックアップの高可用性	アクティブな ASAv の障害が Microsoft Azure パブリック クラウドのバックアップ ASAv 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** **[Monitoring] > [Properties] > [Failover] > [Status]** **[Monitoring] > [Properties] > [Failover] > [History]** バージョン *9.8(1.200)* でも同様です。
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**
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**
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**

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**

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。

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

次の表で、お使いのバージョンのアップグレードパスを参照してください。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） 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
9.8(x)	—	次のいずれかになります。 → 9.9(x) → **9.8(x)**
9.3(x)	—	次のいずれかになります。 → 9.9(x)
9.2(x)	—	次のいずれかになります。 → 9.9(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。 → 9.9(x) → 9.1(7.4)
9.1(1)	→ 9.1(2)	次のいずれかになります。 → 9.9(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。 → 9.9(x) → 9.1(7.4)
9.0(1)	→ 9.0(4)	次のいずれかになります。 → 9.9(x) → 9.1(7.4)
8.6(1)	→ 9.0(4)	次のいずれかになります。 → 9.9(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。 → 9.9(x) → 9.1(7.4)
8.4(5+)	—	次のいずれかになります。 → 9.9(x) → 9.1(7.4) → 9.0(4)
8.4(1) ～ 8.4(4)	→ 9.0(4)	→ 9.9(x) → 9.1(7.4)
8.3(x)	→ 9.0(4)	次のいずれかになります。 → 9.9(x) → 9.1(7.4)
8.2(x) 以前	→ 9.0(4)	次のいずれかになります。 → 9.9(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 Upgrade Guide』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 9.9(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
CSCvg72879	9.9.1/SecGW：QP-HA w/ の 1 秒未満のフェールオーバーにより、10 ～ 20% のパケット損失が数分間発生する場合がある
CSCvi36891	SecGW：ASR 中に、VPN コンテキスト/ルールのないウィンドウがクラスタに存在する
CSCvp16482	ASDM の同時セッションを確立すると ASA がリロードされる

解決済みのバグ

このセクションでは、リリースごとに解決済みのバグを一覧表で示します。

バージョン 9.9(2) 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
CSCtk36754	webvpn ログインページの HTTP GET が多いと、UnicornProxyThread の CPU 使用率が高くなる
CSCvb99424	ASA IKEv2 RA VPN が「No License」ステータスを AnyConnect ユーザに明確には通知しない
CSCvc91266	RPF が最初に有効になる場合に ASA BFD echo 関数が失敗する
CSCvd08983	TACACS 認証と設定済みの「password-policy lifetime」を使用した ASA がアクセスを拒否する
CSCvd97780	ASA/FTD がパケット キャプチャの「trace」出力に誤った結果を表示する
CSCve02467	ENH：igp stale-route の低いほうのタイムアウト値を 10 秒未満の値に下げる必要がある
CSCve76799	ENH：KVM AHV Nutanix にインストールされると ASAv がブート アップできない
CSCve79555	キャプチャをクリアするときの ASA/FTD のトレースバック（assertion "0" failed: "mps_hash_table_debug.c" ファイル）

問題 ID 番号	説明
CSCvf26463	ルーテッド モードの ASA 9.8.1 BVI が ASA から生成されたトラフィックに対するルート ルックアップを実行していない
CSCvf40650	証明書がスタンバイに同期しない/すべての証明書がスタンバイの導入後障害でクリアされる
CSCvf68666	FP2100 IFT の顧客が PC へのイメージのダウンロードに ASDM を使用できない
CSCvf75628	Hyper-V 上の ASAv が誤った「show interface」出力を表示する：半二重、10 Mbps
CSCvf92262	CSCvc82150 に対する修正にもかかわらず、ASA WebVPN HTTP の Strict-Transport-Security ヘッダーが欠落する
CSCvg01119	IPV4：ルーティングアップデートのバッファリングされた信頼性メカニズムの実装
CSCvg01827	永久ライセンスの予約ライセンスが ASAv にインストールされない
CSCvg06695	「Detect service module failure」により、Firepower 2100 Threat Defense ペアのレポートが失敗する
CSCvg29442	IPSec が有効になっていると、HA は 6.2.3 FMC および 6.2.1 KP で Active-Failed 状態になる
CSCvg58629	HTTP サーバと Anyconnect SSL VPN は、FTD の同じインターフェイス/ポートに共存できない
CSCvg90061	CSM がtcp-state-bypass ログの解析に失敗した
CSCvh56214	ASA および Putty：着信パケットが復号化時に文字化けした
CSCvh99159	ASDM の RADIUS 認証/許可が失敗する

バージョン 9.9(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
CSCth11758	集約認証のデバッグではパスワードをマスクする必要がある
CSCuj98977	「show service set conn detail」を実行したときのスレッド SSH での ASA のトレースバック
CSCvb53233	%ASA-1-199010 と %ASA-1-716528 の syslog メッセージによる ASA 9.1(7)9 のトレースバック

問題 ID 番号	説明
CSCvb97470	asa Rest-api：コンポーネントモニタリング：空の値/空白値
CSCvd67907	ASA SSL クライアントが再ネゴシエーション要求に応答しない
CSCve02467	ENH：igp stale-route の低いほうのタイムアウト値を 10 秒未満の値に下げる必要がある
CSCve72964	DATAPATH-1-2084 ASA 9.(8)1 でのトレースバック
CSCve73025	週末の VPN ロードテスト後に 1700 個の「4 バイトブロック」がすべて枯渇した
CSCve94886	NAT ルールの変更時とパケットキャプチャが有効になっているときの ASA with Firepower Services でトレースバックが発生する
CSCve97874	ASA：バージョン 9.6 以降での空き DMA メモリの不足
CSCvf10327	ENH：サブインターフェイスの作成時に一意の IPv6 リンクローカルアドレスが割り当てられる
CSCvf16310	AnyConnect クライアントに IPv6 アドレスが断続的に割り当てられる
CSCvf16808	アクティブユニットに SSH 接続できない//TCP 接続の上限を超えている
CSCvf17214	破損した PKCS12 として ASA が ECDSA をエクスポートする
CSCvf25666	空きメモリが不足している ASA で既存のクラスタの参加が失敗し、トレースバックとリロードが発生する可能性がある
CSCvf26463	ルーテッド モードの ASA 9.8.1 BVI が ASA から生成されたトラフィックに対するルート ルックアップを実行していない
CSCvf28292	DAP 設定は復元されるが、バックアップ復元後に非アクティブになる
CSCvf28749	mroute が設定されている場合に ASA が register stop を送信しない
CSCvf31539	DCD が有効になっている場合に ASA 接続がアイドル状態でスタックする
CSCvf34791	firepower - asa コアを搭載した ASA での 6.2.2 1290 sfr のインストール
CSCvf37947	カスタム ルーテッド コンテキストで ASA が BVi0 インターフェイスを作成する
CSCvf38655	バージョンアップ後の fover_parse での ASA トレースバック
CSCvf39679	既存の EIGRP 設定に新しいネットワークを追加できない
CSCvf40650	証明書がスタンバイに同期しない/すべての証明書がスタンバイの導入後障害でクリアされる

問題 ID 番号	説明
CSCvf43150	ASA// 9.6 // FTP インスペクションで、PAT を使用したアクティブ FTP 上のデータトラフィックに新しい NAT 全体を割り当てられない
CSCvf43650	NSF が有効な状態で ASA フェールオーバーが実行されると OSPF ルートがピアデバイスにインストールされない
CSCvf44142	ASA 9.x：DNS インスペクションによって PTR クエリに「0」が追加される
CSCvf44950	iOS および OS X IKEv2 のネイティブクライアントが EAP-TLS を使用して ASA に接続できない
CSCvf51066	FXOS 上の ASA が SNMP Ifspeed OID （1.3.6.1.2.1.2.2.1.5）応答値 = 0 を送信している
CSCvf54081	TLS バージョン 1.1 の接続に失敗し、t1_lib.c:3106 に共有署名アルゴリズムなし
CSCvf54981	ASA：80 バイトメモリブロックの枯渇
CSCvf56506	データパスでの ASA 9.6(2)、9.6(3) のトレースバック
CSCvf56917	ポートチャネルでのポートフラップ時に ASA が LACP PDU を送信しない
CSCvf57908	トランスペアレント ファイアウォール：誤った DSAP 値で Ethertype の ACL がインストールされる
CSCvf61419	NAT によるスレッド DATAPATH でのトレースバック
CSCvf63108	送信元 IP アドレスが 0.0.0.0 の IGMP レポートパケットを ASA がドロップする
CSCvf64643	エラー：キャプティブポータルポートが使用できない。もう一度やり直す必要がある
CSCvf72930	FTD が登録時にスレッド名 appAgent_monitor_nd_thread でトレースバックすることがある
CSCvf74218	AWS GovCloud の ASAv イメージが時間単位の課金モードで動作しない
CSCvf76281	IKEv2 RA 証明書認証。新しいセッションを割り当てることができない。最大セッション数に到達した
CSCvf79262	OpenSSL CVE-2017-3735「incorrect text display of the certificate」
CSCvf80539	リブート後に管理専用に復帰する
CSCvf81222	パケットが PBR に到達し、接続が確立されたときの 112 バイト bin でのメモリリーク

問題 ID 番号	説明
CSCvf81932	K7 ライセンスによる一部のインスペクションでの「Incomplete command」エラー
CSCvf83709	CCL リンク障害によってスレーブがキックアウトされた後に再参加してもマルチコンテキストモードで v3 ユーザが失われる
CSCvf85065	ASA：スレッド名 idfw_proc によるトレースバック
CSCvf87899	ASA：まれに発生したスケジューラの破損によってコンソールロックが発生する
CSCvf89504	NAT が含まれていると ASA クラスタが IP フラグメントを断続的にドロップする
CSCvf92262	CSCvc82150 に対する修正にもかかわらず、ASA WebVPN HTTP の Strict-Transport-Security ヘッダーが欠落する
CSCvf94973	ASDM を介して AnyConnect イメージをアップロードするときの FP 2100 での ASA のトレースバック
CSCvg01016	ASA が DCERPC インスペクションのピンホールを作成せず、debug dcerpc が「MEOW not found」と表示する。
CSCvg01132	ASA：9.2(4) から 9.2(4)18 へのアップグレード後にシリアル接続がハングする
CSCvg01827	永久ライセンスの予約ライセンスが ASAv にインストールされない
CSCvg05250	「clear local-host <IP>」がすべてのホスト/接続の ASA クラスタ全体に存在するすべてのスタブフローを削除する
CSCvg06695	「Detect service module failure」により FP2100 Threat Defense ペアがステータスのレポートに失敗する
CSCvg09778	DNS インスペクションにより CP 処理で ASA-SSP HA がリロードする
CSCvg17478	Show OSPF Database コマンドによるトレースバック
CSCvg20796	サイト間セキュリティ VPN トンネルを介して DNS サーバが到達可能な場合に ASA ローカル DNS 解決が失敗する
CSCvg21077	1 つのノードが再参加し、トラフィックが再起動されると、snpi_untranslate が原因でユニット 100% CPU が発生する
CSCvg23028	SSP 上の REST-API の残存
CSCvg25694	トレースバックのアサート、スレッド名：cli_xml_server

問題 ID 番号	説明
CSCvg25983	ASA サイト間クラスタリング：ASA がユニキャスト ARP 要求を受信すると追加分の ARP が生成されない
CSCvg29442	IPSec が有効になっていると、HA は 6.2.3 FMC および 6.2.1 KP で Active-Failed 状態になる
CSCvg33669	「OCTEON:DROQ[8] idx: 494 len:0」メッセージがデバイスのコンソールアクセス時に表示される
CSCvg55617	ASA 9.8.1+ IKEv2 VPN のロードバランシングが IKE_AUTH の後に DELETE を送信する

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 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。