Cisco ASA シリーズ 9.10(x) リリースノート

Cisco ASA シリーズ 9.10(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 9.10(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 コンフィギュレーション ガイド（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**。

- 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。

- これらの暗号は、Firepower 2100（KP）プラットフォーム用の FIPS モードの DTLS 1.2 では現在サポートされていません。
  - DHE-RSA-AES256-SHA
  - AES256-SHA
  - DHE-RSA-AES128-SHA
  - AES128-SHA

- 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 9.10(1) 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。

- 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 9.10(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	
Azure 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 ASAv 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 ASAv	ASAv は Azure 中国市場で入手できます。
DPDK の ASAv 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 ASAv 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	

機能	説明
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**
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 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 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**
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 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 人のユーザがログアウトすると、その IP アドレスのすべてのユーザ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** *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** *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。
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 に 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**

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（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** *9.8(3)* でも同様。
AnyConnect 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、AnyConnect リモート アクセス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**
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。FXOS にクラスタを展開する際にネットワークを設定できるようになりました。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**
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**

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。
Microsoft Azure Government クラウドでの 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** **[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	
Firepower 2100 の NTP 認証のサポート	FXOS で SHA1 NTP サーバ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

機能	説明
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**
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**
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**
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**

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。

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
9.9(x)	—	次のいずれかになります。 → **9.10(x)** → **9.9(x)**
9.8(x)	—	次のいずれかになります。 → **9.10(x)** → **9.9(x)** → **9.8(x)**
9.7(x)	—	次のいずれかになります。 → **9.10(x)** → **9.9(x)** → **9.8(x)** → 9.7(x)
9.6(x)	—	次のいずれかになります。 → **9.10(x)** → **9.9(x)** → **9.8(x)** → 9.7(x) → 9.6(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
9.5(x)	—	次のいずれかになります。 → **9.10(x)** → **9.9(x)** → **9.8(x)** → 9.7(x) → 9.6(x) → 9.5(x)
9.4(x)	—	次のいずれかになります。 → **9.10(x)** → **9.9(x)** → **9.8(x)** → 9.7(x) → 9.6(x) → 9.5(x) → 9.4(x)
9.3(x)	—	次のいずれかになります。 → **9.10(x)** → **9.9(x)** → **9.8(x)** → 9.7(x) → 9.6(x) → 9.5(x) → 9.4(x) → 9.3(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
9.2(x)	—	次のいずれかになります。 → **9.10(x)** → **9.9(x)** → **9.8(x)** → 9.7(x) → 9.6(x) → 9.5(x) → 9.4(x) → 9.3(x) → 9.2(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。 → **9.10(x)** → **9.9(x)** → **9.8(x)** → 9.7(x) → 9.6(x) → 9.5(x) → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3)、9.1(4)、9.1(5)、9.1(6)、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
9.1(1)	→ 9.1(2)	次のいずれかになります。 → **9.10(x)** → **9.9(x)** → **9.8(x)** → 9.7(x) → 9.6(x) → 9.5(x) → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3)、9.1(4)、9.1(5)、9.1(6)、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。 → **9.10(x)** → **9.9(x)** → **9.8(x)** → 9.7(x) → 9.6(x) → 9.5(x) → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3)、9.1(4)、9.1(5)、9.1(6)、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(1)	→ 9.0(2)、9.0(3) または 9.0(4)	次のいずれかになります。 → **9.10(x)** → **9.9(x)** → **9.8(x)** → 9.7(x) → 9.6(x) → 9.5(x) → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3)、9.1(4)、9.1(5)、9.1(6)、9.1(7.4)
8.6(1)	→ 9.0(2)、9.0(3) または 9.0(4)	次のいずれかになります。 → **9.10(x)** → **9.9(x)** → **9.8(x)** → 9.7(x) → 9.6(x) → 9.5(x) → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3)、9.1(4)、9.1(5)、9.1(6)、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(2)、9.0(3) または 9.0(4)	次のいずれかになります。 → **9.10(x)** → **9.9(x)** → **9.8(x)** → 9.7(x) → 9.6(x) → 9.5(x) → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3)、9.1(4)、9.1(5)、9.1(6)、9.1(7.4)
8.4(5+)	—	次のいずれかになります。 → **9.10(x)** → **9.9(x)** → **9.8(x)** → 9.7(x) → 9.6(x) → 9.5(x) → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3)、9.1(4)、9.1(5)、9.1(6)、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
8.4(1) ～ 8.4(4)	次のいずれかになります。 → 9.0(2)、9.0(3) または 9.0(4) → 8.4(6)	→ **9.10(x)** → **9.9(x)** → **9.8(x)** → 9.7(x) → 9.6(x) → 9.5(x) → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3)、9.1(4)、9.1(5)、9.1(6)、9.1(7.4)
8.3(x)	→ 8.4(6)	次のいずれかになります。 → **9.10(x)** → **9.9(x)** → **9.8(x)** → 9.7(x) → 9.6(x) → 9.5(x) → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3)、9.1(4)、9.1(5)、9.1(6)、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
8.2(x) 以前	→ 8.4(6)	次のいずれかになります。 → **9.10(x)** → **9.9(x)** → **9.8(x)** → 9.7(x) → 9.6(x) → 9.5(x) → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3)、9.1(4)、9.1(5)、9.1(6)、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 Cisco バグ追跡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 Help & FAQ を参照してください。

バージョン 9.10(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。

警告 ID 番号	説明
CSCuz92333	ASA では、RouterDeadInterval sec - NSF Cisco よりも長い RS ビットを設定してはならない
CSCva36446	SSL ハンドシェイクの成功直後に ASA が Anyconnect セッションの受け入れを停止するか、または接続を終了する
CSCvb37736	ブレードのフォーマット設定で「Format Failure」になる
CSCvd64182	接続されたスイッチポートがシャットダウンされても、管理インターフェイスが表示される
CSCvg40735	GTP インスペクションが CPU 使用率をスパイクさせることがある
CSCvg69028	実行中の「show access-list」のスレッド名 idfw_proc での ASA トレースバック
CSCvg74549	オブジェクトグループ（display_hole_og）を使用してアクセスリストを保存/表示しようとするとトレースバックする
CSCvg91150	アサート「0」の ASA トレースバックが失敗した：ファイル「timer_services.c」
CSCvh13868	プライオリティキューイングが ASA5516 プラットフォームで正しく機能しない
CSCvh13869	ASA IKEv2 が aaa セッションを開けない：「セッション数の上限 [2048] に達しました（session limit [2048] reached）」
CSCvi12735	アクセスリスト設定を削除するときのトレースバックとリロード
CSCvi71622	スタンバイ FTD の DATAPATH でのトレースバック
CSCvj00363	パケットトレーサとキャプチャの組み合わせで ASA がトレースバックとリロードを起こすことがある
CSCvj40282	syslog 通知時のスレッド icmp_thread のトレースバック
CSCvj84062	QoS ポリシングによってトラフィックが予期どおりに制限されない
CSCvj88461	集約プレフィックスをフラッディングする前に特定のプレフィックスの回収アドバタイズメントがフラッディングされる
CSCvk12607	FPR4110：「crypto engine accelerator-bias ipsec」が有効になっている場合、キー再生成時に ASA が VPN トラフィックをドロップする
CSCvk13703	FlowControl が有効な場合に ASA5585 がプライオリティ RX リングを使用しない
CSCvk18330	アクティブな FTP データ転送が FTP インスペクションと NAT で失敗する

警告 ID 番号	説明
CSCvk22322	アクティブユニット（cachefs_umount を含む）から設定を同期する際の ASA トレースバック（ウォッチドッグタイムアウト）
CSCvk29263	設定セッション内で変更をコミットした後に SSH セッションがスタックする
CSCvk34142	フラッシュラップにロギングする場合の 2100 FTD でのウォッチドッグ
CSCvk47577	ASA では、malloc バッファの問題により、チェックヒープでトレースバックが発生することがある
CSCvk51181	インターフェイスの編集と展開後に FTD IPV6 トラフィックが停止する：パート 1/2
CSCvk64990	ASA：Cisco Secure Desktop ホストでのスキャナバイパス
CSCvk65105	ユーザが Anyconnect から切断された場合でも IP ローカルプールから IP がスタックされる
CSCvk69317	暗号部分での設定の生成により設定変更せずに変更される
CSCvk69762	スレッド名 appAgent_monitor_nd_thread での Lina のトレースバック
CSCvk70301	VTI IKEv1：responder-only がキー再生成時にトンネルを切断する
CSCvk72958	インターフェイスに適用されている QoS が機能しない
CSCvm00066	ASA が「フラッシュからの読み取り中」に数時間にわたってスタックする
CSCvm00480	ASA5585-SSP-10 のコアでの CPU スパイク
CSCvm08769	アクティブ ユニットの IP を使用してスタンバイ ユニットが BFD パケットを送信すると BGP のネイバーシップが障害を起こす
CSCvm10086	「sw-module module ips reload」の発行時の ASA のトレースバックとリロード
CSCvm11643	ASA ログで生成されたハッシュ値の不整合
CSCvm25582	ASA で長いセッションのトラフィックの暗号化が停止する
CSCvm36320	不正な ACL の一致
CSCvm36461	ASA トレースバックスレッド名：CMGR Server Processand after upgrade FiePOWER module
CSCvm40288	HA リンクでのポートチャネルの問題

警告 ID 番号	説明
CSCvm49260	誤ったインターフェイスを使用して ASA が syslog トラフィックを送信している
CSCvm50421	ACE での OSPF と IPv6 の併用によるクラスタ参加時のクラスタスレーブノードで ASA のトレースバックが発生する
CSCvm53545	crashinfo ファイルを生成せずに ASA がトレースバックしリロードすることがある
CSCvm63062	ASA が HTTP のダイレクト認証ポートのリスニングを停止する
CSCvm67174	広範なグループポリシーの設定のプッシュ時に ASA の REST-API がサーバエラーで失敗する
CSCvm67783	VTI と併用すると、BGP が 180 秒で切断される
CSCvm70296	FTD 6.2.3.5 Lina プロセスでの警告トレースバックで HA が損失し、停止する
CSCvm70848	ASA：「Failed to create session mgmt entry for SPI <>」により、IPSec SA のインストールが失敗する
CSCvm71014	アクセスリストの欠落/拡張の問題により停止する
CSCvm72541	クラスタ内での新しいマスターの選択後に、接続されたルートが配信されない
CSCvm80779	ASA が H323 H225 を検査しない
CSCvm82290	IRB 設定でホストが到達不能な場合に ASA コア ブロックが枯渇する
CSCvm82993	9.10.0.6 から 9.10.0.8 への ASA のアップグレード中にブレードでアップグレードが失敗した
CSCvm86163	ASA ラウンドロビン PAT IP のステッキ性が機能しない
CSCvm86443	イベントマネージャの出力でトレースルートの1行目のみがキャプチャされる
CSCvm88306	10GE インターフェイスドライバ（ixgbe）に関連する ASA5585 の DATAPATH のトレースバック
CSCvm91014	BVI IF を NTP 送信元インターフェイスとして設定すると NTP 同期が機能しない
CSCvm93860	REST-API の大規模なデータ転送がデバイスとの間で失敗している
CSCvm93972	CP 処理スレッド（スレッドでの長時間にわたる CPU ホグを伴う）を使用する ASA5515-X でのトレースバック

警告 ID 番号	説明
CSCvm95669	ASA 5506 における http://x.x.x.x/asasfr-5500x-boot-6.2.3-4.img コピー中のエラー（デバイスにスペースが残っていない）
CSCvm96400	ASA/IKEv2-L2L：同じプロキシ ID を持つ 2 つの IPsec トンネルが許可されない
CSCvm96779	暗号化されたフェールオーバーリンクを使用した FTD HA で 1550 ブロックのブロック枯渇が確認される
CSCvm97185	スレッド名 DATAPATH-19-14446 の FTD がクラッシュし、フェールオーバーが発生する
CSCvm98344	フェールオーバー発生後、ASA が新しい IP ではなく古い MAC を使用して既存の管理接続を閉じる

バージョン 9.10(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。

警告 ID 番号	説明
CSCup37416	古い VPN コンテキストエントリにより ASA がトラフィックの暗号化を停止する
CSCuv68725	ASA が「log disable」オプションを使用して ACE を削除できない
CSCux69220	DHCP での WebVPN 「enable intf」、ASA ブート時の CLI の欠落
CSCvb29688	CSCup37416 に対する修正にもかかわらず、古い VPN コンテキスト エントリにより ASA がトラフィックの暗号化を停止する
CSCvc62565	スタンバイとの同期時にフェールオーバー crypto IPsec IKEv2 設定が一致しない
CSCvd13180	AVT：ASA 9.5.2 の Content-Security-Policy ヘッダーの欠落
CSCvd13182	AVT：ASA 9.5.2 での X-Content-Type-Options の欠落
CSCvd28906	十分な LCMB メモリを割り当てることができないため、5506 での最初のブート時に ASA がトレースバックする
CSCvd44525	ASA「show tech」の一部のコマンドが 2 回実行され、running-config/ak47 detailed/startup-config エラーが表示される
CSCvd76939	ASA ポリシーマップ設定がクラスタのスレーブに複製されない
CSCve53415	キャプチャ実行中に DATAPATH スレッドで ASA がトレースバックする

警告 ID 番号	説明
CSCve85565	syslog が VPN トンネルを介して送信されるとトレースバックする
CSCve94917	CSCvb29688 に対する修正にもかかわらず、9.1 コードで古い VPN コンテキストに関する問題が確認された
CSCve95403	FIPS ブート テスト後に送信されたログが原因で ASA がブートループする
CSCvf18160	WebVPNと共有 storage-url config でのフェールオーバー同期時の ASA のトレースバック
CSCvf39539	送受信したバイト数と IP アドレス スイッチに NetFlow が大きな値を返す
CSCvf40179	エラー：暗号マップを作成できない：エントリを追加するときに上限に到達する
CSCvf82832	ASA：962 へのアップグレード後の ICMPv6 syslog メッセージ
CSCvf85831	イメージのアップロード中に ASDM がエラーを表示する
CSCvf96773	PAT プールの範囲が非常に大きいことによるスタンバイ ASA の 高い CPU 使用率
CSCvg05442	DATAPATH プロセスと WebVPN プロセス間でのデッドロックによる ASA のトレースバック
CSCvg36254	FTD 診断インターフェイスが br1 管理サブネットの ARP をプロキシする
CSCvg43389	1550 ブロックの枯渇による ASA のトレースバック
CSCvg58133	ASA のホスト名が「ASAv」の場合、スマートライセンスが機能しない
CSCvg65072	Cisco ASA SW、FTD SW、および AnyConnect セキュア モビリティ クライアント SAML 認証のセッション固定攻撃に対する脆弱性
CSCvg76652	ポートチャネルのサブ インターフェイス不一致のデフォルト DLY 値
CSCvg90365	トランスペアレント ASA で IPv6 アドレスにより ICMP/Telnet トラフィックが失敗する
CSCvh05081	ASA モジュールによって生成される SACK パケットの SLE 値と SRE 値を ASA が非ランダム化しない
CSCvh14743	NAT 検出ペイロードを使用した DPD により Strongswan/サードパーティ製クライアントとの IKEv2 MOBIKE セッションが失敗する
CSCvh30261	コンテキスト変更/設定の同期時に ASA のウォッチドッグがトレースバックする

警告 ID 番号	説明
CSCvh46202	VPN 経由のフラグメント化されたトラフィックにより 2048 バイト ブロックのリークが遅くなる
CSCvh47057	ASA：インスペクションが有効になっているときにゾーン内に設定されたインターフェイスで ICMP フローが「no-adjacency」によりドロップする
CSCvh53276	L2FW を通過する IPv6 プロトコルの 112 個のパケットが無効な IP 長メッセージでドロップされている
CSCvh53616	SSL により Firepower Threat Defense デバイス上の ASA がトレースバックする
CSCvh55035	Firepower Threat Defense デバイスが Nexus 9000 を使用して ERSPAN を確立できない
CSCvh55340	REST API の完全バックアップを介して設定を実行している ASA に指定されたコンテキスト設定が含まれていない
CSCvh62705	Firepower 2110 ASA：コンテキスト全体の共有管理が GW に到達できない
CSCvh70603	フェールオーバー スタンバイ ユニットのライセンスステータスが [無効（Invalid）] から [スタンバイ状態では適用できません（Not Applicable in Standby State）] に変化する
CSCvh71738	アクセスグループ設定の削除後に FQDN オブジェクトが解決される
CSCvh75060	REST-API が特定のクエリに対して空の応答を返す
CSCvh77671	ASAv：spin_lock のパニックによる DATAPATH スレッドでのトレースバック
CSCvh79732	Cisco 適応型セキュリティ アプライアンスにおけるサービス拒否攻撃に対する脆弱性
CSCvh81737	Cisco 適応型セキュリティ アプライアンスにおけるサービス拒否攻撃に対する脆弱性
CSCvh81870	Cisco 適応型セキュリティ アプライアンスにおけるサービス拒否攻撃に対する脆弱性
CSCvh83849	デュアル ISP とバックアップ IPSEC トンネルを使用した DHCP リレーによりフラップが発生する
CSCvh91053	DHCP 送信中の ASA が DHCP を介して AC クライアントへのアドレスの割り当てを拒否するか、または割り当てない
CSCvh91399	ASA5500 シリーズのファイアウォールのアップグレードによりブートループが発生する（ROMMON を通過できない）

警告 ID 番号	説明
CSCvh92381	9.6.3.1 上で ASA がトレースバックし、ブート ループの状態になる
CSCvh95302	IPv6 アドレスがインターフェイスに設定されている場合、ASDM/WebVPN がリロード後に動作を停止する
CSCvh95960	capture コマンドで「match」キーワードを使用すると、キャプチャで IPv6 トラフィックが無視される
CSCvh97782	ベンダーのべき剰余の実装内で KP が不正なメモリ アクセスをトレースバックする
CSCvh98781	ASA/FTD 導入エラー「Management interface is not allowed as Data is in use by this instance」
CSCvi01312	WebVPN：Confluence アプリケーションと Jira アプリケーションでの複数のレンダリングの問題
CSCvi01376	デフォルト以外の SSL コマンドがリブート時に Firepower 4100 から削除される
CSCvi03103	BGP ASN によってポリシーの展開が失敗する
CSCvi07636	ASA：スレッド名 UserFromCert でのトレースバック
CSCvi07974	FTD：snort プロセスの再起動時にレイヤ 2 プロトコルパケット（例：BPDUs）がドロップされる
CSCvi08450	ASA での CWS リダイレクションが特定の状況で SSL Client Hello の再送信を適切に処理しない
CSCvi16264	DATAPATH がコンパイル中の ACL 構造体にアクセスするとウォッチドッグのタイムアウトにより ASA がトレースバックし、リロードする
CSCvi19125	「np-sp-invalid-spi」という ASP によってマルチキャスト ip-proto-50（ESP）がドロップされる
CSCvi19220	IPv6 から IPv4 への NAT 変換の実行後に ASA が暗号化に失敗する
CSCvi19263	ASA：VPN コンテキストのスピンロック解放中にトレースバックする
CSCvi22507	IKEv1 RRI：応答専用のリバース ルートがフェーズ 1 のキー再生成中に削除される
CSCvi31540	ペイロード暗号化なし（NPE）の ASA での「show tech」を使用したトレースバックとリロード
CSCvi33962	WebVPN リライター：BMC Remedy でドロップダウン メニューが機能しない

警告 ID 番号	説明
CSCvi34164	ASA が TCP/UDP syslog に 104001 メッセージおよび 104002 メッセージを送信しない
CSCvi35805	ASA カットスルー プロキシでユーザは Web サイトにアクセスできるが「authentication failed」が表示される
CSCvi37644	PKI：ASA が「Add CA req to pool failed. Pool full.」というエラーで CRL の処理に失敗する
CSCvi38151	ASA ペア：IPv6 スタティック/接続済みルートがアクティブ/スタンバイ ペア間で同期/複製されない
CSCvi42008	stuck uauth エントリが AnyConnect ユーザ接続を拒否する
CSCvi42965	ASA が「show memory」出力の下に正確な空きメモリを報告しない
CSCvi44246	ポートチャネルのサブインターフェイスでは、Threat Defense ペアの両方のユニットで同じ MAC アドレスが共有される
CSCvi44713	「show memory binsize」および「show memory top-usage」では正しい情報が表示されず、すべて PC 0x0 を表示する
CSCvi45567	snmpv1&2c ホスト グループが設定されていると snmpwalk を実行できない
CSCvi45807	ASA：リブート後に DNS expire-entry-timer 設定が表示されなくなる
CSCvi46759	ホップ制限 0 でのパケットの処理を ASA に許可する（RFC 8200 に準拠）
CSCvi48170	SNMP により低速メモリリークが発生する
CSCvi49383	Azure：クラウド ハイ アベイラビリティを実行している ASAv がウォッチドッグ クラッシュ ループになる
CSCvi51515	REST-API:500 内部サーバ エラー
CSCvi53708	CLI と REST-API の間の ASA NAT の位置の不一致が原因で REST が誤った設定を削除する
CSCvi55070	IKEv1 RRI：発信専用のリバース ルートがフェーズ 1 のキー再生成中に削除される
CSCvi55464	ASA5585 デバイスの電源装置のシリアル番号が SNMP 応答に含まれない
CSCvi58089	webvpn でのメモリ リーク
CSCvi59968	Firepower 2100 での SNMP Get 要求に対する不適切な応答 1.3.6.1.2.1.1.2.0
CSCvi64007	フェールオーバー後のゼロ化 RSA キーにより REST API がシステム コンテキストへの変更に失敗する

警告 ID 番号	説明
CSCvi65512	FTD：システムの負荷が比較的低い状態で AAB が snort を強制的に再起動することがある
CSCvi66905	PIM 自動 RP パケットがクラスタ マスターのスイッチオーバー後にドロップされる
CSCvi70606	ASA 9.6(4)：WebVPN ページが正しくロードされていない
CSCvi76577	ASA：netsnmp:Snmpwalk がホストグループの一部の IP グループで失敗する。
CSCvi77352	デバイスがそれ自体をクラスタから削除すると不正な更新が実行される
CSCvi79691	LDAP over SSL 暗号化エンジン エラー
CSCvi79999	VTI 使用時の ARP トラフィックにより 256 バイトのブロック リークが確認される
CSCvi80849	Cisco Firepower 2100 シリーズ POODLE TLS セキュリティスキャナのアラート
CSCvi82779	ASA が DATAPATH スレッドでトレースバックを生成する
CSCvi85382	ASA-IC-6GE-SFP-A モジュールが取り付けられている場合の ASA5515 の DMA のメモリ不足
CSCvi86799	多数のインターフェイスと QoS により「show service-policy」の出力時に ASA がトレースバックする
CSCvi87214	IPv6 トラフィックに対するネイバー要請メッセージが確認される
CSCvi87921	FIPS モードの TLS では、ASA 自己署名 RSA 証明書が許可されない
CSCvi89194	pki ハンドル：増加し、減少しない
CSCvi90633	ASDM AC のダウンロード時に GUI 言語を編集しても FPR-21XX の変更が無視される
CSCvi95544	「any」キーワードが設定されているアクセス制御ライセンスで ASA が IPv6 トラフィックを正しく照合しない
CSCvi96442	スレーブ ユニットが S2S の UDP/500 および IPSec パケットをマスターにリダイレクトせずにドロップする
CSCvi97729	フェールオーバーが「新規アクティブ」に移行しているときに to-the-box トラフィックがデータ インターフェイスの外にルーティングされる
CSCvi99743	Telnet アクセスを使用して「failover active」を実行した後に生じるスレッド「Logger」でのスタンバイ トレースバック

警告 ID 番号	説明
CSCvj05640	SNMP サーバが有効になっていない場合、SNMP アドレスでのトレースバックがマッピングされない
CSCvj15572	インターフェイスの MAC アドレスの変更時にフローオフロードのリライト ルールが更新されない
CSCvj17314	バージョン 9.7 以前では ASA が SAML 設定に「no signature」を受け入れない
CSCvj22491	クラスタ：インターフェイスのダウンからアップへのシナリオにおける ifc monitor debounce-time の拡張
CSCvj26450	ASA PKI OCSP 障害：CRYPTO_PKI：OCSP 応答データの復号化に失敗した
CSCvj32264	ASA：zonelabs-integrity：プロセス「Integrity FW task」によるトレースバックと高 CPU
CSCvj37448	ASA：リロード後にデバイスが SSL サーバ証明書パケットで ID 証明書のみを送信する
CSCvj37924	CWE-20：不適切な入力検証
CSCvj39858	トレースバック：スレッド名：IPsec message handler
CSCvj41748	WebVPN を介した Bonita BPM アプリの Web ページへのアクセスが失敗する
CSCvj42269	システム メモリが 101% と報告する syslog 321006 を ASA 9.8.2 が受信する
CSCvj42450	スレッド名 DATAPATH-14-17303 での ASA のトレースバック
CSCvj44262	portal-access-rule が「deny」から「permit」に変更される
CSCvj46777	Firepower Threat Defense 2100 ASA の原因不明のトレースバック
CSCvj47256	後続のフェールオーバーが 2 回実行されと ASA SIP セッションと Skinny セッションがドロップされる
CSCvj48340	ASA のメモリ リーク：snp_svc_insert_dtls_session
CSCvj49883	Firepower Threat Defense での ASA のトレースバック 2130-ASA-K9
CSCvj50024	ASA portchannel lacp max-bundle 1 hot-sby ポートがリンク障害後にアップ状態にならない
CSCvj54840	コンテキスト ストレス テストの作成/削除により nameif_install_arp_punt_service でトレースバックが発生する

警告 ID 番号	説明
CSCvj56008	ScanSafe 機能が HTTPS トラフィックに対してまったく機能しない
CSCvj56909	ASA モジュールによって生成される SACK パケットの SLE 値と SRE 値を ASA が非ランダム化しない
CSCvj59347	CLI コマンドの結果として最大 255 文字のエラーの上限が削除されるか、または増加する
CSCvj65581	2100 シリーズ アプライアンスでの ftdrpcd プロセスからの過剰なロギング
CSCvj67740	スタティック IPv6 ルート プレフィックスが ASA 設定から削除される
CSCvj67776	clear crypto ipsec ikev2 のコマンドがスタンバイに複製されない
CSCvj72309	FTD が BGP のグレースフル リスタート後に End-of-RIB のマーカーを送信しない
CSCvj73581	cli_xml_server スレッドでのトレースバック
CSCvj74210	「show service-policy inspect gtp pdp-context detail」実行時の「SSH」でのトレースバック
CSCvj75220	「virtual http」または「virtual telnet」の使用により、「same-security permit intra-interface」が誤って必要になる
CSCvj75793	2100/4100/9300：Management Center からキャプチャを停止/一時停止しても CPU 使用率が低下しない
CSCvj79765	アクティブ ASA での NetFlow 設定がスタンバイ ユニットで逆順に複製される
CSCvj85516	Firepower Threat Defense で「management」という名前のインターフェイスのパケット キャプチャが失敗する
CSCvj88514	IP ローカル プールが同じ名前で設定されている
CSCvj90428	FXOS を使用した ASA でのクロック同期の問題
CSCvj91449	各リブート後に IPv6 に対して logging host コマンドが有効になっている場合の ASA のトレースバック
CSCvj91619	1550 ブロックの枯渇により ASA が 6.2.3.3 をリロードする
CSCvj95451	webvpn-l7-rewriter：IE でブックマークのログアウトが失敗する
CSCvj97157	JS ファイルでのクライアント リライターの問題により Web ページがロードされない

警告 ID 番号	説明
CSCvj97514	ASA スマート ライセンス メッセージングが「nonce failed to match」で失敗する
CSCvj98964	SCTP トラフィックにより ASA がトレースバックすることがある
CSCvk00985	ASA：9.6.4、9.8.2：フェールオーバー ロギング メッセージがユーザ コンテキストに表示される
CSCvk02250	「show memory binsize」および「show memory top-usage」で正しい情報が表示されない（修正完了）
CSCvk04592	ハーフクローズ状態の lina conn テーブルでフローがスタックする
CSCvk07522	webvpn：Firefox と Chrome でブックマークのレンダリングが失敗する。IE では問題なし
CSCvk08377	9.8.2.20 を実行している ASA 5525 でメモリが枯渇する。
CSCvk08535	ASA が IKEv1 L2L トンネルグループに関する警告メッセージを生成する
CSCvk11898	v2 ハンドオフの処理中に GTP ソフト トレースバックが確認される
CSCvk14768	スレッド名 DATAPATH-1-2325 での ASA のトレースバック
CSCvk18378	show process（rip：inet_ntop6）実行時の ASA のトレースバックとリロード
CSCvk18578	ASA SSLVPN ログイン ページのカスタマイズをロードするために必要な圧縮の有効化
CSCvk19435	GTP APN 制限の解析時に不要な IE が存在するエラー
CSCvk24297	Windows 10 バージョン 1803 の IKEv2 フラグメンテーション機能が有効になっているため EAP を使用した IKEv2 RA が失敗する
CSCvk25729	大きな ACL のブート時のコンパイルに時間がかかり機能停止が生じる
CSCvk26887	無効なコンテンツ エンコーディングによりローカル CA からの証明書のインポートが失敗する
CSCvk27686	ASDM/Telnet/SSHを介して QoS メトリックにアクセスするときに ASA のトレースバックとリロードが発生することがある
CSCvk28023	WebVPN：文法ベースのパーサーがメタタグを処理できない
CSCvk30228	ASAv や FTDv の展開が Microsoft Azure で失敗したりコンソールの応答が遅くなったりする
CSCvk30665	ASA の「snmp-server enable traps memory-threshold」で CPU が占有され、「no buffer」でドロップする

警告 ID 番号	説明
CSCvk30739	ASA CP コアのピン接続によりコアローカル ブロックが枯渇する
CSCvk34648	高スループットの LAN 間 VPN トラフィックによりデータ キー再生成で Firepower 2100 トンネルがフラップする
CSCvk36087	ASDM を介して ASA にログインすると syslog 611101 に 0.0.0.0 の IP がリモート IP として表示される
CSCvk36733	huasan 製スイッチで ASA の EtherChannel をアクティブ モードで設定すると MAC アドレスがフラッピングする
CSCvk37890	Firepower 2110、webvpn の条件付きデバッグが原因で Threat Defense がトレースバックする
CSCvk38176	GTPインスペクションおよびフェールオーバーによるトレースバックとリロード
CSCvk43865	トレースバック：mutex ロック実行中の ASA 9.8.2.28
CSCvk45443	ASA クラスタ：NAT と高トラフィックによる CCL でのトラフィック ループ
CSCvk47583	ASA WebVPN：SAP Netweaver の誤った書き換え
CSCvk50732	MAC で Safari 11.1.x ブラウザを使用した AnyConnect 4.6 の Web 展開が失敗する
CSCvk50815	GTP インスペクションが TCP パケットを処理してはならない
CSCvk54779	フラグメント化したパケットに関する非同期キューの問題によりブロックが枯渇する：9344
CSCvk57516	Firepower Threat Defense：暗号マップが正しくないために DMA メモリが不足して VPN 障害が発生する
CSCvk62896	SA の削除中に生じる ASA IKEv2 のクラッシュ
CSCvk67239	「Thread Name: Logger Page fault: Address not mapped」での FTD または ASA のトレースバックとリロード
CSCvk67569	ASA が、クライアントレス WebVPN の HTTP 応答ページで返されたチャンク化済み転送エンコーディングを処理できない
CSCvk70676	ASA がメッセージ本文として HTTP を送信するとクライアントレス WebVPN が失敗する
CSCvm06114	RDP ブックマーク プラグインが起動しない

警告 ID 番号	説明
CSCvm07458	EEM を使用して VPN 接続イベントを追跡するとトレースバックとリロードが発生することがある
CSCvm19791	「capture stop」コマンドが asp-drop タイプのキャプチャで機能しない
CSCvm23370	ASA：PC cssls_get_crypto_ctxt によるメモリ リーク
CSCvm25972	ASA トレースバック：スレッド名 NIC Status Poll
CSCvm26004	ASA での AAB の計算が正しくないと、ランダムな AAB 呼び出しが発生する
CSCvm54827	Firepower 2100 ASA スマート ライセンスのホスト名の変更がスマート アカウントに反映されない
CSCvm56019	Cisco 適応型セキュリティ アプライアンスの WebVPN：VPN がブラウザを介して接続しない
CSCvm67316	ASA：CSCvm70848 の IKEv2/IPSec デバッグを追加
CSCvm70848	ASA：「Failed to create session mgmt entry for SPI <>」により、IPSec SA のインストールが失敗する
CSCvm80874	ASAv/FP2100 スマート ライセンス：ライセンスを登録/更新できない

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。