

Cisco ASA シリーズ 9.12(x) リリースノート

Cisco ASA シリーズ 9.12(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 9.12(x) のリリース情報が記載されています。

特記事項

- **9.12(4.50)/7.18(1.152) 以降で ASDM 署名付きイメージをサポート** : ASA は、ASDM イメージがシスコのデジタル署名付きイメージであるかどうかを検証するようになりました。この修正を適用した ASA バージョンで古い ASDM イメージを実行しようとする、ASDM がブロックされ、「%ERROR: Signature not valid for file disk0:/<filename>」というメッセージが ASA CLI に表示されます。ASDM リリース 7.18(1.152) 以降は、この修正が適用されていないものも含め、すべての ASA バージョンと下位互換性があります。(CSCwb05291、CSCwb05264)
- **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。

- **9.12(1) での SSH セキュリティの改善と新しいデフォルト設定**：次の SSH セキュリティの改善点を参照してください。

- SSH バージョン 1 はサポートされなくなりました。バージョン 2 のみがサポートされています。 **ssh version 1** コマンドは **ssh version 2** に移行されます。
- Diffie-Hellman Group 14 SHA256 キー交換のサポート。この設定がデフォルト (**ssh key-exchange group dh-group14-sha256**) になりました。以前のデフォルトは Group 1 SHA1 でした。SSH クライアントが Diffie-Hellman Group 14 SHA256 をサポートしていることを確認してください。サポートしていない場合は、「Couldn't agree on a key exchange algorithm」などのエラーが表示されることがあります。たとえば、OpenSSH では Diffie-Hellman Group 14 SHA256 がサポートされています。
- 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 (**ssh cipher integrity high** コマンドによって定義された **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。

- **9.12(1) での Diffie-Hellman グループ 1 の削除**：ASA IKE および IPsec モジュールで使用される Diffie-Hellman グループ 1 は安全ではないと見なされ、削除されました。

IKEv1：次のサブコマンドが削除されました。

- **crypto ikev1 policy priority**
 - **group 1**

IKEv2：次のサブコマンドが削除されました。

- **crypto ikev2 policy priority**
 - **group 1**

IPsec：次のサブコマンドが削除されました。

- **crypto ipsec profile name**
 - **set pfs group1**

SSL：次のコマンドが削除されました。

- **ssl dh-group group1**

Crypto Map：次のサブコマンドが削除されました。

- **crypto map name sequence set pfs group1**
- **crypto dynamic-map name sequence set pfs group1**
- **crypto map name sequence set ikev1 phase1-mode aggressive group1**

- **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も保持されます。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。

- **NULL-SHA TLSv1 暗号は廃止され、9.12(1) では削除されている**：NULL-SHA は暗号化を提供せず、現在の脅威に対して安全とは見なされなくなったため、**tls-proxy mode** コマンド/オプションおよび **show ssl ciphers all** の出力に TLSv1 でサポートされている暗号を一覧表示すると削除されます。**ssl cipher tlsv1 all** コマンドと **ssl cipher tlsv1 custom NULL-SHA** コマンドも廃止され、削除されます。
- **ローカル CA サーバーは 9.12(1) で廃止され、以降のリリースで削除される**：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を行うために有効になります。この機能は古くなったため、**crypto ca server** コマンドは廃止されています。
- **9.12(1) ではデフォルトの trustpool が削除されている**：PSB 要件、SEC-AUT-DEFROOT に準拠するため、「デフォルト」の信頼できる CA バンドルが ASA イメージから削除されています。その結果、**crypto ca trustpool import default** コマンドと **crypto ca trustpool import clean default** コマンドも、その他の関連ロジックとともに削除されています。ただし、既存の展開では、これらのコマンドを使用して以前にインポートされた証明書はそのまま残ります。
- **ssl encryption コマンドが 9.12(1) で削除されている**：9.3(2) で廃止が発表され、**ssl cipher** に置き換えられました。9.12(1) では、**ssl encryption** が削除され、サポートされなくなりました。

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 9.12(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
トラブルシューティング機能	
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
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

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) 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。
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

ASA 9.12(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。
ASA および FTD を同じ Firepower 9300 の別のモジュールでサポート	ASA および FTD 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。
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。
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	<p>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。</p> <p>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。</p> <p>変更されたコマンドはありません。</p>
Cisco Umbrella の強化	<p>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 サーバも特定できるようになりました。さらに、Umbrella サーバ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спек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。</p> <p>新規/変更されたコマンド：local-domain-bypass、resolver、umbrella fail-open</p>
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。	<p>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。</p> <p>新規/変更されたコマンド：object-group-search threshold</p>
NAT のポートブロック割り当てに対する暫定ログ	<p>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）。</p> <p>新規/変更されたコマンド：xlate block-allocation pba-interim-logging seconds</p>
VPN 機能	
debug aaa の新しい condition オプション	<p>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。</p> <p>新規/変更されたコマンド：debug aaa condition</p>
IKEv2 での RSA SHA-1 のサポート	<p>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。</p> <p>新規/変更されたコマンド：rsa-sig-sha1</p>

機能	説明
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
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

ハイ アベイラビリティとスケラビリティの各機能

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。各バンド 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
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

ルーティング機能

機能	説明
認証のための OSPF キー チェーンのサポート	<p>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。</p> <p>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。</p> <p>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</p>
証明書機能	
登録用 URL のローカル CA を設定可能な FQDN	<p>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。</p> <p>新規/変更されたコマンド：fqdn</p>
管理、モニタリング、およびトラブルシューティング機能	
enable ログイン時にパスワードの変更が必要になりました	<p>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。</p> <p>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。</p> <p>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。</p> <p>新規/変更されたコマンド：enable password</p>

機能	説明
管理セッションの設定可能な制限	<p>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。</p> <p>新規/変更されたコマンド：quota management-session、show quota management-session</p>
管理権限レベルの変更通知	<p>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。</p> <p>新規/変更されたコマンド：show aaa login-history</p>
IPv6 での NTP サポート	<p>NTP サーバに IPv6 アドレスを指定できるようになりました。</p> <p>新規/変更されたコマンド：ntp server</p>
SSH によるセキュリティの強化	<p>次の SSH セキュリティの改善を参照してください。</p> <ul style="list-style-type: none"> • 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。 <p>新規/変更されたコマンド：ssh cipher integrity、ssh key-exchange group dh-group14-sha256</p>
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	<p>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。</p> <p>新規/変更されたコマンド：http server basic-auth-client</p>
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	<p>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。</p> <p>新規/変更されたコマンド：capture interface cluster cp-cluster</p>

機能	説明
debug conn コマンド	<p>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。</p> <p>新規/変更されたコマンド： debug conn</p>
show tech-support に追加の出力が含まれている	<p>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。</p> <ul style="list-style-type: none"> • show ipv6 interface • show aaa-server • show fragment <p>新規/変更されたコマンド： show tech-support</p>

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
9.10(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)
9.3(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
9.2(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)
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)

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(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、『[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 9.12(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
CSCUw51499	ACE の追加/削除、ACL オブジェクト/オブジェクトグループの編集で TCM が機能しない
CSCvu29395	アクティブな IGMP join でマスターロールの変更を実行中にクラッシュが発生した
CSCvg59385	ASA ScanSafe コネクタのセカンダリ CWS タワーへのフェールオーバーに時間がかかりすぎる
CSCvj93609	spin_lock_release_actual での ASA トレースバック
CSCvm77115	無効な TSC 値による Lina のトレースバック
CSCvm85823	SSH、ssh_exec を実行できない：コンソールでの open(pager) エラー
CSCvo76866	2100 でのトレースバック：ウォッチドッグ
CSCvo80853	Cisco Firepower Threat Defense ソフトウェアのパケットにおけるサービス拒否攻撃に対する脆弱性
CSCvp04134	9.12.1 へのアップグレード時に HTTP CLI Exec でトレースバックする
CSCvp57417	ASAv のダウングレード時に、ファイアウォールがトレースバックしてリロードすることがある
CSCvp67033	ASA：IPv6 の名前エイリアスを識別できず、「incomplete command」エラーメッセージが表示される
CSCvp70833	ASA/FTD：同じサービスの NAT ルールがエラー「エラー：NAT がポートを予約できません (ERROR: NAT unable to reserve ports)」を 2 回表示する
CSCvp94478	ASA scp がかなり遅い
CSCvq12070	2 つ以上の同時 ASDM セッションを確立できない
CSCvq34340	出力最適化機能による 9344 ブロックサイズの枯渇による FTD トラフィックの停止
CSCvq37913	vpn-sessiondb がスタンバイ ASA に複製されない
CSCvq50587	ASA/FTD がスレッド名「BGP Router」でトレースバックし、リロードすることがある

問題 ID 番号	説明
CSCVq51284	FPR 2100、low block 9472 がデバイスを介してパケット損失を発生させる
CSCVq55426	IPv6 デフォルトルートを追加すると CLI が 50 秒間ハングする
CSCVq61601	FTD での OpenSSL の脆弱性 CVE-2019-1559
CSCVq65864	rest-api agent を有効にすると HTTP CLI Exec でトレースバックする
CSCVq70536	FTD : HA を中断し、グレースフルリスタートが設定にある場合に展開が失敗する
CSCVq73534	Cisco ASA ソフトウェアのケルベロス認証バイパスの脆弱性
CSCVq76198	FreeBSD システムのトラフィックの中断
CSCVq78126	HA-IKEv2 のクリプトマップ設定で逆ルートを設定した後も V ルートが見つからない
CSCVq83060	SNMP : フェールオーバーリンクの情報をマルチモードの OID から取得できない
CSCVq87797	マルチコンテキスト 5585 ASA、透過的コンテキストで管理インターフェイス設定が失われる
CSCVq88644	tcp-proxy でのトレースバック
CSCVq89361	Cisco Firepower 1000 シリーズの SSL/TLS におけるサービス拒否攻撃に対する脆弱性
CSCVq99107	ASA で SFP のホットスワップが有効になっていない
CSCvr03705	次のハブが同じである場合に AD を持つと同時にトンネリングされたデフォルトルートが必要になる
CSCvr07460	暗号 PKI の動作に関連して ASA がトレースバックおよびリロードする
CSCvr09399	動的フローオフロードを無効にできない
CSCvr09468	CLI 「Show nat pool」の ASA トレースバックとリロード
CSCvr10777	Ikev2 デーモンでの ASA トレースバック
CSCvr13278	リロード後に PPPoE セッションが起動しない
CSCvr13823	Cisco Firepower Threat Defense ソフトウェア管理アクセスリストバイパスの脆弱性
CSCvr15503	ASA : SSH と ASDM セッションが CLOSE_WAIT でスタックし、ASA の MGMT が不足する

問題 ID 番号	説明
CSCvr20449	実際には失敗しているポリシー展開が FMC で成功したとレポートされる
CSCvr20757	Cisco Umbrella DNS インスペクションの実行中に ASA でブロックリークが発生する
CSCvr20876	メモリが少ないとカーネルが起動し (OOM) 、デバイスがリロードされ、KP の rlimit が変更される
CSCvr21803	入力 FTD インターフェイスに挿入された誤ったパケットによりスイッチ上で Mac アドレスがフラップする
CSCvr25768	ASA が display_hole_og でトレースバックすることがある
CSCvr29638	FMC から ACP を展開した後、FPR2110 で HA FTD がトレースバックする
CSCvr42344	PBR に設定されたアクセスリストからのルールの削除時の snp_policy_based_route_lookup でのトレースバック
CSCvr50266	リロードの問題によってデュアルスタック ASA v フェールオーバーがトリガーされる
CSCvr50509	一部の 3DES 関連の設定がブート後に失われる
CSCvr50630	ASA トレースバック : SCTP バルク同期と HA 同期
CSCvr51426	ASA はアカウンティングパケットでマスクを送信していない
CSCvr51998	BGP 経由でデフォルトルートを学習後、ASA スタティックルートが ASP テーブルから消える
CSCvr54054	アイデンティティ NAT トラフィックに対して MAC の書き換えが実行される
CSCvr55400	スレッド名「cli_xml_server」で FTD/LINA がトレースバックし、リロードされる
CSCvr55518	ルールの作成に失敗したときにクリーンアップが行われない
CSCvr55825	Cisco ASA および FTD ソフトウェアのパストラバーサル脆弱性
CSCvr56031	スレッド名「cli_xml_server」で FTD/LINA がトレースバックし、リロードされる
CSCvr57605	リロード後の ASA のライセンスコンテキスト数がプラットフォームの制限を超える
CSCvr58411	新しいスタティックスポークを追加または変更した場合、新しいスタティックハブ/スポーク設定の RRI がハブで動作しない

問題 ID 番号	説明
CSCvr60111	設定がスタンバイから削除され、アクティブ時に展開が失敗する
CSCvr66768	PBR 設定がプッシュされているときに FTD 展開時に LINA がトレースバックする
CSCvr68146	FTD クラスタを自動で再参加させることができない
CSCvr68872	セカンダリユニットが、フェールオーバー リンク ダウン時のスプリット ブレイン シナリオでプラットフォーム コンテキスト カウント制限を超過する
CSCvr79974	フェールオーバーリンクでのパケット損失時に設定が複製されないことがある
CSCvr81457	TLS トラッカー (tls_trk_sniff_for_tls) がブロックを解放しようとする、FTD がトレースバックする
CSCvr83372	書き込み中に I/O エラーが発生する (fd='28', error='Resource temporarily unavailable (11)')
CSCvr85295	Cisco Adaptive Security Appliance と Firepower Threat Defense ソフトウェア リモート
CSCvr86077	re_multi_match_ascii によるデータパスでの ASA のトレースバック/ページフォルト
CSCvr90079	show run all で HSTS 設定オプションが更新されない
CSCvr90965	Azure で FTDv 展開を行うと、「no dns domain-lookup any」により回復不能なトレース状態が発生する
CSCvr92168	Cisco ASA および Cisco FTD ソフトウェアの OSPF パケット処理によるメモリーリークの脆弱性
CSCvr92327	ASA/FTD がスレッド名「PTHREAD-1533」でトレースバックおよびリロードすることがある
CSCvr93978	スレッド DATAPATH-0-2064 で ASA がトレースバックし、リロードする
CSCvs01422	FTD のデバイスモードの変更時に Lina がトレースバックする
CSCvs02954	ASA OSPF : トポロジが変更されると RIB からプレフィックスが削除され、別の SPF が実行されると再び追加される
CSCvs03023	クラスタリングモジュールは、タイムアウトエラーとクロックジャンプを回避するために、ハードウェアクロックの更新をスキップする必要がある

問題 ID 番号	説明
CSCvs04179	ASA : ssh または fover_rx スレッドで 9.8.4.12 がトレースバックし、リロードする
CSCvs05262	デクリメント TTL で間違った結果が表示される
CSCvs07668	SIP インスペクションが有効になっていると、スレッド DATAPATH-1-15076 で FTD がトレースバックし、リロードする
CSCvs07982	ASA トレースバック : sctpProcessNextSegment - SCTP_INIT_CHUNK
CSCvs09533	3 つ以上のインラインセットを介してトラフィックを処理すると、FP2100 がトレースバックし、リロードする
CSCvs15276	エラー : IPv6 ICMP の設定時に ::/0 のエントリが存在する
CSCvs15972	SSL ポリシーが有効な場合にネットワークパフォーマンスが低下する
CSCvs16073	ホストとホストグループが設定された SNMP ポーリングが失敗する
CSCvs27264	ASA の mroute エントリが更新されない
CSCvs28213	アサーション slib_malloc.c を使用したスレッド名 SSH での ASA トレースバック
CSCvs28580	高負荷状態で SSL トラフィックを処理するときのトレースバック
CSCvs29779	ASA が「DATAPATH-12-1899」プロセスの完了を待っているときにトレースバックし、リロードすることがある
CSCvs31443	ASA が「%ASA-5-321001: Resource 'memory' limit」メッセージで負のメモリ値を報告する
CSCvs31470	OSPF Hello により 9K ブロックが枯渇し、制御ポイントの CPU が 100% になり、クラスタが不安定になる
CSCvs32023	出力最適化処理をオフにする
CSCvs33102	ASA/FTD がスレッド名「EIGRP-IPv4」でトレースバックし、リロードすることがある
CSCvs33852	バージョン 9.6.4.34 へのアップグレード後、アクセスグループを追加できない
CSCvs38785	syslog のタイムスタンプ形式が一貫していない
CSCvs39589	データチャネルがネゴシエートされていない場合は ASA が SSH タイムアウトを実行しない
CSCvs40230	ICMP が機能せず、「inspect-icmp-seq-num-not-matched」によって失敗する

問題 ID 番号	説明
CSCvs40531	AnyConnect 4.8 が FPR1000 シリーズで動作していない
CSCvs43154	アグレッシブ警告メッセージのためにセカンダリ ASA がフェールオーバーに参加できない
CSCvs45548	再アクティブ化モードが時間切れになることで、障害が発生したサーバーが不適切なタイミングで再アクティブ化される
CSCvs47252	コマンド「clear capture/」を実行している場合の ASA トレースバックとリロード
CSCvs48437	ASA が同時に 2 つの UDP ポートに syslog を送信できない
CSCvs50459	Cisco ASA および Cisco FTD の不正な OSPF パケット処理によるサービス拒否攻撃に対する脆弱性
CSCvs52169	AnyConnect からのデバイス ID が長すぎると、ASA が不正な形式の RADIUS メッセージを送信する
CSCvs53705	AnyConnect セッションが誤って制限されている
CSCvs55603	ACL で一致した場合に ICMP 応答がドロップされた
CSCvs59056	Float-Conn が有効になっている場合、ASA/FTD トンネルスタティックルートが準最適なルックアップによって無視される
CSCvs59966	OID 「cipSecGlobalActiveTunnels」について間違った値がレポートされる (ASDM と同様)
CSCvs63484	SAML トークンがハッシュテーブルから削除されない
CSCvs70260	IKEv2 vpn-filter がボリュームベースのキー再生成コリジョン後に暗黙的な拒否によりトラフィックをドロップする
CSCvs71698	管理デフォルトルートがデフォルト データ ルーティングと競合する
CSCvs73663	IPsec message handler スレッドでの ASA のトレースバック
CSCvs76605	FXOS 2.6(1.174) にリストされているモジュールのバージョンが間違っている
CSCvs77818	トレースバック : spin_lock_fair_mode_enqueue : ロック (np_conn_shrlock_t) が長期間にわたって保持されている
CSCvs79023	スレッド名での ASA/FTD のトレースバック : DNS インスペクションによる DATAPATH
CSCvs80157	スレッド名 IKE Daemon での ASA のトレースバック

問題 ID 番号	説明
CSCvs80536	ASA キャプチャで FP41xx の不正なインターフェイスが適用される
CSCvs82726	マルチコンテキストモードで CSCvs31470 に対処するためのプレースホルダ
CSCvs85196	ASA SIP 接続が連続した複数回のフェールオーバー後にドロップする：ピンホールタイムアウト/インスペクションによるクローズ
CSCvs87795	ASA：バックアップコンテキストが失敗し「ERROR: No such file or directory」と表示される
CSCvs88413	バージョン 9.8 へのアップグレードにポートチャネルのバンドルに失敗する
CSCvs90100	ASA/FTD がスレッド名「License Thread」でトレースバックおよびリロードすることがある
CSCvs91389	FTD トレースバック Lina プロセス
CSCvs91869	FPR-1000 シリーズのランダム番号生成エラー
CSCvs97863	フラッシュファイルシステムでのクローズ時の fsync コールの数を減らす
CSCvs97908	無効な scp セッションが他のアクティブな http と scp のセッションを終了させる
CSCvt01397	LINA 設定がプッシュされなかったにもかかわらず、展開は正常としてマークされる
CSCvt02409	FPR9300 3 ノードクラスタのネストされた VLAN トラフィックで 9.12.2.151 snp_cluster_ingress がトレースバックする
CSCvt04560	クラスタ展開でのファイアウォールで SCTP ハートビートが失敗する
CSCvt05862	サーバーが管理インターフェイスを介して到達可能な場合、IPv6 DNS サーバーの解決が失敗する
CSCvt06606	フローオフロードが FTD 6.2(3.10) と FXOS 2.6(1.169) の組み合わせで機能しない
CSCvt06841	ASA でのキャプチャを使用して設定すると、誤ったアクセスリストのヒットカウントが表示される
CSCvt11661	DOC：show asp dropでの mp-svc-flow-control の意味を明確にする
CSCvt11742	ASA/FTD がスレッド名「ssh」でトレースバックし、リロードすることがある
CSCvt12463	ASA：Unicorn Admin Handler スレッドでのトレースバック

問題 ID 番号	説明
CSCvt13822	ASA : 一致する暗号マップエントリがないため、VTI が IPSec トンネルを拒否する
CSCvt15163	Cisco ASA および FTD ソフトウェアの Web サービスに関する情報漏洩の脆弱性
CSCvt21041	スレッド「ctm_ipsec_display_msg」での FTD のトレースバック
CSCvt22356	ASA のリブート後、ASA クラスタの Health-check monitor-interface debounce-time が 9000ms にリセットされる
CSCvt23643	データを復旧するための、VPN フェールオーバーリカバリに約 30 秒かかる
CSCvt24328	FTD : lina_host_file_open_raw 関数に関連するトレースバックとリロード
CSCvt25225	ASA : OSPF 同期中の設定同期状態時のアクティブユニットの HA トレースバックとリロード
CSCvt26031	ASA が IPv6 を使用してスマートライセンスを登録できない
CSCvt26067	セカンダリインターフェイスが FTD で使用されている場合、アクティブ FTP が失敗する
CSCvt27585	スタンバイからのフェールオーバー切り替え実行中に KP でのクラッシュが確認された
CSCvt28182	sctp-state-bypass がインライン FTD に対して呼び出されない
CSCvt33785	ランダム VPN ピアの IPSec SA が作成されない
CSCvt35945	9.8 トレインで SSH バージョン 2 を有効にする場合に Encryption-3DES-AES が必要であってはならない
CSCvt45863	IP ヘッダーの長さがパケット長と一致しない場合に暗号リングが停止する
CSCvt46289	Firepower 1000 シリーズで ASA LDAPS 接続が失敗する
CSCvt46830	FPR2100 「show crypto accelerator statistics」カウンタは対称暗号を追跡しない
CSCvt51987	ASA での 80 サイズのブロックの枯渇によりトラフィックが停止する
CSCvt64035	remote access mib : ラップアラウンド前に SNMP 64 ビットのみが 4Gb を報告する
CSCvt64952	「Show crypto accelerator load-balance detail」が欠落しており、出力が未定義

問題 ID 番号	説明
CSCvt65982	RRI ルートの削除時にスレーブユニットでルートフォールバックが発生しない
CSCvt66351	NetFlow のレポートのフローのバイト数が非常に大きい
CSCvt68294	Firepower 4120 の最大 VPN セッション制限を 20,000 に調整する
CSCvt70664	ASA : AnyConnect の Radius Acct-Requests に acct-session-time アカウンティング属性がない
CSCvt73407	ASA デバイスのユーザー名 enable_15 に対する TACACS フォールバック認証が失敗する
CSCvt73806	FP2120 LINA アクティブボックスでの FTD のトレースバックとリロード。[VPN]
CSCvt75241	FPR2100 で FTD をリロードした後、VPN でアダプタイズされたスタティックルートの再配布が失敗する
CSCvt78068	FP1000/1100 シリーズプラットフォームの FTD で時刻同期が正しく機能しない
CSCvt86188	診断インターフェイスを介して SNMP トラップを生成できない

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 9.12(4) 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
CSCuw51499	ACE の追加/削除、ACL オブジェクト/オブジェクトグループの編集で TCM が機能しない
CSCvg59385	ASA ScanSafe コネクタのセカンダリ CWS タワーへのフェールオーバーに時間がかかりすぎる
CSCvj93609	spin_lock_release_actual での ASA トレースバック
CSCvm77115	無効な TSC 値による Lina のトレースバック
CSCvm85823	SSH、ssh_exec を実行できない：コンソールでの open(pager) エラー
CSCvo76866	2100 でのトレースバック：ウォッチドッグ

問題 ID 番号	説明
CSCvo80853	Cisco Firepower Threat Defense ソフトウェアのパッケージにおけるサービス拒否攻撃に対する脆弱性
CSCvp04134	9.12.1 へのアップグレード時に HTTP CLI Exec でトレースバックする
CSCvp57417	ASAv のダウングレード時に、ファイアウォールがトレースバックしてリロードすることがある
CSCvp57643	FTD/ASA : クラスタ/HA : マスター/アクティブ ユニットではすべてのルート変更がスレーブ/スタンバイに更新されない
CSCvp67033	ASA : IPv6 の名前エイリアスを識別できず、「incomplete command」エラーメッセージが表示される
CSCvp70833	ASA/FTD : 同じサービスの NAT ルールがエラー「エラー : NAT がポートを予約できません (ERROR: NAT unable to reserve ports)」を 2 回表示する
CSCvp94478	ASA scp がかなり遅い
CSCvq12070	2 つ以上の同時 ASDM セッションを確立できない
CSCvq34340	出力最適化機能による 9344 ブロックサイズの枯渇による FTD トラフィックの停止
CSCvq37913	vpn-sessiondb がスタンバイ ASA に複製されない
CSCvq50587	ASA/FTD がスレッド名「BGP Router」でトレースバックし、リロードすることがある
CSCvq50944	OSPFv3 ネイバーシップが約 30 分ごとにフラッピングしている
CSCvq51284	FPR 2100、low block 9472 がデバイスを介してパケット損失を発生させる
CSCvq55426	IPv6 デフォルトルートを追加すると CLI が 50 秒間ハングする
CSCvq61601	FTD での OpenSSL の脆弱性 CVE-2019-1559
CSCvq65864	rest-api agent を有効にすると HTTP CLI Exec でトレースバックする
CSCvq70536	FTD : HA を中断し、グレースフルリスタートが設定にある場合に展開が失敗する
CSCvq73534	Cisco ASA ソフトウェアのケルベロス認証バイパスの脆弱性
CSCvq76198	FreeBSD システムのトラフィックの中断
CSCvq78126	HA-IKEv2 のクリプトマップ設定で逆ルートを設定した後も V ルートが見つからない

問題 ID 番号	説明
CSCvq83060	SNMP : フェールオーバーリンクの情報をマルチモードのOIDから取得できない
CSCvq87797	マルチコンテキスト 5585 ASA、透過的コンテキストで管理インターフェイス設定が失われる
CSCvq88644	tcp-proxy でのトレースバック
CSCvq89361	Cisco Firepower 1000 シリーズの SSL/TLS におけるサービス拒否攻撃に対する脆弱性
CSCvq99107	ASA で SFP のホットスワップが有効になっていない
CSCvr03705	次のハブが同じである場合に AD を持つと同時にトンネリングされたデフォルトルートが必要になる
CSCvr07460	暗号 PKI の動作に関連して ASA がトレースバックおよびリロードする
CSCvr09399	動的フローオフロードを無効にできない
CSCvr09468	CLI 「Show nat pool」の ASA トレースバックとリロード
CSCvr10777	Ikev2 デーモンでの ASA トレースバック
CSCvr13278	リロード後に PPPoE セッションが起動しない
CSCvr13823	Cisco Firepower Threat Defense ソフトウェア管理アクセスリストバイパスの脆弱性
CSCvr15503	ASA : SSH と ASDM セッションが CLOSE_WAIT でスタックし、ASA の MGMT が不足する
CSCvr20449	実際には失敗しているポリシー展開が FMC で成功したとレポートされる
CSCvr20757	Cisco Umbrella DNS インспекションの実行中に ASA でブロックリークが発生する
CSCvr20876	メモリが少ないとカーネルが起動し (OOM) 、デバイスがリロードされ、KP の rlimit が変更される
CSCvr21803	入力 FTD インターフェイスに挿入された誤ったパケットによりスイッチ上で Mac アドレスがフラップする
CSCvr25768	ASA が display_hole_og でトレースバックすることがある
CSCvr29638	FMC から ACP を展開した後、FPR2110 で HA FTD がトレースバックする
CSCvr42344	PBR に設定されたアクセスリストからのルールの削除時の snp_policy_based_route_lookup でのトレースバック

問題 ID 番号	説明
CSCvr50266	リロードの問題によってデュアルスタック ASAv フェールオーバーがトリガーされる
CSCvr50509	一部の 3DES 関連の設定がブート後に失われる
CSCvr50630	ASA トレースバック : SCTP バルク同期と HA 同期
CSCvr51426	ASA はアカウントングパケットでマスクを送信していない
CSCvr51998	BGP 経由でデフォルトルートを学習後、ASA スタティックルートが ASP テーブルから消える
CSCvr54054	アイデンティティ NAT トラフィックに対して MAC の書き換えが実行される
CSCvr55400	スレッド名「cli_xml_server」でFTD/LINAがトレースバックし、リロードされる
CSCvr55518	ルールの作成に失敗したときにクリーンアップが行われない
CSCvr55825	Cisco ASA および FTD ソフトウェアのパストラバーサル脆弱性
CSCvr56031	スレッド名「cli_xml_server」でFTD/LINAがトレースバックし、リロードされる
CSCvr57605	リロード後の ASA のライセンスコンテキスト数がプラットフォームの制限を超える
CSCvr58411	新しいスタティックスポークを追加または変更した場合、新しいスタティックハブ/スポーク設定の RRI がハブで動作しない
CSCvr60111	設定がスタンバイから削除され、アクティブ時に展開が失敗する
CSCvr66768	PBR 設定がプッシュされているときに FTD 展開時に LINA がトレースバックする
CSCvr68146	FTD クラスタを自動で再参加させることができない
CSCvr68872	セカンダリユニットが、フェールオーバー リンク ダウン時のスプリットブレイン シナリオでプラットフォーム コンテキスト カウント制限を超過する
CSCvr79974	フェールオーバーリンクでのパケット損失時に設定が複製されないことがある
CSCvr81457	TLS トラッカー (tls_trk_sniff_for_tls) がブロックを解放しようとする、FTD がトレースバックする

問題 ID 番号	説明
CSCvr83372	書き込み中に I/O エラーが発生する (fd='28', error='Resource temporarily unavailable (11)')
CSCvr85295	Cisco Adaptive Security Appliance と Firepower Threat Defense ソフトウェア リモート
CSCvr86077	re_multi_match_ascii によるデータパスでの ASA のトレースバック/ページ フォルト
CSCvr90079	show run all で HSTS 設定オプションが更新されない
CSCvr90965	Azure で FTDv 展開を行うと、「no dns domain-lookup any」により回復不能なトレース状態が発生する
CSCvr92168	Cisco ASA および Cisco FTD ソフトウェアの OSPF パケット処理によるメモリリークの脆弱性
CSCvr92327	ASA/FTD がスレッド名「PTHREAD-1533」でトレースバックおよびリロードすることがある
CSCvr93978	スレッド DATAPATH-0-2064 で ASA がトレースバックし、リロードする
CSCvs01422	FTD のデバイスモードの変更時に Lina がトレースバックする
CSCvs02954	ASA OSPF : トポロジが変更されると RIB からプレフィックスが削除され、別の SPF が実行されると再び追加される
CSCvs03023	クラスタリングモジュールは、タイムアウトエラーとクロックジャンプを回避するために、ハードウェアクロックの更新をスキップする必要がある
CSCvs04179	ASA : ssh または fover_rx スレッドで 9.8.4.12 がトレースバックし、リロードする
CSCvs05262	デクリメント TTL で間違った結果が表示される
CSCvs07668	SIP インспекションが有効になっていると、スレッド DATAPATH-1-15076 で FTD がトレースバックし、リロードする
CSCvs07982	ASA トレースバック : sctpProcessNextSegment - SCTP_INIT_CHUNK
CSCvs09533	3 つ以上のインラインセットを介してトラフィックを処理すると、FP2100 がトレースバックし、リロードする
CSCvs15276	エラー : IPv6 ICMP の設定時に ::0 のエントリが存在する
CSCvs15972	SSL ポリシーが有効な場合にネットワークパフォーマンスが低下する
CSCvs16073	ホストとホストグループが設定された SNMP ポーリングが失敗する

問題 ID 番号	説明
CSCvs27264	ASA の mroute エントリが更新されない
CSCvs28213	アサーション <code>slib_malloc.c</code> を使用したスレッド名 SSH での ASA トレースバック
CSCvs28580	高負荷状態で SSL トラフィックを処理するときのトレースバック
CSCvs29779	ASA が「DATAPATH-12-1899」プロセスの完了を待っているときにトレースバックし、リロードすることがある
CSCvs31443	ASA が「%ASA-5-321001: Resource 'memory' limit」メッセージで負のメモリ値を報告する
CSCvs31470	OSPF Hello により 9K ブロックが枯渇し、制御ポイントの CPU が 100% になり、クラスタが不安定になる
CSCvs32023	出力最適化処理をオフにする
CSCvs33102	ASA/FTD がスレッド名「EIGRP-IPv4」でトレースバックし、リロードすることがある
CSCvs33852	バージョン 9.6.4.34 へのアップグレード後、アクセスグループを追加できない
CSCvs38785	syslog のタイムスタンプ形式が一貫していない
CSCvs39589	データチャネルがネゴシエートされていない場合は ASA が SSH タイムアウトを実行しない
CSCvs40230	ICMP が機能せず、「inspect-icmp-seq-num-not-matched」によって失敗する
CSCvs40531	AnyConnect 4.8 が FPR1000 シリーズで動作していない
CSCvs43154	アグレッシブ警告メッセージのためにセカンダリ ASA がフェールオーバーに参加できない
CSCvs45548	再アクティブ化モードが時間切れになることで、障害が発生したサーバーが不適切なタイミングで再アクティブ化される
CSCvs47252	コマンド「clear capture/」を実行している場合の ASA トレースバックとリロード
CSCvs48437	ASA が同時に 2 つの UDP ポートに syslog を送信できない
CSCvs50459	Cisco ASA および Cisco FTD の不正な OSPF パケット処理によるサービス拒否攻撃に対する脆弱性
CSCvs52169	AnyConnect からのデバイス ID が長すぎると、ASA が不正な形式の RADIUS メッセージを送信する

問題 ID 番号	説明
CSCvs53705	AnyConnect セッションが誤って制限されている
CSCvs55603	ACL で一致した場合に ICMP 応答がドロップされた
CSCvs59056	Float-Conn が有効になっている場合、ASA/FTD トンネルスタティックルートが準最適なルックアップによって無視される
CSCvs59966	OID 「cipSecGlobalActiveTunnels」について間違った値がレポートされる (ASDM と同様)
CSCvs63484	SAML トークンがハッシュテーブルから削除されない
CSCvs70260	IKEv2 vpn-filter がボリュームベースのキー再生成コリジョン後に暗黙的な拒否によりトラフィックをドロップする
CSCvs71698	管理デフォルトルートがデフォルト データ ルーティングと競合する
CSCvs73663	IPsec message handler スレッドでの ASA のトレースバック
CSCvs76605	FXOS 2.6(1.174)にリストされているモジュールのバージョンが間違っている
CSCvs77818	トレースバック : spin_lock_fair_mode_enqueue : ロック (np_conn_shrlock_t) が長期間にわたって保持されている
CSCvs79023	スレッド名での ASA/FTD のトレースバック : DNS インスペクションによる DATAPATH
CSCvs80157	スレッド名 IKE Daemon での ASA のトレースバック
CSCvs80536	ASA キャプチャで FP41xx の不正なインターフェイスが適用される
CSCvs82726	マルチコンテキストモードで CSCvs31470 に対処するためのプレースホルダ
CSCvs85196	ASA SIP 接続が連続した複数回のフェールオーバー後にドロップする : ピンホールタイムアウト/インスペクションによるクローズ
CSCvs87795	ASA : バックアップコンテキストが失敗し 「ERROR: No such file or directory」と表示される
CSCvs88413	バージョン 9.8 へのアップグレードにポートチャネルのバンドルに失敗する
CSCvs90100	ASA/FTD がスレッド名 「License Thread」 でトレースバックおよびリロードすることがある
CSCvs91389	FTD トレースバック Lina プロセス

問題 ID 番号	説明
CSCvs91869	FPR-1000 シリーズのランダム番号生成エラー
CSCvs97863	フラッシュファイルシステムでのクローズ時の fsync コールの数を減らす
CSCvs97908	無効な scp セッションが他のアクティブな http と scp のセッションを終了させる
CSCvt01397	LINA 設定がプッシュされなかったにもかかわらず、展開は正常としてマークされる
CSCvt02409	FPR93003 ノードクラスタのネストされた VLAN トラフィックで 9.12.2.151 snp_cluster_ingress がトレースバックする
CSCvt03598	Cisco ASA ソフトウェアおよび FTD ソフトウェア Web サービスの読み取り専用パストラバーサル脆弱性
CSCvt04560	クラスタ展開でのファイアウォールで SCTP ハートビートが失敗する
CSCvt05862	サーバーが管理インターフェイスを介して到達可能な場合、IPv6 DNS サーバーの解決が失敗する
CSCvt06606	フローオフロードが FTD 6.2(3.10) と FXOS 2.6(1.169) の組み合わせで機能しない
CSCvt06841	ASA でのキャプチャを使用して設定すると、誤ったアクセスリストのヒットカウントが表示される
CSCvt11661	DOC : show asp drop での mp-svc-flow-control の意味を明確にする
CSCvt11742	ASA/FTD がスレッド名「ssh」でトレースバックし、リロードすることがある
CSCvt12463	ASA : Unicorn Admin Handler スレッドでのトレースバック
CSCvt13822	ASA : 一致する暗号マップエントリがないため、VTI が IPSec トンネルを拒否する
CSCvt15163	Cisco ASA および FTD ソフトウェアの Web サービスに関する情報漏洩脆弱性
CSCvt21041	スレッド「ctm_ipsec_display_msg」での FTD のトレースバック
CSCvt22356	ASA のリポート後、ASA クラスタの Health-check monitor-interface debounce-time が 9000ms にリセットされる
CSCvt23643	データを復旧するための、VPN フェールオーバーリカバリに約 30 秒かかる
CSCvt24328	FTD : lina_host_file_open_raw 関数に関連するトレースバックとリロード

問題 ID 番号	説明
CSCvt25225	ASA : OSPF 同期中の設定同期状態時のアクティブユニットの HA トレースバックとリロード
CSCvt26031	ASAv が IPv6 を使用してスマートライセンスを登録できない
CSCvt26067	セカンダリインターフェイスが FTD で使用されている場合、アクティブ FTP が失敗する
CSCvt27585	スタンバイからのフェールオーバー切り替え実行中に KP でのクラッシュが確認された
CSCvt28182	sctp-state-bypass がインライン FTD に対して呼び出されない
CSCvt33785	ランダム VPN ピアの IPsec SA が作成されない
CSCvt35945	9.8 トレインで SSH バージョン2を有効にする場合に Encryption-3DES-AES が必要であってはならない
CSCvt45863	IPヘッダーの長さがパケット長と一致しない場合に暗号リングが停止する
CSCvt46289	Firepower 1000 シリーズで ASA LDAPS 接続が失敗する
CSCvt46830	FPR2100 「show crypto accelerator statistics」 カウンタは対称暗号を追跡しない
CSCvt51987	ASA での 80 サイズのブロックの枯渇によりトラフィックが停止する
CSCvt52782	ASA トレースバックスレッド名 : webvpn_task
CSCvt64035	remote access mib : ラップアラウンド前に SNMP 64ビットのみが 4Gb を報告する
CSCvt64952	「Show crypto accelerator load-balance detail」 が欠落しており、出力が未定義
CSCvt65982	RRIルートの削除時にスレーブユニットでルートフォールバックが発生しない
CSCvt66351	NetFlow のレポートのフローのバイト数が非常に大きい
CSCvt68294	Firepower 4120 の最大 VPN セッション制限を 20,000 に調整する
CSCvt70664	ASA : AnyConnect の Radius Acct-Requests に acct-session-time アカウンティング属性がない
CSCvt73407	ASA デバイスの ユーザー名 enable_15 に対する TACACS フォールバック認証が失敗する

問題 ID 番号	説明
CSCvt73806	FP2120 LINA アクティブボックスでの FTD のトレースバックとリロード。 [VPN]
CSCvt75241	FPR2100 で FTD をリロードした後、VPN でアドバタイズされたスタティックルートの再配布が失敗する
CSCvt78068	FP1000/1100 シリーズプラットフォームの FTD で時刻同期が正しく機能しない
CSCvt86188	診断インターフェイスを介して SNMP トラップを生成できない

バージョン 9.12(3) 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
CSCvf83160	スレッド名 DATAPATH-2-1785 でのトレースバック
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)」
CSCvj61580	スレッドでの ASA トレースバック：DATAPATH-8-2035
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)
CSCvk29685	ASA の DATAPATH でのトレースバック
CSCvm36362	ルートトラッキングエラー
CSCvm40288	HA リンクでのポートチャネルの問題
CSCvm64400	IKEv2 : IKEv2-PROTO-2 : 「プラットフォームからの PSH の割り当てに失敗しました (IKEv2-PROTO-2: Failed to allocate PSH from platform)」
CSCvm70274	tcp プロキシ：データベースでの ASA のトレースバック
CSCvn76875	BGP のグレースフルリスタートが断続的に動作しなくなる
CSCvn77388	SDI - 一時停止されたサーバーにより、正常なサーバーでの認証の完了に 15 秒の遅延が発生する
CSCvn78593	FTD でコントロールプレーン ACL が正しく機能しない
CSCvn78870	範囲外の allocate-interface コマンドによる ASA マルチコンテキストのトレースバックとリロード

問題 ID 番号	説明
CSCvn86777	メモリが不足している FTD で展開を行うとインターフェイス nameif が削除される : finetune mmap thresh
CSCvo03700	クラスタがスレーブユニットで有効になっている場合にスレッドロガーで ASA がトレースバックすることがある
CSCvo14961	「dns_cache_timer」プロセスの終了を待機している間に ASA がトレースバックし、リロードすることがある。
CSCvo17775	新しいサブインターフェイスが追加され、「ac-address auto」が有効になると EIGRP が中断する
CSCvo28118	メンバーがクラスタに参加しようとするとき VPN クラスタリング HA のタイマースレッドでトレースバックが発生する
CSCvo43795	OSPF プロセスのクリア後も OSPF プロセス ID が変更されない
CSCvo45755	box stall mid-transfer への ASA SCP 転送
CSCvo47390	スレッド SSH での ASA トレースバック
CSCvo47562	キー再生成中に PKI ハンドルが解放されないため、VPN セッションが失敗する
CSCvo48838	長すぎる設定行のエラーを Lina が適切に報告しない
CSCvo51265	Cisco 適応型セキュリティ アプライアンス ソフトウェアのセキュアコピーのサービス拒否 (DoS) 攻撃に対する脆弱性
CSCvo58847	トンネル置き換えシナリオが原因で発生した高 IKE CPU に対処するための機能強化
CSCvo60580	「show inventory」コマンド発行時の ASA のトレースバックとリロード
CSCvo62031	IKE デバッグ実行中の ASA のトレースバックとリロード
CSCvo65741	ASA : フェールオーバーが発生して BGP ルートが変更されると、ルーティングテーブルで BGP ルートがクリアされる
CSCvo66534	影響を受けるスレッドとしてデータパスを示すトレースバックとリロード
CSCvo68184	セカンダリ FTD の診断 I/F の管理専用が表示されなくなる
CSCvo72462	ルールを復号しないとトラフィックが中断する
CSCvo73250	ENH : 警告「重複する要素が見つかりました (found duplicate element)」の ACE の詳細

問題 ID 番号	説明
CSCvo74350	ASA がトレースバックしリロードすることがある。WebVPN トラフィックに関連する可能性がある
CSCvo74397	ENH : 「コマンドは無視されました。設定中です... (Command Ignored, configuration in progress...)」にプロセス情報を追加
CSCvo78789	Cisco 適応型セキュリティアプライアンスのスマートトンネルに関する脆弱性
CSCvo80501	手動フェールオーバーの実行時にスタンバイファイアウォールがトレースバックしてリロードする
CSCvo83169	Cisco ASA ソフトウェアと FTD ソフトウェアの FTP のインスペクションサービス拒否攻撃に対する脆弱性
CSCvo86038	flow-offloaded フローでの同時 FIN が接続の失効につながる
CSCvo87930	w3m を使用した ipv6 の HTTP が失敗する
CSCvo88762	FTD インライン/トランスペアレントでパケットが入力インターフェイスを介して送り返される
CSCvo90153	ASA が特殊文字を含むユーザーを https 経由で認証できない
CSCvo97979	インターフェイス設定の delay コマンドが再起動後に変更される
CSCvp04134	9.12.1 へのアップグレード時に HTTP CLI Exec でトレースバックする
CSCvp04186	cts import-pac tftp : 構文が機能しない
CSCvp07143	DTLS 1.2 および AnyConnect oMTU
CSCvp10132	AnyConnect 接続が TCP 接続制限の超過エラーで失敗する
CSCvp12052	ASA がトレースバックおよびリロードすることがある。webvpn に関連する可能性がある
CSCvp12582	ASA のウェルウンポート名ではなくポート番号をアクセスリストで表示するオプション
CSCvp14674	ASAv Azure : ASAv のフェールオーバー時にルートテーブルの BGP 伝達設定がリセットされる
CSCvp16536	SIP インスペクションによりデータパスで ASA のトレースバックとリロードが確認される
CSCvp18878	ASA : データパスでのウォッチドッグのトレースバック
CSCvp19549	FTD lina がスレッド名 cli_xml_server でコア化する

問題 ID 番号	説明
CSCvp19910	ヘッダー TEID : 0 の gtpv1 identification req メッセージを処理できない
CSCvp19998	ASA がヘッダー TEID:0 の GTPV1 SGSN Context Req メッセージをドロップする
CSCvp23109	ASA HA IKEv2 汎用 RA - 「AnyConnect Premium All In Use」がスタンバイ状態で正しく表示されない
CSCvp24728	FTD によってランダムな SGT タグが追加される
CSCvp29692	ポリシー展開失敗後からのロールバック後に FIPS モードが無効になる
CSCvp32617	9.6.2 以降で「確立済み TCP」が機能しない
CSCvp33341	Cisco ASA および Firepower Threat Defense ソフトウェア WebVPN クロスサイト スクリプティングの脆弱性
CSCvp35141	ASA が POST 要求に対して無効なリダイレクト応答を送信する
CSCvp35384	IKEv2 RA 汎用クライアント - asp テーブルエントリの発信時にスタックする - 古い SPI で暗号化されたトラフィック
CSCvp43066	DHCP リレーとして設定されている場合に DHCP サーバーから送信された DHCP NACK が ASA によってサイレントにドロップされる
CSCvp45882	Cisco ASA ソフトウェアと FTD ソフトウェアの SIP のインスペクション サービス拒否攻撃に対する脆弱性
CSCvp49576	xlate_detach のウォッチドッグによる FTD のトレースバック
CSCvp49790	Cisco ASA ソフトウェアと FTD ソフトウェアの OSPF LSA 処理のサービス拒否攻撃に対する脆弱性
CSCvp55901	HA アクティブユニットの ASA で LINA が繰り返しトレースバックする
CSCvp59864	IP アドレスがローカルプールでスタックし、AnyConnect クライアントが切断されていても「使用中」と表示される
CSCvp63068	スレッド名 : CP DP SFR イベント処理のトレースバック
CSCvp67392	リバースパスチェックにより ASA/FTD HA データインターフェイスのハートビートがドロップされる
CSCvp70020	再起動後、「ssh version 1 2」が running-config に追加される
CSCvp71180	RADIUS チャレンジを使用した MCA+AAA+OTP がチャレンジでの aggauth ハンドルの送信に失敗する
CSCvp72412	syslog メッセージのタイムゾーン

問題 ID 番号	説明
CSCvp76944	Cisco ASA および FTD ソフトウェア WebVPN CPU のサービス妨害 (DoS) 脆弱性
CSCvp80775	クライアント側 WebVPN リライタでのサポートされていないランタイム JavaScript の例外処理
CSCvp84546	ASA 9.9.2 クライアントレス WebVPN - HTML の処理時に HTML エンティティが誤って復号化される
CSCvp85736	クラスタマスターのリロードによって管理仮想 IP への ping が失敗する
CSCvq00005	SSL 復号化 DND の保持による LINA での FTD のトレースバックとリロード
CSCvq01459	9.12.2.1 へのアップグレード後の LINA トレースバック
CSCvq05113	設定の最初の 10 個のインターフェイスで ASA フェールオーバー LANTEST メッセージが送信される
CSCvq11513	トレースバック : 「saml identity-provider」 コマンドでマルチコンテキスト ASA がクラッシュする
CSCvq12070	2 つ以上の同時 ASDM セッションを確立できない
CSCvq12411	CSCvj98964 の修正があるにもかかわらず、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
CSCvq13442	コンテキストを削除すると、ssh key-exchange がグローバルにデフォルトになる
CSCvq21607	CLI を使用してバックアップを復元すると、「ssl trust-point」 コマンドが削除される
CSCvq24134	ASA IKEv2 - フェーズ 2 のキー再生成の開始後に ASA が追加の削除メッセージを送信する
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
CSCvq25626	バッファへのロギング時の ASAv のウォッチドッグ
CSCvq26794	存在しない原因を含む GTP 応答メッセージがドロップされて、TID が 0 のエラーメッセージが発行される
CSCvq27010	ASA-SFR データプレーンの通信でフラッピングが発生した際にメモリリークが起こる

問題 ID 番号	説明
CSCvq34160	fp1000 シリーズプラットフォームへの ASDM 接続の確立時のトレースバックとリロード
CSCvq39317	ASA がファイルの整合性を確認できない
CSCvq44665	FTD/ASA : アサート snp_tcp_intercept_assert_disabled によるデータパスでのトレースバック
CSCvq46587	フェールオーバー後、アクティブユニットの TCP セッションがタイムアウトに達したときに削除されない
CSCvq54667	SSL ネゴシエーションの問題により、SSL VPN が確立できない場合がある
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
CSCvq60131	デバイスへの EZVPN スポークの移動時に ASA のトレースバックが発生する
CSCvq63024	デュアルスタック ASA の手動フェールオーバーの問題
CSCvq64742	スレッド名 ssh での ASA5515-K9 スタンバイトレースバック
CSCvq65241	スレッド名での Saleen の ASA トレースバック : IPv6 IDB
CSCvq65864	96.4.0.41 へのアップグレード時に HTTP CLI Exec でトレースバックする
CSCvq69111	トレースバック : スレッド名でのクラスタユニット lina のアサーション : クラスタコントローラ
CSCvq70468	ASA クラスタが OSPF ルートをフラッシュしない
CSCvq70775	FPR2100 FTD スタンバイユニットで 9K ブロックがリークする
CSCvq75743	ASA : 3 ホップ離れた宛先に対する BGP の再帰ルートルックアップが失敗する
CSCvq77547	ポートチャネルでのフェールオーバー記述子の不一致により、フェールオーバーで接続の複製が失敗する
CSCvq80318	Internal-Data0/1 の列挙時に ASA が PCI cfg 領域に関する誤ったエラーメッセージを生成する
CSCvq80735	ネイバーが 1 つのインターフェイスと同じサブネット上にある場合、BGP にネイバーを追加できない
CSCvq91645	フローオフロードハッシュの動作変更
CSCvq92126	スレッド IPsec Message Handler での ASA のトレースバック

問題 ID 番号	説明
CSCvr10777	Ikev2 デーモンでの ASA トレースバック
CSCvr20757	ASAv が Cisco Umbrella の実行中に使用できなくなる
CSCvr25768	ASA が display_hole_og でトレースバックすることがある
CSCvr50266	リロードの問題によってデュアルスタック ASAv フェールオーバーがトリガーされる
CSCvr66768	PBR 設定がプッシュされているときに FTD 展開時に LINA がトレースバックする
CSCvr85295	Cisco Adaptive Security Appliance と Firepower Threat Defense ソフトウェア リモート

バージョン 9.12(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
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
CSCvj06993	NSF による ASA の HA : ASA の HA でインターフェイス障害が発生した場合に NSF が正しくトリガーされない
CSCvj82652	disk0 が読み取り専用マウントされているため展開の変更がデバイスにプッシュされない
CSCvk15393	ASA デバイスは、スレッド名 ha_trans_data_tx でリロードします。
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
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
CSCvm50421	ACE での OSPF/EIGRP と IPv6 の同時使用が原因で ASA が同期設定中にスレーブ/スタンバイでトレースバックする
CSCvn13880	マルチキャストルーティングが有効な場合にタイマー イベントが原因でユニットがスレッド PIM IPv4 または IGMP IPv4 でトレースバックする
CSCvn17347	CPU プロファイリング結果表示時のトレースバックとリロード
CSCvn22833	Firepower 4100 の ASA で ADI プロセスの開始に失敗する

問題 ID 番号	説明
CSCvn25949	ASA への REST API イメージのアップロード中にデジタル署名の検証に失敗した
CSCvn31347	ACL : アクセスグループの設定エラー後に ACL を設定できない
CSCvn38453	ASA : FIPS が有効な場合に Quovadis ルート証明書をトラストポイントとしてロードできない
CSCvn40592	証明書チェーンで「No certificate」コマンドを実行すると誤った証明書が削除される
CSCvn46358	VPN ステータス メッセージの送信による lina msglyr インフラの過負荷
CSCvn55007	キー再生成後に DTLS が失敗する
CSCvn67137	NetFlow の使用時に ASA5506 が徐々にメモリ リークを起こすことがある
CSCvn68527	KP : AnyConnect がプールから使用している IP が使用可能と表示される
CSCvn69213	複数のスレッドが同じロックを待機しているために発生する ASA のトレースバックとリロード : ウォッチドッグ
CSCvn72650	6.3.0 リリースでの FTD アドレスがマッピングされないトレースバック
CSCvn75368	FPR プラットフォームの IPsec VPN が断続的にダウンする
CSCvn78674	シスコ適応型セキュリティ アプライアンスのクライアントレス SSL VPN におけるクロスサイトスクリプティングの脆弱性
CSCvn80394	ASA SNMP による CPU の占有
CSCvn94100	「Process Name: lina」 Netflow による ASA のトレースバック
CSCvn95711	スレッド名のトレースバック : IKEV2 ipsec-proposal にプロトコルを追加した後の Unicorn Admin ハンドラ
CSCvn96898	SCP のダウンロードにより DMA_Pool で発生するバイナリ サイズ 1024 のメモリ リーク
CSCvn97591	パケット トレーサが「ERROR: TRACER: NP failed tracing packet」で失敗し、循環 ASP でキャプチャをドロップする
CSCvn97733	syslog ID 111005 が正しく生成されない
CSCvo02097	ASA クラスタを 9.10.1.7 にアップグレードするとトレースバックが発生する
CSCvo03808	OOM が原因で FMC からの展開が失敗し、理由が示されない

問題 ID 番号	説明
CSCvo04444	Ikev2 トンネルの作成に失敗する
CSCvo06216	CSCuz22961 の hanover におけるスプリット DNS コミットの問題に対する 255 文字以上のサポート
CSCvo09046	ASA クラスタを 9.10.1.7 にアップグレードするとメモリ不足が生じる
CSCvo11077	新しい IKEv1 トンネルを確立して終了すると IPSec でメモリ リークが検出される
CSCvo11406	シスコ適応型セキュリティ アプライアンスのクライアントレス SSL VPN におけるクロスサイト スクリプティングの脆弱性
CSCvo12057	DHCPRelay がユニキャスト フラグ付きの DHCP Offer パケットを消費しない
CSCvo13497	「log default」 キーワードのあるアクセスリストを削除できない
CSCvo15497	トンネルグループ : 「no ikev2 local-authentication pre-shared-key」 でローカル証明書の認証が削除される
CSCvo19247	アウトバウンド SSL パケットの処理中のトレースバック
CSCvo20847	同期時に xlate の割り当ての破損が原因でアクティブ FTP がクラスタを介して失敗する
CSCvo21210	PDTS の numa ノード情報が正しくないためロード バランシングが正しく行われない
CSCvo23222	マルチコンテキスト展開でのリソースの問題により AnyConnect セッションが拒否される
CSCvo27109	9.6(4)6 から 9.6(4)20 へのアップグレード時にスタンバイがリブートループに陥ることがある
CSCvo38051	ctm_ipsec_pfkey_parse_msg における ctm_ipsec_pfkey.c:602 での segfault
CSCvo39356	スレッド名でのトレースバック : IP アドレスの割り当て
CSCvo42174	ASA IPSec VPN EAP が PKI の有効な証明書をロードできない
CSCvo43679	FTDLina のトレースバック (Normaliser によるシステムでのパケットループが原因)
CSCvo45230	ASA5506 : IBR : インターフェイスが IBR モードの BVI にある場合にホスト名を使用して ping を実行できない
CSCvo55151	VTI が存在する場合に crypto ipsec inner-routing-lookup の設定を許可しないようにする必要がある

バージョン 9.12(1) で解決済みのバグ

問題 ID 番号	説明
CSCvo56675	フェールオーバー状態の変更または xlate のクリアを原因とする ASA または FTD のトレースバックとリロード
CSCvo62077	SFR VPN イベントのメモリ リーク
CSCvo63240	アップグレード後にスマートトンネルのブックマークが機能せず、証明書エラーとなる
CSCvo93872	GTP トラフィックの検査中のメモリ リーク
CSCvp16482	ASDM の同時セッションを確立すると FXOS プラットフォーム上の ASA がリロードされる
CSCvp36425	スレッド名 octnic_hm_thread での ASA 5506/5508/5516 のトレースバック

バージョン 9.12(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
CSCux69220	DHCP での WebVPN 「enable intf」、ASA ブート時の CLI の欠落
CSCuz70352	リモートアクセス VPN を介して SSH 接続できない (Telnet、ASDM 動作時)
CSCvb21927	IKEv2 証明書認証の PRF SHA2 相互運用性サードパーティ
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
CSCvd21406	「any」という名前のインターフェイスを持つ複数の PAT ルールが原因で 305006 「portmap translation creation failed」となる
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
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
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
CSCvf85831	イメージのアップロード中に ASDM がエラーを表示する
CSCvg00565	「debug menu」セルフテストの実行時に glib/g_slice で ASA がクラッシュする

問題 ID 番号	説明
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
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
CSCvg78582	ENH : ASA 9.8.2 での HTTP セキュア ヘッダー X-XSS-Protection の欠落
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。
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
CSCvh77456	Cisco Firepower Threat Defense ソフトウェアの FTP インスペクションにおけるサービス妨害の脆弱性
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妨害の脆弱性
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
CSCvh86252	snort のタイムアウトによるブラックリストフロー タイムアウトのインライン変更
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
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
CSCvi03103	BGP ASN によってポリシーの展開が失敗する
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

問題 ID 番号	説明
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
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
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 ユーザー接続を拒否する
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)
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
CSCvi54162	ピアが存在しない場合に「ha-replace」アクションが動作しない
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
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
CSCvi71622	スタンバイ FTD の DATAPATH でのトレースバック
CSCvi77643	HTTP のインスペクションによる FPR4120 でのダウンロードのハングとダウンロードの速度低下
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
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
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
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
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

問題 ID 番号	説明
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
CSCvj01704	SFR モジュールのシャットダウン後に ASA が Spyker のみでリポートにより トレースバック状態になる
CSCvj18111	FTD : N1 フラグのフロー保持を IPS インターフェイスで適用してはならない
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
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
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
CSCvj43591	ASA DHCP を使用した Firepower 2110 が正常に動作しない
CSCvj47119	「clear capture /all」により Firepower 9300 MI の Firepower Threat Defense がクラッシュすることがある
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
CSCvj50008	WebVPN HSTS ヘッダーに RFC 6797 に従った includeSubDomains 応答がない
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
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
CSCvj58342	セキュリティ コンテキストの削除後にマルチキャストがドロップされる

問題 ID 番号	説明
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 <code>ftdrpcd</code> プロセスからの過剰なロギング
CSCvj67258	2 タプルおよび 4 タプルのハッシュ テーブルをロックレスに変更する
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	<code>clear crypto ipsec ikev2</code> 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	<code>cli_xml_server</code> スレッドでのトレースバック
CSCvj74210	「 <code>show service-policy inspect gtp pdp-context detail</code> 」実行時の「SSH」でのトレースバック
CSCvj75220	「 <code>virtual http</code> 」または「 <code>virtual telnet</code> 」の使用により、「 <code>same-security permit intra-interface</code> 」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「 <code>management</code> 」という名前のインターフェイスの packets キャプチャが失敗する
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
CSCvj88514	IP ローカルプールが同じ名前を設定されている
CSCvj89470	Cisco 適応型セキュリティアプライアンスのダイレクトメモリアクセスにおけるサービス拒否攻撃に対する脆弱性
CSCvj91449	各リブート後に IPv6 に対して <code>logging host</code> 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
CSCvj91815	CSM から ASA にファイルをコピーしようとしたときに発生する無効な HTTP 応答 (SSL 通信中の IO エラー)
CSCvj91858	Cisco 適応型セキュリティアプライアンスのアクセスコントロールリストにおけるバイパスの脆弱性

問題 ID 番号	説明
CSCVj92444	ASA がネイバー損失後にタイプ 7 NSSA を保持する
CSCVj95451	webvpn-17-rewriter : IE でブックマークのログアウトが失敗する
CSCVj97159	復号化された IKE_AUTH_Reply で ASA IKEv2 キャプチャ タイプ isakmp 設定の「Initiator Request」フラグが正しくない
CSCVj97213	ASA IKEv2 キャプチャ タイプ isakmp が破損したパケットを保存しているか、またはパケットが欠落している
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ー 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
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
CSCvk14258	ASA5585-SSP-## のクラッシュ出力でハードウェアの ASP-## が報告される。完全なモデル名を正しく報告する必要がある
CSCvk14537	SSH/Telnet の管理セッションが pc ftpc_suspend でスタックすることがある
CSCvk18330	アクティブな FTP データ転送が FTP インспекションと NAT で失敗する
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

問題 ID 番号	説明
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arserがメタタグを処理できない
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
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
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
CSCvk30775	ENH : 「show tech」出力への「show fragment」の追加
CSCvk30779	ENH : 「show tech」出力への「show ipv6 interface」の追加
CSCvk30783	ENH : 「show tech」出力への「show aaa-server」の追加
CSCvk31035	KVM (FTD) : 外部からの Web サーバーのマッピングが他のプラットフォームと一貫した動作をしない
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спек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

問題 ID 番号	説明
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
CSCvk46038	エラー : 権限付与が設定のキャッシュ中にすでに取得されている
CSCvk47583	ASA WebVPN : SAP Netweaver の誤った書き換え
CSCvk48437	ASA - VTI トンネルインターフェイス nameif が SNMP の「snmp-server host」コマンドで使用できない
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
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
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	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 のトレースバック
CSCvk66529	FPR 9300 の FTD で事前フィルタが有効になっている状態で TCP ヘッダー が破損する
CSCvk66771	CPU プロファイラがしきい値に達しないままサンプルを収集せずに実行を 停止する
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
CSCvk72192	オーバーヘッドによるメモリ使用率が含まれているために「show memory」 の「free memory」が正しく出力されない
CSCvk72958	インターフェイスに適用されている QoS が機能しない
CSCvm01053	FPR9K-SM-44 での ASA 9.8(2)24 のトレースバック
CSCvm06114	RDP ブックマーク プラグインが起動しない

問題 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
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
CSCvm15880	FPR 9k ASA クラスターのマルチコンテキストモード/vpn モードの配信が原因で設定がトランスペアレントモードの場合にリブートループが生じる
CSCvm17985	BVI インターフェイスの管理アクセスを使用した write net コマンドの開始が成功しない
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
CSCvm24706	GTP 削除ベアラー要求がドロップされている
CSCvm25972	ASA トレースバック : スレッド名 NIC Status Poll
CSCvm36138	v1 ホストが設定されている状態でそのホストからの v2c walk が成功する
CSCvm43975	SIP インспекションの脆弱性による Cisco ASA および FTD のサービス拒否または高 CPU
CSCvm49283	オブジェクトグループの検索しきい値の作成がデフォルトで無効になっており、設定可能である。機能停止の原因となる。
CSCvm53531	Cisco 適応型セキュリティ アプライアンス ソフトウェアの特権昇格の脆弱性
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
CSCvm55091	FP プラットフォームで「No Switchover」のステータスのままで HA 障害を起こしたプライマリユニットがアクティブと表示される
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
CSCvm56371	同じ dACL が接続されているすべての AnyConnect クライアントの dACL を ASA が誤って削除する
CSCvm56719	スレッド名 vpnfol_thread_msg での高可用性スタンバイユニットのトレースバック
CSCvm65725	サーバーの応答が大きすぎた場合に (ERR_RESPONSE_TOO_BIG) ASA Kerberos 認証で TCP への切り替えが失敗する

問題 ID 番号	説明
CSCvm67273	ASA : PC alloc_fo_ipsec_info_buffer_ver_1+136 によるメモリ リーク
CSCvm67316	ASA : CSCvm70848 の IKEv2/IPSec デバッグを追加
CSCvm72378	ASA : CLI : ユーザーにネットワークオブジェクト「ANY」の作成を許可してはならない
CSCvm78449	log default コマンドでアクセスコントロールライセンスエントリを変更できない
CSCvm80779	ASA が H323 H225 を検査しない
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
CSCvm82930	FTD : 重複する NAT ステートメントが設定されている場合に SSH から ASA へのデータ インターフェイスが失敗する
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
CSCvm87970	WebVPN クライアントレス : パスワード管理に関する問題
CSCvm88004	ASA 上の SSH サービスが入力された文字や貼り付けられた各文字を自身のパケットにエコー バックする
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
CSCvm92359	ブロック枯渇スナップショットが ASA でキャプチャされなかった
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)
CSCvn03966	FTD : 「object-group-search」が flexconfig を介してプッシュされるとすべての ACL が削除されて機能停止が発生する
CSCvn04688	サーバーのホストキーが 128 文字に設定されている場合に TACAC を使用した ASA AAA 認証が機能しない
CSCvn09322	FTD デバイスがアクティブ状態になった後に 5 分以内にリブートされる
CSCvn09367	管理者が ASA 5500-X に CXSC モジュールを取り付けられないようにする
CSCvn09612	非アクティブなオフロードセッションで ASA/FTD 接続アイドルタイマーが増加しない
CSCvn09640	FTD : パーサーからの ethertype ACL を信頼する機能が必要である。BPDU の通過を許可する必要がある

問題 ID 番号	説明
CSCvn13556	トランスペアレントモードでの実行時にポートチャンネルIFのインターフェイス番号が未割り当てと表示される
CSCvn15757	NULL チェックなしの SCTP トラフィック インспекションにより ASA がトレースバックすることがある
CSCvn19823	ASA : 失敗した SSL 接続が削除されず、DMA メモリが枯渇する
CSCvn22833	Firepower 4100 の ASA で ADI プロセスの開始に失敗する
CSCvn23254	Nameif がインターフェイスで設定されている場合に SNMPv2 が空の ifHCInOctets 値をプルする
CSCvn29446	アクティブ ASA での除外設定をスタンバイ ASA と同期できない
CSCvn30108	ASAv での「show memory」 CLI 出力が正しくない
CSCvn30393	AnyConnect の認証/DAP アセスメントの実行中に ASA が emweb/https でトレースバックする
CSCvn32657	call-home で使用したインターフェイス設定を削除すると ASA がトレースバックする
CSCvn33943	HA 設定の同期を使用した wccp_int_statechange() でのスタンバイ ノードのトレースバック
CSCvn35014	OS アップグレード時の ASA ルートの変更
CSCvn44201	IOS XE 16.5.1 以降で実行されているネイバーから送信された LLS TLV を持つ OSPF hello パケットが ASA によって破棄される
CSCvn44748	「show interface」の実行時に指定した仮想 MAC アドレスを表示できなかった
CSCvn46425	フェールオーバーは有効になっているが他のデバイスが到達不能の場合に AnyConnect の証明書認証と定期証明書認証が失敗する
CSCvn47599	RA VPN + SAML 認証により RADIUS サーバーに対して 2 つの許可要求が発生する
CSCvn47800	ファイバの枯渇により ASA が新しい AnyConnect 接続の認証を停止する
CSCvn49180	ASA/FTD : CCL リンクのメンバインターフェイスの変更後に MAC アドレスが更新されない
CSCvn56095	SSL 暗号化ハードウェア オフロードで選択的な ack が発生しない
CSCvn61662	CXSC モジュールが継続的にリロードされるために ASA 5500-X が crashinfo を書き込まずにリロードすることがある

問題 ID 番号	説明
CSCvn62470	ASA によってドロップされた Anyconnect クライアントの DNS 要求が包括可能である
CSCvn62787	フロー テーブル設定の更新中に devcmd 障害時における CRUZ への複数回の再試行をサポートする方法
CSCvn64418	Nokia 7705 ルータでの ISA300 interop の問題
CSCvn66248	ファイルがオフボックスで変更されて再度コピーされた場合に「boot config」を設定しても効果がない
CSCvn67222	DPD がフェールオーバー後に機能せずフェールバックした場合に（まれに）機能停止が発生することがある
CSCvn69213	複数のスレッドが同じロックを待機しているために発生する ASA のトレースバックとリロード：ウォッチドッグ
CSCvn73962	IPSec を使用したデータパスでの ASA 5585 9.8.3.14 のトレースバック
CSCvn76829	SSL クライアントとしての ASA がハンドシェイク エラー パスでメモリリークを起こす
CSCvn77636	ASA/webvpn：FF および Chrome：文法ベースのパースャーでブックマークがレンダリングされない
CSCvn94100	「Process Name: lina」 Netflow による ASA のトレースバック
CSCvn97517	WebVPN：URL エントリが無効/埋め込みツールバー内の「Go to」アドレスが有効にならない
CSCvo06216	CSCuz22961 の hanover におけるスプリット DNS コミットの問題に対する 255 文字以上のサポート
CSCvo09046	ASA クラスタを 9.10.1.7 にアップグレードするとメモリ不足が生じる

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。

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2023 Cisco Systems, Inc. All rights reserved.

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。