

Cisco Secure Firewall ASA シリーズ 9.18(x) リリースノート

初版：2022年6月6日

最終更新：2024年10月2日

Secure Firewall ASA シリーズ 9.18(x) リリースノート

このドキュメントには、ASA ソフトウェアバージョン 9.18 のリリース情報が記載されていません。

特記事項

- **9.18(2)/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)
- **9.18 以降からのダウングレードの問題**：9.18 では動作が変更され、**access-group** コマンドがその **access-list** コマンドの前にリストされます。ダウングレードすると、**access-group** コマンドはまだ **access-list** コマンドをロードしていないため拒否されます。以前に **forward-reference enable** コマンドを有効にしていた場合でも、このコマンドは現在削除されているため同じ結果となります。ダウングレードする前にすべての **access-group** コマンドを手動でコピーし、ダウングレード後に再入力してください。
- **同じポートを使用した同じインターフェイスで HTTPS/ASDM (HTTPS 認証を使用) および SSL を有効にした場合の 9.18(1) アップグレードの問題**：同じインターフェイス上で SSL ([webvpn]>[インターフェイスの有効化 (enable interface)]) と HTTPS/ASDM (**http**) アクセスの両方を有効にした場合、**https://ip_address** から AnyConnect にアクセスでき、**https://ip_address/admin** から ASDM にアクセスできます。どちらもポート 443 を使用します。ただし、HTTPS 認証 (**aaa authentication http console**) も有効にする場合は、9.18(1) 以降、ASDM アクセス用に別のポートを指定する必要があります。**http** コマンドを使用してアップグレードする前に、ポートを変更してください。(CSCvz92016)
- **9.18(2.7) での Cisco Secure Firewall 3100 の動作変更**：Cisco Secure Firewall 3100 の固定ポートで **fec** コマンドを使用して FEC を Auto に設定すると、25 GB SR、CSR、および LR トランシーバのデフォルトのタイプが cl74-fc ではなく cl108-rs に設定されるようになりました。(CSCwc75082)

システム要件

ASDM には、4 コア以上の CPU を搭載したコンピュータが必要です。コア数が少ないと、メモリ使用量が高くなる可能性があります。

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 Secure Firewall 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 9.18(4) の新機能

リリース : 2023 年 10 月 3 日

機能	説明
ハイ アベイラビリティとスケラビリティの各機能	
ASA の高可用性のための偽フェールオーバーの削減	ASA 高可用性のデータプレーンに追加のハートビートモジュールが導入されました。このハートビートモジュールは、コントロールプレーンのトラフィックの輻輳や CPU の過負荷が原因で発生する可能性のある、偽フェールオーバーやスプリットブレインシナリオを回避するのに役立ちます。 9.20(1) でも同様です。

機能	説明
show failover statistics にクライアント統計情報を追加	<p>フェールオーバークライアントのパケット統計情報が拡張され、デバッグ機能が向上しました。show failover statistics コマンドは、np-clients (データパスクライアント) および cp-clients (コントロールプレーンクライアント) の情報を表示するように拡張されています。</p> <p>変更されたコマンド：show failover statistics cp-clients、show failover statistics dp-clients</p> <p>9.20(2) でも同様です。</p>
show failover statistics events に新しいイベントを追加	<p>show failover statistics events コマンドが拡張され、アプリケーションエージェントによって通知されるローカル障害 (フェールオーバーリンクの稼働時間、スーパーバイザハートビート障害、およびディスクフルの問題) を表示するようになりました。</p> <p>変更されたコマンド：show failover statistics events</p> <p>9.20(2) でも同様です。</p>
インターフェイス機能	
FXOS local-mgmt show コマンドの改善	<p>FXOS local-mgmt のインターフェイス show コマンドに関する追加項目は次のとおりです。</p> <ul style="list-style-type: none"> • show portmanager switch tail-drop-allocated buffers all コマンドが追加されました。 • show portmanager switch status コマンドにイーサネットポート ID が含まれます。 • Cisco Secure Firewall 3100 に、show portmanager switch default-rule-drop-counter コマンドが追加されました。 <p>新規/変更された FXOS コマンド：show portmanager switch tail-drop-allocated buffers all、show portmanager switch status、show portmanager switch default-rule-drop-counter</p>
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	

ASA 9.18(3) の新機能

機能	説明
show tech support の改善	<p>次の項目に対して、show tech support への出力が追加されました。</p> <ul style="list-style-type: none"> • Cisco Secure Firewall 3100 の show storage detail、show slot expand detail (show tech support brief 内) • ASA Virtual のフラッシュ内の dpdk.log からの最近のメッセージ • Firepower 1010 の制御リンク状態 • show failover 統計情報 • FXOS local-mgmt show portmanager switch tail-drop-allocated buffers all • show controller • DPDK mbuf プール統計情報 <p>新規/変更されたコマンド：show tech support</p>

ASA 9.18(3) の新機能

リリース日：2023年2月16日

機能	説明
プラットフォーム機能	
Firepower 1010E	<p>Firepower 1010E が導入されました。このモデルは、Power Over Ethernet ポートが搭載されていないことを除き Firepower 1010 と同じです。</p> <p>7.19(1.90) または 7.18(2.1) での ASDM サポート。ASDM 7.19(1) ではこのモデルをサポートしていません。</p> <p>9.18(2.218) でも同様。このモデルは 9.19(1) ではサポートされていません。</p>
インターフェイス機能	
Secure Firewall 3100 固定ポートのデフォルトの前方誤り訂正 (FEC) が、25 GB+ SR、CSR、および LR トランシーバの cl74-fc から cl108-rs に変更されました	<p>Secure Firewall 3100 の固定ポートで FEC を Auto に設定すると、25 GB SR、CSR、および LR トランシーバのデフォルトのタイプが cl74-fc ではなく cl108-rs に設定されるようになりました。</p> <p>新規/変更されたコマンド：fec</p> <p>9.19(1) および 9.18(2.7) でも同様です。</p>
VPN 機能	

機能	説明
SAML を使用した AnyConnect 接続認証	DNS ロードバランシングクラスタでは、SAML 認証を ASA で設定するときに、設定が適用されるデバイスに一意に解決されるローカルベース URL を指定できます。 新規/変更されたコマンド : local-base-urlurl

ASA 9.18(2) の新機能

リリース日 : 2022 年 8 月 10 日

機能	説明
インターフェイス機能	
BGP および管理トラフィックのループバックインターフェイスをサポート	ループバック インターフェイスを追加して、次の機能に使用できるようになりました。 <ul style="list-style-type: none"> • AAA • BGP • SNMP • SSH • Syslog • Telnet 新規/変更されたコマンド : interface loopback 、 logging host 、 neighbor update-source 、 snmp-server host 、 ssh 、 telnet
ping コマンドの変更	ループバック インターフェイスの ping をサポートするために、 ping コマンドの動作が変更されました。コマンドでインターフェイスを指定する場合、送信元 IP アドレスは指定されたインターフェイスの IP アドレスと一致しますが、実際の実出力インターフェイスは、データルーティングテーブルを使用したルートルックアップによって決定されます。 新規/変更されたコマンド : ping

ASA 9.18(1) の新機能

リリース日 : 2022 年 6 月 6 日

機能	説明
プラットフォーム機能	

ASA 9.18(1) の新機能

機能	説明
AWS GuardDuty の ASAv-AWS Security center integration	Amazon GuardDuty サービスを ASAv と統合できるようになりました。この統合ソリューションは、Amazon GuardDuty によって報告された脅威分析データや結果（悪意のある IP アドレス）をキャプチャして処理するのに役立ちます。ASAv で悪意のある IP アドレスを設定およびフィードし、基盤となるネットワークとアプリケーションを保護できます。
ファイアウォール機能	
ACL とオブジェクトの前方参照は常に有効にです。さらに、アクセス制御のオブジェクトグループ検索がデフォルトで有効になりました。	<p>アクセスグループまたはアクセスルールを設定するときに、まだ存在していない ACL またはネットワークオブジェクトを参照できます。</p> <p>さらに、オブジェクトグループ検索が新規展開のアクセス制御に対してデフォルトで有効になりました。デバイスをアップグレードしても、引き続きこのコマンドは無効になります。有効にする場合（推奨）、手動で行う必要があります。</p> <p>注意 ダウングレードすると、access-group コマンドはまだ access-list コマンドをロードしていないため拒否されます。以前に forward-reference enable コマンドを有効にしていた場合でも、このコマンドは現在削除されているため同じ結果となります。ダウングレードする前にすべての access-group コマンドを手動でコピーし、ダウングレード後に再入力してください。</p> <p>forward-reference enable コマンドを削除し、新規展開のデフォルト値を変更して object-group-search access-control を有効にしました。</p>
ルーティング機能	
PBR のパスモニタリングメトリック。	<p>PBR はメトリックを使用して、トラフィックを転送するための最適なパス（出力インターフェイス）を決定します。パスモニタリングは、メトリックが変更されたモニタリング対象インターフェイスを PBR に定期的に通知します。PBR は、モニタリング対象インターフェイスの最新のメトリック値をパスモニタリングデータベースから取得し、データパスを更新します。</p> <p>新規/変更されたコマンド：clear path-monitoring、policy-route、show path-monitoring</p>
インターフェイス機能	
Cisco Secure Firewall 3100 のフロー制御に対応するためのフレームの一時停止	<p>トラフィック バーストが発生している場合、バーストが NIC の FIFO バッファまたは受信リングバッファのバッファリング容量を超えると、パケットがドロップされる可能性があります。フロー制御用のポーズフレームをイネーブルにすると、このような問題の発生を抑制できます。</p> <p>新規/変更されたコマンド：flowcontrol send on</p>
Secure Firewall 3130 および 3140 のブレイクアウトポート	<p>Cisco Secure Firewall 3130 および 3140 の 40 GB インターフェイスごとに 4 つの 10 GB ブレイクアウトポートを構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：breakout</p>

機能	説明
ライセンス機能	
キャリアライセンスの Secure Firewall 3100 サポート	キャリアライセンスは、Diameter、GTP/GPRS、SCTP 検査を有効にします。 新規/変更されたコマンド： feature carrier
証明書の機能	
相互 LDAPS 認証。	ASA が認証のために証明書を要求したときに LDAP サーバーに提示するように ASA のクライアント証明書を設定できます。この機能は、LDAP over SSL を使用する場合に適用されます。LDAP サーバーがピア証明書を要求するように設定されている場合、セキュア LDAP セッションが完了せず、認証/許可要求が失敗します。 新規/変更されたコマンド： ssl-client-certificate
認証：証明書名または SAN の検証	機能固有の参照 ID が設定されている場合、ピア証明書 ID は、指定された一致基準 crypto ca reference-identity <name> コマンドで検証されます。ピア証明書のサブジェクト名または SAN に一致するものが見つからない場合、または reference-identity サブモードコマンドで指定された FQDN が解決されない場合、接続は終了します。 reference-identity CLI は、AAA サーバーホスト設定および ddns 設定のサブモードコマンドとして設定されます。 新規/変更されたコマンド： ldap-over-ssl 、 ddns update method 、および show update method 。
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	
複数の DNS サーバーグループ	複数の DNS サーバーグループを使用できるようになりました。1つのグループがデフォルトで、他のグループを特定のドメインに関連付けることができます。DNS サーバーグループに関連付けられたドメインに一致する DNS 要求は、そのグループを使用します。たとえば、内部の eng.cisco.com サーバー宛てのトラフィックで内部の DNS サーバーを使用する場合は、 eng.cisco.com を内部の DNS グループにマッピングできます。ドメインマッピングと一致しないすべての DNS 要求は、関連付けられたドメインを持たないデフォルトの DNS サーバーグループを使用します。たとえば、 DefaultDNS グループには、外部インターフェイスで使用可能なパブリック DNS サーバーを含めることができます。 新規/変更されたコマンド： dns-group-map 、 dns-to-domain
ダイナミックログインのレート制限	ブロック使用量が指定されたしきい値を超えたときにログインレートを制限する新しいオプションが追加されました。ブロックの使用量が通常の値に戻るとレート制限が無効になるため、ログインレートを動的に制限されます。 新規/変更されたコマンド： logging rate-limit

機能	説明
Secure Firewall 3100 デバイスのパケットキャプチャ	スイッチパケットをキャプチャするプロビジョニングが追加されました。このオプションは、Secure Firewall 3100 デバイスに対してのみ有効にできます。 新規/変更されたコマンド： capture real-time
VPN 機能	
IPsec フローがオフロードされません。	Cisco Secure Firewall 3100 では、IPsec フローはデフォルトでオフロードされます。IPsec サイト間 VPN またはリモートアクセス VPN セキュリティ アソシエーション (SA) の初期設定後、IPsec 接続はデバイスのフィールドプログラマブルゲートアレイ (FPGA) にオフロードされるため、デバイスのパフォーマンスが向上します。 新規/変更されたコマンド： clear flow-offload-ipsec 、 flow-offload-ipsec 、 show flow-offload-ipsec
認証用の証明書と SAML	証明書および SAML 認証用にリモートアクセス VPN 接続プロファイルを設定できます。ユーザーは、SAML 認証/承認が開始される前に、マシン証明書やユーザー証明書を認証するように VPN を設定できます。これは、ユーザー固有の SAML DAP 属性と DAP 証明書属性を使用して実行できます。 新規/変更されたコマンド： authentication saml certificate 、 authentication certificate saml 、 authentication multiple-certificate saml

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。

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。

アップグレードパス：ASA アプライアンス

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。

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。

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 9.16 は ASA 5506-X、5508-X、および 5516-X の最終バージョンです。
 ASA 9.14 は ASA 5525-X、5545-X、および 5555-X の最終バージョンです。
 ASA 9.12 は ASA 5512-X、5515-X、5585-X、および ASASM 用の最終バージョン、
 ASA 9.2 は ASA 5505 の最終バージョンです。
 ASA 9.1 は ASA 5510、5520、5540、5550、および 5580 の最終バージョンです。

表 1: アップグレードパス

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
9.17	—	次のいずれかになります。 → 9.18
9.16	—	次のいずれかになります。 → 9.18 → 9.17
9.15	—	次のいずれかになります。 → 9.18 → 9.17 → 9.16
9.14	—	次のいずれかになります。 → 9.18 → 9.17 → 9.16 → 9.15

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
9.13	—	次のいずれかになります。 → 9.18 → 9.17 → 9.16 → 9.15 → 9.14
9.12	—	次のいずれかになります。 → 9.18 → 9.17 → 9.16 → 9.15 → 9.14
9.10	—	次のいずれかになります。 → 9.18 → 9.17 → 9.16 → 9.15 → 9.14 → 9.12
9.9	—	次のいずれかになります。 → 9.18 → 9.17 → 9.16 → 9.15 → 9.14 → 9.12

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	—	次のいずれかになります。 → 9.18 → 9.17 → 9.16 → 9.15 → 9.14 → 9.12
9.7	—	次のいずれかになります。 → 9.18 → 9.17 → 9.16 → 9.15 → 9.14 → 9.12 → 9.8
9.6	—	次のいずれかになります。 → 9.18 → 9.17 → 9.16 → 9.15 → 9.14 → 9.12 → 9.8

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	—	次のいずれかになります。 → 9.18 → 9.17 → 9.16 → 9.15 → 9.14 → 9.12 → 9.8
9.4	—	次のいずれかになります。 → 9.18 → 9.17 → 9.16 → 9.15 → 9.14 → 9.12 → 9.8
9.3	—	次のいずれかになります。 → 9.18 → 9.17 → 9.16 → 9.15 → 9.14 → 9.12 → 9.8

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	—	次のいずれかになります。 → 9.18 → 9.17 → 9.16 → 9.15 → 9.14 → 9.12 → 9.8
9.1(2)、9.1(3)、9.1(4)、9.1(5)、 9.1(6)、または 9.1(7.4)	—	次のいずれかになります。 → 9.14 → 9.12 → 9.8 → 9.1(7.4)
9.1(1)	→ 9.1(2)	次のいずれかになります。 → 9.14 → 9.12 → 9.8 → 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。 → 9.14 → 9.12 → 9.8 → 9.6 → 9.1(7.4)
9.0(1)	→ 9.0(4)	次のいずれかになります。 → 9.14 → 9.12 → 9.8 → 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
8.6(1)	→ 9.0(4)	次のいずれかになります。 → 9.14 → 9.12 → 9.8 → 9.1(7.4)
8.5(1)	→ 9.0(4)	次のいずれかになります。 → 9.12 → 9.8 → 9.1(7.4)
8.4(5+)	—	次のいずれかになります。 → 9.12 → 9.8 → 9.1(7.4) → 9.0(4)
8.4(1) ~ 8.4(4)	→ 9.0(4)	→ 9.12 → 9.8 → 9.1(7.4)
8.3	→ 9.0(4)	次のいずれかになります。 → 9.12 → 9.8 → 9.1(7.4)
8.2 以前	→ 9.0(4)	次のいずれかになります。 → 9.12 → 9.8 → 9.1(7.4)

アップグレードパス : Firepower 2100 の ASA (プラットフォームモード)

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、Firepower 2100 上のプラットフォームモードの ASA に対応する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になります。推奨バージョンは**太字**で示されています。

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。

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。

表 2: アップグレードパス

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
9.17	—	次のいずれかになります。 → 9.18
9.16	—	次のいずれかになります。 → 9.18 → 9.17
9.15	—	次のいずれかになります。 → 9.18 → 9.17 → 9.16
9.14	—	次のいずれかになります。 → 9.18 → 9.17 → 9.16 → 9.15
9.13	—	次のいずれかになります。 → 9.18 → 9.17 → 9.16 → 9.15 → 9.14

現在のバージョン	暫定アップグレードバージョン	ターゲットバージョン
9.12	—	次のいずれかになります。 → 9.18 → 9.17 → 9.16 → 9.15 → 9.14
9.10	→ 9.17	次のいずれかになります。 → 9.18
9.10	—	次のいずれかになります。 → 9.17 → 9.16 → 9.15 → 9.14 → 9.12
9.9	→ 9.17	次のいずれかになります。 → 9.18
9.9	—	次のいずれかになります。 → 9.17 → 9.16 → 9.15 → 9.14 → 9.12
9.8	→ 9.17	次のいずれかになります。 → 9.18

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	—	次のいずれかになります。 → 9.17 → 9.16 → 9.15 → 9.14 → 9.12

アップグレードパス : Firepower 4100/9300 用の ASA 論理デバイス

アップグレードについては、次のガイドラインを参照してください。

- **FXOS** : 2.2.2 以降では、上位バージョンに直接アップグレードできます。2.2.2 より前のバージョンからアップグレードする場合は、各中間バージョンにアップグレードする必要があります。現在の論理デバイスバージョンをサポートしていないバージョンにFXOSをアップグレードすることはできないことに注意してください。次の手順でアップグレードを行う必要があります。現在の論理デバイスをサポートする最新のバージョンにFXOSをアップグレードします。次に、論理デバイスをそのFXOSバージョンでサポートされている最新のバージョンにアップグレードします。たとえば、FXOS 2.2/ASA 9.8 から FXOS 2.13/ASA 9.19 にアップグレードする場合は、次のアップグレードを実行する必要があります。
 1. FXOS 2.2→FXOS 2.11 (9.8 をサポートする最新バージョン)
 2. ASA 9.8→ASA 9.17 (2.11 でサポートされている最新バージョン)
 3. FXOS 2.11→FXOS 2.13
 4. ASA 9.17→ASA 9.19
- **ASA** : ASA では、上記のFXOS要件に注意して、現在のバージョンから任意の上位バージョンに直接アップグレードできます。

表 3: ASA または Threat Defense、および Firepower 4100/9300 の互換性

FXOS のバージョン	モデル	ASA のバージョン	Threat Defense バージョン
2.14(1)	Firepower 4112	9.18	7.4 (推奨)
		9.17	7.3
		9.16	7.2
		9.15	7.1
		9.14	7.0
			6.7
		6.6	
	Firepower 4145	9.18	7.4 (推奨)
			7.3
			7.2
			7.1
			7.0
			6.7
	Firepower 9300 SM-56	9.15	6.6
Firepower 9300 SM-48	9.14		
2.13	Firepower 4112	9.18	7.3 (推奨)
		9.17	7.2
		9.16	7.1
		9.15	7.0
		9.14	6.7
			6.6
	Firepower 4145	9.18	7.3 (推奨)
			7.2
			7.1
			7.0
			6.7
			6.6
	Firepower 9300 SM-56	9.15	
Firepower 9300 SM-48	9.14		

FXOS のバージョン	モデル	ASA のバージョン	Threat Defense バージョン
2.12	Firepower 4112	9.18 (推奨) 9.17 9.16 9.15 9.14	7.2 (推奨) 7.1 7.0 6.7 6.6
	Firepower 4145 Firepower 4125 Firepower 4115	9.18 (推奨) 9.17 9.16	7.2 (推奨) 7.1 7.0
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40	9.15 9.14 9.12	6.7 6.6 6.4
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	9.18 (推奨) 9.17 9.16 9.15	7.2 (推奨) 7.1 7.0 6.7
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24	9.14 9.12	6.6 6.4

FXOS のバージョン	モデル	ASA のバージョン	Threat Defense バージョン
2.11	Firepower 4112	9.17 (推奨)	7.1 (推奨)
		9.16	7.0
		9.15	6.7
		9.14	6.6
	Firepower 4145	9.17 (推奨)	7.1 (推奨)
	Firepower 4125	9.16	7.0
	Firepower 4115	9.15	6.7
	Firepower 9300 SM-56	9.14	6.6
	Firepower 9300 SM-48	9.12	6.4
	Firepower 9300 SM-40		
	Firepower 4150	9.17 (推奨)	7.1 (推奨)
	Firepower 4140	9.16	7.0
	Firepower 4120	9.15	6.7
	Firepower 4110	9.14	6.6
	Firepower 9300 SM-44	9.12	6.4
	Firepower 9300 SM-36	9.8	
	Firepower 9300 SM-24		

FXOS のバージョン	モデル	ASA のバージョン	Threat Defense バージョン	
2.10 (注) 7.0.2+ および 9.16(3.11)+ との 互換性を確保す するには、FXOS 2.10(1.179)+ が必 要です。	Firepower 4112	9.16 (推奨) 9.15 9.14	7.0 (推奨) 6.7 6.6	
	Firepower 4145 Firepower 4125 Firepower 4115	9.16 (推奨) 9.15 9.14	7.0 (推奨) 6.7 6.6	
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40	9.12	6.4	
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	9.16 (推奨) 9.15 9.14 9.12	7.0 (推奨) 6.7 6.6 6.4	
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24	9.8		
	2.9	Firepower 4112	9.15 (推奨) 9.14	6.7 (推奨) 6.6
		Firepower 4145 Firepower 4125 Firepower 4115	9.15 (推奨) 9.14 9.12	6.7 (推奨) 6.6 6.4
		Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
		Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	9.15 (推奨) 9.14 9.12 9.8	6.7 (推奨) 6.6 6.4
		Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		

FXOS のバージョン	モデル	ASA のバージョン	Threat Defense バージョン
2.8	Firepower 4112	9.14	6.6 (注) 6.6.1+ では FXOS 2.8(1.125)+ が必要です。
	Firepower 4145 Firepower 4125 Firepower 4115	9.14 (推奨) 9.12 (注) Firepower 9300 SM-56 には ASA 9.12(2)+ が必要	6.6 (推奨) (注) 6.6.1+ では FXOS 2.8(1.125)+ が必要です。 6.4
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		6.4 6.2.3
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	9.14 (推奨) 9.12 9.8	6.6 (推奨) (注) 6.6.1+ では FXOS 2.8(1.125)+ が必要です。 6.4 6.2.3
2.6(1.157) (注) ASA 9.12+ および FTD 6.4+ では、同じ Firepower 9300 シャーシ内の別のモジュールで実行できるようになりました。	Firepower 4145 Firepower 4125 Firepower 4115	9.12 (注) Firepower 9300 SM-56 には ASA 9.12.2+ が必要	6.4
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	9.12 (推奨) 9.8	6.4 (推奨) 6.2.3
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		

FXOS のバージョン	モデル	ASA のバージョン	Threat Defense バージョン
2.6(1.131)	Firepower 9300 SM-48 Firepower 9300 SM-40	9.12	サポート対象外
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110		
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		
2.3(1.73)	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	9.8 (注) FXOS 2.3(1.130)+ を実行している 場合、フローオ フロードには 9.8(2.12)+ が必要 です。	6.2.3 (推奨) (注) 6.2.3.16+ には FXOS 2.3.1.157+ が必要
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		
2.3(1.66) 2.3(1.58)	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	9.8 (注) FXOS 2.3(1.130)+ を実行している 場合、フローオ フロードには 9.8(2.12)+ が必要 です。	
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		
2.2	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110 Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24	9.8	Threat Defense バージョンは サポートが終了しています

ダウングレードについての注記

FXOS イメージのダウングレードは公式にはサポートされていません。シスコがサポートする唯一のFXOSのイメージバージョンのダウングレード方法は、デバイスの完全な再イメージ化を実行することです。

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 でのみバグを探ることができます。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 \[英語\]](#) を参照してください。

バージョン 9.18(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。

ID	見出し
CSCwe47689	FXOS は、選択したフロー/パケットのカウントをタグ付けして表示するオプションを提供する必要がある
CSCwe68349	KP-HA で ACP の展開に失敗する
CSCwe98264	7.2.4-114 の KP ドライバコードで Snort3 がクラッシュする
CSCwf18926	スレッド名 PTHREAD-1549 での ASAv VMware のトレースバックとリロード
CSCwf63480	証明書の検証に失敗した後に Umbrella の登録が成功する
CSCwf65710	「show service policy」で現在の接続数が負になる - conn limit exceeded
CSCwh36906	スレッド名 PIM IPv4 での FTD トレースバック
CSCwh43230	強力な暗号化ライセンスが HA の ASA ファイアウォールに適用されない。
CSCwh47053	ASA/FTD がスレッド名「dns_cache_time」でトレースバックし、リロードすることがある

ID	見出し
CSCwh58090	ASA コード 9.18(3)53 で FP4110 が直接原因なしでクラッシュする
CSCwh58467	ASA が「warmstart」SNMP トラップを送信しない
CSCwh60504	WM : Lina が無効なオペコード (sig 4) により dispatch_lb_poll_worker でクラッシュする
CSCwh65128	LINA show tech-support が sf_troubleshoot.pl (トラブルシューティング ファイル) の一部として生成されない
CSCwh66359	CLI でロギングタイムスタンプを有効にした後に、ASDM がログのタイムスタンプを認識できない
CSCwh68482	ASA/FTD : プロセス名 lina でのトレースバック
CSCwh68964	FTD FP2100 : バックスラッシュ「\」を含むユーザー名で LDAP 外部認証が失敗することがある
CSCwh69346	ASA : CLI を使用して設定を復元する際のトレースバックとリロード
CSCwh69585	モジュールの 1 つで Cruz アダプタがダウンする
CSCwh69843	トランスペアレントモードの ASA が、すべてのノードに等しい IPv6 ルータアダプタイズメントパケットを送信しない
CSCwh71050	FXOS : NTP エントリの重複により、エラーメッセージが表示される : 到達不能または無効な NTP サーバー
CSCwh71161	ASA FTD : スレッド名 update_mem_reference でのトレースバックとリロード。
CSCwh71314	ASA/FTD : 誤った計算が原因でトレースバックが発生し、負の転送バイト数が memcopy 機能に渡される
CSCwh76458	Bidir PIM の使用時に mroute エントリがない場合、ASA/FTD でマルチキャストトラフィックがドロップされる。
CSCwh77348	ASA : クラスタ設定で「show nat pool detail」コマンドを実行すると、トレースバックとリロードが発生する
CSCwh78691	ASA/FTD がスレッド名「lina」でトレースバックし、リロードすることがある
CSCwh80716	PPPoE に接続されたインターフェイスが予期せずダウンすることがある

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 9.18(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。

ID	見出し
CSCvt25221	QoS ポリシー展開時のスレッド名 cli_xml_server での FTD トレースバック
CSCvu24703	FTD - フローオフロードはレート制限機能 (QoS) と共存できる必要がある
CSCvx04003	CP への ARP スロットリング欠如のミス表示により、オーバーサブスクリプションになる
CSCvx71936	FXOS : 障害「パスワード暗号化キーが設定されていません (The password encryption key has not been set.)」が FPR1000 および FPR2100 デバイスで表示された
CSCwa89116	MIB 用の IKEv2/SNMP/Session-mgr のセッションインデックス処理をクリーンアップする
CSCwa93215	DNS ルックアップでプライマリで HA フェールオーバーを実行すると、プライマリノードが VPN クラスタから切断される
CSCwa96920	プロセス Lina で ASA/FTD が トレースバック および リロード することがある
CSCwb24306	/mnt/disk0/log/asa_snmp.log の ログ エントリ が 重複 する
CSCwb44848	ASA/FTD が プロセス名 lina で トレースバック および リロード する
CSCwb66382	ASAv : 9344 ジャンボフレームを有効にした後にブロックが自動的に作成されず、OSPF MD5 が壊れる
CSCwb94431	発信インターフェイスリストが Null の場合、その他のドロップではなく MFIB RPF 失敗カウンタが増加する
CSCwb95453	ASA : 管理コンテキストによって生成されるすべてのログのタイムスタンプが同じである
CSCwc49180	92.13 で SNMP 統合を有効にした後に satsclient hap がリセットし、ブートループが発生する
CSCwc49655	FTPS が ssl3_get_record を取得 : KK および DR ルール接続中の不正なレコードの種類
CSCwc67031	NAT-T が有効なピンホール接続を備えた vti ハブがループし、snort ビジードロップを引き起こしている
CSCwc82205	ASA/FTD がスレッド名「lina」でトレースバックし、リロードすることがある

ID	見出し
CSCwvc87963	ASAv 「ライセンス情報を取得できません。後でもう一度お試しください (Unable to retrieve license info. Please try again later) 」
CSCwvc89924	内部データ 「no buffer」 インターフェイスカウンタをポーリングするための FXOS ASA/FTD の SNMP OID
CSCwvd02864	logging/syslog は、SNMP トラップとログ履歴の影響を受ける
CSCwvd04210	ASA : ASDMセッションが CLOSE_WAIT でスタックし、その結果 MGMT が不足する
CSCwvd07278	TCMがオフのとき、ユニットがクラスタに参加するときの ASA/FTD tmatch コンパイルチェック
CSCwvd09870	外部ブラウザとラウンドロビン DNS を使用した AnyConnect SAML が断続的に失敗する
CSCwvd10822	ディスク障害が原因で他のユニットの検査エンジンに障害が発生したため、フェールオーバーがトリガーされる
CSCwvd10880	2100/3100 デバイスでの重要な正常性アラート 「ユーザー設定 (FSM.sam.dme.AaaUserEpUpdateUserEp) 」である
CSCwvd16906	ASA/FTD がポリシー展開後にスレッド名 「lina」 でトレースバックし、リロードすることがある
CSCwvd22413	EIGRPv6 - LINA で 「mem_lock : アサーション mem_refcount' が失敗しました (mem_lock: Assertion mem_refcount' failed) 」でクラッシュした
CSCwvd23188	ASA/FTD がスレッド名 「lina」 でトレースバックし、リロードすることがある
CSCwvd30856	per-user-override が設定されている場合、vpn-filter のないユーザーが追加のアクセス権を取得できることがある
CSCwvd33054	DHCP リレーが DHCP オファーパケットをループバックしているため、FTD/ASA で dhcprelay が失敗する
CSCwvd34288	FP1000 : LINA モードでの起動プロセス中に、インターフェイス間のブロードキャストがリークし、ストームが発生する
CSCwvd37135	ASA/FTD がスレッド名 fover_fail_check でトレースバックおよびリロードする
CSCwvd38583	ASA/FTD : コマンド 「no snmp-server enable oid mempool」 がデフォルトで有効になっているか、アップグレード時に強制される
CSCwvd43666	/opt/cisco/config/var/log/ASAconsole.log の logrotate がいない理由を分析する

ID	見出し
CSCwd46741	fxos ログローテーションでファイルの循環に失敗し、ファイルサイズが大きくなる
CSCwd46780	ASA/FTD : スレッド名 appAgent_reply_processor_thread でトレースバックおよびリロードする
CSCwd53635	AWS : Geneve トンネルインターフェイスで SSL 復号が失敗する
CSCwd56296	FTD Lina がスレッド名「IP Init Thread」でトレースバックおよびリロードする
CSCwd58188	インラインペアの状態が、ハードウェアバイパスからスタンバイモードに自動回復できない。
CSCwd58528	QPHA アクティブノードでEMIX トラフィックプロファイルを実行している間のメモリの枯渇である
CSCwd59736	ASA/FTD : アップグレード中の SNMP グループ設定によりトレースバックおよびリロードする
CSCwd62138	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
CSCwd63961	属性値が大きすぎることによる、DAP ルールとの AC クライアントの一致の失敗
CSCwd66815	サポートのための Lina の変更 - FQDN ベースのトラフィックを処理する際に、Snort3 が daq-pdts でトレースバックする
CSCwd67101	FPR1150 : ease secure all を実行すると、実行形式エラーが表示され、リロードするまでデバイスがハングする
CSCwd68088	ASA/FTD : RFC 推奨事項に基づいて異なる TLS diffie-hellman 素数を導入する
CSCwd68346	カーネルクラッシュによる ASA MIO ブレードのハートビート障害で、メザニンコアが発生する
CSCwd68745	QEMU KVM コンソールが [カーネルを起動中 (Booting the kernel)] ページでスタックする
CSCwd69454	セカンダリユニットのポートチャネルインターフェイスは、リロード後に待機状態になる
CSCwd71254	ASA/FTD が idfw fqdn ハッシュルックアップでトレースバックおよびリロードすることがある
CSCwd72680	FXOS : FTD アクセス コントロール ポリシー展開中の高い CPU 使用率によってトリガーされる FP2100 FTW タイムアウト

ID	見出し
CSCwd74839	ユニットがクラスタに再参加するときの 30 秒以上のデータ損失
CSCwd78624	HA が設定された ASA は、複数の入出力エラーメッセージでトレースバックおよびリロードすることがある
CSCwd80343	7.0.4 を実行している MI FTD でディスク使用率が高い
CSCwd81123	プロセス smConlogger の FXOS での CPU 使用率が高い
CSCwd81538	peer_proxy_tx_q の 9344 ブロック枯渇による FTD トラフィック障害
CSCwd82235	LINA がスレッド名 update_cpu_usage 下の FPR-1010 でトレースバックする
CSCwd84046	Microsoft SCEP 登録で ASA ID 証明書の取得に失敗する - PKCS7 を確認できない
CSCwd84133	ASA/FTD がスレッド名「telnet/ci」でトレースバックおよびリロードすることがある
CSCwd84153	ASA/FTD がスレッド名「lina」でトレースバックし、リロードすることがある
CSCwd84868	フローオフロードが使用されていない場合に、いくつかの devcmd 障害と checkheaps トレースバックが発生する。
CSCwd85927	webvpn ユーザーが 36k 要素で DAP アクセスリストに一致する場合、トレースバックおよびリロードする
CSCwd86535	ASA/FTD : Netflow タイマーインフラでのトレースバックとリロード
CSCwd86929	カットスループロキシが HTTPS トラフィックで機能しない
CSCwd87438	syslog のロギングメカニズムの強化
CSCwd88585	ASA/FTD NAT プールクラスタの割り当てとユニット間の予約の不一致である
CSCwd89095	リロード後に Stratix5950 および ISA3000 LACP チャネルメンバー SFP ポートが一時停止になる
CSCwd89848	シャーシとブレード間のハートビート損失による ASA/FTD の障害
CSCwd91421	ASA/FTD が logging_cfg 処理でトレースバックおよびリロードすることがある
CSCwd92804	FPR2100 で FAN LED がオレンジに点滅する
CSCwd93376	クライアントレス VPN ユーザーが、WebVPN ポータルから大きなファイルをダウンロードできない

ID	見出し
CSCwd94096	ASA が別の認証および承認サーバーを使用している場合、Anyconnect ユーザーが接続できない
CSCwd94183	ssp_ntp.log ログローテーションの問題により、マルチインスタンスでの FXOS 更新のサポート後にブレードが起動しない
CSCwd95436	セカンダリの再起動時のプライマリ ASA のトレースバックである
CSCwd95908	ASA/FTD がトレースバックおよびリロードする、スレッド名 : rtcli async executor process
CSCwd96493	起動時に FPR1010 で数秒間リンクアップが見られる
CSCwd96500	FTD : FPR3100 で WebVPN キープアウトまたは証明書マップを設定できない
CSCwd96755	バックアップの実行時に ASA が予期せずリロードされる
CSCwd96766	41xx : ブレードが再起動信号をキャプチャまたはログに記録しない
CSCwd97020	ASA/FTD : 外部 IDP SAML 認証が「Bad Request」というメッセージで失敗する
CSCwe00864	クラスタの参加に失敗すると、ライセンスコマンドがクラスタデータユニットで失われる
CSCwe03529	PAT プールの展開中の FTD トレースバックとリロード
CSCwe03631	「logging history <mode>」でレート制限を指定する必要がある
CSCwe03991	tmatch コンパイルプロセス中に FTD/ASA がトレースバックおよびリロードする
CSCwe05913	FTD トレースバック/リロード - Icmp エラーパケット処理に snp_nat_xlate_identity が含まれる
CSCwe06562	FPR1K/FPR2K : サブインターフェイスの数が多いトランスペアレントモードでのフェールオーバー時間の増加
CSCwe07722	クラスタデータユニットが、ASP の理由「VPN reclassify failure」で非 VPN トラフィックをドロップする。
CSCwe08729	FPR1120 : HA でのスイッチオーバー後に接続がティアダウンされる
CSCwe09074	CRL チェックに失敗すると、トラストポイントの[なし (None)]オプションが機能しない
CSCwe09811	ポリシー展開の NAT ステートメントの追加/削除/編集集中に FTD がトレースバックおよびリロードする

ID	見出し
CSCwe10290	FTD が WSA からの GRE トラフィックをドロップする
CSCwe10548	設定が欠落している認証方式として LDAP を使用した ASA バインディングである
CSCwe11119	ASA : SNMP パケットの処理中にトレースバックおよびリロードする
CSCwe12407	SSL ハンドルのリークによる高 Lina メモリ使用量である
CSCwe12705	multimode-tmatch_df_hijack_walk トレースバックが、FO に接続したスイッチインターフェイスでのシャットダウン/シャットダウン解除中に観測される
CSCwe14174	FTD - メモリ割り当てに不適切な値を提供する「show memory top-usage」である
CSCwe14417	FTD : 宛先に到達可能になっても IPSLA プリエンプションが機能しない
CSCwe14514	キャプチャ設定の削除中のスタンバイユニットの ASA/FTD トレースバックとリロードである
CSCwe18472	[FTD Multi-Instance][SNMP] - CPU OID が、関連する CPU の不完全なリストを返す
CSCwe18974	ASA/FTD がスレッド名「CTMDaemon」でトレースバックおよびリロードすることがある
CSCwe20043	ASA5516 の FTD でジャンボフレームが有効になっている場合、256 バイトのメモリブロックが開始時に枯渇する
CSCwe20714	プライマリデバイスがアクティブな場合にトラフィックがドロップする
CSCwe20918	オープンな AC VPN Agent が単一の証明書とユーザー名/パスワードを使用してマルチ証明書認証 TG に接続できる
CSCwe21187	UDP タイムアウトが期限切れになるまで、ASP ドロップ理由 no-mcast-intrf により、ASA/FTD がマルチキャストパケットをドロップすることがある
CSCwe21280	マルチキャスト接続の確立またはティアダウン syslog メッセージが生成されない場合がある
CSCwe22302	wtmp ファイルがログローテーションされないため、パーティション「/opt/cisco/config」がいっぱいになる
CSCwe23039	NTP ポーリング頻度を 5 分から 1 秒に変更すると、役に立たない大きなログファイルが生成される

ID	見出し
CSCwe24532	/opt/cisco/platform/logs/ の下の nvram.out ログローテーションファイルの複数のインスタンス
CSCwe25342	ASA/FTD : snmp-server が設定されていない場合の SNMP 関連のメモリリーク動作
CSCwe26342	スレッド名 asacli/0 を示す ASA トレースバックとリロード
CSCwe26612	フェールオーバー スイッチオーバー後に FTD が OSPF 隣接関係を形成するのに想定以上に時間がかかる
CSCwe28094	VPN トンネルの作成時に「すべてのカウンタをクリア (clear counters all)」を実行した後、ASA/FTD がトレースバックおよびリロードすることがある
CSCwe28407	icmp_thread での LINA トレースバック
CSCwe28726	作成されたコンテキストを削除すると、コマンド「app-agent heartbeat」が削除される
CSCwe29179	CLUSTER : フロー所有者からの CLU 追加フロー要求よりも前に、ICMP 応答がディレクタに到着する
CSCwe29529	FTD MI が BVI に接続された VLAN 上の PVID を調整しない
CSCwe29583	ASA/FTD が lua_getinfo のスレッド名「None」でトレースバックおよびリロードすることがある
CSCwe29850	ASA/FTD Show chunkstat top コマンドの実装である
CSCwe30228	cf_reinject_hide フラグが原因で、ASA/FTD が関数「snp_fp_l2_capture_internal」でトレースバックすることがある
CSCwe30867	ローエンドプラットフォームで ntp ログから hwclock を設定するための回避策
CSCwe36176	ASA/FTD : 多数の (サブ) インターフェイスと HTTP サーバーが有効になっていると、フェールオーバーの遅延が大きくなる
CSCwe37453	共有管理インターフェイスを使用して、管理者およびユーザーコンテキストでスタンバイユニットからゲートウェイに到達できない
CSCwe38029	スタンバイユニットで複数のトレースバックが観察される。
CSCwe39425	2100 : 電源スイッチの切り替えにより、異常なシャットダウンが発生し、「PowerCycleRequest」がリセットされる

ID	見出し
CSCwe40463	ピアからの削除がない場合、同時 IKE SA 処理中に古い IKEv2 SA が形成される
CSCwe41336	データインターフェイスを管理として使用して 7.2.3 ベータ版をアップグレードした後、FDM WM-HA ssh が機能しない
CSCwe41898	ASA : FTD アクセス コントロール ポリシー展開中の高い CPU 使用率によってトリガーされる FP2100 FTW タイムアウトである
CSCwe42061	FTD インターフェイスで BVI を削除すると、他の BVI でパケットドロップが発生する
CSCwe44311	FP2100 : 再帰的なメッセージ <code>-<date>.1.gz rotated filenames</code> を回避するために LINA asa.log ファイルを更新する
CSCwe44672	Syslog ASA-6-611101 が 1 つの SSH 接続に対して 2 回生成される
CSCwe45093	per-user-override が設定されている場合、vpn-filter のないユーザーが追加のアクセス権を取得できることがある (IKEv2 RAVPN)
CSCwe45569	management-access が有効になっているために 7.0 から 7.2.x 以降への FTD アップグレードがクラッシュする
CSCwe45779	有効な隣接関係がないためにフローティング接続がデフォルト値でない場合、ASA/FTD は BVI へのトラフィックをドロップする
CSCwe50946	管理インターフェイスのリンクステータスが FXOS と ASA の間で同期されない
CSCwe50993	SFR モジュールの SNMP がダウンし、復旧しない
CSCwe51286	ASA/FTD がスレッド名「lina」でトレースバックし、リロードすることがある
CSCwe51443	OpenSSL の脆弱性の ASA 評価 CVE-2022-0778
CSCwe52120	tx checksum-offload が有効になっている場合、SSL 復号された接続が egress interface a pppoe で失敗する。
CSCwe54529	FPR2140 の FTD : TCP 正規化による Lina のトレースバックとリロード
CSCwe58207	logging history が有効になっている場合、ASA/FTD でメモリリークが発生する
CSCwe58700	ASA/FTD : クラスタイベントメッセージ「正常性チェックで左側のクラスタを制御していることが検出されました (Health check detected that control left cluster)」の改訂

ID	見出し
CSCwe59380	FTD : VRF ルーティングに依存する接続で「timeout floating-conn」が期待どおりに動作しない
CSCwe59737	p3_tree_lookup のウォッチドッグタイムアウトを指すトレースバックが原因で ASA/FTD がリブートする
CSCwe59919	スレッド名「NetSnmp Event mib process」での FTD トレースバックとリロード
CSCwe61928	FTD がデフォルトゲートウェイを使用して RP に到達している場合、リロード後に PIM 登録パケットが RP に送信されない
CSCwe61969	ASA マルチコンテキストの「management-only」インターフェイス属性が作成中に同期されない
CSCwe62361	ハートビートが失われ、「NPUとの通信が失われた」ために ASA がリブートする
CSCwe62703	複数のセッションが開かれている場合、新しい context サブコマンドが HA スタンバイで複製されない。
CSCwe62971	Umbrella DNS コネクタ設定を削除しようとする、ポリシー展開が失敗する
CSCwe62997	snmp_tracer_format_route での ASA/FTD トレースバックである
CSCwe63067	tcp インターセプト統計により、ASA/FTD がスレッド名「lina」でトレースバックし、リロードすることがある
CSCwe63232	ASA/FTD : クラスタ内のフローオフロード状態が同じであることを確認する
CSCwe63266	無効なファームウェア MF-111-234949 の障害/エラーが必要
CSCwe64043	リロード時に Cisco ASA および FTD ACL がインストールされない
CSCwe64404	ASA/FTD がトレースバックおよびリロードすることがある
CSCwe64557	ASA : サポートされていないプラットフォームで SFR モジュール設定を防止する
CSCwe64563	作成されたコンテキストを削除すると、コマンド「neighbor xxxx ha-mode graceful-restart」が削除された
CSCwe65245	SNMP ポーリング レートが非常に高い場合、FP2100 シリーズ デバイスが過剰なメモリを使用することがある
CSCwe65492	KP がデコードできない無効なコアファイルを生成する 7.2.4-64

ID	見出し
CSCwe65634	ASA : ACL DAP の同期中にスタンバイデバイスがトレースバックおよびリロードすることがある
CSCwe66132	ASA/FTD がスレッド名「lina」でトレースバックし、リロードすることがある
CSCwe67751	SIP IPv6 パケットの最後のフラグメントの MF は 1 であり、より多くのパケットが予想されることを示している
CSCwe67816	isakmp キャプチャを削除するときに、ASA/FTD がトレースバックおよびリロードする
CSCwe68159	フェールオーバーの fover_trace.log ファイルがフラッシュに書き込まれ、すぐに上書きされる
CSCwe70202	異なる「相手装置動作モード」が誤って認識されたため、フェールオーバーが複数回無効になる可能性がある。
CSCwe70378	接続がスタンバイ FTD に複製されない
CSCwe71220	Thead 名 CP Processing での FTD 3100 のクラッシュ
CSCwe71284	ASA/FTD がスレッド名「DATAPATH-3-21853」でトレースバックおよびリロードする必要がある
CSCwe72535	外部認証を使用して FTD にログインできない
CSCwe73116	クロスインターフェイスアクセス : VPN を介した管理アクセスインターフェイスへの ICMP ping が機能しない
CSCwe74059	logrotate によって 9.16 ASA または 7.0 FTD のファイルが圧縮されない
CSCwe74089	ASA/FTD がスレッド名「DATAPATH-1-1656」でトレースバックおよびリロードすることがある
CSCwe74328	AnyConnect - hostscan が有効な場合、モバイルデバイスは接続できない
CSCwe74916	リンクステートの伝達により、Inline-set でインターフェイスが DOWN を維持する
CSCwe76722	ASA/FTD : カスタム VRF を使用すると、from-the-box ping が失敗する
CSCwe77123	ASA/FTD : VPN ピア間に遅延がある場合の、IPSEC VPN を介した FPR2100 での TCP スループットの低下
CSCwe78977	ASA/FTD がスレッド名「pix_flash_config_thread」でトレースバックおよびリロードすることがある

ID	見出し
CSCwe79072	ASA/FTD がスレッド名「lina」でトレースバックし、リロードすることがある
CSCwe80063	ポートチャネルのサブインターフェイスのデフォルト DLY 値が親 PortChannel と一致しない
CSCwe81684	ASA : 「management-only」の解析でスタンバイ障害がパーサー/フェールオーバーサブシステムに報告されない
CSCwe82704	マルチインスタンス HA でデータ/データ共有として設定された PortChannel サブインターフェイスが「待機」状態になる
CSCwe83255	ASA/FTD がスレッド名「lina」でトレースバックし、リロードすることがある
CSCwe85432	SIP インспекションが有効になっていると、スレッド DATAPATH-14-11344 で ASA/FTD がトレースバックし、リロードする
CSCwe86225	スレッド名 cli_xml_server in tm_job_add を示す ASA/FTD のトレースバックとリロード
CSCwe87134	Lina コアが高トラフィックのテスト中に作成される
CSCwe88772	プロセス名 cli_xml_request_process での ASA のトレースバックとリロード
CSCwe89030	証明書のサブジェクト DN からのシリアル番号属性をユーザー名として使用する必要がある
CSCwe89731	サービスダウンの通知デーモン誤アラームである
CSCwe90095	証明書からのユーザー名 (Username-from-certificate) 機能は、電子メール属性を抽出できない
CSCwe90202	ASA : 動的設定変更の「management-only」の解析時にスタンバイ障害が発生する
CSCwe90720	ha_msg の破損による解析スレッドでの ASA のトレースバックとリロード
CSCwe92905	ngfwManager プロセスが継続的に再起動し、ZMQ Out of Memory のトレースバックが発生する
CSCwe93202	FXOS REST API : タイプ「ecdsa」のキーリングを作成できない
CSCwe93489	threat-detection がプレフィックス付き IPv6 の例外オブジェクトを認識しない
CSCwe93532	ASA/FTD がスレッド名「lina」でトレースバックし、リロードすることがある

ID	見出し
CSCwe93537	threat-detectionで個々の IPv6 エントリをクリアできない
CSCwe93561	Cisco ASA および FTD VPN Web クライアントサービスのクライアント側要求のスマグリングの脆弱性
CSCwe94287	複数の DHCP サーバーが設定されている場合、FTD DHCP リレーが NACK をドロップする
CSCwe95729	Cisco ASA および FTD SAML 認証バイパスの脆弱性
CSCwe95757	ASA/FTD がスレッド名「lina」でトレースバックし、リロードすることがある
CSCwe96023	ASA/FTD : 6.6.5 から 7.0.1 へのアップグレード直後の SNMP 関連のトレースバックとリロード
CSCwe96068	ASA : CLU RX/TX キューでの大量のアンダーラン/オーバーランに対する設定可能な CLU
CSCwe97277	VPN トラフィックの実行中にヒットレスアップグレードを実行すると、ASA のトレースバックとリロードが観察される
CSCwe98687	7.2.4 : 単一の巧妙に細工された UDP SIP 登録要求を使用したブロックの枯渇
CSCwe99040	tcpmod_proxy_continue_bp プロセスでのスレッドデータパスのトレースバックとリロード
CSCwe99550	asa log infra でファイル固有のロギングを一時停止/再開するノブを追加。
CSCwf00865	一方のスポークで IPSec フローがオフロードされ、もう一方でオフロードされていない場合、FTD/ASA ハブアンドスポーク (U ターン) VPN が失敗する
CSCwf01064	9.18.2 以降、TCP ping が全く機能しない
CSCwf04831	ASA/FTD がスレッド名「ci/console」でトレースバックし、リロードすることがある
CSCwf04870	ASA : 「Ping<ifc_name> xxxx」が 9.18.x 以降、期待どおりに機能しない
CSCwf05295	FP1000 シリーズで実行されている FTD が、「Client Hello」メッセージの後の TLS フローのパケットをドロップすることがある。
CSCwf06377	BS および QP のハートビートタイムアウトを 6 秒に設定
CSCwf07791	ASA で SNMP PDU および SNMP VAR チャンクが不足している
CSCwf08043	フラグメント化されたパケットによる Lina のトレースバックとリロード

ID	見出し
CSCwf08515	FPR3100 : ASA/FTD の高トラフィックがすべてのデータインターフェイスに影響し、「demux drops」のカウンタが高い値を示す
CSCwf10910	FTD : 7.3.0 を実行している ZMQ でのトレースバック
CSCwf12005	ASA が user-agent と host なしで OCSP 要求を送信する
CSCwf12408	ASA : 9.16.4 へのアップグレード後、最初のリブート時にすべてのタイプ 8 パスワードが失われる
CSCwf12985	FTDv : dpdk プールの枯渇と rx_buff_alloc_failure による VMware 展開でのトラフィック障害
CSCwf14126	プロセス名 Lina を示す ASA のトレースバックとリロード
CSCwf14735	Nat/Pat に関連する、プロセス名 lina での ASA のトレースバックとリロード
CSCwf14811	TCP ノーマライザには、パケットドロップなどのアクションを示す統計が必要
CSCwf15858	大量の認証プロファイルを送信するユーザーに対して SSL を介した LDAP 認証が機能しない
CSCwf15863	非常に限定的な「vpn-idle-timeout」値により、SSL セッションの切断と再接続が継続的に発生する。
CSCwf15902	Hyper-V の ASA v が管理インターフェイスでパケットをドロップする
CSCwf17042	ASDM が、バックアップ復元時にクラス インспекション オプションでカスタムの policy-map をデフォルトマップに置き換える。
CSCwf17814	ASA/FTD がスレッド名「19」でトレースバックし、リロードすることがある（空きブロックチェックサムエラー）
CSCwf20338	ASA がスレッド名「DHCPv6 Relay」でトレースバックおよびリロードすることがある
CSCwf21106	ASA/FTD : SNMP およびインターフェイスの変更中の、スレッド名 snmp_master_callback_thread でのトレースバック
CSCwf22005	ASA packet-tracer が常に最初の ACL ルールを表示するが、正しい ACL と一致する
CSCwf22483	シャーシへの SSH により、設定で許可されていない IP の 3 ウェイハンドシェイクが可能

ID	見出し
CSCwf23564	パススルーデバイスとして GRE TUNNEL および FTD を介した MD5 認証を使用すると、BGP を確立できない
CSCwf26407	FP2130 : ポートチャネルのメンバーの関連付けを解除できず、展開に失敗し、FTD/FMC でメンバーが失われる
CSCwf26534	ASA/FTD : SIP-SDP ヘッダーの接続情報が、destination static Any で変換されないままになる
CSCwf26939	FTD がエラー「IPv4 宛先の実際のオブジェクトアドレス範囲が広すぎます (IPv4 dst real obj address range is huge)」で NAT ルールの作成に失敗することがある
CSCwf28488	emblem が設定され、buffer logging が debug に設定されている場合に一貫性のないログメッセージが表示される
CSCwf30716	マルチコンテキストの ASA で、MIO HB のリカバリ後でもスタンバイデバイスが失敗状態で表示される。
CSCwf30727	validation-usage ssl-server を使用しない場合、ASA と Umbrella の統合が機能しない。
CSCwf30824	CIMC IPMI ハングの問題の自動リカバリとして CIMC リセットを追加
CSCwf31701	スレッド名 **CP Crypto Result Processing** での ASA トレースバックとリロード
CSCwf31820	グローバル VRF またはユーザー VRF 間のルーティング時にファイアウォールがパケットをドロップすることがある
CSCwf33574	アップグレード後に ASA access-list エントリのハッシュが同じになる
CSCwf33904	[IMS_7_4_0] - 仮想 FDM のアップグレードが失敗する : UpgradeOnStandby 実行後に HA configStatus='OUT_OF_SYNC となる
CSCwf34500	FTD : GRE トラフィックが CPU コア間で負荷分散される
CSCwf35207	ASA : ASA で ACL を更新中にトレースバックとリロードが発生する
CSCwf35233	シスコの適応型セキュリティ アプライアンス ソフトウェアと Firepower Threat Defense の DoS
CSCwf35500	FXOS/SSP : システムでの DIMM の修正可能なエラーイベントの可視性が向上する
CSCwf35573	TLS サーバーのアイデンティティプロブのタイムアウトが長すぎると、トラフィックが影響を受ける可能性がある

ID	見出し
CSCwf37160	証明書グループマップが設定されている場合、AnyConnect Ikev2 ログインに失敗する
CSCwf39163	ASAv : snmpwalk 実行中の ICMP ping パケットにより Azure 環境で高遅延が発生する
CSCwf42144	プロセス名「Lina」を示す ASA/FTD のトレースバックが発生することがある
CSCwf43288	クラスタ構成のセットアップで、スレッド名「ssh/client」でのトレースバックが発生する
CSCwf43537	FTD クラスタのアップグレード中にスレッド名 cli_xml_request_process で Lina がクラッシュする
CSCwf44537	nat_remove_policy_from_np で 99.20.1.16 lina がクラッシュする
CSCwf47227	priority-queue コマンドにより、すべてのポートチャネルインターフェイスでサイレント出力パケットがドロップされる
CSCwf47924	Cisco ASA および FTD VPN Web クライアントサービスのクライアント側要求のスマグリングの脆弱性
CSCwf48599	廃止された暗号を使用した VPN ロードバランシング クラスタ暗号化
CSCwf49573	ASA/FTD : 「show memory webvpn all objects」を発行する際のトレースバックとリロード
CSCwf50497	DNS キャッシュエントリの枯渇によりトレースバックが発生する
CSCwf51933	アップグレード後にドット付きの FTD ユーザー名が AAA-RADIUS 外部認証ログインに失敗する
CSCwf52810	ASA SNMP ポーリングが機能せず、show コマンドで「Unable to honour this request now」と表示される
CSCwf54418	重複検出後に形成された古い IKEv2 SA のクリアにかかる時間の短縮
CSCwf54510	スレッド名 DHCPRA Monitor での ASA トレースバックおよびリロード
CSCwf56811	メモリヘッダー検証によるプロセス名 lina での ASA トレースバックとリロード
CSCwf58876	KP2140-HA、リロードされたプライマリユニットがピアユニットを検出できない
CSCwf59571	FTD/Lina : ローエンドプラットフォームでの Msglyr プールメモリの減少により ZMQ が OUT OF MEMORY を発行する。

ID	見出し
CSCwf60311	9.16.4.19 へのアップグレード後に スレッド名 DATAPATH-53-18309 で ASA でトレースバックが発生する
CSCwf60590	トランスペアレントモードの FTD で「show route all summary」を実行すると、CLISH の動作が遅くなる。
CSCwf62729	非 FIPS モードと FIPS モードの両方で異常トラフィックが発生している RAVPN インターフェイスで Lina がクラッシュする
CSCwf62885	AWS GWLB の背後にある FTDv シングルアームプロキシが、geneve-invalid-udp-checksum が原因でドロップする
CSCwf63872	フェールオーバー スイッチオーバー後に FTD が OSPF 隣接関係を形成するのに想定以上に時間がかかる
CSCwf71606	リロード時に Cisco ASA および FTD ACL がインストールされない
CSCwf71812	FTD Lina エンジンが、アサーションが原因でデータパスでトレースバックすることがある
CSCwf72434	最大数に関するシステム制限ルールに達したときに意味のあるログを追加
CSCwf72510	HA の両方のデバイスが FMC にイベントを送信しないようにする
CSCwf73189	NAT 障害により、FTD が WSA からの GRE トラフィックをドロップする
CSCwf73773	最後の 20 の rmu 要求応答パケットのダンプに失敗する
CSCwf75214	リロード後にキー文字列がバックスラッシュ「\」で終わる場合、ASA は IKEv2 リモート PSK を削除する
CSCwf77191	ASA アプライアンスモード - 「connect fxos [admin]」で「ERROR: failed to open connection」が返される。
CSCwf78321	ASA : クライアントレス WebVPN によるチェックヒープのトレースバックとリロード
CSCwf81058	FTD : [有効 (Enabled)] と表示される Firepower 3100 の動的フローオフロード
CSCwf82247	ルートの同じプレフィックス/メトリックが別の VRF で設定されている場合、ポリシーの展開が失敗する。
CSCwf85757	Cisco ASA ソフトウェアおよび FTD ソフトウェアの SAML アサーションのハイジャックの脆弱性
CSCwf87070	WM RM : SFP ポート 9 のステータスが SFP 10 11 12 のポートの状態の後に表示される

ID	見出し
CSCwf88124	トランクモードのスイッチポートが、電力損失後に VLAN トラフィックを通過させない
CSCwf88552	ASA/FTD : NAT L7 インспекションの書き換えによるトレースバックとリロード
CSCwf92135	ASA : スレッド名「fover_FSM_thread」および「ha_ntfy_prog_process_timer」でのトレースバックとリロード
CSCwf92646	EC521 の SHA384 を使用した ECDSA 自己署名証明書
CSCwf94677	両方の HA ユニットが同時にリロードされた後、「failover standby config-lock」設定が失われる
CSCwf95147	OSPFv3 トラフィックがトランスペアレントモードで一元化される
CSCwf96938	FMC : UDP ポート 6081 を使用した ACP ルールが後続の展開後に削除される
CSCwh00692	トレースバック @<capture_file_show+605 at ../infrastructure/capture/capture_file_finesse.c:282>
CSCwh02457	AWS 上の ASA v を 9.18.2 以降の任意のバージョンにアップグレードした後、Radius 認証が機能しない
CSCwh04365	メモリヘッダー検証によるプロセス名 lina での ASA トレースバックとリロード- webvpn 側の修正
CSCwh04395	マルチコンテキストセットアップで ASDM アプリケーションがランダムに終了または中断し、アラートメッセージが表示される
CSCwh04730	メモリバッファが破損している場合に ASA/FTD HA checkheaps がクラッシュする
CSCwh06452	OID.1.3.6.1.2.1.2.2 を使用した SNMP 応答のインターフェイス速度の不一致
CSCwh08481	FreeB および VPN 機能を使用した Lina プロセスでの ASA トレースバック
CSCwh08683	FTDv/AWS : Lina と FTD クラスタ間の NTP クロックオフセット
CSCwh11764	ASA/FTD が、スレッド名「RAND_DRBG_bytes」および n5 プラットフォーム上の CTM 機能でトレースバックおよびリロードすることがある
CSCwh13474	PSEQ (Power-Sequencer) ファームウェア - device-id のチェックを削除
CSCwh13821	キャプチャバッファサイズを変更すると、ASA/FTD がトレースバックおよびリロードすることがある

ID	見出し
CSCwh23100	Cisco ASA および FTD ソフトウェアのリモートアクセス VPN の不正アクセスの脆弱性
CSCwh23100	Cisco ASA および FTD ソフトウェアのリモートアクセス VPN の不正アクセスの脆弱性
CSCwh23567	リロード時にスタンバイで PAC キーファイルが欠落している
CSCwh27230	インターフェイスがインラインモードの場合、アイドルタイムアウト後に接続がクリアされない。
CSCwh28144	特定の OID 1.3.6.1.2.1.25 が応答しない
CSCwh30891	SNMPV3 設定の追加時に ASA/FTD がスレッド名「ssh」でトレースバックおよびリロードすることがある
CSCwh31495	FTD : CPU コアによって NAT ルールが削除されたことによるトレースバックとリロード
CSCwh37733	FTD が MAC アドレス 0000.000.000 で UDP500 パケットに応答する
CSCwh41127	ASA/FTD : スタンドアロン ASA の「overlaps with inside standby interface address」 NAT64 エラー
CSCwh45108	Cisco ASA および FTD ソフトウェアのリモートアクセス VPN の不正アクセスの脆弱性
CSCwh45108	Cisco ASA および FTD ソフトウェアのリモートアクセス VPN の不正アクセスの脆弱性
CSCwh49483	show inventory all の実行中に ASA/FTD がトレースバックおよびリロードすることがある

バージョン 9.18(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。

ID	見出し
CSCvz34289	場合によっては、軽量プロキシへの移行が Do Not Decrypt フローで機能しない
CSCvz36903	クラスタのキープアライブパケットに新しいブロックを割り当てている間に ASA でトレースバックとリロードが発生する
CSCvz41551	FP2100 : 脅威検出統計を備えた ASA/FTD が、スレッド名「lina」でトレースバックおよびリロードすることがある

ID	見出し
CSCvz71596	「アクティブとスタンバイのインターフェイスの数が一致していません」という警告の syslog がトリガーされるはずである
CSCwa04262	Cisco ASA ソフトウェアの SSL VPN クライアント側リクエストの、「/」URI を介したスマグリングの脆弱性
CSCwa36535	構成サイズが大きいため、スタンバイユニットがフェールオーバーの参加に失敗
CSCwa59907	LINA は、スレッド名「snmp_client_callback_thread」でトレースバックを観察した
CSCwa72929	プライバシーアルゴリズムの AES192 または AES256 を使用した場合、SNMPv3 ポーリングが失敗することがある
CSCwa74063	NLP への管理アクセスが有効になった後、NLP ルールのインストールの回避策が無効になる
CSCwa82850	ASA フェールオーバーで、参加ノードを「スタンバイ準備完了」と宣言する前にコンテキストの不一致が検出されない
CSCwa97917	電源再投入後に ISA3000 がブートループの状態になる
CSCwb00871	ENH : 拡張時またはストレス時のウォッチドッグを減らすために log_handler_file の遅延を削減
CSCwb03704	ASA/FTD データパススレッドがデッドロックに陥り、トレースバックを生成することがある
CSCwb04000	ASA/FTD : VTI にルーティングされるパケットに DF ビットが設定されている
CSCwb05291	Cisco ASDM および ASA ソフトウェアのクライアント側で任意のコードが実行される脆弱性
CSCwb31551	インバウンドパケットに SGT ヘッダーが含まれている場合、FPR2100 が 5 タプルごとに適切に配布できない
CSCwb44848	ASA/FTD がプロセス名 lina でトレースバックおよびリロードする
CSCwb89963	スレッド名 : 「Datapath」 での ASA トレースバックとリロード
CSCwc02488	ASA/FTD がスレッド名「None」でトレースバックし、リロードすることがある
CSCwc03069	インターフェイスの internal data0/0 は cli からは up/up になるが、SNMP ポーリングからは up/down になる

ID	見出し
CSCwvc03332	FP2100 の FTD が、リブートプロセス中に HA アクティブユニットとして引き継ぐことができる
CSCwvc03507	CPU ホグの証拠がほとんどないにもかかわらず、内部データインターフェイスでのバッファドロップがない
CSCwvc07262	スタンバイ ASA が、9.16(3) へのアップグレード後、設定の複製中にブートループになる。
CSCwvc08646	SSH クライアントからログインすると、パスワードのないユーザーがパスワードの変更を求められる
CSCwvc10145	FTDv クラスタユニットがクラスタに再参加せず、エラーメッセージ「NLP SSL リスニングソケットを開けませんでした」が表示される
CSCwvc10241	アップグレードまたはデバイスのリブート後の一時的な HA スプリットブレイク
CSCwvc10483	ASA/FTD がスレッド名「appAgent_subscribe_nd_thread」でトレースバックする
CSCwvc11511	FTD: 7.0.2 へのアップグレード後の SNMP エラー
CSCwvc11597	SFR が 6.7.0.3 にアップグレードされると、ASA のトレースバックが発生する
CSCwvc13017	../inspect/proxy.h:439 で FTD/ASA のトレースバックとリロードが発生する
CSCwvc18524	コマンド「show environment」で ASA/FTD 電圧情報が不足している
CSCwvc23844	空きメモリが 30% を超えているにもかかわらず、ASA の CPU およびスタックメモリの割り当てエラーが高い
CSCwvc24906	スレッド ID 1637 で ASA/FTD のトレースバックとリロードが発生する
CSCwvc26648	ASA/FTD がスレッド名 Lina または Datatath でトレースバックおよびリロードする
CSCwvc27846	アップグレードとリロードの後の HA 同期中にトレースバックおよびリロードする。
CSCwvc28334	Cisco ASA および FTD ソフトウェアの RSA 秘密キーリークの脆弱性
CSCwvc28532	インラインセットインターフェイスの内部フロー処理によってフラグメント化された GRE トラフィックが原因で、9344 ブロックでリークが発生する
CSCwvc28806	プロセス名 Lina で ASA がトレースバックし、リロードする

ID	見出し
CSCwc28928	ASA : VTY セッションで SLA デバッグが表示されない
CSCwc31457	クリアテキストトークンを使用した ASA プロセス (暗号化できない場合)
CSCwc32246	オブジェクトサブネット 0.0.0.0 0.0.0.0 が使用されている場合、NAT64 はすべての IPv6 アドレスを 0.0.0.0/0 に変換する
CSCwc36905	「slib_malloc.c でヒープメモリが破損」した結果、ASA がトレースバックしリロードする
CSCwc37256	アップグレード後に SSL AnyConnect アクセスがブロックされる
CSCwc38567	SCH コードの実行中に ASA/FTD がトレースバックおよびリロードする場合があります
CSCwc40352	Lina NetFlow から許可されたイベントが Stealthwatch に送信され、後で Snort によってブロックされる
CSCwc40381	ASA : カットスループロキシが有効になっている場合の HTTPS トラフィック認証の問題
CSCwc44289	FTD : IPv4 <> IPv6 NAT 変換を実行するときのトレースバックとリロード
CSCwc45108	ASA/FTD : 9344 サイズのブロックリークを引き起こす GTP インスペクション
CSCwc45397	ASA HA : プライマリの復元で、バックアップ後に行われた新しいインターフェイス設定が削除されない
CSCwc45575	nopassword キーワードを持つユーザー名を使用した ssh の場合、ASA/FTD がトレースバックおよびリロードする
CSCwc47962	ASA : 「no monitor-interface service-module」 コマンドがリロード後になくなる
CSCwc48375	インバウンド IPSEC SA が非アクティブのままスタックする : 「show crypto ipsec sa」 の 1 つのアウトバウンド SPI に対して多数のインバウンド SPI がある
CSCwc49095	フラグメントが結合されて PDTS に送信される場合、ASA/FTD 2100 プラットフォームがトレースバックおよびリロードする
CSCwc50887	FTD : CCL リンク経由でリダイレクトされる UDP フローの NAT IPv4 <> IPv6 でのトレースバックとリロード
CSCwc50891	MPLS タギングが FTD によって削除される

ID	見出し
CSCwc51326	FXOS ベースの Firepower プラットフォームで、RX リングウォーターマークの値が高いにもかかわらず、「バッファなし」ドロップを示す
CSCwc52351	「any」およびグローバル IP/範囲がブロードキャスト IP に一致する NAT が原因で起こる ASA/FTD クラスタスプリットブレイン
CSCwc53280	ASA パーサーが OSPF プロセスの下で不完全なネットワークステートメントを受け取り、show run に表示される
CSCwc54217	FPR2140 でフェールオーバーに関する syslog が出力されない
CSCwc54984	IKEv2 キーの再生成 : Create_Child_SA 応答の直後に受信した新しい SPI に対して無効な SPI を応答する
CSCwc60037	ASA が IPSEC エラーでキーの再生成に失敗する: アウトバウンドハードウェア コンテキストの割り当てに失敗する
CSCwc61912	ASA/FTD OSPFv3 が IPv6 のメッセージタイプ 8 LSA を生成しない
CSCwc64923	ASA/FTD がスレッド名「lina」IP ルーティング「ndbshr」でトレースバックおよびリロードすることがある
CSCwc66757	ASA/FTD がスレッド名「lina」でトレースバックし、リロードすることがある
CSCwc67687	ASA HA フェールオーバーによって HTTP サーバーの再起動の失敗と ASDM の停止がトリガーされる
CSCwc67886	ASA/FTD がスレッド名「lina_notify_file_monitor_thread」でトレースバックおよびリロードすることがある
CSCwc70962	FTD/ASA の「書き込みスタンバイ」により ECDSA 暗号が有効になり、AC SSLv3 ハンドシェイクが失敗する
CSCwc72155	ASA/FTD が関数「snp_cluster_trans_allocb」でトレースバックおよびリロードする
CSCwc72284	TACACS アカウンティングに、クライアントの誤った IPv6 アドレスが含まれる
CSCwc73224	スタンバイデバイスの Call Home 設定がリロード後に失われる
CSCwc74103	ASA/FTD がスレッド名「DATAPATH-11-32591」でトレースバックおよびリロードすることがある
CSCwc74858	FTD : スレッド名 DATAPATH でのトレースバック
CSCwc77519	FPR1120-ASA : リロード後にプライマリがアクティブロールになる

ID	見出し
CSCwc77680	ASA/FTD がスレッド名「DATAPATH-0-4948」でトレースバックおよびリロードすることがある
CSCwc77892	起動後の ASA syslog の CGroups エラー
CSCwc79366	展開中に、デバイスが構成要求の処理中にスタックする
CSCwc80234	アクティブとスタンバイ間の「inspect snmp」設定が異なる
CSCwc81184	ASA/FTD が SNMP プロセス障害によりトレースバックおよびリロードする
CSCwc81945	インターフェイス NAT を備えた GCP クラスタで、データユニットのトラフィックが「LU allocate xlate failed」でドロップされる
CSCwc81960	アクセスリストでオブジェクトグループを使用すると、ルートマップで「match ip address」を設定できない
CSCwc82124	9.18.2 へのアップグレード後、ASA NAT ルールが期待どおりに機能しない
CSCwc82188	FMC UI から長いキャプチャコマンドを適用した場合、FTD がトレースバックおよびリロードする
CSCwc83346	ASA/FTD がスレッド名 IKE Daemon でトレースバックおよびリロードする
CSCwc88897	DNS インспекションポリシー変更後の Cisco Umbrella のヌルポインタが原因で ASA がトレースバックおよびリロードする
CSCwc89924	内部データ「no buffer」インターフェイスカウンタをポーリングするための FXOS ASA/FTD の SNMP OID
CSCwc90091	ユーザー統計がある ASA 9.12(4)47 が、「policy-server xxxx global」の可視性に影響する
CSCwc93166	ユーザーコンテキストで write standby を使用すると、セカンダリファイアウォールのライセンスステータスが無効な状態のままになる
CSCwc93964	ASA が、メモリトラッキング中に Unicorn スレッドで WebVPN トレースバックを使用する
CSCwc94085	6.6.5 からのアップグレード後、FIPS が有効になっている DTLSv1.2 を確立できない
CSCwc94466	Cisco ASA/FTD Firepower 2100 SSL/TLS におけるサービス妨害攻撃に対する脆弱性
CSCwc94501	ASA/FTD が ctm_n5 リセットによりトレースバックする

ID	見出し
CSCwc94547	「debug menu fxos_parser 4」発行時に Lina がトレースバックおよびリロードする
CSCwc95290	vpn-context に ESP ルールがないため、IPSec トラフィックがドロップすることがある
CSCwc96805	スレッド unicorn の tcp インターセプト統計によりトレースバックおよびリロードする
CSCwc99242	リロード後に ISA3000 LACP チャンネルメンバー SFP ポートが中断状態になる
CSCwd00386	「snp_clear_acl_log_flow_all」が原因で設定をクリアすると、ASA/FTD がトレースバックおよびリロードすることがある
CSCwd00778	SNMP ポーリングによる ifAdminStatus の出力が異常
CSCwd02864	バッファへのロギングに影響を与えるバッファサイズの変更
CSCwd03793	FTD トレースバックとリロード
CSCwd03810	アップグレード後に ASA カスタムログインページが webvpn 経由で機能しない
CSCwd04210	ASA : ASDM セッションが CLOSE_WAIT でスタックし、その結果 MGMT が不足する
CSCwd05756	syslog コンポーネントによる Lina の FTD トレースバック
CSCwd06005	ノード離脱中に ASA/FTD クラスタがトレースバックおよびリロードする
CSCwd09870	外部ブラウザとラウンドロビン DNS を使用した AnyConnect SAML が断続的に失敗する
CSCwd11303	ikev2 プロセスで ASA がトレースバックを生成し、リロードすることがある
CSCwd11855	ASA/FTD がスレッド名「ikev2_fo_event」でトレースバックおよびリロードすることがある
CSCwd14972	ASA/FTD がスレッド名 pix_flash_config_thread でトレースバックおよびリロードする
CSCwd16294	GTP インスペクションで、オプションの IE ヘッダー長が短すぎると、パケットがドロップされる
CSCwd16517	GTP ドロップが、バッファと syslog に常に記録されない
CSCwd16689	ASA/FTD がブロックデータの破損によりトレースバックする

ID	見出し
CSCwd17856	ASA が「snmp_ma_kill_restart: vf is NULL」というメッセージでトレースバック/リロードする
CSCwd18744	FTD 「Other unit has different set of hwidb index」により HA に参加できない
CSCwd19053	ASA/FTD が、配布リストを使用して多数のネットワークオブジェクトの展開をトレースバックすることがある
CSCwd20627	ASA/FTD : NAT 設定の展開の失敗
CSCwd22349	ASA : 「定期認証証明書」が有効になっている AnyConnect 証明書ベースの認証に接続できない
CSCwd22907	SNMP 通知スレッドでの ASA/FTD の高い CPU 使用率
CSCwd23188	ASA/FTD がスレッド名「lina」でトレースバックし、リロードすることがある
CSCwd23913	プレフィックスリストを使用して BGP ネイバーを追加した後に、HA の FTD が複数回トレースバックする。
CSCwd25201	SNMP トラップサーバーが設定されていない場合に、ASA/FTD の SNMP トラップがキューに入れられる
CSCwd25256	TCM が有効になっている状態で、access-group 以外のコマンドが 2 回無効になると、新しい ACL が ASA で機能しない
CSCwd26867	リブートがトリガーされたら、デバイスがアクティブ状態に移行しない必要がある
CSCwd28236	アクティブ IP とスタンバイ IP の両方を使用しているスタンバイユニットが、nat 「any」により重複 IP の問題の原因となる
CSCwd31181	Lina がトレースバックおよびリロードする : VPN 親チャンネル (SAL) に無効な基盤となるチャンネルがある
CSCwd31960	カスタム NAT が設定されている場合、VPN 経由の管理アクセスが機能しない
CSCwd37135	ASA/FTD がスレッド名 fover_fail_check でトレースバックおよびリロードする
CSCwd38805	Syslog 106016 がデフォルトでレート制限されていない
CSCwd39468	LINA がスレッド名 ci/console でトレースバックおよびリロードする

ID	見出し
CSCwd40260	有用性の強化：ペイロードを解析できない場合、ASA/FTD によってサイレントにドロップされる
CSCwd41083	ASA が DNS インスペクションによりトレースバックおよびリロードする
CSCwd42620	説明にエスケープされた値を含むオブジェクトを展開すると、以降のすべての展開が失敗する可能性がある
CSCwd46780	ASA/FTD：スレッド名 appAgent_reply_processor_thread でトレースバックおよびリロードする
CSCwd48633	ASA：Webvpn ポータルが使用されている場合にトレースバックおよびリロードする
CSCwd50218	ASA の復元で vlan 設定が適用されない
CSCwd51757	接続レート OID の SNMP GET を使用してポーリング結果を取得できない
CSCwd53135	ASA/FTD：しきい値を超えるフローのオブジェクトグループ検索 Syslog
CSCwd53340	snort が 4085～4096 バイトのサイズのメッセージを送信すると、FTD PDTS LINA RX キューがスタックすることがある
CSCwd53635	AWS：Geneve トンネルインターフェイスで SSL 復号が失敗する
CSCwd56254	FTD で実行すると、「show tech-support」の生成内容に「show inventory」が含まれない
CSCwd56296	FTD Lina がスレッド名「IP Init Thread」でトレースバックおよびリロードする
CSCwd56774	「show asp drop」の紛らわしいドロップ理由
CSCwd56995	application/octet-stream と text/plain を使用した Web コンテンツへのクライアントレスアクセス
CSCwd57698	ina_duart_write での再帰パニック
CSCwd59736	ASA/FTD：アップグレード中の SNMP グループ設定によりトレースバックおよびリロードする
CSCwd61016	ASA：EEM が設定されている場合、リポート時に「Sync Config」ステータスでスタンバイがスタックすることがある
CSCwd62138	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
CSCwd62859	Cisco ASA および FTD AnyConnect の SSL/TLS VPN におけるサービス拒否攻撃に対する脆弱性

ID	見出し
CSCwd63580	FPR2100 : アプライアンスモードの ASA でのフェールオーバー コンバージェンス時間の増加
CSCwd63961	属性値が大きすぎることによる、DAPルールとのACクライアントの一致の失敗
CSCwd64480	ASAのコンテキストのカスケード接続を介したパケットが、ソフトウェアアップグレード後にゲートウェイコンテキストでドロップされる
CSCwd66815	CSCwb04975をサポートするためのLinaの変更 : FQDNベースのトラフィックを処理する際に、Snort3 が daq-pdts でトレースバックする
CSCwd71254	ASA/FTD が idfw fqdn ハッシュルックアップでトレースバックおよびリロードすることがある
CSCwd74116	DSID リークによる DH 計算エラーのため、S2S トンネルが機能しない
CSCwd77581	ICMPv6 オプション処理でのシステムクラッシュ
CSCwd82235	LINA がスレッド名 update_cpu_usage 下の FPR-1010 でトレースバックする
CSCwd84133	ASA/FTD がスレッド名「telnet/ci」でトレースバックおよびリロードすることがある
CSCwd84868	フローオフロードが使用されていない場合に、いくつかの devcmd 障害と checkheaps トレースバックが発生する。
CSCwd85178	AWS ASA v PAYG ライセンスが GovCloud リージョンで機能しない。
CSCwd91421	ASA/FTD が logging_cfg 処理でトレースバックおよびリロードすることがある
CSCwd93376	クライアントレス VPN ユーザーが、WebVPN ポータルから大きなファイルをダウンロードできない
CSCwd94096	ASA が別の認証および承認サーバーを使用している場合、Anyconnect ユーザーが接続できない
CSCwd95043	Cisco ASA および FTD VPN Web クライアントサービスのクライアント側要求のスマグリングの脆弱性
CSCwd95908	ASA/FTD がトレースバックおよびリロードする、スレッド名 : rtcli async executor process
CSCwd97020	ASA/FTD : 外部 IDP SAML 認証が「Bad Request」というメッセージで失敗する

バージョン 9.18(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。

ID	見出し
CSCvw82067	大量のフラグメント化されたトラフィックにより ASA/FTD 9344 ブロックが枯渇する
CSCvy50598	インターフェースの停止時に BGP テーブルが接続ルートを削除しない
CSCvz36903	クラスタのキープアライブパケットに新しいブロックを割り当てている間に ASA でトレースバックとリロードが発生する
CSCvz69729	不安定なクライアントプロセスは、FTD で LINA zmqio トレースバックを引き起こす可能性がある
CSCwa59907	LINA は、スレッド名「snmp_client_callback_thread」でトレースバックを観察した
CSCwa75966	ASA : ページ違反のあるスレッド名 Unicorn Proxy Thread でのリロードとトレースバック : アドレスがマッピングされていない
CSCwa97917	電源再投入後に ISA3000 がブートループの状態になる
CSCwb05291	Cisco ASDM および ASA ソフトウェアのクライアント側で任意のコードが実行される脆弱性
CSCwb06847	ASA/FTD がスレッド名「DATAPATH-9-11543」でトレースバックおよびリロードする必要がある
CSCwb17963	動的レート制限メカニズムを識別できず、syslog サーバーで 1 秒あたりのメッセージ制限に従っていない
CSCwb19648	crasLocalAddress の SNMP クエリで SSL/DTLS トンネルに割り当てられた IP が返されない
CSCwb52401	Cisco Firepower Threat Defense ソフトウェアの特権昇格の脆弱性
CSCwb53172	FTD : IKEv2 トンネルが 24 時間ごとにフラップし、暗号アーカイブが生成される
CSCwb53328	Smart Call Home プロセス sch_dispatch_to_url によって ASA/FTD のトレースバックとリロードが引き起こされる
CSCwb54791	ASA DHCP サーバーが予約済みアドレスを Linux デバイスにバインドできない
CSCwb63827	Cisco 適応型セキュリティアプライアンスと Firepower Threat Defense ソフトウェアの DoS の脆弱性

ID	見出し
CSCwb67040	FP4112 4115 : スレッド名 netfs_thread_init でのトレースバックとリロード
CSCwb68642	スレッド名 SXP CORE での ASA のトレースバック
CSCwb69503	FIPS が有効になっている場合に、ASA が aes128-gcm@openssh.com を設定できない
CSCwb71460	スレッド名 fover_parse での ASA トレースバックが SNMP 関連機能によってトリガーされる
CSCwb73248	タイマーインフラ/ネットフロータイマーでFWのトレースバックが発生する
CSCwb74571	ゾーンメンバーを使用する ASA ルーテッドモードで PBR が機能しない
CSCwb79812	RIP が接続されているすべての Anyconnect ユーザーをアドバタイズしており、再配布用のルートマップと一致しない
CSCwb80559	オフロードすべきでない SGT タグ付きパケットが FTD でオフロードされる
CSCwb80862	変換後の宛先で組み込みの「任意の」オブジェクトを使用している場合、ASA/FTD プロキシはすべてのトラフィックに ARP 要求を送信する
CSCwb82796	IKE トンネルを切断すると、ASA/FTD ファイアウォールがトレースバックおよびリロードすることがある
CSCwb83388	ASA HA アクティブ/スタンバイトレースバックが、約2ヵ月ごとに確認される。
CSCwb83691	FMC から開始されたキャプチャが原因で ASA/FTD のトレースバックとリロードが発生する
CSCwb85633	メモリの snmpwalk 出力が show memory/show memory details と一致しない
CSCwb87498	EIGRP ルート更新処理中の Lina のトレースバックとリロード。
CSCwb90074	ASA : マルチコンテキスト混合モード SFR リダイレクションの検証
CSCwb90532	NAT 関連の機能 nat_policy_find_location で ASA/FTD のトレースバックとリロードが発生する
CSCwb92709	インターフェイスがコンテキストから削除されると、「snmpwalk」を使用してインターフェイスを監視できない
CSCwb93932	タイマー サービス アサーションによる ASA/FTD のトレースバックとリロード

ID	見出し
CSCwb94190	フォワーディングリファレンス関数と FIPS が有効になっている ACL を適用すると、ASA がグレースフルシャットダウンする
CSCwb94312	SSH 設定を ASA バージョン 9.16 以降に適用できない
CSCwb97251	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
CSCwc02488	ASA/FTD がスレッド名「None」でトレースバックし、リロードすることがある
CSCwc03069	インターフェイスの internal data0/0 は cli からは up/up になるが、SNMP ポーリングからは up/down になる
CSCwc09414	ASA/FTD がスレッド名「ci/console」でトレースバックし、リロードすることがある
CSCwc10483	ASA/FTD がスレッド名「appAgent_subscribe_nd_thread」でトレースバックする
CSCwc10792	ASA/FTD IPSEC のデバッグで、ピアアドレスの変更とタイマー削除の理由が見つからない
CSCwc11597	SFR が 6.7.0.3 にアップグレードされると、ASA のトレースバックが発生する
CSCwc11663	CSM または CLI を使用して DNS インスペクションポリシーを変更すると、ASA のトレースバックとリロードが発生する
CSCwc13017	../inspect/proxy.h:439 で FTD/ASA のトレースバックとリロードが発生する
CSCwc13994	ASA : バックアップ後にインターフェイス設定で新しい構成を削除せずに復元する
CSCwc18312	EEM スクリプト内で実行される「show nat pool cluster」コマンドにより、トレースバックとリロードが発生する
CSCwc23356	ASA/FTD がスレッド名「DATAPATH-20-7695」でトレースバックおよびリロードすることがある
CSCwc23695	ASA/FTD がユーザー証明書の SAN フィールドから UPN を解析できない
CSCwc24422	クライアントのマシン証明書に空のサブジェクトがある場合、ACSSLVPN で証明書の認証と DAP に失敗する
CSCwc24906	スレッド ID 1637 で ASA/FTD のトレースバックとリロードが発生する

バージョン 9.18(1) で解決済みのバグ

ID	見出し
CSCwc28532	インラインセットインターフェイスの内部フロー処理によってフラグメント化された GRE トラフィックが原因で、9344 ブロックでリークが発生する
CSCwc28928	ASA : VTY セッションで SLA デバッグが表示されない
CSCwc32246	オブジェクトサブネット 0.0.0.0 0.0.0.0 が使用されている場合、NAT64 はすべての IPv6 アドレスを 0.0.0.0/0 に変換する

バージョン 9.18(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。

ID	見出し
CSCvw56551	インターフェイス設定を変更すると、ASA で NAT の表面的な警告メッセージが表示される
CSCvw62288	ASA : syslog レートが高い場合に 256 バイトのブロックが枯渇する
CSCvx97053	異なるコンテキストで同じインターフェイスとネットワークに ipv6 アドレス/プレフィックスを設定できない
CSCvy04430	管理セッションが数週間後に接続に失敗
CSCvy40401	IPsec の設定で NULL 暗号化を使用すると、L2L VPN セッションの起動が失敗する
CSCvz03524	sha1 ではなく sha256 リクエストが原因で PKI の「OCSP 失効チェック」が失敗する
CSCvz05541	ASA55XX : ソフトウェアアップグレード後に拡張モジュールインターフェイスが起動しない
CSCvz44645	FTD がスレッド名「lina」でトレースバックおよびリロードする可能性がある
CSCvz60578	MASTER_POST_CONFIG 状態のクラスタユニットは、一定期間後に無効状態に移行しなければならない
CSCvz68336	複数のインラインペアでの単一接続が原因で SSL 復号化が機能しない
CSCvz69729	不安定なクライアントプロセスは、FTD で LINA zmqio トレースバックを引き起こす可能性がある
CSCvz70688	default-information originate が最初に設定されると、設定に対する stub コマンドが許可されない

ID	見出し
CSCvz70958	dhcpp_add_ip_l_stby が原因でスタンバイのコントロールプレーンの CPU 使用率が高くなる
CSCvz72771	ASA/FTD がスタックトレースの「c_assert_cond_terminate」でトレースバックおよびリロードすることがある
CSCvz76746	管理トンネルを実装している間、ユーザーはオープン接続を使用して AnyConnect をバイパスできる
CSCvz76966	Cisco 適応型セキュリティアプライアンスと Firepower Threat Defense ソフトウェアの DNS で DoS の脆弱性
CSCvz81888	asa-9.14.3 から asa-9.15.1/9.16.1.28 にアップグレードした後、NTP が * (同期済み) ステータスに変更されない
CSCvz86256	プライマリ ASA は、スプリットブレインが検出され、ピアがコールドスタンバイになるとすぐに GARP を送信する必要がある
CSCvz88149	ブロック解放中に Lina のトレースバックとリロードにより、FTD ブートループが発生する
CSCvz89126	マルチ コンテキスト スイッチオーバーが ASDM から実行される場合、ASA で ASDM セッション/クォータカウントの不一致が発生する
CSCvz89327	OSPFv2 フローにクラスター集中型「c」フラグがない
CSCvz90375	起動時の ASA 9.14 の使用可能な DMA メモリが不足し、サポートされる AnyConnect セッションが減少する
CSCvz91218	高速トラフィックでのインターフェイスリングのドロップにより、スタンバイユニットで Statelink hello メッセージがドロップした
CSCvz92016	Cisco ASA および FTD ソフトウェアの Web サービスインターフェイスにおける権限昇格の脆弱性
CSCvz92932	ASA show tech の実行により、CPU でスパイクが発生し、IKEv2 セッションに影響を与える
CSCvz94153	IPV4 アドレスが設定されていない場合、IPV6 での NTP 同期が失敗する
CSCvz95108	デバイスでのメジャーバージョンの変更によるアップグレード後の FTD 展開の失敗
CSCvz95949	FP1120 9.14.3 : アクティブなデバイスの再起動後に一時的なスプリットブレインが発生
CSCvz99222	インラインセットの show コマンドと clear コマンドが機能しない

ID	見出し
CSCwa02929	FTD が SSL フローエラーの CORRUPT_MESSAGE でトラフィックをブロックする
CSCwa03341	スタンバイのサブインターフェイス mac は、mac-address コマンドなしでは古い mac に戻らない
CSCwa08262	マッピングされたグループポリシーを持つ AnyConnect ユーザーは、トンネルグループの下にあるデフォルト GP から属性を取得する
CSCwa11052	バージョン 9.14(2)15 へのアップグレード後に SNMP が応答しなくなる
CSCwa13873	「failover active」コマンドの実行後に、状態遷移における遅延が原因で ASA フェールオーバー スプリット ブレインが発生
CSCwa14485	Cisco Firepower Threat Defense ソフトウェアで確認されたサービス拒否攻撃に対する脆弱性
CSCwa14725	IKE デーモンスレッドでの ASA および FTD のトレースバックとリロード
CSCwa15185	ASA/FTD : LUA から不要なプロセス呼び出しを削除
CSCwa18858	ASA が、「ラベル長 164 バイトがプロトコルの制限である 63 バイトを超えている」という理由で非 DNS トラフィックをドロップする
CSCwa18889	マルチインスタンスの Lina と FXOS の間でクロックドリフトを検出
CSCwa19443	フローオフロード - 比較状態の値が長期間エラー状態のままになる
CSCwa19713	asp ドロップタイプ「no-adjacency」が原因で BVI インターフェイスで設定された ASA によってトラフィックがドロップした
CSCwa28822	FTD が UI 管理を FDM から FMC に移すと、トラフィックエラーが発生する
CSCwa28895	FTD SSL 復号トラフィックの遅延。SSL プロキシが構成可能/動的な最大 TCP ウィンドウサイズを許可する
CSCwa30114	オブジェクトサービスでポートの範囲を使用すると、「NAT がポートを予約できません」というエラーが発生
CSCwa33898	Cisco 適応型セキュリティ アプライアンスのソフトウェアクライアントレス SSL VPN で確認されたヒープオーバーフローの脆弱性
CSCwa34287	ASA : アップグレード後のリロードの後に NTP 同期が失われる
CSCwa35200	AnyConnect SSL の一部の syslog が、ユーザーコンテキストではなく管理コンテキストで生成される

ID	見出し
CSCwa36672	ASDM を使用してキャプチャを実行するとき、FPR4100 の ASA でトレースバックとリロードが発生する
CSCwa36678	FMC からの展開中にトレースバックを使用してランダム FTD がリロードされる
CSCwa38277	広範なプールを備えた ASA NAT66 が IPv6 で機能しない
CSCwa40719	トレースバック : セカンダリファイアウォールがスレッド名「fover_parse」でリロード
CSCwa41834	pix_startup_thread により ASA/FTD のトレースバックとリロードが発生
CSCwa41936	Cisco FTD の Bleichenbacher 攻撃に対する脆弱性
CSCwa42594	ASA : GTP ヘッダーに SEQ および EXT フィールドがある場合、IP ヘッダーチェックの検証に失敗する
CSCwa47041	Cisco 適応型セキュリティアプライアンスと Firepower Threat Defense ソフトウェアの DAP に関する DoS 脆弱性
CSCwa49480	SNMP OID が約 1 時間半後に動作を停止する (FTD)
CSCwa53489	ハッシュテーブルへのアクセス中に無効なメモリアクセスが原因で Lina のトレースバックとリロードが発生する
CSCwa54045	SAML ネイティブブラウザ処理でメモリリークが発生する
CSCwa55562	同じ送信元 IP に異なる CG-NAT ポートブロックが割り当てられたことが原因で、ホストごとの PAT ポートブロックが枯渇する
CSCwa55878	FTD サービスモジュールの障害 : 「ND がダウンした可能性があります」という誤ったアラーム
CSCwa56449	HTTP cli EXEC コードで ASA のトレースバックが発生する
CSCwa56975	コントロールプレーンで DHCP オファーが表示されない
CSCwa57115	オブジェクトで存在しない ACL を削除した後、新しいアクセスリストが有効にならない
CSCwa58686	OGS コンパイル動作における ASA および FTD の変更によりブートループが発生する
CSCwa61218	OID 「1.3.6.1.4.1.9.9.171.1.3.2.1.2」をポーリングすると、関連するトンネルの負のインデックス値が得られる
CSCwa65389	ASDM を介してインターフェイス設定を変更すると、Unicorn Admin Handler で ASA のトレースバックとリロードが発生する

ID	見出し
CSCwa67882	オフロードされた GRE トンネルは、サイレントにオフロードを解除し、CPU にパントされる場合がある
CSCwa68660	ASA を 9.12.4.x にアップグレードした後、FTP インспекションが正しく機能しなくなる
CSCwa73172	スレッド名「PIX Garbage Collector」で ASA のリロードとトレースバックが発生する
CSCwa74900	debug webvpn cifs 255 を有効にすると、トレースバックとリロードが発生する
CSCwa75966	ASA : ページ違反のあるスレッド名 Unicorn Proxy Thread でのリロードとトレースバック : アドレスがマッピングされていない
CSCwa77073	SNMP が予期しない結果の順序で snmpgetbulk に応答している
CSCwa79494	スポークからの IPSec トンネルがフラッピングすると、ハブでトラフィックエラーが継続的に発生する
CSCwa79980	FPR の SNMP get コマンドがインターフェイスインデックスを表示しない
CSCwa81795	Cisco ASA および FTD ソフトウェアの VPN 承認バイパスの脆弱性
CSCwa85043	トレースバック : ASA/FTD がスレッド名「Logger」でトレースバックおよびリロードする場合がある
CSCwa85138	トランザクションコミット診断に関する複数の問題が発生する
CSCwa87315	ASA/FTD が、スレッド名「IP Address Assign」でトレースバックおよびリロードする場合がある
CSCwa89243	9.15.1.17 にアップグレードした後、SNMP がポーリングに応答しなくなった
CSCwa91090	AnyConnect TLSv1.2 セッション確立中に SSL ハンドシェイクログに不明なセッションが表示される
CSCwa94894	ASA/FTD は、スレッド名「DATAPATH-4-9608」でトレースバックおよびリロードする場合がある
CSCwa96759	Lina が tcpmod_proxy_handle_mixed_mode でトレースバックおよびリロードする場合がある
CSCwa97784	ASA : ジャンボサイズの packets が L2TP トンネル上でフラグメント化されない
CSCwa98684	ポリシーの展開中にコンソールに過度の警告が発生する

ID	見出し
CSCwb00595	Mempool_DMA 割り当ての問題/メモリーリークが発生
CSCwb01700	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
CSCwb01919	FP2140 ASA 9.16.2 HA ユニットが lua_getinfo (getfuncname) でトレースバックおよびリロードする
CSCwb08644	Scaled S2S+AC-DTLS+SNMP の長時間テスト時に IKEv2 でクラッシュが発生する
CSCwb11939	ASA/FTD MAC の変更が、INSPECT がオンになっているフラグメント化されたパケットの処理で見られる
CSCwb16920	以前にアクティブだったメモリ追跡が無効になっている場合でも、CPU プロファイルを再アクティブ化できない
CSCwb18252	FTD/ASA : BFD 機能のトレースバックにより予期しないリブートを引き起こす
CSCwb25809	シングルパス : 古い ifc が原因でトレースバック
CSCwb54791	ASA DHCP サーバーが予約済みアドレスを Linux デバイスにバインドできない
CSCwb66761	Cisco Firepower Threat Defense ソフトウェアの Generic Routing Encapsulation に関する DoS 脆弱性
CSCwb69503	FIPS が有効になっている場合に、ASA が aes128-gcm@openssh.com を設定できない
CSCwb80862	変換後の宛先で組み込みの「任意の」オブジェクトを使用している場合、ASA/FTD プロキシはすべてのトラフィックに ARP 要求を送信する
CSCwb85633	メモリの snmpwalk 出力が show memory/show memory details と一致しない

シスコの一般規約

シスコのソフトウェア使用時には、シスコの一般規約（その他の関連規約を含む）が適用されます。以下の住所宛てに物理コピーをリクエストできます。Cisco Systems, Inc., P.O. Box 641387, San Jose, CA 95164-1387。シスコから購入したシスコ以外のソフトウェアでは、該当するベンダーのライセンス条項に従う必要があります。関連項目：<https://cisco.com/go/generalterms>

関連資料

ASA の詳細については、『[Navigating the Cisco Secure Firewall 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。

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)

© 2024 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。