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

最終更新：2023 年 5 月 24 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(x) のリリース情報が記載されています。

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と、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）
- **インスタンスタイプ g5ne.4xLarge の ASA 仮想 における Alibaba Cloud パフォーマンスの低下**：Alibaba Cloud のインスタンスタイプ g5ne.4xLarge の ASA 仮想 では、Alibaba インフラストラクチャの根本的な問題により、特に 1 秒あたりの接続数（CPS）についてパフォーマンスが低下します。回避策はありません。（CSCwb24458、CSCwb61168）

- **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

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 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(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	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。 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。 *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。
インターフェイス機能	

機能	説明
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	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。 新規/変更されたコマンド： **fec** *9.19(1)* および *9.18(2.7)* でも同様。

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。 • BGP • SSH • SNMP • Syslog • AAA • Telnet 新規/変更されたコマンド：**interface loopback**、**logging host**、**neighbor update-source**、**snmp-server host**、**ssh**、**telnet**

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	
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。

機能	説明
Alibaba の仮想展開	これで、Alibaba Cloud に Secure Firewall ASA Virtual を展開できます。サポートされる機能は次のとおりです。 • QCOW2 イメージパッケージ。 • 基本的な製品の稼働。 • Day-0 構成。 • 公開キーまたはパスワードを使用した SSH。 デバッグ目的で ASAv にアクセスするための Alibaba UI コンソール。 • Alibaba UI の停止/再起動。 • サポートされているインスタンスタイプ：ecs.g5ne.large、ecs.g5ne.xlarge、ecs.g5ne.2xlarge、ecs.g5ne.4xlarge。 • BYOL ライセンスのサポート。
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。	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。 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。 **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。 **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。
ルーティング機能	
PBR のパスモニタリングメトリック。	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ースを 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。 新規/変更されたコマンド：**clear path-monitoring**、**policy-route**、**show path-monitoring**
インターフェイス機能	

機能	説明
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	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。 新規/変更されたコマンド： **flowcontrol send on**
Secure Firewall 3130 および 3140 のブレークアウトポート	Cisco Secure Firewall 3130 および 3140 の 40 GB インターフェースごとに 4 つの 10 GB ブレークアウトポートを構成できるようになりました。 新規/変更されたコマンド： **breakout**
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l 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	

機能	説明
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ギング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、ロギングレートが動的に制限されます。 新規/変更されたコマンド： **logging rate-limit**
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す。	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。

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 9.16(x) は ASA 5506-X、5508-X、および 5516-X の最終バージョンです。

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

ASA 9.12(x) は ASA 5512-X、5515-X、5585-X、および ASASM 用の最終バージョン、

ASA 9.2(x) は ASA 5505 用の最終バージョン、

ASA 9.1(x) は ASA 5510、5520、5540、5550、および 5580 用の最終バージョンです。

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

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

現在のバージョン	暫定アップグレードバージョン	ターゲットバージョン
9.3(x)	—	次のいずれかになります。 → **9.18(×)** → 9.17(x) → **9.16(x)** → 9.15(x) → 9.14(x) → 9.12(x) → 9.8(x)
9.2(x)	—	次のいずれかになります。 → **9.18(×)** → 9.17(x) → **9.16(x)** → 9.15(x) → 9.14(x) → 9.12(x) → 9.8(x)
9.1(2)、9.1(3)、9.1(4)、9.1(5)、9.1(6)、または 9.1(7.4)	—	次のいずれかになります。 → 9.14(x) → **9.12(x)** → 9.8(x) → 9.1(7.4)
9.1(1)	→ 9.1(2)	次のいずれかになります。 → 9.14(x) → **9.12(x)** → 9.8(x) → 9.1(7.4)

現在のバージョン	暫定アップグレードバージョン	ターゲットバージョン
9.0(2)、9.0(3)、または 9.0(4)	—	次のいずれかになります。 → 9.14(x) → **9.12(x)** → 9.8(x) → 9.6(x) → 9.1(7.4)
9.0(1)	→ 9.0(4)	次のいずれかになります。 → 9.14(x) → **9.12(x)** → 9.8(x) → 9.1(7.4)
8.6(1)	→ 9.0(4)	次のいずれかになります。 → 9.14(x) → **9.12(x)** → 9.8(x) → 9.1(7.4)
8.5(1)	→ 9.0(4)	次のいずれかになります。 → **9.12(x)** → 9.8(x) → 9.1(7.4)
8.4(5+)	—	次のいずれかになります。 → **9.12(x)** → 9.8(x) → 9.1(7.4) → 9.0(4)
8.4(1) ～ 8.4(4)	→ 9.0(4)	→ **9.12(x)** → 9.8(x) → 9.1(7.4)

現在のバージョン	暫定アップグレードバージョン	ターゲットバージョン
8.3(x)	→ 9.0(4)	次のいずれかになります。 → **9.12(x)** → 9.8(x) → 9.1(7.4)
8.2(x) 以前	→ 9.0(4)	次のいずれかになります。 → **9.12(x)** → 9.8(x) → 9.1(7.4)

アップグレードリンク

アップグレードを完了するには、『ASA アップグレード ガイド』を参照してください。

未解決のバグおよび解決されたバグ

このリリースで未解決のバグおよび解決済みのバグには、Cisco Bug Search Tool を使用してアクセスできます。この Web ベース ツールから、この製品やその他のシスコハードウェアおよびソフトウェア製品でのバグと脆弱性に関する情報を保守するシスコ バグ トラッキング システムにアクセスできます。

（注） Cisco Bug Search Tool にログインしてこのツールを使用するには、Cisco.com アカウントが必要です。アカウントがない場合は、アカウントを登録できます。シスコサポート契約がない場合は、ID でのみバグを探すことができます。検索は実行できません。

Cisco Bug Search Tool の詳細については、Bug Search Tool（BST）ヘルプおよび FAQ を参照してください。

バージョン 9.18(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
CSCwd31197	AWS GLWB 環境で FTDv Snort3 のクラッシュが発生する
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

ID	見出し
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
CSCwd97356	タップモードのインラインペアを使用した FTD のインターフェイスキャプチャで、出力パケットが欠落することがある
CSCwe06562	FPR2100：BVI 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コンバージェンス時間の増加
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
CSCwe09730	Pthread-6076 による、Azure の vFTD（7.2.1）でのクラッシュ時に、FTD/ASA がトレースバックおよびリロードする
CSCwe10290	FTD が WSA からの GRE トラフィックをドロップする
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
CSCwe28290	ASA が、SYNACK パケットの誤った MAC アドレスを表示する。

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(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
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す。
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

ID	見出し
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
CSCwc03332	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
CSCwc03507	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
CSCwc07262	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。

ID	見出し
CSCwc08646	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
CSCwc10145	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
CSCwc10241	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 スプリットブレイン
CSCwc10483	ASA/FTD がスレッド名「appAgent_subscribe_nd_thread」でトレースバックする
CSCwc11511	FTD: 7.0.2 へのアップグレード後の SNMP エラー
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
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
CSCwc18524	コマンド「show environment」で ASA/FTD 電圧情報が不足している
CSCwc23844	空きメモリが 30% を超えているにもかかわらず、ASAv の CPU およびスタックメモリの割り当てエラーが高い
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
CSCwc26648	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
CSCwc27846	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。
CSCwc28334	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
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
CSCwc28806	プロセス名 Lina で ASA がトレースバックし、リロードする
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

ID	見出し
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る
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
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 でフェイルオーバーに関する syslog が出力されない

ID	見出し
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_inotify_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
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

ID	見出し
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 インスペク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
CSCwc94501	ASA/FTD が ctm_n5 リセットによりトレースバックする
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

ID	見出し
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
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

ID	見出し
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 親チャネル（SAL）に無効な基盤となるチャネルがある
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
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

ID	見出し
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、リブート時に「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
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
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

ID	見出し
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 ASAv 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
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	インターフェイスの停止時に 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

ID	見出し
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場合がある
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
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

ID	見出し
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
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

ID	見出し
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、AC SSLVPN 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
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

ID	見出し
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場合がある
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
CSCvz70958	dhcpp_add_ipl_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

ID	見出し
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
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 から属性を取得します
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

ID	見出し
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
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

ID	見出し
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
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
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 インスペク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
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
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	トレースバッグ：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

ID	見出し
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：ジャンボサイズのパケットが 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
CSCwb00595	Mempool_DMA 割り当ての問題/メモリリークが発生
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

ID	見出し
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

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 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。

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。