Cisco Secure Firewall ASA 9.24(x) リリースノート

最終更新：2026 年 2 月 26 日

Cisco Secure Firewall ASA 9.24(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 9.24(x) のリリース情報が記載されています。

特記事項

- **ASA Virtual を 9.24 からダウングレードできません**：新しい Grub ブートローダーを含む 9.24 にアップグレードした後は、以前のバージョンにダウングレードできません。新しいバージョンにアップグレードするには、まず 9.24 にアップグレードする必要があります。
- **OCI の ASA Virtual について、Arm インスタンスでは、レガシーハイパーバイザ（特に SR-IOV が有効）でスループットが低下する可能性があります。**詳細は、https://docs.oracle.com/en-us/iaas/Content/Compute/known-issues.htm を参照してください。サポートが必要な場合は、OCI にお問い合わせください。

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 9.24(1) の新機能

リリース日：**2025 年 12 月 3 日**

機能	説明
プラットフォーム機能	
Cisco Secure Firewall 220	Cisco Secure Firewall 220 は、コストと機能のバランスを取るため、ブランチオフィスやリモートロケーション向けにお求めやすい価格のセキュリティアプライアンスです。
Cisco Secure Firewall 6160、6170	Cisco Secure Firewall 6160 および 6170 は、要求が厳しいデータセンターおよび電気通信ネットワーク用の超ハイエンドファイアウォールです。例外的な価格対パフォーマンス、モジュール型機能、および高いスループットを備えています。
ASA Virtual Grub ブートローダーが UEFI ファームウェアおよびセキュアブートでアップグレードされました。	Grub ブートローダーの Grub 0.94 から Grub 2.12 へのアップグレードでは、レガシー BIOS モードとともに、セキュアブート機能の有無にかかわらない UEFI ファームウェアをサポートするようになりました。セキュアブート機能により、ブートレベルのマルウェア保護が提供されます。新しい展開では、MS-DOS パーティション分割ディスクの代わりに GPT パーティション分割イメージも使用されます。アップグレードする場合、UEFI およびセキュアブートに変更することはできません。新しい展開でのみ新しいオプションを使用できます。 （注） 9.24 にアップグレードした後は、以前のバージョンにダウングレードすることはできません。新しいバージョンにアップグレードするには、最初に 9.24 にアップグレードする必要があります。
ASA Virtual AWS デュアル アーム クラスタリング	デュアルアームモードでは、検査後、ASA Virtual は NAT を実行し、外部インターフェイスからインターネットゲートウェイを介して直接インターネットにアウトバウンドトラフィックを転送します。アウトバウンドトラフィックは、GWLB と GWLB エンドポイントを往復することなく、検査後にインターネットに直接転送されるため、トラフィックホップが 2 つだけ減少します。この削減は、マルチ VPC 展開に共通の出力パスを提供する場合に特に役立ちます。デュアルアーム展開の場合、出力通信のみがサポートされます。
ASA Virtual 自動スケーリングを使用した GCP クラスタリング	自動スケーリングを使用した GCP クラスタリングが、ASAv30、ASAv50、および ASAv100 でサポートされるようになりました。

機能	説明
ASA VirtualOCI アンペア A1 ARM コンピューティングシェーピング サポート	OCI の新しい形。 （注） OCI の ASA Virtual について、Arm インスタンスでは、レガシーハイパーバイザ（特に SR-IOV が有効）でスループットが低下する可能性があります。詳細は、https://docs.oracle.com/en-us/iaas/Content/Compute/known-issues.htm を参照してください。サポートが必要な場合は、OCI にお問い合わせください。
ASA VirtualKVM フローオフロード	KVM 用 DPU でフローオフロードがサポートされるようになりました。
ASA Virtual Nutanix AOS 6.8 のサポート	Nutanix AOS 6.8 では、パブリッククラウドの VPC と同様に VPC がサポートされます。
ASA Virtual Caracal に対する OpenStack のサポート	ASA Virtual 展開は、OpenStack の Caracal リリースでサポートされています。
ASA Virtual MANA NIC サポート	ASA Virtual は、次のインスタンスで、Microsoft Azure の MANA NIC ハードウェアをサポートします。 • Standard_D8s_v5 • Standard_D16s_v5
ファイアウォール機能	
Cisco Secure Firewall 6100 のアプリケーションの可視性と制御（AVC）	アプリケーションの可視性と制御（AVC）を使用すると、IP アドレスとポートだけでなく、アプリケーションに基づいてアクセス制御ルールを作成できます。AVC は脆弱性データベース（VDB）をダウンロードします。このデータベースでは、アクセス制御ルールで使用できるネットワークサービスオブジェクトとグループが作成されます。オブジェクトはさまざまなアプリケーションを定義し、グループはアプリケーションカテゴリを定義します。これにより、IP アドレスやポートを指定せずに、アプリケーションまたは接続のクラス全体を簡単にブロックできます。 次のコマンドが導入または変更されました。**avc**、**avc download vdb**、**clear avc**、**clear object-group**、**network-service reload**、**show avc**、**show service-policy**。また、ネットワークサービスオブジェクト定義の一部として **app-id** コマンドを入力することができなくなります。 サポートされているプラットフォーム： Cisco Secure Firewall 6100
ハイ アベイラビリティとスケーラビリティの各機能	
VPN モードを変更するための再起動は必要ありません	分散モードと集中型モードの間で VPN モードを変更する場合、再起動は必要なくなりました。ただし、モードを変更する前に、すべてのノードでクラスタリングを無効にする必要があります。

機能	説明
データノードはクラスターに同時に参加できます	以前は、制御ノードで一度に 1 つのデータノードのみがクラスターに参加できました。設定の同期に時間がかかる場合、データノードの結合に時間がかかることがあります。同時結合はデフォルトで有効になっています。NAT および VPN 分散モードが有効になっている場合、同時結合は使用できません。 次のコマンドが追加/変更されました。**concurrent-join**、**show cluster info concurrent-join incompatible-config**
クラスターノード結合での MTU ping テストでは、MTU を小さくすることでより多くの情報が提供されます。	クラスターに参加したノードは、クラスター制御リンク MTU と一致するパケットサイズで制御ノードに ping を送信することで MTU の互換性をチェックします。ping が失敗した場合は、MTU を 2 で割った値を試し、MTU ping が成功するまで 2 で割った値を返しません。通知が生成されるため、MTU を適切な値に修正して再試行できます。スイッチ MTU サイズを推奨値に増やすことを推奨しますが、スイッチ設定を変更できない場合は、クラスター制御リンクの有効な値を使用してクラスターを形成できます。 次のコマンドが追加/変更されました。**show cluster history**
CPU 使用率が高いクラスター制御リンクの正常性チェックの改善	クラスターノードの CPU 使用率が高い場合、正常性チェックは一時停止され、ノードは異常とはマークされません。正常性チェックを一時停止する CPU 使用率のしきい値を設定できます。 次のコマンドが追加/変更されました。**cpu-healthcheck-threshold**
Cisco Secure Firewall 6100 でのクラスタリング	最大 4 つの Cisco Secure Firewall 6100 ノードを Spanned EtherChannel または個別インターフェイスモードでクラスター化できます。
クラスタリングでの枯渇モニタリングのブロック	ブロックの枯渇が発生すると、ASA は障害対応ログを収集し、syslog を送信します。クラスタリングの場合、ノードはクラスターから移動するため、他のノードがトラフィックを処理できるようになります。ASA は、クラッシュおよびリロードを強制して枯渇から回復することもできます。 追加/変更されたコマンド：**fault-monitor**、**block-depletion**、**block-depletion recovery-action**、**block-depletion monitor-interval**
分散型サイト間 VPN モードのダイナミック PAT サポート	分散型モードでダイナミック PAT がサポートされるようになりました。ただし、インターフェイス PAT はまだサポートされていません。
インターフェイス機能	
DNS サーバーとドメインのリストを IPv6 クライアントにアドバタイズする再帰 DNS サーバー（RDNSS）および DNS 検索リスト（DNSSL）オプション	再帰 DNS サーバー（RDNSS）および DNS 検索リスト（DNSSL）オプションを設定することで、ルータアドバタイズメントを使用して DNS サーバーとドメインを SLAAC クライアントに提供できるようになりました。 新規/変更されたコマンド：**ipv6 nd ra dns-search-list domain**、**ipv6 nd ra dns server**、**show ipv6 nd detail**、**show ipv6 nd ra dns-search-list**、 **show ipv6 nd ra dns server**、**show ipv6 nd summary**
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
SSH X.509 証明書認証	X.509v3 証明書を使用して SSH のユーザーを認証できるようになりました（RFC 6187）。 （注） この機能は、Firepower 4100/9300 ではサポートされていません。 新規/変更されたコマンド：**aaa authorization exec ssh-x509**、**ssh authentication method**、**ssh trustpoint sign**、**ssh username-from-certificate**、**validation-usage ssh-client** *9.20(4)* でも同様です。
AES-256-GCM SSH 暗号	ASA は、SSH の AES-256-GCM 暗号をサポートしています。デフォルトでは、暗号化レベル [すべて（all）] と [高（high）] で有効になっています。 新規/変更されたコマンド： **ssh cipher encryption** *9.20(4)* でも同様です。
Linux カーネルクラッシュダンプ	Linux カーネルクラッシュダンプ機能を使用すると、カーネルクラッシュイベントをデバッグし、根本原因を見つけることができます。この機能は、デフォルトでイネーブルにされています。 新規/変更されたコマンド：**show kernel crash-dump**、**kernel crash-dump**、**crashinfoforce kernel-dump**
ASA Virtual での同意トークンを使用したルートシェルアクセスのサポート	ASA Virtual は、承認ユーザーが管理者パスワードなしで障害対応または診断の目的で Linux ルートシェルにワンタイムアクセスできるようにする新しい同意トークンメカニズムをサポートします。 新規/変更されたコマンド：**consent-token generate-challenge shell-access**、**consent-token accept-response shell-access**
ASDM 機能	
ASDM 証明書認証	ASDM 7.24 に付属している ASDM ランチャー 1.9(10) では、ユーザー証明書認証がサポートされるようになりました。以前は、この機能は Java Web Start でのみサポートされていました（7.18 で廃止）。ASA コマンドが 9.18 で廃止されていないため、ASDM ランチャー 1.9(10) を含む ASDM バージョンを使用する場合は証明書認証を使用するように以前の ASA バージョンを設定できます。 新規/変更されたコマンド：**http authentication-certificate**、**http username-from-certificate** 新規/変更された画面： • ASDM ランチャーのログインウィンドウ。
VPN 機能	

機能	説明
SGT over VTI	VTI トンネルで Cisco TrustSec SGT タグがサポートされるようになりました。 新規/変更されたコマンド：**cts manual**, **propagate sgt**、**policy static sgt**
VTI 向け ECMP および BFD 障害検出のサポート	1 つ以上のダイナミック VTI インターフェイスを Equal-Cost Multi-Path（ECMP）ゾーンに含めることができます。ゾーンを使用すると、スポークへのトラフィックのロードバランシングができます。Bidirectional Forwarding Detection（BFD）リンクの検出が高速になり、障害のある VTI リンクを数ミリ秒またはマイクロ秒単位で検出します。 新規/変更されたコマンド：**bfd template**、**vtemplate-bfd**、**vtemplate-zone-member**、**show zone**、**show conn all**、**show route**
分散型サイト間 VPN のループバック インターフェイスのサポート	分散サイト間モードでループバック インターフェイスを使用して、サイト間 VPN トンネルを作成できるようになりました。ロケーションネットワークに関連付けられている外部アドレスとは異なり、ループバック インターフェイスは独立しています。これは、アドレスを別のクラスターに移動し、ルーティングプロトコルを使用して新しい場所をアップストリームルータに伝播できることを意味します。その後、ピアのトラフィックは新しい場所に送信されます。
Cisco Secure Firewall 6100 の IPsec フロー オフロードおよび DTLS 暗号化アクセラレーション	Cisco Secure Firewall 6100 は AES-GCM-128 および AES-GCM-256 暗号のみをサポートします。
KVM上の ASA Virtual のIPsec フローオフロード	IPSec フローオフロードが KVM の DPU でサポートされるようになりました。

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

アップグレードするバージョン

シスコサポート & ダウンロードサイトでは、推奨リリースに金色の星が付いています。次に例を示します。

図 *1*：推奨リリース

現在のバージョンの表示

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。

アップグレードのガイドライン

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。

アップグレードパス

次の表に、ASA のアップグレードパスを示します。

（注） ASA 9.20 は Firepower 2100 の最終バージョンです。

ASA 9.18 は Firepower 4110、4120、4140、4150、および Firepower 9300 のセキュリティモジュール SM-24、SM-36、SM-44 の最終バージョンです。

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
9.23	—	次のいずれかになります。 → 9.24

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
9.22	—	次のいずれかになります。 → 9.24 → 9.23
9.20	—	次のいずれかになります。 → 9.24 → 9.23 → 9.22
9.19	—	次のいずれかになります。 → 9.24 → 9.23 → 9.22 → 9.20
9.18	—	次のいずれかになります。 → 9.24 → 9.23 → 9.22 → 9.20 → 9.19
9.17	—	次のいずれかになります。 → 9.24 → 9.22 → 9.20 → 9.19 → 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
9.16	—	次のいずれかになります。 → 9.24 → 9.23 → 9.22 → 9.20 → 9.19 → 9.18 → 9.17
9.15	—	次のいずれかになります。 → 9.24 → 9.23 → 9.22 → 9.20 → 9.19 → 9.18 → 9.17 → 9.16
9.14	—	次のいずれかになります。 → 9.24 → 9.23 → 9.22 → 9.20 → 9.19 → 9.18 → 9.17 → 9.16

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。 → 9.24 → 9.23 → 9.22 → 9.20 → 9.19 → 9.18 → 9.17 → 9.16
9.12	—	次のいずれかになります。 → 9.24 → 9.23 → 9.22 → 9.20 → 9.19 → 9.18 → 9.17 → 9.16
9.10	—	次のいずれかになります。 → 9.24 → 9.23 → 9.22 → 9.20 → 9.19 → 9.18 → 9.17 → 9.16 → 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
9.9	—	次のいずれかになります。 → 9.24 → 9.23 → 9.22 → 9.20 → 9.19 → 9.18 → 9.17 → 9.16 → 9.12
9.8	—	次のいずれかになります。 → 9.24 → 9.23 → 9.22 → 9.20 → 9.19 → 9.18 → 9.17 → 9.16 → 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
9.7	—	次のいずれかになります。 → 9.24 → 9.23 → 9.22 → 9.20 → 9.19 → 9.18 → 9.17 → 9.16 → 9.12
9.6	—	次のいずれかになります。 → 9.24 → 9.23 → 9.22 → 9.20 → 9.19 → 9.18 → 9.17 → 9.16 → 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
9.5	—	次のいずれかになります。 → 9.24 → 9.23 → 9.22 → 9.20 → 9.19 → 9.18 → 9.17 → 9.16 → 9.12
9.4	—	次のいずれかになります。 → 9.24 → 9.23 → 9.22 → 9.20 → 9.19 → 9.18 → 9.17 → 9.16 → 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
9.3	—	次のいずれかになります。 → 9.24 → 9.23 → 9.22 → 9.20 → 9.19 → 9.18 → 9.17 → 9.16 → 9.12
9.2	—	次のいずれかになります。 → 9.24 → 9.23 → 9.22 → 9.20 → 9.19 → 9.18 → 9.17 → 9.16 → 9.12
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
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

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

- FXOS：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。（FXOS 2.0.1 ～ 2.2.1 は 2.8.1 までアップグレードできます。2.0.1 より前のバージョンについては、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

- Firewall Threat Defense：上記の FXOS 要件に加えて、Firewall Threat Defense に対して中間アップグレードが必要になる場合があります。正確なアップグレードパスについては、ご使用のバージョンのFirewall Management Center アップグレードガイドを参照してください。
- Cisco ASA：Cisco 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 *2 : Firepower 4100/9300* と *ASA* および *Firewall Threat Defense* の互換性

FXOS のバージョン	モデル	ASA のバージョン	Firewall Threat Defense バージョン
2.18	Firepower 4112	**9.24**（推奨） 9.23 9.22 9.20 9.19	**10.x**（推奨） 7.7 7.6 7.4 7.3
	Firepower 4145 Firepower 4125 Firepower 4115	**9.24**（推奨） 9.23 9.22 9.20 9.19	**10.x**（推奨） 7.7 7.6 7.4 7.3
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		

FXOS のバージョン	モデル	ASA のバージョン	Firewall Threat Defense バージョン
2.17	Firepower 4112	**9.23**（推奨） 9.22 9.20 9.19 9.18	**7.7**（推奨） 7.6 7.4 7.3 7.2
	Firepower 4145 Firepower 4125 Firepower 4115 Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40	**9.23**（推奨） 9.22 9.20 9.19 9.18	**7.7**（推奨） 7.6 7.4 7.3 7.2
2.16	Firepower 4112	**9.22**（推奨） 9.20 9.19 9.18 9.17	**7.6**（推奨） 7.4 7.3 7.2 7.1
	Firepower 4145 Firepower 4125 Firepower 4115 Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40	**9.22**（推奨） 9.20 9.19 9.18 9.17	**7.6**（推奨） 7.4 7.3 7.2 7.1

FXOS のバージョン	モデル	ASA のバージョン	Firewall Threat Defense バージョン
2.14(1)	Firepower 4112	**9.20**（推奨） 9.19 9.18 9.17 9.16 9.14	**7.4**（推奨） 7.3 7.2 7.1 7.0 6.6
	Firepower 4145 Firepower 4125 Firepower 4115 Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40	**9.20**（推奨） 9.19 9.18 9.17 9.16 9.14	**7.4**（推奨） 7.3 7.2 7.1 7.0 6.6
2.13	Firepower 4112	**9.19**（推奨） 9.18 9.17 9.16 9.14	**7.3**（推奨） 7.2 7.1 7.0 6.6
	Firepower 4145 Firepower 4125 Firepower 4115 Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40	**9.19**（推奨） 9.18 9.17 9.16 9.14	**7.3**（推奨） 7.2 7.1 7.0 6.6

FXOS のバージョン	モデル	ASA のバージョン	Firewall Threat Defense バージョン
2.12	Firepower 4112	**9.18**（推奨） 9.17 9.16 9.14	**7.2**（推奨） 7.1 7.0 6.6
	Firepower 4145 Firepower 4125 Firepower 4115	**9.18**（推奨） 9.17 9.16 9.14 9.12	**7.2**（推奨） 7.1 7.0 6.6 6.4
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.18**（推奨） 9.17 9.16 9.14 9.12	**7.2**（推奨） 7.1 7.0 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	Firewall Threat Defense バージョン
2.11	Firepower 4112	**9.17**（推奨） 9.16 9.14	**7.1**（推奨） 7.0 6.6
	Firepower 4145 Firepower 4125 Firepower 4115	**9.17**（推奨） 9.16 9.14 9.12	**7.1**（推奨） 7.0 6.6 6.4
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.17**（推奨） 9.16 9.14 9.12 9.8	**7.1**（推奨） 7.0 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	Firewall 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るには、FXOS 2.10(1.179)+ が必要です。	Firepower 4112	**9.16**（推奨） 9.14	**7.0**（推奨） 6.6
	Firepower 4145 Firepower 4125 Firepower 4115	**9.16**（推奨） 9.14 9.12	**7.0**（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	**9.16**（推奨） 9.14 9.12 9.8	**7.0**（推奨） 6.6 6.4
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		
2.9	Firepower 4112	9.14	6.6
	Firepower 4145 Firepower 4125 Firepower 4115	9.14 9.12	6.6 6.4
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	9.14 9.12 9.8	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	Firewall 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		
	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
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		
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	Firewall 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	**9.12**（推奨） 9.8	
	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	**9.8**	Firewall Threat Defense バージョンはサポートが終了しています
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		

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 でのみバグを探すことができます。検索は実行できません。

Cisco Bug Search Tool の詳細については、Bug Search Tool Help & FAQ [英語] を参照してください。

バージョン 9.24(x) で未解決のバグ

このリリースに未解決のバグはありません。

バージョン 9.24(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
CSCvh98118	「debug ip ...」関連のデバッグで「logging デバッグトレース持続」が失敗します
CSCvm76755	DP-CP arp-in キューと adj-absent キューを分離する必要があります
CSCwa38880	スタンバイ ユニットで access-list/ access-group の順序が異なっています。完全同期は、ノードに参加中に発生します。
CSCwb07908	スタンバイ FTD/ASA が 0.0.0.0 の送信元 IP で DNS クエリを送信する
CSCwc57341	インラインペアの FTW バイパス動作モードが間違って「Phy バイパス」になっている
CSCwc82675	ASA/FTD：複数の AnyConnect パッケージを設定した後に、高 Lina メモリ使用量が観測される

ID	見出し
CSCwd92327	2k プラットフォームでは、数字で始まるユーザーの外部認証が失敗する
CSCwf04460	Ctrl+C を押して cancel show tech fprm detail コマンドを実行すると、fxos ディレクトリが表示されなくなる。
CSCwf25454	古い anyconnect エントリが原因でルーティングの問題が発生する
CSCwf72285	DAP：debug dap trace が 3000 行を超えると正常に表示されない
CSCwh10931	「show webvpn saml idp」CLI コマンドを呼び出したときの ASA/FTD のトレースバックとリロード
CSCwh41925	ZMQプロキシでのLinaトレースバックが、サービスの損失を引き起こす。
CSCwh53745	ASA：DNS クエリ応答のために着信接続を開始するための予期しないログ
CSCwi39206	3100/4200: Qdmaドライバウォッチドッグタイムアウト
CSCwi95690	スーパーバイザーと VIC アダプタ間の接続障害により、「Adapter 1/x/y is unreachable」の障害が発生する
CSCwk09488	RA 認証中に ISE から SGT を処理できなかった場合に誤った syslog が生成される
CSCwk33387	mgmt0/診断発信トラフィック用の SNMP が見つからない。
CSCwk42676	仮想 ASA/FTD がスレッド PTHREAD でトレースバックし、リロードすることがある
CSCwm04866	TCP syslog サーバーにログを送信することによる 1550 ブロックの枯渇を防ぐためのデバッグメニューコマンド
CSCwm51747	FXOS のアップグレード後に公開キー認証を使用した SSH アクセスが失敗する
CSCwm61345	FXOS: vdc.log が原因でディレクトリ /var/tmp が FXOS 障害 F0182 をトリガーする（過剰なロギング、ログローテーション）
CSCwm74289	NAT トラップのレートの制限が必要
CSCwm80732	ASA/FTD - TCP プロキシの競合状態によるトレースバックとリロード
CSCwm95189	Redis は、ディスク上に永続するオープンソースのメモリ内データベースです。An
CSCwm95191	Linux カーネルで、次の脆弱性が解決された。s
CSCwm96652	クラスタがユニットに対して誤った NAT を割り当てており、トラフィックがユニットに適切に転送されない

ID	見出し
CSCwn00475	priority-queue によるメモリブロック 80 および 9344 のリーク
CSCwn10661	FPR2k デバイスで CMI を使用して実行されている FTD に、203.0.113.129 の ARP が存在しない
CSCwn19190	メモリフラグメンテーションにより、lina で大きなページを使用できなくなる
CSCwn22610	コア生成を含む fs-daemon のハプリセット
CSCwn24777	SSL 事前認証接続による ASA ブロックの枯渇
CSCwn27872	「eigrp_interface_ioctl」API で、約 25KB のメモリの大きなチャンクがスタックに割り当てられる
CSCwn32978	スレッド名 Datapath でのトレースバックとリロード
CSCwn35495	フェールオーバー時に FXOS でプライマリ FTD インスタンスの MAC アドレスが正しく更新されない
CSCwn36712	スタンバイの 8305 の NAT 迂回がフェールオーバー後に更新されないため、プライマリのスタンバイ FTD が FMC でオフラインと表示される
CSCwn39081	SNMP ウォークが IP アドレスではなく IPSEC ピアの ASCII 値になる。
CSCwn40572	MI：仮想 MAC が設定されている場合、Vlan 情報が FXOS レベルで適用されない
CSCwn40702	freeb_core_local_internal での ASA のトレースバックとリロード
CSCwn45049	Coverity システム SA の警告、2024 年 9 月 9 日、Coverity の不具合 922530 922529 922528 922630 921809 921808
CSCwn45510	S2S VPN トンネルの子 SA の再ネゴシエーションが失敗する
CSCwn47308	FPR 1100/2100/3100 のクリティカルな正常性アラート「user configuration(FSM.sam.dme.AaaUserEpUpdateUserEp)」
CSCwn50760	9.20.3.7 へのアップグレード後の ASA トレースバック
CSCwn51845	ASA 9.20.3.4 を実行しているクラスタメンバーでトレースバックが確認される
CSCwn59032	ASA 9.18.4.22（FPR 2130 プラットフォームモード）へのアップグレード後に FCM GUI にアクセスできなくなる
CSCwn59379	インターフェイスメンバーがダウンした場合、ポートチャネルの帯域幅情報が更新されない。

ID	見出し
CSCwn60726	スレッド名 vtemplate process でトレースバックおよびリロードする
CSCwn61041	ウォッチドッグを含む bgp * IPv6 ユニキャスト中のトレースバックとリロード
CSCwn63839	BVI との arp permit-nonconnected の設定時にスレッド名 Lina でトレースバックする
CSCwn64025	ASA：他のネイバーから学習した IPv6 EIGRP ルートが、フェイルオーバー後の更新に含まれない
CSCwn65415	ASA：ネクストホップの ARP エントリなしで接続が作成された場合、floating-conn で UDP 接続が閉じられない
CSCwn69488	ASA/FTD がスレッド名 IP RIB Update でトレースバックおよびリロードする
CSCwn71596	インターフェイスリンクのダウン（Init、mac-link-down）が確認された：ケーブルの取り外し/再接続後に EtherChannel メンバーシップがダウン/ダウン/ダウンの状態になる
CSCwn71946	show blocks old core local を使用すると、予期しないリロードが発生する可能性がある。
CSCwn73351	アジア/バンコクのタイムゾーンオプションが、firepower1k で実行している ASA に表示されない
CSCwn73399	Cisco Secure Firewall Adaptive Security Appliance および Secure Firewall Threat Defense ソフトウェア IKEv2 サービス妨害の脆弱性
CSCwn75667	設定時にバナー motd が表示されない
CSCwn76079	SSH は管理コンテキストで動作するものの、ssh key-exchange を変更するとユーザーコンテキストで動作しない
CSCwn79553	到達不能な LDAP/AD を照会すると、FTD の外部認証で遅延またはタイムアウトが発生することがある
CSCwn80419	設定可能なオプションとして SVC Rx/Tx キューが必要
CSCwn80765	CiscoSSH が有効な場合に ASA を搭載した ISA3000 が SSH アクセスを拒否する
CSCwn81118	RTSP パケットが送信キューでスタックして 9k ブロックが枯渇する。
CSCwn81784	FMC を介して句 91 FEC を選択すると、QSFP-100G-CU3M で fec 528 ではなく fec 544 が設定されます。

ID	見出し
CSCwn81995	SNMP インスペクションが有効になっている場合のメモリ破損によるトレースバックとリロード
CSCwn84557	「spin_lock_fair_mode_enqueue」による Lina のトレースバックとリロード
CSCwn86002	クイックコア機能に切り替えてもコア破損が引き続き発生する
CSCwn87513	タイムゾーンがヨーロッパ/ダブリン（GMT）に設定されていると、ASA クロックが 2 時間同期しない。
CSCwn90327	FP1150 ASA/FTD がウォッチドッグタイマーによってトリガーされ、トレースバックおよびリロードする
CSCwn90900	RA VPN に関連する SNMP OID のポーリングが原因となり、ASA/FTD のメモリ使用率が高くなる
CSCwn90958	Cisco Secure Firewall Adaptive Security Appliance および Cisco Secure Firewall Threat Defense ソフトウェアの認証済みコマンドインジェクションの脆弱性
CSCwn91612	Cisco Secure Firewall Adaptive Security Appliance および Cisco Secure Firewall Threat Defense ソフトウェアの認証済みコマンドインジェクションの脆弱性
CSCwn91996	WM-DT-7.7.0-40：デバイスコンソールでスイッチの設定の失敗とスイッチの Mac エラーが確認される
CSCwn92248	FPR2100 および FPR1100：ポートチャネルインターフェイスが LACP でフラップする
CSCwn92894	「show chunkstat top-usage」の出力にすべてのエントリが表示されないことがある
CSCwn93319	ASA/FTD がスレッド名「DATAPATH」でトレースバックし、リロードすることがある
CSCwn93411	snmpd サービスの障害による FXOS のリセットとリロード
CSCwn95939	受信した CRL がキャッシュされた CRL より古い場合に syslog を生成
CSCwn95945	受信した CRL 署名の検証が失敗した場合に syslog を生成
CSCwn96929	ASA：スレッド名 SSH でのトレースバックとリロード
CSCwn96963	FTD が VPN ヘアピンのない VPN ルーティングとして syslog 430002 を生成する

ID	見出し
CSCwn97630	IPv6 パケット処理が原因で DATAPATH で FTD リブートおよびトレースバックが発生する
CSCwn98402	デバッグ可能性：アップグレード後に FP2100 ポートチャネル インターフェイスがフラップする
CSCwo00102	不正なウィンドウサイズ情報を受信したために、Snort3 が無効なシーケンス番号でパケットをトリミングする
CSCwo00225	アップグレード前に設定されている場合、VNI 送信元 MTU がアップグレード後に IPv6 に認識されない
CSCwo00332	Firepower がリロード後に SSL トラストポイント設定を削除する
CSCwo00444	FPR3100/4200 プラットフォームでの暗号ハードウェアオフロードに影響する Nitrox Engine（Crypto Accelerator）の問題
CSCwo00702	コミュニティリストは、リストの最後の項目が削除されるまでエラーをスローしない必要がある
CSCwo00880	Cisco Secure Firewall Adaptive Security Appliance および Secure Firewall Threat Defense ソフトウェア VPN Web サーバーのサービス妨害（DoS）脆弱性
CSCwo05712	有用性強化：FXOS ディスクエラーをよりわかりやすくする
CSCwo05801	FXOS 2.14.1.167 での SNMP ウォークにより警告ループが発生
CSCwo08042	Unicorn Proxy スレッドでのトレースバックにより、ASAv が予期せずリロードする
CSCwo08306	ローカルへのコマンド承認のフォールバックが、権限 15 のユーザーに対してのみ機能する。
CSCwo08724	snort 障害中にピアユニットが準備完了状態になる前に、アクティブな HA ユニットが障害状態になる
CSCwo09060	4096 ビットの RSA キーを持つ SSL トラストポイントが、CLI で更新されると ASA で許可されない
CSCwo09195	FQDN を無効化した後の展開中のトレースバックとリロード。
CSCwo09439	ASA/FTD がスレッド名「DATAPATH-3-4280」でトレースバックし、リロードすることがある
CSCwo09618	EEM によるデバッグの有効化が失敗する
CSCwo09921	FMC GUI の whois lookup コマンドがエラーを適切に処理しない。

ID	見出し
CSCwo13550	ディスパッチキュードロップで、ドロップされたフローのスナップショットまたはタプルビューがない。
CSCwo15021	Cisco Secure Firewall Adaptive Security Appliance および Secure Firewall Threat Defense ソフトウェア IKEv2 サービス妨害の脆弱性
CSCwo15022	Cisco Secure Firewall Adaptive Security Appliance および Secure Firewall Threat Defense ソフトウェア IKEv2 サービス妨害の脆弱性
CSCwo15023	Cisco Secure Firewall Adaptive Security Appliance および Secure Firewall Threat Defense ソフトウェア IKEv2 サービス妨害の脆弱性
CSCwo15024	Cisco Secure Firewall Adaptive Security Appliance および Secure Firewall Threat Defense ソフトウェア IKEv2 サービス妨害の脆弱性
CSCwo15026	Cisco Secure Firewall Adaptive Security Appliance および Secure Firewall Threat Defense ソフトウェア IKEv2 サービス妨害の脆弱性
CSCwo15027	Cisco Secure Firewall Adaptive Security Appliance および Secure Firewall Threat Defense ソフトウェア リモートアクセス SSL VPN のサービス妨害（DoS）脆弱性
CSCwo15715	IKEv2 キー再生成が、IKE キー再生成中のフラグメンテーションによって失敗する
CSCwo16488	FXOS で、パッチイメージを使用してイメージインストールを起動および開始できる
CSCwo18838	ASA/FTD がスレッド名「lina_exec_startup_thread」でトレースバックし、リロードすることがある
CSCwo18850	Cisco Secure Firewall Adaptive Security Appliance、Secure Firewall Threat Defense ソフトウェア HTTPサーバー リモートでのコード実行の脆弱性
CSCwo19762	マルチコンテキストモードで mac-address auto を再度有効にすると、クラスタ内のデータノードに再度参加できない
CSCwo21767	カスタム設定に対してポートスキャンアラートが生成されない
CSCwo22091	Radius を使用した認証/承認のときに FTD が「0.0.0.0」NAS-IP-Address 属性を送信する
CSCwo24772	debug packet-condition が期待どおりに機能しない
CSCwo24856	9K ブロックの枯渇により、ファイアウォールを通過するすべてのトラフィックが遅延する
CSCwo25236	お客様が突然、ASA への SSH アクセスを失った

ID	見出し
CSCwo26258	FPR 4200 シリーズでのリロードまたはアップグレード後における Management0 から Management1 へのデフォルトルートの変更
CSCwo27260	ユニットがアクティブになるまでに約 13 秒かかる
CSCwo31094	NFS が有効になっているディスクアクセスの問題によって、仮想 ASA がトレースバックおよびリロードする
CSCwo33815	FMC：プラットフォーム設定から SNMP ホストを削除すると、展開に予想よりも時間がかかる
CSCwo35783	ネイバーとのルートの追加/更新/取り消しに対するデバッグを強化
CSCwo35788	有用性強化：高度なデバッグ用の新しい「show bgp internal」コマンド
CSCwo35938	管理専用マルチキャストルートがないため、IPv6 管理通信が失われる。
CSCwo36485	vaccess_nameif_action スレッドで ASA/FTD がトレースバックおよびリロードする
CSCwo41250	メモリ不足状態時のスレッド DATAPATH-1-23988 でのトレースバックとリロード
CSCwo42102	show tech-support fprm detail コマンドが長時間スタックする
CSCwo42230	メモリリークが原因でスプリットブレインが発生
CSCwo42326	ENH：テクニカルサポートファイルの「show system detail」に SystemID を含める
CSCwo44732	ARP が到達不能なネクストホップのパケットをひそかにドロップする
CSCwo45497	IKEV2 統計からのカウンタが VPN-Sessiondb のトンネル数と一致しない
CSCwo45848	SecGW：データノードが cluster_ccp_make_rpc_call failed to clnt_call エラーでクラスタに参加できない
CSCwo46142	ポートチャネルメンバーのインターフェイスがフラップによって非アクティブなメンバーになる
CSCwo47978	ASA がスレッド名「fover_parse」でトレースバックし、リロードすることがある
CSCwo48439	スレッド名 Unicorn Admin Handler でのトレースバックとリロード
CSCwo49425	logging recipient-address でロギングメールメッセージのシビラティ（重大度）レベルが上書きされない

ID	見出し
CSCwo49744	DNS とデフォルトゲートウェイが、データインターフェイスを介して管理される FTD で削除される
CSCwo49928	Cisco Secure Firewall Adaptive Security Appliance および Secure Firewall Threat Defense ソフトウェア IKEv2 サービス妨害の脆弱性
CSCwo50417	Warwick Avenue：MGMT 1/2 インターフェイスがダウン状態の場合、LLDP ネイバーが検出されない
CSCwo54996	9344 ブロックのリークによるトラフィック障害
CSCwo56698	Cisco Secure Firewall Threat Defense ソフトウェアの地理位置情報リモートアクセス VPN バイパスの脆弱性
CSCwo57740	「${dsk_a} がないか操作できません。ブレードをリブートしています。（${dsk_a} missing or inoperable. Rebooting Blade.）」というエラーにより、不足しているか操作できないディスクが指定されない。
CSCwo58033	[クラスター] コンテキストで NAT プールの枯渇が発生すると、CPU 使用率が 100% になる。
CSCwo58191	FTD：snort によって検査されるパケットの大規模な遅延
CSCwo58260	GRE | IPinIP 接続の「built」および「teardown」メッセージを Lina syslog に追加します
CSCwo60609	ドクタリングルールのタイプがダイナミックであり、インターフェイスがある場合、DNS ドクタリングが正しく機能しない
CSCwo61241	checkSystemCPUs 障害により、論理アプリケーションが「Start Failed」でスタックする
CSCwo64788	FPR9K-SM-56 クラスター：アプリケーション インストール ループで FTD がスタック状態になり、エラー「pooled address is unknown」が発生する
CSCwo65060	FTD HA | ポートチャネルの同じ MAC が原因でネットワーク障害が発生する。
CSCwo65866	プライマリ FTD インスタンスが FCM から無効になっている場合、ネットワーク障害が発生する
CSCwo66872	snmp_logging_thread がコントロールプレーンの CPU を多く使用している
CSCwo71052	リロード後に FPR1010 Ethernet1/1 トランクポートで Vlan トラフィックが渡されない
CSCwo74496	無関係な BFD ピアがダウンした後、ASA が着信 BFD パケットを処理しないことが原因で BFD がフラップする

ID	見出し
CSCwo75483	SNMP エージェントとして使用される HA の FTD マルチインスタンスでシャーシへの SNMP ポーリングが失敗する
CSCwo75810	SNMP 設定が同じ FTD のタイプとバージョン間で一貫して適用されない
CSCso76165	rsync によるデプロイメントの失敗
CSCwo76436	ピアスイッチのリロード時に、インターフェイス MAC 用の 3100 マーベル 4.3.14 CPSS パッチがスタック状態になる
CSCwo76559	3110 で SNMP 通知スレッドでの ASA/FTD トレースバックとリロードが発生する
CSCwo77665	「低」に設定されている場合、FMC のポートスキャンイベントで誤った送信元/宛先が表示される
CSCwo78969	ユニットがクラスタに再参加するときのスレッド名 DATAPATH でのトレースバック
CSCwo79028	フェイルオーバー後の FQDN 解決が次の DNS ポーリング間隔まで保留される
CSCwo79798	リロード後に暗号化チェックサムが変更される
CSCwo80223	代替パス経由で受信したシングルホップ BFD セッションで BFD パケットがドロップされない
CSCwo82639	ローカルユーザーの詳細がクラスタセットアップのデータノードに複製されない。
CSCwo82658	ASDM：アイデンティティ証明書を追加するときに、キーペアがすでに存在するというエラーが表示される
CSCwo83389	FXOS の複数の場所での RSA キーの長さの違い
CSCwo84467	DATA ノードがまだ一括同期状態のときに BGP が即座に起動する L3 クラスタリング
CSCwo86422	CCL を介した一方向通信により分割クラスターが発生する
CSCwo87763	ASA/FTD：HA セットアップでのリロード後にプライマリスタンバイユニットがアクティブになる
CSCwo87938	バックアウトの変更により、FIPS モードでクラスタリングを有効にできない
CSCwo88204	sch_dispatch_to_url での Smart Call Home プロセスによって ASA/FTD のトレースバックとリロードが発生する

ID	見出し
CSCwo88518	クラスター内のいずれかのノードでコマンドレプリケーションが失敗した場合、クラスターからノードを FMC にキックアウトする
CSCwo89233	アクセスリスト後のコマンド commit noconfirm revert-save でクラスターノードへのコマンド複製が失敗し、追加のデバッグが発生する
CSCwo91436	FPR 4125 マルチインスタンス：Snort およびシステムコアの 高 CPU 使用率（100%）により FMC 重大アラートが発生する
CSCwo91748	Lina：ACL 削除後に show access-list を実行すると、スレッド名 SSH でトレースバックが発生する
CSCwo91965	ASAv が予期せず再起動する
CSCwo92226	ASA：SSH セッションが閉じられても asacli プロセスが終了しない
CSCwo94260	FTD：SIP パケットから SGT インラインタグが削除される
CSCwo94274	FP4100/930 の致命的なエラー：リセットコード 0x0040 でウォッチドッグ前に未完了のチェーンが観察された
CSCwo94483	非CP スレッドでのトレースバック後にLINA がリロードせずに非アクティブのままになる
CSCwo97439	ACL：AAA 承認コマンドが適用された後に、ASA で「OOB アクセスリストの設定の変更が検出されました（OOB Access-list config change detected）」という誤った警告が表示されることがある
CSCwo99690	Call-Home 設定で「Call-Home Reporting Anonymous」オプションを無効にしているときにエラーが発生した
CSCwp00977	FTD 断続 syslog アラート：mcelog デーモンが実行されない。デーモンを再起動する。
CSCwp01015	機能 mp_percore での ASA/FTD のトレースバックとリロード
CSCwp02224	プライマリ/スタンバイデバイスの FXOS バージョンをアップグレードすると、FPR フェイルオーバー スプリット ブレインが発生する
CSCwp04235	ASA のトレースバックとリロード
CSCwp06882	Hyper-V で実行している ASA を 9.20.3.9 から 9.20.3.16 にアップグレードした後に CPU 使用率が高くなる
CSCwp06890	接続すると、Finisar ポートの SFF_SFP_10G_25G_CSR_S V03 モジュールがバウンスします。
CSCwp08772	ASA：tls-proxy maximum-session コマンドエラー

ID	見出し
CSCwp10889	想定される ACL に基づいてトラフィックアクションが実行されている場合でも、パケットトレーサが誤った ACL を表示する。
CSCwp10957	SSL エラーにより、Cisco Smart Software Manager（CSSM）への接続が終了する
CSCwp11382	ASA/FTD：ssl trust-point コマンドがリロード後に削除された
CSCwp13016	FTD/ASA SSH：端末モニターにログが表示されない
CSCwp13399	「show tech-support fprm」の結果を tar 自体のコアに収集する
CSCwp13540	クライアントレス VPN のファイルパスに日本語テキストを使用したファイルのアップロードに対して、誤った URL が表示される
CSCwp14123	Tmatch メモリが、主に ARP-DP によって消費される。
CSCwp16529	「show cluster info load-monitor details」を使用すると、バッファドロップに対して負の値が表示される
CSCwp16739	ASA クラッシュ情報ファイルが FP4200 デバイスで生成されない
CSCwp17700	少なくとも 1 つの syslog ホストで EMBLEM 形式が有効になっている場合、Syslog 形式が正しく出力されない。
CSCwp18885	「Kernel Panic」により Firepower 9300/4100 でトレースバックおよびリロードが発生する場合がある
CSCwp22214	トラフィックがボックスを通過しているときに、複数のメールドロップと enq の失敗が発生する
CSCwp22612	Umbrella DNS 設定を削除しようとすると、FTD でポリシー展開が失敗する
CSCwp22743	wpk - 1gsx リンクは wpk で稼働中だが、スイッチ側では接続されていないと表示される
CSCwp25033	ICMP に到達できないストームにより、2 ユニットの FTD クラスターで CPU が高くなる可能性があります
CSCwp26815	スタンバイ ASA デバイスでの「WebVPNタイマープロセス」による CPU 使用率
CSCwp32469	エラー：Msglyr::ZMQWrapper::registerSender() が ZeroMQ ソケットのバインドに失敗した
CSCwp33077	SAML IdP エンティティ ID が 128 文字の上限より増加する
CSCwp33410	dmesg および kern.log ファイルが Tx Queue=0 ログでフラッディングする

ID	見出し
CSCwp34610	Windows および MacOS ネイティブ VPN クライアントで IKEv2-EAP 認証が失敗する
CSCwp36133	インターフェイス PAT（接続先インターフェイス）へのフォールスルーの動作が期待どおりに機能しないため、動作を明確にする。
CSCwp37284	ユーザーが [クライアントレス VPN] ページからログアウトをクリックすると、「CSRF Token Mismatch」エラーが表示される。
CSCwp39319	大規模な CRL の処理中に ASA メモリがリークする。
CSCwp60027	FTD ログで再起動の理由をキャプチャする
CSCwp60849	生成された ASA コアファイルが破損している
CSCwp60896	デバイスのリロード後に ASA のクロックが UTC に戻る
CSCwp64615	ASA/FTD：'invalid-ip-length' または 'sp-security-failed' の ASP ドロップキャプチャが、一致基準で機能しない。
CSCwp66721	SSL 暗号化でのメモリリークにより、FTD 7.7.0 を実行しているローエンドデバイスで Lina メモリ使用率が高くなる
CSCwp67356	HA 状態が ColdStandby から Active に移行しない
CSCwp83345	クラスター：マルチブレードシャーシで、特定の VLAN 宛てのブロードキャスト通信が送信されない
CSCwp87708	アップグレード後に FP1140 重大 FXOS 障害アラート（F1000413）が発生する
CSCwp89969	ファイアウォールの再起動/リブート完了により遅延が発生する
CSCwp90780	.tgz コンテキストファイルを復元すると、割り当てられたインターフェイスが 'system' 設定から削除される
CSCwp92390	FTD - FXOS FTD OID ツリーの SNMP ウォークが空またはタイムアウトを返す
CSCwp93368	Azure に展開された FTDv ファイアウォールで LINA トレースバックが観測された：snp_vxlan_encap_and_send_to_remote_peer
CSCwp97402	WA：大規模な snmp 設定がある展開中に、tmatch テーブルでロックの競合が発生するため、トレースバックおよびリロードする
CSCwp97862	フェイルオーバー IPSEC PSK が 78 文字以上の場合、HA が「Could not set failover ipsecpre-shared-key」で中断する

ID	見出し
CSCwp99130	FPR42xx：SNMP ポーリングにおいて、FanTray が実際に動作しているにもかかわらず、誤ってダウン状態で報告される
CSCwq07441	HA で設定されたインターフェイスのモニタリングが原因で、ASA を実行している FP2110 でメモリリークが観測された
CSCwq07808	イーサネットインターフェイスで速度を変更した後、FP3105 トレースバックとリロードが発生する
CSCwq11260	Fluentbit と呼ばれる syslog サーバーが fox syslog 形式を認識できず、出力ができない
CSCwq13032	3100/4200：アップグレード後に 1G 管理インターフェイスがフラッピングする
CSCwq15499	RAVPN 地理位置情報：サービス アクセス オブジェクトですべてまたは特定の国を有効にすると、展開が失敗する
CSCwq16926	2 つのプロセスが TD サブネット構造を解放しようとすると、トレースバックとリロードが発生する
CSCwq17612	HA によってリロードがトリガーされると、コンソールに誤った「フェイルオーバーリセット」ログが出力される。
CSCwq18679	CSM/CLI の ASA：最後の ACL 回線に access-list ACL_name 回線 line_nr コメントが存在せず、「Specified remark does not exist」というメッセージが表示される
CSCwq21101	無効なホストヘッダーにより、ASA インターフェイス IP アドレスが表示される
CSCwq21442	3RU MI インスタンスがベースラインまたは作成後にオフラインになる
CSCwq22206	キー再生成中に 'IKEv2 negotiation aborted due to ERROR: Platform errors' により、VPN が失われた
CSCwq24140	CIMC リセットによってセキュリティモジュールの再起動がトリガーされる。
CSCwq27217	ASA：脅威検出時にトレースバックとリロードが発生し、その後インターフェイスが不安定になる。
CSCwq29375	ASA/FTD：FP_PUNT の置換中にアサートがトリガーされた（aaa アカウントの一致）
CSCwq29706	SNMP 設定を編集後にトレースバックとリロードが発生する。

ID	見出し
CSCwq31137	Firepower 9300：DNM-2X100G インターフェイスが FXOS 2.17.0.518 へのアップグレード後にトラフィックを通過しない。
CSCwq31342	DNS 設定で FPR4200 | FPR3100 マルチインスタンスシャーシの展開が失敗した
CSCwq32085	crypto_archive を生成した後に FP3100/4200 を再起動すると、「KC ILK issue detected」というエラーがコンソールで発生した
CSCwq35960	OSPF：高可用性セットアップの両方のユニットで Lina がトレースバックおよびリロードする。
CSCwq39942	CVE-2025-32463：sudo：Sudo 1.9.17p1 より前では、ローカルユーザーが次を取得できる。
CSCwq39943	CVE-2025-32462：sudo：1.9.17p1 より前では、ユーザーは意図しないマシンでコマンドを実行できる。
CSCwq40256	暗号マップ ACL が特定のポートを使用している場合、インバウンド IPsec パケットが IPsec オフロードによってドロップされる。
CSCwq43711	アイドル SSH セッションが Fin フラグで正常に終了せず、設定されたタイムアウトを超えて存続する
CSCwq46058	ASA SNMP 応答の問題：奇数の OID に対してのみ応答が送信され、偶数には送信されない
CSCwq46143	SSE-ASAc 同期中に復元された修正を再コミットする
CSCwq46544	SSL 復号再署名ポリシーで curl を使用して大きなファイルをダウンロードする場合、ダウンロード速度が低下する問題を解決するために debug menu tls-offload option <> が提供されます
CSCwq47622	'TLS サーバーアイデンティティ検出' を有効にした後、Lina がトレースバックおよびリロードする
CSCwq48842	FTD：Snort を介した遅延パケットが発生したため、tcp-seq-past-win によってパケットがドロップされた
CSCwq50189	ASAv の展開が失敗した：コンソールが連続してスタック状態になる
CSCwq50373	HA での ASA/FTD：ブートアップ中の snmptranslate プロセスにより、高 CPU および IPC タイムアウトが発生し、スプリットブレインを引き起こす
CSCwq51981	FTD パッカートレーサが、ヒットしないルールのアクセスリストにコメントルール ID を表示する
CSCwq52188	'asp load-balance per-packet' を実行中に FTD がトレースバックする

ID	見出し
CSCwq52255	FTD 管理 IP アドレスへの SSH ログインで、/mnt/boot/application/*.de ファイルがないため、FTD CLISH ではなく FXOS シェルにログインする。
CSCwq53328	マルチキャストおよびユニキャストパケットが、ランダムなサブインターフェイスの正しいインスタンスに到達しない。
CSCwq54109	FTD 3130 HA Lina がトレースバックする（ikev2_bin2hex_string）
CSCwq55887	FMC 7.6 NAT 送信元および IP が統合イベントビューア内に入力されない
CSCwq56279	7.6 - Firepower 3100 シリーズ：CSCso00444 の修正が含まれていないバージョンから HA ペアを 7.6 にアップグレードすると、一部のファイアウォールがトレースバックおよびリロードループに入る。
CSCwq60586	バンドルイメージ存在検証エラーにより、FTD アップグレードが失敗した
CSCwq65955	FPR 4200：HA リンク ARP パケットがドロップされ、内部アップリンク linkChange カウンタが増加する
CSCwq70133	パスワードを変更した後、パスワードの有効期限がリセットされない
CSCwq70773	ASP ルールエンジンの問題を完全およびランタイムで表示
CSCwq72156	特定の条件において、複数の SNMP サーバーのいずれかに SNMP トラップが送信されない
CSCwq73994	ASA：Hyper-V でパフォーマンスと高い CPU 使用率が見られた
CSCwq74204	IKEv1 L2Lvpn がフェーズ 2 で、アップグレード後に "Rejecting IPsec tunnel: no matching crypto map entry" で失敗する。
CSCwq74738	RAVPN SSL/IKEV2 認証エラー：AAA プロセスの不正なファイバクラス
CSCwq74986	FTD：起動ループでインスタンスがスタック状態になる
CSCwq75116	IPv6 機能が停止し、リンクローカルアドレスが [DUPLICATE] とマークされ、スプリットブレインが原因で、フェイルオーバー後に IPv6 トラフィックが停止する
CSCwq76130	クラスタリング：クラスターリダイレクトのオフロードにより、SNMP トラフィックがドロップする
CSCwq78991	レプリケーション中に不完全な ACL ポリシールールを取得するが、ファイアウォールがクラスターに参加する
CSCwq79815	Cisco Secure Firewall Adaptive Security Appliance ソフトウェアおよび Secure Firewall Threat Defense ソフトウェア VPN Web サーバーの不正アクセスの脆弱性

ID	見出し
CSCwq79831	Cisco Secure Firewall Adaptive Security Appliance ソフトウェアおよび Secure Firewall Threat Defense ソフトウェア VPN Web サーバーのリモートコード実行の脆弱性
CSCwq81480	FTD MI：アップグレード後に SNMP ポーリングが機能しない
CSCwq82095	特定の IDP のメッセージが表示され SAML 応答が拒否された
CSCwq82225	'show service policy' で初期関連のドロップに対してドロップカウンタが増加しない
CSCwq85028	TCP サーバーを使用できないためにブロックされると、パケットキャプチャに誤った情報が表示される。
CSCwq85986	FP4225：SFP を含むインターフェイス：10/25G_LR_S（または CSR_S）が、ピア側のリブート後に起動しない。
CSCwq90072	2 つのコンテキストで ASDM 解析が失敗する
CSCwq92373	WA MI：2 つのアプリケーションが次の理由で応答しなくなる：アプリケーションインスタンス ftd. sma のエラーが報告された。再起動ループが原因で、インスタンス xxx が無効になっている。このアプリケーションインスタンスの再インストールを検討してください。
CSCwq92728	SSH 認証の TACACS+ 要求に ASA クライアント IP がない
CSCwq95241	Heimdall PID がないため FP2130 で再起動する
CSCwq95810	「no http server Basic-auth-client ASDM」で、ASDM から ASA への接続が許可される。
CSCwq96870	Firepower のシャットダウン時にインターフェイスが起動する
CSCwq98101	FTD HA でインラインセットが設定されている場合、ポリシー展開が失敗する
CSCwq98648	ASAv で RAM 割り当てが少ないと、'asdm image' コマンドで予期しない動作をトリガーする
CSCwr01482	SFP を挿入すると、FPR4215「Not supported」アラームが発生する
CSCwr04957	複数のオブジェクトの名前を変更した後に、展開が失敗する、またはトラフィックが設定されたルールに一致しない。
CSCwr05406	natAddrMapTable での snmpwalk 中に、HA stby ノードでトレースバックする
CSCwr05837	SNMP プロセスが継続的に再起動する

ID	見出し
CSCwr06290	ASA/FTD：DCERPC インスペクションによるスレッド名 CP Processing での ASA トレースバック
CSCwr10732	「logging permit-hostdown」が設定されているにもかかわらず、接続ブロッキングがアクティブになる
CSCwr12965	HA の両方のユニットが同時に暗号化アルゴリズムを変更した
CSCwr14186	"show asp drop" コマンドの使用方法に cmd-invalid-encap asp-drop タイプのコンテキストを追加
CSCwr15697	80 の枯渇による ssl_decrypt_cb のブロック
CSCwr19123	スタンバイがアクティブに変更されると、FPR HA ESP シーケンス番号の不一致により、アンチリプレイドロップが発生する。
CSCwr21375	FTD ポートステータスが FMC に正しく反映されない。
CSCwr21683	デプロイメントによってパフォーマンスプロファイルが変更され、実行中の構成を取得できない
CSCwr22256	FQDN リストが解決済み IP の 200 を超えるエントリを拡張しているときに、トレースバックが発生する
CSCwr22508	アップグレードが成功した後に、デバイスが起動せず、スタック状態になる
CSCwr24999	FP3140 FTD HA アップグレードでスタック状態になる
CSCwr26857	アイドル状態ではないにもかかわらず、1 時間後に SMB TCP 接続が終了したため、ファイルポリシーが動作を停止した
CSCwr27095	以前の tunnel-group に基づいて、AnyConnect ユーザーがプロンプトを誤って取得する
CSCwr28908	ASA：asdm イメージを保存した後にトレースバックとリロードが発生する
CSCwr29314	暗号アクセラレータの表示は、最大暗号化スループットが 3K の場合 6 Gbps、FTDv の場合は 225Mbps であることを示します。
CSCwr31782	Cisco Secure Client SAML：IKEv2-IPsec と証明書マッピングを使用すると、外部ブラウザで証明書を要求することがある
CSCwr35582	ASA で継続的に logs_archive.asa-interface-idb.log が生成される
CSCwr42577	ASA/FTD がスレッド名「lina」を障害元スレッドに挙げてトレースバックし、リロードすることがある。

ID	見出し
CSCwr42969	ダイナミック オフロード フローが途中で中断された
CSCwr43586	「Unable to obtain connection lock (connection-lock)」という理由により、自己発信 ICMP TTL 超過メッセージが断続的にドロップする
CSCwr48605	パケットで誤ったオプションを受信したためLinaがトレースバックする。
CSCwr49028	SDI プロトコルを使用すると、セキュア クライアント トンネル グループ認証が影響を受ける。
CSCwr49171	Nitrox と KC2 間のインターラケン（ILK）リンク障害により、トラフィックバックプレッシャ/トラフィック障害が発生する
CSCwr50466	ASA/FTD：'show ssl objects' で X509_STORE_CTX に誤った値が表示される。
CSCwr51629	RTSP フローが、"First TCP packet not SYN" というドロップ理由でドロップされる
CSCwr55089	ASA/FTD：スレッド名 DATAPATH でトレースバックおよびリロードが発生する
CSCwr57552	レート制限 conn-limit SNMP トラップ
CSCwr59870	Hyper-v で Netvsc ドライバを実行すると、ブートループの問題が発生する
CSCwr61452	IPSec SA ポインタでのメモリ破損により ASA のトレースバックとリロードが発生する
CSCwr62800	ASAv で高いネットワーク遅延が観察された
CSCwr79344	Lina で ASA/FTD がトレースバックおよびリロードする
CSCwr84343	L2 テーブル作成時の ASA/FTD トレースバックとリロードが失敗する
CSCwr85470	FTD が順序が乱れたパケットをサイレントでドロップする
CSCws05886	手動フェイルオーバー中に ASA がトレースバックする

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。

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。