Cisco ASA シリーズ 9.6(x) リリースノート

初版：2016 年 3 月 21 日

最終更新：2017 年 12 月 13 日

Cisco ASA シリーズ 9.6(x) リリースノート

このドキュメントには、Cisco ASA ソフトウェアバージョン 9.6(x) のリリース情報が記載されています。

特記事項

- 潜在的なトラフィック停止（9.6(2.1) ～ 9.6(3)）：バグ CSCvd78303 が原因で、ASA は 213 日間の稼働時間後にトラフィックを渡すことを停止する可能性があります。各ネットワークへの影響は異なりますが、接続が制限されるという問題から始まり、停止などのより広範な影響を及ぼす可能性もあります。可能な場合は、こうしたバグのない新しいバージョンにアップグレードする必要があります。それまでは、ASA を再起動することでさらに 213 日間稼働させることができます。別の回避策を利用できる場合もあります。影響を受けるバージョンおよび詳細については、Field Notice FN-64291 を参照してください。
- Microsoft Azure サポートを含む ASAv 9.5.2(200) の各機能は 9.6(1) では使用できません。これらは、9.6(2) では使用可能です。
- ASDM 7.6(2) は、マルチコンテキストモードで AnyConnect クライアントプロファイルをサポートしています。この機能には、AnyConnect バージョン 4.2.00748 または 4.3.03013 以降が必要です。
- （ASA 9.6.2）マルチモード設定を使用している場合のアップグレードの影響：9.5.2 から 9.6.1 にアップグレードし、続いて 9.6.2 にアップグレードすると、マルチモード設定の既存の RAVPN が動作を停止します。9.6.2 イメージへのアップグレード後に、各コンテキストの記憶域を提供し、すべてのコンテキストで新しい AnyConnect イメージを取得するための再設定が必要となります。
- （ASA 9.6(2)）SSH 公開キー認証使用時のアップグレードの影響：SSH 認証が更新されることにより、SSH 公開キー認証を有効にするための新たな設定が必要となります。そのため、公開キー認証を使用した既存の SSH 設定はアップグレード後機能しません。公開キー認証は、Amazon Web サービス（AWS）の ASAv のデフォルトであるため、AWS のユーザはこの問題を確認する必要があります。SSH 接続を失う問題を避けるには、アップグレードの前に設定を更新します。または（ASDM アクセスが有効になっている場合）アップグレード後に ASDM を使用して設定を修正できます。

  ユーザ名が「admin」の場合の設定例を示します。

```
username admin nopassword privilege 15
username admin attributes
  ssh authentication publickey 55:06:47:eb:13:75:fc:5c:a8:c1:2c:bb:
  07:80:3a:fc:d9:08:a9:1f:34:76:31:ed:ab:bd:3a:9e:03:14:1e:1b hashed
```

ssh authentication コマンドを使用するには、アップグレードの前に次のコマンドを入力します。

```
aaa authentication ssh console LOCAL
username admin password <password> privilege 15
```

nopassword キーワードが存在している場合、これを維持するのではなく、代わりにユーザ名に対応したパスワードを設定することを推奨します。**nopassword** キーワードは、パスワードの入力不可を意味するのではなく、任意のパスワードを入力できます。9.6(2) より前のバージョンでは、**aaa** コマンドは SSH 公開キー認証に必須ではありませんでした。このため、**nopassword** キーワードはトリガーされませんでした。本バージョンより **aaa** コマンドは必須となり、**password**（または **nopassword**）キーワードが存在する場合、自動的に **username** の通常のパスワード認証を許可するようになりました。

アップグレード後は、**username** コマンドに対する **password** または **nopassword** キーワードの指定は任意となり、ユーザがパスワードを入力できないように指定できます。よって、公開キー認証のみを強制的に使用する場合は、**username** コマンドを入力しなおします。

```
username admin privilege 15
```

- Firepower 9300 で ASA をアップグレードする場合のアップグレードの影響：バックエンドにおけるライセンス権限付与名義の変更により、ASA 9.6（1）/FXOS 1.1.4 にアップグレードした場合、最初のリロードの際にスタートアップ コンフィギュレーションが正しく解析されず、アドオンの権利付与に対応する設定が拒否されることがあります。

  スタンドアロン ASA では、新バージョンでのリロード後、権限付与が処理され、「承認済み」状態になるのを待ち（[show license all] または[Monitoring] > [Properties] > [Smart License]）、そのまま設定を保存しないで、もう一度リロード（[reload] または[Tools] > [System Reload]）してください。リロードすると、スタートアップ コンフィギュレーションが正しく解析されます。

  フェールオーバーペアにアドオンの権限付与がある場合は、FXOS リリースノートのアップグレード手順に従い、さらに各装置のリロード後にフェールオーバーをリセットしてください（**failover reset**）。

  クラスタに関しては、FXOS のリリースノートのアップグレード手順に従います。以降、さらなる操作は不要です。

- ASA 5508-X および 5516-X を 9.5（x）以降へアップグレードする場合における問題：ASA バージョン 9.5（x）以降へアップグレードする前に、ジャンボフレーム予約を一度も有効

にしたことがない場合は、最大のメモリフットプリントをチェックする必要があります。製造上の不具合により、ソフトウェアのメモリ制限が誤って適用されていることがあります。以下の修正を適用せずに9.5（x）以降にアップグレードした場合、デバイスはブートアップ時にクラッシュします。この場合、ROMMON （「Load an Image for the ASA 5500-X Series Using ROMMON」） を使用して 9.4 にダウングレードし、次の手順を実行して再度アップグレードする必要があります。

1. 次のコマンドを入力して障害のステータスをチェックします。

```
ciscoasa# show memory detail | include Max memory footprint
Max memory footprint        =    456384512
Max memory footprint        =            0
Max memory footprint        =    456384512
```

456,384,512 より少ない値が [Max memory footprint] に戻される場合は障害が発生しているため、アップグレード前に次の手順を実施する必要があります。表示されるメモリが 456,384,512 以上であれば、この手順の残りをスキップして通常通りにアップグレードできます。

2. グローバル コンフィギュレーション モードを開始します。

```
ciscoasa# configure terminal
ciscoasa(config)#
```

3. 一時的にジャンボフレーム予約を有効にします。

```
ciscoasa(config)# jumbo-frame reservation
WARNING: This command will take effect after the running-config
is saved and the system has been rebooted. Command accepted.
INFO: Interface MTU should be increased to avoid fragmenting
jumbo frames during transmit
```

（注） ASA はリロードしません。

4. 設定を保存します。

```
ciscoasa(config)# write memory
Building configuration...
Cryptochecksum: b511ec95 6c90cadb aaf6b306 41579572
14437 bytes copied in 1.320 secs (14437 bytes/sec)
[OK]
```

5. ジャンボフレーム予約を無効にします。

```
ciscoasa(config)# no jumbo-frame reservation
WARNING: This command will take effect after the running-config is saved and
the system has been rebooted. Command accepted.
```

（注） ASA はリロードしません。

6. コンフィギュレーション ファイルを再保存します。

```
ciscoasa(config)# write memory
Building configuration...
Cryptochecksum: b511ec95 6c90cadb aaf6b306 41579572
14437 bytes copied in 1.320 secs (14437 bytes/sec)
[OK]
```

7. これで、バージョン 9.5（x）以降へアップグレードできます。

- ASA 9.x で使用する RSA ツールキットのバージョンは、ASA 8.4 で使用されたバージョンとは異なるため、これらの 2 つのバージョン間で PKI の動作に違いが生じます。

  たとえば、9.x ソフトウェアを実行している ASA では、フィールド長が 73 文字までの [Organizational Name Value]（OU）フィールドをもつ証明書のインポートが許可されます。8.4 ソフトウェアを実行している ASA では、60 文字までの OU フィールド名をもつ証明書のインポートが許可されます。この相違のため、ASA 9.x でインポートできる証明書を ASA 8.4 ではインポートできません。ASA 9.x 証明書をバージョン 8.4 を実行している ASA にインポートしようとすると、エラー「ERROR: Import PKCS12 operation failed.」が表示されます。

システム要件

このセクションでは、このリリースを実行するためのシステム要件を一覧表で示します。

ASA と ASDM の互換性

ASA/ASDM ソフトウェアおよびハードウェアの要件およびモジュールの互換性を含む互換性の詳細については、『Cisco ASA Compatibility』を参照してください。

VPN の互換性

VPN の互換性については、『Supported VPN Platforms, Cisco ASA 5500 Series 』を参照してください。

新機能

このセクションでは、各リリースの新機能を示します。

（注） 『syslog message guide』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 9.6(4) の新機能

リリース：2017年12月13日

このリリースに新機能はありません。

ASA 9.6(3.1) の新機能

リリース：2017年4月3日

（注） バージョン 9.6(3) は、バグ CSCvd78303 に基づき Cisco.com から削除されました。

機能	説明
AAA 機能	
SSH公開キー認証を使用するユーザの認証とパスワードを使用するユーザの認証を区別します。	9.6(2) より前のリリースでは、ローカルユーザデータベース（**ssh authentication**）を使用して AAA SSH 認証を明示的に有効にしなくても、SSH 公開キー認証（**aaa authentication ssh console LOCAL**）を有効にすることができました。9.6(2) では、ASA で AAA SSH 認証を明示的に有効にする必要がありました。このリリースでは、AAA SSH 認証を明示的に有効にする必要はありません。ユーザに対して **ssh authentication** コマンドを設定すると、このタイプの認証を使用するユーザのローカル認証がデフォルトで有効になります。さらに、明示的に AAA SSH 認証を設定すると、この設定はパスワード付きのユーザ名にのみ適用されます。また、任意の AAA サーバ タイプ（**aaa authentication ssh console radius_1** など）を使用できます。たとえば、一部のユーザはローカルデータベースを使用して公開キー認証を使用し、他のユーザは RADIUS でパスワードを使用できます。 変更されたコマンドはありません。

ASA 9.6(2) の新機能

リリース：2016年8月24日

機能	説明
プラットフォーム機能	
Firepower 4150 用の ASA を導入しました。	Firepower 4150 用の ASA を導入しました。 FXOS 2.0.1 が必要です。 追加または変更されたコマンドはありません。

機能	説明
ASAv のホット プラグ インターフェイス	システムがアクティブの状態で、ASAv の Virtio 仮想インターフェイスを追加または削除できます。ASAv に新しいインターフェイスを追加すると、仮想マシンがインターフェイスを検出し、プロビジョニングが行われます。既存のインターフェイスを削除すると、仮想マシンはインターフェイスに関連付けられているリソースを解放します。ホットプラグインターフェイスはカーネルベース仮想マシン（KVM）のハイパーバイザ上にある Virtio 仮想インターフェイスに制限されます。
ASAv10 での Microsoft Azure サポート	Microsoft Azure は、プライベート Microsoft Hyper V ハイパーバイザを使用するパブリッククラウド環境です。ASAv は、Hyper V ハイパーバイザの Microsoft Azure 環境でゲストとして実行されます。Microsoft Azure 上の ASAv は、4 つの vCPU、14 GB、4 つのインターフェイスをサポートする Standard D3 の 1 つのインスタンス タイプをサポートします。 バージョン *9.5(2.200)* でも同様です。
ASAv の Management 0/0 インターフェイスでの通過トラフィック サポート	ASAv の Management 0/0 インターフェイスでトラフィックを通過させることができるようになりました。以前は、Microsoft Azure 上の ASAv のみで通過トラフィックをサポートしていました。今後は、すべての ASAv で通過トラフィックがサポートされます。任意で、このインターフェイスを管理専用に設定できますが、デフォルトでは管理専用に設定されていません。 次のコマンドが変更されました。 **management-only**

コモンクライテリア証明書	ASA は、コモンクライテリアの要件に適合するように更新されました。この証明書に追加された次の機能については、この表の行を参照してください。
	• ASDM での ASA SSL サーバモードマッチング
	• SSL クライアントの RFC 6125 サポート：
	  • セキュアな syslog サーバの接続とスマートライセンシング接続のための参照 ID
	  • ASA クライアントによるサーバ証明書の拡張キーの使用状況確認
	  • ASA が TLS1.1 と 1.2 の TLS クライアントとして動作する際の相互認証
	• PKI デバッグメッセージ
	• 暗号キー抹消検査
	• IKEv2 の IPsec/ESP トランスポートモードのサポート
	• 追加された syslog メッセージ

ファイアウォール機能	
TCP 経由での DNS インスペクション	DNS over TCP トラフィック（TCP/53）を検査できるようになりました。 次のコマンドが追加されました。 **tcp-inspection**

機能	説明
MTP3 User Adaptation（M3UA）インスペクション	M3UA トラフィックを検査できるようになりました。また、ポイントコード、サービスインジケータ、およびメッセージのクラスとタイプに基づいてアクションを適用できるようになりました。 次のコマンドが追加または変更されました。**clear service-policy inspect m3ua** {**drops** | **endpoint** [*IP_address*]}、**inspect m3ua**、**match dpc**、**match opc**、**match service-indicator**、**policy-map type inspect m3ua**、**show asp table classify domain inspect-m3ua**、**show conn detail**、**show service-policy inspect m3ua** {**drops** | **endpoint** *IP_address*}、**ss7 variant**、**timeout endpoint**
Session Traversal Utilities for NAT（STUN）インスペクション	Cisco Spark を含む WebRTC アプリケーションの STUN トラフィックを検査できるようになりました。インスペクションでは、リターントラフィックに必要なピンホールが開きます。 次のコマンドが追加または変更されました。**inspect stun**、**show conn detail**、**show service-policy inspect stun**
Cisco クラウド Web セキュリティのアプリケーション層健全性チェック	サーバが正常かどうかを判断する際に、クラウド Web セキュリティアプリケーションの健全性をチェックするように Cisco クラウド Web セキュリティを設定できるようになりました。アプリケーションの健全性を確認することで、プライマリサーバが TCP スリーウェイハンドシェイクに応答する場合に、システムはバックアップサーバにフェールオーバーできますが、要求を処理することはできません。これにより、より信頼性の高いシステムを実現します。 次のコマンドが追加されました。**health-check application url**、**health-check application timeout**
ルートの収束に対する接続ホールドダウンタイムアウト	接続で使用されているルートがもう存在していない、または非アクティブになったときに、システムが接続を保持する時間を設定できるようになりました。このホールドダウン期間内にルートがアクティブにならない場合、接続は解放されます。ルートの収束がさらに迅速に行われるようにホールドダウンタイマーを短縮することができます。ただし、ほとんどのネットワークでは、ルートのフラッピングを防止するためにデフォルトの 15 秒が適切です。 次のコマンドが追加されました。 **timeout conn-holddown** バージョン *9.4(3)* でも同様です。

機能	説明
TCP オプション処理の変更	TCP マップを設定する際にパケットの TCP ヘッダー内の TCP MSS および MD5 オプションに対するアクションを指定できるようになりました。さらに、MSS、タイムスタンプ、ウィンドウサイズ、および選択的確認応答オプションのデフォルトの処理が変更されました。以前は、これらのオプションは、ヘッダーに特定のタイプのオプションが 2 つ以上ある場合でも許可されていました。現在は、パケットに特定のタイプのオプションが 2 つ以上含まれている場合、そのパケットはデフォルトでドロップされます。たとえば、以前は 2 つのタイムスタンプオプションがあるパケットは許可されていましたが、現在はドロップされます。 MD5、MSS、選択的確認応答、タイムスタンプ、およびウィンドウサイズに対し、同じタイプの複数のオプションを有効にするための TCP マップを設定できます。MD5 オプションの場合、以前のデフォルトではオプションがクリアされたのに対し、現在のデフォルトでは許可されます。また、MD5 オプションを含むパケットをドロップすることもできます。MSS オプションの場合は、TCP マップで最大セグメントサイズを設定できます（トラフィック クラスごとに）。他のすべての TCP オプションのデフォルトに変更はありません。これらはクリアされます。 次のコマンドが変更されました。 **tcp-options**
トランスペアレントモードで、ブリッジグループごとのインターフェイス数が最大で 64 に増加	ブリッジグループあたりのインターフェイスの最大数が 4 から 64 に拡張されました。 変更されたコマンドはありません。
トランスペアレントモードでのマルチキャスト接続のフローオフロードのサポート	トランスペアレントモードの Firepower 4100 および 9300 シリーズ デバイスで、NIC に直接切り替えられるマルチキャスト接続をオフロードできるようになりました。マルチキャストオフロードは、インターフェイスを 2 つだけ含むブリッジグループに使用できます。 この機能には、新規のコマンドまたは ASDM 画面はありません。
カスタマイズ可能な ARP レート制限	1 秒あたり許可される ARP パケットの最大数を設定できます。デフォルト値は ASA モデルによって異なります。この値は ARP ストーム攻撃を防ぐためにカスタマイズできます。 次のコマンドを追加しました。**arp rate-limit**、**show arp rate-limit**
IEEE 802.2 論理リンク制御（LLC）パケットの Destination Service Access Point（DSAP）アドレスに対する Ethertype ルールのサポート	IEEE 802.2 論理リンク制御パケットの宛先サービスアクセスポイントのアドレスに対する Ethertype のアクセス制御ルールを作成できるようになりました。この追加により、**bpdu** キーワードが対象トラフィックに一致しなくなります。**dsap 0x42** に対して **bpdu** ルールを書き換えます。 次のコマンドが変更されました。 **access-list ethertype**
リモートアクセス機能	

機能	説明
マルチコンテキストモードの場合の証明書の事前入力/ユーザ名	AnyConnect SSL サポートが拡張され、これまでシングル モードでのみ使用可能だった証明書の事前入力とユーザ名取得機能の CLI がマルチコンテキストモードでも有効にできるようになりました。 変更されたコマンドはありません。
リモートアクセス VPN のフラッシュ仮想化	マルチコンテキストモードのリモートアクセス VPN はフラッシュ仮想化をサポートします。使用可能な合計フラッシュに基づき、コンテキストごとにプライベート記憶域と共有ストレージの場所が設定できます。 • プライベート記憶域：該当ユーザのみに関連付けられ、該当ユーザ対象コンテンツ固有のファイルを保存します。 • 共有ストレージ：有効になると、この領域にファイルがアップロードされ、あらゆるユーザコンテキストが読み取り/書き込みできるようこの領域へのアクセスが許可されます。 次のコマンドが導入されました。**limit-resource storage**、**storage-url**
マルチコンテキストモードでの AnyConnect クライアントプロファイルのサポート	マルチコンテキストモードで AnyConnect クライアントプロファイルがサポートされました。ASDM を使用して新しいプロファイルを追加するには、AnyConnect セキュア モビリティ クライアント リリース 4.2.00748 または 4.3.03013 以降が必要です。
マルチコンテキストモードの AnyConnect 接続のステートフル フェールオーバー	マルチコンテキストモードで AnyConnect 接続のステートフル フェールオーバーがサポートされました。 変更されたコマンドはありません。
マルチコンテキストモードでリモートアクセス VPN ダイナミック アクセス ポリシー（DAP）がサポートされました。	マルチコンテキスト モードで、コンテキストごとに DAP を設定できるようになりました。 変更されたコマンドはありません。
マルチコンテキストモードでリモートアクセス VPN CoA（認可変更）がサポートされました。	マルチコンテキストモードで、コンテキストごとに CoA を設定できるようになりました。 変更されたコマンドはありません。
マルチコンテキストモードで、リモートアクセス VPN のローカライズがサポートされました。	ローカリゼーションがグローバルでサポートされました。複数のコンテキストで共有されるローカリゼーション ファイル セットは 1 つだけです。 変更されたコマンドはありません。
Umbrella ローミング セキュリティ モジュールのサポート	アクティブな VPN がない場合には、DNS 層のセキュリティを強化するため、AnyConnect セキュア モビリティ クライアントの Umbrella ローミング セキュリティ モジュールを設定できます。 変更されたコマンドはありません。

機能	説明
IKEv2 の IPsec/ESP トランスポートモードのサポート	ASA IKEv2 ネゴシエーションでトランスポートモードがサポートされるようになりました。これは、トンネル（デフォルト）モードの代わりに使用できます。トンネルモードでは IP パケット全体がカプセル化されます。トランスポートモードでは IP パケットの上位層プロトコルだけがカプセル化されます。トランスポートモードでは、送信元ホストと宛先ホストの両方が IPSec をサポートしている必要があります。また、トランスポートモードは、トンネルの宛先ピアが IP パケットの最終宛先である場合にだけ使用されます。 次のコマンドが変更されました。**crypto map set ikev2 mode**
IPsec 内部パケットに対するパケット単位のルーティングルックアップ	デフォルトでは、外部 ESP パケットに対してはパケット単位の隣接関係（アジャセンシー）ルックアップが行われ、IPsec トンネル経由で送信されるパケットに対してはルックアップが行われません。一部のネットワークトポロジでは、ルーティングアップデートによって内部パケットのパスが変更され、ローカル IPsec トンネルが引き続きアップ状態である場合、トンネル経由のパケットは正しくルーティングされず、宛先に到達しません。これを防止するには、新しいオプションを使用し、IPsec 内部パケットに対してパケット単位のルーティングルックアップを有効にします。 次のコマンドが追加されました。**crypto ipsec inner-routing-lookup**
証明書とセキュアな接続の機能	
ASA クライアントによるサーバ証明書の拡張キーの使用状況確認	syslog、スマートライセンスサーバ証明書は、[Extended Key Usage] フィールドに [ServerAuth] を含める必要があります。そうしない場合、接続は失敗します。
ASA が TLS1.1 と 1.2 の TLS クライアントとして動作する際の相互認証	サーバが認証のために ASA からクライアント証明書を要求した場合、ASA はそのインターフェイス用に設定されたクライアントアイデンティティ証明書を送信します。証明書は **ssl trust-point** コマンドで設定されます。
PKI デバッグメッセージ	ASA PKI モジュールは、SCEP 登録、HTTP を使用した失効チェックなどのために CA サーバへ接続します。これらすべての ASA PKI 通信はデバッグ追跡のため、debug crypto ca メッセージ 5 を付してログに記録されます。
ASDM での ASA SSL サーバモードマッチング	証明書マップと照合するために、証明書で認証を行う ASDM ユーザに対して証明書を要求できるようになりました。 次のコマンドを変更しました。**http authentication-certificate match**
セキュアな syslog サーバの接続とスマートライセンシング接続のための参照 ID	TLS クライアント処理は、RFC 6125 のセクション 6 に定義されるサーバ ID の検証ルールをサポートするようになりました。ID 確認は syslog サーバとスマートライセンスサーバへの TLS 接続の PKI 確認中に行われます。提示された ID が設定されたリファレンス ID と一致しない場合、接続を確立できません。 次のコマンドが追加または変更されました。**crypto ca reference-identity**、**logging host**、**call home profile destination address**

機能	説明
暗号キー抹消検査	ASA の暗号化システムは、新しい暗号キー抹消要件に適合するように更新されました。キーはすべてゼロで上書きされ、データを読み出して上書きが正しく行われたか確認する必要があります。
SSH 公開キー認証の改善	以前のリリースでは、ローカルユーザデータベース（**(aaa authentication ssh console LOCAL)**）を使用して AAA SSH 認証を有効にしなくても、SSH 公開キー認証（**(ssh authentication)**）を有効にすることができました。この設定は修正されたため、AAA SSH 認証を明示的に有効にする必要があります。ユーザが秘密キーの代わりにパスワードを使用できないよう、パスワード未定義のユーザ名を作成できるようになりました。 次のコマンドが変更されました。**ssh authentication**、**username**
インターフェイス機能	
Firepower 4100/9300 シャーシの ASA のMTU サイズ増加	Firepower 4100 および 9300 で、最大 MTU を 9188 バイトに設定できます。これまでは 9000 バイトが最大でした。この MTU は FXOS 2.0.1.68 以降でサポートされます。 次のコマンドが変更されました。**mtu**
ルーティング機能	
Bidirectional Forwarding Detection（BFD）のサポート	ASAは、BFD ルーティングプロトコルをサポートするようになりました。BFD テンプレート、インターフェイスおよびマッピングの設定が新たにサポートされました。BFD を使用するための BGP ルーティングプロトコルのサポートも追加されました。 次のコマンドが追加または変更されました。 **authentication**、**bfd echo**、**bfd interval**、**bfd map**、**bfd slow-timers**、**bfd template**、**bfd-template**、**clear bfd counters**、**echo**、**debug bfd**、**neighbor fall-over bfd**、**show bfd drops**、**show bfd map**、**show bfd neighbors**、**show bfd summary**

機能	説明
IPv6 DHCP	ASA で IPv6 アドレッシングの次の機能がサポートされました。 • DHCPv6 アドレスクライアント：ASA は DHCPv6 サーバから IPv6 グローバルアドレスとオプションのデフォルトルートを取得します。 • DHCPv6 プレフィックス委任クライアント：ASA は DHCPv6 サーバから委任プレフィックスを取得します。ASA は、これらのプレフィックスを使用して他の ASA インターフェイスのアドレスを設定し、ステートレスアドレス自動設定（SLAAC）クライアントが同じネットワーク上で IPv6 アドレスを自動設定できるようにします。 • 委任プレフィックスの BGP ルータアドバタイズメント • DHCPv6 ステートレスサーバ：SLAAC クライアントが ASA に情報要求（IR）パケットを送信すると、ASA はドメインインネームなどの他の情報を SLAAC クライアントに提供します。ASA は、IR パケットを受け取るだけで、クライアントにアドレスを割り当てません。 次のコマンドが追加または変更されました。**clear ipv6 dhcp statistics**、**domain-name**、**dns-server**、**import**、**ipv6 address autoconfig**、**ipv6 address dhcp**、**ipv6 dhcp client pd**、**ipv6 dhcp client pd hint**、**ipv6 dhcp pool**、**ipv6 dhcp server**、**network**、**nis address**、**nis domain-name**、**nisp address**、**nisp domain-name**、**show bgp ipv6 unicast**、**show ipv6 dhcp**、**show ipv6 general-prefix**、**sip address**、**sip domain-name**、**sntp address**
高可用性と拡張性の各機能	
アクティブ/スタンバイフェールオーバーを使用するとき、AnyConnect からのダイナミック ACL の同期時間が改善されました。	フェールオーバーペアで AnyConnect を使用するとき、関連付けられているダイナミック ACL（dACL）のスタンバイユニットへの同期時間が改善されました。以前は、大規模な dACL の場合、スタンバイユニットが可用性の高いバックアップを提供するのではなく同期作業で忙しい間は、同期時間が長時間に及ぶことがありました。 変更されたコマンドはありません。
ライセンシング機能	

機能	説明
ASAv の永続ライセンス予約	Cisco Smart Software Manager との通信が許可されていない非常にセキュアな環境では、ASAv 用に永続ライセンスを要求できます。9.6(2) では、Amazon Web サービスの ASAv 向けに、この機能のサポートが追加されました。この機能は Microsoft Azure ではサポートされません。 （注） すべてのアカウントがパーマネントライセンスの予約について承認されているわけではありません。設定を開始する前にこの機能についてシスコの承認があることを確認します。 次のコマンドが導入されました。**license smart reservation、license smart reservation cancel、license smart reservation install、license smart reservation request universal、license smart reservation return** バージョン *9.5(2.200)* でも同様です。
ASAv のサテライトサーバのサポート	デバイスがセキュリティ上の理由でインターネットにアクセスができない場合、オプションで、仮想マシン（VM）としてローカル Smart Software Manager サテライトサーバをインストールできます。 変更されたコマンドはありません。
ASAv の短かい文字列の拡張機能向けの永続ライセンス予約	スマートエージェント（1.6.4 への）の更新により、要求と認証コードには短い文字列が使用されます。 変更されたコマンドはありません。
Firepower 4100/9300 シャーシ 上の ASA の永続ライセンス予約	Cisco Smart Software Manager との通信が許可されていない非常にセキュアな環境では、FirePOWER 9300 および FirePOWER 4100 の ASA 用に永続ライセンスを要求できます。永続ライセンスには、標準層、高度暗号化（該当する場合）、セキュリティコンテキスト、キャリアライセンスをはじめ、使用可能なすべてのライセンス権限が含まれます。FXOS 2.0.1 が必要です。 すべての設定はFirepower 4100/9300 シャーシで実行され、ASA の設定は不要です。

機能	説明
ASAv用スマートエージェントのv1.6へのアップグレード	スマートエージェントはバージョン 1.1 からバージョン 1.6 へアップグレードされました。このアップグレードは永続ライセンス予約をサポートするほか、ライセンスアカウントに設定された権限に従って、高度暗号化（3DES/AES）ライセンス権限の設定もサポートします。 （注） バージョン 9.5 （2.200）からダウングレードした場合、ASAv はライセンス登録状態を保持しません。**license smart register idtoken** *id_token* **force** コマンドを使用し、再登録する必要があります。Smart Software Manager から ID トークンを取得します。 次のコマンドが導入されました。**show license status**、**show license summary**、**show license udi**、**show license usage** 次のコマンドが変更されました。**show license all**、**show tech-support license** 次のコマンドが非推奨になりました。 **show license cert**、**show license entitlement**、**show license pool**、**show license registration** バージョン *9.5(2.200)* でも同様です。
モニタリング機能	
type asp-drop のパケットキャプチャは、ACL と一致フィルタリングをサポートします。	asp-drop タイプのパケットキャプチャを作成するとき、ACL または一致するオプションを指定してキャプチャの範囲を制限できるようになりました。 次のコマンドが変更されました。**capture type asp-drop**
フォレンジック分析の強化	ASA で実行されているすべてのプロセスのコアダンプを作成できます。主な ASA プロセスのテキストセクションを抽出し、検証用にコピーできます。 次のコマンドが変更されました。**copy system:text**、**verify system:text**、**crashinfo force dump process**
NetFlow経由の接続ごとのトラッキングパケット数の追跡	NetFlow ユーザがある接続上で双方向に送受信されるレイヤ 4 パケットの数を確認することを可能にする 2 つのカウンタが追加されました。これらのカウンタを使用して、平均パケットレートおよびサイズを判断し、トラフィックタイプ、異常、イベントをより適切に予測できます。 変更されたコマンドはありません。

機能	説明
フェールオーバーの SNMP engineID の同期	フェールオーバーペアでは、一対の ASA の SNMP engineID は両方のユニットで同期されます。ASA ごとに、同期された engineID、ネイティブ engineID、およびリモート engineID による engineID が 3 セット維持されます。 SNMPv3 ユーザは、ローカライズされた **snmp-server user** 認証とプライバシーオプションを保存するためのプロファイルを作成するときに ASA の engineID も指定できます。ユーザがネイティブ engineID を指定しない場合、**show running config** 出力に engineID がユーザごとに 2 つずつ表示されます。 次のコマンドが変更されました。**snmp-server user** バージョン *9.4(3)* でも同様です。

ASA 9.6(1) の新機能

リリース：**2016年3月21日**

（注） Microsoft Azure サポートを含む ASAv 9.5.2(200) の各機能は 9.6(1) では使用できません。 これらは、9.6(2) では使用可能です。

機能	説明
プラットフォーム機能	
Firepower 4100 シリーズ の ASA	Firepower 4110、4120、4140 用の ASA を導入しました。 FXOS 1.1.4 が必要です。 追加または変更されたコマンドはありません。
ISA 3000 の SD カードのサポート	ISA 3000 の外部ストレージとして SD カードが使用できるようになりました。カードは、ASA ファイルシステムのディスク 3 として表示されます。プラグアンドプレイをサポートするにはハードウェアバージョン 2.1 以降が必要です。ハードウェアバージョンをチェックするには、**show module** コマンドを使用します。 追加または変更されたコマンドはありません。
ISA 3000 のデュアル電源サポート	ISA 3000 のデュアル電源では、ASA OS に望ましい構成としてデュアル電源を設定できます。1 つの電源に障害が発生すると、ASA はアラームを発します。デフォルトでは、ASA は単一電源を想定していますが、装備される電源のいずれかが機能しているかぎりアラームを発しません。 次のコマンドが導入されました。**power-supply dual**
ファイアウォール機能	

機能	説明
Diameter インスペクションの改善	TCP/TLS トラフィック上の Diameter を検査し、厳密なプロトコル準拠チェックを適用し、クラスタモードで SCTP 上の Diameter を検査できるようになりました。 次のコマンドが導入または変更されました。**client clear-text**、**inspect diameter**、**strict-diameter**
クラスタモードでの SCTP ステートフル インスペクション	SCTP ステートフル インスペクションがクラスタモードで動作するようになりました。また、クラスタモードで SCTP ステートフル インスペクション バイパスを設定することもできます。 追加または変更されたコマンドはありません。
H.460.18 互換性に関連する H.225 SETUP メッセージの前に着信する H.255 FACILITY メッセージに対する H.323 インスペクションのサポート。	H.225 FACILITY メッセージが H.225 SETUP メッセージの前に着信する（これは、エンドポイントが H.460.18 に準拠する場合に発生する場合があります）ことを許可するように H.323 インスペクション ポリシー マップを設定できるようになりました。 次のコマンドが導入されました。**early-message**
Security Exchange Protocol（SXP）バージョン 3 の Cisco TrustSec サポート。	ASA の Cisco Trustsec は、ホストバインディングよりも効率的な SGT とサブネット間のバインディングを可能にする SXPv3 を実装するようになりました。 次のコマンドが導入または変更されました。**cts sxp mapping network-map** *maximum_hosts*、**cts role-based sgt-map**、**show cts sgt-map**、**show cts sxp sgt-map**、**show asp table cts sgt-map**
Firepower 4100 シリーズのフローオフロードのサポート。	ASA からオフロードされ、Firepower 4100 シリーズの NIC で直接切り替える必要があるフローを特定できるようになりました。 FXOS 1.1.4 が必要です。 追加または変更されたコマンドはありません。
リモートアクセス機能	
IKEv2 フラグメンテーション、RFC-7383 サポート	ASA では、IKEv2 パケットのこの標準的なフラグメンテーションがサポートされるようになりました。これにより、Apple、Strongswan など、他の IKEv2 の実装との相互運用性を実現します。ASA は、AnyConnect クライアントなどの RFC-7383 をサポートしないシスコ製品との後方互換性を保つため、独自の IKEv2 フラグメンテーションを引き続きサポートします。 次のコマンドが導入されました。 **crypto ikev2 fragmentation**、**show running-config crypto ikev2**、**show crypto ikev2 sa detail**
Firepower 9300 と Firepower 4100 シリーズでの VPN スループット パフォーマンス強化	**crypto engine accelerator-bias** コマンドが Firepower 9300 と Firepower 4100 シリーズ上の ASA セキュリティモジュールでサポートされるようになりました。このコマンドにより、IPSec または SSL に対して暗号コアを「優先的に使用」できます。 次のコマンドが変更されました。 **crypto engine accelerator-bias**

機能	説明
設定可能な SSH 暗号機能と HMAC アルゴリズム	ユーザはSSH暗号化を管理するときに暗号化モードを選択し、さまざまなキー交換アルゴリズムに対して HMAC と暗号化を設定できます。アプリケーションに応じて、暗号の強度を強くしたり弱くする必要がある場合があります。セキュアなコピーのパフォーマンスは暗号化アルゴリズムに一部依存します。デフォルトで、ASA は 3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr の順にアルゴリズムをネゴシエートします。提示された最初のアルゴリズム（3des-cbc）が選択された場合、aes128-cbc などの一層効率的なアルゴリズムが選択された場合よりも大幅にパフォーマンスが低下します。たとえば、提示された暗号方式に変更するには、**ssh cipher encryption custom aes128-cbc** を使用します。 次のコマンドが導入されました。**ssh cipher encryption**、**ssh cipher integrity** *9.1(7)* 、*9.4(3)* および *9.5(3)* でも使用可能です。
IPv6 の HTTP リダイレクトサポート	ASDM アクセスまたはクライアントレス SSL VPN 用の HTTPS に HTTP リダイレクトを有効にすると、IPv6アドレスへ送信されるトラフィックもリダイレクトできるようになりました。 次のコマンドに機能が追加されました。**http redirect** *9.1(7)* および *9.4(3)* でも使用可能です。
ルーティング機能	
IS-IS ルーティング	ASA で Intermediate System to Intermediate System（IS-IS）のルーティングプロトコルがサポートされました。IS-IS ルーティングプロトコルを使用した、データのルーティング、認証の実行、およびルーティング情報の再配布とモニタについて、サポートが追加されました。 次のコマンドを導入しました。 **advertise passive-only, area-password, authentication key, authentication mode, authentication send-only, clear isis, debug isis, distance, domain-password, fast-flood, hello padding, hostname dynamic, ignore-lsp-errors, isis adjacency-filter, isis advertise prefix, isis authentication key, isis authentication mode, isis authentication send-only, isis circuit-type, isis csnp-interval, isis hello-interval, isis hello-multiplier, isis hello padding, isis lsp-interval, isis metric, isis password, isis priority, isis protocol shutdown, isis retransmit-interval, isis retransmit-throttle-interval, isis tag, is-type, log-adjacency-changes, lsp-full suppress, lsp-gen-interval, lsp-refresh-interval, max-area-addresses, max-lsp-lifetime, maximum-paths, metric, metric-style, net, passive-interface, prc-interval, protocol shutdown, redistribute isis, route priority high, route isis, set-attached-bit, set-overload-bit, show clns, show isis, show router isis, spf-interval, summary-address.**
高可用性と拡張性の各機能	

機能	説明
ルーテッドおよびスパンド EtherChannel モードのサイト固有の IP アドレスのポート	スパンド EtherChannel のルーテッドモードでのサイト間クラスタリングの場合、サイト個別の MAC アドレスに加えて、サイト個別の IP アドレスを設定できるようになりました。サイト IP アドレスを追加することにより、グローバル MAC アドレスからの ARP 応答を防止するために、ルーティング問題の原因になりかねない Data Center Interconnect（DCI）経由の移動によるオーバーレイトランスポート仮想化（OTV）デバイスの ARP 検査を使用することができます。MAC アドレスをフィルタ処理するために VACL を使用できないスイッチには、ARP 検査が必要です。 次のコマンドが変更されました。**mac-address**、**show interface**
管理機能	
ローカルの **username** および **enable** パスワードでより長いパスワード（127 文字まで）がサポートされます。	127 文字までのローカル **username** および **enable** パスワードを作成できます（以前の制限は 32 文字でした）。32 文字以上のパスワードを作成すると、PBKDF2（パスワードベースキー派生関数 2）のハッシュを使用して設定に保存されます。これよりも短いパスワードは引き続き MD5 ベースのハッシュを使用します。 次のコマンドを変更しました。**enable**、**username**
CISCO-ENHANCED-MEMPOOL-MIB の cempMemPoolTable のサポート	CISCO-ENHANCED-MEMPOOL-MIB の cempMemPoolTable がサポートされました。これは、管理型システムのすべての物理エンティティのメモリプールモニタリングエントリのテーブルです。 （注） CISCO-ENHANCED-MEMPOOL-MIB は 64 ビットのカウンタを使用して、プラットフォーム上の 4 GB 以上のメモリのレポーティングをサポートします。 追加または変更されたコマンドはありません。 *9.1(7)* および *9.4(3)* でも使用可能です。
REST API バージョン 1.3.1	REST API バージョン 1.3.1 のサポートが追加されました。

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。

ASA のアップグレードパス

現在のバージョンとモデルを表示するには、次のいずれかの方法を使用します。

- CLI：**show version** コマンドを使用します。
- ASDM：**[Home]** > **[Device Dashboard]** > **[Device Information]** の順に選択します。

次の表で、お使いのバージョンのアップグレードパスを参照してください。バージョンによっては、新しいバージョンにアップグレードする前に、中間アップグレードが必要な場合があります。推奨バージョンは**太字**で示されています。

現在のバージョン	暫定アップグレードバージョン	ターゲットバージョン
9.3(x)	—	次のいずれかになります。 → 9.4(x) → 9.3(x)
9.2(x)	—	次のいずれかになります。 → 9.4(x) → 9.3(x) → 9.2(x)
9.1(2)、9.1(3)、9.1(4)、9.1(5)、9.1(6)、または 9.1(7.4)	—	次のいずれかになります。 → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3)、9.1(4)、9.1(5)、9.1(6)、9.1(7.4)
9.1(1)	→ 9.1(2)	次のいずれかになります。 → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3)、9.1(4)、9.1(5)、9.1(6)、9.1(7.4)
9.0(2)、9.0(3)、または 9.0(4)	—	次のいずれかになります。 → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3)、9.1(4)、9.1(5)、9.1(6)、9.1(7.4)

現在のバージョン	暫定アップグレードバージョン	ターゲットバージョン
9.0(1)	→ 9.0(2)、9.0(3) または 9.0(4)	次のいずれかになります。 → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3)、9.1(4)、9.1(5)、9.1(6)、9.1(7.4)
8.6(1)	→ 9.0(2)、9.0(3) または 9.0(4)	次のいずれかになります。 → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3)、9.1(4)、9.1(5)、9.1(6)、9.1(7.4)
8.5(1)	→ 9.0(2)、9.0(3) または 9.0(4)	次のいずれかになります。 → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3)、9.1(4)、9.1(5)、9.1(6)、9.1(7.4)
8.4(5+)	—	次のいずれかになります。 → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3)、9.1(4)、9.1(5)、9.1(6)、9.1(7.4)
8.4(1) ～ 8.4(4)	次のいずれかになります。 → 9.0(2)、9.0(3) または 9.0(4) → 8.4(6)	→ 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3)、9.1(4)、9.1(5)、9.1(6)、9.1(7.4)

現在のバージョン	暫定アップグレードバージョン	ターゲットバージョン
8.3(x)	→ 8.4(6)	次のいずれかになります。 → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3)、9.1(4)、9.1(5)、9.1(6)、9.1(7.4)
8.2(x) 以前	→ 8.4(6)	次のいずれかになります。 → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3)、9.1(4)、9.1(5)、9.1(6)、9.1(7.4)

アップグレードリンク

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

未解決のバグおよび解決されたバグ

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

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

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

バージョン 9.6(x) で未解決のバグ

次の表に、このリリースノートの発行時点で未解決のバグを示します。

警告 ID 番号	説明
CSCvb72148	ASAv5：メモリを 2 GB から 1 G へ削減し、9.4.1 から 9.6.2 へアップグレードした後に http を再度有効にできない

警告 ID 番号	説明
CSCvb95568	DOC：コマンドリファレンスですべての ASA SCH コマンドをドキュメント化する
CSCvd21406	「any」という名前のインターフェイスを持つ複数の PAT ルールが原因で 305006「portmap translation creation failed」となる
CSCve72751	スレッド名 DATAPATH での ASA トレースバック
CSCve78652	スレッド名 CTM message handler での ASA クラッシュ
CSCve95924	コンソール接続でアクセスされない限り、ASA はリロード後に起動しない
CSCvf10327	ENH：サブインターフェイスの作成時に一意の IPv6 リンクローカルアドレスが割り当てられる
CSCvf20094	「management-access <interface>」によってその int 上のすべての管理ソケットが開く
CSCvf30738	DATAPATH でアクティブ ASA がクラッシュしている
CSCvf39539	送受信したバイト数と IP アドレススイッチに NetFlow が大きな値を返す
CSCvf43974	Rest-API クエリが既存のリソースについて「Resource-not-found」を返す
CSCvf70284	フェールオーバー環境では、接続テーブルがアップグレード中に同期されない
CSCvf81672	EtherChannel に障害が発生した場合のフェールオーバー後に ASA ルートがフラッシュされる
CSCvf84839	SSL 復号/再署名による選択 ACK でのシーケンス番号が正しくない
CSCvg00265	OGS が有効になっている場合に、フェールオーバー HA がまたはメモリが不足しているクラスタに ASA が再参加できない
CSCvg05368	クラスタ参加時にスレーブユニットが PAT のすべての接続で枯渇している ASA-3-202010: NAT/PAT プールを生成する
CSCvg15947	ASA WebVPN スマートトンネル：Windows 8 および Windows 10 で DNS 解決が失敗する
CSCvg32530	宛先 IP としてのサブネットアドレスに ASA ブロードキャストのパケットが送信される
CSCvg39694	FP4120/ASA 9.6(3)230 「established tcp」が SW アップグレード後に動作しなくなる
CSCvg40735	GTP インスペクションが CPU 使用率をスパイクさせることがある

警告 ID 番号	説明
CSCvg53904	OSPF Not-So-Stubby Area のタイプ 7 がタイプ 5 に変換されない
CSCvg58385	ASA が PPPoe/VPDN インターフェイスで二重入力パケットトラフィックを誤って報告する
CSCvg69028	実行中の「show access-list」のスレッド名 idfw_proc での ASA トレースバック
CSCvg69301	ACL および NAT オブジェクトが IP から FQDN オブジェクトに変更された場合にトレースバックする
CSCvg69380	ASA：まれに発生した CP 処理での破損によってコンソールロックが発生する
CSCvg73584	SNP APP ID の使用率が高い
CSCvg74220	spin_lock_fair_mode_enqueue での ASA トレースバック：ロック（np_conn_shrlock_t）
CSCvg74549	オブジェクトグループ（display_hole_og）を使用してアクセスリストを保存/表示しようとするとトレースバックする
CSCvg82650	RDP セッションが ASA での SSL 証明書の変更後に確立されない。
CSCvg83588	DOC：IPsec over NAT-T がデフォルトで有効になっている
CSCvg91150	アサート「0」の ASA トレースバックが失敗した：ファイル「timer_services.c」
CSCvg93503	ASA では、「show module」で正しい BIOS バージョンが表示されない
CSCvg95033	「wr standby」が使用されている場合の IKE Reciver スレッドでのトレースバック
CSCvg95284	ASA でクリプトマップが有効になっているインターフェイスが shut/no shut された後に、リバースルートがインストールに失敗する
CSCvg95648	ASA：サブインターフェイスを使用する場合、フェールオーバー中にいくつかの ipv6 パケットがドロップする
CSCvg97594	ntp が設定されている場合、次回の登録試行時に誤った時間が表示され、登録を停止する
CSCvg98106	IPv6 アドレスへの ASA ping が指定された送信元 IP ではなく出力インターフェイスの送信元 IP を選択する
CSCvh02975	inspect sip で SDP ヘッダーの RTCP 属性が処理されていない
CSCvh07457	時間範囲オブジェクトと ACL の設定/変更時のトレースバック

警告 ID 番号	説明
CSCvh08040	ACE ヒットカウントが増加している場合でも、ACL ヒットカウントは増加していない
CSCvh11175	コアダンプが設定されたフェールオーバー遅延

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 9.6(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。

警告 ID 番号	説明
CSCto19051	ASA/FTD lina Heimdal Kerberos コードの脆弱性を解決する
CSCua53312	サーバからの DNS 応答が大きく、切り捨てられている場合、FQDN ACL エントリは不完全である可能性がある
CSCuj69650	ASA が「logging permit-hostdown」を使用して新しい接続をブロックし、TCP syslog がダウンしている
CSCuj98977	「show service set conn detail」を実行したときのスレッド SSH での ASA のトレースバック
CSCuu90811	GCM 暗号が使用されていると TLS CTP が TLSv 1.2 で機能しない
CSCuv63875	show ospf コマンドを実行中にスレッド名 ci/console で ASA がトレースバックする
CSCuw37752	FTP データ接続のスケーリングがダイナミック PAT で失敗する
CSCuz22961	スプリット DNS 値の 255 文字を超えてサポートする
CSCuz52474	2016 年 5 月の OpenSSL の pix-asa の評価
CSCuz72137	有効な ARP エントリが利用可能であっても、ASA が「novalid adjacency」でパケットをドロップする
CSCuz77293	クラスタスレーブに OSPF マルチキャスト フィルタ ルールがない
CSCva42669	SFR を使用した IP プロトコル 97 フローで相当大きなバイト数が確認される
CSCva92997	snp_fp_qos での 9.7.1 のトレースバック
CSCvb28491	show counters protocol ip を実行できない

警告 ID 番号	説明
CSCvb53233	%ASA-1-199010 と %ASA-1-716528 の syslog メッセージによる ASA 9.1(7)9 のトレースバック
CSCvb75685	「no vpnclient enable」の入力後、EZVPN NEM クライアントが再接続できない
CSCvb81438	TCP 接続はインライン モード インターフェイスを使用する FTD クラスタを介して失敗する可能性がある
CSCvb91810	ASA：異なるインターフェイスにより明確なルートが存在する場合にインターフェイスベースのルートルックアップが適切でない
CSCvb97470	asa Rest-api：コンポーネントモニタリング：空の値/空白値
CSCvc07112	スケジューラ破損の問題に対する検出と自動修正の機能を実装する
CSCvc24380	mqc_enable_qos_for_tunnel のスレッド名 IKE Daemon でのトレースバック
CSCvc27704	TCP が syslog のトランスポートプロトコルとして使用されるとログが失われる
CSCvc56526	CEP レコードの編集ページのロードに時間がかかる
CSCvc56919	IPv4 トンネルを介したリバース UDP/TCP IPv6 トラフィックのトラフィックがドロップする
CSCvc82270	ASA 1550 ブロックの段階的な枯渇
CSCvc83462	WebVPN を介して gzip 圧縮が機能しない
CSCvc85369	ASA が IPv6 MLD クエリに応答しない
CSCvc91839	XML 解析が正しくないため、FTD デバイスでポリシーを展開できない
CSCvc96614	ASA：単一のコマンド内に 9 個を超えるプロポーザルが設定されていると IKEv2 ipsec-proposal コマンドが削除される
CSCvd00293	VTI：一部のセッションが vpn-sessiondb からクリアされない
CSCvd01130	IP フォンが VPN トンネルの背後にあると ASA TCP SIP インスペクションの変換が機能しない
CSCvd08200	ASA での低速なメモリリーク
CSCvd14266	DATAPATH-41-16976 スレッドでの ASA トレースバック
CSCvd15843	データの受け渡し中に発生したグループポリシーの「vpn-idle-timeout」が原因で、ポート フォワーディング セッションがタイムアウト

警告 ID 番号	説明
CSCvd17581	ASA IKEv1：INVALID_ID_INFO Notify にゼロ以外の SPI を設定する
CSCvd20013	EZVPN クライアントでの「Thread Name: IPsec message handler」 でのトレースバック
CSCvd20408	FTD：lina CLI でのインターフェイスキャプチャによりすべてのトラフィックがデータプレーンでドロップされる
CSCvd21458	RSA キーはクラスタセットアップのコンテキスト間での同期に失敗する可能性がある
CSCvd24066	IM インスペクションが有効になっていると、ASA が Web トラフィックをドロップする
CSCvd26699	ASA が誤って syslog ID 201011 をトリガーする
CSCvd26939	SNMP が Firepower Threat Defense のすべての管理対象デバイスに同じホスト名をリストする
CSCvd29150	管理ルートの削除によりデータプレーンルートも削除される
CSCvd33044	アクセスコントロール ポリシー展開時の「cli_xmlserver_thread」 での FTD トレースバック
CSCvd33602	ASA が TACACS 監査パケットでエポックを送信しない
CSCvd33787	uauth による syslog.c でのアサーション
CSCvd35811	スレッド名 DATAPATH でのトレースバック
CSCvd36992	EtherChannel：無効になっているインターフェイス上の古いネイバーの SYSTEM ID が 5585-60 LACP の状態に表示される
CSCvd37850	9.6.2 DHCPRA：最大リレーバインディング数（500）を超過した
CSCvd43309	新しく作成されたオブジェクトグループのアクセスリストが一致しない
CSCvd47888	Cisco 適応型セキュリティアプライアンスのユーザ名列挙情報開示の脆弱性
CSCvd49262	ジャイアントオブジェクトグループ（display_hole_og）を使用してアクセスリストを保存/表示しようとするとトレースバックする
CSCvd49550	9.5.1 以上の ASAで managment0/0 を src-ip として使用すると SXP ソケットを表示しない
CSCvd50107	リマーク表示中に実行中の「show access-list」のスレッド名 idfw_proc で ASA がトレースバックする

警告 ID 番号	説明
CSCvd50389	RT#687120：クライアントレス VPN - SAML のブックマークに関する問題
CSCvd53381	設定を保存/表示すると時間範囲の ACL により ASA がトレースバックする
CSCvd55115	クラスタ内の ASA によりマスターとスレーブ間のユーザグループマッピングが適切でなくなる
CSCvd55999	%ASA-3-216001：ci_cons_shell での内部エラー：スレッドデータの誤用
CSCvd58094	PBR が設定されている場合に ARP スレッドで ASA がトレースバックする
CSCvd58321	Web フォルダのファイルブラウザ アプレット コードの署名証明書に期限が切れている
CSCvd58417	DCERPC インスペクションでパケットがドロップされ、通信が切断される
CSCvd61308	[実行コンフィギュレーション]エラーにより、マルチコンテキストの ASA バックアップが失敗する
CSCvd62509	ASDM で「アクセスルール」を表示している際のスレッド名 accept/http での ASA トレースバック
CSCvd64416	ASA のすべてのコンテキストがリロード時に同じ EIGRP ルータ ID を使用する
CSCvd64693	EIGRP を無効化および有効化した後で、EIGRP ルートが管理ルーティングテーブル vrf で誤ってアドバタイズされている
CSCvd65797	NAT 関連オブジェクトを FQDN に変更すると ASA がトレースバックすることがある
CSCvd66303	ESXi vCenter 6.5 での ASAv の導入中に発生したエラー
CSCvd68518	スレッド名 Unicorn Admin Handler でのトレースバック
CSCvd69551	時刻を指定して再アクティブ化モードが設定されているセカンダリ LDAP サーバへの接続にASA が失敗する
CSCvd69804	ASA：ipsec inner-routing-lookup の使用時にインターフェイスのステータスを変更することで VPN トラフィックが切断される
CSCvd71473	ASA：多くの DNS クエリを使用するとメモリリークが遅くなる
CSCvd73468	クラスタディレクタ接続がアイドルタイムアウトが原因でタイムアウトする
CSCvd76821	tcp-options md5 allow が tcp-options md5 clear としてスレーブユニットにプッシュされる

警告 ID 番号	説明
CSCvd76939	ASA ポリシーマップ設定がクラスタのスレーブに複製されない
CSCvd77893	アクセスグループの変更中に ASA がアサートのトレースバックを生成することがある
CSCvd78303	213 日の稼働後に ARP 関数が失敗し、「punt-rate-limit-exceeded」というエラーでドロップする
CSCvd79797	DNS サーバがサイト間 IPSec トンネルを通じて DNS サーバに到達可能な場合に ASA ローカル DNS 解決が失敗する
CSCvd79863	ECMP を持つ FTD OSPF で、既存の接続に対してダウン状態のピアにパケットが送信される
CSCvd80721	セキュリティコンテキストで SNMP イベントトラップを生成できない
CSCvd80740	FTD-VPN：VPN RRI がマスターユニットとスレーブユニットの間で同期されていない
CSCvd82064	Cisco 適応型セキュリティアプライアンスにおける認証済みクロスサイトスクリプティングの脆弱性
CSCvd82265	ASAv5 の rest-agent に割り当てられるメモリを増やす
CSCvd86411	ASA 9.6.2.11：クラスタでの CTP uauth による断続的な認証
CSCvd87211	設定されたキャプチャを削除しようとすると ASA がトレースバックする
CSCvd87647	9.1.5 から 9.4.3 へのアップグレード実行中にスレッド名 fover_parse で ASA がトレースバックする
CSCvd89003	SIP インスペクションによりデータパスで ASA のトレースバックが確認される
CSCvd89925	フェールオーバーペアのスタンバイユニットがアクティブに切り替えられない
CSCvd90096	WebVPN が IE に IE8 モードを使用するように強制する
CSCvd92423	ユニコーンプロキシスレッドでの ASA のトレースバック
CSCvd92489	モード転送を使用したトランスフォームセットがダイナミックマップの 11 番目の場合に L2TP/IPsec が失敗する
CSCvd97249	Cisco FirePOWER の検出エンジンの SSL 復号時のメモリ使用による Denial of Service（DoS）の脆弱性
CSCvd97568	フェールオーバーの同期時に FTD のトレースバックが確認される。

警告 ID 番号	説明
CSCvd99476	内部ブックマークサイトのインタラクティブアイコンが正しく表示されない（+CSCO+0undefined）
CSCvd99859	ASA がタイプ TXT の追加 RR のみを含む DNS 応答をドロップすることがある
CSCve02469	BGP のルート集約（auto-summary）とルートアドバタイズメントでの ASA の問題
CSCve02854	SFR バックプレーンが ASA 内部アドレスではなく、ポリシー照合のためのパブリックアドレスをプルしている
CSCve03387	SSH NLP NAT のプロキシ ARP 情報がフェールオーバー時に FTD で更新されない
CSCve03974	FirePOWER サービスを搭載した ASA モジュールがトレースバックとリロードを生成する
CSCve04326	出力インターフェイスがダウンしているときのトラフィックの転送にブラックホールではなく CCL を使用する必要がある
CSCve05841	クラスタに参加し、スレーブとしてアクティブな間に ASA がリロードした
CSCve06367	Show Crypto Acclerator は、ステータスをハードウェアデバイスの起動中と表示する
CSCve06436	ヒットレスアップグレード時に異なるマイナーバージョン間でルートが正常に同期されない
CSCve07856	CSCvd41423 の後の不正な KU により CRL の確認が失敗する
CSCve08664	Dist-S2S：マルチモードで vpn アイドルタイムアウトを通過した後も、トンネルがアップ状態を維持する
CSCve08898	トレースによるキャプチャとキャプチャのクリアによるメモリリーク
CSCve08947	マルチコンテキストで、インターフェイス PAT を使用している場合に特定のポートから送信されたトラフィックを ASA がドロップする
CSCve09249	ASA：アクティブ FTP が NAT の拡張キーワードでは動作しない
CSCve12654	CSM を使用したロールバック機能をサポートする ASA のクラスタリング
CSCve13410	ルート上での設定の追跡により、ASA のアップグレードが有効な隣接関係なしになる
CSCve15873	ASA：マルチキャストパケットがコード 9.6.3 以降ドロップされる

警告 ID 番号	説明
CSCve18293	データパス内で ASA のトレースバックが確認される
CSCve18880	クライアントレスポータルに証明書マップが使用されている場合にユーザ名が証明書から取得されない
CSCve19179	Cisco 適応型セキュリティアプライアンスの WebVPN クロスサイト スクリプティングの脆弱性
CSCve20346	アップグレード後に ASA SNI 接続が失敗する：共有暗号なし
CSCve20438	9.6.3.1 で「activate-tunnel-group-scripts」が使用できない
CSCve20980	CSCOGet_origin ラッパーがロケーションオブジェクトに属している場合は「origin」プロパティを処理しない
CSCve23033	ICMP 到達不能（PMTU）がドロップされ、「Routing failed to locate next hop」が表示される
CSCve23091	ルートがないために自動 RP パケットがドロップされる：ホストへのルートなし
CSCve23155	FXOS シャーシ上の ASA アプリケーションで BTF が停止するが、スマートライセンスにはこの機能が有効であると表示される
CSCve23784	アクセスリスト設定の表示時または実行コンフィギュレーションの保存時に ASA がトレースバックすることがある
CSCve24088	スマートライセンスの ID 証明書の更新の失敗で製品インスタンスの登録が解除されてはならない
CSCve24299	ルートが再配布されたときのスレッド名 IP RIB Update でのトレースバック
CSCve25577	FMC 展開で障害が発生した場合の、シャットダウン時のスレーブ上のインターフェイス
CSCve28027	ASA 上の CUCI Lync バージョン 11.6.3 でコールが動作しない
CSCve29989	ASA：PAT プールソケットの割り当て時に DATAPATH でトレースバックする
CSCve31809	ASA が l2tp クライアントからのリターントラフィックの宛先 Mac アドレスを破損させる
CSCve31880	まれに network_udpmod_get が shr_lock を解放しない
CSCve35799	設定時の CPU Hog CI_CONSOLE でのトレースバック

警告 ID 番号	説明
CSCve37948	UDP/4500 を使用した OSPF over IPSec を介して学習したルートを ASA がインストールしない
CSCve42460	リロード時に「NSF IETF/CISCO」コマンドが削除される
CSCve42583	ASA：FW を通過するための IPv6 プロトコル X ルールが無効な IP 長メッセージを持つパケットをドロップしている
CSCve43146	ASA の 9.5(3) 以降のすべてのバージョンで、ASDM 上での AnyConnect の新規カスタマイズの作成が失敗する
CSCve44561	SFR リダイレクションが有効になっている場合に、ICMP 到達不能タイプ 3 コード 4 を ASA が誤った方向に送信する
CSCve46883	FTD 診断インターフェイスが br1 管理サブネットの ARP をプロキシする
CSCve47393	最大シーケンス番号を持つ OSPF の不正 LSA の脆弱性
CSCve48105	スレーブが稼働している間、マスターのインターフェイスステータスを「init」と報告する
CSCve50118	ASA のメモリリーク：RSA ツールキット
CSCve53582	ASA への SSH 接続が SLA モニタリングと非ゼロのフローティング接続のタイムアウトで失敗する
CSCve53783	「service resetoutside」がすべてのインターフェイス上の to-the-device トラフィックに影響を与え、スタンバイ時に異なる動作をする
CSCve57150	VPN VLAN のマッピングの問題
CSCve57375	膨大な数の sunrpc セッションが原因で CP 処理スレッドでの CPU 占有が発生する
CSCve57548	ASA：crypto_SSL 関数のスレッド名 Datapath でトレースバックする
CSCve58709	ASA 9.5.1 以降、管理インターフェイスではなく、トラフィックが誤ってルーティングされる
CSCve60829	ASA クラスタ：PAT プールを使用したクラスタリンクで UDP がループする可能性がある
CSCve61284	TCP syslog サーバのダウン時に偽の IP データで ASA ログメッセージ 414003 が生成されることがある
CSCve62358	PBR のネクストホップがインターフェイスアドレスの場合に ASA 2048 ブロックが枯渇する
CSCve63762	ASASM：インターフェイス VLAN がリロード後に admin down になる

警告 ID 番号	説明
CSCve71712	webvpn-l7-rewriter：WebVPN ポータルを介した Jira 7.3.0 のログインページが完全に表示されない
CSCve72155	syslog サーバが VPN トンネルを介して到達可能な場合にロケーション「snp_fp_encrypt」でメモリリークが発生する
CSCve72201	ASA WebVPN リライターの問題。クライアントレス VPN を介して Web サイトのタブを参照できない
CSCve72227	ASA5506/5508/5516 で IPSec が起動せず、1,000 を超える IPSec SA カウントでフラップする
CSCve72964	DATAPATH-1-2084 ASA 9.(8)1 でのトレースバック
CSCve73025	週末の VPN ロードテスト後に 1700 個の「4 バイトブロック」がすべて枯渇した
CSCve73556	websns_rcv_tcp で ASA がトレースバックする
CSCve75132	フローブロックイベントの起動でイニシエータのバイト数が正しくない
CSCve77440	WebVPN によるユニコーンプロキシスレッドでのトレースバック
CSCve78986	ASA/9.6.3//WebVPN スマートトンネルは機能するが、イベントビューアを使用して Windows をフラッディングする
CSCve85698	ASA WebVPN リライター：WebVPN ブックマークの scholar.google.com が正しく記述されていない
CSCve91068	Cisco 適応型セキュリティアプライアンスの HREF クロスサイト スクリプティングの脆弱性
CSCve91223	インターフェイス IP と宛先が重複するとスタンバイ ASA が NAT を拒否し、アクティブがこれを許可する
CSCve94349	SNMP：ユーザが再設定後のユーザリストまたはホストに追加されない
CSCve94886	NAT ルールの変更時とパケットキャプチャが有効になっているときの ASA with Firepower Services でトレースバックが発生する
CSCve95969	フラッシュ仮想化機能を最大 250 コンテキストまで拡張できない
CSCve97831	ドメインルックアップが有効な場合に CDA エージェントが「プロービング」でスタックする
CSCve97844	3 回目のフェールオーバー後に ASA OSPF インターフェイスが DOWN の状態（NSF を待機中）でスタックする
CSCve97874	ASA：バージョン 9.6 以降での空き DMA メモリの不足

警告 ID 番号	説明
CSCvf01762	脆弱性 CVE-2017-1000364 および CVE-2017-1000366 の評価
CSCvf01873	HTTP 引数フィールドが正規表現に対応していない
CSCvf03676	SNMP 設定追加後に ASA でポートが予約されていない
CSCvf07075	ASA：暗号アクセラレータがループでトレースバックする
CSCvf11695	フローエクスポートアクションでのホストエントリの重複によりポリシー展開後にトレースバックが行われる
CSCvf14391	AnyConnect プールから送信されたマルチキャスト トラフィックがチェック済みのリバースパスによりドロップされる
CSCvf16142	ASA-5-720012：（VPN - セカンダリ）ASA クラスタ環境で IPSec フェールオーバー ランタイム データを更新できない
CSCvf16310	AnyConnect クライアントに IPv6 アドレスが断続的に割り当てられる
CSCvf16429	IKEv2 リモート アクセス クライアントのセッションが削除状態でスタックする
CSCvf16808	アクティブユニットに SSH 接続できない//TCP 接続の上限を超えている
CSCvf17214	破損した PKCS12 として ASA が ECDSA をエクスポートする
CSCvf17222	SAML 2.0 || (5525) 9.7.1 ASA：ASA コンパイラが SAML 認証のサインイン URL を取得していない
CSCvf21556	ASA：SNMP ホストグループがマルチコンテキスト設定の必要に応じて動作していない
CSCvf22190	ASA メモリリーク：DTLS セッション
CSCvf24063	DATAPATH - snp_vpn_process_natt_pkt で ASA5585 が トレースバックする
CSCvf24387	PKCS12s で ASA にインポートされる EC 証明書が SSL に使用できない
CSCvf25666	空きメモリが不足している ASA で既存のクラスタの参加が失敗し、トレースバックとリロードが発生する可能性がある
CSCvf28292	DAP 設定は復元されるが、バックアップ復元後に非アクティブになる
CSCvf28749	mroute が設定されている場合に ASA が register stop を送信しない
CSCvf31539	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
CSCvf34791	firepower - asa コアを搭載した ASA での 6.2.2 1290 sfr のインストール

警告 ID 番号	説明
CSCvf38655	バージョンアップ後の fover_parse での ASA トレースバック
CSCvf39679	既存の EIGRP 設定に新しいネットワークを追加できない
CSCvf41547	ウォッチドッグプロセスでのトレースバック
CSCvf43019	WebVPN リライターが内部 URL が原因で失敗する
CSCvf43150	ASA// 9.6 // FTP インスペクションで、PAT を使用したアクティブ FTP 上のデータトラフィックに新しい NAT 全体を割り当てられない
CSCvf43650	NSF が有効な状態で ASA フェールオーバーが実行されると OSPF ルートがピアデバイスにインストールされない
CSCvf44142	ASA 9.x：DNS インスペクションによって PTR クエリに「0」が追加される
CSCvf44950	iOS および OS X IKEv2 のネイティブクライアントが EAP-TLS を使用して ASA に接続できない
CSCvf46732	9.6 のコードでマスターになるとシャーシがリロードされた後、ASA でコンテキストが欠落する
CSCvf49899	ENH：GOID の割り当てと同期のクリーンアップ
CSCvf51066	FXOS 上の ASA が SNMP Ifspeed OID （1.3.6.1.2.1.2.2.1.5）応答値 = 0 を送信している
CSCvf54081	TLS バージョン 1.1 の接続に失敗し、t1_lib.c:3106 に共有署名アルゴリズムなし
CSCvf54981	ASA：80 バイトメモリブロックの枯渇
CSCvf56506	データパスでの ASA 9.6(2)、9.6(3) のトレースバック
CSCvf56917	ポートチャネルでのポートフラップ時に ASA が LACP PDU を送信しない
CSCvf57908	トランスペアレント ファイアウォール：誤った DSAP 値で Ethertype の ACL がインストールされる
CSCvf61419	NAT によるスレッド DATAPATH でのトレースバック
CSCvf62365	ASA：セカンダリ ASA がリロードされると、entConfigChange が予期せず送信される
CSCvf63108	送信元 IP アドレスが 0.0.0.0 の IGMP レポートパケットを ASA がドロップする

警告 ID 番号	説明
CSCvf64643	エラー：キャプティブポータルポートが使用できない。もう一度やり直す必要がある
CSCvf72068	FXOS：トランスペアレントモードの ASA/FTD スタンバイユニットがオフロードされたフローのトラフィックを止めることがある
CSCvf74218	AWS GovCloud の ASAv イメージが時間単位の課金モードで動作しない
CSCvf76281	IKEv2 RA 証明書認証。新しいセッションを割り当てることができない。最大セッション数に到達した
CSCvf77377	ホストスキャン：Microsoft および Panda の .dll ファイルのダウンロード時の cscan.log エラー
CSCvf79262	OpenSSL CVE-2017-3735「incorrect text display of the certificate」
CSCvf80539	リブート後に管理専用に復帰する
CSCvf81222	パケットが PBR に到達し、接続が確立されたときの 112 バイト bin でのメモリリーク
CSCvf81932	K7 ライセンスによる一部のインスペクションでの「Incomplete command」エラー
CSCvf82733	FTD CLI に「crypto ikev1 enable」コマンドがインストールされていない
CSCvf83709	CCL リンク障害によってスレーブがキックアウトされた後に再参加してもマルチコンテキストモードで v3 ユーザが失われる
CSCvf85065	ASA：スレッド名 idfw_proc によるトレースバック
CSCvf87899	ASA：まれに発生したスケジューラの破損によってコンソールロックが発生する
CSCvf89504	NAT が含まれていると ASA クラスタが IP フラグメントを断続的にドロップする
CSCvf90278	キャプチャをクリアするときの ASA/FTD のトレースバック（assertion "0" failed: "mps_hash_table_debug.c" ファイル）
CSCvf94973	ASDM を介して AnyConnect イメージをアップロードするときの FP 2100 での ASA のトレースバック
CSCvg01016	ASA が DCERPC インスペクションのピンホールを作成せず、debug dcerpc が「MEOW not found」と表示する。
CSCvg01132	ASA：9.2(4) から 9.2(4)18 へのアップグレード後にシリアル接続がハングする

警告 ID 番号	説明
CSCvg05250	「clear local-host <IP>」がすべてのホスト/接続の ASA クラスタ全体に存在するすべてのスタブフローを削除する
CSCvg08891	ASA 5555 9.6.3 のローカル証明書認証を使用した Wi-Fi 経由で iPhone IKEv2 PKI がリークする
CSCvg09778	DNS インスペクションにより CP 処理で ASA-SSP HA がリロードする
CSCvg17478	Show OSPF Database コマンドによるトレースバック
CSCvg20796	サイト間セキュリティ VPN トンネルを介して DNS サーバが到達可能な場合に ASA ローカル DNS 解決が失敗する
CSCvg21077	1 つのノードが再参加し、トラフィックが再起動されると、snpi_untranslate が原因でユニット 100% CPU が発生する
CSCvg25175	SNMP ポートのスタティック NAT 設定により ASA がハング状態でスタックする
CSCvg25538	転送ポート：アイデンティティ UDP トラフィックにより 1550/2048/9344 バイトのメモリブロックが枯渇する
CSCvg25694	トレースバックのアサート、スレッド名：cli_xml_server
CSCvg30391	ifInDiscards の ASA SNMP OID が常に 0
CSCvg32179	Javascript 要素のリライターの問題
CSCvg33669	「OCTEON:DROQ[8] idx: 494 len:0」メッセージがデバイスのコンソールアクセス時に表示される
CSCvg33985	ASA Webvpn のユーザ名フィールドでは XSS 実行可能スクリプトを受け入れることができない
CSCvg38437	64 文字を超える証明書からの ASA AC クライアントの PKI ユーザ名が 64 文字に切り詰められる
CSCvg45952	ASA のトレースバック：スレッド名 scansafe
CSCvg51984	IKE デーモンの高 CPU 使用率により、拡張された環境での VPN トンネルのコンバージェンスが遅くなる
CSCvg52995	ASA でパスワードの暗号化を有効にした後、システムコンテキストで設定を保存できない
CSCvg53981	ASA 9.8.2 上で「dir /recursive cache:/stc」と「dir cache:stc/2/」が異なる AnyConnect.xsd リストを作成する

警告 ID 番号	説明
CSCvg57954	サービス オブジェクトグループの変更（オブジェクトの追加と削除）で ACE が削除される
CSCvg61829	SSH/Telnet トラフィック、3-WHS、データを含む ACK パケットがドロップされる：理由（intercept-unexpected）
CSCvg66606	GTP エコー応答が ASA クラスタでドロップされる
CSCvg67135	ASA が x25519 という曲線とのサーバキーの交換を受信すると接続を破棄する
CSCvg82932	vpnfol_memory_allocate と pnfol_data_dyn_string_allocator による ASA でのメモリリーク
CSCvg89102	ASA：write erase の後にマルチセッションコマンドが設定される

バージョン 9.6(3.1) で解決済みのバグ

次の表に、このリリースノートの発行時点で解決済みのバグを示します。

警告 ID 番号	説明
CSCuj69650	ASA が「logging permit-hostdown」を使用して新しい接続をブロックし、TCP syslog がダウンしている
CSCum28756	ASA：ユニットがクラスタに再参加した後の SNMPv3 ポーリングの認証失敗
CSCum74032	SNMP ポーリング時のスタンバイでの ASA トレースバック
CSCup37416	古い VPN コンテキストエントリにより ASA がトラフィックの暗号化を停止する
CSCuq80704	ASA が TCP パケットを PAWS 障害として誤って分類する
CSCus29600	ルートを変更しても dhcprelay インターフェイスが変更されない
CSCut07712	ASA：ASP テーブルのルーティングに int. がないため、ボックストラフィックが中断する
CSCuu50708	9.1.5.19 での ASA トレースバック
CSCuv61791	ASA での CWS リダイレクションにより HTTPS トラフィックのシーケンス番号が破損することがある
CSCuv86562	トレースバック：スレッド名 fover_health_monitoring_thread で ASA がクラッシュする
CSCuw71147	http_header_by_name のユニコーンプロキシスレッドでのトレースバック

警告 ID 番号	説明
CSCuw88759	ASA：インターフェイスを接続していない状態でプロトコルとステータスが表示される
CSCuw95262	しばらくしてからフラッシュ操作が失敗し、設定を保存できない
CSCux17527	ボットネットに関連する ASA メモリリーク
CSCux92157	コンポーネント ssh を使用したスレッド名 ssh_init での ASA トレースバックアサート
CSCux98029	ASA はスレッド名 DATAPATH または CP 処理のトレースバックでリロードする
CSCuy22155	マルチキャストルーティングが無効な状態で ASA が予期しない syslog メッセージを生成する
CSCuy43438	クライアントからの接続解除後に IPSec を介して L2TP を接続できない
CSCuy47545	stdby 916.9 以降のリロード後にマルチコンテキストで http 設定が欠落している
CSCuy55468	ユニコーンプロキシスレッドにより CP 競合が発生する
CSCuy89288	AnyConnect DTLS オンデマンド DPD が断続的に送信されない
CSCuz09255	ASA がアクティブ/アクティブ HA で NS に応答しない
CSCuz42390	DRP の ASA ステートフル フェールオーバーが断続的に動作する
CSCuz44968	パーサースイッチによりコマンドがスタンバイにインストールされていない
CSCuz64603	データ処理中の gtp_update_sig_conn_timestamp での GTP トレースバック
CSCuz72244	未指定の Ctrl F-TEID によってドロップされた無効な TID MBReq によってエラー通知がドロップされる
CSCuz77293	クラスタスレーブに OSPF マルチキャスト フィルタ ルールがない
CSCuz80281	IPv6 ネイバー探索パケット処理の動作
CSCuz87146	nat-t-disable 機能が ikev2 で動作していない
CSCuz89989	「ピアアドレスが変更された」という理由で Ikev1 トンネルがドロップする
CSCuz90648	2048/1550/9344 バイトのブロックリークによってトラフィックの中断とモジュールの障害が発生する

警告 ID 番号	説明
CSCuz92074	PAT を使用する ASA は、ポートを含まないフィールドを介して SIP を変換解除できない
CSCuz94158	内部の「任意の」アドレスでハッシュの誤算出が発生する
CSCuz94862	IKEv2：データキー再生成の衝突により非アクティブな IPsec SA がスタックする可能性がある
CSCuz94890	スマートライセンスの交換中にすべてのデータを受信する前に ASAv ACK FIN が送信される
CSCuz95703	QP-D のユーザコンテキストでは管理専用 cli を使用できない
CSCuz98704	アップグレード後の CP 処理スレッドでのトレースバック
CSCva00190	チップリセットによる CTM メッセージハンドラが原因で ASA 9.4.2.6 の CPU 使用率が高くなる
CSCva00939	FQDN が解決された場合に show access-list で ACL 警告メッセージを削除する
CSCva01570	WebVPN でファイル logon.html が予期しない状況で終了する
CSCva02655	ASA がクライアントレス VPN トラフィックの SFR に無効なインターフェイス id を送信する
CSCva02817	サーバから設定された DSCP ビットを使用する ASA にはレート制限がない
CSCva03607	show service-policy の出力が誤った値をレポート
CSCva05513	ASA：ゼロ以外に設定されているフローティングタイムアウトによって SLA モニタが動作しない
CSCva07268	ASA のアップグレード後、クライアントレス経由で 2 回目の認証を行うことができない
CSCva10054	SCTP インスペクションによりデータパスで ASA ASSERT がトレースバックする
CSCva12520	一部の NAT OID で snmpwalk が動作しない
CSCva15911	ASA のリロード時に、ASA はフラッシュではなくディスク 0 として SSD をマウントする
CSCva16471	小さいメトリックのルートがアドバタイズされた場合に、IPv6 OSPF ルートが更新されない

警告 ID 番号	説明
CSCva22048	ASA：複数のコールで同じメディアポートが使用されていると PAT を使用した SIP コールがドロップされる
CSCva24799	TLS プロキシ機能に client trust-point コマンドがない
CSCva24924	config-url が入力された場合、9300 の ASA SM が SSH を介してマルチコンテキストをリロードする
CSCva26771	ASA：パケットがドロップされたときの PBR のメモリリーク
CSCva31378	スレッド名 rtcli async executor process での ASA トレースバック
CSCva32092	OSPFv3/IPv6 フラッピング (ASA クラスタと4500の間の30分ごと)
CSCva35439	ASA データパスのトレースバック（クラスタ）
CSCva36202	リロード後に ASA で BGP ソケットが開かれない
CSCva36884	Cisco ASA クロス サイト スクリプティング の SSLVPN の脆弱性
CSCva38556	Cisco ASA 入力検証ファイルインジェクションの脆弱性
CSCva39094	MPF 変更中の CLI スレッドでの ASA トレースバック
CSCva39804	クラスタへの再参加中に SFR でインターフェイスが削除される
CSCva40844	暗号化アクセラレータリングのタイムアウトによってパケットがドロップされる
CSCva43746	ASA「show inventory」に「Driver Error, invalid query ready」が表示される
CSCva43992	IKEv2 RA 証明書認証。新しいセッションを割り当てることができない。最大セッション数に到達した
CSCva45590	フェールオーバーの無効化/有効化時に ASA OSPFv3 インターフェイス ID が変更される
CSCva46920	show tls-proxy session detail を発行したときのスレッド名 ssh でのトレースバック
CSCva47608	SCTP MH：ピンホールが取り外され、デュアル nat を使用してスタンバイで freq が追加された
CSCva49256	SSH でのメモリリーク
CSCva50554	不適切な設定で起動された場合、ASA はホスト IP アドレスに「::」を使用する

警告 ID 番号	説明
CSCva50838	ASA キャプチャタイプ isakmp が再構築された rfc7383 IKEv2 パケットを保存しない
CSCva52514	ASAv-Azure：waagent は、ロードバランサを使用して ASAv が展開された場合にリロードする可能性がある
CSCva53581	グローバル ARP リクエストプールの増加
CSCva56114	CISCO-MEMORY-POOL-MIB がヒープキャッシュの誤った値を返す
CSCva56343	クラスタリング：L2 エントリのタイムアウトによって TFW 非同期フローパケットがドロップする
CSCva60283	Azure での ASAv 用の 2 つのアップストリーム カーネル パッチ
CSCva62667	シャット ダウン インターフェイスが ASP ルーティングテーブルに表示される
CSCva62861	フェールオーバー後に uauth でエラーが発生する
CSCva66278	SmartLic：シャーシ間のマスター スイッチオーバー ライセンスの競合状態
CSCva68364	SNMPv3 のアクティブな engineID は ASA の交換時にリセットされない
CSCva68987	ICMP インスペクションが無効になっている場合、ASA は ICMP 要求パケットをドロップする
CSCva69346	NAT が一致したときに ASA から DHCP 検出パケットをリレーできない
CSCva69584	OSPF は誤ったマスクを使用してタイプ 5 LSA を生成し、LSDB でスタックする
CSCva69799	FIPS セルフテストの失敗により、ASA がブートループでスタックする
CSCva70095	サーバが tls-proxy にある場合に ASA が TLS1.2 をネゴシエートする
CSCva70979	ポートチャネルインターフェイスでフェールオーバー記述子が更新されない
CSCva71783	応答パケットへの応答で ICMP エラー パケットがドロップされる
CSCva76568	ASA：IKEv1/IKEv2 を有効にすると RADIUS ポートが開く
CSCva77852	ipsecvpn-ikev2_oth：スレッド名 IKEv2 Daemon での 5525 9.4.2.11 のトレースバック
CSCva81412	ASR9000 BGP グレースフルリスタートが予期したとおりに動作しない

警告 ID 番号	説明
CSCva81749	IPSEC プロトコル経由で接続するときに IPV6 アドレスが割り当てられていない
CSCva84079	再起動中に ASAv が頻繁にハングする
CSCva84625	ASAv の show hostname によってスマートライセンスの認証要求が生成される
CSCva84635	ASA：CHILD_SA 衝突によって IKEv2 SA がダウンする
CSCva85382	CTS SGT マッピングの ASA メモリリーク
CSCva85933	FTD 6.1：redistribute connected によって内部データ（NLP）が再配布されている
CSCva86626	HTML5：Guacamole サーバにページの更新が必要
CSCva87077	エコー応答の gtpv1_process_msg での GTP トレースバック
CSCva87160	クライアントレス ssl vpn に対して OTP 認証が機能していない
CSCva88796	AnyConnect セッションが L2TP Uauth セッションのスタックにより接続できない
CSCva90419	issuer-name が attr を使用して証明書マップ内の重複を誤って検出
CSCva90806	「show asp table classify domain permit」を発行した場合の ASA トレースバック
CSCva91420	CTM Message Handler での ASA トレースバック
CSCva92151	Cisco ASA SNMP リモートコード実行の脆弱性
CSCva92813	ASA クラスタ DHCP リレーがサーバ応答をクライアントに転送しない
CSCva92975	トレースバックでクラスタから ASA 5585-60 がドロップされている
CSCva94702	DP-CP キューでのエンキュー障害が検査された TCP 接続を失速させることがある
CSCva95686	FTD：9,000 バイトブロックの枯渇によってトラフィックがドロップされる
CSCva97863	971 EST：show capture でコンソールがハングする
CSCva98240	SIP：ルートからのアドレス：ヘッダーが正しく変換されない
CSCva98532	FTD インラインでは、ブロックする必要がある MPLS スイッチド TCP セッションがブロックされていない

警告 ID 番号	説明
CSCvb03994	IKE_DBG でのトレースバック
CSCvb04685	SNMP 設定を削除できない
CSCvb05667	H.323 インスペクションによりスレッド名 CP Processing でトレースバックが発生する
CSCvb05787	AnyConnect テストでアプリケーションをロードした後のネットワーク udpmod_get でのトレースバック
CSCvb08776	内部 ATA Compact Flash サイズが「show version」に正しく表示されない
CSCvb13690	ASA：ボットネットの更新が多数のエラーで失敗する
CSCvb13737	wr mem/wr standby がスタンバイの設定を同期していない
CSCvb14997	ASA DHCP リレーは、DHCP オファーの一部として受信したネットマスクと gw を書き換える
CSCvb15265	スレッド名 DATAPATH での ASA ページ障害のトレースバック
CSCvb19251	DHCP リレーとしての ASA が DHCP 150 通知メッセージをドロップする
CSCvb19843	ASA でのバッファオーバーフローによりリモートコードが実行される
CSCvb20256	ASA の SSH 実装における Sweet32 の脆弱性
CSCvb21922	FQDN が未解決の場合に show access-list で ACL 警告メッセージを削除する
CSCvb22435	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
CSCvb22848	スレッド名 NIC status poll での ASA 9.1.7-9 のクラッシュ
CSCvb25139	DNS インスペクションが有効になっている場合に IPv6 DNS パケットの形式が不正になる
CSCvb26119	WebVPN リライターが matterport.com で失敗する
CSCvb27868	マルチコンテキストトランスペアレントファイアウォールを使用した ASA 1550 ブロックの枯渇
CSCvb28491	show counters protocol ip を実行できない
CSCvb29411	管理 vrf 経由でのみアクセスできる場合、AAA 認証/認可が失敗する
CSCvb29688	CSCup37416 に対する修正にもかかわらず、古い VPN コンテキストエントリにより ASA がトラフィックの暗号化を停止する

警告 ID 番号	説明
CSCvb30445	ポリシーベースのルーティングが有効な状態で ASA が DATAPATH トレースバックを生成することがある
CSCvb31055	ASA のマルチコンテキスト SNMP PAT インターフェイスが欠落している
CSCvb31833	トレースバック：スレッド名 DATAPATH-0-1790 での ASA
CSCvb32297	WebVPN：VNC プラグイン：Java：接続をピアによってリセット：ソケット書き込みエラー
CSCvb32341	passive-interface を使用した ASA トレースバックが 9.6(2) でデフォルトになる
CSCvb33009	Cisco ASA 署名検証によりブート時にデジタル署名テキストを誤って解釈する
CSCvb33013	Cisco ASA の削除により SB 以外のハードウェアでセキュアなブート コマンドを誤って解釈する
CSCvb36199	スレッド名 snmp ASA5585-SSP-2 が 9.6.2 トレースバックを実行している
CSCvb37456	IKE キー再生成後のフェールオーバーが act デバイスで ph1 キー再生成を開始できない
CSCvb38522	ASA PKI OCSP 障害：CRYPTO_PKI：OCSP 応答データの復号化に失敗した
CSCvb39147	Cisco ASA プラットフォームで NFS スループットレートが低下する
CSCvb40417	ASA の「sh route」コマンドで確認された nlp_int_tap ルート
CSCvb40818	NLP 情報が IPv6 のコマンドに表示される
CSCvb40847	ユーザが手動でログアウトした場合に ASA が認証セッション終了ログを送信しない
CSCvb41097	GTPv2 がインスタンス 1 のハンドオフをドロップしている
CSCvb43120	Checkheaps スレッドでの ASA トレースバック
CSCvb45039	スレッド名 aaa_shim_thread での ASA トレースバック
CSCvb46531	ASDM：ASAv 9.6.2 のメモリ使用率の読み取りが正しくない
CSCvb47006	自動更新スレッドで ASA トレースバックが確認された
CSCvb48640	2016 年 9 月の Openssl の pix-asa の評価

警告 ID 番号	説明
CSCvb49264	v2 ハンドオフのコールフロー後に Delete Bearer Req が 2 番目のデフォルトベアラーを削除できない
CSCvb49273	ISE への送受信の際に ASA 上の CoA によりトレースバックがトリガーされる
CSCvb49445	IKEv2：クライアントからの接続後に セッションがクリアされない
CSCvb50301	スレッド名 rtcli での ASA のトレースバック
CSCvb50609	RADIUS 認可要求が着信側ステーション ID の属性を送信しない
CSCvb50750	SIP トラフィックによるフェールオーバー時の lina コア
CSCvb52157	viewer_dart.js ファイルが正しくロードされない
CSCvb52492	OSPF ルートの問題によりフェールオーバー後に VPN トンネルが失われる
CSCvb52988	スレッド名 emweb/https での ASA トレースバック
CSCvb53094	ASA：マルチコンテキストファイアウォールの使用済みメモリの計算に相違がある
CSCvb55721	サイト IP アドレスを使用したマルチサイトクラスタで ASA により GARP フラッドが実行される
CSCvb57817	EIGRP：帯域幅を拡張したときに多数のエラー処理を追加する必要がある
CSCvb58087	オブジェクトグループ検索の冗長サービス グループ オブジェクトが誤って削除される
CSCvb63503	時間範囲により拒否された場合の IKEv2 での AAA セッションハンドルのリーク
CSCvb63819	OS 9.1.6 から 9.4.3 へのアップグレード時のスレッド fover_parse での ASA-SM のトレースバック
CSCvb64161	ASA によるクライアントのマルチキャストパケットの宛先 MAC アドレスの書き換え頻度がかなり低い
CSCvb66593	URL での webvpn_state クッキー情報の開示
CSCvb68766	スレッド名 IKE Daemon での ASA のトレースバック。
CSCvb74084	SCP が 962で失敗する
CSCvb74249	マルチコンテキストモードで設定された TCP syslog を使用して ASA がトラフィックをドロップしている

警告 ID 番号	説明
CSCvb75266	ASA：パケットトレーサツールの XML 出力に ACL の注釈が正しく表示されない
CSCvb75685	「no vpnclient enable」の入力後、EZVPN NEM クライアントが再接続できない
CSCvb78614	4GE-SSM RJ45 インターフェイスがインターフェイスの「rate limit drops」によりトラフィックをドロップすることがある
CSCvb83446	v1 PDP が IE 障害の解析時に削除されることがある
CSCvb85624	CVE-2016-5195（ダーティ CoW）の pix-asa の評価
CSCvb87586	フェールオーバーおよびプラグイン/プラグアウト後に SSH 管理インターフェイスに障害が発生
CSCvb88126	ASA：CSCuu48197 に対する修正にもかかわらず stuck uauth エントリが AnyConnect 接続を拒否する
CSCvb88358	webvpn-l7 リライター：5515 9.1.6 コンテンツ書き換えの問題（ASA Web ブックマークの場合）
CSCvb89988	WebVPN：内部ページのログインボタンがリライター経由で機能しない
CSCvb92125	書き換え時にラベル長を超えたため ASA が DNS PTR リレーをドロップする
CSCvb92417	クラスタ ASA は「inspect-icmp-seq-num-not-matched」という理由で to-the-box ICMP 応答をドロップする
CSCvb92548	ASA が誤った ACL と有効状態のオブジェクトグループ検索を照合する
CSCvb92823	NOTIFY に埋め込まれている場合に ASA SIP インスペクションによる 200 OK の送信が遅延することがある
CSCvc00015	ASA クラスタの仮想 IP で SNMP ポーリングが実行されると誤った動作になる
CSCvc00689	ASA：IKEv2 によるメモリリーク
CSCvc00760	RDP プラグイン接続がエラーで失敗した
CSCvc01685	PLR：ASAv が無効な予約コードを生成する
CSCvc04741	ASA DHCP リレーに代行受信 DHCP 機能との互換性がない
CSCvc05005	ASA クラスタの TCP/SSL ポートが LISTEN 状態に表示されない
CSCvc06150	ASA が証明書マップに複数の属性エントリを追加できない

警告 ID 番号	説明
CSCvc07112	スケジューラ破損の問題に対する検出と自動修正の機能を実装する
CSCvc07330	WebVPN 実行中に ASAv がクラッシュすることがある
CSCvc14190	EC に負荷がかかっている状態で ASA が SSL VPN セッションの確立に失敗する
CSCvc14448	9.6.2：AnyConnect IKEv2 パフォーマンステスト時のトレースバック
CSCvc14502	ASA マルチコンテキストで到達不能な TCP syslog と logging permit-hostdown のセットへの新しい接続が許可されない
CSCvc16330	ASA-SM 9.5.2 inspect-sctp ライセンスが既存の導入を中断する
CSCvc19318	スレッド名 sch_syslog での ASA のトレースバック
CSCvc22193	DSCP マーキングが IPSec カプセル化を使用した外部 IP ヘッダーにコピーされない
CSCvc23838	WebVPN CIFS での Cisco ASA ヒープのオーバーフロー
CSCvc24380	mqc_enable_qos_for_tunnel のスレッド名 IKE Daemon でのトレースバック
CSCvc24657	MIB オブジェクト cempMemPoolHCUsed が表示されなくなる
CSCvc24788	ASA：OspfV3 ルートがインストールされない
CSCvc25195	AnyConnect が表示されると ASA ポータルが複数コンテキストが設定されていることを公開する
CSCvc25281	クラスタユニットのリブート後に SNMPv3 ユーザの同期がエラーになる
CSCvc25409	SNMP ポーリングの使用時の CloneOctetString での ASA のメモリリーク
CSCvc33796	ACL と NAT テーブルのコンパイルの速度向上の実装
CSCvc36535	インターフェイスの no shutdown 後のスレッド名 ssh、rip igb_disable_rx_queues での ASA トレースバック
CSCvc36805	Firepower Threat Defense（FTD）IKEv2 NAT-T が再起動後に無効になる
CSCvc37557	クライアントレス WebVPN の ASA とバックエンド サーバ間で SSL 接続がハングする
CSCvc38425	FirePOWER モジュールを搭載した ASA がトレースバックを生成してリロードするか、プロセスが実行しない原因となる
CSCvc39121	ASA がマルチコンテキスト モードの場合に外部 DHCP サーバを使用した AnyConnect アドレスの割り当てが失敗する

警告 ID 番号	説明
CSCvc44240	ASA クラスタリング：9.6.2 の SPAN が設定されたポートチャネルインターフェイスで MAC アドレス コマンドが無視される
CSCvc48640	forward-reference enable が設定されている場合に ASA がアクセスリストを動的に更新しない
CSCvc52072	デフォルトの WebVPN グループにランディングする接続について WebVPN ポータルが正しく表示されない
CSCvc52272	ASA インスペクション MPF の ACL の変更が正しい順序で ASP テーブルに表示されない
CSCvc52504	ASA がスレッド名 Unicorn Admin Handler でトレースバックすることがある
CSCvc52879	アクティブ/スタンバイ ASA フェールオーバーペアでアクティブユニットをリロードしてもフェールオーバーをトリガーしない
CSCvc55674	ASA：IPSec SA の起動に失敗した
CSCvc55974	L2L セットアップで IKEv2 ハンドルがリークする
CSCvc58272	ASA が誤ってラッパーの負の数値を処理し、結果としてグラフィカル WebVPN の問題が発生する
CSCvc60254	SIP：複数のセグメントを持つ 200 OK メッセージが正しく再構築されない
CSCvc60964	ASA L3 クラスタ：非対称ルーティングの場合に DHCP リレーが DHCPOFFER をドロップする
CSCvc61818	失敗した試行後の CTP がユーザ名とともにドメインを送信する
CSCvc61845	RDP プラグインの activex 全画面オプションが ASA 9.6.2 バージョンでは使用できない
CSCvc62252	到達可能性がダウンしている間にトラッキングルートが起動しない
CSCvc62556	ASA クラスタスレッド名 qos_metric_daemonでのトレースバック
CSCvc65409	クラスタの gtpv2_process_msg でトレースバックが確認された
CSCvc68229	BGP の BFD サポートコードが tcp/udp 3784 と 3785 を開いてアクセスリストをバイパスする
CSCvc79077	rest-api が有効になっている状態のクラスタ設定の同期時の ASA ウォッチドッグのトレースバック
CSCvc79371	ASA NAT プールが正しく更新されない

警告 ID 番号	説明
CSCvc79454	スクリプトユーザに SSH パブリック認証を設定できない
CSCvc79569	mac address auto コマンが ASA5585-X でデフォルトのプレフィックス 1 を使用する
CSCvc82146	スレッド名 Datapath での ASA のトレースバック
CSCvc86554	トレースバック：ASA 9.5(2)11 クラッシュアクティブ
CSCvc87914	設定の同期の失敗時の ASA のトレースバックとリロード
CSCvc88115	ASA クラスタリング IDFW がユーザマッピングを更新しない
CSCvc88411	RADIUS アカウンティングパケットによる 1550 バイトブロックの枯渇が確認される
CSCvc91839	XML 解析が正しくないため、FTD デバイスでポリシーを展開できない
CSCvc93947	ASA(9.1.7.12)：スタンバイ ASA を介してマルチキャストストリーム用に作成された接続エントリ
CSCvc97734	ポートチャネルインターフェイスで management-only が有効になっていると展開が失敗する
CSCvd01736	DHCP を使用すると L2TP が接続されないことがある
CSCvd03261	ASAv が応答しなくなる/VPN が再起動後に機能しない
CSCvd03343	非システムコンテキストの SSH 公開キー認証を設定できない
CSCvd06022	アップグレード後にスレッド名 IPSEC MESSAGE HANDLER で ASA-FP9300 がクラッシュ
CSCvd06527	SNMPv3 リンクアップ/リンクダウンが管理コンテキストを介して生成される必要がある
CSCvd08200	ASA での低速なメモリリーク
CSCvd08479	ACL の最後のヒットカウントカウンタに誤った時刻が表示される
CSCvd08709	非対称の path icmp トラフィックが分散クラスタリングで失敗する
CSCvd14266	DATAPATH-41-16976 スレッドでの ASA トレースバック
CSCvd15843	データの受け渡し中に発生したグループポリシーの「vpn-idle-timeout」が原因で、ポート フォワーディング セッションがタイムアウト
CSCvd21154	5585 がクラスタを離れた後の 30 秒間にデータインターフェイスのバンドルを解除しない

警告 ID 番号	説明
CSCvd21541	ASA 944 のサービス オブジェクト グループで作成されると、ポートオブジェクトを削除できない
CSCvd21665	RRI および OSPF を搭載した ASA：ASP ルーティングテーブルからルートをフラッシュできない
CSCvd23016	TFTP を使用してキャプチャをコピーすると ASA がトレースバックすることがある
CSCvd23471	ブートアップ時に大型のコンテキスト設定をロードしている間に ASA がトレースバックすることがある
CSCvd24066	IM インスペクションが有効になっていると、ASA が Web トラフィックをドロップする
CSCvd26939	SNMP が FTD のすべての管理対象デバイスに同じホスト名をリストする
CSCvd28859	ASA：ICMP トラフィックの PBR メモリリーク
CSCvd29150	管理ルートの削除によりデータプレーンルートも削除される
CSCvd33044	アクセスコントロール ポリシーの展開時に「cli_xmlserver_thread」で FTD がクラッシュ
CSCvd33787	uauth による syslog.c でのアサーション
CSCvd39113	新しいユニットがセットアップに参加していなかったにもかかわらず、クラスタ C ハッシュテーブルがもう 1 つのユニットで更新される
CSCvd41052	スケジューラキューの破損が 9.6(2) 後の接続障害またはフェールオーバーの問題を引き起こす
CSCvd41423	cRLSign キーの使用を含む証明書によって CRL を署名する必要がある
CSCvd43309	新しく作成されたオブジェクトグループのアクセスリストが一致しない
CSCvd47781	インサービスアップグレード実行中の ASA のトレースバック
CSCvd49262	ジャイアント オブジェクト グループ（display_hole_og）を使用してアクセスリストを保存/表示しようとするとトレースバックする
CSCvd49550	9.5.1 以上の ASA で managment0/0 を src-ip として使用すると SXP ソケットを表示しない
CSCvd50389	RT#687120：クライアントレス VPN - SAML のブックマークに関する問題
CSCvd53884	モジュールのリロード後に Firepower（SFR）モジュールデータプレーンがダウンする

警告 ID 番号	説明
CSCvd55983	スレッド名 dhcp_daemon でのトレースバック
CSCvd58417	DCERPC インスペクションでパケットがドロップされ、通信が切断される
CSCvd61308	[実行コンフィギュレーション]エラーにより、マルチコンテキストの ASA バックアップが失敗する
CSCvd62509	ASDM で「アクセスルール」を表示している際のスレッド名 accept/http での ASA トレースバック
CSCvd63718	スレッド名 IPSEC MESSAGE HANDLER で ASA-FP9300 がクラッシュした
CSCvd64416	ASA のすべてのコンテキストがリロード時に同じ EIGRP ルータ ID を使用する
CSCvd64693	EIGRP を無効化および有効化した後で、EIGRP ルートが管理ルーティングテーブル vrf で誤ってアドバタイズしている
CSCvd65797	NAT 関連オブジェクトを FQDN に変更すると ASA がクラッシュすることがある
CSCvd66303	ESXi vCenter 6.5 での ASAv の導入中に発生したエラー
CSCvd69804	ASA：ipsec inner-routing-lookup の使用時にインターフェイスのステータスを変更することで VPN トラフィックが切断される
CSCvd73468	クラスタディレクタ接続がアイドルタイムアウトが原因でタイムアウトする
CSCvd76939	ASA ポリシーマップ設定がクラスタのスレーブに複製されない
CSCvd77893	アクセスグループの変更中に ASA がアサートのトレースバックを生成することがある
CSCvd78303	213 日の稼働後に ARP 関数が失敗し、「punt-rate-limit-exceeded」というエラーでドロップする

バージョン 9.6(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。

警告 ID 番号	説明
CSCsh75522	Content-Length のカウンタを 4 バイトから 8 バイトのサイズに増やす
CSCtw90511	パケットキャプチャにより、spin_lock が原因でマルチコアプラットフォームで CPU スパイクが発生する

警告 ID 番号	説明
CSCuh89500	ASA：ifSpeed/ifHighSpeed が SNMP によってポートチャネルに入力されていない
CSCum70304	FIPS セルフテストの電源投入の失敗：fipsPostDrbgKat
CSCup37416	古い VPN コンテキストエントリにより ASA がトラフィックの暗号化を停止する
CSCuu40736	capture <name> type inline-tag interface <name> でタグ値 0 がデフォルトになる
CSCuv09640	ASA：「自動有効化」機能が PKF を使用して設定された SSH で動作しない
CSCuw51576	SSH 接続が ASA ではタイムアウトにならない（rtcli でスタック）
CSCuw55813	スレッド名 EIGRP-IPv4 でのスタンバイ ASA のトレースバック
CSCux08783	CWS：ASA は XSS ヘッダーを付加しない
CSCux15273	show memory によって表示される使用可能な空きメモリが不正確である
CSCux29842	HA のプライマリおよびセカンダリ ASA はスレッド名 DataPath でのトレースバックである
CSCux29929	DATAPATH での ASA 9.4.2 トレースバック
CSCux33726	ASA トレースバック：WebVPN の CIFS_file_rename_remove の動作
CSCux33974	ASA の「show chunkstat | redirect」が機能しない
CSCux35538	DHE 暗号による SSL VPN 拡張テストでの ctm_ssl_generate_key のトレースバック
CSCux39988	フェールオーバーペアにおいてトランスペアレントモードでの BVI アドレスの出力が異なる
CSCux45179	SSL セッションが処理を停止：「Unable to create session directory」エラー
CSCux66866	ASASM での arp の量が一定であるため、トラフィックがドロップする
CSCux71197	shut/no sh 後に「show resource usage」が誤ったルート数を提供する
CSCux82023	ASA クラスタでの Shun/脅威検出により、スタブ接続が切断される
CSCux82835	asp transactional-commit nat を有効にすると、nat プールの枯渇が確認される
CSCux83705	デュアルスタックの DNS 応答修正が期待どおりに機能しない

警告 ID 番号	説明
CSCux86769	接続が TLS にフォールバックすると、VLAN マッピングが機能しない
CSCux96716	ユニットがクラスタに参加する場合のトレースバック
CSCux98029	ASA はスレッド名 DATAPATH または CP 処理のトレースバックでリロードする
CSCux99392	CIFS 経由でアップロード/ダウンロードされたファイルのバイトサイズがゼロ（同じ WebFolder）
CSCuy00296	スレッド IPsec message handler でのトレースバック
CSCuy01438	9.5.2 で SIP インスペクションおよび SFR が有効になっている ASA トレースバック
CSCuy03024	スレッド名 idfw_proc を示す ASA トレースバックとリロード
CSCuy05949	ASA：WRITE STANDBY が発行されたときのアクティブコンテキストでの MAC アドレスの変更
CSCuy07753	Firefox 32 ビットバージョン 43 以降では、スマートトンネルが機能しない
CSCuy10665	HA：SFR モジュールのリロード後、両方のユニットのインターフェイス数が一致しない
CSCuy11021	Webvpn ブックマークのサブタイトルが表示されない
CSCuy11281	ASA：バージョン 9.4.2 でのトレースバックのアサート
CSCuy11905	ユーザ名がアクセスリストに記載されている場合の ASA 5585 トレースバック
CSCuy13937	TLS 処理中の CP 処理スレッドにおける ASA ウォッチドッグのトレースバック
CSCuy15798	Radius アカウンティングパケット内での IPv6 割り当てアドレスフィールドのサポートを追加する
CSCuy18640	GTP メッセージプロセスと pdp の作成/削除間の潜在的なデッドロック
CSCuy19933	ASA リライターがタイプの HTML コードを誤って処理する <base>xxx</base>
CSCuy21206	ドロップが Diameter インスペクションおよび tls-proxy で有効になっている場合のトレースバック
CSCuy22561	VPN ロードバランシングは、IPv6 アドレスのロードバランシング証明書を送信しない
CSCuy25163	Cisco ASA ACL ICMP エコー要求のコードフィルタリングの脆弱性

警告 ID 番号	説明
CSCuy27428	9.1(7) へのアップグレード後のスレッド名 snmp での ASA トレースバック
CSCuy30069	ASA 9.5.2 は 512 ビット証明書の CERT_REQ を送信しない
CSCuy32321	ldap 属性マッピングおよび pw 管理による ldap_client_thread でのトレースバック
CSCuy32728	クラスタ暗号化が設定されている場合、VPN LB が動作を停止する
CSCuy32964	ヒットレス fxos アップグレード中のシャーシ間 SSP ASA クラスタのトレースバック
CSCuy34265	設定変更後の ASA アクセスリストの欠落と損失要素
CSCuy41986	チェーン内の複数の証明書が検証されると、OCSP 検証が失敗する
CSCuy42087	ASA：「log default」キーワードのある ACE を削除できない
CSCuy42223	BGP：管理専用インターフェイスでサポートされている理由で展開に失敗
CSCuy43857	ASA WebVPN：Kronos アプリケーションを使用した Java 例外
CSCuy47706	gtpv1_process_pdp_create_req でのトレースバック
CSCuy48237	クライアントレス SSL VPN CIFS ストレステスト：ramfs_webvpn_file_open トレースバック
CSCuy49902	許可されている場合でも、inspect ip-options で「NOP」が許可されない
CSCuy50406	proxyi_rx_q_timeout_timer でのクラッシュ
CSCuy51918	RAMFS dirent 構造でのバッファオーバーフローによりトレースバックが発生する
CSCuy54567	2016 年 6 月の OpenSSL の pix-asa の評価
CSCuy58084	SSH パブリック認証のみのユーザを設定できない（CSCuw90580 と関連）
CSCuy59460	v3 の無効なユーザ名に対して SNMP ポーリングが成功する
CSCuy60320	QP にインストールされていない IPv6 ルート
CSCuy62198	FQDN が 64 文字を超える場合、FQDN ではなく ip にリダイレクトする
CSCuy63642	webvpn-datapath における ASA 9.1(6) トレースバック：スレッド名「DATAPATH-2-1524」
CSCuy65416	「ctm->async_ref == 0」のアサートに失敗：ファイル「ssl_common.c」、行 193-part2

警告 ID 番号	説明
CSCuy65569	Coverity 114172：snp_fp_inspect_ip_options の FORWARD_NULL
CSCuy65571	Coverity 114170：parser_interface_list_invalid の SECURE_CODING
CSCuy67333	修正中の CallId と Refer-To の間の差異によって SIP コール転送が失敗する
CSCuy68174	Coverity 114166：ss_send_health_check_request の NULL_RETURNS
CSCuy71812	Coverity 114217：snp_fp_action_cap_construct_key の NULL_RETURNS
CSCuy72255	Coverity 114176：oct_dbg_read_csr の CHECKED_RETURN
CSCuy72257	Coverity 114177：oct_dbg_write_csr の CHECKED_RETURN
CSCuy73652	FQDN を含むオブジェクトグループを変更する場合のスレッド名 idfw でのトレースバック
CSCuy74218	クラスタパケットのリアセンブルにおいて、スレッド名 DATAPATH のトレースバックをアサート
CSCuy74362	WebVPN FTP クライアントがメッセージ「Error contacting host」で失敗する
CSCuy78802	クラスタのスプリットブレイン後、元のマスターが防御できていないGARP パケットがある
CSCuy80058	webvpn-cache を無効にした場合（cmd＝no で無効化）、FO レプリケーションに失敗
CSCuy83792	Coverity 114304：ProcessConfiguration(vdi::config::Adi の CHECKED_RETURN
CSCuy84044	webworker JS でのリライターエラー
CSCuy86333	BFD：ASA が snp_bfd_pp_process+101 でトレースバックを行う可能性がある
CSCuy87597	ASA：秘密キーの暗号解読における CP 処理スレッドでのトレースバック
CSCuy88971	ASA では EIGRP の候補のデフォルトルート情報が抑制されない
CSCuy89425	AAA：RSA/SDI が新しい PIN を設定できない
CSCuy91405	ASA はポートチャネルの CCL 上で同じフロートラフィックをロードバランシングしてはならない
CSCuy91788	ASAv：空きメモリが OOM 状態のマイナスとして報告される
CSCuy94787	脅威検出によるデータパスまたは高い CPU 使用率のトレースバック

警告 ID 番号	説明
CSCuy95543	malloc_avail_freemem() の効率の向上
CSCuy96391	ASA クライアントレスリライターが「CSCOPut_hash」関数でエラーになる
CSCuy98769	フェールオーバー後、ダウンから待機中への ASA OSPF インターフェイスの移行が遅い
CSCuy99280	ENH：ASAv には事前にロードされた別の証明書が必要である
CSCuz00077	スレッド名 telnet/ci での ASA 9.1.6.4 トレースバック
CSCuz01658	重複する要求をもつ gtp_remove_request でのトレースバック
CSCuz06125	アクティブ ASA およびスタンバイ ASA がアクティブ MAC のみが設定された同じ MAC アドレスを使用する
CSCuz06499	WebVPN：ASA の FQDN が srv と同じである場合、Web ページが完全に書き換えられない
CSCuz08625	SSH スレッドでの ASA トレースバック
CSCuz09394	戻り値の後に var が続く場合、JS リライターステートマシンで無限ループが発生する
CSCuz10371	strncpy_sx.c による ASA トレースバックとリロード
CSCuz14600	Kenton 9.5.1 の「boot system/boot config」コマンドがリロード後に保持されない
CSCuz14808	スレッド名 idfw_proc での 5585-10 トレースバック
CSCuz14875	address-family サブコンフィギュレーションを使用する場合、ASA RIP がクラッシュする
CSCuz16398	NAT 迂回テーブルの変更が正しくない
CSCuz16498	「ERROR: Problem with interface」というエラーメッセージがコンソールに表示される
CSCuz18707	JavaScript エラーにより、イントラネットページが WebVPN 経由でロードされない
CSCuz20742	AWS：2 つのインターフェイスを使用して展開されている場合、ASAv は到達不能である
CSCuz21068	CSCOPut_hash は予期しない要求を開始できる
CSCuz21178	スレッド名 ssh での ASA トレースバック

警告 ID 番号	説明
CSCuz23354	GTP でタイマーのキュー解除に失敗した後、CPU 使用率が高くなる
CSCuz23576	割り当てられたメモリが高（無効）値を示している
CSCuz27165	BTF は 3 つ以上のラベルを持つブラックリスト登録ドメインをブロックしていない
CSCuz28000	クラスタ内のすべてのユニットがリロードされると、コンテキスト設定が拒否されることがある
CSCuz30425	名前を使用したリロード後に network コマンドが BGP から消える
CSCuz34753	ASA QOS がプライオリティとベストエフォートキュー間のパケットを分類できない
CSCuz36545	ドロップダウンメニューが Simfosia Web ページで機能しない
CSCuz36938	最大 snmp ホスト数を超えた場合のネットワークオブジェクト編集時のトレースバック
CSCuz38115	object-group-search を使用して大規模な ACL がインターフェイスに適用された場合の ASA トレースバック
CSCuz38180	ASA：起動後のスタンバイ ASA でのデータパスのページ障害トレースバック
CSCuz38888	MSCA 証明書の登録ページ/VBScript で WebVPN の書き換えに失敗する
CSCuz40081	vpnfo による ASA のメモリリーク
CSCuz40793	HA 設定の同期中に SFR でインターフェイスが削除される
CSCuz41033	スタティック暗号マップと同じ名前が付けられている場合、ダイナミック暗号マップが失敗する
CSCuz41308	show route interface で表示される zone キーワード
CSCuz42390	DRP の ASA ステートフル フェールオーバーが断続的に動作する
CSCuz42986	sfr モジュールのシャットダウン時に ASA（HA）が RST パケットを送信しない
CSCuz50929	多くの「show blocks」出力では ASLR を使用して PC 値が切り捨てられている
CSCuz52474	2016 年 5 月の OpenSSL の pix-asa の評価
CSCuz52859	シングルモードからマルチモードへの移行時に、SNMPv3 noauth のトラップ/ポーリングが機能しない

警告 ID 番号	説明
CSCuz53186	ASA AnyConnect CSTP の著作権メッセージが不適切に変更された
CSCuz54193	ASA：SFR トラフィック リダイレクションを有効にする場合のデータパスにおける ASA でのトレースバック
CSCuz54545	ASA アドレスがトレースバックをマッピングしていない - snmp-server host の設定
CSCuz58142	ASA アクセスリストの欠落と損失要素に関する警告メッセージの拡張
CSCuz60555	メモリが高でない場合、ASA-2-321006 が無効に受信される可能性がある
CSCuz61092	インターフェイス ヘルスチェックのフェールオーバーにより、OSPF は ASA を ABR としてアドバタイズしない
CSCuz63531	メモリ破損の監視、debug ospf のアサート
CSCuz64603	データ処理中の gtp_update_sig_conn_timestamp での GTP トレースバック
CSCuz64784	コンテキスト削除中のすべてのクラスタユニットにおけるデータパスでの ASA トレースバック
CSCuz66269	SCP クライアントでは「no ssh stricthostkeycheck」を使用したパスワードの入力が許可されていない
CSCuz66661	ASA カットスループロキシの無活動タイムアウトが機能しない
CSCuz67349	インスペクションなしで伝送する前に ASA クラスタフラグメントを再構築
CSCuz67590	ASA がスレッド名 cluster rx thread でトレースバックすることがある
CSCuz67596	ASA がスレッド名 Unicorn Admin Handler でトレースバックすることがある
CSCuz70330	ASA：上限に達したときに ASA デバイスで SSH が拒否される
CSCuz72244	未指定の Ctrl F-TEID によってドロップされた無効な TID MBReq によってエラー通知がドロップされる
CSCuz72352	tls-proxy ハンドシェイク中のトレースバック
CSCuz77818	一部のインターフェイスで PIM BiDir DF の選出が「offer」状態でスタックしている
CSCuz79800	ASA が ACL の行と注釈を削除できない - 指定された注釈が存在しない
CSCuz81922	SRTS：「show cluster chassis xlate count」の下で「type」オプションが欠落している

警告 ID 番号	説明
CSCuz90648	2048/1550/9344 バイトのブロックリークによってトラフィックの中断とモジュールの障害が発生する
CSCuz94862	IKEv2：データキー再生成の衝突により非アクティブな IPsec SA がスタックする可能性がある
CSCuz98201	ASAv - 高い CPU 使用率
CSCuz98220	スレッド名 Dispatch Unit での ASA トレースバック
CSCuz98704	アップグレード後の CP 処理スレッドでのトレースバック
CSCva00939	FQDN が解決された場合に show access-list で ACL 警告メッセージを削除する
CSCva01570	WebVPN でファイル logon.html が予期しない状況で終了する
CSCva02121	スレッド名 ci/console でのトレースバック：デバッグメニュー ctm 103 が ASA をクラッシュさせる
CSCva02655	ASA がクライアントレス VPN トラフィックの SFR に無効なインターフェイス id を送信する
CSCva03982	ASA：PBR ルックアップによるクラスタモードでのメモリリーク
CSCva11580	ASA9.(6) 1 つの回帰「内部エラー」（「最大時間超過」ではない）
CSCva12520	一部の NAT OID で snmpwalk が動作しない
CSCva12598	CISCO-ENHANCED-MEMPOOL-MIB::cempMemPoolHCFree.1.1 = Counter64：0 バイト
CSCva14545	oVirt 経由で展開されている場合、ASAv-KVM をブートアップできない
CSCva26771	ASA：パケットがドロップされたときの PBR のメモリリーク
CSCva35439	ASA データパスのトレースバック（クラスタ）
CSCva39804	クラスタへの再参加中に SFR でインターフェイスが削除される
CSCva40844	暗号化アクセラレータリングのタイムアウトによってパケットがドロップされる
CSCva45590	フェールオーバーの無効化/有効化時に ASA OSPFv3 インターフェイス ID が変更される
CSCva62861	フェールオーバー後に uauth でエラーが発生する
CSCva92151	Cisco ASA SNMP リモートコード実行の脆弱性

バージョン 9.6(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	説明
CSCtz98516	「xlate count」の GET BULK のクエリ中に SNMP で観測されたトレースバック
CSCuc11186	ARP：プロキシ IP トラフィックがハイジャックされている
CSCun21186	スレーブから idfw topn ユーザを取得するときの ASA トレースバック
CSCuo08193	nat-t パケット処理中のスレッド名 DATAPATH-1-1382 でのトレースバック
CSCur46371	TLSv1.2 クライアント証明書認証の接続確立に失敗
CSCur87011	ローエンド ASA-X -5512/5515 デバイスでの ASA の DMA メモリ不足
CSCus10787	コンパイル時にトランザクション ACL のコミットにセキュリティポリシーが適用されない
CSCus16416	電源の再投入後に、フェールオーバーペアでライセンスの共有がアクティブ化されない
CSCus53126	ASA トラフィックが「traffic-forward sfr monitor-only」を使用して正しく送信されない
CSCut40770	フレームが 2,048 バイトを超える場合、SFR へのインターフェイス TLV が破損している
CSCut49034	ASA：CL SSL ポータルから AC クライアントへの RDP 接続が原因でスタンバイでの CPU 使用率が高い
CSCut71095	ASA WebVPN のクライアントレス cookie 認証のバイパス
CSCuu02848	SSL の RSA 証明書を手動で設定する場合は、ECDSA SSL 暗号を無効にする
CSCuu06081	ASAv ライセンスの適用は CLI パーサーベースにしてはならない
CSCuu48197	ASA：stuck uauth エントリが AnyConnect ユーザ接続を拒否する
CSCuu82229	DH 19 以降の ikev2 は、phase2 キー再生成後にトラフィックを渡すことができない
CSCuu91304	GET が ScanSafe 接続を切断した後のクライアントからの即時 FIN
CSCuv20449	キャプチャまたは連続 ping を使用する場合のスレッド名 ssh でのトレースバック

ID	説明
CSCuv49446	スレッド DATAPATH で設定を同期しているときのスタンバイデバイスでの ASA トレースバック
CSCuv50709	AnyConnect の切断後にスタンバイ ASA 内部 IP に到達できない
CSCuv58559	MPF で「set connection」を変更する場合のスレッド名 DATAPATH でのトレースバック
CSCuv66333	OCSP 応答を確認するために ASA が正しくないトラストポイントを選択する
CSCuv87150	スレッド名 fover_parse (ak47/ramfs) での ASA トレースバック
CSCuv87760	RAMFS 処理を使用したユニコーンプロキシスレッドでのトレースバック
CSCuv92371	ASA トレースバック：SSH スレッド：多数のユーザがログインしており、dACL が変更されている
CSCuv92384	ASA TCP ノーマライザがハーフオープン CONNS の無効な ACK に対して PUSH ACK を送信する
CSCuv94338	スレッド名 CP Crypto Result Processing での ASA トレースバック
CSCuw02009	ASA：SSH セッションが CLOSE_WAIT でスタックし、ASA が RST を送信する
CSCuw09578	WebVPN ストレステストを使用した ak47_platform.c での ASA 9.3.3.224 トレースバック
CSCuw14334	スレッド名 IP Address Assign でのトレースバック
CSCuw16607	ASA EIGRP がルートを削除するためにネイバーのポイズンリバースを送信しない
CSCuw17930	重複するリモートネットワークに対する S2S IPSec データパスの選択が不適切である
CSCuw19671	ASDM からバックアップ設定を復元するときの ASA トレースバック
CSCuw22130	クラスタからダイナミック PAT ステートメントを削除するときの ASA トレースバック
CSCuw22886	Kenton デバイス（9.5.1）上の EzVPN クライアントに対してスプリットトンネルが機能しない
CSCuw24664	ASA：スレッド名 - netfs_thread_init でのトレースバック
CSCuw26991	ASA：脅威の検出によるスレッド Unicorn Admin Handler でのトレースバック

ID	説明
CSCuw28735	Cisco ASA ソフトウェアバージョン情報開示の脆弱性
CSCuw29566	ASA5585 9.5(1)：Management 0/0 ポートでのフェールオーバー LAN のサポート
CSCuw33860	PRSM ダッシュボードでは RA-VPN トランザクションが 0 と表示される
CSCuw36853	ASA：インターフェイス PAT を使用したクラスタ CCL で ICMP エラーループが発生する
CSCuw39685	sfr トラフィックをフィルタ処理するとメモリ破損が発生する可能性がある
CSCuw41548	channel_put() での DNS トレースバック
CSCuw44038	多数の ldap グループを使用した ldap_client_thread でのウォッチドッグのトレースバック
CSCuw44744	WebVPN リライターでのトレースバック
CSCuw48499	QEMU コアダンプ：qemu_thread_create：リソースを一時的に使用できない
CSCuw51576	SSH 接続がスタンバイ ASA ではタイムアウトにならない（rtcli でスタック）
CSCuw55813	スレッド名 EIGRP-IPv4 でのスタンバイ ASA のトレースバック
CSCuw59388	マルチコンテキストモードで ASDM をコンテキストにロードできない
CSCuw66397	dhcpd auto_config がすでに CLI から有効化されている場合、DHCP サーバのプロセスがスタックする
CSCuw85261	SAML は Oracle OAM トンネルグループを選択できない
CSCuw86069	ASAv ではデフォルトの global_policy または inspection_default を削除/変更できない
CSCuw87331	ASA：スレッド名 DATAPATH-7-1918 でのトレースバック
CSCuw87910	ページへのアクセス時に PCP 10.6 クライアントレス VPN アクセスが拒否される
CSCuw90116	ACL のクリアおよび再設定時の ASA 9.4.1 トレースバック
CSCuw92005	スレッド名：DATAPATH-17-3095：クラスタ内の ASA が予期せずリロードされる
CSCux03626	スレッド名 Unicorn Proxy Thread でのトレースバック
CSCux05081	RSA 4096 キー生成によってフェールオーバーが発生する

ID	説明
CSCux07002	ASA：アサーション「pp->pd==pd」が失敗：ファイル「main.c」、192 行
CSCux08783	CWS：ASA は XSS ヘッダーを付加しない
CSCux09181	9.3.2 以降は http 形式の認証に失敗する
CSCux09310	ECDSA 証明書を使用する場合の ASA トレースバック
CSCux15273	show memory によって表示される使用可能な空きメモリが不正確である
CSCux16427	deny 句の PBR のルート選択が正しくない
CSCux20178	9.2 以降では、OSPF ネイバーが「reload in xx」コマンドの後にダウンする
CSCux21955	ASA：フェールオーバーがパスワード暗号化で機能していない
CSCux23659	Compact Flash の削除と dir コマンド実行後の ASA 9.1.6.10 トレースバック
CSCux29929	DATAPATH での ASA 9.4.2 トレースバック
CSCux30780	gtpv1_process_msg での GTPv1 トレースバック
CSCux36112	PBR：ポリシーベースルーティングによるクラスタモードでのメモリリーク
CSCux37303	Gi 0/0 のポートチャネル設定によってブートループが発生する：FIPS 関連
CSCux37442	ASA の WebVpn ポート フォワーディング バイナリの Cisco 署名付き証明書が期限切れ
CSCux41145	OpenSSL の pix-asa 脆弱性評価（2015 年 12 月）
CSCux42936	SIP インスペクションによるスレッド名 Datapath での ASA 9.5.1 トレースバック
CSCux43978	長いインターフェイス名を持つクラスタ ASA の DHCP リレーが失敗する
CSCux45179	SSL セッションが処理を停止：「Unable to create session directory」エラー
CSCux47195	ASA(9.5.2) が SFR リダイレクションを使用してクライアントに送信される ACK 番号を変更
CSCux56111	「no ipv6-vpn-addr-assign」CLI が機能していない
CSCux59122	ASA L7 ポリシーマップはインスペクションが再適用されている場合にのみ影響を及ぼす
CSCux61257	ASA：スレッド IP Address Assign でのトレースバック

ID	説明
CSCux69987	ASA：NAT ルールに FQDN オブジェクトを追加した後の ASA デバイスでのトレースバック
CSCux70998	スレッド名 IKE Daemon でのリロード
CSCux71197	shut/no sh 後に「show resource usage」が誤ったルート数を提供する
CSCux72610	ASA TACACS+：プロセス tacplus_snd による CPU の使用率が大きい
CSCux72835	ASA 9.5：OCSP チェックで管理の代わりにグローバル ルーティング テーブルが使用されている
CSCux81683	スレッド名 Unicorn Admin Handler での ASA トレースバック
CSCux82835	asp transactional-commit nat を有効にすると、nat プールの枯渇が確認される
CSCux86769	接続が TLS にフォールバックすると、VLAN マッピングが機能しない
CSCux87457	スレッド名 https_proxy での ASA トレースバック
CSCux88237	DATAPATH スレッドでの ASA トレースバック
CSCux93751	Cisco ASA Linux カーネルの脆弱性：CVE-2016-0728
CSCuy01420	スレッド名 Unicorn Proxy Thread での ASA トレースバック
CSCuy03024	スレッド名 idfw_proc を示す ASA トレースバックとリロード
CSCuy11905	ユーザ名がアクセスリストに記載されている場合の ASA 5585 トレースバック
CSCuy13937	TLS 処理中の CP 処理スレッドにおける ASA ウォッチドッグのトレースバック
CSCuy22561	VPN ロードバランシングは、IPv6 アドレスのロードバランシング証明書を送信しない
CSCuy27428	9.1(7) へのアップグレード後のスレッド名 snmp での ASA トレースバック
CSCuy32321	ldap 属性マッピングおよび pw 管理による ldap_client_thread でのトレースバック
CSCuy41986	チェーン内の複数の証明書が検証されると、OCSP 検証が失敗する
CSCuy47706	gtpv1_process_pdp_create_req でのトレースバック

エンドユーザライセンス契約書

エンドユーザライセンス契約書の詳細については、http://www.cisco.com/go/warranty にアクセスしてください。

関連資料

ASA の詳細については、『Navigating the Cisco ASA Series Documentation』を参照してください。

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。