Cisco ASA シリーズ 9.17(x) リリースノート

Cisco ASA シリーズ 9.17(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 9.17(x) のリリース情報が記載されています。

特記事項

- **9.17(1.13)/7.18(1.152) 以降で ASDM 署名付きイメージをサポート**：ASA は、ASDM イメージがシスコのデジタル署名付きイメージであるかどうかを検証するようになりました。この修正を適用した ASA バージョンで古い ASDM イメージを実行しようとすると、ASDM がブロックされ、「%ERROR: Signature not valid for file disk0:/<filename>」というメッセージが ASA CLI に表示されます。ASDM リリース 7.18(1.152) 以降は、この修正が適用されていないものも含め、すべての ASA バージョンと下位互換性があります。（CSCwb05291、CSCwb05264）
- **9.17(1) 以降では ASA 5506-X、5506H-X、5506W-X、ASA 5508-X、および ASA 5516-X はサポートされていません。**ASA 9.16(x) が最後にサポートされたバージョンです。ASA 5508-X および 5516-X の ASA FirePOWER モジュールの場合、最後にサポートされる組み合わせは 9.16/7.0 です。
- **9.17(1) 以降の ISA 3000 での ASA FirePOWER モジュールはサポートされていません。**ISA 3000 は ASA 9.17 以降で引き続きサポートされます。ただし、ASAFire POWER モジュールでサポートされる最後の組み合わせは 9.16/7.0 です。
- **9.17(1) 以降でのクライアントレス SSL VPN はサポートされていません。**クライアントレス SSL VPN はサポートされなくなりました。
  - **webvpn**：次のサブコマンドが削除されています。
    - **apcf**
    - **java-trustpoint**
    - **onscreen-keyboard**
    - **port-forward**
    - **portal-access-rule**
    - **rewrite**
    - **smart-tunnel**
  - **group-policy webvpn**：次のサブコマンドが削除されています。

- **port-forward**
- **smart-tunnel**
- **ssl-clientless**

システム要件

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

ASA と ASDM の互換性

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

VPN の互換性

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

新機能

このセクションでは、各リリースの新機能を示します。

（注） syslog メッセージガイドに、新規、変更済み、および廃止された syslog メッセージを記載しています。

ASA 9.17(1) の新機能

リリース日：**2021 年 12 月 1 日**

機能	説明
プラットフォーム機能	

機能	説明
Cisco Secure Firewall 3100	Cisco Secure Firewall 3110、3120、3130、および 3140 の ASA が導入されました。Cisco Secure Firewall 3100 は、スパンド EtherChannel クラスタリングで最大 6 ユニットをサポートします。ファイアウォールの電源が入っているときに、再起動することなく、同じタイプのネットワークモジュールをホットスワップできます。他のモジュールの変更を行う場合には、再起動が必要です。Secure Firewall 3100 25 Gbps インターフェイスは、Forward Error Correction と、インストールされている SFP に基づく速度検出をサポートします。SSD は自己暗号化ドライブ（SED）です。SSD が 2 つある場合、ソフトウェア RAID を形成します。 新規/変更されたコマンド： **fec, netmod, speed sfp-detect, raid, show raid, show ssd**
自動スケールに対する ASAv のサポート	ASAv は、次のパブリッククラウドサービスの自動スケールをサポートするようになりました。 • Google Cloud Platform（GCP） • Oracle Cloud Infrastrucure（OCI） 自動スケーリングは、キャパシティの要件に基づいて ASAv アプリケーションのインスタンス数を増減します。
AWS の ASAv での拡張インスタンスのサポート	AWS パブリッククラウド上の ASAv は、異なる Nitro インスタンスファミリから AWS Nitro システムインスタンスをサポートするようになりました。 AWS 用 ASAvにより、次のインスタンスのサポートが追加されています。 • c5a.large、c5a.xlarge、c5a.2xlarge、c5a.4xlarge • c5d.large、c5d.xlarge、c5d.2xlarge、c5d.4xlarge • c5ad.large、c5ad.xlarge、c5ad.2xlarge、c5ad.4xlarge • m5n.large、m5n.xlarge、m5n.2xlarge、m5n.4xlarge • m5zn.large、m5zn.xlarge、m5zn.2xlarge サポートされているインスタンスの詳細なリストについては、『Cisco Adaptive Security Virtual Appliance (ASAv) Data Sheet』を参照してください。

機能	説明
Azure の ASAv 拡張インスタンスのサポート	Azure パブリッククラウド上の ASAv は、次のインスタンスをサポートするようになりました。 • Standard_D8s_v3 • Standard_D16s_v3 • Standard_F8s_v2 • Standard_F16s_v2 サポートされているインスタンスの詳細なリストについては、『Cisco Adaptive Security Virtual Appliance (ASAv) Data Sheet』を参照してください。
ASAv の Intel® QuickAssist テクノロジー（QAT）	ASAv は、 Intel QuickAssist（QAT）8970 PCI アダプタを使用する ASAv 展開にハードウェア暗号化アクセラレーションを提供します。ASAv を使用した ASAv のハードウェア暗号化アクセラレーションは、VMware ESXi および KVM でのみサポートされます。
OCI 上の ASAv に対する Single Root I/O Virtualization（SR-IOV）のサポート。	OCI 上の ASAv に Single Root Input/Output Virtualization（SR-IOV）を実装できるようになりました。SR-IOV により、ASAv のパフォーマンスを向上させることができます。SR-IOV モードでの vNIC としての Mellanox 5 はサポートされていません。
ファイアウォール機能	
変換後（マップ後）の宛先としての完全修飾ドメイン名（FQDN）オブジェクトの Twice NAT サポート	www.example.com を指定する FQDN ネットワークオブジェクトを、Twice NAT ルールの変換後（マップ後）の宛先アドレスとして使用できます。システムでは、DNS サーバーから返された IP アドレスに基づいてルールが設定されます。
ネットワークサービス オブジェクトと、ポリシーベースのルーティングおよびアクセス制御におけるネットワークサービス オブジェクトの使用	ネットワークサービス オブジェクトを設定し、それらを拡張アクセス コントロール リストで使用して、ポリシーベース ルーティング ルート マップおよびアクセス コントロール グループで使用できます。ネットワークサービス オブジェクトには、IP サブネットまたは DNS ドメイン名の仕様が含まれ、オプションでプロトコルとポートの仕様が含まれます。これらは、基本的にネットワークオブジェクトとサービスオブジェクトを結合します。この機能には、信頼できる DNS サーバーを定義して、DNS ドメイン名解決が信頼できる送信元から IP アドレスを確実に取得できるようにする機能も含まれています。 次のコマンドが追加または変更されました：**access-list extended**、**app-id**、**clear configure object network-service**、**clear configure object-group network-service**、**clear dns ip-cache**、**clear object**、**clear object-group**、**debug network-service**、**description**、**dns trusted-source**、**domain**、**network-service-member**、**network-service reload**、**object-group network-service**、**object network-service**、**policy-route cost**、**set adaptive-interface cost**、**show asp table classify**、**show asp table network-service**、**show dns trusted-source**、**show dns ip-cache**、**show object**、**show object-group**、**show running-config**、**subnet**

機能	説明
ハイ アベイラビリティとスケーラビリティの各機能	
VMware および KVM 用の ASAv30、ASAv50、および ASAv 100 クラスタリング	ASAv クラスタリングを使用すると、最大 16 の ASAv を単一の論理デバイスとしてグループ化できます。クラスタは、単一デバイスのすべての利便性（管理、ネットワークへの統合）を備える一方で、複数デバイスによって高いスループットおよび冗長性を達成します。ASAv クラスタリングは、ルーテッド ファイアウォール モードの個別インターフェイスモードをサポートします。スパンドEtherChannelはサポートされていません。ASAv は、クラスタ制御リンクに VXLAN 仮想インターフェイス（VNI）を使用します。 新規/変更されたコマンド：**cluster-interface vni**、**nve-only cluster**、**peer-group**、**show cluster info**、**show cluster info instance-type**、**show nve 1**
ハイ アベイラビリティ グループまたはクラスタ内のルートのクリア	以前のリリースでは、**clear route** コマンドはユニットのルーティングテーブルのみをクリアしました。現在、ハイアベイラビリティ グループまたはクラスタで動作している場合、コマンドはアクティブユニットまたはコントロールユニットでのみ使用でき、グループまたはクラスタ内のすべてのユニットのルーティングテーブルをクリアします。 **clear route** コマンドが変更されました。
インターフェイス機能	
ASAv の Geneve インターフェイスサポート	AWS ゲートウェイロードバランサのシングルアームプロキシをサポートするために、ASAv30、ASAv50、および ASAv100 の Geneve カプセル化サポートが追加されました。 新規/変更されたコマンド：**debug geneve**、**debug nve**、**debug vxlan**、**encapsulation**、**packet-tracer geneve**、**proxy single-arm**、**show asp drop**、**show capture**、**show interface**、**show nve**
Secure Firewall 3100 の自動ネゴシエーションは、1 ギガビット以上のインターフェイスで有効または無効にすることができます。	Secure Firewall 3100 の自動ネゴシエーションは、1 ギガビット以上のインターフェイスで有効または無効にすることができます。他のモデルの SFP ポートの場合、**no speed nonegotiate** オプションは速度を 1000 Mbps に設定します。新しいコマンドは、自動ネゴシエーションと速度を個別に設定できることを意味します。 新規/変更されたコマンド：**negotiate-auto**
管理およびトラブルシューティングの機能	

機能	説明
起動時間と tmatch コンパイルステータス。	**show version** コマンドには、システムの起動（ブート）にかかった時間に関する情報が含まれるようになりました。設定が大きいほど、システムの起動に時間がかかることに注意してください。 新しい **show asp rule-engine** コマンドは、tmatch コンパイルのステータスを表示します。Tmatch コンパイルは、アクセスグループ、NAT テーブル、およびその他のいくつかの項目として使用されるアクセスリストに使用されます。これは、非常に大きな ACL と NAT テーブルがある場合には、CPU リソースを消費し、進行中のパフォーマンスに影響を与える可能性がある内部プロセスです。コンパイル時間は、アクセスリスト、NAT テーブルなどのサイズによって異なります。
show access-list element-count 出力の拡張と **show tech-support** コンテンツの強化	**show access-list element-count** の出力は、次のように拡張されています。 • マルチコンテキストモードのシステムコンテキストで使用すると、出力には、すべてのコンテキストのすべてのアクセスリストの要素数が表示されます。 • オブジェクトグループ検索を有効にして使用すると、出力には要素数のオブジェクトグループの数に関する詳細が含まれます。 さらに、**show tech-support** 出力には **show access-list element-count** と **show asp rule-engine** の出力が含まれます。
CiscoSSH スタック	ASA は、SSH 接続に独自の SSH スタックを使用します。代わりに、OpenSSH に基づく CiscoSSH スタックを使用するように選択できるようになりました。デフォルトスタックは引き続き ASA スタックです。Cisco SSH は次をサポートします。 • FIPS の準拠性 • シスコおよびオープンソースコミュニティからの更新を含む定期的な更新 CiscoSSH スタックは次をサポートしないことに注意してください。 • VPN を介した別のインターフェイスへの SSH（管理アクセス） • EdDSA キーペア • FIPS モードの RSA キーペア これらの機能が必要な場合は、引き続き ASA SSH スタックを使用する必要があります。 CiscoSSH スタックでは、SCP 機能に若干の変更があります。ASA **copy** コマンドを使用して SCP サーバとの間でファイルをコピーするには、**ssh** コマンドを使用して、ASA で SCP サーバサブネット/ホストの SSH アクセスを有効にする必要があります。 新規/変更されたコマンド： **ssh stack ciscossh**

機能	説明
パケットトレーサでの PCAP サポート	パケットトレーサツールで PCAP ファイルを再生し、トレース結果を取得できます。**pcap** および **force** は、パケットトレーサでの PCAP の使用をサポートするための 2 つの新しいキーワードです。 新規/変更されたコマンド：**packet-tracer input** および**show packet-tracer**
より強力なローカルユーザーと有効なパスワード要件	ローカルユーザーと有効なパスワードについて、次のパスワード要件が追加されました。 • パスワードの長さ：8 文字以上。以前は、最小値が 3 文字でした。 • 繰り返し文字と連続文字：3 つ以上の連続した ASCII 文字または繰り返しの ASCII 文字は許可されません。たとえば、次のパスワードは拒否されます。 • **abc**user1 • user**543** • user**aaaa** • user2**666** 新規/変更されたコマンド：**enable password**、**username**
ローカルユーザーのロックアウトの変更	設定可能な回数のログイン試行に失敗すると、ASA はローカルユーザーをロックアウトする場合があります。この機能は、特権レベル 15 のユーザーには適用されませんでした。また、管理者がアカウントのロックを解除するまで、ユーザーは無期限にロックアウトされます。管理者がその前に **clear aaa local user lockout** コマンドを使用しない限り、ユーザーは 10 分後にロック解除されるようになりました。特権レベル 15 のユーザーも、ロックアウト設定が適用されるようになりました。 新規/変更されたコマンド：**aaa local authentication attempts max-fail** 、**show aaa local user**
SSH および Telnet パスワード変更プロンプト	ローカルユーザーが SSH または Telnet を使用して ASA に初めてログインすると、パスワードを変更するように求められます。また、管理者がパスワードを変更した後、最初のログインに対してもプロンプトが表示されます。ただし、ASA がリロードすると、最初のログインであっても、ユーザーにプロンプトは表示されません。 VPN などのローカル ユーザー データベースを使用するサービスは、SSH または Telnet ログイン中に変更された場合、新しいパスワードも使用する必要があることに注意してください。 新規/変更されたコマンド： **show aaa local user**
モニタリング機能	

機能	説明
SNMPは、ネットワークオブジェクトの形式で複数のホストをグループ化するときにIPv6をサポートするようになりました	**snmp-server** コマンドの **host-group** コマンドは、IPv6ホスト、範囲、およびサブネットオブジェクトをサポートするようになりました。 新規/変更されたコマンド： **snmp-server host-group**
VPN 機能	
IKEv2 のローカルトンネル ID のサポート	IKEv2 のローカルトンネルID設定のサポートが追加されました。 新規/変更されたコマンド： **set ikev2 local-identity**
DAP 制約による SAML 属性のサポート	DAP ポリシーの選択に使用できる SAML アサーション属性のサポートが追加されました。また、*cisco_group_policy* 属性でグループポリシーを指定する機能も導入されています。
IDP 設定の複数の SAML トラストポイント	この機能は、同じエンティティ ID の複数のアプリケーションをサポートするアプリケーションの SAML IDP 設定ごとに、複数の IDP トラストポイントの追加をサポートします。 新規/変更されたコマンド： **saml idp-trustpoint <trustpoint-name>**
AnyConnect VPN SAML 外部ブラウザ	AnyConnect VPN SAML 外部ブラウザを設定して、パスワードなしの認証、WebAuthN、FIDO2、SSO、U2F、Cookie の永続性による SAML エクスペリエンスの向上など、追加の認証の選択肢を有効にできるようになりました。リモートアクセスVPN接続プロファイルのプライマリ認証方式としてSAMLを使用する場合は、AnyConnectクライアントクライアントがAnyConnectクライアント組み込みブラウザではなく、クライアントのローカルブラウザを使用してWeb認証を実行するように選択できます。このオプションは、VPN認証と他の企業ログインの間のシングルサインオン（SSO）を有効にします。また、生体認証やYubikeysなど、埋め込みブラウザでは実行できないWeb認証方法をサポートする場合は、このオプションを選択します。 新規/変更されたコマンド： **external-browser**
SAML を使用した VPN ロードバランシング	ASA は、SAML 認証を使用した VPN ロードバランシングをサポートす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。

ASA のアップグレードパス

現在のバージョンとモデルを表示するには、次のいずれかの方法を使用します。

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

次の表に、ASA のアップグレードパスを示します。バージョンによっては、新しいバージョンにアップグレードする前に、中間アップグレードが必要な場合があります。推奨バージョンは**太字**で示されています。

（注） 開始バージョンと終了バージョンの間で、各リリースのアップグレードガイドラインを必ず確認してください。場合によっては、アップグレードする前に構成を変更する必要があります。そうしないと、停止が発生する可能性があります。

（注） ASA のセキュリティの問題と、各問題に対する修正を含むリリースについては、ASA Security Advisories を参照してください。

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

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

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

ASA 9.2(x) は ASA 5505 用の最終バージョン、

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

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

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

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

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

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

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

アップグレードリンク

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

未解決のバグおよび解決されたバグ

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

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

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

バージョン 9.17(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。

不具合 ID 番号	説明
CSCvz62406	s2s トラフィック（7.0.1-54）に pat が設定されている場合、6 ノード SSP クラスタのコントロールユニットでクラッシュが観察されました

不具合 ID 番号	説明
CSCwa08743	ASA/FTD トレースバックし、コード 7.0.1 を実行している 2100 でリロードします
CSCwa19713	asp ドロップタイプ「no-adjacency」が原因で BVI インターフェイスで設定された ASA によってトラフィックがドロップしました
CSCwa21054	ASA/FTD は、スレッド名「DATAPATH-2-14497」でトレースバックおよびリロードする場合があります
CSCwa29596	FP1010 HA ASA インターフェイスは、フェールオーバー後に「正常」にならず、通信できません。

バージョン 9.17(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。

不具合 ID 番号	説明
CSCvo77184	VMware ASAv は、e1000 ではなく vmxnet3 にデフォルト設定する必要があります
CSCvz00032	Cisco Firepower Threat Defense ソフトウェアの TCP Proxy DoS 攻撃に対する脆弱性
CSCvz70595	SAML ハンドラの処理中に ASA でトレースバックを検出
CSCwa04461	Cisco ASA ソフトウェアおよび FTD ソフトウェアリモートアクセスの SSL VPN サービス拒否
CSCvu98260	特定のシナリオで HA が nsf を有効にすると、DRP データベースに古いルートが表示されます
CSCvx14489	フェイルオーバー後に ipv6 インターフェイスで snmpwalk が失敗します
CSCvx16317	管理のコンテキストが変更されると、マルチコンテキスト ASA から connect fxos admin で FXOS にアクセスできない
CSCvx54562	FTD の高いシステムオーバーヘッドのメモリ
CSCvx59252	FXOS は管理インターフェイスのログファイルをローテーションしていません
CSCvx75683	「show cluster info trace」の出力が「タグが存在しません」というメッセージにより負担がかかっています
CSCvx76665	2100 および 1010 で表示される「インターフェイスのアップデートに失敗しました」というエラーメッセージ

不具合 ID 番号	説明
CSCvy03324	ASA: ECMP sVTI サポート
CSCvy58705	「clear conf all」または「clear conf failover」は、有効になっているフェールオーバーデバッグをクリアする必要があります
CSCvy69453	WM スタンバイデバイスは、再起動後にコールドスタートトラップを送信しません
CSCvy78525	VRF が設定されている場合、FTD は TCP ping を実行しません
CSCvy79952	ダウングレード後の ASA/FTD トレースバックとリロード
CSCvy82668	SSH セッションが解放されません
CSCvy84336	ポートチャネルのメンバーインターフェイスがアクティブとスタンバイで異なる場合に警告を追加します
CSCvy86817	カスタム CCL IP サブネットが設定されている場合、Cruz CLU フィルタに誤った src/dst IP サブネットがあります
CSCvy96895	フェールオーバー後、ASA がアクティブ IP アドレスとスタンバイ MAC アドレスを使用して VTY セッションを切断します
CSCvy99217	IKEv2: SA エラーコードは、ユーザーにわかりやすいように理由を変換する必要があります
CSCvz14305	IKEv2RA サードパーティのデュアルスタック IPv4 および IPv6 が要求されました。ASA は IKEAuth に応答しません
CSCvz17046	16 ノードクラスタセットアップをアップグレードまたはリロードしようとすると、ASAv がクラッシュしました
CSCvz25454	ASA：129 行の asp-drop キャプチャにドロップ理由がありません
CSCvz51258	show tech-support の出力は、crashinfo がある場合に混乱を招く可能性があり、クリーンアップするまたは直感的にする必要があります
CSCvz67816	FTD で変更される IPV6 DNS PTR クエリ
CSCvz71064	ikev2 トンネルで約 2 分かかる ASA からのコンテキストを削除します
CSCvz71596	「アクティブとスタンバイのインターフェイスの数が一致していません」という警告の syslog がトリガーされるはずです。

エンドユーザーライセンス契約書

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

関連資料

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

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。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。

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

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。