シスコ脆弱性データベース（VDB）アップデート 339 リリース ノート

Cisco Vulnerability Database について

シスコ脆弱性データベース（VDB）は、オペレーティング システム、クライアント、およびアプリケーションのフィンガープリントだけでなく、ホストが影響を受ける可能性がある既知の脆弱性のデータベースです。システムでは、VDB を使用して、特定のホストで感染のリスクが高まるかどうかを判断します。

シスコでは、VDB に対して定期的に更新を提供しています。Firepower Management Center で VDB と関連付けられたマッピングの更新にかかる時間は、ネットワーク マップ内のホストの数によって異なります。一般的に、更新の実行にかかるおおよその時間（分）を判断するには、ホストの数を 1000 で割ります。

VDB の更新は、Cisco.com の VDB ソフトウェアのダウンロードページで確認することができます。

Cisco Firepower Application Detector リファレンスについて

『Cisco Firepower Application Detector リファレンス』には、リリースノートと、VDB リリースでサポートされているアプリケーションディテクタに関する情報が含まれています。本リファレンスに記載されている各アプリケーションについては、次の情報を確認できます。

- 説明：アプリケーションの簡単な説明。
- カテゴリ：アプリケーションの最も重要な機能を説明する一般分類。カテゴリの例としては、「Web サービスプロバイダ」、「e-コマース」、「広告ポータル」、および「ソーシャルネットワーキング」などがあります。
- タグ：アプリケーションに関する追加情報を表示する事前定義のタグ。タグの例としては、「Web メール」、「SSL プロトコル」、「ファイルの共有/転送」、および「広告の表示」などがあります。アプリケーションには、0 個、1 個、または複数個のタグが割り当てられています。
- リスク：アプリケーションが組織のセキュリティポリシーに違反しうる目的で使用される可能性。リスクのレベルは次のとおりです。「非常に高い」、「高」、「中」、「低」、および「非常に低い」。
- ビジネスとの関連性：アプリケーションが、娯楽目的ではなく組織の事業運営の範囲で使用される可能性。関連性のレベルは次のとおりです。「非常に高い」、「高」、「中」、「低」、および「非常に低い」。

サポートされるプラットフォームとソフトウェア バージョン

このガイドは、次のプラットフォームのソフトウェア バージョンでインストールされる脆弱性データベース アップデートに関するガイドです。

Sourcefire 3D システム/Firepower システム バージョン 5.x：

- Cisco FireSIGHT Management Centers（旧 Defense Centers）

Firepower バージョン 6.x：

- Cisco Firepower Management Centers（旧 Defense Centers/FireSIGHT Management Centers）

サポートされるディテクタ タイプ

サポートされているディテクタ タイプは次のとおりです。

- アプリケーション プロトコル
- クライアント
- Web アプリケーション

脆弱性データベースアップデート 339 でサポートされるアプリケーションの合計数

シスコ脆弱性データベース（VDB）アップデート 339 では、3,593 種類のアプリケーションをサポートしています。

脆弱性データベースアップデート 339 の変更ログ

このセクションでは、VDB 338（2020 年 9 月 24 日 13:00:29 UTC）から VDB 339（2020 年 11 月 5 日 21:41:10 UTC）への変更について説明します。

アプリケーション プロトコル ディテクタ

合計追加数：	9
合計削除数：	0
合計更新数	3

クライアント ディテクタ

合計追加数：	0
合計削除数：	0
合計更新数	2

Web アプリケーション ディテクタ

合計追加数：	8
合計削除数：	1
合計更新数	48

FireSIGHT/Firepower ディテクタの更新

合計追加数：	0
合計削除数：	0
合計更新数	0

オペレーティング システム フィンガープリントの詳細

合計追加数：	0
合計削除数：	0
合計更新数	0

オペレーティング システムおよびハードウェア フィンガープリントの詳細

合計追加数：	0
合計削除数：	0

合計更新数	0

脆弱性の参照

合計追加数：	141
合計削除数：	0
合計更新数	0

フィンガープリントの参照

合計追加数：	0
合計削除数：	0
合計更新数	0

ファイル タイプ ディテクタ

合計追加数：	0
合計削除数：	0
合計更新数	1

オペレーティング システム フィンガープリントの詳細：

- 追加または変更なし

オペレーティング システムおよびハードウェア フィンガープリントの詳細：

- 追加または変更なし

フィンガープリント参照の詳細：

- 追加または変更なし

アプリケーション プロトコル ディテクタ：

- DLMS-COSEM：（デバイス言語メッセージ仕様）/COSEM（電力計用 CompanionSpecification）は、計測機器とのデータ交換のためのインターフェイスモデルと通信プロトコルを指定します。（追加）
- DLMS-COSEM Get Response：以前に受信した GET 表示プリミティブに応答を送信する DLMS-COSEM サービス。（追加）
- DLMS-COSEM Set Response：以前に受信した SET 表示プリミティブに応答を送信する DLMS-COSEM サービス。（追加）
- DLMS-COSEM Get Request：1 つまたはすべての属性の値を取得するための DLMS-COSEM サービスリクエスト。（追加）

- DLMS-COSEM Set Request：1 つまたはすべての属性の値を設定するための DLMS-COSEM サービスリクエスト。（追加）
- DLMS-COSEM Initiate Response：ユーザ情報交換のための DLMS-COSEM サービス応答。（追加）
- DLMS-COSEM Initiate Request No Authentication：認証なしによるユーザ情報交換のための DLMS-COSEM サービスリクエスト。（追加）
- DLMS-COSEM Initiate Request Low-Level Authentication：低レベル認証によるユーザ情報交換のための DLMS-COSEM サービスリクエスト。（追加）
- DLMS-COSEM Initiate Request High-Level Authentication：高レベル認証によるユーザ情報交換のための DLMS-COSEM サービスリクエスト。（追加）
- TCX 関連サービス（TCX Flash、TCX Multimedia、TCX Sound、および TCX USB）：一部のフローが STUN として認識されていました。TCX トラフィックフローを正しく分類するためにディテクタが更新されました。（更新済み）
- SSL、HTTPS：TLS ja3 属性を抽出する際のメモリ使用率が拡張されました。（更新済み）
- SSH：フローを適切に分類するためにディテクタが更新されました。（更新済み）

クライアント ディテクタ：

- Ultrasurf：UltraSurf アプリバージョン 20.03 のサポートが追加されました。（更新済み）
- Telegram：SSL のトラフィックからの誤検出を修正するためにパターンが更新されました。（更新済み）

Web アプリケーション ディテクタ：

- Xbox Live：検出パターンが変更されました。（更新済み）
- GMX Mail：GMX Web サイトの複数の地理的ドメインのパターンをカバーするために検出パターンが変更されました。（更新済み）
- GMX：無料 Web メールおよび電子メールサービスプロバイダー。（削除）。
- Twitter：TwitPic のトラフィックからの誤検出を修正するためにパターンが更新されました。（更新済み）
- Ybrant Digital：Lycos のトラフィックからの誤検出を修正するためにパターンが更新されました。（更新済み）
- Apache Nutch：Tinder のトラフィックからの誤検出を修正するためにパターンが更新されました。（更新済み）
- Amazon：AWS のトラフィックからの誤検出を修正するためにパターンが更新されました。（更新済み）
- Aggregate Knowledge：Neustar Information Services のトラフィックからの誤検出を修正するためにパターンが更新されました。（更新済み）

- Office 365：Microsoft Azure のトラフィックからの誤検出を修正するためにパターンが更新されました。（更新済み）
- Microsoft CRM Dynamics：Office 365 のトラフィックからの誤検出を修正するためにパターンが更新されました。（更新済み）
- Tencent Cloud：WeChat のトラフィックからの誤検出を修正するためにパターンが更新されました。（更新済み）
- Webex Teams：Cisco Jabber のトラフィックからの誤検出を修正し、その他の検出漏れをカバーするためにパターンが更新されました。（更新済み）
- Taobao：Tmall のトラフィックからの誤検出を修正するためにパターンが更新されました。（更新済み）
- Alisoft：Leadbolt のトラフィックからの誤検出を修正するためにパターンが更新されました。（更新済み）
- Wooprа：Disqus のトラフィックからの誤検出を修正するためにパターンが更新されました。（更新済み）
- CNET TV：Cnet Web サイトのトラフィックからの誤検出を修正するためにパターンが更新されました。（更新済み）
- Alibaba：Taobao Web サイトのトラフィックからの誤検出を修正するためにパターンが更新されました。（更新済み）
- Google Ads：Doubleclick のトラフィックからの誤検出を修正するためにパターンが更新されました。（更新済み）
- BBC iPlayer：BBC Web サイトのトラフィックからの誤検出を修正するためにパターンが更新されました。（更新済み）
- Soso：Sogou Web サイトのトラフィックからの誤検出を修正するためにパターンが更新されました。（更新済み）
- Lord & Taylor：Saks Fifth Avenue Web サイトのトラフィックからの誤検出を修正するためにパターンが更新されました。（更新済み）
- People.com：TIME.com Web サイトのトラフィックからの誤検出を修正するためにパターンが更新されました。（更新済み）
- Entertainment Weekly：TIME.com Web サイトのトラフィックからの誤検出を修正するためにパターンが更新されました。（更新済み）
- Aliwangwang：Taobao Web サイトのトラフィックからの誤検出を修正するためにパターンが更新されました。（更新済み）
- ibVPN Login：ibVPN Web サイトのトラフィックからの誤検出を修正するためにパターンが更新されました。（更新済み）
- GTA Online：Rockstar Games のトラフィックからの誤検出を修正するためにパターンが更新されました。（更新済み）

- Myspace：Myspace、Myspace Photos、Myspace Videos を区別するためにパターンが更新されました。（更新済み）
- YiXin：Netease のトラフィックからの誤検出を修正するためにパターンが更新されました。（更新済み）
- Crackle Video：Crackle Web サイトのトラフィックからの誤検出を修正するためにパターンが更新されました。（更新済み）
- Hulu Video：Hulu Web サイトのトラフィックからの誤検出を修正するためにパターンが更新されました。（更新済み）
- CC Studios：Comedy Central Web サイトのトラフィックからの誤検出を修正するためにパターンが更新されました。（更新済み）
- Netflix Stream：Netflix Web サイトのトラフィックからの誤検出を修正するためにパターンが更新されました。（更新済み）
- Zynga：Words With Friends からのトラフィックを区別するためにパターンが更新されました。（更新済み）
- T Mobile：Advertising.com のトラフィックからの誤検出を修正するためにパターンが更新されました。（更新済み）
- Facebook：Facebook ビデオ、Facebook フォト、Facebook の検出を区別するためにパターンが更新されました（更新済み）
- Alibaba：Alipay トラフィックからの誤検出を修正するためにパターンが更新されました。（更新済み）
- F-secure：Malwarebytes の誤検出を回避するためにパターンが更新されました。（更新済み）
- Windows Live Skydrive：OneDrive のトラフィックからの誤検出を修正するためにパターンが更新されました。（更新済み）
- Power BI：説明の更新、および検出機能の強化が行われました。（更新済み）
- Microsoft Teams：UDP トラフィックを含むようにカバレッジが拡張されました。（更新済み）
- Azure Service Bus：Azure Service Bus は、アプリケーションとサービス間で情報を送信するために使用できるマルチテナント クラウド メッセージング サービスです。（追加）
- Fiserv：Fiserv は、銀行、信用組合、証券処理組織、保険会社などを含めた金融業界向けテクノロジーソリューションのプロバイダーです。（追加）
- Jaspersoft：Jaspersoft 組み込み分析ソフトウェアは、プログラムによる制御でレポートと分析を設計、埋め込み、管理するための BI プラットフォームです。、（追加）
- QlikView：QlikView は、ビジネスの課題に合わせてカスタマイズされたガイド付き分析アプリケーションとダッシュボードを作成するための、BI データ検出製品です。（追加）

- RingCentral：RingCentral は、企業向けのクラウドベースの通信およびコラボレーション ソリューションを提供する米国の公開プロバイダーです。（追加）
- Tableau：Tableau Software は、データの画像およびグラフィック表示を提供するインタラクティブなデータ可視化およびデータ分析ソフトウェアです。（追加）
- VPN Monster：VPN Monster はロシアに拠点を置く VPN サービスプロバイダーで、ユーザに大幅な匿名性とセキュリティを提供します。（追加）
- OneLogin：クラウドベースのアイデンティティおよびアクセス管理サービス。（追加）
- Smartsheet：検出パターンが修正されました。（更新済み）
- Jira：アプリケーション名が小文字に変更され、検出パターンが追加されました。（更新済み）
- Box：未使用のパターンが削除されました。（更新済み）
- Showbox：未使用パターンが削除されました。（更新済み）
- ServiceNow：OneLogin のトラフィックからの誤検出を修正するためにパターンが更新されました。（更新済み）
- QQ Games：検出パターンが修正されました。（更新済み）
- Google Hangouts：フローを適切に分類するためにディテクタが更新されました（更新済み）
- Google：Facebook のトラフィックからの誤検出を修正するためにパターンが更新されました。（更新済み）
- Imo.im：一部の SMTP および SMB フローが imo.im として分類されていたため、ディテクタが更新されました。（更新済み）

FireSIGHT/Firepower ディテクタの更新：

- 追加または変更なし

ファイル タイプ ディテクタの詳細：

- POSIX_TAR POSIX テープアーカイブファイル：パターンが更新されました。（更新済み）

Snort ID の脆弱性の参照の詳細：

- CVE：2010-1119 - Snort 参照 ID 29623、18958、18957、56042（追加）
- CVE：2015-6098 - Snort 参照 ID 36745、36744、55198、55197（追加）
- CVE：2017-6331 - Snort 参照 ID 55814、55813（追加）
- CVE：2018-15959 - Snort 参照 ID 56151、56150（追加）
- CVE：2018-4314 - Snort 参照 ID 56044、56043（追加）

- CVE：2018-4416 - Snort 参照 ID 56009、56008（追加）
- CVE：2018-4939 - Snort 参照 ID 56151、56150（追加）
- CVE：2018-9995 - Snort 参照 ID 46826、46825、55840、55839（追加）
- CVE：2019-0230 - Snort 参照 ID 41923、41922（追加）
- CVE：2019-0233 - Snort 参照 ID 56001、56000、55999（追加）
- CVE：2019-0604 - Snort 参照 ID 51368、49861、50275、55862（追加）
- CVE：2019-13372 - Snort 参照 ID 55981（追加）
- CVE：2019-13373 - Snort 参照 ID 56002（追加）
- CVE：2019-13374 - Snort 参照 ID 56004（追加）
- CVE：2019-13375 - Snort 参照 ID 56007、56006、56005（追加）
- CVE：2019-15283 - Snort 参照 ID 52102、52103（追加）
- CVE：2019-15285 - Snort 参照 ID 52106、52107（追加）
- CVE：2019-15287 - Snort 参照 ID 52110、52111（追加）
- CVE：2019-15957 - Snort 参照 ID 52119、52120、52121、52122（追加）
- CVE：2019-15993 - Snort 参照 ID 52993、52994、52995、52996、52997（追加）
- CVE：2019-16009 - Snort 参照 ID 52559、52560（追加）
- CVE：2019-16019 - Snort 参照 ID 52633（追加）
- CVE：2019-16021 - Snort 参照 ID 52633（追加）
- CVE：2019-16023 - Snort 参照 ID 52633（追加）
- CVE：2019-16028 - Snort 参照 ID 52627、52628、52629、52630、52631（追加）
- CVE：2019-1888 - Snort 参照 ID 53168（追加）
- CVE：2019-1983 - Snort 参照 ID 53170（追加）
- CVE：2019-8762 - Snort 参照 ID 55799、55798（追加）
- CVE：2019-9670 - Snort 参照 ID 49865、49864（追加）
- CVE：2020-0664 - Snort 参照 ID 55140、55139（追加）
- CVE：2020-0856 - Snort 参照 ID 55206（追加）
- CVE：2020-0941 - Snort 参照 ID 55188、55187（追加）
- CVE：2020-1115 - Snort 参照 ID 55142、55141 （追加）
- CVE：2020-1152 - Snort 参照 ID 55162、55161（追加）

- CVE：2020-1170 - Snort 参照 ID 55922（追加）
- CVE：2020-1245 - Snort 参照 ID 55144、55143（追加）
- CVE：2020-1308 - Snort 参照 ID 55146、55145（追加）
- CVE：2020-13499 - Snort 参照 ID 54478（追加）
- CVE：2020-13500 - Snort 参照 ID 54478（追加）
- CVE：2020-13501 - Snort 参照 ID 54478（追加）
- CVE：2020-13504 - Snort 参照 ID 54480（追加）
- CVE：2020-13505 - Snort 参照 ID 54480（追加）
- CVE：2020-13699 - Snort 参照 ID 54995、54994（追加）
- CVE：2020-13934 - Snort 参照 ID 55801、55800（追加）
- CVE：2020-13935 - Snort 参照 ID 56086（追加）
- CVE：2020-14386 - Snort 参照 ID 56052、56051（追加）
- CVE：2020-14644 - Snort 参照 ID 55933、55932（追加）
- CVE：2020-1472 - Snort 参照 ID 55704、55703、55802（追加）
- CVE：2020-15363 - Snort 参照 ID 55838、55837、55836（追加）
- CVE：2020-15364 - Snort 参照 ID 55835、55834（追加）
- CVE：2020-15505 - Snort 参照 ID 56155、56154（追加）
- CVE：2020-16875 - Snort 参照 ID 55826（追加）
- CVE：2020-16896 - Snort 参照 ID 55994（追加）
- CVE：2020-16898 - Snort 参照 ID 55984（追加）
- CVE：2020-16899 - Snort 参照 ID 55993（追加）
- CVE：2020-16907 - Snort 参照 ID 55943、55942（追加）
- CVE：2020-16913 - Snort 参照 ID 55990、55989（追加）
- CVE：2020-16915 - Snort 参照 ID 55980、55979（追加）
- CVE：2020-16922 - Snort 参照 ID 55983、55982（追加）
- CVE：2020-16947 - Snort 参照 ID 56157、56156（追加）
- CVE：2020-16952 - Snort 参照 ID 56136、56135、56134、56070、56069（追加）
- CVE：2020-17496 - Snort 参照 ID 51621、51620、51837、51836、51835（追加）
- CVE：2020-25213 - Snort 参照 ID 55778（追加）

- CVE：2020-3141 - Snort 参照 ID 55815、55816、55817（追加）
- CVE：2020-3304 - Snort 参照 ID 16195（追加）
- CVE：2020-3359 - Snort 参照 ID 55832（追加）
- CVE：2020-3399 - Snort 参照 ID 55830（追加）
- CVE：2020-3425 - Snort 参照 ID 55818（追加）
- CVE：2020-3426 - Snort 参照 ID 55808（追加）
- CVE：2020-3430 - Snort 参照 ID 55016、55017、55018、55035（追加）
- CVE：2020-3436 - Snort 参照 ID 56087（追加）
- CVE：2020-3456 - Snort 参照 ID 56084、56085（追加）
- CVE：2020-3487 - Snort 参照 ID 55831、55924、55925（追加）
- CVE：2020-3488 - Snort 参照 ID 55806（追加）
- CVE：2020-3492 - Snort 参照 ID 55820（追加）
- CVE：2020-3494 - Snort 参照 ID 55807（追加）
- CVE：2020-3495 - Snort 参照 ID 55035（追加）
- CVE：2020-3510 - Snort 参照 ID 55822（追加）
- CVE：2020-3516 - Snort 参照 ID 55833（追加）
- CVE：2020-3526 - Snort 参照 ID 55819（追加）
- CVE：2020-3528 - Snort 参照 ID 56090、56091（追加）
- CVE：2020-3572 - Snort 参照 ID 56089（追加）
- CVE：2020-3894 - Snort 参照 ID 55013、55012（追加）
- CVE：2020-4211 - Snort 参照 ID 55921、55920、55919、55918（追加）
- CVE：2020-6083 - Snort 参照 ID 53125（追加）
- CVE：2020-6085 - Snort 参照 ID 53049（追加）
- CVE：2020-6086 - Snort 参照 ID 53049、53127（追加）
- CVE：2020-6087 - Snort 参照 ID 53128（追加）
- CVE：2020-6097 - Snort 参照 ID 53565（追加）
- CVE：2020-6104 - Snort 参照 ID 53731、53732（追加）
- CVE：2020-6105 - Snort 参照 ID 53684、53685（追加）
- CVE：2020-6106 - Snort 参照 ID 53742、53743（追加）

- CVE：2020-6107 - Snort 参照 ID 53684、53685（追加）
- CVE：2020-6108 - Snort 参照 ID 53729、53730（追加）
- CVE：2020-6112 - Snort 参照 ID 53990、53991（追加）
- CVE：2020-6113 - Snort 参照 ID 53948、53949（追加）
- CVE：2020-6115 - Snort 参照 ID 53992、53993（追加）
- CVE：2020-6116 - Snort 参照 ID 54010、54011（追加）
- CVE：2020-6117 - Snort 参照 ID 54132、54133、54134（追加）
- CVE：2020-6118 - Snort 参照 ID 54132、54133、54134（追加）
- CVE：2020-6119 - Snort 参照 ID 54132、54133、54134（追加）
- CVE：2020-6120 - Snort 参照 ID 54132、54133、54134（追加）
- CVE：2020-6121 - Snort 参照 ID 54132、54133、54134（追加）
- CVE：2020-6122 - Snort 参照 ID 54132、54133、54134（追加）
- CVE：2020-6123 - Snort 参照 ID 54135、54136、54137（追加）
- CVE：2020-6124 - Snort 参照 ID 54135、54136、54137（追加）
- CVE：2020-6125 - Snort 参照 ID 54138（追加）
- CVE：2020-6126 - Snort 参照 ID 54139、54140、54141（追加）
- CVE：2020-6127 - Snort 参照 ID 54139、54140、54141（追加）
- CVE：2020-6128 - Snort 参照 ID 54139、54140、54141（追加）
- CVE：2020-6129 - Snort 参照 ID 54142、54143、54144（追加）
- CVE：2020-6130 - Snort 参照 ID 54142、54143、54144（追加）
- CVE：2020-6131 - Snort 参照 ID 54142、54143、54144（追加）
- CVE：2020-6132 - Snort 参照 ID 54123、54124、54125（追加）
- CVE：2020-6133 - Snort 参照 ID 54126、54127、54128（追加）
- CVE：2020-6134 - Snort 参照 ID 54129、54130、54131（追加）
- CVE：2020-6135 - Snort 参照 ID 54259、54260、54261（追加）
- CVE：2020-6136 - Snort 参照 ID 54262、54263、54264（追加）
- CVE：2020-6137 - Snort 参照 ID 54251、54252、54253（追加）
- CVE：2020-6138 - Snort 参照 ID 54251、54252、54253（追加）
- CVE：2020-6139 - Snort 参照 ID 54251、54252、54253（追加）

- CVE：2020-6140 - Snort 参照 ID 54251、54252、54253（追加）
- CVE：2020-6141 - Snort 参照 ID 54267、54268、54269（追加）
- CVE：2020-6142 - Snort 参照 ID 54254、54255、54256（追加）
- CVE：2020-6143 - Snort 参照 ID 54257、54258（追加）
- CVE：2020-6144 - Snort 参照 ID 54257、54258（追加）
- CVE：2020-6146 - Snort 参照 ID 54047、54048（追加）
- CVE：2020-6151 - Snort 参照 ID 54411、54412、54413、54414（追加）
- CVE：2020-6152 - Snort 参照 ID 54390、54391（追加）
- CVE：2020-6388 - Snort 参照 ID 55810、55809（追加）
- CVE：2020-6967 - Snort 参照 ID 55743（追加）
- CVE：2020-7047 - Snort 参照 ID 55797（追加）
- CVE：2020-7048 - Snort 参照 ID 55797（追加）
- CVE：2020-8163 - Snort 参照 ID 55821（追加）
- CVE：2020-8193 - Snort 参照 ID 56138（追加）
- CVE：2020-8195 - Snort 参照 ID 56138、56162（追加）
- CVE：2020-8218 - Snort 参照 ID 55640、55639、55638、55637（追加）
- CVE：2020-8758 - Snort 参照 ID 55210、55209、55208、55207（追加）
- CVE：2020-8844 - Snort 参照 ID 55742、55741（追加）
- CVE：2020-9496 - Snort 参照 ID 55978（追加）
- CVE：2020-9609 - Snort 参照 ID 53563、53564（追加）

支援が必要な場合

Cisco Firepower デバイスに関するマニュアルの入手、Cisco Bug Search Tool（BST）の使用、サービス リクエストの送信、追加情報の収集の詳細については、『What's New in Cisco Product Documentation』を参照してください。

『What's New in Cisco Product Documentation』は、シスコの新規および改訂版の技術マニュアルの一覧も示し、RSS フィードとして購読できます。また、リーダー アプリケーションを使用してコンテンツをデスクトップに配信することもできます。RSS フィードは無料のサービスです。Cisco ASA デバイスに関してご質問がある場合や支援が必要な場合は、以下のシスコ サポートに連絡してください。

- 注：TAC リクエストを開くには、Cisco.com ユーザ ID を最初に登録する必要があります。
- Cisco.com ユーザ ID を作成したら、サービス要求のステータス オンラインを開始またはチェックするか、電話で TAC に問い合わせることができます。
  - 米国：1-800-553-2447 無料通話
  - 国際サポート番号
- TAC からテクニカル サポートを受ける方法の詳細については、『Technical Support Reference Guide』（PDF、1 MB）を参照してください。

Talos について

Talos Security Intelligence and Research Group（Talos）は、洗練されたシステムによってサポートされる優れた脅威研究者によって構成され、既知の脅威と新たな脅威の両方を検出および分析し、その脅威から保護するためのシスコ製品の脅威インテリジェンスを作成しています。Talos は、Snort.org、ClamAV、SenderBase.org、および SpamCop の公式ルール セットも保守しています。このチームの専門知識には、ソフトウェア開発、リバースエンジニアリング、脆弱性トリアージ、マルウェア調査、および情報収集が含まれています。