脅威の検出

次のトピックでは、脅威検出の統計情報およびスキャン脅威検出を設定する方法について説明します。

脅威の検出

ASA の脅威検出は、攻撃に対して最前線で防御する機能です。脅威検出は、パケット ドロップの統計を分析し、トラフィック パターンに基づいた「トップ」レポートを蓄積することで、レイヤ 3 と 4 にトラフィックのベースラインを作成します。一方、IPS または次世代 IPS サービスを提供するモジュールは、ASA が許可したトラフィックの攻撃ベクトルをレイヤ 7 まで識別して軽減させますが、すでに ASA がドロップしたトラフィックは認識できません。そのため、脅威検出と IPS を一緒に使用することで、より総合的な脅威に対する防御を可能にします。

脅威検出は次の要素から構成されています。

- さまざまな脅威を収集する複数レベルの統計情報

  脅威検出統計情報は、ASA に対する脅威の管理に役立ちます。たとえば、スキャン脅威検出をイネーブルにすると、統計情報を見ることで脅威を分析できます。次の 2 種類の脅威検出統計情報を設定できます。

  - 基本脅威検出統計情報：システムに対する攻撃アクティビティについての全体的な情報を含みます。基本脅威検出統計情報はデフォルトでイネーブルになっており、パフォーマンスに対する影響はありません。「基本脅威検出統計情報 （2 ページ）」を参照してください。

- 拡張脅威検出統計情報：オブジェクトレベルでアクティビティを追跡するので、ASA は個別のホスト、ポート、プロトコル、または ACL についてのアクティビティを報告できます。拡張脅威検出統計情報は、収集される統計情報によってはパフォーマンスに大きく影響するので、デフォルトでは ACL の統計情報だけがイネーブルになっています。「拡張脅威検出統計情報 （3 ページ）」を参照してください。

- ホストがスキャンを実行する時期を決定するスキャン脅威検出機能オプションとして、スキャン脅威であることが特定されたホストを排除できます。「スキャン脅威検出 （3 ページ）」を参照してください。
- IPv4 アドレスからの次のタイプの VPN 攻撃に対して保護するために使用できる VPN サービスの脅威検出。
  - リモートアクセス VPN への過剰な認証失敗の試行（ユーザー名/パスワードをスキャンするブルートフォース攻撃など）。
  - クライアント初期化攻撃。攻撃者は単一のホストからリモートアクセス VPN ヘッドエンドへの接続試行を繰り返し開始しますが、完了しません。
  - 無効な VPN サービス、つまり内部専用サービスへのアクセス試行。

  アクセスに失敗したとしても、これらの攻撃によってコンピューティングリソースを消費し、場合によってはサービス拒否（DoS）を引き起こす可能性があります。「VPN サービスの脅威検出の設定 （10 ページ）」を参照してください。

基本脅威検出統計情報

ASA は、基本脅威検出統計情報を使用して、次の理由でドロップしたパケットおよびセキュリティ イベントの割合をモニターします。

- ACL による拒否。
- 不正なパケット形式（invalid-ip-header や invalid-tcp-hdr-length など）。
- 接続制限の超過（システム全体のリソース制限とコンフィギュレーションで設定されている制限の両方）。
- DoS 攻撃の検出（無効な SPI、ステートフル ファイアウォール検査の不合格など）。
- 基本ファイアウォール検査に不合格。このオプションは、このリストのファイアウォールに関連したパケット ドロップをすべて含む複合レートです。インターフェイスの過負荷、アプリケーション インスペクションで不合格のパケット、スキャン攻撃の検出など、ファイアウォールに関連しないパケット ドロップは含まれていません。
- 疑わしい ICMP パケットの検出。
- アプリケーション インスペクションに不合格のパケット。
- インターフェイスの過負荷。

- スキャン攻撃の検出。このオプションでは、たとえば最初の TCP パケットが SYN パケットでない、またはスリーウェイ ハンドシェイクで TCP 接続に失敗したなどのスキャン攻撃をモニターします。フル スキャン脅威検出では、このスキャン攻撃レート情報を収集し、ホストを攻撃者として分類して自動的に排除することによって対処します。
- 不完全セッションの検出（TCP SYN 攻撃の検出や戻りデータなし UDP セッション攻撃の検出など）。

ASA は、脅威を検出するとただちにシステム ログ メッセージ（733100）を送信します。ASA は、一定間隔における平均イベント レートと短期バースト間隔におけるバーストイベント レートの 2 種類のレートを追跡します。バースト レート間隔は、平均レート間隔の 1/30 または 10 秒のうち、どちらか大きいほうです。ASA は、受信するイベントごとに平均レート制限とバースト レート制限をチェックします。両方のレートが超過している場合、ASA は、バースト期間におけるレート タイプごとに最大 1 つのメッセージの割合で 2 つの別々のシステム メッセージを送信します。

基本脅威検出は、ドロップまたは潜在的な脅威が存在した場合にだけパフォーマンスに影響します。このようなシナリオでも、パフォーマンスへの影響はわずかです。

拡張脅威検出統計情報

拡張脅威検出統計情報は、ホスト、ポート、プロトコル、ACL などの個別のオブジェクトについて、許可されたトラフィック レートとドロップされたトラフィック レートの両方を表示します。

注意 拡張統計情報をイネーブルにすると、イネーブルにする統計情報のタイプに応じて、ASA のパフォーマンスが影響を受けます。ホストの統計情報をイネーブルにすると、パフォーマンスに大きく影響します。トラフィックの負荷が高い場合は、このタイプの統計情報を一時的にイネーブルにすることを検討してください。ただし、ポート統計情報の影響はそれほど大きくありません。

スキャン脅威検出

典型的なスキャン攻撃では、あるホストがサブネット内の IP アドレスにアクセスできるかどうかを 1 つずつ試します（サブネット内の複数のホストすべてを順にスキャンするか、1 つのホストまたはサブネットの複数のポートすべてを順にスイープする）。スキャン脅威検出機能は、いつホストがスキャンを実行するかを判別します。トラフィック シグニチャに基づく IPS スキャン検出とは異なり、ASA の脅威検出スキャンでは、広範なデータベースが保持され、これに含まれるホスト統計情報をスキャン アクティビティに関する分析に使用できます。

ホスト データベースは、不審なアクティビティを追跡します。このようなアクティビティには、戻りアクティビティのない接続、閉じているサービス ポートへのアクセス、脆弱な TCP 動作（非ランダム IPID など）、およびその他の多くの動作が含まれます。

スキャン脅威レートを超過すると、ASA は syslog メッセージ（733101）を送信し、必要に応じて攻撃者を排除します。ASA は、一定間隔における平均イベント レートと短期バースト間隔におけるバースト イベント レートの 2 種類のレートを追跡します。バースト イベント レートは、平均レート間隔の 1/30 または 10 秒のうち、どちらか大きいほうです。スキャン攻撃の一部と見なされるイベントが検出されるたびに、ASA は平均レート制限とバースト レート制限をチェックします。ホストから送信されるトラフィックがどちらかのレートを超えると、そのホストは攻撃者と見なされます。ホストが受信したトラフィックがどちらかのレートを超えると、そのホストはターゲットと見なされます。

次の表に、スキャン脅威検出のデフォルトのレート制限を示します。

表 *1:* スキャンによる脅威の検出のデフォルトのレート制限

平均レート	バースト レート
直前の 600 秒間で 5 ドロップ/秒。	直近の 20 秒間で 10 ドロップ/秒。
直前の 3600 秒間で 5 ドロップ/秒。	直近の 120 秒間で 10 ドロップ/秒。

注意 スキャンによる脅威の検出機能は、ホストおよびサブネットベースのデータ構造を作成し情報を収集する間、ASA のパフォーマンスとメモリに大きく影響することがあります。

脅威検出のガイドライン

セキュリティ コンテキストのガイドライン

高度な脅威統計および VPN サービスを除き、脅威検出はシングルモードのみでサポートされます。マルチモードでは、TCP 代行受信の統計情報が唯一サポートされている統計情報です。

モニター対象トラフィックのタイプ

- 統計では、through-the-box トラフィックのみがモニターされます。to-the-box トラフィックはモニターされません。
- ACL によって拒否されたトラフィックは、スキャン脅威検出をトリガーしません。ASA から許可され、フローを作成したトラフィックだけがスキャン脅威検出の影響を受けます。
- VPN サービスの場合、IPv4 アドレスからの to-the-box トラフィックのみがモニターされます。

脅威検出のデフォルト

基本脅威検出統計情報は、デフォルトでイネーブルになっています。

次の表に、デフォルト設定を示します。これらのデフォルト設定すべてを表示するには、**show running-config all threat-detection** コマンドを 使用します。

高度な統計情報では、ACL の統計情報はデフォルトでイネーブルになっています。

VPN サービス脅威検出では、すべてのサービスがデフォルトで無効になっています。

表 *2:* 基本的な脅威の検出のデフォルト設定

パケット ドロップの理由	トリガー設定	
	平均レート	バースト レート
• DoS 攻撃の検出 • 不正なパケット形式 • 接続制限の超過 • 疑わしい ICMP パケットの検出	直前の 600 秒間で 100 ドロップ/秒。	直近の 20 秒間で 400 ドロップ/秒。
	直前の 3600 秒間で 80 ドロップ/秒。	直近の 120 秒間で 320 ドロップ/秒。
スキャン攻撃の検出	直前の 600 秒間で 5 ドロップ/秒。	直近の 20 秒間で 10 ドロップ/秒。
	直前の 3600 秒間で 4 ドロップ/秒。	直近の 120 秒間で 8 ドロップ/秒。
不完全セッションの検出（TCP SYN 攻撃の検出や戻りデータなし UDP セッション攻撃の検出など）（複合）	直前の 600 秒間で 100 ドロップ/秒。	直近の 20 秒間で 200 ドロップ/秒。
	直前の 3600 秒間で 80 ドロップ/秒。	直近の 120 秒間で 160 ドロップ/秒。
ACL による拒否	直前の 600 秒間で 400 ドロップ/秒。	直近の 20 秒間で 800 ドロップ/秒。
	直前の 3600 秒間で 320 ドロップ/秒。	直近の 120 秒間で 640 ドロップ/秒。
• 基本ファイアウォール検査に不合格 • アプリケーション インスペクションに不合格のパケット	直前の 600 秒間で 400 ドロップ/秒。	直近の 20 秒間で 1600 ドロップ/秒。
	直前の 3600 秒間で 320 ドロップ/秒。	直近の 120 秒間で 1280 ドロップ/秒。

パケット ドロップの理由	トリガー設定	
	平均レート	バースト レート
インターフェイスの過負荷	直前の 600 秒間で 2000 ドロップ/秒。	直近の 20 秒間で 8000 ドロップ/秒。
	直前の 3600 秒間で 1600 ドロップ/秒。	直近の 120 秒間で 6400 ドロップ/秒。

脅威検出の設定

基本脅威検出統計情報はデフォルトでイネーブルになっており、ユーザーが必要とする唯一の脅威検出サービスである場合があります。さらに脅威検出サービスを実行する場合は、次の手順を使用します。

手順

ステップ 1 基本脅威検出統計情報の設定 （6 ページ）。

基本脅威検出統計情報には、DoS 攻撃（サービス拒絶攻撃）などの攻撃に関連している可能性があるアクティビティが含まれます。

ステップ 2 拡張脅威検出統計情報の設定 （7 ページ）。

ステップ 3 スキャン脅威検出の設定 （9 ページ）。

ステップ 4 VPN サービスの脅威検出の設定 （10 ページ）。

基本脅威検出統計情報の設定

基本脅威検出統計情報は、デフォルトでイネーブルになっています。ディセーブルにすることも、一度ディセーブルにしたあと再度イネーブルにすることもできます。

手順

ステップ 1 基本脅威検出統計情報をイネーブルにします（ディセーブルになっている場合）。

threat-detection basic-threat

例：

```
hostname(config)# threat-detection basic-threat
```

基本脅威検出は、デフォルトでイネーブルになっています。これをディセーブルにするには **no threat-detection basic-threat** を使用します。

ステップ 2 （任意）各イベント タイプのデフォルト設定を変更します。

threat-detection rate {**acl-drop** | **bad-packet-drop** | **conn-limit-drop** | **dos-drop** | **fw-drop** | **icmp-drop** | **inspect-drop** | **interface-drop** | **scanning-threat** | **syn-attack**} **rate-interval** *rate_interval* **average-rate** *av_rate* **burst-rate** *burst_rate*

各イベント タイプの説明については、「基本脅威検出統計情報（ページ 8-1）」を参照してください。

scanning-threat キーワードを指定してこのコマンドを使用すると、スキャン脅威検出機能でもこのコマンドが使用されます。基本脅威検出を設定しない場合でも、**scanning-threat** キーワードを指定してこのコマンドを使用し、スキャン脅威検出でのレート制限を設定できます。

イベント タイプごとに、異なるレート間隔を 3 つまで設定できます。

例：

```
hostname(config)# threat-detection rate dos-drop rate-interval 600 average-rate 60
burst-rate 100
```

拡張脅威検出統計情報の設定

広範な統計情報を収集するように ASA を設定することができます。デフォルトでは、ACL の統計情報はイネーブルになっています。他の統計情報をイネーブルにするには、次の手順を実行します。

手順

ステップ 1 （任意）すべての統計情報をイネーブルにします。

threat-detection statistics

特定の統計情報だけをイネーブルにするには、（この手順で後に示す）各統計情報タイプに対してこのコマンドを入力し、オプションを指定しないでコマンドを入力しないようにします。**threat-detection statistics** を（何もオプションを指定しないで）入力した後、統計情報固有のオプション（たとえば **threat-detection statistics host number-of-rate 2**）を指定してコマンドを入力することで、特定の統計情報をカスタマイズできます。**threat-detection statistics** を（何もオプションを指定しないで）入力した後、特定の統計情報のコマンドを、統計情報固有のオプションを指定しないで入力した場合は、すでにイネーブルになっているので、そのコマンドによる効果は何もありません。

このコマンドの **no** 形式を入力すると、すべての **threat-detection statistics** コマンドが削除されます。これには、デフォルトでイネーブルになる **threat-detection statistics access-list** コマンドも含まれます。

例：

```
hostname(config)# threat-detection statistics
```

ステップ 2 （任意）ACL の統計情報をイネーブルにします（ディセーブルになっている場合）。

threat-detection statistics access-list

ACL の統計情報は、デフォルトでイネーブルになっています。ACL 統計情報は、show threat-detection top access-list コマンドを使用した場合にだけ表示されます。

例：

```
hostname(config)# threat-detection statistics access-list
```

ステップ 3 （任意）ホスト（host キーワード）、TCP および UDP ポート（port キーワード）、または非 TCP/UDP IP プロトコル（protocol キーワード）の統計情報を設定します。

threat-detection statistics {**host** | **port** | **protocol**} [**number-of-rate** {**1** | **2** | **3**}]

number-of-rate キーワードは、統計情報で保持するレート間隔の数を設定します。デフォルトのレート間隔の数は**1**です。メモリの使用量を低く抑えます。より多くのレート間隔を表示するには、値を **2** または **3** に設定します。たとえば、値を **3** に設定すると、直前の 1 時間、8 時間、および 24 時間のデータが表示されます。このキーワードを **1** に設定した場合（デフォルト）、最も短いレート間隔統計情報だけが保持されます。値を **2** に設定すると、短い方から 2 つの間隔が保持されます。

ホストがアクティブで、スキャン脅威ホストデータベース内に存在する限り、ホスト統計情報は累積されます。ホストは、非アクティブになってから 10 分後にデータベースから削除されます（統計情報もクリアされます）。

例：

```
hostname(config)# threat-detection statistics host number-of-rate 2
hostname(config)# threat-detection statistics port number-of-rate 2
hostname(config)# threat-detection statistics protocol number-of-rate 3
```

ステップ 4 （オプション）TCP 代行受信によって代行受信される攻撃の統計情報を設定します。

threat-detection statistics tcp-intercept [**rate-interval** *minutes*] [**burst-rate** *attacks_per_sec*] [**average-rate** *attacks_per_sec*]

それぞれの説明は次のとおりです。

- **rate-interval** は、履歴モニタリング ウィンドウのサイズを、1 ～ 1440 分の範囲で設定します。デフォルトは 30 分です。この間隔の間に、ASA は攻撃の数を 30 回サンプリングします。
- **burst-rate** は、syslog メッセージ生成のしきい値を 25 ～ 2147483647 の範囲内で設定します。デフォルトは 1 秒間に 400 です。バースト レートがこれを超えると、syslog メッセージ 733104 が生成されます。

- **average-rate** は、syslog メッセージ生成の平均レートしきい値を、25 ～ 2147483647 の範囲で設定します。デフォルトは 1 秒間に 200 回です。平均レートがこれを超えると、syslog メッセージ 733105 が生成されます。

TCP 代行受信を有効にするには、SYN フラッド DoS 攻撃からのサーバーの保護（TCP 代行受信） を参照してください。

（注）
このコマンドは、他の threat-detection コマンドとは異なり、マルチ コンテキスト モードで用意されています。

例：

```
hostname(config)# threat-detection statistics tcp-intercept rate-interval 60
burst-rate 800 average-rate 600
```

スキャン脅威検出の設定

攻撃者を識別し、必要に応じて排除するため、スキャン脅威検出を設定できます。

攻撃者に関するシステム ログ メッセージを送信するように ASA を設定できます。または、自動的にホストを排除できます。デフォルトでは、ホストが攻撃者として識別されると、システム ログ メッセージ 730101 が生成されます。ホストから大量のメッセージが送信されることが予想される場合は、アドレスを排除から除外するようにしてください。たとえば、Pluggable Interface Module（PIM）マルチキャストを有効にした場合、PIM ルータまたは PIM メッセージがドロップされます。

手順

ステップ 1 スキャン脅威検出をイネーブルにします。

threat-detection scanning-threat [**shun** [**except** {**ip-address** *ip_address mask* | **object-group** *network_object_group_id*}]]

デフォルトでは、ホストが攻撃者であると識別されると、システム ログ メッセージ 733101 が生成されます。このコマンドを複数回入力し、複数の IP アドレスまたはネットワーク オブジェクト グループを特定して遮断対象から除外できます。

例：

```
hostname(config)# threat-detection scanning-threat shun except
ip-address 10.1.1.0 255.255.255.0
```

ステップ 2 （任意）攻撃元のホストを遮断する期間を設定します。

threat-detection scanning-threat shun duration *seconds*

例：

```
hostname(config)# threat-detection scanning-threat shun duration 2000
```

ステップ 3 （任意）ASA がホストを攻撃者またはターゲットとして識別する場合のデフォルト イベント制限を変更します。

threat-detection rate scanning-threat rate-interval *rate_interval* **average-rate** *av_rate* **burst-rate** *burst_rate*

このコマンドが基本脅威検出コンフィギュレーションの一部としてすでに設定されている場合、それらの設定はスキャン脅威検出機能でも共有され、基本脅威検出とスキャン脅威検出で個別にレートを設定することはできません。このコマンドを使用してレートを設定しない場合は、基本脅威検出機能とスキャン脅威検出機能の両方でデフォルト値が使用されます。個別にコマンドを入力することで、異なるレート間隔を 3 つまで設定できます。

例：

```
hostname(config)# threat-detection rate scanning-threat rate-interval 1200
average-rate 10 burst-rate 20

hostname(config)# threat-detection rate scanning-threat rate-interval 2400
average-rate 10 burst-rate 20
```

VPN サービスの脅威検出の設定

VPN サービスの脅威検出を有効にして、IPv4 アドレスからのサービス妨害（DoS）攻撃を防ぐことができます。次のタイプの攻撃に使用できる個別のサービスがあります。

- リモートアクセス VPN ログイン認証攻撃者が、パスワードスプレー攻撃でログイン試行を繰り返し開始することで認証試行に使用されるリソースを消費し、実数のユーザーが VPN にログインできなくなる可能性があります。
- クライアント初期化攻撃。攻撃者は単一のホストからリモートアクセス VPN ヘッドエンドへの接続試行を繰り返し開始しますが、完了しません。パスワードスプレー攻撃と同様に、この攻撃はリソースを消費し、有効なユーザーが VPN に接続できなくなる可能性があります。
- 無効な VPN サービス、つまり内部使用専用サービスに接続しようとします。この接続を試みる IP アドレスは、ただちに排除されます。

これらのサービスを有効にすると、システムはしきい値を超えたホストを自動的に排除して、それ以上の試行されないようにします。アドレスに対して **no shun** コマンドを使用して、排除を手動で削除できます。

サービスのカウンタを手動で 0 にリセットするには、**clear threat-detection service** コマンドを使用します。

始める前に

適切なホールドダウン値としきい値を決定する場合は、環境での NAT の使用を検討してください。PAT を使用して、同じ IP アドレスから多数の要求を送信できるようにする場合は、認証失敗とクライアント開始サービスの値を大きくして、有効なユーザーが接続を完了するのに十分な時間を確保できるようにする必要があります。たとえば、多くのお客様が非常に短い時間内に接続を試みるホテルなどです。

手順

ステップ 1 リモートアクセス VPN 認証失敗の脅威検出を有効にします。

threat-detection service remote-access-authentication hold-down *minutes* **threshold** *count*

それぞれの説明は次のとおりです。

- **hold-down** *minutes* は、最後の失敗からのホールドダウン期間を定義します。攻撃者の IPv4 アドレスの排除をトリガーするには、前回の失敗とのホールドダウン期間内に連続失敗のしきい値カウントに達する必要があります。たとえば、ホールドダウン期間が 10 分でしきい値が 20 で、単一の IPv4 アドレスからの連続した認証失敗が 20 回あり、2 つの連続した失敗間のタイムスパンが 10 分を超えない場合、送信元 IPv4 アドレスは排除されます。1 ～ 1440 分の時間を指定できます。
- **threshold** *count* は、排除をトリガーするためにホールドダウン期間内に発生する必要がある試行の失敗数を定義します。1 ～ 100 のしきい値を指定できます。

サービスを無効化するには、次のコマンドを使用します。

no threat-detection service remote-access-authentication

例：

次の例では、20 分以内に 10 回の失敗のメトリックを設定します。

```
ciscoasa(config)# threat-detection service remote-access-authentication
hold-down 10 threshold 20
```

ステップ 2 リモートアクセス VPN クライアント開始の脅威検出を有効にします。

threat-detection service remote-access-client-initiations hold-down *minutes* **threshold** *count*

それぞれの説明は次のとおりです。

- **hold-down** *minutes* は、最後の開始からのホールドダウン期間を定義します。クライアントの IPv4 アドレスの排除をトリガーするには、前回の開始とのホールドダウン期間内に、連続する開始のしきい値カウントに達する必要があります。たとえば、ホールドダウン期間が 10 分でしきい値が 20 で、単一の IPv4 アドレスからの連続した開始が 20 回あり、2 つの連続した開始間のタイムスパンが 10 分を超えない場合、送信元 IPv4 アドレスは排除されます。1 ～ 1440 分の時間を指定できます。

- **threshold** *count* は、排除をトリガーするためにホールドダウン期間内に発生する必要がある開始の数を定義します。5 ～ 100 のしきい値を指定できます。

サービスを無効化するには、次のコマンドを使用します。

no threat-detection service remote-access-client-initiations

例：

次の例では、20 分以内に 10 回の開始のメトリックを設定します。

```
ciscoasa(config)# threat-detection service remote-access-client-initiations
hold-down 10 threshold 20
```

ステップ 3 無効な VPN サービスへの接続試行の脅威検出を有効にします。

threat-detection service invalid-vpn-access

サービスを無効化するには、次のコマンドを使用します。

no threat-detection service invalid-vpn-access

例：

次の例では、Invalid VPN Access サービスを有効にしています。

```
ciscoasa(config)# threat-detection service invalid-vpn-access
```

脅威検出のモニタリング

次のトピックでは、脅威検出のモニタリングとトラフィック統計情報を表示する方法を説明します。

基本脅威検出統計情報のモニタリング

次のコマンドを使用して、基本脅威検出統計情報を表示します。

show threat-detection rate [**min-display-rate** *min_display_rate*] [**acl-drop** | **bad-packet-drop** | **conn-limit-drop** | **dos-drop** | **fw-drop** | **icmp-drop** | **inspect-drop** | **interface-drop** | **scanning-threat** | **syn-attack**]

min-display-rate *min_display_rate* 引数により、毎秒あたりの最小表示レートを超過する統計情報に表示内容を限定します。*min_display_rate* は、0 ～ 2147483647 の値に設定できます。

他の引数を使用すると、特定のカテゴリに表示を制限できます。各イベントタイプの説明については、基本脅威検出統計情報 （2 ページ）を参照してください。

出力には、直前の 10 分と直前の 1 時間の固定された 2 期間における平均レート（イベント数/秒）が表示されます。また、最後に終了したバースト間隔（平均レート間隔の 1/30 または 10

秒のうち、どちらか大きいほう）における現在のバースト レート（イベント数/秒）、レートが超過した回数（トリガーした回数）、およびその期間の合計イベント数も表示されます。

ASA は、各バースト期間の終わりにカウント数を保存します。合計で 30 回分のバースト間隔を保存します。現在進行中の未完了バースト間隔は、平均レートに含まれません。たとえば、平均レート間隔が 20 分の場合、バースト間隔は 20 秒になります。最後のバースト間隔が 3:00:00 ～ 3:00:20 で、3:00:25 に **show** コマンドを使用すると、最後の 5 秒間は出力に含まれません。

このルールにおける唯一の例外は、合計イベント数を計算するときに、未完了バースト間隔のイベント数が最も古いバースト間隔（1/30 個目）のイベント数よりすでに多くなっている場合です。この場合、ASA は、最後の 29 回の完了間隔で合計イベント数を計算し、その時点での未完了バースト間隔のイベント数を加算します。この例外により、イベント数の大幅な増加をリアルタイムでモニタできます。

clear threat-detection rate コマンドを使用して統計情報を消去できます。

次に、**show threat-detection rate** コマンドの出力例を示します。

```
hostname# show threat-detection rate

                        Average(eps)    Current(eps) Trigger         Total events
  10-min ACL  drop:                0              0       0                   16
  1-hour ACL  drop:                0              0       0                  112
  1-hour SYN attck:                5              0       2                21438
  10-min  Scanning:                0              0      29                  193
  1-hour  Scanning:              106              0      10               384776
  1-hour Bad  pkts:               76              0       2               274690
  10-min  Firewall:                0              0       3                   22
  1-hour  Firewall:               76              0       2               274844
  10-min DoS attck:                0              0       0                    6
  1-hour DoS attck:                0              0       0                   42
  10-min Interface:                0              0       0                  204
  1-hour Interface:               88              0       0               318225
```

拡張脅威検出統計情報のモニタリング

拡張脅威検出統計情報をモニターするには、次の表に示すコマンドを使用します。ディスプレイの出力には、次の情報が表示されます。

- 固定された期間の平均レート（イベント数/秒）
- 終了した最後のバースト間隔における現在のバースト レート（イベント数/秒）。バースト間隔は、平均レート間隔の 1/30 と 10 秒のうち、どちらか大きいほうの間隔
- レートを超過した回数（ドロップされたトラフィックの統計情報の場合に限る）
- 固定された期間におけるイベントの合計数

ASA は、各バースト期間の終わりにカウント数を保存します。合計で 30 回分のバースト間隔を保存します。現在進行中の未完了バースト間隔は、平均レートに含まれません。たとえば、平均レート間隔が 20 分の場合、バースト間隔は 20 秒になります。最後のバースト間隔が

3:00:00 ～ 3:00:20 で、3:00:25 に **show** コマンドを使用すると、最後の 5 秒間は出力に含まれません。

このルールにおける唯一の例外は、合計イベント数を計算するときに、未完了バースト間隔のイベント数が最も古いバースト間隔（1/30 個目）のイベント数よりすでに多くなっている場合です。この場合、ASA は、最後の 29 回の完了間隔で合計イベント数を計算し、その時点での未完了バースト間隔のイベント数を加算します。この例外により、イベント数の大幅な増加をリアルタイムでモニタできます。

コマンド	目的
show threat-detection statistics [**min-display-rate** *min_display_rate*] **top** [[**access-list** | **host** | **port-protocol**] [**rate-1** | **rate-2** | **rate-3**] | **tcp-intercept** [**all**] **detail**]]	上位10件の統計情報を表示します。オプションを入力しない場合は、カテゴリ全体での上位 10 件の統計情報が表示されます。 **min-display-rate** *min_display_rate* 引数により、毎秒あたりの最小表示レートを超過する統計情報に表示内容を限定します。*min_display_rate* は、0 ～ 2147483647 の値に設定できます。 次の行は、オプション キーワードを示します。
show threat-detection statistics [**min-display-rate** *min_display_rate*] **top access-list** [**rate-1** | **rate-2** | **rate-3**]	許可 ACE と拒否 ACE の両方を含め、パケットに一致する上位 10 件の ACE を表示するには、**access-list** キーワードを使用します。この表示では許可されたトラフィックと拒否されたトラフィックが区別されません。**threat-detection basic-threat** コマンドを使用して基本脅威検出をイネーブルにする場合は、**show threat-detection rate acl-drop** コマンドを使用して、ACL による拒否を追跡できます。 **rate-1** キーワードを指定すると、表示できる最小固定レート間隔の統計情報が表示され、**rate-2** を指定すると次に大きなレート間隔の統計情報が表示されます。3 つの間隔が定義されている場合には、**rate-3** を指定すると最大レート間隔の統計情報が表示されます。たとえば、ディスプレイに直前の 1 時間、8 時間、および 24 時間の統計情報が表示されるとします。**rate-1** キーワードを設定すると、ASA は 1 時間の統計情報だけを表示します。
show threat-detection statistics [**min-display-rate** *min_display_rate*] **top host** [**rate-1** | **rate-2** | **rate-3**]	ホスト統計情報だけを表示するには、**host** キーワードを使用します。 **注**：脅威検出アルゴリズムに起因して、フェールオーバー リンクとステート リンクの組み合わせとして使用されるインターフェイスは上位 10 個のホストに表示されることがあります。これは予期された動作であり、表示される IP アドレスは無視できます。

コマンド	目的
show threat-detection statistics [**min-display-rate** *min_display_rate*] **top port-protocol** [**rate-1** | **rate-2** | **rate-3**]	ポートおよびプロトコルの統計情報を表示するには、**port-protocol** キーワードを使用します。**port-protocol** キーワードを指定すると、ポートとプロトコルの両方の統計情報が表示され（表示するには、両方がイネーブルに設定されている必要があります）、TCP/UDP ポートと IP プロトコル タイプを組み合わせた統計情報が表示されます。TCP（プロトコル 6）と UDP（プロトコル 17）は、IP プロトコルの表示には含まれていませんが、TCP ポートと UDP ポートはポートの表示に含まれています。これらのタイプ（ポートまたはプロトコル）の 1 つの統計情報だけをイネーブルにすると、イネーブルにされた統計情報だけが表示されます。
show threat-detection statistics [**min-display-rate** *min_display_rate*] **top tcp-intercept** [**all**] **detail**]]	TCP 代行受信の統計情報だけを表示するには、**tcp-intercept** キーワードを使用します。表示には、攻撃を受けて保護された上位 10 サーバーが含まれます。**all** キーワードは、トレースされているすべてのサーバーの履歴データを表示します。**detail** キーワードは、履歴サンプリング データを表示します。ASA はレート間隔の間に攻撃の数を 30 回サンプリングするので、デフォルトの 30 分間隔では、60 秒ごとに統計情報が収集されます。
show threat-detection statistics [**min-display-rate** *min_display_rate*] **host** [*ip_address* [*mask*]]	すべてのホスト、特定のホスト、または特定のサブネットの統計情報を表示します。
show threat-detection statistics [**min-display-rate** *min_display_rate*] **port** [*start_port*[-*end_port*]]	すべてのポート、特定のポート、または特定のポート範囲の統計情報を表示します。
show threat-detection statistics [**min-display-rate** *min_display_rate*] **protocol** [*protocol_number* | *protocol*]	すべての IP プロトコルまたは特定のプロトコルの統計情報を表示します。 *protocol_number* 引数は、0 ～ 255 の整数です。プロトコルの引数には、**ah**、**eigrp**、**esp**、**gre**、**icmp**、**icmp6**、**igmp**、**igrp**、**ip**、**ipinip**、**ipsec**、**nos**、**ospf**、**pcp**、**pim**、**pptp**、**snp**、**tcp**、**udp** のいずれかを指定できます。

ホストの脅威検出統計情報の評価

次に、**show threat-detection statistics host** コマンドの出力例を示します。

```
hostname# show threat-detection statistics host

                        Average(eps)    Current(eps) Trigger         Total events
Host:10.0.0.1: tot-ses:289235 act-ses:22571 fw-drop:0 insp-drop:0 null-ses:21438 bad-acc:0

  1-hour Sent byte:              2938              0       0             10580308
  8-hour Sent byte:               367              0       0             10580308
 24-hour Sent byte:               122              0       0             10580308
  1-hour Sent pkts:                28              0       0               104043
```

```
  8-hour Sent pkts:                  3               0       0                104043
 24-hour Sent pkts:                  1               0       0                104043
  20-min Sent drop:                  9               0       1                 10851
  1-hour Sent drop:                  3               0       1                 10851
  1-hour Recv byte:               2697               0       0               9712670
  8-hour Recv byte:                337               0       0               9712670
 24-hour Recv byte:                112               0       0               9712670
  1-hour Recv pkts:                 29               0       0                104846
  8-hour Recv pkts:                  3               0       0                104846
 24-hour Recv pkts:                  1               0       0                104846
  20-min Recv drop:                 42               0       3                 50567
  1-hour Recv drop:                 14               0       1                 50567
Host:10.0.0.0: tot-ses:1 act-ses:0 fw-drop:0 insp-drop:0 null-ses:0 bad-acc:0
  1-hour Sent byte:                  0               0       0                   614
  8-hour Sent byte:                  0               0       0                   614
 24-hour Sent byte:                  0               0       0                   614
  1-hour Sent pkts:                  0               0       0                     6
  8-hour Sent pkts:                  0               0       0                     6
 24-hour Sent pkts:                  0               0       0                     6
  20-min Sent drop:                  0               0       0                     4
  1-hour Sent drop:                  0               0       0                     4
  1-hour Recv byte:                  0               0       0                   706
  8-hour Recv byte:                  0               0       0                   706
 24-hour Recv byte:                  0               0       0                   706
  1-hour Recv pkts:                  0               0       0                     7
```

次の表は出力について示しています。

表 *3 : show threat-detection statistics host*

フィールド	説明
Host	ホストの IP アドレス。
tot-ses	ホストがデータベースに追加されて以降の、このホストでの合計セッション数。
act-ses	ホストが現在関係しているアクティブなセッションの合計数。
fw-drop	ファイアウォール ドロップの数。ファイアウォール ドロップは、基本脅威検出で追跡されたすべてのファイアウォール関連のパケット ドロップを含む組み合わせレートです。これには、ACL での拒否、不良パケット、接続制限の超過、DoS 攻撃パケット、疑わしい ICMP パケット、TCP SYN 攻撃パケット、および戻りデータなし UDP 攻撃パケットなどが含まれます。インターフェイスの過負荷、アプリケーション インスペクションで不合格のパケット、スキャン攻撃の検出など、ファイアウォールに関連しないパケット ドロップは含まれていません。
insp-drop	アプリケーション インスペクションに不合格になったためにドロップされたパケット数。
null-ses	ヌル セッションの数。ヌル セッションは、3 秒間のタイムアウト内に完了しなかった TCP SYN セッション、およびセッション開始の 3 秒後までにサーバーからデータが送信されなかった UDP セッションです。

フィールド	説明
bad-acc	閉じられた状態のホストのポートに対する不正なアクセスの試行回数。ポートがヌルセッションと判断されると（null-sesフィールドの説明を参照）、ホストのポートの状態はHOST_PORT_CLOSEに設定されます。そのホストのポートにアクセスしようとするクライアントはすべて、タイムアウトを待たずにすぐ不正アクセスとして分類されます。
Average(eps)	各間隔における平均レート（イベント数/秒）。 ASAは、各バースト期間の終わりにカウント数を保存します。合計で30回分のバースト間隔を保存します。現在進行中の未完了バースト間隔は、平均レートに含まれません。たとえば、平均レート間隔が20分の場合、バースト間隔は20秒になります。最後のバースト間隔が3:00:00～3:00:20で、3:00:25に**show**コマンドを使用すると、最後の5秒間は出力に含まれません。 このルールにおける唯一の例外は、合計イベント数を計算するときに、未完了バースト間隔のイベント数が最も古いバースト間隔（1/30個目）のイベント数よりすでに多くなっている場合です。この場合、ASAは、最後の29回の完了間隔で合計イベント数を計算し、その時点での未完了バースト間隔のイベント数を加算します。この例外により、イベント数の大幅な増加をリアルタイムでモニタできます。
Current(eps)	終了した最後のバースト間隔における現在のバースト レート（イベント数/秒）。バースト間隔は、平均レート間隔の1/30と10秒のうち、どちらか大きいほうの間隔。Average(eps)の説明で示された例の場合、現在レートは3:19:30～3:20:00のレートです。
Trigger	ドロップされたパケット レートの制限値を超過した回数。送受信バイトとパケットの行で指定された有効なトラフィックの場合、この値は常に0です。これは、有効なトラフィックをトリガーするレート制限がないためです。
Total events	各レート間隔におけるイベントの合計数。現在進行中の未完了バースト間隔は、合計イベント数に含まれません。このルールにおける唯一の例外は、合計イベント数を計算するときに、未完了バースト間隔のイベント数が最も古いバースト間隔（1/30個目）のイベント数よりすでに多くなっている場合です。この場合、ASAは、最後の29回の完了間隔で合計イベント数を計算し、その時点での未完了バースト間隔のイベント数を加算します。この例外により、イベント数の大幅な増加をリアルタイムでモニタできます。

フィールド	説明
20-min、1-hour、8-hour、および24-hour	これらの固定レート間隔の統計情報。各インターバルごとに、以下を示します。 • [Sent byte]：ホストから正常に送信されたバイト数。 • [Sent pkts]：ホストから正常に送信されたパケット数。 • [Sent drop]：ホストから送信された、スキャン攻撃の一部であったためにドロップされたパケット数。 • [Recv byte]：ホストが受信した正常なバイト数。 • [Recv pkts]：ホストが受信した正常なパケット数。 • [Recv drop]：ホストが受信したパケットの中で、スキャン攻撃の一部であったためにドロップされたパケット数。

スキャン脅威検出の排除されたホスト、攻撃者、ターゲットのモニタリング

スキャン脅威検出の排除されたホスト、攻撃者、ターゲットをモニターおよび管理するには、次のコマンドを使用します。これらのコマンドは、スキャン脅威検出専用であり、他のサービスには適用されません。

- **show threat-detection shun**

  現在遮断されているホストを表示します。次に例を示します。

```
hostname# show threat-detection shun

Shunned Host List:
(outside) src-ip=10.0.0.13 255.255.255.255
(inside) src-ip=10.0.0.13 255.255.255.255
```

- **clear threat-detection shun** [*ip_address* [*mask*]]

  ホストを回避対象から解除します。IPアドレスを指定しない場合は、すべてのホストが遮断リストからクリアされます。

  たとえば、10.1.1.6 のホストを解除するには、次のコマンドを入力します。

```
hostname# clear threat-detection shun 10.1.1.6
```

- **show threat-detection scanning-threat** [**attacker** | **target**]

  ASAが攻撃者（遮断リストのホストを含む）と判断したホスト、および攻撃のターゲットにされたホストを表示します。オプションを入力しない場合は、攻撃者とターゲットの両方のホストが表示されます。例：

```
hostname# show threat-detection scanning-threat
Latest Target Host & Subnet List:
    192.168.1.0 (l2l)
    192.168.1.249 (l2l)
Latest Attacker Host & Subnet List:
    192.168.10.234 (outside)
    192.168.10.0 (outside)
    192.168.10.2 (outside)
    192.168.10.3 (outside)
    192.168.10.4 (outside)
    192.168.10.5 (outside)
    192.168.10.6 (outside)
    192.168.10.7 (outside)
    192.168.10.8 (outside)
    192.168.10.9 (outside)
```

VPN サービスの脅威検出のモニタリング

次のトピックで説明するように、syslog および show コマンドを使用して、VPN サービスの脅威検出をモニターできます。

VPN サービスの脅威検出の Syslog モニタリング

これらのサービスに関連する次の syslog メッセージが表示される場合があります。

- %ASA-6-733200: Threat-detection Info: *message*

  このメッセージは、脅威検出に関する一般的な情報イベントを報告します。

- %ASA-4-733201: Threat-detection: Service[*service*] Peer[*peer*]: threshold of *threshold-value* was exceeded. Adding shun to interface *interface*.*Additional_message*

  このメッセージは、指定されたサービスの不審なアクティビティが原因で、脅威検出サービスが IP アドレスを排除したことを示しています。メッセージには追加情報が含まれている場合があります。たとえば、RA VPN クライアント開始試行の場合、追加情報は「SSL（または IKEv2）：RA 過剰なクライアント開始要求（SSL (or IKEv2): RA excessive client initiation requests.）」のようになります。

  show shun コマンドを使用して、排除されたホストのリストを表示できます。IP アドレスが攻撃者ではないことがわかっている場合は、**no shun** コマンドを使用して排除を削除できます。

VPN サービスの脅威検出の show コマンドによるモニタリング

次のコマンドを使用して、VPN サービスの脅威検出の統計情報を表示します。

show threat-detection service [*service*] [**entries** | **details**]

必要に応じて、特定のサービス（**remote-access-authentication**、**remote-access-client-initiations**、または **invalid-vpn-access**）にビューを制限できます。次のパラメータを追加することで、ビューをさらに制限できます。

- **entries**：追跡対象のエントリのみを表示します。たとえば、認証試行に失敗した IP アドレスです。
- **details**：サービスの詳細とサービスエントリの両方を表示します。

選択したオプションに基づいて、ディスプレイ出力には次の情報が表示されます。

- サービスの名前
- サービスの状態：有効または無効
- サービスホールドダウン設定
- サービスしきい値設定
- サービスアクション統計情報
  - [失敗（Failed）]：報告された発生の処理中に障害が発生しました。
  - [ブロッキング（Blocking）]：報告された発生はホールドダウン期間内であり、しきい値に達したか超過しました。その結果、サービスは、不正なピアをブロックするための排除を自動的にインストールしました。
  - [記録（Recording）]：報告された発生がホールドダウン期間外であるか、しきい値に達したか超過しました。その結果、サービスは発生を記録します。
  - [サポート対象外（Unsupported）]：報告された発生は、現在自動排除をサポートしていません。
  - [無効（Disabled）]：発生が報告されました。ただし、サービスは無効になっています。

例

次の例では、すべてのサービスが有効になっており、リモートアクセス認証サービスについて潜在的な攻撃者が追跡されています。

```
ciscoasa# show threat-detection service
Service: invalid-vpn-access
    State     : Enabled
    Hold-down : 1 minutes
    Threshold : 1
    Stats:
        failed      :          0
        blocking    :          0
        recording   :          0
        unsupported :          0
        disabled    :          0
    Total entries: 0
Service: remote-access-authentication
    State     : Enabled
    Hold-down : 10 minutes
    Threshold : 20
    Stats:
        failed      :          0
```

```
        blocking    :          1
        recording   :          4
        unsupported :          0
        disabled    :          0
    Total entries: 3
Name: remote-access-client-initiations
    State     : Enabled
    Hold-down : 10 minutes
    Threshold : 20
    Stats:
        failed      :          0
        blocking    :          0
        recording   :          0
        unsupported :          0
        disabled    :          0
    Total entries: 0
```

次に、**show threat-detection service entries** コマンドの例を示します。

```
ciscoasa# show threat-detection service remote-access-authentication entries
Service: remote-access-authentication
    Total entries: 2

Idx Source              Interface            Count          Age         Hold-down
--- ------------------- -------------------- -------------- ----------- ---------
  1 192.168.100.101/ 32              outside              1         721          0
  2 192.168.100.102/ 32              outside              2         486        114
Total number of IPv4 entries: 2

NOTE: Age is in seconds since last reported. Hold-down is in seconds remaining.
```

次に、**show threat-detection service details** コマンドの例を示します。

```
ciscoasa# show threat-detection service remote-access-authentication details
Service: remote-access-authentication
    State     : Enabled
    Hold-down : 10 minutes
    Threshold : 20
    Stats:
        failed      :          0
        blocking    :          1
        recording   :          4
        unsupported :          0
        disabled    :          0
     Total entries: 2

Idx Source              Interface            Count          Age         Hold-down
--- ------------------- -------------------- -------------- ----------- ---------
  1 192.168.100.101/ 32              outside              1         721          0
  2 192.168.100.102/ 32              outside              2         486        114
Total number of IPv4 entries: 2

NOTE: Age is in seconds since last reported. Hold-down is in seconds remaining.
```

VPN サービス違反に適用された排除の削除

次のコマンドを使用して、VPN サービスに適用された排除をモニターし、排除を削除できます。VPN サービスの脅威検出によって適用される排除は、**show threat-detection shun** コマンドには表示されないことに注意してください。このコマンドは、スキャン脅威検出にのみ適用されます。

- **show shun** [*ip_address*]

  VPN サービスの脅威検出によって自動的に排除されたホスト、または **shun** コマンドを使用して手動で排除されたホストを含む、排除されたホストを表示します。必要に応じて、指定した IP アドレスにビューを制限できます。

- **no shun** *ip_address* [**interface** *if_name*]

  指定した IP アドレスからのみ排除を削除します。アドレスが複数のインターフェイスで排除され、一部のインターフェイスで排除をそのままにしておく場合は、オプションで排除のインターフェイス名を指定できます。

- **clear shun**

  すべての IP アドレスから排除を削除します。

脅威検出の例

次の例では、基本脅威検出統計情報を設定し、DoS 攻撃レートの設定を変更しています。すべての拡張脅威検出統計情報はイネーブルであり、ホスト統計情報のレート間隔数は 2 に減らされています。TCP 代行受信のレート間隔もカスタマイズされています。スキャン脅威検出はイネーブルで、10.1.1.0/24 を除くすべてのアドレスを自動遮断します。スキャン脅威レート間隔はカスタマイズされています。

```
threat-detection basic-threat
threat-detection rate dos-drop rate-interval 600 average-rate 60 burst-rate 100
threat-detection statistics
threat-detection statistics host number-of-rate 2
threat-detection statistics tcp-intercept rate-interval 60 burst-rate 800 average-rate
600
threat-detection scanning-threat shun except ip-address 10.1.1.0 255.255.255.0
threat-detection rate scanning-threat rate-interval 1200 average-rate 10 burst-rate 20
threat-detection rate scanning-threat rate-interval 2400 average-rate 10 burst-rate 20
```

脅威検出の履歴

機能名	プラットフォーム リリース	説明
基本および拡張脅威検出統計情報、スキャン脅威検出	8.0(2)	基本および拡張脅威検出統計情報、スキャン脅威検出が導入されました。 次のコマンドが導入されました：**threat-detection basic-threat**、**threat-detection rate**、**show threat-detection rate**、**clear threat-detection rate**、**hreat-detection statistics**、**show threat-detection statistics**、**threat-detection scanning-threat**、**threat-detection rate scanning-threat**、**show threat-detection scanning-threat**、**show threat-detection shun**、**clear threat-detection shun**。
排除期間	8.0(4)/8.1(2)	排除期間を設定できるようになりました。 **threat-detection scanning-threat shun duration** コマンドが導入されました。
TCP 代行受信の統計情報	8.0(4)/8.1(2)	TCP 代行受信の統計情報が導入されました。 **threat-detection statistics tcp-intercept**、**show threat-detection statistics top tcp-intercept**、**clear threat-detection statistics** コマンドが変更または導入されました。
ホスト統計情報レート間隔のカスタマイズ	8.1(2)	統計情報が収集されるレート間隔の数をカスタマイズできるようになりました。デフォルトのレート数は、3 から 1 に変更されました。 **threat-detection statistics host number-of-rates** コマンドが変更されました。
バースト レート間隔が平均レートの 1/30 に変更されました。	8.2(1)	以前のリリースでは、平均レートの 1/60 でした。メモリを最大限に使用するため、サンプリング間隔が平均レートの間に 30 回に減らされました。
ポートおよびプロトコル統計情報レート間隔のカスタマイズ	8.3(1)	統計情報が収集されるレート間隔の数をカスタマイズできるようになりました。デフォルトのレート数は、3 から 1 に変更されました。 **threat-detection statistics port number-of-rates**、**threat-detection statistics protocol number-of-rates** コマンドが変更されました。

機能名	プラットフォーム リリース	説明
メモリ使用率の向上	8.3(1)	脅威検出のメモリ使用率が向上しました。 **show threat-detection memory** コマンドが導入されました。
VPN サービスの脅威検出	9.20(3)	VPN サービスの脅威検出を設定して、IPv4 アドレスからの次のタイプの VPN 攻撃に対して保護できます。 • リモートアクセス VPN への過剰な認証失敗の試行（ユーザー名/パスワードをスキャンするブルートフォース攻撃など）。 • クライアント初期化攻撃。攻撃者は単一のホストからリモートアクセス VPN ヘッドエンドへの接続試行を繰り返し開始しますが、完了しません。 • 無効な VPN サービス、つまり内部専用サービスへのアクセス試行。 アクセスに失敗したとしても、これらの攻撃によってコンピューティングリソースを消費し、場合によってはサービス拒否（DoS）を引き起こす可能性があります。 **clear threat-detection service**、**show threat-detection service**、**shun**、**threat-detection service** の各コマンドが導入または変更されました。

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。