CHAPTER 62

脅威検出の設定

この章では、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。次の項目を取り上げます。

脅威検出に関する情報

脅威検出機能は、次の要素で構成されます。

- 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。
  - 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、またはアクセス リスト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、デフォルトではアクセス リストの統計情報だけがイネーブルになっています。

- 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遮断できます。

脅威検出のライセンス要件

次の表に、この機能のライセンス要件を示します。

モデル	ライセンス要件
すべてのモデル	基本ライセンス

基本脅威検出統計情報の設定

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。

この項は、次の内容で構成されています。

基本脅威検出統計情報に関する情報

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します。

- アクセス リストによる拒否
- 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の不合格（このオプションは、ここに列挙されているファイアウォール関連のパケット ドロップすべてを含む総合レートです。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
- 検出されたスキャン攻撃（このオプションでは、スキャン攻撃をモニタします。たとえば、最初の TCP パケットが SYN パケットでないことや、TCP 接続で 3 ウェイ ハンドシェイクに失敗することなどです。フル スキャン脅威検出（「スキャン脅威検出の設定」（P.62-15）を参照）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遮断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、ドロップや潜在的な脅威があった場合に限りパフォーマンスに影響を与えます。この状況でも、パフォーマンスへの影響は大きくありません。

ガイドラインと制限事項

この項では、この機能のガイドラインと制限事項について説明します。

セキュリティ コンテキストのガイドライン

シングル モードでだけサポートされています。マルチ モードはサポートされていません。

ファイアウォール モードのガイドライン

ルーテッド ファイアウォール モードとトランスペアレント ファイアウォール モードでサポートされています。

モニタ対象トラフィックのタイプ

through-the-box トラフィックだけがモニタされます。to-the-box トラフィックは、脅威検出に含まれません。

デフォルト設定

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。

表 62-1 に、デフォルト設定を示します。これらのデフォルト設定はすべて、**show running-config all threat-detection** コマンドを使用して表示できます。

表 62-1　基本脅威検出のデフォルト設定

	トリガー設定	
パケット ドロップの理由	**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。

表 62-1　基本脅威検出のデフォルト設定 （続き）

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
アクセス リストによる拒否	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	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。
• 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 3600 秒間で 320 ドロップ/秒。	直近の 120 秒間で 1280 ドロップ/秒。
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。

基本脅威検出統計情報の設定

この項では、イネーブルまたはディセーブルにする方法や、デフォルトの制限を変更する方法など、基本脅威検出統計情報を設定する方法について説明します。

手順の詳細

	コマンド	目的
ステップ 1	**threat-detection basic-threat** **例：** `hostname(config)# threat-detection basic-threat`	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）。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。
ステップ 2	**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* **例：** `hostname(config)# threat-detection rate dos-drop rate-interval 600 average-rate 60 burst-rate 100`	（任意）各イベント タイプのデフォルト設定を変更します。 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に関する情報」（P.62-2）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（「スキャン脅威検出の設定」の項を参照）。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。

基本脅威検出統計情報のモニタリング

基本脅威検出統計情報をモニタするには、次のいずれかのタスクを実行します。

コマンド	目的
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**]	基本脅威検出統計情報を表示します。 **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。 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に関する情報」（P.62-2）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	基本脅威統計情報をクリアします。

例

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
```

基本脅威検出統計情報の機能履歴

表 62-2 に、各機能変更と、それが実装されたプラットフォーム リリースを示します。

表 62-2　基本脅威検出統計情報の機能履歴

機能名	プラットフォーム リリース	機能情報
基本脅威検出統計情報	8.0(2)	基本脅威検出統計情報が導入されました。 **threat-detection basic-threat**、**threat-detection rate**、**show threat-detection rate**、および **clear threat-detection rate** コマンドが導入されました。
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。
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。

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。この項は、次の内容で構成されています。

拡張脅威検出統計情報に関する情報

拡張脅威検出統計情報は、ホスト、ポート、プロトコル、アクセス リスト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。**threat-detection statistics host** コマンドを入力すると、パフォーマンスが著しく影響されます。トラフィックの負荷が高い場合、このタイプの統計情報は一時的にイネーブルにすることを検討できます。一方、**threat-detection statistics port** コマンドの影響は大きくありません。

ガイドラインと制限事項

この項では、この機能のガイドラインと制限事項について説明します。

セキュリティ コンテキストのガイドライン

マルチ モードで使用できるのは、TCP 代行受信統計情報だけです。

ファイアウォール モードのガイドライン

ルーテッド ファイアウォール モードとトランスペアレント ファイアウォール モードでサポートされています。

モニタ対象トラフィックのタイプ

through-the-box トラフィックだけがモニタされます。to-the-box トラフィックは、脅威検出に含まれません。

デフォルト設定

デフォルトでは、アクセス リストの統計情報はイネーブルになっています。

拡張脅威検出統計情報の設定

デフォルトでは、アクセス リスト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。

手順の詳細

	コマンド	目的
ステップ 1	**threat-detection statistics** **例：** `hostname(config)# threat-detection statistics`	（任意）すべての統計情報をイネーブルにします。 特定の統計情報だけをイネーブルにするには、（この表で示す）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。
ステップ 2	**threat-detection statistics access-list** **例：** `hostname(config)# threat-detection statistics access-list`	（任意）アクセス リスト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）。アクセス リストの統計情報は、デフォルトでイネーブルになっています。アクセス リスト統計情報は、**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。このコマンドは、デフォルトでイネーブルになっています。
ステップ 3	**threat-detection statistics host** [**number-of-rate** {**1** | **2** | **3**}] **例：** `hostname(config)# threat-detection statistics host number-of-rate 2`	（任意）ホストの統計情報をイネーブルにします。 **number-of-rate** キーワードは、ホストの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）。

	コマンド	目的
ステップ 4	**threat-detection statistics port** [**number-of-rate** {**1** | **2** | **3**}] **例：** hostname(config)# threat-detection statistics port number-of-rate 2	（任意）TCP および UDP ポートの統計情報をイネーブルにします。 **number-of-rate** キーワードは、ポートの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。
ステップ 5	**threat-detection statistics protocol** [**number-of-rate** {**1** | **2** | **3**}] **例：** hostname(config)# threat-detection statistics protocol number-of-rate 3	（任意）TCP/UDP IP 以外のプロトコルの統計情報をイネーブルにします。 **number-of-rate** キーワードは、プロトコルの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。
ステップ 6	**threat-detection statistics tcp-intercept** [**rate-interval** *minutes*] [**burst-rate** *attacks_per_sec*] [**average-rate** *attacks_per_sec*] **例：** hostname(config)# threat-detection statistics tcp-intercept rate-interval 60 burst-rate 800 average-rate 600	（任意）TCP 代行受信によって代行受信された攻撃の統計情報をイネーブルにします（TCP 代行受信をイネーブルにする方法については第 57 章「接続の設定」を参照してください）。 **rate-interval** キーワードは、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** キーワードは、syslog メッセージ生成のしきい値を、25 ～ 2147483647 の範囲で設定します。デフォルトは 1 秒間に 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** キーワードは、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。 **（注）**　このコマンドは、マルチ コンテキスト モードで使用できます。

拡張脅威検出統計情報のモニタリング

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。

拡張脅威検出統計情報をモニタするには、次のいずれかのタスクを実行します。

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。 **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。 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。 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、許可および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、アクセス リストによる拒否を追跡できます。 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。 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。 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。 **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*] **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。

コマンド	目的
show threat-detection statistics [**min-display-rate** *min_display_rate*] **protocol** [*protocol_number* | **ah** | **eigrp** | **esp** | **gre** | **icmp** | **igmp** | **igrp** | **ip** | **ipinip** | **ipsec** | **nos** | **ospf** | **pcp** | **pim** | **pptp** | **snp** | **tcp** | **udp**]	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。
show threat-detection memory	拡張脅威検出統計情報によって使用されたメモリ量を表示します。

例

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
```

表 62-3 に、各フィールドの説明を示します。

表 62-3　show threat-detection statistics host コマンドのフィールド

フィールド	説明
Host	ホストの IP アドレスを表示します。
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を表示します。
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を表示します。

表 62-3　show threat-detection statistics host コマンドのフィールド （続き）

フィールド	説明
fw-drop	ファイアウォールでのドロップ数を表示します。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、アクセス リストでの拒否、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を表示します。
null-ses	ヌル セッションの数を表示します。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 秒後までにサーバからデータが送信されなかった UDP セッションです。
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を表示します。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）を表示します。 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。
Current(eps)	終了した最後のバースト間隔における現在バースト レート（イベント数/秒）を表示します。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です。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が表示されます。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を表示します。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。

表 62-3　show threat-detection statistics host コマンドのフィールド （続き）

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における統計情報を表示します。
Sent byte	ホストから正常に送信されたバイト数を表示します。
Sent pkts	ホストから正常に送信されたパケット数を表示します。
Sent drop	ホストから送信されたパケットの中で、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を表示します。
Recv byte	ホストが正常に受信したバイト数を表示します。
Recv pkts	ホストが正常に受信したパケット数を表示します。
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を表示します。

拡張脅威検出統計情報の機能履歴

表 62-4 に、各機能変更と、それが実装されたプラットフォーム リリースを示します。

表 62-4　拡張脅威検出統計情報の機能履歴

機能名	プラットフォーム リリース	機能情報
拡張脅威検出統計情報	8.0(2)	拡張脅威検出統計情報が導入されました。 **threat-detection statistics** コマンドおよび **show threat-detection statistics** 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。

表 62-4　拡張脅威検出統計情報の機能履歴 （続き）

機能名	プラットフォーム リリース	機能情報
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。
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。

スキャン脅威検出の設定

この項は、次の内容で構成されています。

スキャン脅威検出に関する情報

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。トラフィック署名に基づく IPS スキャン検出とは異なり、ASA のスキャンによる脅威の検出機能では、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、アクティビティを返さない接続、閉じられているサービス ポートへのアクセス、非ランダム IPID などの脆弱な TCP の動作、およびその他の疑わしいアクティビティを追跡します。

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遮断します。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。

注意　スキャン脅威検出機能は、ホストベースとサブネットベースのデータ構造と情報を作成および収集する間、ASA のパフォーマンスとメモリに大きな影響を与える可能性があります。

ガイドラインと制限事項

この項では、この機能のガイドラインと制限事項について説明します。

セキュリティ コンテキストのガイドライン

シングル モードでだけサポートされています。マルチ モードはサポートされていません。

ファイアウォール モードのガイドライン

ルーテッド ファイアウォール モードとトランスペアレント ファイアウォール モードでサポートされています。

モニタ対象トラフィックのタイプ

- through-the-box トラフィックだけがモニタされます。to-the-box トラフィックは、脅威検出に含まれません。
- アクセス リスト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。

デフォルト設定

表 62-5 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 62-5　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。

バースト レートは、*N* 秒ごとの平均レートとして計算されます。*N* はバースト レート間隔です。バースト レート間隔は、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。

スキャン脅威検出の設定

手順の詳細

	コマンド	目的
ステップ 1	**threat-detection scanning-threat** [**shun** [**except** {**ip-address** *ip_address mask* | **object-group** *network_object_group_id*}]] **例：** `hostname(config)# threat-detection scanning-threat shun except ip-address 10.1.1.0 255.255.255.0`	スキャン脅威検出をイネーブルにします。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。
ステップ 2	**threat-detection scanning-threat shun duration** *seconds* **例：** `hostname(config)# threat-detection scanning-threat shun duration 2000`	（任意）攻撃元のホストを遮断する期間を設定します。

ステップ 3	**threat-detection rate scanning-threat rate-interval** *rate_interval* **average-rate** *av_rate* **burst-rate** *burst_rate*
	
	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`
		（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。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（「基本脅威検出統計情報の設定」（P.62-2）を参照）、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。

遮断されたホスト、攻撃者、ターゲットのモニタリング

遮断されたホスト、攻撃者、およびターゲットをモニタするには、次のいずれかのタスクを実行します。

コマンド	目的
show threat-detection shun	現在遮断されているホストを表示します。

コマンド	目的
clear threat-detection shun [*ip_address* [*mask*]]	ホストを遮断から解除します。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。
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

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

```
hostname# show threat-detection shun
Shunned Host List:
10.1.1.6
192.168.6.7
```

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
```

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

```
hostname# show threat-detection scanning-threat attacker
10.1.2.3
10.8.3.6
209.165.200.225
```

スキャン脅威検出の機能履歴

表 62-6 に、各機能変更と、それが実装されたプラットフォーム リリースを示します。

表 62-6　スキャン脅威検出の機能履歴

機能名	プラットフォーム リリース	機能情報
スキャン脅威検出	8.0(2)	スキャン脅威検出が導入されました。 **threat-detection scanning-threat**、**threat-detection rate scanning-threat**、**show threat-detection scanning-threat**、**show threat-detection shun**、および **clear threat-detection shun** コマンドが導入されました。
遮断期間	8.0(4)/8.1(2)	遮断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。

表 62-6　スキャン脅威検出の機能履歴 （続き）

機能名	プラットフォーム リリース	機能情報
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。
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。

脅威検出の設定例

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
```