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 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。

- 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。

- 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.26-9）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 26-1 に、デフォルト設定を示します。これらのデフォルト設定すべてを表示するには、**show running-config all threat-detection** コマンドを [Tools] > [Command Line Interface] で使用します。

表 26-1　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 26-1　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
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	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

ステップ 1　基本脅威検出をイネーブルまたはディセーブルにするには、[Configuration] > [Firewall] > [Threat Detection] ペインを選択し、[Enable Basic Threat Detection] チェックボックスをオンまたはオフにします。

ステップ 2　[Apply] をクリックします。

基本脅威検出統計情報のモニタリング

基本脅威検出の統計情報をモニタするには、次のタスクを実行します。

パス	目的
[Home] > [Firewall Dashboard] > [Traffic Overview]	基本脅威検出統計情報を表示します。 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.26-2）を参照してください。

基本脅威検出統計情報の機能履歴

表 26-2 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。ASDM は、複数のプラットフォーム リリースとの下位互換性があるため、サポートが追加された特定の ASDM リリースは一覧には含まれていません。

表 26-2　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。 次の画面が導入されました。[Configuration] > [Firewall] > [Threat Detection]、[Home] > [Firewall Dashboard] > [Traffic Overview]。
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、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。

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、ACL 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、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。

手順の詳細

ステップ 1　[Configuration] > [Firewall] > [Threat Detection] ペインを選択します。

ステップ 2　[Scanning Threat Statistics] 領域で、次のオプションのいずれかを選択します。

- すべての統計情報をイネーブルにする：[Enable All Statistics] オプション ボタンをクリックします。
- すべての統計情報をディセーブルにする：[Disable All Statistics] オプション ボタンをクリックします。
- 特定の統計情報のみをイネーブルにする：[Enable Only Following Statistics] オプション ボタンをクリックします。

ステップ 3　[Enable Only Following Statistics] を選択した場合は、次のチェックボックスのうち 1 つ以上をオンにします。

- [Hosts]：ホスト統計情報をイネーブルにします。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）。
- [Access Rules]（デフォルトでイネーブル）：アクセス ルールの統計情報をイネーブルにします。
- [Port]：TCP/UDP ポートの統計情報をイネーブルにします。
- [Protocol]：TCP/UDP 以外の IP プロトコルの統計情報をイネーブルにします。

- [TCP-Intercept]：TCP 代行受信によってインターセプトされた攻撃に関する統計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、「接続の設定」（P.21-8）を参照してください）。

ステップ 4　ホスト、ポート、およびプロトコルの統計情報については、収集するレート間隔の数を変更できます。[Rate Intervals] 領域で、統計タイプのそれぞれに対して [1 hour]、[1 and 8 hours]、または [1, 8 and 24 hours] を選択します。デフォルトの間隔は [1 hour] で、メモリ使用量が低く抑えられます。

ステップ 5　TCP 代行受信の統計情報については、次のオプションを [TCP Intercept Threat Detection] 領域で設定できます。

- [Monitoring Window Size]：履歴モニタリングの時間枠のサイズを 1 ～ 1440 分の範囲内で設定します。デフォルトは 30 分です。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。
- [Burst Threshold Rate]：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 Threshold Rate]：syslog メッセージ生成の平均レートのしきい値を 25 ～ 2147483647 の範囲内で設定します。デフォルトは 1 秒間に 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。

デフォルト値を復元するには、[Set Default] ボタンをクリックします。

ステップ 6　[Apply] をクリックします。

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するには、次のいずれかのタスクを実行します。

パス	目的
[Home] > [Firewall Dashboard] > [Top 10 Access Rules] [Home] > [Firewall Dashboard] > [Top Usage Statistics]	上位 10 件の統計情報を表示します。 [Top 10 Access Rules] については、許可されたトラフィックと拒否されたトラフィックはこの表示では区別されません。[Traffic Overview] > [Dropped Packets Rate] チャートでは、ACL 拒否を追跡できます。 [Top 10 Sources] タブおよび [Top 10 Destinations] タブに、ホストの統計情報が表示されます。**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。 [Top 10 Services] タブには、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。 [Top Ten Protected Servers under SYN Attack] 領域には、TCP 代行受信の統計情報が表示されます。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。[detail] ボタンは、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。 [Interval] ドロップダウン リストで [Last 1 hour]、[Last 8 hour]、または [Last 24 hour] を選択します。

拡張脅威検出統計情報の機能履歴

表 26-3 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。ASDM は、複数のプラットフォーム リリースとの下位互換性があるため、サポートが追加された特定の ASDM リリースは一覧には含まれていません。

表 26-3　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。 次の画面が導入されました。[Configuration] > [Firewall] > [Threat Detection]、[Home] > [Firewall Dashboard] > [Top 10 Access Rules]、[Home] > [Firewall Dashboard] > [Top Usage Status]、[Home] > [Firewall Dashboard] > [Top 10 Protected Servers Under SYN Attack]。
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。 次の画面が導入または変更されました。[Configuration] > [Firewall] > [Threat Detection]、[Home] > [Firewall Dashboard] > [Top 10 Protected Servers Under SYN Attack]。
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。 次の画面が変更されました。[Configuration] > [Firewall] > [Threat Detection]。
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。 次の画面が変更されました。[Configuration] > [Firewall] > [Threat Detection]。
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。

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。

- 「スキャン脅威検出の機能履歴」（P.26-12）

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、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。
- 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。

デフォルト設定

表 26-4 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 26-4　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

ステップ 1　[Configuration] > [Firewall] > [Threat Detection] ペインを選択し、[Enable Scanning Threat Detection] チェックボックスをオンにします。

ステップ 2　（任意）ホストが ASA によって攻撃者と判定された場合に自動的にそのホスト接続を終了するには、[Shun Hosts detected by scanning threat] チェックボックスをオンにします。

ステップ 3　（任意）ホストの IP アドレスを排除対象から外すには、[Networks excluded from shun] フィールドにアドレスを入力します。

複数のアドレスまたはサブネットは、カンマで区切って入力できます。IP アドレス オブジェクトのリストからネットワークを選択するには、[...] ボタンをクリックします。

ステップ 4　（任意）攻撃ホストの排除期間を設定するには、[Set Shun Duration] チェックボックスをオンにしてから、10 ～ 2592000 秒の範囲内の値を入力します。デフォルトの期間は 3600 秒（1 時間）です。デフォルト値を復元するには、[Set Default] をクリックします。

スキャン脅威検出の機能履歴

表 26-5 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。ASDM は、複数のプラットフォーム リリースとの下位互換性があるため、サポートが追加された特定の ASDM リリースは一覧には含まれていません。

表 26-5　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。 次の画面が導入されました。[Configuration] > [Firewall] > [Threat Detection]。
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。 次の画面が変更されました。[Configuration] > [Firewall] > [Threat Detection]。
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。