IPS 異常検出の管理

（注） 4.17 以降、Cisco Security Manager は引き続き IPS の機能をサポートしますが、IPS はサポートが終了しているため、IPS の拡張機能はサポートされません。詳細については、EOL 通知を参照してください。

異常検出は、スキャン動作を示すワームトラフィックを原因とするネットワークの輻輳を認識するように設計されています。異常検出では、他の脆弱なホストをスキャンしている、ネットワーク上の感染したホストも識別されます。

異常検出はデフォルトでイネーブルになりますが、効果的に使用するために調整する必要のある設定がいくつかあります。

（注） 異常検出を設定するには、センサーで IPS ソフトウェアバージョン 6.x 以降を使用する必要があります。また、Cisco IOS IPS と AIP-SSC-5 では異常検出はサポートされません。

この章は次のトピックで構成されています。

異常検出について

センサーの異常検出コンポーネントでは、ワームに感染したホストが検出されます。これによりセンサーでは、Code Red や SQL Slammer などのワームやスキャナからの保護に際してシグニチャ更新への依存度が低くなります。異常検出コンポーネントでは、センサーが正常なアクティビティを学習し、正常な動作として学習した動作から逸脱する動作に対してアラートを送信するか、または動的応答アクションを実行します。

（注） 異常検出では、Nimda などの電子メール ベースのワームは検出されません。

異常検出では、次の 2 つの状況が検出されます。

- ワーム トラフィックによって輻輳し始めたパスでネットワークが起動した場合。
- ワームに感染した単一のソースがネットワークに入り、他の脆弱なホストのスキャンを開始した場合。

ここでは、異常検出についてより詳細に説明します。

ワーム ウイルス

ワーム ウイルスは、自身のコピーを作成してその拡散を促進する自動化された自己伝播型侵入エージェントです。ワーム ウイルスは脆弱なホストを攻撃して感染させ、そのホストをベースとして使用して他の脆弱なホストを攻撃します。ネットワーク インスペクションの 1 つの形式（通常はスキャン）を使用して他のホストを検索し、次のターゲットに伝播します。スキャニング ワーム ウイルスは、プローブする IP アドレスのリストを収集することで脆弱なホストを特定し、ホストにアクセスします。Code Red ワーム、Sasser ワーム、Blaster ワーム、および Slammer ワームは、この方法で広がるワームの例です。

異常検出では、スキャナとして動作している、ワームに感染したホストを識別します。ワーム ウイルスは、拡散するために新しいホストを見つける必要があります。TCP、UDP、およびその他のプロトコルを使用してインターネットをスキャンして、異なる宛先 IP アドレスへの失敗するアクセス試行を生成することでホストを見つけます。スキャナは、非常に多くの宛先 IP アドレスに対して（TCP および UDP で）同じ宛先ポートにイベントを生成する送信元 IP アドレスとして定義されます。

TCP にとって重要なイベントは、特定の時間内に SYN-ACK 応答のない SYN パケットなど、未確立の接続です。TCP を使用してスキャンする、ワームに感染したホストは、異常な数の IP アドレスに対して同じ宛先ポートに未確立接続を生成します。

UDP にとって重要なイベントは、すべてのパケットが一方向にのみ流れる UDP 接続など、一方向の接続です。UDP を使用してスキャンする、ワームに感染したホストは、UDP パケットを生成しますが、複数の宛先 IP アドレスに対して同じ宛先ポートでタイムアウト期間内に同じ IP アドレス上で UDP パケットを受信しません。

ICMP（プロトコル番号 1）など、その他のプロトコルにとって重要なイベントは、送信元 IP アドレスから多数のさまざまな宛先 IP アドレス、すなわち、一方向でのみ受信されるパケットです。

注意 ワーム ウイルスが感染先の IP アドレスのリストを持っていて、拡散のためにスキャンを使用する必要がない場合（たとえば、パッシブ マッピングを使用する場合は、アクティブ スキャニングとは対照的に、ネットワークをリスニングします）、異常検出ワーム ポリシーでは検出されません。感染したホスト内でファイルをプローブしてメーリング リストを受信し、このリストを電子メールで送信するワーム ウイルスは、レイヤ 3 またはレイヤ 4 の異常を生成しないため、検出されません。

異常検出モード

異常検出はまず、ネットワークの最も正常な状態が反映される「正常時」の学習プロセスを実行します。次に、異常検出は正常なネットワークに最適な一連のポリシーしきい値を生成します。この処理は、初期の学習モード フェーズとそれに続く進行中の動作検出モード フェーズの 2 つのフェーズで行われます。

異常検出には次のモードがあります。

- 学習受け入れモード（初期設定）

異常検出はデフォルトで検出モードになっていますが、デフォルトで 24 時間、初期の学習受け入れモードを実行します。このフェーズ中は攻撃が行われないことを前提とします。異常検出では、ナレッジ ベースと呼ばれるネットワーク トラフィックの初期ベースラインが作成されます。定期スケジュールのデフォルトの間隔値は 24 時間で、デフォルトのアクションは循環です。これは、新しいナレッジ ベースが保存およびロードされ、24 時間後に初期ナレッジ ベースが置換されることを意味します。

次の点を考慮してください。

- 異常検出は、空の初期ナレッジベースを処理するときには攻撃を検出しません。デフォルトの 24 時間が経過すると、ナレッジ ベースが保存されてロードされ、異常検出が攻撃を検出するようになります。
- ネットワークの複雑さによっては、異常検出の学習受け入れモードをデフォルトの 24 時間よりも長くした方がよい場合もあります。モードは仮想センサーポリシーで設定します。仮想センサーの定義を参照してください。学習期間が終了した後、仮想センサーを編集し、検出モードに変更します。

- 検出モード

操作の進行中は、センサーを検出モードのままにする必要があります。これは 1 日 24 時間、週 7 日間実行します。ナレッジベースが作成され、初期ナレッジベースが置換されたあとで、異常検出はそのナレッジ ベースに基づいて攻撃を検出します。ナレッジ ベースのしきい値に違反するネットワーク トラフィック フローを見つけると、アラートを送信します。異常検出が異常を探すとき、しきい値に違反しない漸進的な変化がナレッジベースに記録され、新しいナレッジ ベースが作成されます。新しいナレッジ ベースは定期的に保存され、古いナレッジ ベースを置き換えるため、最新のナレッジ ベースが維持されます。

- 非アクティブ モード

異常検出は、非アクティブモードにすることでオフにできます。センサーが非対称環境で稼働している場合など、特定の状況では、異常検出を非アクティブモードにする必要があります。異常検出では、トラフィックが両方向から来ることを前提とするため、センサーがトラフィックの一方向だけを参照するように設定されている場合は、異常検出によってすべてのトラフィックに不完全な接続（スキャナ）があるものと識別され、すべてのトラフィック フローについてアラートが送信されます。

次の例で、デフォルトの異常検出設定についてまとめます。仮想センサーを午後 11:00 に追加して、デフォルトの異常検出設定を変更しなかった場合、異常検出は初期ナレッジベースを使用して動作を開始し、学習のみを実行します。これは検出モードですが、情報を 24 時間収集して初期ナレッジベースを置換するまで、攻撃は検出されません。最初の開始時刻（デフォルトでは午前 10:00）および最初の間隔（デフォルトでは 24 時間）に、学習結果が新しいナレッジベースに保存され、このナレッジベースがロードされて初期ナレッジベースを置換します。異常検出はデフォルトで検出モードとなるため、新しいナレッジベースを使用して攻撃の検出を開始します。

異常検出ゾーン

ネットワークをゾーンに分割することで、偽陰性の率を低下させることができます。ゾーンは、宛先 IP アドレスのセットです。内部、不正、外部の 3 つのゾーンがあり、それぞれに独自のしきい値があります。

外部ゾーンは、デフォルトのインターネット範囲（0.0.0.0 ～ 255.255.255.255）を持つデフォルトのゾーンです。デフォルトでは、内部ゾーンと不正ゾーンにはIPアドレスは含まれません。内部ゾーンまたは不正ゾーンに含まれる IP アドレスのセットに一致しないパケットは、外部ゾーンで処理されます

内部ネットワークの IP アドレス範囲を使用して内部ゾーンを設定することを推奨します。このように設定すると、内部ゾーンには内部ネットワークの IP アドレス範囲に到着するすべてのトラフィックが含まれ、外部ゾーンにはインターネットに送信されるすべてのトラフィックが含まれます。

不正ゾーンには、割り当てられていない IP アドレスや、使用されていない内部 IP アドレス範囲に属する IP アドレスなど、正常なトラフィックに存在してはならない IP アドレスの範囲を設定できます。不正ゾーンには適正なトラフィックが到達しないと想定されるため、このゾーンは正確な検出に非常に役立ちます。これにより、非常に迅速なワーム ウイルス検出を可能にする非常に低いしきい値を設定できます。

異常検出をオフにする場合について

異常検出では、トラフィックは双方向であると見なされます。センサーがトラフィックの一方向だけを参照するように設定されている場合は、異常検出をオフにする必要があります。そうしないと、異常検出が非対称環境で実行されている場合に、すべてのトラフィックに不完全な接続（スキャナ）があるものと識別され、すべてのトラフィック フローについてアラートが送信されます。

Virtual Sensors ポリシーで、異常検出をオフにします。異常検出をディセーブルにする仮想センサーを編集し、[Anomaly Detection Mode] を [Inactive] に変更します。仮想センサーの編集に関する詳細については、仮想センサーのポリシーの編集を参照してください。

異常検出シグニチャの設定

トラフィック異常エンジンには、3 つのプロトコル（TCP、UDP、およびその他）をカバーする 9 つの異常検出シグニチャが含まれます。各シグニチャには 2 つのサブシグニチャがあります。一方はスキャナ用で、もう一方はワームに感染したホスト（またはワーム攻撃されているスキャナ）用です。異常検出は、異常を検出すると、これらのシグニチャのアラートをトリガーします。すべての異常検出シグニチャは、デフォルトでイネーブルになり、各シグニチャのアラート重大度は高く設定されます。

スキャナが検出されても、ヒストグラム異常が発生しない場合、スキャナ シグニチャはその攻撃者（スキャナ）の IP アドレスをファイルに保存します。ヒストグラム シグニチャがトリガーされた場合は、スキャンを行っている攻撃者のアドレスによってそれぞれ（スキャナ シグニチャではなく）ワーム シグニチャがトリガーされます。ヒストグラムがトリガーされているので、アラートの詳細には、ワーム検出に使用されたしきい値が表示されます。その時点から、すべてのスキャナがワーム感染ホストとして検出されます。

次の異常検出イベント アクションが可能です。

- Produce alert：イベント ストアにイベントを書き込みます。
- Deny attacker inline：（インラインのみ）指定された期間、この攻撃者のアドレスから発生した現在のパケットおよび将来のパケットを送信しません。
- Log attacker packets：攻撃者のアドレスが含まれているパケットに対する IP ロギングを開始します。
- Deny attacker service pair inline：送信元 IP アドレスと宛先ポートをブロックします。
- Request SNMP trap：トラップ通知を SNMP トラップ宛先に送信します。このアクションを使用するには、SNMP の設定の説明に従って SNMP トラップ ホストを設定する必要があります。
- Request block host：要求を ARC に送信して、このホスト（攻撃者）をブロックします。このアクションを使用するには、IPS のブロッキングおよびレート制限の設定の説明に従ってデバイスのブロックを設定する必要があります。

Signatures ポリシーでシグニチャにアクションを直接追加するか、Event Actions Overrides ポリシーでリスク レーティングに基づいてシグニチャにより生成されたイベントにアクションを追加できます。

次の表に、異常検出ワーム シグニチャのリストを示します。

表 *1:* 異常検出ワーム シグニチャ

シグネチャ ID	サブシグニチャ ID	名前	説明
13000	[0]	Internal TCP Scanner	内部ゾーンで TCP プロトコル上に単一スキャナを識別しました。
13000	1	Internal TCP Scanner	内部ゾーンで TCP プロトコル上にワーム攻撃を識別しました。TCP ヒストグラムのしきい値を超え、TCP プロトコル上にスキャナが識別されました。
13001	[0]	Internal UDP Scanner	内部ゾーンで UDP プロトコル上に単一スキャナを識別しました。
13001	1	Internal UDP Scanner	内部ゾーンで UDP プロトコル上にワーム攻撃を識別しました。UDP ヒストグラムのしきい値を超え、UDP プロトコル上にスキャナが識別されました。
13002	[0]	Internal Other Scanner	内部ゾーンでほかのプロトコル上に単一スキャナを識別しました。
13002	1	Internal Other Scanner	内部ゾーンでその他のプロトコル上にワーム攻撃を識別しました。その他のヒストグラムのしきい値を超え、その他のプロトコル上にスキャナが識別されました。
13003	[0]	External TCP Scanner	外部ゾーンで TCP プロトコル上に単一スキャナを識別しました。
13003	1	External TCP Scanner	外部ゾーンで TCP プロトコル上にワーム攻撃を識別しました。TCP ヒストグラムのしきい値を超え、TCP プロトコル上にスキャナが識別されました。
13004	[0]	External UDP Scanner	外部ゾーンで UDP プロトコル上に単一スキャナを識別しました。
13004	1	External UDP Scanner	外部ゾーンで UDP プロトコル上にワーム攻撃を識別しました。UDP ヒストグラムのしきい値を超え、UDP プロトコル上にスキャナが識別されました。
13005	[0]	External Other Scanner	外部ゾーンでその他のプロトコル上に単一スキャナを識別しました。

シグネチャ ID	サブシグニチャ ID	名前	説明
13005	1	External Other Scanner	外部ゾーンでその他のプロトコル上にワーム攻撃を識別しました。その他のヒストグラムのしきい値を超え、その他のプロトコル上にスキャナが識別されました。
13006	[0]	Illegal TCP Scanner	不正ゾーンで TCP プロトコル上に単一スキャナを識別しました。
13006	1	Illegal TCP Scanner	不正ゾーンで TCP プロトコル上にワーム攻撃を識別しました。TCP ヒストグラムのしきい値を超え、TCP プロトコル上にスキャナが識別されました。
13007	[0]	Illegal UDP Scanner	不正ゾーンで UDP プロトコル上に単一スキャナを識別しました。
13007	1	Illegal UDP Scanner	不正ゾーンで UDP プロトコル上にワーム攻撃を識別しました。UDP ヒストグラムのしきい値を超え、UDP プロトコル上にスキャナが識別されました。
13008	[0]	Illegal Other Scanner	不正ゾーンでその他のプロトコル上に単一スキャナを識別しました。
13008	1	Illegal Other Scanner	不正ゾーンでその他のプロトコル上にワーム攻撃を識別しました。その他のヒストグラムのしきい値を超え、その他のプロトコル上にスキャナが識別されました。

異常検出の設定

Anomaly Detection ポリシーを使用して、異常検出を設定します。Virtual Sensors ポリシーにも、異常検出にとって重要な設定が含まれます。

この手順では、異常検出の全体的な設定について説明します。これらの設定を設定する前に、次の項を参照してください。

- 異常検出について （1 ページ）
- ワーム ウイルス （2 ページ）
- 異常検出モード （3 ページ）
- 異常検出ゾーン （4 ページ）

• 異常検出をオフにする場合について （4 ページ）
• 異常検出シグニチャの設定 （5 ページ）

ステップ 1 次のいずれかを実行して、変更する異常検出ポリシーを開きます。

- （デバイスビュー）ポリシーセレクタから **[IPS] > [異常検出（Anomaly Detection）]** を選択します。
- （ポリシービュー）ポリシーセレクタから **[IPS] > [異常検出（Anomaly Detection）]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

異常検出ポリシーには、次のタブが含まれています。

- [動作設定（OperationSettings）]：ワームタイムアウトを定義し、異常検出で無視する必要のある IP アドレスを識別します。
- [学習受け入れモード（Learning Accept Mode）]：ナレッジベースの処理方法を含む、学習モードの設定。
- [内部ゾーン（Internal Zone）]、[不正ゾーン（Illegal Zone）]、[外部ゾーン（External Zone）]：定義するネットワークのゾーン。各ゾーンに固有の設定を設定できます。ゾーンの説明については、異常検出ゾーン （4 ページ）を参照してください。

ステップ 2 必要な場合、[動作設定（Operation Settings）] タブをクリックして、次の項目を設定します。

- [ワームタイムアウト（Worm Timeout）]：ワーム終了タイムアウトの時間（秒単位）。範囲は 120 ～ 10,000,000 秒です。デフォルトは 600 秒です。このタイムアウトの使用方法については、異常検出しきい値とヒストグラムについて （12 ページ）を参照してください。
- [無視したアドレスの有効化（Enable Ignored Addresses）] および [無視する送信元/宛先アドレス（Source/Destination Addresses to Ignore）]：異常検出の処理中に無視する必要があるアドレスのリストを設定するかどうか。送信元アドレス（スキャンを開始するアドレス）または宛先アドレス（スキャンされるホスト）のリストを指定できます。

アドレスには、1 つの単一ホスト（10.100.10.1 など）、1 つのアドレス範囲（10.100.10.0-10.100.10.255 など）、あるいは複数の単一ホスト、複数のアドレス範囲、または複数のホストと範囲の組み合わせを含むネットワーク/ホスト オブジェクトを指定できます。[選択（Select）] を選択して、リストからオブジェクトを選択するか、新しいオブジェクトを作成します。

ステップ 3 [学習受け入れモード（Learning Accept Mode）] タブをクリックしてナレッジベースの生成方法および使用方法を定義します。詳細については、異常検出の学習受け入れモードの設定 （10 ページ）を参照してください。

ステップ 4 内部ゾーン、不正ゾーン、および外部ゾーンを設定します。

- 内部ゾーンと不正ゾーンの定義：内部ゾーンは、管理対象のネットワークである内部ネットワークの IP アドレスです。不正ゾーンは、正常なトラフィックでは決して見られない IP アドレス範囲を表している必要があります。たとえば、割り当てられていない IP アドレスや、使用されていない内部 IP アドレス範囲に属する IP アドレスなどです。

[内部ゾーン（Internal Zone）] タブと [不正ゾーン（Illegal Zone）] タブを順番にクリックし、[全般（General）] タブで次の項目を設定します。

- [このゾーンを有効化する（Enable this zone）]：ゾーンが異常検出によって処理されるかどうか。
- [サービスサブネット（Service Subnets）]：ゾーンを構成する IP アドレス。デフォルト（0.0.0.0）では、ゾーンにアドレスは含まれません。ゾーンのアドレスを定義するように、0.0.0.0 を置き換えます。

アドレスには、1 つの単一ホスト（10.100.10.1 など）、1 つのアドレス範囲（10.100.10.0-10.100.10.255 など）、あるいは複数の単一ホスト、複数のアドレス範囲、または複数のホストと範囲の組み合わせを含むネットワーク/ホスト オブジェクトを指定できます。[選択（Select）] を選択して、リストからオブジェクトを選択するか、新しいオブジェクトを作成します。

- [外部ゾーンを有効にするかどうかを決定する（Decide whether to enable the external zone）]：外部ゾーンは、内部ゾーンまたは不正ゾーン用に構成されていないすべての IP アドレスで構成されます。このゾーンにはアドレスを明示的に割り当てません。[外部ゾーン（External Zone）] タブの [全般（General）] サブタブで、[このゾーンを有効化する（Enable this zone）] チェックボックスを使用して、ゾーンを有効化または無効化できます。外部ゾーンはデフォルトで有効になっています。
- [スキャナしきい値とヒストグラムの設定（Configure scanner thresholds and histograms）]：各ゾーンには、[TCPプロトコル（TCP Protocol）]、[UDPプロトコル（UDP Protocol）]、および [その他のプロトコルOther Protocols] のサブタブがあります。これらのタブで、学習されたヒストグラムを上書きする非デフォルト設定を特定のサービスに対して設定できます。これらの設定の詳細については、異常検出しきい値とヒストグラムの設定 （13 ページ）を参照してください。

この時点で、基本的な異常検出の設定が完了しました。

ステップ 5 （デバイス ビューだけ）異常検出モードを設定します。この設定は、[仮想センサー（Virtual Sensors）] ポリシーで定義します。次のヒントを考慮して、適切なポリシーを選択します。

- 仮想センサー（親 IPS デバイスで表される vs0 を除く）で異常検出ポリシーを設定した場合は、親 IPS デバイスを選択し、[Virtual Sensors] ポリシーを選択する必要があります。
- ポリシー ビューで [Anomaly Detection] ポリシーを共有ポリシーとして設定した場合は、ポリシーを割り当てる IPS デバイスまたはポリシーを割り当てる仮想センサーをホスティングする IPS デバイスを選択します。

次に、[Virtual Sensors] ポリシーで次の手順を実行します。

a) テーブルで目的の仮想センサーを選択し、[行の編集（Edit Row）] ボタンをクリックします。
b) [仮想センサーの変更（Modify Virtual Sensors）] ダイアログボックスで、異常検出モード設定の適切なオプション（検出、非アクティブ、学習）を選択します。デフォルトの通常の動作モードは [Detect] です。ただし、非対称ノーマライザ モードを使用している場合は、異常検出モードを非アクティブに設定する必要がある場合があります。これらのモードの詳細については、異常検出モード （3 ページ）を参照してください。このダイアログボックスのその他の設定の詳細については、仮想センサー ダイアログボックスを参照してください。
c) 異常検出を [Learning] モードにした場合は、目的の学習期間の完了後にモードを忘れずに [Detect] に変更してください。

ステップ 6 必要に応じて、追加のアクションを異常検出シグニチャに追加します。たとえば、攻撃がドロップされるように拒否アクションを追加します。または、イベント アクションのオーバーライドを設定して、リスク レーティングに基づくアクションを追加できます。詳細については、異常検出シグニチャの設定 （5 ページ）を参照してください。

ステップ 7 必要な場合、ナレッジ ベースを管理します。

（[Learning Accept Mode] タブで）ナレッジベースを自動的に循環するように設定した場合、ナレッジベースは自動的にリフレッシュされるため、手動での操作は不要です。

新しいデータベースの保存だけを行い、それらを使用しないように異常検出を設定した場合は、更新したナレッジベースを定期的に手動でロードする必要があります。Security Manager ではこれを行うことはできません。代わりに IPS Device Manager（IDM）を使用してください。

IDM（または IME）を使用して、ナレッジベースをロード、削除、および名前変更したり、ナレッジベースを外部サーバにアップロードまたは外部サーバからダウンロードしたりできます。実行できる内容の詳細については、IDM または IME のオンライン ヘルプを参照してください。

異常検出の学習受け入れモードの設定

[Anomaly Detection] ポリシーの [Learning Accept Mode] タブを使用して、センサーで新しいナレッジ ベースを何時間ごとに作成するかを設定します。ナレッジ ベースを作成およびロード（[Rotate]）するか、保存（[Save Only]）するかを設定できます。ナレッジ ベースをロードまたは保存する頻度およびタイミングをスケジュールします。

デフォルトで生成されるファイル名は YYYY-Mon-dd-hh_mm_ss（year-month-day-hour_minute_second）です。Mon は現在の月の 3 文字の略語です。

ナレッジ ベースにはツリー構造があり、次の情報を含みます。

- ナレッジ ベース名
- ゾーン名（Zone name）
- プロトコル
- サービス

ナレッジベースには、各サービスのスキャナしきい値とヒストグラムが保存されます。学習受け入れモードを自動に設定し、アクションを循環に設定した場合、新しいナレッジ ベースは 24 時間ごとに作成され、次の 24 時間に使用されます。学習受け入れモードを自動に設定し、アクションを保存だけに設定した場合、新しいナレッジベースは作成されますがロードはされず、現在のナレッジベースが使用されます。学習受け入れモードを自動に設定しない場合、ナレッジ ベースは作成されません。

ヒント Cisco Security Manager を使用してナレッジベースの生成方法を設定できますが、ナレッジベース自体は管理できません。代わりに IPS Device Manager（IDM）または IPS Manager Express（IME）を使用します。IDM（またはIME）を使用して、ナレッジベースをロード、削除、および名前変更したり、ナレッジベースを外部サーバにアップロードまたは外部サーバからダウンロードしたりできます。実行できる内容の詳細については、IDM または IME のオンラインヘルプを参照してください。

関連項目

- 異常検出モード （3 ページ）
- 異常検出の設定 （7 ページ）
- 異常検出しきい値とヒストグラムについて （12 ページ）

ステップ 1 次のいずれかを実行して、変更する異常検出ポリシーを開きます。

- （デバイスビュー）ポリシーセレクタから **[IPS] > [異常検出（Anomaly Detection）]** を選択します。
- （ポリシービュー）ポリシーセレクタから **[IPS] > [異常検出（Anomaly Detection）]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

ステップ 2 [学習受け入れモード（Learning Accept Mode）] タブをクリックし、次のオプションを設定します。

- [学習ナレッジベースを自動的に受け入れる（Automatically accept learning knowledge base）]：センサーでナレッジベースを自動的に更新するかどうかを指定します。このオプションを選択しない場合、異常検出では新しいナレッジ ベースが自動的には作成されず、このタブの他のオプションを設定できません。
- [アクション（Action）]：ナレッジベースを作成時に保存するかどうかを指定します。

[ローテーション（Rotate）]（デフォルト）を選択した場合、定義したスケジュールに従って新しいナレッジベースが作成されてロードされます。[保存のみ（Save Only）] を選択した場合、新しいナレッジベースが作成されますが、ロードされません。IDM または IME を使用してナレッジ ベースを調べ、異常検出にロードするかどうかを決定できます。

ステップ 3 [スケジュール（Schedule）]フィールドで、新しいナレッジベースを生成するスケジュールを選択します。デフォルトのスケジュールは、定期的に午前 10 時に開始され、24 時間実行されます。次のオプションがあります。

- [定期的（Periodic）]：再帰的な期間に基づいてスケジュールします。次のオプションを設定します。
  - [開始時刻（Start Time）]：hh:mm:ss 形式（24 時間制）での学習期間の開始時刻。
  - [時間単位の学習間隔（Learning Interval in hours）]：新しいナレッジベースを作成する前に異常検出でネットワークから学習する時間の長さ。

- [カレンダーのスケジュール（Calendar Schedule）]：特定の時刻または曜日に基づいてスケジュールします。ダイアログボックスは、[Time of Day] テーブルおよび [Days of the Week] テーブルを表示するように変更されます。これらの時刻は選択したすべての日に適用されます。異なる日に異なる時刻は指定できません。
  - 時間または日を追加するには、該当するテーブルの下にある [行の追加（Add Row）]（+）ボタンをクリックします。時刻は hh:mm:ss 形式（24 時間制）です。日の場合は、リストから日を選択します。
  - 既存の時間または日を編集するには、その時間または日を選択し、[行の編集（Edit Row）]（鉛筆）ボタンをクリックします。
  - 時間または日を削除するには、その時間または日を選択し、[行の削除（Delete Row）]（ゴミ箱）ボタンをクリックします。少なくとも 1 つの時間と日が設定されていることを確認してください。

異常検出しきい値とヒストグラムについて

異常検出では、しきい値およびヒストグラムを使用して、スキャン動作が攻撃であるかどうかを判断します。

学習モード中に、異常検出は各 TCP および UDP ポートのヒストグラムを作成し、その他のプロトコルについては、ネットワークの正常な動作のベースラインを作成します（異常検出モード （3 ページ）を参照）。たとえば、TCP ポートのヒストグラムには、1 分間に特定の数の宛先アドレスに対して不完全な接続を行う送信元アドレスの「正常」な数がリストされます。ヒストグラムには、少数（5）、中程度の数（20）、および多数（100）の宛先アドレスという 3 つのバケットが含まれます（宛先バケットは固定数です）。サービスおよびゾーンごとに個別のヒストグラムが保持されます（異常検出ゾーン （4 ページ）を参照）。

たとえば、学習モードでは、TCP ポート 80 に対して次のヒストグラムが作成される場合があります。

宛先アドレスの数	送信元アドレスの数
Low（5）	18
中程度（20）	6
高（100）	2

これらの学習したヒストグラムに加えて、異常検出スキャナではしきい値を設定します。一般的なスキャナしきい値を設定し、特定のサービス（TCP ポート、UDP ポート、またはその他のプロトコル）に対してしきい値を上書き（別の値を設定）できます。各ゾーンには独自のしきい値があります。

異常検出が、ワームがアクティブにスキャンされる検出モードに移行すると、しきい値とヒストグラムは次のように使用されます。

- サービスのしきい値を超えるまで、ヒストグラムは無視されます。たとえば、上記の TCP/80 トラフィックの表について考えます。しきい値が 200（デフォルト）に設定されている場合、スキャナアラートをトリガーするにはスキャナが 1 分間に 200 台のホストをスキャンする必要があります。7 つの送信元アドレスが 50 台のホストをスキャンし（これは、20 ～ 99 の宛先をスキャンするホストが 6 台を超えないと予想されるヒストグラムでは異常です）、単一のスキャナが 100 個のアドレスだけをスキャンした場合、アラートは生成されず、異常は検出されません。
- スキャナしきい値を超過すると、異常検出では、ヒストグラムを使用して、サービスがワームに攻撃されているかどうかが判断されます。この例では、送信元が 200 を超える宛先をスキャンする場合、異常検出はネットワーク内で収集されたアクティビティを評価します。7 台のホストが 50 台のホストをスキャンしたため、ワーム アラートが生成されます。

ワームに攻撃されている場合、異常検出は学習を停止し、現在の学習情報をクリアします。また、一時的にしきい値が下がります。

- ワーム攻撃が検出されると、ワームタイムアウトカウンターが開始されます。タイムアウトに達すると、スキャナがリセットされます。ワーム攻撃が継続する場合は、新しいアラートが生成されます。ワーム タイムアウトは、[Anomaly Detection] ポリシーの [Operation Settings] タブで設定します。

デフォルトのままにした場合、異常検出は、ネットワークの実際の動作から、ネットワークについて学習した内容に基づいてヒストグラムを生成します。ただし、ネットワークを理解していれば、これらのヒストグラムを微調整して誤検知を減らし、ゾーンごとに、TCP/UDP ポートまたはその他のプロトコルごとに予想される（または望ましいまたは許容される）動作の独自の定義を作成できます。関心のあるサービスのみについて独自のヒストグラムを作成し、他のすべてのポートについてはデフォルトのままにすることができます。また、各ゾーンの一般的なスキャナしきい値を設定し、特定のサービスに対しては異なるしきい値を設定できます。

しきい値とヒストグラムを設定する方法の詳細については、異常検出しきい値とヒストグラムの設定 （13 ページ）を参照してください。

異常検出しきい値とヒストグラムの設定

異常検出では、しきい値およびヒストグラムを使用して、スキャン動作が攻撃であるかどうかを判断します。ほとんどの場合は、異常検出が学習モード中に生成するデフォルトのしきい値とヒストグラムを使用できます（異常検出モード （3 ページ）を参照）。ただし、これらの設定の微調整が必要な場合があります。独自のヒストグラムの作成よりも、しきい値の変更の方が行う可能性が高くなります。

これらの設定値を設定する前に、異常検出しきい値とヒストグラムについて （12 ページ）を読んでください。しきい値とヒストグラムを設定するために、これらがどのように連携して使用されるかを理解する必要があります。

ステップ 1 次のいずれかを実行して、変更する異常検出ポリシーを開きます。

- （デバイスビュー）ポリシーセレクタから **[IPS] > [異常検出（Anomaly Detection）]** を選択します。
- （ポリシービュー）ポリシーセレクタから **[IPS] > [異常検出（Anomaly Detection）]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

ステップ 2 しきい値またはヒストグラムを変更するゾーンのタブをクリックします。[内部ゾーン（Internal Zone）]、[不正ゾーン（Illegal Zone）]、[外部ゾーン（External Zone）] の各ゾーンに別固の値を設定します。ゾーンの説明については、異常検出ゾーン （4 ページ）を参照してください。

各ゾーンのタブには、[General]、[TCP Protocol]、[UDP Protocol]、[Other Protocols] の 4 つのサブタブがあります。[General] タブでは、ゾーンの IP アドレスと、ゾーンがイネーブルになっているかどうかを定義します（外部ゾーンには他のゾーンで指定されていないすべての IP アドレスが含まれるため、外部ゾーンに対して特定のアドレスは設定しません）。

その他のタブでは、しきい値とヒストグラムを定義します。

ステップ 3 しきい値またはヒストグラムを変更するプロトコルのタブを選択します。[TCPプロトコル（TCP Protocol）]、[UDPプロトコル（UDP Protocol）]、[その他のプロトコル（Other Protocol）]

各タブで、次のオプションを設定します。

- [有効（Enabled）]：プロトコルに対して異常検出を有効にするかどうか。このオプションで、すべての TCP、UDP、または TCP/UDP 以外のプロトコルでの検出をオフにできます。このオプションを選択解除した場合、タブに設定されている他の設定はすべて無視されます。
- [宛先ポートマップ（Destination Port Map）] または [プロトコル番号マップ（Protocol Number Map）] テーブル：このテーブルには、デフォルト以外のマッピングを設定している TCP/UDP ポート、またはその他のプロトコルが一覧表示されます。デフォルトでは、すべてのポートとプロトコルがイネーブルになり、デフォルト スキャナしきい値が使用されます。

次の場合にのみ、このテーブルに項目を追加します。ポートまたはプロトコルの検出を無効にする。ポートまたはプロトコルに異なるしきい値を設定する。または、学習したヒストグラムの代わりに使用されるポートまたはプロトコルの明示的なヒストグラムを設定する。

- マッピングを追加するには、[行の追加（Add Row）]（+）ボタンをクリックし、[宛先またはプロトコルマップの追加（Add Dest or Protocol Map）] ダイアログボックスに入力します。詳細については、[Add Dest Port Map]/[Modify Dest Port Map] または [Add Protocol Map]/[Modify Protocol Map] ダイアログボックス （15 ページ）を参照してください。
- マッピングを編集するには、マッピングを選択し、[行の編集（Edit Row）]（鉛筆）ボタンをクリックします。
- マッピングを削除するには、マッピングを選択し、[行の削除（Delete Row）]（ゴミ箱）ボタンをクリックします。マッピングを削除すると、サービスはデフォルト設定に戻ります。
- [スキャナしきい値（Scanner Threshold）]：TCP、UDP、またはその他のプロトコルすべてに対するしきい値。このしきい値は、マッピングテーブルでスキャナオーバーライドを設定したサービス以外のすべてのサービスに使用されます。範囲は 5 ～ 1000 です。デフォルトは 200 です。

- [しきい値ヒストグラム（Threshold Histogram）]：TCP、UDP、またはその他のプロトコルすべてに対するデフォルトのヒストグラム。このヒストグラムは、マッピングテーブルでスキャナオーバーライドを設定したサービス以外のすべてのサービスに使用されます。

このテーブルの内容は固定されています。項目の追加や削除はできません。ただし、行を選択して[行の編集（Edit Row）]（鉛筆）をクリックすると、しきい値設定に指定されている送信元アドレスの数を変更できます。 [Histogram] ダイアログボックス （17 ページ）を参照してください。

ステップ 4 デフォルト以外の設定を定義するゾーンとプロトコルの組み合わせごとに、このプロセスを繰り返します。

[Add Dest Port Map]/[Modify Dest Port Map] または [Add Protocol Map]/[Modify Protocol Map] ダイアログボックス

[Add Dest Port Map]/[Modify Dest Port Map] ダイアログボックスを使用して、TCP または UDP の宛先ポート スキャナ設定を追加または修正し、[Add Protocol Map]/[Modify Protocol Map] ダイアログボックスを使用して、その他のプロトコルのスキャナ設定を追加または修正します。

これらの設定を設定する前に、次の項を参照してください。

- 異常検出しきい値とヒストグラムについて （12 ページ）
- 異常検出しきい値とヒストグラムの設定 （13 ページ）

ヒント 異常検出でワーム攻撃を探すために、ポートまたはプロトコルを追加する必要はありません。デフォルトで、すべてのポートとプロトコルが処理されます。特定の設定を設定する必要があるのは、特定のポートまたはプロトコルで検出をオフにする場合、またはデフォルト以外のしきい値またはヒストグラムが必要な場合だけです。

ナビゲーション パス

異常検出ポリシーの [内部ゾーン（Internal Zone）]、[不正ゾーン（Illegal Zone）] または [外部ゾーン（External Zone）] タブのサブタブである [TCPプロトコル（TCP Protocol）]、[UDPプロトコル（UDP Protocol）]、または [その他のプロトコル（Other Protocol）] で、[宛先ポートマップ（Destination Port Map）] テーブルまたは [プロトコル番号マップ（Protocol Number Map）] テーブルの下にある [行の追加（Add Row）] ボタンをクリックするか、行を選択して [行の編集（Edit Row）] ボタンをクリックします。ここで実行する必要のある手順の詳細については、異常検出しきい値とヒストグラムの設定 （13 ページ）を参照してください。

フィールド リファレンス

表 *2:* 宛先ポートまたはプロトコルマップのダイアログボックス

要素	説明
宛先ポート番号 （宛先ポートマップのダイアログボックスのみ）	デフォルト以外の値を定義する宛先ポート番号。指定できる範囲は 0 ～ 65535 です。 単一のポート番号を入力するか、単一のポート番号を含むポートリスト オブジェクトの名前を入力します。[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。
プロトコル番号 （[Add Protocol Map]/[Modify Protocol Map] ダイアログボックスのみ）	TCP/UDP 以外のプロトコルのプロトコル番号。プロトコル番号のリストについては、 http://www.ietf.org/rfc/rfc1700.txt [英語] で RFC 1700 を参照し、「Protocol Numbers」を検索してください。見出しを探します（この記事の執筆時点では2つ目の検索ヒット）。指定できる範囲は 0 ～ 255 です。 たとえば、ICMP はプロトコル 1 です。
[有効（Enabled）]	このサービスをイネーブルにするかどうか。サービスをイネーブルにしない場合、関連ポートまたはプロトコルは異常検出で処理されません。
[スキャナ設定のオーバーライド（Override Scanner Settings）]	このサービスまたはプロトコルのスキャナ設定を上書きするかどうか。ダイアログボックスの残りのフィールドをイネーブルにするには、このオプションを選択する必要があります。
Scanner Threshold	このポートまたはプロトコルのスキャナしきい値。範囲は 5 ～ 1000 です。デフォルトは 200 です。

要素	説明
[Threshold Histogram] テーブル	このポートまたはプロトコルのヒストグラム。このテーブルを空のままにした場合は、デフォルトのヒストグラムが使用されます。少数、中程度、多数の宛先アドレス用に、それぞれ異なるしきい値レベル（送信元アドレス）の最大 3 行を指定できます。 • しきい値を追加するには、[行の追加（Add Row）] ボタンをクリックし、[Histogram] ダイアログボックス （17 ページ）に入力します。すでに 3 行がある場合は、[Add] ボタンがディセーブルになります。 • しきい値を編集するには、しきい値を選択し、[行の編集（Edit Row）] ボタンをクリックします。宛先バケットは、テーブルにすでに定義されている宛先バケットには変更できません。 • しきい値を削除するには、しきい値を選択し、[行の削除（Delete Row）] ボタンをクリックします。テーブルに含まれていないバケットは、バケットのデフォルトのヒストグラムを使用します。

[Histogram] ダイアログボックス

[Histogram] ダイアログボックスを使用して、ヒストグラムのエントリを作成または修正します。作成または修正するヒストグラムによって、異常検出で生成されたデフォルトのヒストグラムが上書きされます。これらのヒストグラムの使用方法の詳細については、次の項を参照してください。

- 異常検出しきい値とヒストグラムについて （12 ページ）
- 異常検出しきい値とヒストグラムの設定 （13 ページ）

ナビゲーション パス

[Anomaly Detection] ポリシーで、次のいずれかを行います（ 異常検出の設定 （7 ページ）を参照）。

- [内部ゾーン（Internal Zone）]、[不正ゾーン（Illegal Zone）]、または [外部ゾーン（External Zone）] タブのサブタブである [TCP プロトコル（TCP Protocol）]、[UDP プロトコル（UDP Protocol）]、または [その他のプロトコル（Other Protocol）] で、[しきい値ヒストグラム（Threshold Histogram）] テーブルの行を選択して [行の編集（Edit Row）] ボタンをクリックします。
- [宛先またはプロトコルマップの追加（Add Dest or Protocol Map）] または [宛先またはプロトコルマップの変更（Modify Dest or Protocol Map）] ダイアログボックスで、[行の追加（Add Row）] ボタンをクリックするか、行を選択して [行の編集（Edit Row）] ボタンを選択します。マップ ダイアログボックスを開く方法については、[Add Dest Port Map]/[Modify

Dest Port Map] または [Add Protocol Map]/[Modify Protocol Map] ダイアログボックス （15 ページ）を参照してください。

フィールド リファレンス

表 3 : [Histogram] ダイアログボックス

要素	説明
[宛先 IP アドレス数（Number of Destination IP Addresses）]	定義しているヒストグラム バケット。バケットには、固定数の宛先アドレスがあります（低（5 アドレス）、中（20）、高（100））。 **ヒント** ヒストグラムには、宛先バケットごとに 1 つのエントリ（低、中、高）を含めることができます。このため、この値は、編集しているヒストグラムにすでに定義されている値には変更できません。
Number of Source IP Addresses	関連付けられた数の宛先アドレスを同時にスキャンすることを許可する送信元アドレスの数。目的の数値を入力します。 範囲は 0 ～ 4096 です。ヒストグラムを編集している場合は、現在の値が表示されます。

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。