CHAPTER 12

異常検出の設定

（注） IPS SSP を搭載した Cisco ASA 5585-X は、現在、Cisco IPS 7.1 をサポートする唯一のプラットフォームです。他の Cisco IPS センサーは、いずれも現在 IPS 7.1 をサポートしていません。

（注） IPS SSP を搭載した Cisco ASA 5585-X は、ASA 8.2(4.4) 以降および ASA 8.4(2) 以降でサポートされています。ASA 8.3(*x*) ではサポートされていません。

（注） AIP SSC-5 は異常検出をサポートしていません。

この章では、複数のセキュリティ ポリシーを作成し、個々の仮想センサーに適用する方法について説明します。内容は次のとおりです。

セキュリティ ポリシーの概要

（注） AIM IPS、AIP SSC-5、および NME IPS は、複数のポリシーの適用をサポートしていません。

複数のセキュリティ ポリシーを作成し、個々の仮想センサーに適用することができます。セキュリティ ポリシーは、シグニチャ定義ポリシー、イベント アクション規則ポリシー、および異常検出ポリシーで構成されます。Cisco IPS には、デフォルトのシグニチャ定義（sig0）、デフォルトのイベント アクション規則ポリシー（rules0）、およびデフォルトの異常検出ポリシー（ad0）が含まれています。仮想センサーにデフォルトのポリシーを割り当てることもできれば、新しいポリシーを作成することも可能です。複数のセキュリティ ポリシーを使用することにより、さまざまな要件に基づくセキュリティ ポリシーを作成し、そのカスタマイズしたポリシーを個々の VLAN または物理インターフェイスに適用できます。

異常検出コンポーネント

（注）　AIP SSC-5 は異常検出をサポートしていません。

ここでは、異常検出の各種コンポーネントについて説明します。内容は次のとおりです。

異常検出について

注意　異常検出は、トラフィックが両方向から来ることを前提としています。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。

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 アップデート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。

詳細情報

- ワームの動作の詳細については、「ワーム」（P.12-3）を参照してください。
- 異常検出をオフにする手順については、「異常検出のディセーブル化」（P.12-37）を参照してください。

ワーム

注意　異常検出は、トラフィックが両方向から来ることを前提としています。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。

ワームは、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 ワームは、プローブする IP アドレスのリストを生成することによって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。

異常検出は、スキャナとして動作していることを手がかりとして、ワームに感染したホストを特定します。ワームは、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 や UDP などのプロトコルを使用してインターネットやネットワークをスキャンし、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によって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 プロトコルにとって重要なイベントは、一定時間内に SYN-ACK 応答のない SYN パケットなどの未確立の接続です。TCP プロトコルを使用してスキャンする、ワームに感染したホストは、同じ宛先ポートにおいて異常な数の IP アドレスに対する未確立接続を生成します。

UDP プロトコルにとって重要なイベントは、すべてのパケットが一方向だけに送信される単方向接続（UDP 接続など）です。ワームに感染したホストが UDP プロトコルを使用してスキャンを行う場合、タイムアウト期間内に同じクワッド上で複数の宛先 IP アドレスについて同じ宛先ポートで UDP パケットを生成しますが、受信はしません。

それ以外のプロトコル（ICMP など）にとって重要なイベントは、送信元 IP アドレスから多くの異なる宛先 IP アドレスに送信されるイベント、つまり一方向でのみ受信されるパケットです。

注意　感染の標的とする IP アドレスのリストがワームにあり、自己増殖のためにスキャンする必要がない場合（能動的なスキャンとは逆にネットワークをリッスンする受動的なマッピングなど）、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することによってメーリング リストを受信し、そのリストにメールを送信するワームも検出されません。これは、レイヤ 3/ レイヤ 4 の異常が生成されからためです。

詳細情報

異常検出をオフにする手順については、「異常検出のディセーブル化」（P.12-37）を参照してください。

異常検出モード

異常検出は、最初に「正常時」学習プロセスを実行します。この処理の間にネットワークの正常な状態の大部分が異常検出に反映されます。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。

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

  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。異常検出は、ネットワーク トラフィックの初期ベースラインを作成します。これはナレッジ ベース（KB）と呼ばれます。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 KB が保存およびロードされ、24 時間後に初期 KB と置き換わることを意味します。

  （注）　異常検出は、空の初期 KB 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、KB が保存およびロードされ、異常検出も攻撃の検出を開始します。

  （注）　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。

- 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。KB が作成され、初期 KB と置き換えられると、異常検出はその KB に基づいて攻撃を検出します KB のしきい値に違反するネットワーク トラフィック フローを検知すると、アラートを送信します。異常検出は、異常を検出しながら、しきい値に違反しない段階的な変化を KB に記録して新しい KB を作成します。新しい KB が定期的に保存され、元の KB と置き換えられるため、KB は常に最新の状態に維持されます。

- 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動している場合など、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い場合、異常検出は初期 KB で動作を開始し、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 KB を置換するまで、攻撃を検出できません。最初の収集期間（デフォルトで 24 時間）が経過した後の最初の開始時刻（デフォルトでは午前 10:00）に、学習結果が新しい KB に保存され、この KB がロードされて初期 KB と置き換わります。異常検出はデフォルトで検出モードになっているため、新しい KB が用意できると、攻撃の検出を開始します。

詳細情報

- ワームの動作の詳細については、「ワーム」（P.12-3）を参照してください。
- センサーのモードを変更する手順については、「仮想センサーの追加、編集、削除」（P.8-13）を参照してください。

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。ゾーンには、内部、不正、外部の 3 つがあり、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。

詳細情報

ゾーンの設定の詳細については、「内部ゾーンの設定」（P.12-14）、「不正ゾーンの設定」（P.12-22）、および「不正ゾーンの設定」（P.12-22）を参照してください。

異常検出の設定手順

異常検出の検出部分を設定できます。しきい値のセットを設定し、学習によって KB に追加されたしきい値を上書きできます。ただし、異常検出は検出の設定に関係なく学習を継続します。KB をインポート、エクスポート、ロードできるほか、KB データを表示することもできます。

異常検出を設定するときには、次の手順に従ってください。

1. 仮想センサーに追加する異常検出ポリシーを作成します。デフォルトの異常検出ポリシー ad0 を使用することもできます。
2. 異常検出ポリシーを仮想センサーに追加します。
3. 異常検出ゾーンとプロトコルを設定します。
4. デフォルトでは、動作モードが検出に設定されていますが、最初の 24 時間は学習を実行し、KB のデータを作成します。初期 KB は空で、デフォルトの 24 時間の間に、異常検出が KB に取り込むデータを収集します。学習プロセスの時間をデフォルトの 24 時間よりも長くする場合は、モードを手動で学習受け入れモードに設定する必要があります。
5. センサーを最低でも 24 時間（デフォルト）、学習受け入れモードで動作させます。初期 KB 用にネットワークの正常な状態の情報を収集できるように、センサーを最低 24 時間、学習受け入れモードで動作させる必要があります。ただし、ネットワークの複雑さに応じて学習受け入れモードの時間を変更する必要があります。

（注） 最低 24 時間はセンサーを学習受け入れモードにしておくことを推奨しますが、それよりも長く（場合によっては 1 週間）学習受け入れモードで動作させると、さらによい結果が得られます。

この期間の後、センサーは初期 KB をネットワークの正常なアクティビティのベースラインとして保存します。

6. 異常検出を手動で学習受け入れモードに設定した場合は、検出モードに戻してください。
7. 異常検出パラメータを設定します。
   - ワームのタイムアウトと、異常検出がバイパスする送信元 IP アドレスおよび宛先 IP アドレスを設定します。このタイムアウトの後、スキャナしきい値は設定された値に戻ります。
   - 異常検出が検出モードのときに KB の自動更新をイネーブルにするかどうかを決定します。
   - デフォルトの Produce Alert 以外のイベント アクションも実行されるように、18 個の異常検出ワーム シグニチャを設定します。たとえば、Deny Attacker イベント アクションをシグニチャに設定します。

詳細情報

- 異常検出のモードを変更する手順については、「仮想センサーの追加、編集、削除」（P.8-13）を参照してください。
- 新しい異常検出ポリシーを設定する手順については、「異常検出ポリシーの設定」（P.12-8）を参照してください。
- ゾーンの設定の詳細については、「内部ゾーンの設定」（P.12-14）、「不正ゾーンの設定」（P.12-22）、および「不正ゾーンの設定」（P.12-22）を参照してください。
- 異常検出モードの詳細については、「異常検出モード」（P.12-4）を参照してください。
- 学習受け入れモードの設定の詳細については、「学習受け入れモードの設定」（P.12-11）を参照してください。
- 異常検出シグニチャの設定の詳細については、「異常検出シグニチャ」（P.12-6）を参照してください。
- Deny Attacker イベント アクションの詳細については、「イベント アクション」（P.11-8）を参照してください。

異常検出シグニチャ

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。アラートの重大度

次の異常検出イベント アクションが可能です。

- [Produce Alert]：イベントをイベント ストアに書き込みます。
- [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。
- [SNMP Trap]：SNMP 通知の実行要求を NotificationApp に送信します。
- [Request Block Host]：このホスト（攻撃者）をブロックする要求を ARC に送信します。

表 12-1 に、異常検出ワーム シグニチャを示します。

表 12-1　異常検出ワーム シグニチャ

シグニチャ 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	内部ゾーンでその他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。
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。

表 12-1　異常検出ワーム シグニチャ（続き）

シグニチャ ID	サブシグニチャ ID	名前	説明
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。

詳細情報

シグニチャにアクションを割り当てる手順については、「シグニチャへのアクションの割り当て」（P.9-19）を参照してください。

異常検出ポリシーの設定

ここでは、異常検出ポリシーを作成する方法について説明します。内容は次のとおりです。

[Anomaly Detections] ペイン

（注） 異常検出ポリシーを追加、クローニング、または削除するには、管理者またはオペレータであることが必要です。

注意 AIM IPS、AIP SSC-5、および NME IPS は、センサーの仮想化をサポートしていないため、複数のポリシーをサポートしません。

異常検出ポリシーを追加、クローニング、または削除するには、[Anomaly Detections] ペインを使用します。デフォルトの異常検出ポリシーは ad0 です。ポリシーを追加すると、センサーに制御トランザクションが送信され、新しいポリシー インスタンスが作成されます。応答が成功すると、[Anomaly Detections] に新しいポリシー インスタンスが追加されます。リソースの制限などにより、制御トランザクションが失敗した場合は、エラー メッセージが表示されます。

プラットフォームが仮想ポリシーをサポートしていない場合は、コンポーネントごとに 1 つのインスタンスしか追加できず、新しいインスタンスを作成したり既存のインスタンスを削除したりすることはできません。この場合、[Add]、[Clone]、および [Delete] ボタンは使用できません。

[Anomaly Detections] ペインのフィールド定義

[Anomaly Detections] ペインには次のフィールドがあります。

- [Policy Name]：異常検出ポリシーの名前を示します。
- [Assigned Virtual Sensor]：この異常検出ポリシーが割り当てられた仮想センサーを示します。

[Add Policy] および [Clone Policy] ダイアログボックスのフィールド定義

[Add Policy] および [Clone Policy] ダイアログボックスには次のフィールドがあります。

- [Policy Name]：異常検出ポリシーの名前を示します。

異常検出ポリシーの追加、クローニング、削除

異常検出ポリシーを追加、クローニング、または削除するには、次の手順を実行します。

ステップ 1　管理者権限またはオペレータ権限を持つアカウントを使用して IME にログインします。

ステップ 2　[Configuration] > *sensor_name* > [Policies] > [Anomaly Detections] を選択し、[Add] をクリックします。

ステップ 3　[Policy Name] フィールドに、異常検出ポリシーの名前を入力します。

ヒント　変更を破棄してダイアログボックスを閉じるには、[Cancel] をクリックします。

ステップ 4　[OK] をクリックします。[Anomaly Detections] ペインのリストに異常検出ポリシーが表示されます。

ステップ 5　既存の異常検出ポリシーをクローニングするには、リストで異常検出ポリシーを選択し、[Clone] をクリックします。[Clone Policy] ダイアログボックスが表示されます。既存の異常検出ポリシー名に「_copy」が追加されています。

ステップ 6　[Policy Name] フィールドに、一意の名前を入力します。

ヒント　変更を破棄してダイアログボックスを閉じるには、[Cancel] をクリックします。

ステップ 7　[OK] をクリックします。クローニングされた異常検出ポリシーが [Anomaly Detections] ペインに表示されます。

ステップ 8　異常検出ポリシーを削除するには、そのポリシーを選択し、[Delete] をクリックします。そのポリシーを完全に削除するかどうかを確認する [Delete Policy] ダイアログボックスが表示されます。

注意　デフォルトの異常検出ポリシーである ad0 は削除できません。

ステップ 9　[Yes] をクリックします。削除した異常検出ポリシーは、[Anomaly Detections] ペインのリストに表示されなくなります。

[ad0] ペイン

[ad0] ペイン（デフォルト）には、異常検出の設定ツールがあります。次の 5 つのタブがあります。

- [Operation Settings]：ワームのタイムアウトと、異常検出処理の実行中にセンサーが無視する送信元 IP アドレスおよび宛先 IP アドレスを設定できます。
- [Learning Accept Mode]：センサーによる学習 KB の自動受け入れと学習済み KB の受け入れスケジュールの設定をイネーブルにできます。
- [Internal Zone]：内部ゾーンの宛先 IP アドレスとしきい値を設定できます。
- [Illegal Zone]：不正ゾーンの宛先 IP アドレスとしきい値を設定できます。
- [External Zone]：外部ゾーンのしきい値を設定できます。

動作設定

ここでは、動作設定を行う方法について説明します。内容は次のとおりです。

- 「[Operation Settings] タブ」（P.12-10）
- 「[Operation Settings] タブのフィールド定義」（P.12-11）
- 「異常検出の動作設定」（P.12-11）

[Operation Settings] タブ

（注）　異常検出の動作設定を行うには、管理者またはオペレータであることが必要です。

[Operation Settings] タブでは、ワーム検出のタイムアウトを設定できます。このタイムアウトの後、スキャナしきい値は設定された値に戻ります。異常検出が KB の情報を収集するときにセンサーが無視する送信元 IP アドレスおよび宛先 IP アドレスも設定できます。異常検出は、これらの送信元 IP アドレスおよび宛先 IP アドレスを追跡せず、KB のしきい値はこれらの IP アドレスの影響を受けません。

[Operation Settings] タブのフィールド定義

[Operation Settings] タブには次のフィールドがあります。

- [Worm Timeout]：ワーム終了タイムアウトの時間を秒単位で設定できます。範囲は 120 ～ 10,000,000 秒です。デフォルトは 600 秒です。
- [Configure IP address ranges to ignore during anomaly detection processing]：異常検出の処理中に無視する IP アドレスを入力します。
  - [Enable ignored IP Addresses]：オンにすると、無視された IP アドレスのリストがイネーブルになります。
  - [Source IP Addresses]：異常検出で無視する送信元 IP アドレスを入力します。
  - [Destination IP Addresses]：異常検出で無視する宛先 IP アドレスを入力します。

異常検出の動作設定

異常検出の動作設定を行うには、次の手順を実行します。

ステップ 1　管理者権限またはオペレータ権限を持つアカウントを使用して IME にログインします。

ステップ 2　[Configuration] > *sensor_name* > [Policies] > [Anomaly Detections] > [ad0] > [Operation Settings] を選択します。

ステップ 3　[Worm Timeout] フィールドに、ワーム検出がタイムアウトになるまでの時間を秒単位で入力します。範囲は 120 ～ 10,000,000 秒です。デフォルトは 600 秒です。

ステップ 4　無視された IP アドレスのリストをイネーブルにするには、[Enable ignored IP Addresses] チェックボックスをオンにします。

（注）　[Enable ignored IP Addresses] チェックボックスをオンにしなければ、入力した IP アドレスはすべて無視されません。

ステップ 5　[Source IP Addresses] フィールドに、異常検出で無視する送信元 IP アドレスまたはアドレスの範囲を入力します。有効な形式は 10.10.5.5,10.10.2.1-10.10.2.30 です。

ステップ 6　[Destination IP Addresses] フィールドに、異常検出で無視する宛先 IP アドレスまたはアドレスの範囲を入力します。

ヒント　変更を破棄するには、[Reset] をクリックします。

ステップ 7　変更を適用し、変更後の設定を保存するには、[Apply] をクリックします。

学習受け入れモードの設定

ここでは、学習受け入れモードの設定方法について説明します。内容は次のとおりです。

- 「[Learning Accept Mode] タブ」（P.12-12）
- 「KB とヒストグラム」（P.12-12）

- 「[Learning Accept Mode] タブのフィールド定義」（P.12-13）
- 「[Add Start Time] および [Edit Start Time] ダイアログボックスのフィールド定義」（P.12-13）
- 「学習受け入れモードの設定」（P.12-13）

[Learning Accept Mode] タブ

（注）　学習受け入れモードを設定するには、管理者またはオペレータであることが必要です。

[Learning Accept Mode] タブでは、センサーが一定時間ごとに新しい KB を作成するかどうかを設定します。KB を作成し、ロード（[Rotate]）するか保存（[Save Only]）するかを設定できます。KB のロードまたは保存の頻度と時期を設定できます。生成されたファイルのデフォルト名は *YYYY-Mon-dd-hh_mm_ss* です。*Mon* は、当月の 3 文字の省略形です。

KB とヒストグラム

KB はツリー構造になっており、次の情報が含まれています。

- KB 名
- ゾーン名
- Protocol
- サービス

KB には、スキャナしきい値とヒストグラムがサービスごとに保存されます。学習受け入れモードを自動に設定し、アクションを [Rotate] に設定した場合、新しい KB は 24 時間ごとに作成され、作成後 24 時間にわたり使用されます。学習受け入れモードを自動に設定し、アクションを [Save Only] に設定すると、新しい KB は作成されますが、現在の KB 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、KB は作成されません。

（注）　学習受け入れモードでは、センサーのローカル時刻が使用されます。

スキャナしきい値は、1 つの送信元 IP アドレスがスキャンできるゾーン IP アドレスの最大数を定義します。ヒストグラムしきい値は、指定された数を超えるゾーン IP アドレスをスキャンできる送信元 IP アドレスの最大数を定義します。

異常検出は、攻撃が行われていない状態で学習したヒストグラムからの逸脱を発見した場合（つまり、定義されている数を超えるゾーン宛先 IP アドレスを同時にスキャンする送信元 IP アドレスの数が超過した場合）、ワーム攻撃と認識します。たとえば、ポート 445 に対するスキャンしきい値が 300 の場合、異常検出は、350 個のゾーン宛先 IP アドレスをスキャンするスキャナを検出すると、マス スキャナが検出されたことを示すアクションを生成します。ただし、このスキャナでは、ワーム攻撃が進行中かどうかはまだ確認されていません。表 12-2 で、この例について説明します。

表 12-2　ヒストグラムの例

送信元 IP アドレス数	10	5	2
宛先 IP アドレス数	5	20	100

異常検出は、ポート 445 で 50 を超えるゾーン宛先 IP アドレスを同時にスキャンする送信元 IP アドレスを 6 つ検出すると、ポート 445 でワーム攻撃が検出されたことを示す、送信元 IP アドレスの指定がないアクションを作成します。動的なフィルタしきい値の 50 が新しい内部スキャンしきい値となり、それにより異常検出はスキャナのしきい値定義を引き下げます。その結果、異常検出は、新しいスキャンしきい値（50）を超えてスキャンする送信元 IP アドレスごとに追加の動的フィルタを作成します。

KB が学習した内容を異常検出ポリシーまたはゾーンごとにオーバーライドできます。ネットワーク トラフィックの詳細が判明している場合は、偽陽性を制限するためにオーバーライドを使用する必要が生じることもあります。

[Learning Accept Mode] タブのフィールド定義

[Learning Accept Mode] タブには次のフィールドがあります。

- [Automatically accept learning knowledge base]：オンにすると、センサーが自動的に KB をアップデートします。オンにしない場合、異常検出は新しい KB を作成しません。
- [Action]：KB を循環させるか保存するかを指定できます。[Save Only] を選択すると、新しい KB が作成されます。作成された KB を調べ、異常検出にロードするかどうかを決定できます。[Rotate] を選択した場合は、定義したスケジュールに従って新しい KB が作成され、ロードされます。
- [Schedule]：[Calendar Schedule] または [Periodic Schedule] を選択できます。
  - [Periodic Schedule]：最初の学習スナップショットの日時と、それ以降のスナップショットの間隔を設定できます。デフォルトは、24 時間形式での定期スケジュールです。
  - [Start Time]：新しい KB を開始する時刻を入力します。有効な形式は hh:mm:ss です。
  - [Learning Interval]：異常検出が新しい KB を作成する前にネットワークから学習する時間を入力します。
  - [Calendar Schedule]：KB を作成する日時を設定できます。
  - [Times of Day]：[Add] をクリックし、[Add Start Time] ダイアログボックスに日時を入力します。
  - [Days of the Week]：設定する曜日のチェックボックスをオンにします。

[Add Start Time] および [Edit Start Time] ダイアログボックスのフィールド定義

[Add Start Time] および [Edit Start Time] ダイアログボックスには次のフィールドがあります。

- [Start Time]：学習受け入れモードの開始時刻として、時、分、秒を入力します。有効な形式は、24 時間形式の hh:mm:ss です。

学習受け入れモードの設定

異常検出の学習受け入れモードを設定するには、次の手順を実行します。

ステップ 1　管理者権限またはオペレータ権限を持つアカウントを使用して IME にログインします。

ステップ 2　[Configuration] > *sensor_name* > [Policies] > [Anomaly Detections] > [ad0] > [Learning Accept Mode] を選択します。

ステップ 3　異常検出が KB を自動的にアップデートするように設定するには、[Automatically accept learning knowledge base] チェックボックスをオンにします。

ステップ 4　[Action] ドロップダウン リストから、次のいずれかのアクション タイプを選択します。

- [Rotate]：新しい KB が作成され、ロードされます。これがデフォルトです。
- [Save Only]：新しい KB が作成されますが、ロードされません。作成された KB を表示し、ロードするかどうかを決定できます。

ステップ 5　[Schedule] ドロップダウン リストから、次のいずれかのスケジュール タイプを選択します。

- [Calendar Schedule]：ステップ 6 に進みます。
- [Periodic Schedule]：ステップ 7 に進みます。

ステップ 6　次の手順でスケジュールを設定します。

a. [Add] をクリックして開始時刻を追加します。

b. 開始時刻の時、分、秒を 24 時間形式で入力します。

ヒント　変更を破棄して [Add Start Time] ダイアログボックスを閉じるには、[Cancel] をクリックします。

c. [OK] をクリックします。

d. [Days of the Week] フィールドで、異常検出モジュールによって KB スナップショットをキャプチャする曜日のチェックボックスをオンにします。

ステップ 7　次の手順で定期スケジュール（デフォルト）を設定します。

a. [Start Time] フィールドに、開始時刻の時、分、秒を 24 時間形式で入力します。

b. [Learning Interval] フィールドに、以降の KB スナップショットの間隔を入力します。

ヒント　変更を破棄するには、[Reset] をクリックします。

ステップ 8　変更を適用し、変更後の設定を保存するには、[Apply] をクリックします。

内部ゾーンの設定

ここでは、内部ゾーンの設定方法について説明します。内容は次のとおりです。

- 「[Add Protocol Number] および [Edit Protocol Number] ダイアログボックスのフィールド定義」（P.12-18）
- 「内部ゾーンの設定」（P.12-18）

[Internal Zone] タブ

（注）　内部ゾーンを設定するには、管理者またはオペレータであることが必要です。

[Internal Zone] タブには、次の 4 つのタブがあります。

- [General]：内部ゾーンをイネーブルにし、内部ゾーンに含めるサブネットを設定します。
- [TCP Protocol]：TCP プロトコルをイネーブルにし、独自のしきい値とヒストグラムを設定できます。
- [UDP Protocol]：UDP プロトコルをイネーブルにし、独自のしきい値とヒストグラムを設定できます。
- [Other Protocols]：その他のプロトコルをイネーブルにし、独自のしきい値とヒストグラムを設定できます。

内部ゾーンは、内部ネットワークを表している必要があります。また、内部ネットワークの IP アドレス範囲を宛先とするトラフィックをすべて受信する必要があります。

[General] タブ

[General] タブでは、ゾーンをイネーブルにします。ゾーンがディセーブルである場合、そのゾーンを宛先とするパケットは無視されます。ゾーンはデフォルトでイネーブルになります。

次に、このゾーンに属する IP アドレスを追加します。すべてのゾーンに IP アドレスを設定しなければ、すべてのパケットがデフォルト ゾーンである外部ゾーンに送信されます。

フィールド定義

[General] タブには次のフィールドがあります。

- [Enable the Internal Zone]：オンにすると、内部ゾーンがイネーブルになります。
- [Service Subnets]：内部ゾーンに適用するサブネットを入力します。有効な形式は 10.10.5.5,10.10.2.1-10.10.2.30 です。

[TCP Protocol] タブ

[TCP Protocol] タブでは、内部ゾーンの TCP プロトコルをイネーブルまたはディセーブルにします。TCP プロトコルの宛先ポートを設定できます。デフォルトのしきい値を使用することもできれば、スキャナ設定をオーバーライドし、独自のしきい値とヒストグラムを追加することもできます。

フィールド定義

[TCP Protocol] タブには次のフィールドがあります。

- [Enable the TCP Protocol]：オンにすると、TCP プロトコルがイネーブルになります。
- [Destination Port Map] タブ：TCP プロトコルに特定のポートを関連付けることができます。

  - [Port Number]：設定されているポート番号が表示されます。
  - [Service Enabled]：サービスがイネーブルであるかどうか。
  - [Scanner Overridden]：スキャナがオーバーライドされているかどうか。
  - [Overridden Scanner Settings]：設定されているスキャナ設定が表示されます。
  - [Threshold]：しきい値の設定が表示されます。
  - [Histogram]：設定されているヒストグラムが表示されます。
- [Default Thresholds] タブ：デフォルトのしきい値とヒストグラムが表示されます。デフォルトのしきい値は、KB に含まれず設定によってオーバーライドされていないサービスに使用されます。
  - [Scanner Threshold]：スキャナしきい値を変更できます。
  - [Threshold Histogram]：デフォルトのしきい値ヒストグラムが表示されます。
  - [Number of Destination IP Addresses]：低、中、高にグループ化された宛先 IP アドレスの数が表示されます。
  - [Number of Source IP Addresses]：宛先 IP アドレスの各グループに関連付けられた送信元 IP アドレスの数が表示されます。

[Add Destination Port] および [Edit Destination Port] ダイアログボックスのフィールド定義

[Add Destination Port] および [Edit Destination Port] ダイアログボックスには次のフィールドがあります。

- [Destination Port number]：宛先ポート番号を入力します。有効な範囲は 0 ～ 65535 です。
- [Enable the Service]：オンにすると、サービスがイネーブルになります。
- [Override Scanner Settings]：オンにすると、デフォルトのスキャナ設定がオーバーライドされ、すべてのヒストグラムを追加、編集、削除、および選択できます。
- [Scanner Threshold]：スキャナしきい値を設定できます。有効な範囲は 5 ～ 1000 です。デフォルトは 100 です。
- [Threshold Histogram]：追加したヒストグラムが表示されます。
  - [Number of Destination IP Addresses]：追加した宛先 IP アドレスの数が表示されます。
  - [Number of Source IP Addresses]：追加した送信元 IP アドレスの数が表示されます。

[Add Histogram] および [Edit Histogram] ダイアログボックスのフィールド定義

[Add Histogram] および [Edit Histogram] ダイアログボックスには次のフィールドがあります。

- [Number of Destination IP Addresses]：低、中、高の各グループの宛先 IP アドレス数を追加できます。宛先 IP アドレス数は、低が 5、中が 20、高が 100 です。
- [Number of Source IP Addresses]：送信元 IP アドレスの数を追加できます。有効な範囲は 0 ～ 4096 です。

[UDP Protocol] タブ

[UDP Protocol] タブでは、内部ゾーンの UDP プロトコルをイネーブルまたはディセーブルにします。UDP プロトコルの宛先ポートを設定できます。デフォルトのしきい値を使用することもできれば、スキャナ設定をオーバーライドし、独自のしきい値とヒストグラムを追加することもできます。

フィールド定義

[UDP Protocol] タブには次のフィールドがあります。

- [Enable the UDP Protocol]：オンにすると、UDP プロトコルがイネーブルになります。
- [Destination Port Map] タブ：UDP プロトコルに特定のポートを関連付けることができます。
  - [Port Number]：設定されているポート番号が表示されます。
  - [Service Enabled]：サービスがイネーブルであるかどうか。
  - [Scanner Overridden]：スキャナがオーバーライドされているかどうか。
  - [Overridden Scanner Settings]：設定されているスキャナ設定が表示されます。
  - [Threshold]：しきい値の設定が表示されます。
  - [Histogram]：設定されているヒストグラムが表示されます。
- [Default Thresholds] タブ：デフォルトのしきい値とヒストグラムが表示されます。
  - [Scanner Threshold]：スキャナしきい値を変更できます。
  - [Threshold Histogram]：デフォルトのしきい値ヒストグラムが表示されます。
  - [Number of Destination IP Addresses]：低、中、高にグループ化された宛先 IP アドレスの数が表示されます。
  - [Number of Source IP Addresses]：宛先 IP アドレスの各グループに関連付けられた送信元 IP アドレスの数が表示されます。

[Other Protocols] タブ

[Other Protocols] タブでは、内部ゾーンのその他のプロトコルをイネーブルまたはディセーブルにします。その他のプロトコルのプロトコル番号マップを設定できます。デフォルトのしきい値を使用することもできれば、スキャナ設定をオーバーライドし、独自のしきい値とヒストグラムを追加することもできます。

フィールドの説明

[Other Protocols] タブには次のフィールドがあります。

- [Enable Other Protocols]：オンにすると、その他のプロトコルがイネーブルになります。
- [Protocol Number Map] タブ：その他のプロトコルに特定のプロトコル番号を関連付けることができます。
  - [Protocol Number]：設定されているプロトコル番号が表示されます。
  - [Service Enabled]：サービスがイネーブルであるかどうか。
  - [Scanner Overridden]：スキャナがオーバーライドされているかどうか。
  - [Overridden Scanner Settings]：設定されているスキャナ設定が表示されます。
  - [Threshold]：しきい値の設定が表示されます。
  - [Histogram]：設定されているヒストグラムが表示されます。

- [Default Thresholds] タブ：デフォルトのしきい値とヒストグラムが表示されます。
  - [Scanner Threshold]：スキャナしきい値を変更できます。
  - [Threshold Histogram]：デフォルトのしきい値ヒストグラムが表示されます。
  - [Number of Destination IP Addresses]：低、中、高にグループ化された宛先 IP アドレスの数が表示されます。
  - [Number of Source IP Addresses]：宛先 IP アドレスの各グループに関連付けられた送信元 IP アドレスの数が表示されます。

[Add Protocol Number] および [Edit Protocol Number] ダイアログボックスのフィールド定義

[Add Protocol Number] および [Edit Protocol Number] ダイアログボックスには次のフィールドがあります。

- [Protocol number]：プロトコル番号を入力します。
- [Enable the Service]：サービスをイネーブルにできます。
- [Override Scanner Settings]：オンにすると、すべてのヒストグラムを追加、編集、削除、および選択できます。
- [Scanner Threshold]：スキャナしきい値を設定できます。有効な範囲は 5 ～ 1000 です。デフォルトは 100 です。
- [Threshold Histogram]：追加したヒストグラムが表示されます。
  - [Number of Destination IP Addresses]：追加した宛先 IP アドレスの数が表示されます。
  - [Number of Source IP Addresses]：追加した送信元 IP アドレスの数が表示されます。

内部ゾーンの設定

内部ゾーンを異常検出用に設定するには、次の手順を実行します。

ステップ 1　管理者権限またはオペレータ権限を持つアカウントを使用して IME にログインします。

ステップ 2　[Configuration] > *sensor_name* > [Policies] > [Anomaly Detections] > [ad0] > [Internal Zone] を選択し、[General] タブをクリックします。

ステップ 3　内部ゾーンをイネーブルにするには、[Enable the Internal Zone] チェックボックスをオンにします。

（注）　[Enable the Internal Zone] チェックボックスをオンにしなければ、設定したプロトコルは無視されます。

ステップ 4　[Service Subnets] フィールドに、内部ゾーンを適用するサブネットを入力します。有効な形式は 10.10.5.5,10.10.2.1-10.10.2.30 です。

ステップ 5　TCP プロトコルを設定するには、[TCP Protocol] タブをクリックします。

ステップ 6　TCP プロトコルをイネーブルにするには、[Enable the TCP Protocol] チェックボックスをオンにします。

（注）　[Enable the TCP Protocol] チェックボックスをオンにしなければ、TCP プロトコルの設定は無視されます。

ステップ 7　[Destination Port Map] タブをクリックし、[Add] をクリックして、宛先ポートを追加します。

ステップ 8　[Destination Port Number] フィールドに宛先ポート番号を入力します。有効な範囲は 0 ～ 65535 です。

ステップ 9　内部ゾーンをイネーブルにするには、[Enable the Service] チェックボックスをオンにします。

ステップ 10　そのポートのスキャナ値をオーバーライドするには、[Override Scanner Settings] チェックボックスをオンにします。デフォルトのスキャナ値を使用することもできれば、デフォルト値をオーバーライドし、独自のスキャナ値を設定することもできます。

ステップ 11　新しいスキャナ設定のヒストグラムを追加するには、[Add] をクリックします。

ステップ 12　[Number of Destination IP Addresses] ドロップダウン リストから値（[High]、[Medium]、または [Low]）を選択します。

ステップ 13　[Number of Source IP Addresses] フィールドに、このヒストグラムに関連付ける送信元 IP アドレスの数を入力します。有効な範囲は 0 ～ 4096 です。

ヒント　変更を破棄して [Add Histogram] ダイアログボックスを閉じるには、[Cancel] をクリックします。

ステップ 14　[OK] をクリックします。[Add Destination Port] ダイアログボックスのリストに新しいスキャナ設定が表示されます。

ヒント　変更を破棄して [Add Destination Port] ダイアログボックスを閉じるには、[Cancel] をクリックします。

ステップ 15　[OK] をクリックします。[Destination Port Map] タブのリストに新しい宛先ポート マップが表示されます。

ステップ 16　宛先ポート マップを編集するには、リストで宛先ポート マップを選択し、[Edit] をクリックします。

ステップ 17　フィールドに変更を加え、[OK] をクリックします。[Destination Port Map] タブのリストに編集済みの宛先ポート マップが表示されます。

ステップ 18　宛先ポート マップを削除するには、その宛先ポート マップを選択し、[Delete] をクリックします。その宛先ポート マップは、[Destination Port Map] タブのリストに表示されなくなります。

ステップ 19　デフォルトのしきい値を編集するには、[Default Thresholds] タブをクリックします。

ステップ 20　編集するしきい値ヒストグラムを選択し、[Edit] をクリックします。

ステップ 21　[Number of Destination IP Addresses] ドロップダウン リストから別の値（[High]、[Medium]、または [Low]）を選択します。

ステップ 22　[Number of Source IP Addresses] フィールドで、このヒストグラムに関連付ける送信元 IP アドレスの数を編集します。有効な範囲は 0 ～ 4096 です。[Default Thresholds] タブのリストに編集済みのしきい値ヒストグラムが表示されます。

ヒント　変更を破棄して [Edit Histogram] ダイアログボックスを閉じるには、[Cancel] をクリックします。

ステップ 23　UDP プロトコルを設定するには、[UDP Protocol] タブをクリックします。

ステップ 24　UDP プロトコルをイネーブルにするには、[Enable the UDP Protocol] チェックボックスをオンにします。

（注）　[Enable the UDP Protocol] チェックボックスをオンにしなければ、UDP プロトコルの設定は無視されます。

ステップ 25　[Destination Port Map] タブをクリックし、[Add] をクリックして、宛先ポートを追加します。

ステップ 26　[Destination Port Number] フィールドに宛先ポート番号を入力します。有効な範囲は 0 ～ 65535 です。

ステップ 27　内部ゾーンをイネーブルにするには、[Enable the Service] チェックボックスをオンにします。

ステップ 28　そのポートのスキャナ値をオーバーライドするには、[Override Scanner Settings] チェックボックスをオンにします。デフォルトのスキャナ値を使用することもできれば、デフォルト値をオーバーライドし、独自のスキャナ値を設定することもできます。

ステップ 29　新しいスキャナ設定のヒストグラムを追加するには、[Add] をクリックします。

ステップ 30　[Number of Destination IP Addresses] ドロップダウン リストから値（[High]、[Medium]、または [Low]）を選択します。

ステップ 31　[Number of Source IP Addresses] フィールドに、このヒストグラムに関連付ける送信元 IP アドレスの数を入力します。有効な範囲は 0 ～ 4096 です。

ヒント　変更を破棄して [Add Histogram] ダイアログボックスを閉じるには、[Cancel] をクリックします。

ステップ 32　[OK] をクリックします。[Add Destination Port] ダイアログボックスのリストに新しいスキャナ設定が表示されます。

ヒント　変更を破棄して [Add Destination Port] ダイアログボックスを閉じるには、[Cancel] をクリックします。

ステップ 33　[OK] をクリックします。[Destination Port Map] タブのリストに新しい宛先ポート マップが表示されます。

ステップ 34　宛先ポート マップを編集するには、リストで宛先ポート マップを選択し、[Edit] をクリックします。

ステップ 35　フィールドに変更を加え、[OK] をクリックします。[Destination Port Map] タブのリストに編集済みの宛先ポート マップが表示されます。

ステップ 36　宛先ポート マップを削除するには、その宛先ポート マップを選択し、[Delete] をクリックします。その宛先ポート マップは、[Destination Port Map] タブのリストに表示されなくなります。

ステップ 37　デフォルトのしきい値を編集するには、[Default Thresholds] タブをクリックし、編集するしきい値ヒストグラムを選択して、[Edit] をクリックします。

ステップ 38　[Number of Destination IP Addresses] ドロップダウン リストから別の値（[High]、[Medium]、または [Low]）を選択します。

ステップ 39　[Number of Source IP Addresses] フィールドで、このヒストグラムに関連付ける送信元 IP アドレスの数を編集します。有効な範囲は 0 ～ 4096 です。[Default Thresholds] タブのリストに編集済みのしきい値ヒストグラムが表示されます。

ヒント 変更を破棄して [Edit Histogram] ダイアログボックスを閉じるには、[Cancel] をクリックします。

ステップ 40 その他のプロトコルを設定するには、[Other Protocols] タブをクリックします。

ステップ 41 その他のプロトコルをイネーブルにするには、[Enable Other Protocols] チェックボックスをオンにします。

（注） [Enable Other Protocols] チェックボックスをオンにしなければ、その他のプロトコルの設定は無視されます。

ステップ 42 [Protocol Number Map] タブをクリックし、[Add] をクリックして、プロトコル番号を追加します。

ステップ 43 [Protocol Number] フィールドにプロトコル番号を入力します。有効な範囲は 0 ～ 255 です。

ステップ 44 そのプロトコルのサービスをイネーブルにするには、[Enable the Service] チェックボックスをオンにします。

ステップ 45 そのプロトコルのスキャナ値をオーバーライドするには、[Override Scanner Settings] チェックボックスをオンにします。デフォルトのスキャナ値を使用することもできれば、デフォルト値をオーバーライドし、独自のスキャナ値を設定することもできます。

ステップ 46 新しいスキャナ設定のヒストグラムを追加するには、[Add] をクリックします。

ステップ 47 [Number of Destination IP Addresses] ドロップダウン リストから値（[High]、[Medium]、または [Low]）を選択します。

ステップ 48 [Number of Source IP Addresses] フィールドに、このヒストグラムに関連付ける送信元 IP アドレスの数を入力します。有効な範囲は 0 ～ 4096 です。

ヒント 変更を破棄して [Add Histogram] ダイアログボックスを閉じるには、[Cancel] をクリックします。

ステップ 49 [OK] をクリックします。[Add Protocol Number] ダイアログボックスのリストに新しいスキャナ設定が表示されます。

ヒント 変更を破棄して [Add Protocol Number] ダイアログボックスを閉じるには、[Cancel] をクリックします。

ステップ 50 [OK] をクリックします。[Protocol Number Map] タブのリストに新しいプロトコル番号が表示されます。

ステップ 51 プロトコル番号マップを編集するには、リストでプロトコル番号マップを選択し、[Edit] をクリックします。

ステップ 52 フィールドに変更を加え、[OK] をクリックします。[Protocol Number Map] タブのリストに編集済みのプロトコル番号マップが表示されます。

ステップ 53 プロトコル番号マップを削除するには、そのプロトコル番号マップを選択し、[Delete] をクリックします。そのプロトコル番号マップは、[Protocol Number Map] タブのリストに表示されなくなります。

ステップ 54 デフォルトのしきい値を編集するには、[Default Thresholds] タブをクリックし、編集するしきい値ヒストグラムを選択して、[Edit] をクリックします。

ステップ 55　[Number of Destination IP Addresses] ドロップダウン リストから別の値（[High]、[Medium]、または [Low]）を選択します。

ステップ 56　[Number of Source IP Addresses] フィールドで、このヒストグラムに関連付ける送信元 IP アドレスの数を編集します。有効な範囲は 0 ～ 4096 です。[Default Thresholds] タブのリストに編集済みのしきい値ヒストグラムが表示されます。

ヒント　変更を破棄して [Edit Histogram] ダイアログボックスを閉じるには、[Cancel] をクリックします。

ヒント　変更を破棄するには、[Reset] をクリックします。

ステップ 57　変更を適用し、変更後の設定を保存するには、[Apply] をクリックします。

不正ゾーンの設定

ここでは、不正ゾーンの設定方法について説明します。内容は次のとおりです。

[Illegal Zone] タブ

（注）　不正ゾーンを設定するには、管理者またはオペレータであることが必要です。

[Illegal Zone] タブには、次の 4 つのタブがあります。

- [General]：不正ゾーンをイネーブルにし、内部ゾーンに含めるサブネットを指定します。
- [TCP Protocol]：TCP プロトコルをイネーブルにし、独自のしきい値とヒストグラムを設定できます。
- [UDP Protocol]：UDP プロトコルをイネーブルにし、独自のしきい値とヒストグラムを設定できます。

- [Other Protocols]：その他のプロトコルをイネーブルにし、独自のしきい値とヒストグラムを設定できます。

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。

[General] タブ

[General] タブでは、ゾーンをイネーブルにします。ゾーンがディセーブルである場合、そのゾーンを宛先とするパケットは無視されます。ゾーンはデフォルトでイネーブルになります。

次に、このゾーンに属する IP アドレスを追加します。すべてのゾーンに IP アドレスを設定しなければ、すべてのパケットがデフォルト ゾーンである外部ゾーンに送信されます。

フィールドの説明

[General] タブには次のフィールドがあります。

- [Enable the Internal Zone]：オンにすると、内部ゾーンがイネーブルになります。
- [Service Subnets]：内部ゾーンに適用するサブネットを入力します。有効な形式は 10.10.5.5,10.10.2.1-10.10.2.30 です。

[TCP Protocol] タブ

[TCP Protocol] タブでは、不正ゾーンの TCP プロトコルをイネーブルまたはディセーブルにします。TCP プロトコルの宛先ポートを設定できます。デフォルトのしきい値を使用することもできれば、スキャナ設定をオーバーライドし、独自のしきい値とヒストグラムを追加することもできます。

フィールドの説明

[TCP Protocol] タブには次のフィールドがあります。

- [Enable the TCP Protocol]：オンにすると、TCP プロトコルがイネーブルになります。
- [Destination Port Map] タブ：TCP プロトコルに特定のポートを関連付けることができます。
  - [Port Number]：設定されているポート番号が表示されます。
  - [Service Enabled]：サービスがイネーブルであるかどうか。
  - [Scanner Overridden]：スキャナがオーバーライドされているかどうか。
  - [Overridden Scanner Settings]：設定されているスキャナ設定が表示されます。
  - [Threshold]：しきい値の設定が表示されます。
  - [Histogram]：設定されているヒストグラムが表示されます。
- [Default Thresholds] タブ：デフォルトのしきい値とヒストグラムが表示されます。デフォルトのしきい値は、KB に含まれず設定によってオーバーライドされていないサービスに使用されます。
  - [Scanner Threshold]：スキャナしきい値を変更できます。
  - [Threshold Histogram]：デフォルトのしきい値ヒストグラムが表示されます。
  - [Number of Destination IP Addresses]：低、中、高にグループ化された宛先 IP アドレスの数が表示されます。
  - [Number of Source IP Addresses]：宛先 IP アドレスの各グループに関連付けられた送信元 IP アドレスの数が表示されます。

[Add Destination Port] および [Edit Destination Port] ダイアログボックスのフィールド定義

[Add Destination Port] および [Edit Destination Port] ダイアログボックスには次のフィールドがあります。

- [Destination Port number]：宛先ポート番号を入力します。有効な範囲は 0 ～ 65535 です。
- [Enable the Service]：オンにすると、サービスがイネーブルになります。
- [Override Scanner Settings]：オンにすると、デフォルトのスキャナ設定がオーバーライドされ、すべてのヒストグラムを追加、編集、削除、および選択できます。
- [Scanner Threshold]：スキャナしきい値を設定できます。有効な範囲は 5 ～ 1000 です。デフォルトは 100 です。
- [Threshold Histogram]：追加したヒストグラムが表示されます。
  - [Number of Destination IP Addresses]：追加した宛先 IP アドレスの数が表示されます。
  - [Number of Source IP Addresses]：追加した送信元 IP アドレスの数が表示されます。

[Add Histogram] および [Edit Histogram] ダイアログボックスのフィールド定義

[Add Histogram] および [Edit Histogram] ダイアログボックスには次のフィールドがあります。

- [Number of Destination IP Addresses]：低、中、高の各グループの宛先 IP アドレス数を追加できます。宛先 IP アドレス数は、低が 5、中が 20、高が 100 です。
- [Number of Source IP Addresses]：送信元 IP アドレスの数を追加できます。有効な範囲は 0 ～ 4096 です。

[UDP Protocol] タブ

[UDP Protocol] タブでは、不正ゾーンの UDP プロトコルをイネーブルまたはディセーブルにします。UDP プロトコルの宛先ポートを設定できます。デフォルトのしきい値を使用することもできれば、スキャナ設定をオーバーライドし、独自のしきい値とヒストグラムを追加することもできます。

フィールドの説明

[UDP Protocol] タブには次のフィールドがあります。

- [Enable the UDP Protocol]：オンにすると、UDP プロトコルがイネーブルになります。
- [Destination Port Map] タブ：UDP プロトコルに特定のポートを関連付けることができます。
  - [Port Number]：設定されているポート番号が表示されます。
  - [Service Enabled]：サービスがイネーブルであるかどうか。
  - [Scanner Overridden]：スキャナがオーバーライドされているかどうか。
  - [Overridden Scanner Settings]：設定されているスキャナ設定が表示されます。
  - [Threshold]：しきい値の設定が表示されます。
  - [Histogram]：設定されているヒストグラムが表示されます。

- [Default Thresholds] タブ：デフォルトのしきい値とヒストグラムが表示されます。
  - [Scanner Threshold]：スキャナしきい値を変更できます。
  - [Threshold Histogram]：デフォルトのしきい値ヒストグラムが表示されます。
  - [Number of Destination IP Addresses] : 低、中、高にグループ化された宛先 IP アドレスの数が表示されます。
  - [Number of Source IP Addresses]：宛先 IP アドレスの各グループに関連付けられた送信元 IP アドレスの数が表示されます。

[Other Protocols] タブ

[Other Protocols] タブでは、不正ゾーンのその他のプロトコルをイネーブルまたはディセーブルにします。その他のプロトコルのプロトコル番号マップを設定できます。デフォルトのしきい値を使用することもできれば、スキャナ設定をオーバーライドし、独自のしきい値とヒストグラムを追加することもできます。

フィールドの説明

[Other Protocols] タブには次のフィールドがあります。

- [Enable Other Protocols]：オンにすると、その他のプロトコルがイネーブルになります。
- [Protocol Number Map] タブ：その他のプロトコルに特定のプロトコル番号を関連付けることができます。
  - [Protocol Number]：設定されているプロトコル番号が表示されます。
  - [Service Enabled]：サービスがイネーブルであるかどうか。
  - [Scanner Overridden]：スキャナがオーバーライドされているかどうか。
  - [Overridden Scanner Settings]：設定されているスキャナ設定が表示されます。
  - [Threshold]：しきい値の設定が表示されます。
  - [Histogram]：設定されているヒストグラムが表示されます。
- [Default Thresholds] タブ：デフォルトのしきい値とヒストグラムが表示されます。
  - [Scanner Threshold]：スキャナしきい値を変更できます。
  - [Threshold Histogram]：デフォルトのしきい値ヒストグラムが表示されます。
  - [Number of Destination IP Addresses] : 低、中、高にグループ化された宛先 IP アドレスの数が表示されます。
  - [Number of Source IP Addresses]：宛先 IP アドレスの各グループに関連付けられた送信元 IP アドレスの数が表示されます。

[Add Protocol Number] および [Edit Protocol Number] ダイアログボックスのフィールド定義

[Add Protocol Number] および [Edit Protocol Number] ダイアログボックスには次のフィールドがあります。

- [Protocol number]：プロトコル番号を入力します。
- [Enable the Service]：サービスをイネーブルにできます。

- [Override Scanner Settings]：オンにすると、すべてのヒストグラムを追加、編集、削除、および選択できます。
- [Scanner Threshold]：スキャナしきい値を設定できます。有効な範囲は 5 ～ 1000 です。デフォルトは 100 です。
- [Threshold Histogram]：追加したヒストグラムが表示されます。
  - [Number of Destination IP Addresses]：追加した宛先 IP アドレスの数が表示されます。
  - [Number of Source IP Addresses]：追加した送信元 IP アドレスの数が表示されます。

不正ゾーンの設定

不正ゾーンを異常検出用に設定するには、次の手順を実行します。

ステップ 1　管理者権限またはオペレータ権限を持つアカウントを使用して IME にログインします。

ステップ 2　[Configuration] > *sensor_name* > [Policies] > [Anomaly Detections] > [ad0] > [Illegal Zone] を選択します。

ステップ 3　[General] タブをクリックします。

ステップ 4　不正ゾーンをイネーブルにするには、[Enable the Illegal Zone] チェックボックスをオンにします。

（注）　[Enable the Illegal Zone] チェックボックスをオンにしなければ、設定したプロトコルは無視されます。

ステップ 5　[Service Subnets] フィールドに、不正ゾーンを適用するサブネットを入力します。有効な形式は 10.10.5.5,10.10.2.1-10.10.2.30 です。

ステップ 6　TCP プロトコルを設定するには、[TCP Protocol] タブをクリックします。

ステップ 7　TCP プロトコルをイネーブルにするには、[Enable the TCP Protocol] チェックボックスをオンにします。

（注）　[Enable the TCP Protocol] チェックボックスをオンにしなければ、TCP プロトコルの設定は無視されます。

ステップ 8　[Destination Port Map] タブをクリックし、[Add] をクリックして、宛先ポートを追加します。

ステップ 9　[Destination Port Number] フィールドに宛先ポート番号を入力します。有効な範囲は 0 ～ 65535 です。

ステップ 10　内部ゾーンをイネーブルにするには、[Enable the Service] チェックボックスをオンにします。

ステップ 11　そのポートのスキャナ値をオーバーライドするには、[Override Scanner Settings] チェックボックスをオンにします。デフォルトのスキャナ値を使用することもできれば、デフォルト値をオーバーライドし、独自のスキャナ値を設定することもできます。

ステップ 12　新しいスキャナ設定のヒストグラムを追加するには、[Add] をクリックします。

ステップ 13　[Number of Destination IP Addresses] ドロップダウン リストから値（[High]、[Medium]、または [Low]）を選択します。

ステップ 14　[Number of Source IP Addresses] フィールドに、このヒストグラムに関連付ける送信元 IP アドレスの数を入力します。有効な範囲は 0 ～ 4096 です。

ヒント 変更を破棄して [Add Histogram] ダイアログボックスを閉じるには、[Cancel] をクリックします。

ステップ 15 [OK] をクリックします。[Add Destination Port] ダイアログボックスのリストに新しいスキャナ設定が表示されます。

ヒント 変更を破棄して [Add Destination Port] ダイアログボックスを閉じるには、[Cancel] をクリックします。

ステップ 16 [OK] をクリックします。[Destination Port Map] タブのリストに新しい宛先ポート マップが表示されます。

ステップ 17 宛先ポート マップを編集するには、リストで宛先ポート マップを選択し、[Edit] をクリックします。

ステップ 18 フィールドに変更を加え、[OK] をクリックします。[Destination Port Map] タブのリストに編集済みの宛先ポート マップが表示されます。

ステップ 19 宛先ポート マップを削除するには、その宛先ポート マップを選択し、[Delete] をクリックします。その宛先ポート マップは、[Destination Port Map] タブのリストに表示されなくなります。

ステップ 20 デフォルトのしきい値を編集するには、[Default Thresholds] タブをクリックし、編集するしきい値ヒストグラムを選択して、[Edit] をクリックします。

ステップ 21 [Number of Destination IP Addresses] ドロップダウン リストから別の値（[High]、[Medium]、または [Low]）を選択します。

ステップ 22 [Number of Source IP Addresses] フィールドで、このヒストグラムに関連付ける送信元 IP アドレスの数を編集します。有効な範囲は 0 ～ 4096 です。[Default Thresholds] タブのリストに編集済みのしきい値ヒストグラムが表示されます。

ヒント 変更を破棄して [Edit Histogram] ダイアログボックスを閉じるには、[Cancel] をクリックします。

ステップ 23 UDP プロトコルを設定するには、[UDP Protocol] タブをクリックします。

ステップ 24 UDP プロトコルをイネーブルにするには、[Enable the UDP Protocol] チェックボックスをオンにします。

（注） [Enable the UDP Protocol] チェックボックスをオンにしなければ、UDP プロトコルの設定は無視されます。

ステップ 25 [Destination Port Map] タブをクリックし、[Add] をクリックして、宛先ポートを追加します。

ステップ 26 [Destination Port Number] フィールドに宛先ポート番号を入力します。有効な範囲は 0 ～ 65535 です。

ステップ 27 内部ゾーンをイネーブルにするには、[Enable the Service] チェックボックスをオンにします。

ステップ 28 そのポートのスキャナ値をオーバーライドするには、[Override Scanner Settings] チェックボックスをオンにします。デフォルトのスキャナ値を使用することもできれば、デフォルト値をオーバーライドし、独自のスキャナ値を設定することもできます。

ステップ 29 新しいスキャナ設定のヒストグラムを追加するには、[Add] をクリックします。

ステップ 30 [Number of Destination IP Addresses] ドロップダウン リストから値（[High]、[Medium]、または [Low]）を選択します。

ステップ 31　[Number of Source IP Addresses] フィールドに、このヒストグラムに関連付ける送信元 IP アドレスの数を入力します。有効な範囲は 0 ～ 4096 です。

ヒント　変更を破棄して [Add Histogram] ダイアログボックスを閉じるには、[Cancel] をクリックします。

ステップ 32　[OK] をクリックします。[Add Destination Port] ダイアログボックスのリストに新しいスキャナ設定が表示されます。

ヒント　変更を破棄して [Add Destination Port] ダイアログボックスを閉じるには、[Cancel] をクリックします。

ステップ 33　[OK] をクリックします。[Destination Port Map] タブのリストに新しい宛先ポート マップが表示されます。

ステップ 34　宛先ポート マップを編集するには、リストで宛先ポート マップを選択し、[Edit] をクリックします。

ステップ 35　フィールドに変更を加え、[OK] をクリックします。[Destination Port Map] タブのリストに編集済みの宛先ポート マップが表示されます。

ステップ 36　宛先ポート マップを削除するには、その宛先ポート マップを選択し、[Delete] をクリックします。その宛先ポート マップは、[Destination Port Map] タブのリストに表示されなくなります。

ステップ 37　デフォルトのしきい値を編集するには、[Default Thresholds] タブをクリックし、編集するしきい値ヒストグラムを選択して、[Edit] をクリックします。

ステップ 38　[Number of Destination IP Addresses] ドロップダウン リストから別の値（[High]、[Medium]、または [Low]）を選択します。

ステップ 39　[Number of Source IP Addresses] フィールドで、このヒストグラムに関連付ける送信元 IP アドレスの数を編集します。有効な範囲は 0 ～ 4096 です。[Default Thresholds] タブのリストに編集済みのしきい値ヒストグラムが表示されます。

ヒント　変更を破棄して [Edit Histogram] ダイアログボックスを閉じるには、[Cancel] をクリックします。

ステップ 40　その他のプロトコルを設定するには、[Other Protocols] タブをクリックします。

ステップ 41　その他のプロトコルをイネーブルにするには、[Enable Other Protocols] チェックボックスをオンにします。

（注）　[Enable Other Protocols] チェックボックスをオンにしなければ、その他のプロトコルの設定は無視されます。

ステップ 42　[Protocol Number Map] タブをクリックし、[Add] をクリックして、プロトコル番号を追加します。

ステップ 43　[Protocol Number] フィールドにプロトコル番号を入力します。有効な範囲は 0 ～ 255 です。

ステップ 44　そのプロトコルのサービスをイネーブルにするには、[Enable the Service] チェックボックスをオンにします。

ステップ 45　そのプロトコルのスキャナ値をオーバーライドするには、[Override Scanner Settings] チェックボックスをオンにします。デフォルトのスキャナ値を使用することもできれば、デフォルト値をオーバーライドし、独自のスキャナ値を設定することもできます。

ステップ 46　新しいスキャナ設定のヒストグラムを追加するには、[Add] をクリックします。

ステップ 47　[Number of Destination IP Addresses] ドロップダウン リストから値（[High]、[Medium]、または [Low]）を選択します。

ステップ 48　[Number of Source IP Addresses] フィールドに、このヒストグラムに関連付ける送信元 IP アドレスの数を入力します。有効な範囲は 0 ～ 4096 です。

ヒント　変更を破棄して [Add Histogram] ダイアログボックスを閉じるには、[Cancel] をクリックします。

ステップ 49　[OK] をクリックします。[Add Protocol Number] ダイアログボックスのリストに新しいスキャナ設定が表示されます。

ヒント　変更を破棄して [Add Protocol Number] ダイアログボックスを閉じるには、[Cancel] をクリックします。

ステップ 50　[OK] をクリックします。[Protocol Number Map] タブのリストに新しいプロトコル番号が表示されます。

ステップ 51　プロトコル番号マップを編集するには、リストでプロトコル番号マップを選択し、[Edit] をクリックします。

ステップ 52　フィールドに変更を加え、[OK] をクリックします。[Protocol Number Map] タブのリストに編集済みのプロトコル番号マップが表示されます。

ステップ 53　プロトコル番号マップを削除するには、そのプロトコル番号マップを選択し、[Delete] をクリックします。そのプロトコル番号マップは、[Protocol Number Map] タブのリストに表示されなくなります。

ステップ 54　デフォルトのしきい値を編集するには、[Default Thresholds] タブをクリックし、編集するしきい値ヒストグラムを選択して、[Edit] をクリックします。

ステップ 55　[Number of Destination IP Addresses] ドロップダウン リストから別の値（[High]、[Medium]、または [Low]）を選択します。

ステップ 56　[Number of Source IP Addresses] フィールドで、このヒストグラムに関連付ける送信元 IP アドレスの数を編集します。有効な範囲は 0 ～ 4096 です。[Default Thresholds] タブのリストに編集済みのしきい値ヒストグラムが表示されます。

ヒント　変更を破棄して [Edit Histogram] ダイアログボックスを閉じるには、[Cancel] をクリックします。

ヒント　変更を破棄するには、[Reset] をクリックします。

ステップ 57　変更を適用し、変更後の設定を保存するには、[Apply] をクリックします。

外部ゾーンの設定

ここでは、外部ゾーンの設定方法について説明します。内容は次のとおりです。

[External Zone] タブ

（注）　外部ゾーンを設定するには、管理者またはオペレータであることが必要です。

[External Zone] タブには、次の 3 つのタブがあります。

- [TCP Protocol]：TCP プロトコルをイネーブルにし、独自のしきい値とヒストグラムを設定できます。
- [UDP Protocol]：UDP プロトコルをイネーブルにし、独自のしきい値とヒストグラムを設定できます。
- [Other Protocols]：その他のプロトコルをイネーブルにし、独自のしきい値とヒストグラムを設定できます。

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

[TCP Protocol] タブ

[TCP Protocol] タブでは、外部ゾーンの TCP プロトコルをイネーブルまたはディセーブルにします。TCP プロトコルの宛先ポートを設定できます。デフォルトのしきい値を使用することもできれば、スキャナ設定をオーバーライドし、独自のしきい値とヒストグラムを追加することもできます。

フィールド定義

[TCP Protocol] タブには次のフィールドがあります。

- [Enable the TCP Protocol]：オンにすると、TCP プロトコルがイネーブルになります。
- [Destination Port Map] タブ：TCP プロトコルに特定のポートを関連付けることができます。
  - [Port Number]：設定されているポート番号が表示されます。

  - [Service Enabled]：サービスがイネーブルであるかどうか。
  - [Scanner Overridden]：スキャナがオーバーライドされているかどうか。
  - [Overridden Scanner Settings]：設定されているスキャナ設定が表示されます。
  - [Threshold]：しきい値の設定が表示されます。
  - [Histogram]：設定されているヒストグラムが表示されます。
- [Default Thresholds] タブ：デフォルトのしきい値とヒストグラムが表示されます。デフォルトのしきい値は、KB に含まれず設定によってオーバーライドされていないサービスに使用されます。
  - [Scanner Threshold]：スキャナしきい値を変更できます。
  - [Threshold Histogram]：デフォルトのしきい値ヒストグラムが表示されます。
  - [Number of Destination IP Addresses]：低、中、高にグループ化された宛先 IP アドレスの数が表示されます。
  - [Number of Source IP Addresses]：宛先 IP アドレスの各グループに関連付けられた送信元 IP アドレスの数が表示されます。

[Add Destination Port] および [Edit Destination Port] ダイアログボックスのフィールド定義

[Add Destination Port] および [Edit Destination Port] ダイアログボックスには次のフィールドがあります。

- [Destination Port number]：宛先ポート番号を入力します。有効な範囲は 0 ～ 65535 です。
- [Enable the Service]：オンにすると、サービスがイネーブルになります。
- [Override Scanner Settings]：オンにすると、デフォルトのスキャナ設定がオーバーライドされ、すべてのヒストグラムを追加、編集、削除、および選択できます。
- [Scanner Threshold]：スキャナしきい値を設定できます。有効な範囲は 5 ～ 1000 です。デフォルトは 100 です。
- [Threshold Histogram]：追加したヒストグラムが表示されます。
  - [Number of Destination IP Addresses]：追加した宛先 IP アドレスの数が表示されます。
  - [Number of Source IP Addresses]：追加した送信元 IP アドレスの数が表示されます。

[Add Histogram] および [Edit Histogram] ダイアログボックスのフィールド定義

[Add Histogram] および [Edit Histogram] ダイアログボックスには次のフィールドがあります。

- [Number of Destination IP Addresses]：低、中、高の各グループの宛先 IP アドレス数を追加できます。宛先 IP アドレス数は、低が 5、中が 20、高が 100 です。
- [Number of Source IP Addresses]：送信元 IP アドレスの数を追加できます。有効な範囲は 0 ～ 4096 です。

[UDP Protocol] タブ

[UDP Protocol] タブでは、外部ゾーンの UDP プロトコルをイネーブルまたはディセーブルにします。UDP プロトコルの宛先ポートを設定できます。デフォルトのしきい値を使用することもできれば、スキャナ設定をオーバーライドし、独自のしきい値とヒストグラムを追加することもできます。

フィールドの説明

[UDP Protocol] タブには次のフィールドがあります。

- [Enable the UDP Protocol]：オンにすると、UDP プロトコルがイネーブルになります。
- [Destination Port Map] タブ：UDP プロトコルに特定のポートを関連付けることができます。
  - [Port Number]：設定されているポート番号が表示されます。
  - [Service Enabled]：サービスがイネーブルであるかどうか。
  - [Scanner Overridden]：スキャナがオーバーライドされているかどうか。
  - [Overridden Scanner Settings]：設定されているスキャナ設定が表示されます。
  - [Threshold]：しきい値の設定が表示されます。
  - [Histogram]：設定されているヒストグラムが表示されます。
- [Default Thresholds] タブ：デフォルトのしきい値とヒストグラムが表示されます。
  - [Scanner Threshold]：スキャナしきい値を変更できます。
  - [Threshold Histogram]：デフォルトのしきい値ヒストグラムが表示されます。
  - [Number of Destination IP Addresses]：低、中、高にグループ化された宛先 IP アドレスの数が表示されます。
  - Number of Source IP Addresses]:宛先 IP アドレスの各グループに関連付けられた送信元 IP アドレスの数が表示されます。

[Other Protocols] タブ

[Other Protocols] タブでは、外部ゾーンのその他のプロトコルをイネーブルまたはディセーブルにします。その他のプロトコルのプロトコル番号マップを設定できます。デフォルトのしきい値を使用することもできれば、スキャナ設定をオーバーライドし、独自のしきい値とヒストグラムを追加することもできます。

フィールドの説明

[Other Protocols] タブには次のフィールドがあります。

- [Enable Other Protocols]：オンにすると、その他のプロトコルがイネーブルになります。
- [Protocol Number Map] タブ：その他のプロトコルに特定のプロトコル番号を関連付けることができます。
  - [Protocol Number]：設定されているプロトコル番号が表示されます。
  - [Service Enabled]：サービスがイネーブルであるかどうか。
  - [Scanner Overridden]：スキャナがオーバーライドされているかどうか。
  - [Overridden Scanner Settings]：設定されているスキャナ設定が表示されます。
  - [Threshold]：しきい値の設定が表示されます。
  - [Histogram]：設定されているヒストグラムが表示されます。

- [Default Thresholds] タブ：デフォルトのしきい値とヒストグラムが表示されます。
  - [Scanner Threshold]：スキャナしきい値を変更できます。
  - [Threshold Histogram]：デフォルトのしきい値ヒストグラムが表示されます。
  - [Number of Destination IP Addresses]：低、中、高にグループ化された宛先 IP アドレスの数が表示されます。
  - [Number of Source IP Addresses]：宛先 IP アドレスの各グループに関連付けられた送信元 IP アドレスの数が表示されます。

[Add Protocol Number] および [Edit Protocol Number] ダイアログボックスのフィールド定義

[Add Protocol Number] および [Edit Protocol Number] ダイアログボックスには次のフィールドがあります。

- [Protocol number]：プロトコル番号を入力します。
- [Enable the Service]：サービスをイネーブルにできます。
- [Override Scanner Settings]：オンにすると、すべてのヒストグラムを追加、編集、削除、および選択できます。
- [Scanner Threshold]：スキャナしきい値を設定できます。有効な範囲は 5 ～ 1000 です。デフォルトは 100 です。
- [Threshold Histogram]：追加したヒストグラムが表示されます。
  - [Number of Destination IP Addresses]：追加した宛先 IP アドレスの数が表示されます。
  - [Number of Source IP Addresses]：追加した送信元 IP アドレスの数が表示されます。

外部ゾーンの設定

外部ゾーンを異常検出用に設定するには、次の手順を実行します。

ステップ 1　管理者権限またはオペレータ権限を持つアカウントを使用して IME にログインします。

ステップ 2　[Configuration] > *sensor_name* > [Policies] > [Anomaly Detections] > [ad0] > [External Zone] を選択します。

ステップ 3　外部ゾーンをイネーブルにするには、[Enable the External Zone] チェックボックスをオンにします。

（注）　[Enable the External Zone] チェックボックスをオンにしなければ、設定したプロトコルは無視されます。

ステップ 4　TCP プロトコルを設定するには、[TCP Protocol] タブをクリックします。

ステップ 5　TCP プロトコルをイネーブルにするには、[Enable the TCP Protocol] チェックボックスをオンにします。

（注）　[Enable the TCP Protocol] チェックボックスをオンにしなければ、TCP プロトコルの設定は無視されます。

ステップ 6　[Destination Port Map] タブをクリックし、[Add] をクリックして、宛先ポートを追加します。

ステップ 7　[Destination Port Number] フィールドに宛先ポート番号を入力します。有効な範囲は 0 ～ 65535 です。

ステップ 8　内部ゾーンをイネーブルにするには、[Enable the Service] チェックボックスをオンにします。

ステップ 9　そのポートのスキャナ値をオーバーライドするには、[Override Scanner Settings] チェックボックスをオンにします。デフォルトのスキャナ値を使用することもできれば、デフォルト値をオーバーライドし、独自のスキャナ値を設定することもできます。

ステップ 10　新しいスキャナ設定のヒストグラムを追加するには、[Add] をクリックします。

ステップ 11　[Number of Destination IP Addresses] ドロップダウン リストから値（[High]、[Medium]、または [Low]）を選択します。

ステップ 12　[Number of Source IP Addresses] フィールドに、このヒストグラムに関連付ける送信元 IP アドレスの数を入力します。有効な範囲は 0 ～ 4096 です。

ヒント　変更を破棄して [Add Histogram] ダイアログボックスを閉じるには、[Cancel] をクリックします。

ステップ 13　[OK] をクリックします。[Add Destination Port] ダイアログボックスのリストに新しいスキャナ設定が表示されます。

ヒント　変更を破棄して [Add Destination Port] ダイアログボックスを閉じるには、[Cancel] をクリックします。

ステップ 14　[OK] をクリックします。[Destination Port Map] タブのリストに新しい宛先ポート マップが表示されます。

ステップ 15　宛先ポート マップを編集するには、リストで宛先ポート マップを選択し、[Edit] をクリックします。

ステップ 16　フィールドに変更を加え、[OK] をクリックします。[Destination Port Map] タブのリストに編集済みの宛先ポート マップが表示されます。

ステップ 17　宛先ポート マップを削除するには、その宛先ポート マップを選択し、[Delete] をクリックします。その宛先ポート マップは、[Destination Port Map] タブのリストに表示されなくなります。

ステップ 18　デフォルトのしきい値を編集するには、[Default Thresholds] タブをクリックし、編集するしきい値ヒストグラムを選択して、[Edit] をクリックします。

ステップ 19　[Number of Destination IP Addresses] ドロップダウン リストから別の値（[High]、[Medium]、または [Low]）を選択します。

ステップ 20　[Number of Source IP Addresses] フィールドで、このヒストグラムに関連付ける送信元 IP アドレスの数を編集します。有効な範囲は 0 ～ 4096 です。[Default Thresholds] タブのリストに編集済みのしきい値ヒストグラムが表示されます。

ヒント　変更を破棄して [Edit Histogram] ダイアログボックスを閉じるには、[Cancel] をクリックします。

ステップ 21　UDP プロトコルを設定するには、[UDP Protocol] タブをクリックします。

ステップ 22　UDP プロトコルをイネーブルにするには、[Enable the UDP Protocol] チェックボックスをオンにします。

（注）　[Enable the UDP Protocol] チェックボックスをオンにしなければ、UDP プロトコルの設定は無視されます。

ステップ 23　[Destination Port Map] タブをクリックし、[Add] をクリックして、宛先ポートを追加します。

ステップ 24　[Destination Port Number] フィールドに宛先ポート番号を入力します。有効な範囲は 0 ～ 65535 です。

ステップ 25　内部ゾーンをイネーブルにするには、[Enable the Service] チェックボックスをオンにします。

ステップ 26　そのポートのスキャナ値をオーバーライドするには、[Override Scanner Settings] チェックボックスをオンにします。デフォルトのスキャナ値を使用することもできれば、デフォルト値をオーバーライドし、独自のスキャナ値を設定することもできます。

ステップ 27　新しいスキャナ設定のヒストグラムを追加するには、[Add] をクリックします。

ステップ 28　[Number of Destination IP Addresses] ドロップダウン リストから値（[High]、[Medium]、または [Low]）を選択します。

ステップ 29　[Number of Source IP Addresses] フィールドに、このヒストグラムに関連付ける送信元 IP アドレスの数を入力します。有効な範囲は 0 ～ 4096 です。

ヒント　変更を破棄して [Add Histogram] ダイアログボックスを閉じるには、[Cancel] をクリックします。

ステップ 30　[OK] をクリックします。[Add Destination Port] ダイアログボックスのリストに新しいスキャナ設定が表示されます。

ヒント　変更を破棄して [Add Destination Port] ダイアログボックスを閉じるには、[Cancel] をクリックします。

ステップ 31　[OK] をクリックします。[Destination Port Map] タブのリストに新しい宛先ポート マップが表示されます。

ステップ 32　宛先ポート マップを編集するには、リストで宛先ポート マップを選択し、[Edit] をクリックします。

ステップ 33　フィールドに変更を加え、[OK] をクリックします。[Destination Port Map] タブのリストに編集済みの宛先ポート マップが表示されます。

ステップ 34　宛先ポート マップを削除するには、その宛先ポート マップを選択し、[Delete] をクリックします。その宛先ポート マップは、[Destination Port Map] タブのリストに表示されなくなります。

ステップ 35　デフォルトのしきい値を編集するには、[Default Thresholds] タブをクリックし、編集するしきい値ヒストグラムを選択して、[Edit] をクリックします。

ステップ 36　[Number of Destination IP Addresses] ドロップダウン リストから別の値（[High]、[Medium]、または [Low]）を選択します。

ステップ 37　[Number of Source IP Addresses] フィールドで、このヒストグラムに関連付ける送信元 IP アドレスの数を編集します。有効な範囲は 0 ～ 4096 です。[Default Thresholds] タブのリストに編集済みのしきい値ヒストグラムが表示されます。

ヒント　変更を破棄して [Edit Histogram] ダイアログボックスを閉じるには、[Cancel] をクリックします。

ステップ 38　その他のプロトコルを設定するには、[Other Protocols] タブをクリックします。

ステップ 39　その他のプロトコルをイネーブルにするには、[Enable Other Protocols] チェックボックスをオンにします。

（注）　[Enable Other Protocols] チェックボックスをオンにしなければ、その他のプロトコルの設定は無視されます。

ステップ 40　[Protocol Number Map] タブをクリックし、[Add] をクリックして、プロトコル番号を追加します。

ステップ 41　[Protocol Number] フィールドにプロトコル番号を入力します。有効な範囲は 0 ～ 255 です。

ステップ 42　そのプロトコルのサービスをイネーブルにするには、[Enable the Service] チェックボックスをオンにします。

ステップ 43　そのプロトコルのスキャナ値をオーバーライドするには、[Override Scanner Settings] チェックボックスをオンにします。デフォルトのスキャナ値を使用することもできれば、デフォルト値をオーバーライドし、独自のスキャナ値を設定することもできます。

ステップ 44　新しいスキャナ設定のヒストグラムを追加するには、[Add] をクリックします。

ステップ 45　[Number of Destination IP Addresses] ドロップダウン リストから値（[High]、[Medium]、または [Low]）を選択します。

ステップ 46　[Number of Source IP Addresses] フィールドに、このヒストグラムに関連付ける送信元 IP アドレスの数を入力します。有効な範囲は 0 ～ 4096 です。

ヒント　変更を破棄して [Add Histogram] ダイアログボックスを閉じるには、[Cancel] をクリックします。

ステップ 47　[OK] をクリックします。[Add Protocol Number] ダイアログボックスのリストに新しいスキャナ設定が表示されます。

ヒント　変更を破棄して [Add Protocol Number] ダイアログボックスを閉じるには、[Cancel] をクリックします。

ステップ 48　[OK] をクリックします。[Protocol Number Map] タブのリストに新しいプロトコル番号が表示されます。

ステップ 49　プロトコル番号マップを編集するには、リストでプロトコル番号マップを選択し、[Edit] をクリックします。

ステップ 50　フィールドに変更を加え、[OK] をクリックします。[Protocol Number Map] タブのリストに編集済みのプロトコル番号マップが表示されます。

ステップ 51　プロトコル番号マップを削除するには、そのプロトコル番号マップを選択し、[Delete] をクリックします。そのプロトコル番号マップは、[Protocol Number Map] タブのリストに表示されなくなります。

ステップ 52　デフォルトのしきい値を編集するには、[Default Thresholds] タブをクリックします。

ステップ 53　編集するしきい値ヒストグラムを選択し、[Edit] をクリックします。

ステップ 54　[Number of Destination IP Addresses] ドロップダウン リストから別の値（[High]、[Medium]、または [Low]）を選択します。

ステップ 55　[Number of Source IP Addresses] フィールドで、このヒストグラムに関連付ける送信元 IP アドレスの数を編集します。有効な範囲は 0 ～ 4096 です。[Default Thresholds] タブのリストに編集済みのしきい値ヒストグラムが表示されます。

ヒント 変更を破棄して [Edit Histogram] ダイアログボックスを閉じるには、[Cancel] をクリックします。

ヒント 変更を破棄するには、[Reset] をクリックします。

ステップ 56 変更を適用し、変更後の設定を保存するには、[Apply] をクリックします。

異常検出のディセーブル化

センサーをトラフィックの一方向だけを参照するように設定している場合は、異常検出をディセーブルにする必要があります。そうしなければ、異常検出が非対称トラフィックをワーム スキャナと同じような不完全な接続と認識し、アラートを起動するため、大量のアラートが生成されます。

異常検出をディセーブルにするには、次の手順を実行します。

ステップ 1 管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2 分析エンジン サブモードを開始します。

```
sensor# configure terminal
sensor(config)# service analysis-engine
sensor(config-ana)#
```

ステップ 3 ディセーブルにする異常検出ポリシーが含まれる仮想センサー名を入力します。

```
sensor(config-ana)# virtual-sensor vs0
sensor(config-ana-vir)#
```

ステップ 4 異常検出動作モードをディセーブルにします。

```
sensor(config-ana-vir)# anomaly-detection
sensor(config-ana-vir-ano)# operational-mode inactive
sensor(config-ana-vir-ano)#
```

ステップ 5 分析エンジン サブモードを終了します。

```
sensor(config-ana-vir-ano)# exit
sensor(config-ana-vir)# exit
sensor(config-ana-)# exit
Apply Changes:?[yes]:
```

ステップ 6 変更を適用する場合は Enter を押します。変更を破棄する場合は「no」と入力します。