CHAPTER 10

異常検出の設定

（注） IPS SSP を搭載した Cisco ASA 5585-X は、現在のところ、Cisco IPS 7.1 をサポートする唯一のプラットフォームです。現時点では、他に IPS バージョン 7.1 をサポートしている Cisco IPS センサーはありません。

（注） IPS SSP を搭載した Cisco ASA 5585-X は、ASA 8.2(4.4) 以上および ASA 8.4(2) 以上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。

この章では、複数のセキュリティ ポリシーを作成して、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。次の事項について説明します。

セキュリティ ポリシーの概要

複数のセキュリティ ポリシーを作成して、個々の仮想センサーに適用できます。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、異常検出ポリシー、それぞれ 1 つで構成されます。Cisco IPS には、sig0 というデフォルトのシグニチャ定義ポリシー、rules0 というデフォルトのイベント アクション規則ポリシー、ad0 というデフォルトの異常検出ポリシーが含まれています。デフォルト ポリシーを仮想センサーに割り当てるか、新しいポリシーを作成することができます。セキュリティ ポリシーを複数使用すると、さまざまな要件に基づいてセキュリティ ポリシーを作成し、このカスタマイズしたポリシーを VLAN または物理インターフェイスごとに適用できます。

異常検出のコンポーネント

次の項では、異常検出のさまざまなコンポーネントについて説明します。次の事項について説明します。

異常検出について

注意　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下できます。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.10-3）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.10-35）を参照してください。

ワーム

注意　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、ワームに感染したホストを、スキャナのようなその動作で識別します。ワームでは、拡散を目的として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またはネットワークをスキャンして、さまざまな宛先 IP アドレスへのアクセス試行を生成し、失敗しながら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、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 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、通常と異なる数の 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 プロトコルで重要なイベントは、すべてのパケットが 1 方向だけに進む、UDP 接続などの単一方向接続です。UDP 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、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クワッド上で UDP パケットを受信しません。

ICMP などのその他のプロトコルで重要なイベントは、単一の送信元 IP アドレスから異なる多数の宛先 IP アドレスに向かいます。つまり、1 方向だけで受信されるパケットです。

注意　感染対象の IP アドレスのリストを備えており、拡散のためにスキャニングを必要としないワーム（たとえば、アクティブ スキャニングではなくネットワークをリスニングするパッシブ マッピングを使用）は、異常検出ワーム ポリシーによって検出されません。感染したホスト内のファイルをプローブしてメーリング リストを取得し、このリストを電子メールで送信するワームも検出されません。これは、この場合、レイヤ 3 およびレイヤ 4 では、異常を生じないためです。

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.10-35）を参照してください。

異常検出のモード

異常検出では、まず、最も標準的なネットワーク状態を反映する時間に、「平時」学習処理を実施します。異常検出では、次に、通常のネットワークで最適な、一連のポリシーしきい値を導出します。

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、デフォルトでは検出モードですが、デフォルト期間の 24 時間は、初期学習受け入れモードを実施します。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（KB）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。つまり、新しい KB が保存およびロードされて、24 時間後に初期 KB が置換されます。

  （注） 初期 KB は空であり、初期 KB によって処理するとき、異常検出で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、これにより、異常検出で攻撃も検出されるようになります。

  （注） ネットワークの複雑さによっては、デフォルトの 24 時間を超えて異常検出を学習受け入れモードにしておく必要があります。

- 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 が置換された後で、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 フローを監視し、アラートを送信します。異常検出では異常を検索すると同時に、しきい値に違反しない、KB に対する漸進的な変更を記録し、その結果新しい KB が作成されます。新しい KB は定期的に保存され、古い KB を置き換えることによって、最新の KB 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。センサーが非同期環境で実行されている場合など、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。11:00 pm に仮想センサーを追加し、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 を使用して動作を開始し、学習だけを実行します。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 KB に保存され、この KB がロードされて初期 KB を置換します。異常検出はデフォルトで検出モードになっており、異常検出で新しい KB を使用するようになったため、異常検出は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.10-3）を参照してください。
- センサーを異なる異常検出モードに設定する手順については、「仮想センサーの追加、編集、削除」（P.6-11）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、false negative 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。ゾーンは、内部、不正、および外部の 3 種類あり、それぞれ独自のしきい値を持ちます。

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。内部ゾーンと不正ゾーンの一連の IP アドレスと一致しないパケットは、外部ゾーンによって処理されます。

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。このように設定した場合、内部ゾーンは、設定した IP アドレス範囲に着信するすべてのトラフィックになり、外部ゾーンは、インターネット向けに発信されるすべてのトラフィックになります。

正常なトラフィックでは決して見られない IP アドレス範囲によって不正ゾーンを設定できます。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 アドレスです。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

異常検出ゾーンの設定の詳細については、「内部ゾーンの設定」（P.10-14）、「不正ゾーンの設定」（P.10-22）、および「外部ゾーンの設定」（P.10-29）を参照してください。

異常検出の設定シーケンス

異常検出の検出部分を設定できます。KB で学習されたしきい値をオーバーライドする一連のしきい値を設定できます。ただし、異常検出では、検出の設定方法にかかわらず、学習を続行します。KB のインポート、エクスポート、およびロードを行ったり、KB のデータを表示したりすることもできます。

異常検出を設定するときは、次のシーケンスに従ってください。

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。または、デフォルトの異常検出ポリシー ad0 を使用できます。
2. 異常検出ポリシーを仮想センサーに追加します。
3. 異常検出ゾーンおよびプロトコルを設定します。
4. デフォルトでは、動作モードに検出を設定しますが、最初の 24 時間は、データを設定した KB を作成するために学習が実行されます。初期 KB は空で、デフォルトの 24 時間の間、異常検出では、KB にデータを設定するために使用するデータを収集します。デフォルト期間の 24 時間を超えて学習させる場合は、モードを手動で学習受け入れに設定する必要があります。
5. センサーを学習受け入れモードで実行する時間は、最低 24 時間（デフォルト）にしてください。

   センサーを学習受け入れモードで実行するときは、初期 KB 用に通常状態のネットワークに関する情報を収集するために、最低 24 時間実行してください。ただし、学習受け入れモードの期間は、ネットワークの複雑さに合わせて変更する必要があります。

   （注）　センサーを学習受け入れモードにする期間は最低 24 時間を推奨していますが、1 週間までの範囲でもっと長くすれば、その方が適切です。

   この期間が過ぎると、センサーは、ネットワークの通常のアクティビティを示すベースラインとして、初期 KB を保存します。

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、検出モードに切り替えてください。
7. 異常検出パラメータを設定します。
   - ワーム タイムアウトおよび異常検出でバイパスする必要のある送信元と宛先の IP アドレスを設定します。このタイムアウトが終わると、スキャナのしきい値は設定値に戻ります。
   - 異常検出が検出モードのときに自動 KB 更新をイネーブルにするかどうかを決めます。
   - 18 個の異常検出ワーム シグニチャを設定して、デフォルトの Produce Alert だけでなく、他にもイベント アクションを実行するようにします。たとえば、Deny Attacker イベント アクションを設定します。

詳細情報

- 異常検出をさまざまなモードにする手順については、「仮想センサーの追加、編集、削除」（P.6-11）を参照してください。
- 新しい異常検出ポリシーを設定にする手順については、「異常検出ポリシーの追加、クローニング、および削除」（P.10-9）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.10-14）、「不正ゾーンの設定」（P.10-22）、および「外部ゾーンの設定」（P.10-29）を参照してください。
- 異常検出モードの詳細については、「異常検出のモード」（P.10-3）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.10-13）を参照してください。
- 異常検出シグニチャの設定については、「異常検出シグニチャ」（P.10-6）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.9-8）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。異常を検出した異常検出では、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ため、ワーム検出に使用されているしきい値がアラートの詳細に表示されます。これ以降、すべてのスキャナは、ワームに感染した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 アドレスおよび宛先ポートをブロックします。
- [SNMP Trap]：NotificationApp に要求を送信して、SNMP 通知を実行します。

- [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。

表 10-1 に異常検出ワーム シグニチャを示します。

表 10-1　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。
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。

表 10-1　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	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.7-18）を参照してください。

異常検出の設定

ここでは、異常検出ポリシーの作成方法について説明します。次の事項について説明します。

[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必要があります。

[Anomaly Detections] ペインでは、異常検出ポリシーの追加、クローニング、または削除を行うことができます。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、新しいポリシー インスタンスを作成する制御トランザクションがセンサーに送信されます。正常応答の場合は、新しいポリシー インスタンスが [Anomaly Detections] の下に追加されます。リソースの制約などによって制御トランザクションが失敗すると、エラー メッセージが表示されます。

プラットフォームで仮想ポリシーをサポートしていない場合、各コンポーネントにつき 1 つのインスタンスしか持てないため、ポリシーの新規作成や既存のポリシーの削除は行えません。この場合、[Add] ボタン、[Clone] ボタン、[Delete] ボタンはディセーブルになります。

[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]：この異常検出ポリシーの名前を識別します。
- [Assigned Virtual Sensor]：この異常検出ポリシーが割り当てられている仮想センサーを識別します。

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

[Add Policy]/[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]：この異常検出ポリシーの名前を識別します。

異常検出ポリシーの追加、クローニング、および削除

異常検出ポリシーの追加、クローニング、または削除を行うには、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 IDM にログインします。

ステップ 2　[Configuration] > [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　変更を廃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。異常検出ポリシーが [Anomaly Detections] パネルのリストに表示されます。

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、リストで選択して、[Clone] をクリックします。既存の異常検出ポリシー名に「_copy」を付加して [Clone Policy] ダイアログボックスが表示されます。

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　変更を廃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] パネルのリストに表示されます。

ステップ 8　異常検出ポリシーを削除するには、ポリシーを選択して、[Delete] をクリックします。[Delete Policy] ダイアログボックスが開き、このポリシーを恒久的に削除してよいかどうかを確認するメッセージが表示されます。

注意　デフォルトの異常検出ポリシー 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が [Anomaly Detections] ペインのリストに表示されなくなりました。

[ad0] ペイン

[ad0] ペイン（デフォルト）には、異常検出を設定するツールが含まれています。5 つのタブがあります。

- [Operation Settings]：ワーム タイムアウト、および異常検出処理の間にセンサーで無視する送信元と宛先の IP アドレスを設定できます。
- [Learning Accept Mode]：センサーによる学習される KB の自動受け入れをイネーブルにでき、学習された KB を受け入れるスケジュールを設定できます。
- [Internal Zone]：内部ゾーンの宛先 IP アドレスおよびしきい値を設定できます。
- [Illegal Zone]：不正ゾーンの宛先 IP アドレスおよび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。

動作設定の構成

ここでは、動作設定の設定方法について説明します。次の事項について説明します。

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

[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必要があります。

[Operation Settings] タブでは、ワーム検出タイムアウトを設定できます。このタイムアウトが終わると、スキャナのしきい値は設定値に戻ります。異常検出で KB 用の情報を収集しているときに、センサーに無視させる送信元と宛先の IP アドレスを設定することもできます。異常検出では、これらの送信元と宛先の 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。

[Operating 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期間（秒数）を入力できます。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必要のある IP アドレスを入力できます。
  - [Enable ignored IP Addresses]：オンにした場合、無視される 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 アドレスを入力できます。
  - [Destination IP Addresses]：異常検出で無視する宛先 IP アドレスを入力できます。

異常検出の動作設定の構成

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 IDM にログインします。

ステップ 2　[Configuration] > [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、ワーム検出のタイムアウトを待機する秒数を入力します。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　無視される 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] チェックボックスはオンにする必要があり、オンにしないと入力したいずれの IP アドレスも無視されません。

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 アドレスのアドレスまたは範囲を入力します。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 アドレスのアドレスまたは範囲を入力します。

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　[Apply] をクリックして、変更を適用し、改訂したコンフィギュレーションを保存します。

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。次の事項について説明します。

- 「[Learning Accept Mode] タブ」（P.10-12）
- 「KB およびヒストグラム」（P.10-12）

- 「[Learning Accept Mode] タブのフィールド定義」（P.10-13）
- 「[Add Start Time]/[Edit Start Time] ダイアログボックスのフィールド定義」（P.10-13）
- 「学習受け入れモードの設定」（P.10-13）

[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必要があります。

一定時間ごとにセンサーに新しい KB を作成させるかどうかを設定するには、[Learning Accept Mode] タブを使用します。KB を作成およびロード（[Rotate]）するのか、保存（[Save Only]）するのかを設定できます。KB 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できます。

生成されるデフォルトのファイル名は *YYYY-Mon-dd-hh_mm_ss* です。ここで、*Mon* は当月を表す 3 文字の省略形です。

KB およびヒストグラム

KB にはツリー構造があり、次の情報を含みます。

- KB の名前
- ゾーン名
- プロトコル
- サービス

KB には、各サービスのスキャナのしきい値およびヒストグラムが保持されています。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は、24 時間ごとに新しい KB が作成されて次の 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 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ていない場合、KB は作成されません。

（注）　学習受け入れモードでは、センサーの現地時間が使用されます。

スキャナのしきい値は、単一の送信元 IP アドレスで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。ヒストグラムのしきい値は、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。

異常検出では、攻撃が行われていないときに学習したヒストグラムからの逸脱を検出した場合（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）、ワーム攻撃であると識別します。たとえば、スキャニングしきい値が 300 で、ポート 445 のヒストグラムの場合、異常検出では、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 10-2 は、この例を示します。

表 10-2　ヒストグラムの例

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

異常検出では、ポート 445 で 50 個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 つ識別すると、異常検出でポート 445 へのワーム攻撃を識別したことを示す、送信元 IP アドレス未指定のアクションを作成します。動的なフィルタしきい値の 50 は、新しい内部スキャンしきい値に指定されるため、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 アドレスごとの追加の動的フィルタを異常検出で作成するために、異常検出では、スキャナのしきい値定義を小さくします。

KB が学習した内容は、異常検出ポリシーごと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 トラフィックが判明している場合は、false positive 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] : オンにした場合、センサーは、KB を自動的に更新します。オフにすると、異常検出では、新しい KB を自動的に作成しません。
- [Action] : KB を循環させるのか保存するのかを指定できます。[Save Only] を選択した場合は、新しい KB が作成されます。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 が作成およびロードされます。
- [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時刻および後続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] : 新しい KB を作成する前に、異常検出でネットワークから学習する期間を入力します。
  - [Calendar Schedule] : KB を作成する曜日および時刻を設定できます。
  - [Times of Day] : [Add] をクリックし、[Add Start Time] ダイアログボックスに時刻を入力します。
  - [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]/[Edit Start Time] ダイアログボックスのフィールド定義

[Add Start Time]/[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を時間、分、および秒で入力できます。有効な形式は、24 時間制の 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 IDM にログインします。

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

ステップ 3　異常検出に KB を自動的に更新させる場合は、[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 が作成されてロードされます。これはデフォルトです。
- [Save Only]：新しい KB は作成されますが、ロードされません。表示後に、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　カレンダー スケジュールを設定するには、次の手順を実行します。

a.　[Add] をクリックして開始時刻を追加します。

b.　24 時間制形式を使用して、開始時刻を時間、分、秒で入力します。

ヒント　変更を廃棄して [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で 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　定期スケジュール（デフォルト）を設定するには、次の手順を実行します。

a.　[Start Time] フィールドに、24 時間制形式を使用して、開始時刻を時間、分、秒で入力します。

b.　[Learning Interval] フィールドに、後続の 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　[Apply] をクリックして、変更を適用し、改訂したコンフィギュレーションを保存します。

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。次の事項について説明します。

[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必要があります。

[Internal Zone] タブには、4 つのタブがあります。

- [General]：内部ゾーンをイネーブルにし、このゾーンに含まれるサブネットを指定できます。
- [TCP Protocol]：TCP プロトコルをイネーブルにして、独自のしきい値および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て、独自のしきい値および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て、独自のしきい値および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す必要があります。内部 IP アドレス範囲に着信するすべてのトラフィックを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の場合、このゾーンへのパケットは無視されます。デフォルトでは、ゾーンはイネーブルです。

次に、このゾーンに属す IP アドレスを追加します。ゾーンの IP アドレスをまったく設定していない場合は、すべてのパケットが、デフォルト ゾーンの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]：オンにした場合、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できます。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か、スキャナ設定をオーバーライドして独自のしきい値およびヒストグラムを追加できます。

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：特定のポートを TCP プロトコルと関連付けできます。
  - [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にされているかどうか。
  - [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]：しきい値の設定値が表示されます。
  - [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]：スキャナの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]：low、medium、high で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と関連付けられている送信元 IP アドレスの数が表示されます。

[Add Destination Port]/[Edit Destination Port] ダイアログボックス

[Add Destination Port]/[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できます。有効な範囲は 0 ～ 65535 です。
- [Enable the Service]：オンにした場合、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をオーバーライドして、ヒストグラムを追加、編集、削除したり、すべて選択したりできます。
- [Scanner Threshold]：スキャナの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]/[Edit Histogram] ダイアログボックス

[Add Histogram]/[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]：宛先 IP アドレスの数（high、medium、または low）を追加できます。low は宛先 IP アドレス 5 個、medium は 20 個、high は 100 個です。
- [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か、スキャナ設定をオーバーライドして独自のしきい値およびヒストグラムを追加できます。

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：特定のポートを UDP プロトコルと関連付けできます。

  - [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にされているかどうか。
  - [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]：しきい値の設定値が表示されます。
  - [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]：スキャナの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]：low、medium、high で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と関連付けられている送信元 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か、スキャナ設定をオーバーライドして独自のしきい値およびヒストグラムを追加できます。

フィールドの説明

[Other Protocol] 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：具体的なプロトコル番号をその他のプロトコルに関連付けできます。
  - [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にされているかどうか。
  - [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]：しきい値の設定値が表示されます。
  - [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]：スキャナの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]：low、medium、high で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と関連付けられている送信元 IP アドレスの数が表示されます。

[Add Protocol Number]/[Edit Protocol Number] ダイアログボックス

[Add Protocol Number]/[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できます。
- [Enable the Service]：サービスをイネーブル化できます。
- [Override Scanner Settings]：オンにすると、ヒストグラムを追加、編集、削除したり、すべて選択したりできます。
- [Scanner Threshold]：スキャナの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

異常検出の内部ゾーンを設定するには、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 IDM にログインします。

ステップ 2　[Configuration] > [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] チェックボックスはオンにする必要があり、オンにしないと、設定するすべての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] チェックボックスはオンにする必要があり、オンにしないと TCP プロトコル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、さらに [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　このポート上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 10　こ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か、デフォルト値をオーバーライドして独自のスキャナ値を設定できます。

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 リストで、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、このヒストグラムと関連付ける送信元 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　変更を廃棄して [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。新しいスキャナ設定が、[Add Destination Port] ダイアログボックスのリストに表示されます。

ヒント　変更を廃棄して [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。新しい宛先ポート マップが [Destination Port Map] タブのリストに表示されます。

ステップ 16　宛先ポート マップを編集するには、リストでそのマップを選択し、[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。編集した宛先ポート マップが [Destination Port Map] タブのリストに表示されます。

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

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 リストで、値（[High]、[Medium]、または [Low]）を変更します。

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

ヒント　変更を廃棄して [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] チェックボックスはオンにする必要があり、オンにしないと UDP プロトコル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、さらに [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　このポート上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 28　こ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か、デフォルト値をオーバーライドして独自のスキャナ値を設定できます。

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 リストで、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、このヒストグラムと関連付ける送信元 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　変更を廃棄して [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。新しいスキャナ設定が、[Add Destination Port] ダイアログボックスのリストに表示されます。

ヒント　変更を廃棄して [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。新しい宛先ポート マップが [Destination Port Map] タブのリストに表示されます。

ステップ 34　宛先ポート マップを編集するには、リストでそのマップを選択し、[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。編集した宛先ポート マップが [Destination Port Map] タブのリストに表示されます。

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

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から [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 リストで、値（[High]、[Medium]、または [Low]）を変更します。

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

ヒント　変更を廃棄して [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する必要があり、オンにしないと、その他のプロトコル設定は無視されます。

ステップ 42　[Protocol Number Map] タブをクリックしてから [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　こ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　こ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か、デフォルト値をオーバーライドして独自のスキャナ値を設定できます。

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 リストで、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、このヒストグラムと関連付ける送信元 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　変更を廃棄して [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。新しいスキャナ設定が、[Add Protocol Number] ダイアログボックスのリストに表示されます。

ヒント　変更を廃棄して [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。新しいプロトコル番号マップが [Protocol Number Map] タブのリストに表示されます。

ステップ 51　プロトコル番号マップを編集するには、リストでそのマップを選択し、[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。編集プロトコル番号マップが [Protocol Number Map] タブのリストに表示されます。

ステップ 53　プロトコル番号マップを削除するには、そのマップを選択して [Delete] をクリックします。これで、こ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した。

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から [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 リストで、値（[High]、[Medium]、または [Low]）を変更します。

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

ヒント　変更を廃棄して [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　[Apply] をクリックして、変更を適用し、改訂したコンフィギュレーションを保存します。

不正ゾーンの設定

（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必要があります。

ここでは、不正ゾーンの設定方法について説明します。次の事項について説明します。

[Illegal Zone] タブ

[Illegal Zone] タブには、4 つのタブがあります。

- [General]：不正ゾーンをイネーブルにし、このゾーンに含まれるサブネットを指定できます。
- [TCP Protocol]：TCP プロトコルをイネーブルにして、独自のしきい値および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て、独自のしきい値および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て、独自のしきい値および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の場合、このゾーンへのパケットは無視されます。デフォルトでは、ゾーンはイネーブルです。

次に、このゾーンに属す IP アドレスを追加します。ゾーンの IP アドレスをまったく設定していない場合は、すべてのパケットが、デフォルト ゾーンの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 Illegal Zone]：オンにした場合、不正ゾーンがイネーブルになります。

- [Service Subnets]：不正ゾーンに適用するサブネットを入力できます。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か、スキャナ設定をオーバーライドして独自のしきい値およびヒストグラムを追加できます。

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：特定のポートを TCP プロトコルと関連付けできます。
  - [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にされているかどうか。
  - [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]：しきい値の設定値が表示されます。
  - [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 になく、コンフィギュレーション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]：スキャナの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]：low、medium、high で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と関連付けられている送信元 IP アドレスの数が表示されます。

[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か、スキャナ設定をオーバーライドして独自のしきい値およびヒストグラムを追加できます。

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：特定のポートを UDP プロトコルと関連付けできます。
  - [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にされているかどうか。
  - [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]：しきい値の設定値が表示されます。
  - [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]：スキャナの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]：low、medium、high で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と関連付けられている送信元 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か、スキャナ設定をオーバーライドして独自のしきい値およびヒストグラムを追加できます。

フィールドの説明

[Other Protocol] 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：具体的なプロトコル番号をその他のプロトコルに関連付けできます。
  - [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にされているかどうか。
  - [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]：しきい値の設定値が表示されます。
  - [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]：スキャナの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]：low、medium、high で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と関連付けられている送信元 IP アドレスの数が表示されます。

[Add Protocol Number]/[Edit Protocol Number] ダイアログボックス

[Add Protocol Number]/[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できます。
- [Enable the Service]：サービスをイネーブル化できます。

- [Override Scanner Settings]：オンにすると、ヒストグラムを追加、編集、削除したり、すべて選択したりできます。
- [Scanner Threshold]：スキャナの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

異常検出の不正ゾーンを設定するには、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 IDM にログインします。

ステップ 2　[Configuration] > [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] チェックボックスはオンにする必要があり、オンにしないと設定するすべての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] チェックボックスはオンにする必要があり、オンにしないと TCP プロトコル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、さらに [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　このポート上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 11　こ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か、デフォルト値をオーバーライドして独自のスキャナ値を設定できます。

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 リストで、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、このヒストグラムと関連付ける送信元 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 変更を廃棄して [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。

新しいスキャナ設定が、[Add Destination Port] ダイアログボックスのリストに表示されます。

ヒント 変更を廃棄して [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。新しい宛先ポート マップが [Destination Port Map] タブのリストに表示されます。

ステップ 17 宛先ポート マップを編集するには、リストでそのマップを選択し、[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。編集した宛先ポート マップが [Destination Port Map] タブのリストに表示されます。

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

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から [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 リストで、値（[High]、[Medium]、または [Low]）を変更します。

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

ヒント 変更を廃棄して [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] チェックボックスはオンにする必要があり、オンにしないと UDP プロトコル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、さらに [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 このポート上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 28 こ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か、デフォルト値をオーバーライドして独自のスキャナ値を設定できます。

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 リストで、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、このヒストグラムと関連付ける送信元 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　変更を廃棄して [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。新しいスキャナ設定が、[Add Destination Port] ダイアログボックスのリストに表示されます。

ヒント　変更を廃棄して [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。新しい宛先ポート マップが [Destination Port Map] タブのリストに表示されます。

ステップ 34　宛先ポート マップを編集するには、リストでそのマップを選択し、[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。編集した宛先ポート マップが [Destination Port Map] タブのリストに表示されます。

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

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から [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 リストで、値（[High]、[Medium]、または [Low]）を変更します。

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

ヒント　変更を廃棄して [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する必要があり、オンにしないと、その他のプロトコル設定は無視されます。

ステップ 42　[Protocol Number Map] タブをクリックしてから [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　こ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　こ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か、デフォルト値をオーバーライドして独自のスキャナ値を設定できます。

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 リストで、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、このヒストグラムと関連付ける送信元 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　変更を廃棄して [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。新しいスキャナ設定が、[Add Protocol Number] ダイアログボックスのリストに表示されます。

ヒント　変更を廃棄して [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。新しいプロトコル番号マップが [Protocol Number Map] タブのリストに表示されます。

ステップ 51　プロトコル番号マップを編集するには、リストでそのマップを選択し、[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。編集プロトコル番号マップが [Protocol Number Map] タブのリストに表示されます。

ステップ 53　プロトコル番号マップを削除するには、そのマップを選択して [Delete] をクリックします。これで、こ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した。

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から [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 リストで、値（[High]、[Medium]、または [Low]）を変更します。

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

ヒント　変更を廃棄して [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　[Apply] をクリックして、変更を適用し、改訂したコンフィギュレーションを保存します。

外部ゾーンの設定

（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必要があります。

ここでは、外部ゾーンの設定方法について説明します。次の事項について説明します。

[External Zone] タブ

[External Zone] タブには、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て、独自のしきい値および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て、独自のしきい値および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て、独自のしきい値および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。内部ゾーンと不正ゾーンの一連の IP アドレスと一致しないパケットは、外部ゾーンによって処理されます。

[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か、スキャナ設定をオーバーライドして独自のしきい値およびヒストグラムを追加できます。

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：特定のポートを TCP プロトコルと関連付けできます。
  - [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にされているかどうか。
  - [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]：しきい値の設定値が表示されます。
  - [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 になく、コンフィギュレーション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]：スキャナの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]：low、medium、high で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と関連付けられている送信元 IP アドレスの数が表示されます。

[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か、スキャナ設定をオーバーライドして独自のしきい値およびヒストグラムを追加できます。

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：特定のポートを UDP プロトコルと関連付けできます。
  - [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にされているかどうか。
  - [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]：しきい値の設定値が表示されます。
  - [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]：スキャナの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]：low、medium、high で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と関連付けられている送信元 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か、スキャナ設定をオーバーライドして独自のしきい値およびヒストグラムを追加できます。

フィールドの説明

[Other Protocol] 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：具体的なプロトコル番号をその他のプロトコルに関連付けできます。
  - [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にされているかどうか。
  - [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]：しきい値の設定値が表示されます。
  - [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]：スキャナの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]：low、medium、high で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と関連付けられている送信元 IP アドレスの数が表示されます。

外部ゾーンの設定

異常検出の外部ゾーンを設定するには、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 IDM にログインします。

ステップ 2　[Configuration] > [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] チェックボックスはオンにする必要があり、オンにしないと設定するすべての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] チェックボックスはオンにする必要があり、オンにしないと TCP プロトコル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、さらに [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　このポート上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 9　こ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か、デフォルト値をオーバーライドして独自のスキャナ値を設定できます。

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 リストで、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、このヒストグラムと関連付ける送信元 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　変更を廃棄して [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。新しいスキャナ設定が、[Add Destination Port] ダイアログボックスのリストに表示されます。

ヒント　変更を廃棄して [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。新しい宛先ポート マップが [Destination Port Map] タブのリストに表示されます。

ステップ 15　宛先ポート マップを編集するには、リストでそのマップを選択し、[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。編集した宛先ポート マップが [Destination Port Map] タブのリストに表示されます。

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

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から [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 リストで、値（[High]、[Medium]、または [Low]）を変更します。

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

ヒント　変更を廃棄して [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] チェックボックスはオンにする必要があり、オンにしないと UDP プロトコル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、さらに [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　このポート上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 26　こ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か、デフォルト値をオーバーライドして独自のスキャナ値を設定できます。

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 リストで、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、このヒストグラムと関連付ける送信元 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　変更を廃棄して [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。新しいスキャナ設定が、[Add Destination Port] ダイアログボックスのリストに表示されます。

ヒント　変更を廃棄して [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。新しい宛先ポート マップが [Destination Port Map] タブのリストに表示されます。

ステップ 32　宛先ポート マップを編集するには、リストでそのマップを選択し、[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。編集した宛先ポート マップが [Destination Port Map] タブのリストに表示されます。

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

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から [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 リストで、値（[High]、[Medium]、または [Low]）を変更します。

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

ヒント　変更を廃棄して [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する必要があり、オンにしないと、その他のプロトコル設定は無視されます。

ステップ 40　[Protocol Number Map] タブをクリックしてから [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　こ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　こ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か、デフォルト値をオーバーライドして独自のスキャナ値を設定できます。

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 リストで、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、このヒストグラムと関連付ける送信元 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　変更を廃棄して [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。新しいスキャナ設定が、[Add Protocol Number] ダイアログボックスのリストに表示されます。

ヒント　変更を廃棄して [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。新しいプロトコル番号マップが [Protocol Number Map] タブのリストに表示されます。

ステップ 49　プロトコル番号マップを編集するには、リストでそのマップを選択し、[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。編集プロトコル番号マップが [Protocol Number Map] タブのリストに表示されます。

ステップ 51　プロトコル番号マップを削除するには、そのマップを選択して [Delete] をクリックします。これで、こ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した。

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て、[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 リストで、値（[High]、[Medium]、または [Low]）を変更します。

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

ヒント　変更を廃棄して [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　[Apply] をクリックして、変更を適用し、改訂したコンフィギュレーションを保存します。

異常検出のディセーブル化

注意　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。

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

ステップ 2　[Configuration] > [Policies] > [IPS Policies] を選択します。

ステップ 3　異常検出をオフにする仮想センサーを選択し、[Edit] をクリックします。

ステップ 4　[Anomaly Detection] の下の [AD Operational Mode] ドロップダウン リストから、異常検出モードとして [Inactive] を選択します。

ヒント　変更を廃棄して、[Edit Virtual Sensor] 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 5　[OK] 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 6　[Apply] をクリックして、変更を適用し、改訂したコンフィギュレーションを保存します。

詳細情報

ワームの動作の詳細については、「ワーム」（P.10-3）を参照してください。