CHAPTER 9

異常検出の設定

（注） 現在、Cisco IPS 7.1 をサポートしているプラットフォームは、IPS SSP を搭載した Cisco ASA 5585-X のみです。それ以外の Cisco IPS センサーは、IPS 7.1 を現在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。

この章では、異常検出（AD）およびその機能と、機能の設定方法について説明します。次のような構成になっています。

セキュリティ ポリシー

複数のセキュリティ ポリシーを作成し、それらを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、および異常検出ポリシーから構成されます。Cisco IPS には、sig0 という名前のデフォルトのシグニチャ定義ポリシー、rules0 という名前のデフォルトのイベント アクション規則ポリシー、および ad0 という名前のデフォルトの異常検出ポリシーが用意されています。仮想センサーにこれらのデフォルト ポリシーを割り当てることも、新しいポリシーを作成することもできます。複数のセキュリティ ポリシーを使用すれば、それぞれ異なる要件に基づいたセキュリティ ポリシーを作成し、そうしたカスタマイズされたポリシーを VLAN や物理インターフェイスごとに適用することが可能になります。

異常検出について

注意　異常検出では、両方向からトラフィックが取得されることを前提とします。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は、ワームに感染したホストを検出します。これにより、センサーでは、Code Red や SQL Slammer などのワームと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）　異常検出は、Nimda などの電子メール ベースのワームを検出しません。

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

- 異常検出を無効にする手順については、「異常検出の無効」（P.9-49）を参照してください。
- ワームがどのように動作するかの詳細については、「ワーム」（P.9-2）を参照してください。

ワーム

注意　異常検出では、両方向からトラフィックが取得されることを前提とします。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、そのホストにアクセスします。Code Red ワーム、Sasser ワーム、Blaster ワーム、および Slammer ワームは、この方法で広がるワームの例です。

異常検出では、スキャナとしての動作によって、ワームに感染したホストを識別します。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。ワームは、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、さまざまな宛先 IP アドレスへの不成功なアクセス試行を生成することによりこれらの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、異常な数の IP アドレスに対して同じ宛先ポートに未確立の接続を生成します。

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単一方向に伝送する UDP 接続などの単一方向接続です。ワームに感染したホストは、UDP プロトコルを使用してスキャンを行い、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と同じクアッド上でタイムアウト期間内に UDP パケットを受信しません。

ICMP などの他のプロトコルにとって重要なイベントは、送信元 IP アドレスからさまざまな宛先 IP アドレスに送信されます（つまり、単一方向で受信されるパケット）。

注意　ワームが感染する IP アドレスのリストを持ち、スキャニングを使用してワーム自体を拡散する必要がない場合（たとえば、アクティブ スキャニングとは異なり、パッシブ マッピングを使用してネットワークをリッスンする）、ワームは異常検出ワーム ポリシーによって検出されません。また、感染したホスト内のファイルをプローブすることによりメーリング 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、レイヤ 3 またはレイヤ 4 の異常が生成されないためです。

詳細情報

異常検出を無効にする手順については、「異常検出の無効」（P.9-49）を参照してください。

異常検出モード

異常検出は、最初に、ネットワークの最も通常の状態を反映する「平時」学習プロセスを実行します。次に、異常検出は、通常のネットワークに最適なポリシーしきい値セットを派生します。

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ありますが、デフォルトの期間である 24 時間、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。周期スケジュールのデフォルトの間隔値は 24 時間であり、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、24 時間後に初期 KB が置き換えられます。

（注）　異常検出では、空の初期 KB を処理するときに攻撃は検出されません。デフォルトの 24 時間後、KB は保存およびロードされ、異常検出によって攻撃が検出されるようになります。

（注）　ネットワークの複雑さに応じて、異常検出をデフォルトの 24 時間以上、学習受け入れモードのままにすることができます。

- 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 が置換されたあとで、異常検出は KB に基づいて攻撃を検出します。異常検出は、KB のしきい値に違反するネットワーク トラフィック フローを見つけると、アラートを送信します。異常検出は異常を探すときに、しきい値に違反しない KB の段階的な変更を記録し、新しい KB を作成します。新しい KB は定期的に保存され、古い KB を置き換えるため、最新の KB が保持されます。
- 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無効にできます。ある状況では、異常検出を非アクティブ モードにする必要があります（センサーが非対称環境で動作している場合など）。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。

例

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 11:00 pm に追加し、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 の処理を開始し、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 10:00 am）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であり、異常検出には新しい KB があるため、攻撃の検出が開始されます。

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、「IPS SSP 上での仮想センサーの追加、編集、および削除」（P.6-3）を参照してください。
- ワームがどのように動作するかの詳細については、「ワーム」（P.9-2）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。内部、不正、および外部の 3 つのゾーンが存在し、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が 0.0.0.0 ～ 255.255.255.255 の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の IP アドレス 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。このように設定した場合、内部ゾーンは使用している IP アドレス範囲に送信されるすべてのトラフィックであり、外部ゾーンはインターネットに送信されるすべてのトラフィックです。

不正ゾーンは、通常のトラフィックでは決して見られない IP アドレス範囲（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 アドレス範囲の一部など）で設定できます。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

ゾーンの設定手順については、「内部ゾーンの設定」（P.9-11）、「不正ゾーンの設定」（P.9-20）、および「外部ゾーンの設定」（P.9-28）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。KB 学習しきい値を上書きするしきい値セットを設定できます。ただし、異常検出は、検出をどのように設定するかに関係なく学習を続行します。また、KB をインポート、エクスポート、およびロードし、KB のデータを参照することもできます。

異常検出の設定時は、次の手順を実行します。

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である ad0 を使用します。

2. 仮想センサーに異常検出ポリシーを追加します。
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、動作モードは検出に設定されます。ただし、最初の 24 時間は、データが入力された KB を作成するために学習が実行されます。初期 KB は空であるため、デフォルトの 24 時間、異常検出は KB に入力するために使用するデータを収集します。学習期間をデフォルトの 24 時間以上にする場合は、手動でモードを学習受け入れに設定する必要があります。
5. センサーが少なくとも 24 時間（デフォルト値）学習受け入れモードで動作するようにします。

   初期 KB に対してネットワークの通常の状態に関する情報を収集できるよう、センサーを少なくとも 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。この時間の経過後に、センサーは、ネットワークの通常のアクティビティのベースラインとして初期 KB を保存します。

   （注） センサーを少なくとも 24 時間、学習受け入れモードのままにすることが推奨されます。ただし、さらに長い時間（最大 1 週間）センサーを学習受け入れモードで動作させることが理想的です。

6. 異常検出を手動で学習受け入れモードに設定する場合は、再び検出モードに切り替えます。
7. 次のように、異常検出パラメータを設定します。
   - ワーム タイムアウトと、異常検出でバイパスする必要がある送信元および宛先 IP アドレスを設定します。
   - このタイムアウトの経過後、スキャナしきい値が設定された値に戻ります。
   - 異常検出が検出モードにある場合に、自動 KB 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 アクションを持つよう 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 アクションを持つようシグニチャを設定します。

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、「IPS SSP 上での仮想センサーの追加、編集、および削除」（P.6-3）を参照してください。
- 新しい異常検出ポリシーの設定手順については、「異常検出ポリシーの使用」（P.9-8）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.9-11）、「不正ゾーンの設定」（P.9-20）、および「外部ゾーンの設定」（P.9-28）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.9-3）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.9-37）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.9-6）を参照してください。
- 拒否攻撃者イベント アクションの詳細については、「イベント アクション」（P.8-4）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。異常検出で異常が見つかると、これらのシグニチャに関するアラートがトリガーされます。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。アラートの詳細は、ヒストグラムがトリガーされたため、ワーム検出に使用されるしきい値を示します。その時点から、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。

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送信されたこ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るパケットに対する IP ロギングを開始します。
- deny-attacker-service-pair-inline：送信元 IP アドレスと宛先ポートをブロックします。
- request-snmp-trapRequest：NotificationApp に要求を送信して SNMP 通知を実行します。
- request-block-host：このホスト（攻撃者）をブロックするよう、ARC に要求を送信します。

表 9-1 に、異常検出ワーム シグニチャのリストを示します。

表 9-1　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 プロトコルを介して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。

表 9-1　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
13001	1	Internal UDP Scanner	内部ゾーンで UDP プロトコル上にワーム攻撃を識別しました。UDP ヒストグラムのしきい値を超え、UDP プロトコル上にスキャナが識別されました。
13002	0	Internal Other Scanner	内部ゾーンでほかのプロトコル上に単一スキャナを識別しました。
13002	1	Internal Other Scanner	内部ゾーンでほかのプロトコル上にワーム攻撃を識別しました。ほかのヒストグラムのしきい値を超え、ほか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 プロトコルを介して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	外部ゾーンで他のプロトコルを介して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。
13006	1	Illegal TCP Scanner	不正ゾーンで TCP プロトコルを介してワーム攻撃を識別しました。TCP ヒストグラムのしきい値が超え、TCP プロトコルを介して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。

表 9-1　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
13008	0	Illegal Other Scanner	不正ゾーンでほかのプロトコルを介して単一スキャナを識別しました。
13008	1	Illegal Other Scanner	不正ゾーンでほかのプロトコルを介してワーム攻撃を識別しました。他のヒストグラムのしきい値を超え、他のプロトコルを介してスキャナが識別されました。

詳細情報

アクションをシグニチャに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.7-16）を参照してください。

異常検出ポリシーの使用

サービス異常検出サブモードで **service anomaly-detection** *name* コマンドを使用して、異常検出ポリシーを作成します。この異常検出ポリシーの値は、編集するまでデフォルトの異常検出ポリシーである ad0 と同じです。

また、特権 EXEC モードで、**copy anomaly-detection** *source_destination* コマンドを使用して、既存のポリシーのコピーを作成し、必要に応じて新しいポリシーの値を編集することもできます。

特権 EXEC モードで **list anomaly-detection-configurations** コマンドを使用して、異常検出ポリシーをリストします。

グローバル コンフィギュレーション モードで **no service anomaly-detection** *name* コマンドを使用して、異常検出ポリシーを削除します。グローバル コンフィギュレーション モードで **default service anomaly-detection** *name* コマンドを使用して、異常検出ポリシーを工場出荷時の設定にリセットします。

異常検出ポリシーを作成、コピー、表示、編集、および削除するには、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　異常検出ポリシーを作成します。

```
ips-ssp# configure terminal
ips-ssp(config)# service anomaly-detection MyAnomaly Detection
Editing new instance MyAnomaly Detection.
ips-ssp(config-ano)# exit
Apply Changes?[yes]: yes
ips-ssp(config)# exit
ips-ssp#
```

ステップ 3　または、既存の異常検出ポリシーを新しい異常検出ポリシーにコピーします。

```
ips-ssp# copy anomaly-detection ad0 ad1
ips-ssp#
```

（注）　ポリシーがすでに存在しているか、新しいポリシーに必要な容量が不足していると、エラーが表示されます。

ステップ 4　デフォルトの異常検出ポリシー値を受け入れるか、次のようなパラメータの編集を行います。

a. 動作の設定を行います。

b. ゾーンを設定します。

c. 学習受け入れモードを設定します。

d. KB の操作方法を学習します。

ステップ 5　センサーに異常検出ポリシーのリストを表示します。

```
ips-ssp# list anomaly-detection-configurations
Anomaly Detection
   Instance    Size    Virtual Sensor
   ad0         255     vs0
   temp        707     N/A
   MyAnomaly Detection        255     N/A
   ad1         141     vs1
ips-ssp#
```

ステップ 6　異常検出ポリシーを削除します。

```
ips-ssp# configure terminal
ips-ssp(config)# no service anomaly-detection MyAnomaly Detection
ips-ssp(config)# exit
ips-ssp#
```

（注）　デフォルトの異常検出ポリシーである ad0 を削除することはできません。

ステップ 7　異常検出インスタンスが削除されたことを確認します。

```
ips-ssp# list anomaly-detection-configurations
Anomaly Detection
   Instance    Size    Virtual Sensor
   ad0         204     vs0
   ad1         141     N/A
ips-ssp#
```

ステップ 8　異常検出ポリシーを工場出荷時の設定にリセットします。

```
ips-ssp# configure terminal
ips-ssp(config)# default service anomaly-detection ad1
ips-ssp(config)#
```

詳細情報

- 動作の設定手順については、「異常検出動作の設定」（P.9-10）を参照してください。
- 異常検出ゾーンの設定手順については、「内部ゾーンの設定」（P.9-11）、「不正ゾーンの設定」（P.9-20）、および「外部ゾーンの設定」（P.9-28）を参照してください。
- 学習受け入れモードの設定手順については、「学習受け入れモードの設定」（P.9-38）を参照してください。
- KB を操作する手順については、「KB ファイルの操作」（P.9-40）を参照してください。

異常検出動作の設定

サービス異常検出サブモードで **worm-timeout** コマンドを使用して、ワーム検出タイムアウトを設定します。このタイムアウトの経過後、スキャナしきい値が設定された値に戻ります。サービス異常検出サブモードで **ignore** コマンドを使用して、異常検出が KB のために情報を収集するときにセンサーが無視する送信元および宛先 IP アドレスを設定します。異常検出はこれらの送信元および宛先 IP アドレスを追跡せず、KB しきい値はこれらの IP アドレスの影響を受けません。

オプション

次のオプションが適用されます。

- **worm-timeout**：ワーム終了タイムアウトの時間（秒単位）を指定します。範囲は 120 ～ 10,000,000 秒です。デフォルトは 600 秒です。
- **ignore**：異常検出の処理中に無視する IP アドレスを指定します。
  - **enabled [true | false]**：無視される IP アドレスのリストをイネーブルまたはディセーブルにします。デフォルトはイネーブルです。
  - **source-ip-address-range**：処理中に異常検出が無視する送信元 IP アドレスを指定します。
  - **dest-ip-address-range**：処理中に異常検出が無視する宛先 IP アドレスを指定します。

（注）　IP アドレスの形式は、<A.B.C.D>-<A.B.C.D>[,<A.B.C.D>-<A.B.C.D>] のようになります。

異常検出動作設定の指定

異常検出動作設定を指定するには、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　異常検出サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service anomaly-detection ad1
```

ステップ 3　ワーム タイムアウトを指定します。

```
ips-ssp(config-ano)# worm-timeout 800
```

ステップ 4　設定を確認します。

```
ips-ssp(config-ano)# show settings
   worm-timeout: 800 seconds default: 600
```

ステップ 5　異常検出の処理中に無視する宛先 IP アドレスを指定します。

```
ips-ssp(config-ano)# ignore
ips-ssp(config-ano-ign)# dest-ip-address-range 10.10.5.5,10.10.2.1-10.10.2.30
```

ステップ 6　異常検出の処理中に無視する送信元 IP アドレスを指定します。

```
ips-ssp(config-ano-ign)# source-ip-address-range 10.20.30.108-10.20.30.191
```

ステップ 7　設定を確認できます。

```
ips-ssp(config-ano-ign)# show settings
   ignore
   -----------------------------------------------
      enabled: true default: true
      source-ip-address-range: 10.20.30.108-10.20.30.191 default: 0.0.0.0
      dest-ip-address-range: 10.10.5.5,10.10.2.1-10.10.2.30 default: 0.0.0.0
   -----------------------------------------------
ips-ssp(config-ano-ign)#
```

ステップ 8　異常検出サブモードを終了します。

```
ips-ssp(config-ano-ign)# exit
ips-ssp(config-ano)# exit
Apply Changes:?[yes]:
```

ステップ 9　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

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。次のような構成になっています。

内部ゾーンについて

内部ゾーンは、使用している内部ネットワークを表す必要があります。また、使用している IP アドレス範囲に送信されるすべてのトラフィックを受信する必要があります。ゾーンがディセーブルな場合は、このゾーンに対するパケットが無視されます。デフォルトでは、ゾーンは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。すべてのゾーンに対して IP アドレスを設定しない場合は、すべてのパケットがデフォルトのゾーンである外部ゾーンに送信されます。

内部ゾーンに対して TCP、UDP、および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できます。TCP および UDP プロトコルに対して宛先ポートを設定したり、その他のプロトコルに対してプロトコル番号を設定したりできます。デフォルトしきい値を使用するか、あるいはスキャナ設定を上書きして、独自のしきい値とヒストグラムを追加できます。

内部ゾーンの設定

サービス異常検出サブモードで **internal-zone** {**enabled** | **ip-address-range** | **tcp** | **udp** |**other**} コマンドを使用して、内部ゾーンをイネーブルにし、IP アドレスを内部ゾーンに追加し、プロトコルを指定します。

オプション

次のオプションが適用されます。

- **enabled** {**true** | **false** }：ゾーンをイネーブルまたはディセーブルにします。
- **ip-address-range**：ゾーンのサブネットの IP アドレスを指定します。有効な値は <A.B.C.D>-<A.B.C.D>[,<A.B.C.D>-<A.B.C.D>] です。

（注） 範囲内の 2 番目の IP アドレスは、最初の IP アドレス以上である必要があります。

- **tcp**：TCP プロトコルを設定できます。
- **udp**：UDP プロトコルを設定できます。
- **other**：TCP と UDP 以外の他のプロトコルを設定できます。

内部ゾーンの設定

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　異常検出内部ゾーン サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service anomaly-detection ad0
ips-ssp(config-ano)# internal-zone
ips-ssp(config-ano-int)#
```

ステップ 3　内部ゾーンをイネーブルにします。

```
ips-ssp(config-ano-int)# enabled true
```

ステップ 4　内部ゾーンに含める IP アドレスを設定します。

```
ips-ssp(config-ano-int)# ip-address-range 192.0.2.72-192.0.2.108
```

ステップ 5　TCP プロトコルを設定します。

ステップ 6　UDP プロトコルを設定します。

ステップ 7　その他のプロトコルを設定します。

詳細情報

- TCP プロトコルの設定手順については、「内部ゾーンに対する TCP プロトコルの設定」（P.9-13）を参照してください。
- UDP プロトコルの設定手順については、「内部ゾーンに対する UDP プロトコルの設定」（P.9-15）を参照してください。
- その他のプロトコルの設定手順については、「内部ゾーンに対する他のプロトコルの設定」（P.9-18）を参照してください。

内部ゾーンに対する TCP プロトコルの設定

サービス異常検出内部ゾーン サブモードで **tcp** {**enabled** | **dst-port** *number* | **default-thresholds**} コマンドを使用して、TCP サービスをイネーブルにし、設定します。

オプション

次のオプションが適用されます。

- **enabled** {**true** | **false** }：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。
- **default-thresholds**：宛先ポート マップで指定されないすべてのポートに使用されるしきい値を定義します。
  - **threshold-histogram {low | medium | high} num-source-ips** *number*：しきい値ヒストグラムの値を設定します。
  - **scanner-threshold**：スキャナしきい値を設定します。デフォルトは 200 です。
- **dst-port** *number*：特定の宛先ポートに対してしきい値を定義します。有効な値は 0 ～ 65535 です。
- **enabled** {**true** | **false**}：サービスをイネーブルまたはディセーブルにします。
- **override-scanner-settings** {**yes** | **no**}：スキャナ値を上書きできます。
  - **threshold-histogram {low | medium | high} num-source-ips** *number*：しきい値ヒストグラムの値を設定します。
  - **scanner-threshold**：スキャナしきい値を設定します。デフォルトは 200 です。

内部ゾーン TCP プロトコルの設定

内部ゾーンに対して TCP プロトコルを設定するには、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　異常検出内部ゾーン サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service anomaly-detection ad0
ips-ssp(config-ano)# internal-zone
ips-ssp(config-ano-int)#
```

ステップ 3　TCP プロトコルをイネーブルにします。

```
ips-ssp(config-ano-int)# tcp
ips-ssp(config-ano-int-tcp)# enabled true
```

ステップ 4　特定のポートを TCP プロトコルに関連付けます。

```
ips-ssp(config-ano-int-tcp)# dst-port 20
ips-ssp(config-ano-int-tcp-dst)#
```

ステップ 5　そのポートのサービスをイネーブルにします。

```
ips-ssp(config-ano-int-tcp-dst)# enabled true
```

ステップ 6　そのポートのスキャナ値を上書きします。デフォルトのスキャナ値を使用するか、あるいはそれらの値を上書きし、独自のスキャナ値を設定できます。

```
ips-ssp(config-ano-int-tcp-dst)# override-scanner-settings yes
ips-ssp(config-ano-int-tcp-dst-yes)#
```

ステップ 7　新しいスキャナ設定に対してヒストグラムを追加します。宛先 IP アドレスの数（low、medium、または high）と、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。

```
ips-ssp(config-ano-int-tcp-dst-yes)# threshold-histogram low num-source-ips 100
```

ステップ 8　スキャナしきい値を設定します。

```
ips-ssp(config-ano-int-tcp-dst-yes)# scanner-threshold 100
```

ステップ 9　他のすべての未指定ポートに対してデフォルトしきい値を設定します。

```
ips-ssp(config-ano-int-tcp-dst-yes)# exit
ips-ssp(config-ano-int-tcp-dst)# exit
ips-ssp(config-ano-int-tcp)# exit
ips-ssp(config-ano-int-tcp)# default-thresholds
ips-ssp(config-ano-int-tcp-def)# default-thresholds
ips-ssp(config-ano-int-tcp-def)# threshold-histogram medium num-source-ips 120
ips-ssp(config-ano-int-tcp-def)# scanner-threshold 120
```

ステップ 10　TCP 設定を確認します。

```
ips-ssp(config-ano-int-tcp)# show settings
   tcp
   ------------------------------------------------
      dst-port (min: 0, max: 65535, current: 4)
      ------------------------------------------------
         number: 20
         ------------------------------------------------
            override-scanner-settings
            ------------------------------------------------
               yes
               ------------------------------------------------
                  scanner-threshold: 120 default: 200
                  threshold-histogram (min: 0, max: 3, current: 1)
                  ------------------------------------------------
                     dest-ip-bin: low
                     num-source-ips: 100
                  ------------------------------------------------
               ------------------------------------------------
            ------------------------------------------------
            enabled: true default: true
         ------------------------------------------------
         number: 23
         ------------------------------------------------
            override-scanner-settings
            ------------------------------------------------
               no
               ------------------------------------------------
               ------------------------------------------------
            ------------------------------------------------
            enabled: true <defaulted>
         ------------------------------------------------
         number: 113
         ------------------------------------------------
            override-scanner-settings
            ------------------------------------------------
               no
               ------------------------------------------------
               ------------------------------------------------
            ------------------------------------------------
            enabled: true <defaulted>
         ------------------------------------------------
         number: 567
         ------------------------------------------------
            override-scanner-settings
```

```
            ------------------------------------------------
               no
               ------------------------------------------------
               ------------------------------------------------
            ------------------------------------------------
            enabled: true <defaulted>
         ------------------------------------------------
      ------------------------------------------------
      default-thresholds
      ------------------------------------------------
         scanner-threshold: 120 default: 200
         threshold-histogram (min: 0, max: 3, current: 3)
         ------------------------------------------------
            <protected entry>
            dest-ip-bin: low <defaulted>
            num-source-ips: 10 <defaulted>
            <protected entry>
            dest-ip-bin: medium
            num-source-ips: 120 default: 1
            <protected entry>
            dest-ip-bin: high <defaulted>
            num-source-ips: 1 <defaulted>
         ------------------------------------------------
      ------------------------------------------------
      enabled: true <defaulted>
   ------------------------------------------------
ips-ssp(config-ano-int-tcp)#
```

内部ゾーンに対する UDP プロトコルの設定

サービス異常検出内部ゾーン サブモードで **udp** {**enabled** | **dst-port** *number* | **default-thresholds**} コマンドを使用して、UDP サービスをイネーブルにし、設定します。

オプション

次のオプションが適用されます。

- **enabled** {**true** | **false** }：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。
- **default-thresholds**：宛先ポート マップで指定されないすべてのポートに使用されるしきい値を定義します。
  - **threshold-histogram {low | medium | high} num-source-ips** *number*：しきい値ヒストグラムの値を設定します。
  - **scanner-threshold**：スキャナしきい値を設定します。デフォルトは 200 です。
- **dst-port** *number*：特定の宛先ポートに対してしきい値を定義します。有効な値は 0 ～ 65535 です。
- **enabled** {**true** | **false**}：サービスをイネーブルまたはディセーブルにします。
- **override-scanner-settings** {**yes** | **no**}：スキャナ値を上書きできます。
  - **threshold-histogram {low | medium | high} num-source-ips** *number*：しきい値ヒストグラムの値を設定します。
  - **scanner-threshold**：スキャナしきい値を設定します。デフォルトは 200 です。

内部ゾーン UDP プロトコルの設定

ゾーンに対して UDP プロトコルを設定するには、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　異常検出内部ゾーン サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service anomaly-detection ad0
ips-ssp(config-ano)# internal-zone
ips-ssp(config-ano-int)#
```

ステップ 3　UDP プロトコルをイネーブルにします。

```
ips-ssp(config-ano-int)# udp
ips-ssp(config-ano-int-udp)# enabled true
```

ステップ 4　特定のポートを UDP プロトコルに関連付けます。

```
ips-ssp(config-ano-int-udp)# dst-port 20
ips-ssp(config-ano-int-udp-dst)#
```

ステップ 5　そのポートのサービスをイネーブルにします。

```
ips-ssp(config-ano-int-udp-dst)# enabled true
```

ステップ 6　そのポートのスキャナ値を上書きします。デフォルトのスキャナ値を使用するか、あるいはそれらの値を上書きし、独自のスキャナ値を設定できます。

```
ips-ssp(config-ano-int-udp-dst)# override-scanner-settings yes
ips-ssp(config-ano-int-udp-dst-yes)#
```

ステップ 7　新しいスキャナ設定に対してヒストグラムを追加します。宛先 IP アドレスの数（low、medium、または high）と、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。

```
ips-ssp(config-ano-int-udp-dst-yes)# threshold-histogram low num-source-ips 100
```

ステップ 8　スキャナしきい値を設定します。

```
ips-ssp(config-ano-int-udp-dst-yes)# scanner-threshold 100
```

ステップ 9　他のすべての未指定ポートに対してデフォルトしきい値を設定します。

```
ips-ssp(config-ano-int-udp-dst-yes)# exit
ips-ssp(config-ano-int-udp-dst)# exit
ips-ssp(config-ano-int-udp)# default-thresholds
ips-ssp(config-ano-int-udp-def)# default-thresholds
ips-ssp(config-ano-int-udp-def)# threshold-histogram medium num-source-ips 120
ips-ssp(config-ano-int-udp-def)# scanner-threshold 120
```

ステップ 10　UDP 設定を確認します。

```
ips-ssp(config-ano-int-udp)# show settings
   udp
   ----------------------------------------------
      dst-port (min: 0, max: 65535, current: 4)
      ----------------------------------------------
         number: 20
         ----------------------------------------------
            override-scanner-settings
            ----------------------------------------------
               yes
               ----------------------------------------------
                  scanner-threshold: 100 default: 200
                  threshold-histogram (min: 0, max: 3, current: 1)
```

```
                  ------------------------------------------------
                     dest-ip-bin: low
                     num-source-ips: 100
                  ------------------------------------------------
               ------------------------------------------------
            ------------------------------------------------
            enabled: true default: true
         ------------------------------------------------
         number: 23
         ------------------------------------------------
            override-scanner-settings
            ------------------------------------------------
               no
               ------------------------------------------------
               ------------------------------------------------
            ------------------------------------------------
            enabled: true <defaulted>
         ------------------------------------------------
         number: 113
         ------------------------------------------------
            override-scanner-settings
            ------------------------------------------------
               no
               ------------------------------------------------
               ------------------------------------------------
            ------------------------------------------------
            enabled: true <defaulted>
         ------------------------------------------------
         number: 567
         ------------------------------------------------
            override-scanner-settings
            ------------------------------------------------
               no
               ------------------------------------------------
               ------------------------------------------------
            ------------------------------------------------
            enabled: true <defaulted>
         ------------------------------------------------
      ------------------------------------------------
      default-thresholds
      ------------------------------------------------
         scanner-threshold: 120 default: 200
         threshold-histogram (min: 0, max: 3, current: 3)
         ------------------------------------------------
            <protected entry>
            dest-ip-bin: low <defaulted>
            num-source-ips: 10 <defaulted>
            <protected entry>
            dest-ip-bin: medium
            num-source-ips: 120 default: 1
            <protected entry>
            dest-ip-bin: high <defaulted>
            num-source-ips: 1 <defaulted>
         ------------------------------------------------
      ------------------------------------------------
      enabled: true <defaulted>
   ------------------------------------------------
ips-ssp(config-ano-int-udp)#
```

内部ゾーンに対する他のプロトコルの設定

サービス異常検出内部ゾーン サブモードで **other** {**enabled** | **protocol** *number* | **default-thresholds**} コマンドを使用して、他のサービスをイネーブルにし、設定します。

オプション

次のオプションが適用されます。

- **enabled** {**true** | **false** }：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。
- **default-thresholds**：宛先ポート マップで指定されないすべてのポートに使用されるしきい値を定義します。
  - **threshold-histogram {low | medium | high} num-source-ips** *number*：しきい値ヒストグラムの値を設定します。
  - **scanner-threshold**：スキャナしきい値を設定します。デフォルトは 200 です。
- **protocol-number** *number*：特定のプロトコルに対するしきい値を定義します。有効な値は 0 ～ 255 です。
- **enabled** {**true** | **false**}：サービスをイネーブルまたはディセーブルにします。
- **override-scanner-settings** {**yes** | **no**}：スキャナ値を上書きできます。
  - **threshold-histogram {low | medium | high} num-source-ips** *number*：しきい値ヒストグラムの値を設定します。
  - **scanner-threshold**：スキャナしきい値を設定します。デフォルトは 200 です。

内部ゾーンの他のプロトコルの設定

ゾーンに対して他のプロトコルを設定するには、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　異常検出内部ゾーン サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service anomaly-detection ad0
ips-ssp(config-ano)# internal-zone
ips-ssp(config-ano-int)#
```

ステップ 3　他のプロトコルをイネーブルにします。

```
ips-ssp(config-ano-int)# other
ips-ssp(config-ano-int-oth)# enabled true
```

ステップ 4　他のプロトコルに対して特定の番号を関連付けます。

```
ips-ssp(config-ano-int-oth)# protocol-number 5
ips-ssp(config-ano-int-oth-pro)#
```

ステップ 5　そのポートのサービスをイネーブルにします。

```
ips-ssp(config-ano-int-oth-pro)# enabled true
```

ステップ 6　そのプロトコルに対するスキャナ値を上書きします。デフォルトのスキャナ値を使用するか、あるいはそれらの値を上書きし、独自のスキャナ値を設定できます。

```
ips-ssp(config-ano-int-oth-pro)# override-scanner-settings yes
ips-ssp(config-ano-int-oth-pro-yes)#
```

ステップ 7　新しいスキャナ設定に対してヒストグラムを追加します。宛先 IP アドレスの数（low、medium、または high）と、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。

```
ips-ssp(config-ano-int-oth-pro-yes)# threshold-histogram high num-source-ips 75
```

ステップ 8　スキャナしきい値を設定します。

```
ips-ssp(config-ano-int-oth-pro-yes)# scanner-threshold 100
```

ステップ 9　他のすべての未指定ポートに対してデフォルトしきい値を設定します。

```
ips-ssp(config-ano-int-oth-pro-yes)# exit
ips-ssp(config-ano-int-oth-pro)# exit
ips-ssp(config-ano-int-oth)# default-thresholds
ips-ssp(config-ano-int-oth-def)# default-thresholds
ips-ssp(config-ano-int-oth-def)# threshold-histogram medium num-source-ips 120
ips-ssp(config-ano-int-oth-def)# scanner-threshold 120
```

ステップ 10　他の設定を確認します。

```
ips-ssp(config-ano-int-oth)# show settings
   other
   -----------------------------------------------
      protocol-number (min: 0, max: 255, current: 1)
      -----------------------------------------------
         number: 5
         -----------------------------------------------
            override-scanner-settings
            -----------------------------------------------
               yes
               -----------------------------------------------
                  scanner-threshold: 95 default: 200
                  threshold-histogram (min: 0, max: 3, current: 1)
                  -----------------------------------------------
                     dest-ip-bin: high
                     num-source-ips: 75
                  -----------------------------------------------
               -----------------------------------------------
            -----------------------------------------------
            enabled: true default: true
         -----------------------------------------------
      -----------------------------------------------
      default-thresholds
      -----------------------------------------------
         scanner-threshold: 200 <defaulted>
         threshold-histogram (min: 0, max: 3, current: 3)
         -----------------------------------------------
            <protected entry>
            dest-ip-bin: low <defaulted>
            num-source-ips: 10 <defaulted>
            <protected entry>
            dest-ip-bin: medium <defaulted>
            num-source-ips: 1 <defaulted>
            <protected entry>
            dest-ip-bin: high <defaulted>
            num-source-ips: 1 <defaulted>
         -----------------------------------------------
      -----------------------------------------------
      enabled: true default: true
   -----------------------------------------------
ips-ssp(config-ano-int-oth)#
```

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。次のような構成になっています。

不正ゾーンについて

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（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 アドレス範囲の一部など）を表す必要があります。

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

内部ゾーンに対して TCP、UDP、および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できます。TCP および UDP プロトコルに対して宛先ポートを設定したり、その他のプロトコルに対してプロトコル番号を設定したりできます。デフォルトしきい値を使用するか、あるいはスキャナ設定を上書きして、独自のしきい値とヒストグラムを追加できます。

不正ゾーンの設定

サービス異常検出サブモードで **illegal-zone** {**enabled** | **ip-address-range** | **tcp** | **udp** |**other**} コマンドを使用して、不正ゾーンをイネーブルにし、IP アドレスを不正ゾーンに追加し、プロトコルを指定します。

オプション

次のオプションが適用されます。

- **enabled** {**true** | **false** }：ゾーンをイネーブルまたはディセーブルにします。
- **ip-address-range**：ゾーンのサブネットの IP アドレスを指定します。有効な値は <A.B.C.D>-<A.B.C.D>[,<A.B.C.D>-<A.B.C.D>] です。

  （注）　範囲内の 2 番目の IP アドレスは、最初の IP アドレス以上である必要があります。

- **tcp**：TCP プロトコルを設定できます。
- **udp**：UDP プロトコルを設定できます。
- **other**：TCP と UDP 以外の他のプロトコルを設定できます。

不正ゾーンの設定

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　異常検出不正ゾーン サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service anomaly-detection ad0
ips-ssp(config-ano)# illegal-zone
ips-ssp(config-ano-ill)#
```

ステップ 3　不正ゾーンをイネーブルにします。

```
ips-ssp(config-ano-ill)# enabled true
```

ステップ 4　不正ゾーンに含める IP アドレスを設定します。

```
ips-ssp(config-ano-ill)# ip-address-range 192.0.2.72-192.0.2.108
```

ステップ 5　TCP プロトコルを設定します。

ステップ 6　UDP プロトコルを設定します。

ステップ 7　その他のプロトコルを設定します。

詳細情報

- TCP プロトコルの設定手順については、「不正ゾーンに対する TCP プロトコルの設定」（P.9-21）を参照してください。
- UDP プロトコルの設定手順については、「不正ゾーンに対する UDP プロトコルの設定」（P.9-24）を参照してください。
- その他のプロトコルの設定手順については、「不正ゾーンに対する他のプロトコルの設定」（P.9-26）を参照してください。

不正ゾーンに対する TCP プロトコルの設定

サービス異常検出不正ゾーン サブモードで **tcp** {**enabled** | **dst-port** *number* | **default-thresholds**} コマンドを使用して、TCP サービスをイネーブルにし、設定します。

オプション

次のオプションが適用されます。

- **enabled** {**true** | **false** }：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。
- **default-thresholds**：宛先ポート マップで指定されないすべてのポートに使用されるしきい値を定義します。
  - **threshold-histogram {low | medium | high} num-source-ips** *number*：しきい値ヒストグラムの値を設定します。
  - **scanner-threshold**：スキャナしきい値を設定します。デフォルトは 200 です。
- **dst-port** *number*：特定の宛先ポートに対してしきい値を定義します。有効な値は 0 ～ 65535 です。
- **enabled** {**true** | **false**}：サービスをイネーブルまたはディセーブルにします。

- **override-scanner-settings** {**yes** | **no**}：スキャナ値を上書きできます。
  - **threshold-histogram {low | medium | high} num-source-ips** *number*：しきい値ヒストグラムの値を設定します。
  - **scanner-threshold**：スキャナしきい値を設定します。デフォルトは 200 です。

不正ゾーン TCP プロトコルの設定

不正ゾーンに対して TCP プロトコルを設定するには、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　異常検出不正ゾーン サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service anomaly-detection ad0
ips-ssp(config-ano)# illegal-zone
ips-ssp(config-ano-ill)#
```

ステップ 3　TCP プロトコルをイネーブルにします。

```
ips-ssp(config-ano-ill)# tcp
ips-ssp(config-ano-ill-tcp)# enabled true
```

ステップ 4　特定のポートを TCP プロトコルに関連付けます。

```
ips-ssp(config-ano-ill-tcp)# dst-port 20
ips-ssp(config-ano-ill-tcp-dst)#
```

ステップ 5　そのポートのサービスをイネーブルにします。

```
ips-ssp(config-ano-ill-tcp-dst)# enabled true
```

ステップ 6　そのポートのスキャナ値を上書きします。デフォルトのスキャナ値を使用するか、あるいはそれらの値を上書きし、独自のスキャナ値を設定できます。

```
ips-ssp(config-ano-ill-tcp-dst)# override-scanner-settings yes
ips-ssp(config-ano-ill-tcp-dst-yes)#
```

ステップ 7　新しいスキャナ設定に対してヒストグラムを追加します。宛先 IP アドレスの数（low、medium、または high）と、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。

```
ips-ssp(config-ano-ill-tcp-dst-yes)# threshold-histogram low num-source-ips 100
```

ステップ 8　スキャナしきい値を設定します。

```
ips-ssp(config-ano-ill-tcp-dst-yes)# scanner-threshold 100
```

ステップ 9　他のすべての未指定ポートに対してデフォルトしきい値を設定します。

```
ips-ssp(config-ano-ill-tcp-dst-yes)# exit
ips-ssp(config-ano-ill-tcp-dst)# exit
ips-ssp(config-ano-ill-tcp)# exit
ips-ssp(config-ano-ill-tcp)# default-thresholds
ips-ssp(config-ano-ill-tcp-def)# default-thresholds
ips-ssp(config-ano-ill-tcp-def)# threshold-histogram medium num-source-ips 120
ips-ssp(config-ano-ill-tcp-def)# scanner-threshold 120
```

ステップ 10　TCP 設定を確認します。

```
ips-ssp(config-ano-ill-tcp)# show settings
   tcp
   ------------------------------------------------
      dst-port (min: 0, max: 65535, current: 4)
      ------------------------------------------------
         number: 20
         ------------------------------------------------
            override-scanner-settings
            ------------------------------------------------
               yes
               ------------------------------------------------
                  scanner-threshold: 100 default: 200
                  threshold-histogram (min: 0, max: 3, current: 1)
                  ------------------------------------------------
                     dest-ip-bin: low
                     num-source-ips: 100
                  ------------------------------------------------
               ------------------------------------------------
            ------------------------------------------------
            enabled: true default: true
         ------------------------------------------------
         number: 23
         ------------------------------------------------
            override-scanner-settings
            ------------------------------------------------
               no
               ------------------------------------------------
               ------------------------------------------------
            ------------------------------------------------
            enabled: true <defaulted>
         ------------------------------------------------
         number: 113
         ------------------------------------------------
            override-scanner-settings
            ------------------------------------------------
               no
               ------------------------------------------------
               ------------------------------------------------
            ------------------------------------------------
            enabled: true <defaulted>
         ------------------------------------------------
         number: 567
         ------------------------------------------------
            override-scanner-settings
            ------------------------------------------------
               no
               ------------------------------------------------
               ------------------------------------------------
            ------------------------------------------------
            enabled: true <defaulted>
         ------------------------------------------------
      ------------------------------------------------
      default-thresholds
      ------------------------------------------------
         scanner-threshold: 120 default: 200
         threshold-histogram (min: 0, max: 3, current: 3)
         ------------------------------------------------
            <protected entry>
            dest-ip-bin: low <defaulted>
            num-source-ips: 10 <defaulted>
            <protected entry>
            dest-ip-bin: medium
```

```
            num-source-ips: 120 default: 1
            <protected entry>
            dest-ip-bin: high <defaulted>
            num-source-ips: 1 <defaulted>
          -----------------------------------------------
      -----------------------------------------------
      enabled: true <defaulted>
   -----------------------------------------------
ips-ssp(config-ano-ill-tcp)#
```

不正ゾーンに対する UDP プロトコルの設定

サービス異常検出不正ゾーン サブモードで **udp** {**enabled** | **dst-port** *number* | **default-thresholds**} コマンドを使用して、UDP サービスをイネーブルにし、設定します。

オプション

次のオプションが適用されます。

- **enabled** {**true** | **false** }：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。
- **default-thresholds**：宛先ポート マップで指定されないすべてのポートに使用されるしきい値を定義します。
  - **threshold-histogram {low | medium | high} num-source-ips** *number*：しきい値ヒストグラムの値を設定します。
  - **scanner-threshold**：スキャナしきい値を設定します。デフォルトは 200 です。
- **dst-port** *number*：特定の宛先ポートに対してしきい値を定義します。有効な値は 0 ～ 65535 です。
- **enabled** {**true** | **false**}：サービスをイネーブルまたはディセーブルにします。
- **override-scanner-settings** {**yes** | **no**}：スキャナ値を上書きできます。
  - **threshold-histogram {low | medium | high} num-source-ips** *number*：しきい値ヒストグラムの値を設定します。
  - **scanner-threshold**：スキャナしきい値を設定します。デフォルトは 200 です。

不正ゾーン UDP プロトコルの設定

ゾーンに対して UDP プロトコルを設定するには、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　異常検出不正ゾーン サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service anomaly-detection ad0
ips-ssp(config-ano)# illegal-zone
ips-ssp(config-ano-ill)#
```

ステップ 3　UDP プロトコルをイネーブルにします。

```
ips-ssp(config-ano-ill)# udp
ips-ssp(config-ano-ill-udp)# enabled true
```

ステップ 4　特定のポートを UDP プロトコルに関連付けます。

```
ips-ssp(config-ano-ill-udp)# dst-port 20
ips-ssp(config-ano-ill-udp-dst)#
```

ステップ 5　そのポートのサービスをイネーブルにします。

```
ips-ssp(config-ano-ill-udp-dst)# enabled true
```

ステップ 6　そのポートのスキャナ値を上書きします。デフォルトのスキャナ値を使用するか、あるいはそれらの値を上書きし、独自のスキャナ値を設定できます。

```
ips-ssp(config-ano-ill-udp-dst)# override-scanner-settings yes
ips-ssp(config-ano-ill-udp-dst-yes)#
```

ステップ 7　新しいスキャナ設定に対してヒストグラムを追加します。宛先 IP アドレスの数（low、medium、または high）と、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。

```
ips-ssp(config-ano-ill-udp-dst-yes)# threshold-histogram low num-source-ips 100
```

ステップ 8　スキャナしきい値を設定します。

```
ips-ssp(config-ano-ill-udp-dst-yes)# scanner-threshold 100
```

ステップ 9　他のすべての未指定ポートに対してデフォルトしきい値を設定します。

```
ips-ssp(config-ano-ill-udp-dst-yes)# exit
ips-ssp(config-ano-ill-udp-dst)# exit
ips-ssp(config-ano-ill-udp)# exit
ips-ssp(config-ano-ill-udp)# default-thresholds
ips-ssp(config-ano-ill-udp-def)# default-thresholds
ips-ssp(config-ano-ill-udp-def)# threshold-histogram medium num-source-ips 120
ips-ssp(config-ano-ill-udp-def)# scanner-threshold 120
```

ステップ 10　UDP 設定を確認します。

```
ips-ssp(config-ano-ill-udp)# show settings
   udp
   ----------------------------------------------
      dst-port (min: 0, max: 65535, current: 4)
      ----------------------------------------------
         number: 20
         ----------------------------------------------
            override-scanner-settings
            ----------------------------------------------
               yes
               ----------------------------------------------
                  scanner-threshold: 100 default: 200
                  threshold-histogram (min: 0, max: 3, current: 1)
                  ----------------------------------------------
                     dest-ip-bin: low
                     num-source-ips: 100
                  ----------------------------------------------
               ----------------------------------------------
            ----------------------------------------------
            enabled: true default: true
         ----------------------------------------------
         number: 23
         ----------------------------------------------
            override-scanner-settings
            ----------------------------------------------
               no
               ----------------------------------------------
               ----------------------------------------------
            ----------------------------------------------
```

```
            enabled: true <defaulted>
          ----------------------------------------------
          number: 113
          ----------------------------------------------
            override-scanner-settings
            ------------------------------------------------
              no
              ------------------------------------------------
              ------------------------------------------------
            ------------------------------------------------
            enabled: true <defaulted>
          ----------------------------------------------
          number: 567
          ----------------------------------------------
            override-scanner-settings
            ------------------------------------------------
              no
              ------------------------------------------------
              ------------------------------------------------
            ------------------------------------------------
            enabled: true <defaulted>
          ----------------------------------------------
        ----------------------------------------------
        default-thresholds
        ----------------------------------------------
          scanner-threshold: 120 default: 200
          threshold-histogram (min: 0, max: 3, current: 3)
          ----------------------------------------------
            <protected entry>
            dest-ip-bin: low <defaulted>
            num-source-ips: 10 <defaulted>
            <protected entry>
            dest-ip-bin: medium
            num-source-ips: 120 default: 1
            <protected entry>
            dest-ip-bin: high <defaulted>
            num-source-ips: 1 <defaulted>
          ----------------------------------------------
        ----------------------------------------------
        enabled: true <defaulted>
      ----------------------------------------------
ips-ssp(config-ano-ill-udp)#
```

不正ゾーンに対する他のプロトコルの設定

サービス異常検出不正ゾーン サブモードで **other** {**enabled** | **protocol** *number* | **default-thresholds**} コマンドを使用して、他のサービスをイネーブルにし、設定します。

オプション

次のオプションが適用されます。

- **enabled** {**true** | **false** }：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。
- **default-thresholds**：宛先ポート マップで指定されないすべてのポートに使用されるしきい値を定義します。
  - **threshold-histogram {low | medium | high} num-source-ips** *number*：しきい値ヒストグラムの値を設定します。

  - **scanner-threshold**：スキャナしきい値を設定します。デフォルトは 200 です。
- **protocol-number** *number*：特定のプロトコルに対するしきい値を定義します。有効な値は 0 ～ 255 です。
- **enabled** {**true** | **false**}：サービスをイネーブルまたはディセーブルにします。
- **override-scanner-settings** {**yes** | **no**}：スキャナ値を上書きできます。
  - **threshold-histogram {low | medium | high} num-source-ips** *number*：しきい値ヒストグラムの値を設定します。
  - **scanner-threshold**：スキャナしきい値を設定します。デフォルトは 200 です。

不正ゾーンの他のプロトコルの設定

ゾーンに対して他のプロトコルを設定するには、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　異常検出不正ゾーン サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service anomaly-detection ad0
ips-ssp(config-ano)# illegal-zone
ips-ssp(config-ano-ill)#
```

ステップ 3　他のプロトコルをイネーブルにします。

```
ips-ssp(config-ano-ill)# other
ips-ssp(config-ano-ill-oth)# enabled true
```

ステップ 4　他のプロトコルに対して特定の番号を関連付けます。

```
ips-ssp(config-ano-ill-oth)# protocol-number 5
ips-ssp(config-ano-ill-oth-pro)#
```

ステップ 5　そのポートのサービスをイネーブルにします。

```
ips-ssp(config-ano-ill-oth-pro)# enabled true
```

ステップ 6　そのプロトコルに対するスキャナ値を上書きします。デフォルトのスキャナ値を使用するか、あるいはそれらの値を上書きし、独自のスキャナ値を設定できます。

```
ips-ssp(config-ano-ill-oth-pro)# override-scanner-settings yes
ips-ssp(config-ano-ill-oth-pro-yes)#
```

ステップ 7　新しいスキャナ設定に対してヒストグラムを追加します。宛先 IP アドレスの数（low、medium、または high）と、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。

```
ips-ssp(config-ano-ill-oth-pro-yes)# threshold-histogram high num-source-ips 75
```

ステップ 8　スキャナしきい値を設定します。

```
ips-ssp(config-ano-ill-oth-pro-yes)# scanner-threshold 100
```

ステップ 9　他のすべての未指定ポートに対してデフォルトしきい値を設定します。

```
ips-ssp(config-ano-ill-oth-pro-yes)# exit
ips-ssp(config-ano-ill-oth-pro)# exit
ips-ssp(config-ano-ill-oth)# default-thresholds
ips-ssp(config-ano-ill-oth-def)# default-thresholds
ips-ssp(config-ano-ill-oth-def)# threshold-histogram medium num-source-ips 120
ips-ssp(config-ano-ill-oth-def)# scanner-threshold 120
```

ステップ 10　その他のプロトコルの設定を確認します。

```
ips-ssp(config-ano-ill-oth)# show settings
   other
   -----------------------------------------------
      protocol-number (min: 0, max: 255, current: 1)
      -----------------------------------------------
         number: 5
         -----------------------------------------------
            override-scanner-settings
            -----------------------------------------------
               yes
               -----------------------------------------------
                  scanner-threshold: 95 default: 200
                  threshold-histogram (min: 0, max: 3, current: 1)
                  -----------------------------------------------
                     dest-ip-bin: high
                     num-source-ips: 75
                  -----------------------------------------------
               -----------------------------------------------
            -----------------------------------------------
            enabled: true default: true
         -----------------------------------------------
      -----------------------------------------------
      default-thresholds
      -----------------------------------------------
         scanner-threshold: 200 <defaulted>
         threshold-histogram (min: 0, max: 3, current: 3)
         -----------------------------------------------
            <protected entry>
            dest-ip-bin: low <defaulted>
            num-source-ips: 10 <defaulted>
            <protected entry>
            dest-ip-bin: medium <defaulted>
            num-source-ips: 1 <defaulted>
            <protected entry>
            dest-ip-bin: high <defaulted>
            num-source-ips: 1 <defaulted>
         -----------------------------------------------
      -----------------------------------------------
      enabled: true default: true
   -----------------------------------------------
ips-ssp(config-ano-ill-oth)#
```

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。次のような構成になっています。

外部ゾーンについて

外部ゾーンは、デフォルトのインターネット範囲が 0.0.0.0 ～ 255.255.255.255 の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の IP アドレス 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。

外部ゾーンに対して TCP、UDP、および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できます。TCP および UDP プロトコルに対して宛先ポートを設定したり、その他のプロトコルに対してプロトコル番号を設定したりできます。デフォルトしきい値を使用するか、あるいはスキャナ設定を上書きして、独自のしきい値とヒストグラムを追加できます。

外部ゾーンの設定

サービス異常検出サブモードで **external-zone** {**enabled** | **tcp** | **udp** |**other**} コマンドを使用して、外部ゾーンをイネーブルにし、プロトコルを指定します。

オプション

次のオプションが適用されます。

- **enabled** {**true** | **false** }：ゾーンをイネーブルまたはディセーブルにします。
- **tcp**：TCP プロトコルを設定できます。
- **udp**：UDP プロトコルを設定できます。
- **other**：TCP と UDP 以外の他のプロトコルを設定できます。

外部ゾーンの設定

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　異常検出外部ゾーン サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service anomaly-detection ad0
ips-ssp(config-ano)# external-zone
ips-ssp(config-ano-ext)#
```

ステップ 3　外部ゾーンをイネーブルにします。

```
ips-ssp(config-ano-ext)# enabled true
```

ステップ 4　TCP プロトコルを設定します。

ステップ 5　UDP プロトコルを設定します。

ステップ 6　その他のプロトコルを設定します。

詳細情報

- TCP プロトコルの設定手順については、「外部ゾーンに対する TCP プロトコルの設定」（P.9-30）を参照してください。
- UDP プロトコルの設定手順については、「外部ゾーンに対する UDP プロトコルの設定」（P.9-32）を参照してください。

- その他のプロトコルの設定手順については、「外部ゾーンに対するその他のプロトコルの設定」（P.9-35）を参照してください。

外部ゾーンに対する TCP プロトコルの設定

サービス異常検出外部ゾーン サブモードで **tcp** {**enabled** | **dst-port** *number* | **default-thresholds**} コマンドを使用して、TCP サービスをイネーブルにし、設定します。

オプション

次のオプションが適用されます。

- **enabled** {**true** | **false** }：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。
- **default-thresholds**：宛先ポート マップで指定されないすべてのポートに使用されるしきい値を定義します。
  - **threshold-histogram {low | medium | high} num-source-ips** *number*：しきい値ヒストグラムの値を設定します。
  - **scanner-threshold**：スキャナしきい値を設定します。デフォルトは 200 です。
- **dst-port** *number*：特定の宛先ポートに対してしきい値を定義します。有効な値は 0 ～ 65535 です。
- **enabled** {**true** | **false**}：サービスをイネーブルまたはディセーブルにします。
- **override-scanner-settings** {**yes** | **no**}：スキャナ値を上書きできます。
  - **threshold-histogram {low | medium | high} num-source-ips** *number*：しきい値ヒストグラムの値を設定します。
  - **scanner-threshold**：スキャナしきい値を設定します。デフォルトは 200 です。

外部ゾーン TCP プロトコルの設定

外部ゾーンに対して TCP プロトコルを設定するには、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　異常検出外部ゾーン サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service anomaly-detection ad0
ips-ssp(config-ano)# external-zone
ips-ssp(config-ano-ext)#
```

ステップ 3　TCP プロトコルをイネーブルにします。

```
ips-ssp(config-ano-ext)# tcp
ips-ssp(config-ano-ext-tcp)# enabled true
```

ステップ 4　特定のポートを TCP プロトコルに関連付けます。

```
ips-ssp(config-ano-ext-tcp)# dst-port 20
ips-ssp(config-ano-ext-tcp-dst)#
```

ステップ 5　そのポートのサービスをイネーブルにします。

```
ips-ssp(config-ano-ext-tcp-dst)# enabled true
```

ステップ 6　そのポートのスキャナ値を上書きします。デフォルトのスキャナ値を使用するか、あるいはそれらの値を上書きし、独自のスキャナ値を設定できます。

```
ips-ssp(config-ano-ext-tcp-dst)# override-scanner-settings yes
ips-ssp(config-ano-ext-tcp-dst-yes)#
```

ステップ 7　新しいスキャナ設定に対してヒストグラムを追加します。宛先 IP アドレスの数（low、medium、または high）と、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。

```
ips-ssp(config-ano-ext-tcp-dst-yes)# threshold-histogram low num-source-ips 100
```

ステップ 8　スキャナしきい値を設定します。

```
ips-ssp(config-ano-ext-tcp-dst-yes)# scanner-threshold 100
```

ステップ 9　他のすべての未指定ポートに対してデフォルトしきい値を設定します。

```
ips-ssp(config-ano-ext-tcp-dst-yes)# exit
ips-ssp(config-ano-ext-tcp-dst)# exit
ips-ssp(config-ano-ext-tcp)# exit
ips-ssp(config-ano-ext-tcp)# default-thresholds
ips-ssp(config-ano-ext-tcp-def)# default-thresholds
ips-ssp(config-ano-ext-tcp-def)# threshold-histogram medium num-source-ips 120
ips-ssp(config-ano-ext-tcp-def)# scanner-threshold 120
```

ステップ 10　TCP 設定を確認します。

```
ips-ssp(config-ano-ext-tcp)# show settings
   tcp
   ----------------------------------------------
      dst-port (min: 0, max: 65535, current: 4)
      ---------------------------------------------
         number: 20
         -----------------------------------------------
            override-scanner-settings
            ------------------------------------------------
               yes
               ------------------------------------------------
                  scanner-threshold: 100 default: 200
                  threshold-histogram (min: 0, max: 3, current: 1)
                  ------------------------------------------------
                     dest-ip-bin: low
                     num-source-ips: 100
                  ------------------------------------------------
               ------------------------------------------------
            ------------------------------------------------
            enabled: true default: true
         -----------------------------------------------
         number: 23
         -----------------------------------------------
            override-scanner-settings
            ------------------------------------------------
               no
               ------------------------------------------------
               ------------------------------------------------
            ------------------------------------------------
            enabled: true <defaulted>
         -----------------------------------------------
         number: 113
         -----------------------------------------------
            override-scanner-settings
            ------------------------------------------------
               no
               ------------------------------------------------
               ------------------------------------------------
```

```
            ------------------------------------------------
            enabled: true <defaulted>
          ------------------------------------------------
          number: 567
          ------------------------------------------------
            override-scanner-settings
            ------------------------------------------------
              no
              ------------------------------------------------
              ------------------------------------------------
            ------------------------------------------------
            enabled: true <defaulted>
          ------------------------------------------------
        ------------------------------------------------
        default-thresholds
        ------------------------------------------------
          scanner-threshold: 120 default: 200
          threshold-histogram (min: 0, max: 3, current: 3)
          ------------------------------------------------
            <protected entry>
            dest-ip-bin: low <defaulted>
            num-source-ips: 10 <defaulted>
            <protected entry>
            dest-ip-bin: medium
            num-source-ips: 120 default: 1
            <protected entry>
            dest-ip-bin: high <defaulted>
            num-source-ips: 1 <defaulted>
          ------------------------------------------------
        ------------------------------------------------
        enabled: true <defaulted>
    ------------------------------------------------
ips-ssp(config-ano-ext-tcp)#
```

外部ゾーンに対する UDP プロトコルの設定

サービス異常検出外部ゾーン サブモードで **udp** {**enabled** | **dst-port** *number* | **default-thresholds**} コマンドを使用して、UDP サービスをイネーブルにし、設定します。

オプション

次のオプションが適用されます。

- **enabled** {**true** | **false** }：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。
- **default-thresholds**：宛先ポート マップで指定されないすべてのポートに使用されるしきい値を定義します。
  - **threshold-histogram {low | medium | high} num-source-ips** *number*：しきい値ヒストグラムの値を設定します。
  - **scanner-threshold**：スキャナしきい値を設定します。デフォルトは 200 です。
- **dst-port** *number*：特定の宛先ポートに対してしきい値を定義します。有効な値は 0 ～ 65535 です。
- **enabled** {**true** | **false**}：サービスをイネーブルまたはディセーブルにします。
- **override-scanner-settings** {**yes** | **no**}：スキャナ値を上書きできます。
  - **threshold-histogram {low | medium | high} num-source-ips** *number*：しきい値ヒストグラムの値を設定します。

- **scanner-threshold**：スキャナしきい値を設定します。デフォルトは 200 です。

外部ゾーン UDP プロトコルの設定

ゾーンに対して UDP プロトコルを設定するには、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　異常検出外部ゾーン サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service anomaly-detection ad0
ips-ssp(config-ano)# external-zone
ips-ssp(config-ano-ext)#
```

ステップ 3　UDP プロトコルをイネーブルにします。

```
ips-ssp(config-ano-ext)# udp
ips-ssp(config-ano-ext-udp)# enabled true
```

ステップ 4　特定のポートを UDP プロトコルに関連付けます。

```
ips-ssp(config-ano-ext-udp)# dst-port 20
ips-ssp(config-ano-ext-udp-dst)#
```

ステップ 5　そのポートのサービスをイネーブルにします。

```
ips-ssp(config-ano-ext-udp-dst)# enabled true
```

ステップ 6　そのポートのスキャナ値を上書きします。デフォルトのスキャナ値を使用するか、あるいはそれらの値を上書きし、独自のスキャナ値を設定できます。

```
ips-ssp(config-ano-ext-udp-dst)# override-scanner-settings yes
ips-ssp(config-ano-ext-udp-dst-yes)#
```

ステップ 7　新しいスキャナ設定に対してヒストグラムを追加します。宛先 IP アドレスの数（low、medium、または high）と、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。

```
ips-ssp(config-ano-ext-udp-dst-yes)# threshold-histogram low num-source-ips 100
```

ステップ 8　スキャナしきい値を設定します。

```
ips-ssp(config-ano-ext-udp-dst-yes)# scanner-threshold 100
```

ステップ 9　他のすべての未指定ポートに対してデフォルトしきい値を設定します。

```
ips-ssp(config-ano-ext-udp-dst-yes)# exit
ips-ssp(config-ano-ext-udp-dst)# exit
ips-ssp(config-ano-ext-udp)# default-thresholds
ips-ssp(config-ano-ext-udp-def)# default-thresholds
ips-ssp(config-ano-ext-udp-def)# threshold-histogram medium num-source-ips 120
ips-ssp(config-ano-ext-udp-def)# scanner-threshold 120
```

ステップ 10　UDP 設定を確認します。

```
ips-ssp(config-ano-ext-udp)# show settings
   udp
   -----------------------------------------------
      dst-port (min: 0, max: 65535, current: 4)
      -----------------------------------------------
         number: 20
         -----------------------------------------------
            override-scanner-settings
            -----------------------------------------------
               yes
```

```
                  ------------------------------------------------
                     scanner-threshold: 100 default: 200
                     threshold-histogram (min: 0, max: 3, current: 1)
                     ------------------------------------------------
                        dest-ip-bin: low
                        num-source-ips: 100
                     ------------------------------------------------
                  ------------------------------------------------
               ------------------------------------------------
               enabled: true default: true
            ------------------------------------------------
            number: 23
            ------------------------------------------------
               override-scanner-settings
               ------------------------------------------------
                  no
                  ------------------------------------------------
                  ------------------------------------------------
               ------------------------------------------------
               enabled: true <defaulted>
            ------------------------------------------------
            number: 113
            ------------------------------------------------
               override-scanner-settings
               ------------------------------------------------
                  no
                  ------------------------------------------------
                  ------------------------------------------------
               ------------------------------------------------
               enabled: true <defaulted>
            ------------------------------------------------
            number: 567
            ------------------------------------------------
               override-scanner-settings
               ------------------------------------------------
                  no
                  ------------------------------------------------
                  ------------------------------------------------
               ------------------------------------------------
               enabled: true <defaulted>
            ------------------------------------------------
         ------------------------------------------------
         default-thresholds
         ------------------------------------------------
            scanner-threshold: 120 default: 200
            threshold-histogram (min: 0, max: 3, current: 3)
            ------------------------------------------------
               <protected entry>
               dest-ip-bin: low <defaulted>
               num-source-ips: 10 <defaulted>
               <protected entry>
               dest-ip-bin: medium
               num-source-ips: 120 default: 1
               <protected entry>
               dest-ip-bin: high <defaulted>
               num-source-ips: 1 <defaulted>
            ------------------------------------------------
         ------------------------------------------------
         enabled: true <defaulted>
      ------------------------------------------------
ips-ssp(config-ano-ext-udp)#
```

外部ゾーンに対するその他のプロトコルの設定

サービス異常検出外部ゾーン サブモードで **other** {**enabled** | **protocol** *number* | **default-thresholds**} コマンドを使用して、その他のサービスをイネーブルにし、設定します。

オプション

次のオプションが適用されます。

- **enabled** {**true** | **false** }：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。
- **default-thresholds**：宛先ポート マップで指定されないすべてのポートに使用されるしきい値を定義します。
  - **threshold-histogram {low | medium | high} num-source-ips** *number*：しきい値ヒストグラムの値を設定します。
  - **scanner-threshold**：スキャナしきい値を設定します。デフォルトは 200 です。
- **protocol-number** *number*：特定のプロトコルに対するしきい値を定義します。有効な値は 0 ～ 255 です。
- **enabled** {**true** | **false**}：サービスをイネーブルまたはディセーブルにします。
- **override-scanner-settings** {**yes** | **no**}：スキャナ値を上書きできます。
  - **threshold-histogram {low | medium | high} num-source-ips** *number*：しきい値ヒストグラムの値を設定します。
  - **scanner-threshold**：スキャナしきい値を設定します。デフォルトは 200 です。

外部ゾーンの他のプロトコルの設定

ゾーンに対して他のプロトコルを設定するには、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　異常検出外部ゾーン サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service anomaly-detection ad0
ips-ssp(config-ano)# external-zone
ips-ssp(config-ano-ext)#
```

ステップ 3　他のプロトコルをイネーブルにします。

```
ips-ssp(config-ano-ext)# other
ips-ssp(config-ano-ext-oth)# enabled true
```

ステップ 4　他のプロトコルに対して特定の番号を関連付けます。

```
ips-ssp(config-ano-ext-oth)# protocol-number 5
ips-ssp(config-ano-ext-oth-pro)#
```

ステップ 5　そのポートのサービスをイネーブルにします。

```
ips-ssp(config-ano-ext-oth-pro)# enabled true
```

ステップ 6　そのプロトコルに対するスキャナ値を上書きします。デフォルトのスキャナ値を使用するか、あるいはそれらの値を上書きし、独自のスキャナ値を設定できます。

```
ips-ssp(config-ano-ext-oth-pro)# override-scanner-settings yes
ips-ssp(config-ano-ext-oth-pro-yes)#
```

ステップ 7　新しいスキャナ設定に対してヒストグラムを追加します。宛先 IP アドレスの数（low、medium、または high）と、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。

```
ips-ssp(config-ano-ext-oth-pro-yes)# threshold-histogram high num-source-ips 75
```

ステップ 8　スキャナしきい値を設定します。

```
ips-ssp(config-ano-ext-oth-pro-yes)# scanner-threshold 100
```

ステップ 9　他のすべての未指定ポートに対してデフォルトしきい値を設定します。

```
ips-ssp(config-ano-ext-oth-pro-yes)# exit
ips-ssp(config-ano-ext-oth-pro)# exit
ips-ssp(config-ano-ext-oth)# default-thresholds
ips-ssp(config-ano-ext-oth-def)# default-thresholds
ips-ssp(config-ano-ext-oth-def)# threshold-histogram medium num-source-ips 120
ips-ssp(config-ano-ext-oth-def)# scanner-threshold 120
```

ステップ 10　その他のプロトコルの設定を確認します。

```
ips-ssp(config-ano-ext-oth)# show settings
   other
   -----------------------------------------------
      protocol-number (min: 0, max: 255, current: 1)
      -----------------------------------------------
         number: 5
         -----------------------------------------------
            override-scanner-settings
            -----------------------------------------------
               yes
               -----------------------------------------------
                  scanner-threshold: 95 default: 200
                  threshold-histogram (min: 0, max: 3, current: 1)
                  -----------------------------------------------
                     dest-ip-bin: high
                     num-source-ips: 75
                  -----------------------------------------------
               -----------------------------------------------
            -----------------------------------------------
            enabled: true default: true
         -----------------------------------------------
      -----------------------------------------------
      default-thresholds
      -----------------------------------------------
         scanner-threshold: 200 <defaulted>
         threshold-histogram (min: 0, max: 3, current: 3)
         -----------------------------------------------
            <protected entry>
            dest-ip-bin: low <defaulted>
            num-source-ips: 10 <defaulted>
            <protected entry>
            dest-ip-bin: medium <defaulted>
            num-source-ips: 1 <defaulted>
            <protected entry>
            dest-ip-bin: high <defaulted>
            num-source-ips: 1 <defaulted>
         -----------------------------------------------
      -----------------------------------------------
      enabled: true default: true
   -----------------------------------------------
ips-ssp(config-ano-ext-oth)#
```

学習受け入れモードの設定

ここでは、KB およびヒストグラムと、学習受け入れモードの設定方法について説明します。次のような構成になっています。

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 名
- ゾーン名
- プロトコル
- サービス

スキャナしきい値と各サービスのヒストグラムは、KB に保存されます。学習受け入れモードを自動に設定し、アクションを循環に設定した場合、新しい KB は 24 時間ごとに作成され、次の 24 時間使用されます。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は、新しい KB が作成されますが、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は、センサーの現地時間を使用します。

スキャナしきい値は、単一の送信元 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、ゾーン IP アドレスの指定された数よりも多く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、攻撃が進行中でないときに学習したヒストグラムから逸脱した場合（つまり、定義されたゾーン宛先 IP アドレスよりも多くを同時にスキャンする送信元 IP アドレスの数を超えた場合）にワーム攻撃が識別されます。たとえば、スキャニングしきい値が 300 であり、ポートのヒストグラムが 445 である場合は、異常検出で 350 個のゾーン宛先 IP アドレスをスキャンするスキャナが識別されると、マス スキャナが検出されたことを示すアクションが生成されます。ただし、このスキャナは、ワーム攻撃が進行中であることを確認しません。表 9-2 に、この例を示します。

表 9-2　ヒストグラム例

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

異常検出が、ポート 445 で 50 個を超えるゾーン宛先 IP アドレスをスキャンする 6 個の同時送信元 IP アドレスを識別した場合は、異常検出がポート 445 でワーム攻撃を識別したことを示す、未指定の送信元 IP アドレスを持つアクションが生成されます。ダイナミック フィルタしきい値である 50 により、新しい内部スキャニングしきい値が指定され、新しいスキャニングしきい値（50）よりも多くをスキャンする各送信元 IP アドレスに対して追加のダイナミック フィルタを生成するよう異常検出がスキャナのしきい値定義を小さくします。

KB が異常検出ポリシーとゾーンごとに学習したことを上書きできます。使用しているネットワーク トラフィックを理解している場合は、オーバーライドを使用して偽陽性を制限できます。

学習受け入れモードの設定

サービス異常検出サブモードで **learning-accept-mode** コマンドを使用して、センサーが長い時間ごとに新しい KB を作成するかどうかを設定します。KB を作成およびロード（循環）するか、保存（保存だけ）するかを設定できます。KB がロードまたは保存される頻度とタイミングをスケジュールできます。

更新された新しい KB ファイルの名前は、現在の日時である *YYYY-Mon-dd-hh_mm_ss* になります。ここで、*Mon* は 3 文字で構成される月の略語です。

（注）　異常検出学習受け入れモードは、センサーの現地時間を使用します。

オプション

次のオプションが適用されます。

- **learning-accept-mode**：KB を保存およびロードするかどうかと、いつ KB を保存およびロードするかを指定します。
  - **auto**：KB を自動的に受け入れるようセンサーを設定します。
  - **manual**：KB を保存しません。

    （注）　KB は、**anomaly-detection** [**load** | **save**] コマンドを使用して保存およびロードできます。

- **action**：KB を循環または保存するかどうかを指定できます。
  - **save-only**：新しい KB を保存します。この KB を調べて、異常検出にロードするかどうかを決定できます。

    （注）　KB は、**anomaly-detection load** コマンドを使用してロードできます。

  - **rotate**：定義したスケジュールに基づいて、新しい KB を保存し、現在の KB としてロードします。
- **schedule**：KB を受け入れるスケジュールを設定します。
  - **calendar-schedule [days-of-week] [times-of-day]**：特定の日時に学習受け入れモードを開始します。
  - **periodic-schedule [interval] [start-time]**：特定の周期間隔で学習受け入れモードを開始します。

学習受け入れモードの設定

最初の保存は、設定時刻と開始時刻間の完全な間隔後に開始されます。たとえば、時刻が現在 16:00 であり、1 時間の間隔で開始時刻を 16:30 に設定した場合、16:00 と 16:30 の間には 1 時間の間隔がないため、最初の KB は 17:30 に保存されます。

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　異常検出サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service anomaly-detection ad1
```

ステップ 3　KB をどのように保存およびロードするかを指定します。

a. KB が自動的に保存およびロードされることを指定します。ステップ 4 に進みます。

```
ips-ssp(config-ano)# learning-accept-mode auto
ips-ssp(config-ano-auto)#
```

b. KB を手動で保存およびロードすることを指定します。ステップ 6 に進みます。

```
ips-ssp(config-ano)# learning-accept-mode manual
ips-ssp(config-ano-man)#
```

ステップ 4　KB をどのように自動的に受け入れるかを指定します。

a. KB を検査し、ロードするかどうかを決定するために KB を保存します。ステップ 6 に進みます。

```
ips-ssp(config-ano-aut)# action save-only
```

b. 定義したスケジュールに基づいて、KB を保存し、現在の KB としてロードします。ステップ 5 に進みます。

```
ips-ssp(config-ano-aut)# action rotate
```

ステップ 5　自動的な KB の保存およびロードをスケジュールします。

- カレンダー スケジュール：このスケジュールでは、KB が毎月曜日の夜 12 時に保存およびロードされます。

```
ips-ssp(config-ano-aut)# schedule calendar-schedule
ips-ssp(config-ano-aut-cal)# days-of-week monday
ips-ssp(config-ano-aut-cal)# times-of-day time 24:00:00
```

- 周期スケジュール：このスケジュールでは、KB が毎日夜 12 時に保存およびロードされます。

```
ips-ssp(config-ano-aut)# schedule periodic-schedule
ips-ssp(config-ano-aut-per)# start-time 24:00:00
ips-ssp(config-ano-aut-per)# interval 24
```

ステップ 6　設定を確認できます。

```
ips-ssp(config-ano-aut-per)# exit
ips-ssp(config-ano-aut)# show settings
   auto
   ----------------------------------------------
      action: rotate default: rotate
      schedule
      ------------------------------------------------
         periodic-schedule
         ------------------------------------------------
            start-time: 12:00:00 default: 10:00:00
            interval: 24 hours default: 24
         ------------------------------------------------
      ------------------------------------------------
   ----------------------------------------------
```

ステップ 7　異常検出サブモードを終了します。

```
ips-ssp(config-ano-aut)# exit
ips-ssp(config-ano)# exit
Apply Changes:?[yes]:
```

ステップ 8　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

詳細情報

異常検出 KB を手動で保存およびロードする手順については、「手動による KB の保存およびロード」（P.9-41）を参照してください。

KB ファイルの操作

ここでは、KB ファイルの表示、ロード、保存、コピー、名前変更、および削除を行う方法について説明します。また、2 つの KB ファイルを比較し、KB ファイルのしきい値を表示する手順についても説明します。次のような構成になっています。

KB ファイルの表示

特権 EXEC モードで **show ad-knowledge-base** [*virtual-sensor*] **files** コマンドを使用して、仮想センサーに利用可能な KB ファイルを表示します。

（注） ファイル名の前の * は、この KB ファイルが現在ロードされている KB ファイルであることを示します。

KB ファイルを表示するには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　すべての仮想センサーに対して KB ファイルを表示します。

```
ips-ssp# show ad-knowledge-base files
Virtual Sensor vs0
    Filename                Size   Created
    initial                 84     04:27:07 CDT Wed Jan 29 2010
*   2010-Jan-28-10_00_01    84     04:27:07 CDT Wed Jan 29 2010
Virtual Sensor vs1
    Filename                Size   Created
    initial                 84     14:35:38 CDT Tue Mar 14 2011
    2011-Mar-16-10_00_00    84     10:00:00 CDT Thu Mar 16 2011
    2011-Mar-17-10_00_00    84     10:00:00 CDT Fri Mar 17 2011
    2011-Mar-18-10_00_00    84     10:00:00 CDT Sat Mar 18 2011
    2011-Mar-19-10_00_00    84     10:00:00 CDT Sun Mar 19 2011
    2011-Mar-20-10_00_00    84     10:00:00 CDT Mon Mar 20 2011
    2011-Mar-21-10_00_00    84     10:00:00 CDT Tue Mar 21 2011
    2011-Mar-22-10_00_00    84     10:00:00 CDT Wed Mar 22 2011
    2011-Mar-23-10_00_00    84     10:00:00 CDT Thu Mar 23 2011
    2011-Mar-24-10_00_00    84     10:00:00 CDT Fri Mar 24 2011
    2011-Mar-25-10_00_00    84     10:00:00 CDT Sat Mar 25 2011
    2011-Mar-26-10_00_00    84     10:00:00 CDT Sun Mar 26 2011
    2011-Mar-27-10_00_00    84     10:00:00 CDT Mon Mar 27 2011
    2010-Jan-02-10_00_00    84     10:00:00 CDT Thu Jan 02 2010
    2010-Jan-03-10_00_00    84     10:00:00 CDT Fri Jan 03 2010
    2010-Jan-04-10_00_00    84     10:00:00 CDT Sat Jan 04 2010
```

```
    2010-Jan-05-10_00_00   84     10:00:00 CDT Sun Jan 05 2010
    2010-Jan-06-10_00_00   84     10:00:00 CDT Mon Jan 06 2010
ips-ssp#
```

ステップ 3　特定の仮想センサーに対して KB ファイルを表示します。

```
ips-ssp# show ad-knowledge-base vs0 files
Virtual Sensor vs0
    Filename               Size   Created
    initial                84     10:24:58 CDT Tue Mar 14 2011
    2011-Mar-16-10_00_00   84     10:00:00 CDT Thu Mar 16 2011
    2011-Mar-17-10_00_00   84     10:00:00 CDT Fri Mar 17 2011
    2011-Mar-18-10_00_00   84     10:00:00 CDT Sat Mar 18 2011
    2011-Mar-19-10_00_00   84     10:00:00 CDT Sun Mar 19 2011
    2011-Mar-20-10_00_00   84     10:00:00 CDT Mon Mar 20 2011
```

手動による KB の保存およびロード

特権 EXEC モードで以下のコマンドを使用して、手動で KB を保存およびロードします。

オプション

次のオプションが適用されます。

- **show ad-knowledge-base** *virtual-sensor* **files**：仮想センサーごとに利用可能な KB ファイルを表示します。
- **anomaly-detection** *virtual-sensor* **load** {**initial** | **file** *name*}：指定された仮想センサーに対して KB ファイルを現在の KB として設定します。AD がアクティブな場合、ファイルは現在の KB としてロードされます。
- **anomaly-detection** *virtual-sensor* **save** [*new-name*]：現在の KB ファイルを取得し、ローカルで保存します。

手動による KB の保存およびロード

手動で KB を保存およびロードするには、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　ロードする KB を特定します。

```
ips-ssp# show ad-knowledge-base vs0 files
Virtual Sensor vs0
    Filename               Size   Created
    initial                84     10:24:58 CDT Tue Mar 14 2011
    2011-Mar-16-10_00_00   84     10:00:00 CDT Thu Mar 16 2011
    2011-Mar-17-10_00_00   84     10:00:00 CDT Fri Mar 17 2011
    2011-Mar-18-10_00_00   84     10:00:00 CDT Sat Mar 18 2011
    2011-Mar-19-10_00_00   84     10:00:00 CDT Sun Mar 19 2011
    2011-Mar-20-10_00_00   84     10:00:00 CDT Mon Mar 20 2011
```

ステップ 3　特定の仮想センサーに対して KB ファイルを現在の KB ファイルとしてロードします。

```
ips-ssp# anomaly-detection vs0 load file 2011-Mar-16-10_00_00
ips-ssp#
```

ステップ 4　現在の KB ファイルを保存し、新しい名前で保管します。

```
ips-ssp# anomaly-detection vs0 save my-KB
ips-ssp#
```

（注）　このコマンドを入力したときに異常検出がアクティブでない場合は、エラーが生成されます。初期ファイルを上書きすることはできません。

KB のコピー、名前変更、および消去

KB ファイルのコピー、名前変更、および消去を手動で行うには、特権 EXEC モードで以下のコマンドを使用します。

オプション

次のオプションが適用されます。

- **copy ad-knowledge-base** *virtual-sensor* {**current** | **initial** | **file** *name*} *destination-url* : 指定された宛先 URL に KB ファイル（現在、初期、または入力したファイル名）をコピーします。

  （注）　既存の名前にファイルをコピーすると、上書きされます。

- **copy ad-knowledge-base** *virtual-sensor source-url new-name* : 新しいファイル名を持つ KB を、指定した送信元 URL にコピーします。

  （注）　**current** キーワードを *new-name* として使用することはできません。新しい現在の KB ファイルは、**load** コマンドで作成されます。

- **rename ad-knowledge-base** *virtual-sensor* {**current** | **file** ***name***} *new-name* : 既存の KB ファイルの名前を変更します。
- **erase ad-knowledge-base** [*virtual-sensor* [*name*]] : 仮想センサーからすべての KB ファイル、または 1 つの KB ファイル（*name* オプションを使用する場合）を削除します。

初期 KB ファイル、または現在の KB としてロードされた KB ファイルを消去することはできません。送信元および宛先 URL の実際の形式は、ファイルによって異なります。有効なタイプは次のとおりです。

- ftp: : FTP ネットワーク サーバの場合のコピー元またはコピー先の URL。このプレフィクスの構文は、次のとおりです。

  ftp:[//[username@] location]/relativeDirectory]/filename

  ftp:[//[username@]location]//absoluteDirectory]/filename

- scp: : SCP ネットワーク サーバの場合のコピー元またはコピー先の URL。このプレフィクスの構文は、次のとおりです。

  scp:[//[username@] location]/relativeDirectory]/filename

  scp:[//[username@] location]//absoluteDirectory]/filename

（注） FTP または SCP プロトコルを使用する場合、パスワードの入力を求められます。SCP プロトコルを使用する場合は、リモート ホストを SSH 既知ホスト リストに追加する必要があります。

- http: : Web サーバの場合のコピー元 URL。このプレフィクスの構文は、次のとおりです。
  http:[[/[username@]location]/directory]/filename
- https: : Web サーバの場合のコピー元 URL。このプレフィクスの構文は、次のとおりです。
  https:[[/[username@]location]/directory]/filename

（注） HTTPS プロトコルを使用する場合は、リモート ホストが TLS の信頼できるホストである必要があります。

KB ファイルのコピー、名前変更、および削除

KB ファイルのコピー、名前変更、および削除を行うには、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　コピーする KB ファイルを特定します。

```
ips-ssp# show ad-knowledge-base vs0 files
Virtual Sensor vs0
    Filename               Size   Created
    initial                84     10:24:58 CDT Tue Mar 14 2011
    2011-Mar-16-10_00_00   84     10:00:00 CDT Thu Mar 16 2011
    2011-Mar-17-10_00_00   84     10:00:00 CDT Fri Mar 17 2011
    2011-Mar-18-10_00_00   84     10:00:00 CDT Sat Mar 18 2011
    2011-Mar-19-10_00_00   84     10:00:00 CDT Sun Mar 19 2011
    2011-Mar-20-10_00_00   84     10:00:00 CDT Mon Mar 20 2011
```

ステップ 3　KB ファイルを、IP アドレス 10.1.1.1 を持つコンピュータ上のユーザにコピーします。

```
ips-ssp# copy ad-knowledge-base vs0 file 2011-Mar-16-10_00_00
scp://cidsuser@10.1.1.1/AD/my-KB
password: ********
ips-ssp#
```

ステップ 4　KB ファイルの名前を変更します。

```
ips-ssp# rename ad-knowledge-base vs0 2011-Mar-16-10_00_00 My-KB
ips-ssp#
```

ステップ 5　特定の仮想センサーから KB ファイルを削除します。

```
ips-ssp# erase ad-knowledge-base vs0 2011-Mar-16-10_00_00
ips-ssp#
```

ステップ 6　1 つの仮想センサーから、現在および初期の KB ファイルとしてロードされたファイルを除くすべての KB ファイルを削除します。

```
ips-ssp# erase ad-knowledge-base vs0
Warning: Executing this command will delete all virtual sensor 'vs0' knowledge bases
except the file loaded as current and the initial knowledge base.
Continue with erase? [yes]: yes
ips-ssp#
```

ステップ 7　すべての仮想センサーから、現在および初期の KB ファイルとしてロードされたファイルを除くすべての KB ファイルを削除します。

```
ips-ssp# erase ad-knowledge-base
Warning: Executing this command will delete all virtual sensor knowledge bases except the
file loaded as current and the initial knowledge base.
Continue with erase? [yes]: yes
sensor#
```

詳細情報

- **load** コマンドを使用して新しい KB を作成する手順については、「手動による KB の保存およびロード」（P.9-41）を参照してください。
- SSH 既知ホスト リストにホストを追加する手順については、「SSH 既知ホスト リストへのホストの追加」（P.4-35）を参照してください。
- TLS の信頼できるホストを追加する手順については、「TLS の信頼できるホストの追加」（P.4-40）を参照してください。

2 つの KB 間の違いの表示

特権 EXEC モードで **show ad-knowledge-base** *virtual-sensor* **diff** {**current** | **initial** | **file** *name1*}{**current** | **initial** | **file** *name2*} [*diff-percentage*] コマンドを使用して、2 つの KB 間の違いを表示します。

オプション

次のオプションが適用されます。

- *virtual-sensor*：比較する KB ファイルを含む仮想センサーの名前を指定します。
- *name1*：比較する最初の既存の KB ファイルの名前を指定します。
- *name2*：比較する 2 番目の既存の KB ファイルの名前を指定します。
- **current**：現在ロードされている KB を指定します。
- **initial**：初期 KB を指定します。
- **file**：既存の KB ファイルの名前を指定します。
- *diff-percentage*：（任意）しきい値が指定された割合よりも異なるサービスを表示します。有効な値は 1 ～ 100 です。デフォルトは 10% です。

2 つの KB の比較

2 つの KB を比較するには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　比較するファイルを特定します。

```
ips-ssp# show ad-knowledge-base vs0 files
Virtual Sensor vs0
    Filename               Size   Created
    initial                84     04:27:07 CDT Wed Jan 29 2010
*   2011-Jun-28-10_00_01   84     04:27:07 CDT Thu Jun 29 2011
ips-ssp#
```

ステップ 3　現在ロードされているファイル（* が付いたファイル）を仮想センサー vs0 の初期 KB と比較します。

```
ips-ssp# show ad-knowledge-base vs0 diff initial file 2011-Jun-28-10_00_01
Initial Only Services/Protocols
   External Zone
      TCP Services
         Service = 30
         Service = 20
      UDP Services
         None
      Other Protocols
         Protocol = 1
   Illegal Zone
      None
   Internal Zone
      None
2011-Jun-28-10_00_01 Only Services/Protocols
   External Zone
      None
   Illegal Zone
      None
   Internal Zone
      None
Thresholds differ more than 10%
   External Zone
      None
   Illegal Zone
      TCP Services
         Service = 31
         Service = 22
      UDP Services
         None
      Other Protocols
         Protocol = 3
   Internal Zone
      None
ips-ssp#
```

KB のしきい値の表示

特権 EXEC モードで **show ad-knowledge-base** *virtual-sensor* **thresholds** {**current** | **initial** | **file** *name*} [**zone** {**external** | **illegal** | **internal**]} {[**protocol** {**tcp** | **udp**}] [**dst-port** *port*] | [**protocol other**] [**number** *protocol-number*]} コマンドを表示して、KB のしきい値を表示します。

オプション

次のオプションが適用されます。

- *virtual-sensor*：比較する KB ファイルを含む仮想センサーの名前を指定します。
- *name*：既存の KB ファイルの名前を指定します。
- **current**：現在ロードされている KB を指定します。
- **initial**：初期 KB を指定します。
- **file**：既存の KB ファイルの名前を指定します。
- **zone**：（任意）指定されたゾーンのしきい値を表示します。デフォルトでは、すべてのゾーンの情報が表示されます。

- **external**：外部ゾーンのしきい値を表示します。
- **illegal**：不正ゾーンのしきい値を表示します。
- **internal**：内部ゾーンのしきい値を表示します。
- **protocol**：（任意）指定されたプロトコルのしきい値を表示します。デフォルトでは、すべてのプロトコルに関する情報が表示されます。
- **tcp**：TCP プロトコルのしきい値を表示します。
- **udp**：UDP プロトコルのしきい値を表示します。
- **other**：TCP または UDP 以外の他のプロトコルのしきい値を表示します。
- **dst-port**：（任意）指定されたポートのしきい値を表示します。デフォルトでは、すべての TCP ポートまたは UDP ポートに関する情報が表示されます。
- *port*：ポート番号を指定します。有効な値は 0 ～ 65535 です。
- **number**：（任意）指定された他のプロトコル番号のしきい値を表示します。デフォルトでは、他のすべてのプロトコルに関する情報が表示されます。
- *protocol-number*：プロトコル番号を指定します。有効な値は 0 ～ 255 です。

KB しきい値の表示

KB しきい値を表示するには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　しきい値を表示するファイルを特定します。

```
ips-ssp# show ad-knowledge-base vs1 files
Virtual Sensor vs1
    Filename               Size   Created
    initial                84     10:24:58 CDT Tue Mar 14 2011
    2011-Mar-16-10_00_00   84     10:00:00 CDT Thu Mar 16 2011
    2011-Mar-17-10_00_00   84     10:00:00 CDT Fri Mar 17 2011
    2011-Mar-18-10_00_00   84     10:00:00 CDT Sat Mar 18 2011
    2011-Mar-19-10_00_00   84     10:00:00 CDT Sun Mar 19 2011
    2011-Mar-27-10_00_00   84     10:00:00 CDT Mon Mar 27 2011
    2011-Apr-24-05_00_00   88     05:00:00 CDT Mon Apr 24 2011
*   2011-Apr-25-05_00_00   88     05:00:00 CDT Tue Apr 25 2011
```

ステップ 3　不正ゾーンに対する特定のファイルに含まれるしきい値を表示します。

```
ips-ssp# show ad-knowledge-base vs0 thresholds file 2011-Nov-11-10_00_00 zone illegal

   AD Thresholds
      Creation Date = 2011-Nov-11-10_00_00
      KB = 2011-Nov-11-10_00_00
      Illegal Zone
         TCP Services
            Default
               Scanner Threshold
                  User Configuration = 200
               Threshold Histogram - User Configuration
                  Low = 10
                  Medium = 3
                  High = 1
         UDP Services
            Default
               Scanner Threshold
                  User Configuration = 200
               Threshold Histogram - User Configuration
```

```
                  Low = 10
                  Medium = 3
                  High = 1
            Other Services
               Default
                  Scanner Threshold
                     User Configuration = 200
                  Threshold Histogram - User Configuration
                     Low = 10
                     Medium = 3
                     High = 1
ips-ssp#
```

ステップ 4　現在の KB 不正ゾーン、プロトコル TCP、および宛先ポート 20 に含まれるしきい値を表示します。

```
ips-ssp# show ad-knowledge-base vs0 thresholds current zone illegal protocol tcp dst-port
20

   AD Thresholds
      Creation Date = 2011-Nov-14-10_00_00
      KB = 2011-Nov-14-10_00_00
      Illegal Zone
         TCP Services
            Default
               Scanner Threshold
                  User Configuration = 200
               Threshold Histogram - User Configuration
                  Low = 10
                  Medium = 3
                  High = 1
ips-ssp#
```

ステップ 5　現在の KB 不正ゾーンと他のプロトコルに含まれるしきい値を表示します。

```
ips-ssp# show ad-knowledge-base vs0 thresholds current zone illegal protocol other

   AD Thresholds
      Creation Date = 2011-Nov-14-10_00_00
      KB = 2011-Nov-14-10_00_00
      Illegal Zone
         Other Services
            Default
               Scanner Threshold
                  User Configuration = 200
               Threshold Histogram - User Configuration
                  Low = 10
                  Medium = 3
                  High = 1
ips-ssp#
```

異常検出の統計情報の表示

特権 EXEC モードで **show statistics anomaly-detection** [*virtual-sensor-name*] コマンドを使用して、異常検出の統計情報を表示します。攻撃が進行中かどうかを確認できます（`Attack in progress` または *`No attack`*）。また、次の KB がいつ保存されるかを確認することもできます（`Next KB rotation at 10:00:00 UTC Wed Apr 26 2011`）。

（注）　**clear** コマンドは、異常検出統計情報には利用できません。

異常検出統計情報を表示するには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　特定の仮想センサーに対して異常検出統計情報を表示します。

```
ips-ssp# show statistics anomaly-detection vs0
Statistics for Virtual Sensor vs0
   No attack
   Detection - ON
   Learning - ON
   Next KB rotation at 10:00:00 UTC Wed Apr 26 2011
   Internal Zone
      TCP Protocol
      UDP Protocol
      Other Protocol
   External Zone
      TCP Protocol
      UDP Protocol
      Other Protocol
   Illegal Zone
      TCP Protocol
      UDP Protocol
      Other Protocol
ips-ssp#
```

ステップ 3　すべての仮想センサーに対して統計情報を表示します。

```
ips-ssp# show statistics anomaly-detection
Statistics for Virtual Sensor vs0
   No attack
   Detection - ON
   Learning - ON
   Next KB rotation at 10:00:01 UTC Wed Jun 29 2011
   Internal Zone
      TCP Protocol
      UDP Protocol
      Other Protocol
   External Zone
      TCP Protocol
      UDP Protocol
      Other Protocol
   Illegal Zone
      TCP Protocol
      UDP Protocol
      Other Protocol
Statistics for Virtual Sensor vs1
   No attack
   Detection - ON
   Learning - ON
   Next KB rotation at 10:00:00 UTC Wed Jul 29 2011
   Internal Zone
      TCP Protocol
      UDP Protocol
      Other Protocol
   External Zone
      TCP Protocol
      UDP Protocol
      Other Protocol
   Illegal Zone
      TCP Protocol
      UDP Protocol
      Other Protocol
ips-ssp#
```

異常検出の無効

一方向のトラフィックだけを検出するようにセンサーを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。そうしないと、異常検出がワーム スキャナのように、非対称トラフィックを不完全接続と見なし、アラートを起動するので、多数のアラートを受信することになります。

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。

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

ステップ 3　ディセーブルにする異常検出ポリシーを含む仮想センサー名を入力します。

```
ips-ssp(config-ana)# virtual-sensor vs0
ips-ssp(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。

```
ips-ssp(config-ana-vir)# anomaly-detection
ips-ssp(config-ana-vir-ano)# operational-mode inactive
ips-ssp(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。

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

ステップ 6　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

詳細情報

ワームがどのように動作するかの詳細については、「ワーム」（P.9-2）を参照してください。