CHAPTER 4

ゾーンの作成と設定

この章では、Detector モジュールのゾーンを作成し、管理する方法について説明します。

この章は、次の項で構成されています。

ゾーンの概要

ゾーンは、Detector モジュールが DDoS 攻撃の監視の対象とするネットワーク要素です。次のいずれかまたはすべてのネットワーク オブジェクトを表現するゾーンを作成できます。

- ネットワーク サーバ、ネットワーク クライアント、ルータ
- ネットワーク リンクまたはサブネット、またはネットワーク全体
- 個々のインターネット ユーザまたは企業
- インターネット サービス プロバイダー（ISP）

DDoS 攻撃を感知すると、Detector モジュールでは、Cisco Anomaly Guard Module を自動的にアクティブにしてゾーンを攻撃から保護するか、ユーザに対して Cisco Anomaly Guard Module を手動でアクティブにするように通知することができます。Detector モジュールは、ゾーンのネットワーク アドレスの範囲が重なっていなければ、複数のゾーンのトラフィックを同時に監視できます。新しいゾーンを作成するときは、次のアトリビュートを含んだゾーン設定を作成します。

- ゾーンの説明：ゾーンの名前と説明を定義します。
- ゾーンのネットワーク定義：ゾーンのネットワーク IP アドレスとサブネット マスクを含んだ、ゾーンのネットワーク アトリビュートを定義します。
- ポリシー　テンプレート：ユーザがラーニング　プロセスを実行するときに Detector モジュールが作成するポリシーのタイプを定義します。各ゾーン テンプレートには、一連のポリシー テンプレートが含まれています。
- ポリシー：ゾーンのトラフィックを分析し、ゾーンが異常なトラフィックを受信したときにアクションを実行します。各ゾーンの設定は、それぞれ独自のポリシー セットで構成されています。これらのポリシーは、ゾーン テンプレートから作成されたデフォルトのポリシー、またはラーニング プロセス実行中に作成されたゾーン固有のポリシーのいずれかです。ゾーンのトラフィックがいずれかのポリシーのしきい値を超過すると、攻撃と見なされ、そのポリシーはアクションを実行します。ポリシーのアクションは、通知の送信から、Cisco Anomaly Guard Module をアクティブにしてゾーンを DDoS 攻撃から保護することにまで及びます。

- ゾーン フィルタ：必要な保護レベルにゾーンのトラフィックを誘導し、Detector モジュールによる特定のトラフィック フローの処理方法を定義します。ゾーン フィルタを使用して、特定のトラフィック フローをカウントしたり、Detector モジュールの異常検出機能をバイパスしたりできます。デフォルトのフィルタ設定を変更して、Detector モジュールがトラフィック フローに適用する異常検出機能を決定する、カスタマイズされたゾーンのフィルタ設定を作成できます。

次の方法により、ゾーンを作成することができます。

- 定義済みの Detector モジュールまたは Cisco Anomaly Guard Module のゾーン テンプレートを使用する：いずれかの Detector ゾーン テンプレートまたは Guard ゾーン テンプレートの設定に基づいてゾーンを作成します。Guard ゾーン テンプレートにより、ユーザは Detector モジュールと Cisco Anomaly Guard Module との間でゾーンの設定情報を同期させることができます。CLI を使用して、ゾーンの同期の手動機能と自動機能を設定できます（詳細については、『*Cisco Traffic Anomaly Detector Module Configuration Guide*』を参照）。

  Detector ゾーン テンプレートは、Detector モジュールでのみ使用するものです。ゾーンの設定情報を同期させる必要がない場合は、Detector モジュールのゾーン テンプレートを使用します。

  各ゾーン テンプレートには、Detector モジュールが監視するネットワーク サービスを定義する、あらかじめ定義された一連のポリシーがあります。また、ゾーン テンプレートには、Detector モジュールがラーニング プロセス中にゾーンのトラフィックを分析し、検出したサービスに対してポリシーを作成するときに使用する、一連のポリシー テンプレートも含まれています。Detector モジュールがラーニング プロセス中に作成する新しいポリシーは、それぞれ対応するポリシー テンプレートの規則を使用して構築されます。
- 既存のゾーンをテンプレートとして使用する：既存のゾーンのポリシーとポリシーのしきい値を含んでいる、既存のゾーン設定に基づいて新しいゾーンを作成します。新しいゾーンのトラフィック特性が既存のゾーンと一致している場合は、新しいゾーンに対してラーニング プロセスを実行する必要はありません。2 つのゾーンの間でトラフィックの特性が異なる場合は、新しいゾーンに対してラーニング プロセスを実行し、Detector モジュールがゾーンのトラフィックを分析して、新しいゾーンの設定に必要なポリシーの変更を加えられるようにする必要があります。

ゾーン保護のアクティベーション方式と保護範囲のオプション

GUARD_ ゾーン テンプレートを使用して、ゾーンの同期に対するゾーン設定を定義する場合、Cisco Anomaly Guard Module がゾーン保護を自動的にアクティブにするために使用するトリガー（アクティベーション方式）を定義できます。また、Cisco Anomaly Guard Module が保護する領域の範囲も定義できます。たとえば、Cisco Anomaly Guard Module は、ゾーン全体を保護することも、ゾーン内の特定の領域だけを保護することもできます。

この項は、次の情報で構成されています。

保護のアクティベーション方式

Cisco Anomaly Guard Module は、ゾーン名、または宛先変更されたトラフィックから抽出する情報に基づいて、ゾーン保護をアクティブにすることができます。

保護をアクティブにする方式として、次のものを使用できます。

- ゾーン名：Cisco Anomaly Guard Module は、ゾーン名に基づいてゾーン保護をアクティブにします。保護がアクティブになるには、外部から示される攻撃の兆候にゾーン名が含まれている必要があります。これは、ゾーン保護をアクティブにするために Cisco Anomaly Guard Module が使用するデフォルトの方式です。
- IP アドレス：Cisco Anomaly Guard Module は、ゾーンの一部である IP アドレスまたはサブネットで構成された外部からの攻撃の兆候を受信した場合に、ゾーン保護をアクティブにします。Cisco Anomaly Guard Module はゾーンのデータベースをスキャンし、受信 IP アドレスまたはサブネットを含むアドレス範囲を持つゾーンをアクティブにします。受信 IP アドレスを含むアドレス範囲を持つ複数のゾーンが設定されている場合、Cisco Anomaly Guard Module は、プレフィックスが最も長く一致するゾーンをアクティブにすることを選択します。つまり、受信した IP アドレスが含まれていて、アドレス範囲が最も詳細に特定されるゾーンです。受信した IP アドレスまたはサブネットは、ゾーンの IP アドレス範囲に全体が含まれている必要があります。

- パケット：Cisco Anomaly Guard Module は、データベースでゾーンのパケットを受信した場合に、ゾーン保護をアクティブにします。Cisco Anomaly Guard Module がパケットを受信すると、ゾーンのデータベースをスキャンし、受信パケットの IP アドレスを含むアドレス範囲を持つゾーンをアクティブにします。受信パケットの IP アドレスを含むアドレス範囲を持つ複数のゾーンが設定されている場合、Cisco Anomaly Guard Module は、プレフィックスが最も長く一致するゾーンをアクティブにします。つまり、受信したパケットの IP アドレスが含まれていて、アドレス範囲が最も詳細に特定されるゾーンです。受信した IP アドレスまたはサブネットは、ゾーンの IP アドレス範囲に全体が含まれている必要があります。

ゾーンの保護の範囲

アクティベーション範囲は、Cisco Anomaly Guard Module が外部からの攻撃の兆候を受信した場合に、ゾーン全体またはゾーンの一部に対して保護モードをアクティブにするかどうかを定義します。この兆候には、外部デバイス（Detector モジュールなど）からのコマンドや、ゾーンを宛先とするトラフィック（パケット）があります。

Cisco Anomaly Guard Module は、次のアクティベーション範囲をサポートします。

- ゾーン全体：ゾーン全体の保護をアクティブにします。Cisco Anomaly Guard Module は、ゾーンを宛先とするトラフィックを受信した場合、またはゾーンの一部である IP アドレスまたはサブネットで構成される外部からの攻撃の兆候を受信した場合に、保護をアクティブにします。
- IP アドレスのみ：ゾーン内部の指定した IP アドレスまたはサブネットのみ保護をアクティブにします。Cisco Anomaly Guard Module は、ゾーンを宛先とするトラフィックを受信した場合、またはゾーンの一部である IP アドレスまたはサブネットで構成される外部からの攻撃の兆候を受信した場合、サブゾーンと呼ばれる新しいゾーンを作成します（次の項の「サブゾーンについて」を参照）。これが、アクティベーション範囲パラメータのデフォルト設定です。

サブゾーンについて

ゾーンの一部（ソース ゾーンのすべての IP アドレス範囲を含まないゾーン）に対して保護モードをアクティブにした場合、Cisco Anomaly Guard Module はサブゾーンを作成します。サブゾーンの IP アドレス範囲は、ソース ゾーンのアドレス範囲に含まれています。

サブゾーンの設定は、IP アドレスと名前を除いてソース ゾーンの設定と同じです。サブゾーンの名前は、ソース ゾーンの名前の最初の 30 文字、IP アドレス、およびサブネットで構成され、名前、IP アドレス、およびサブネットはアンダースコアで連結されています。サブゾーンが単一の IP アドレスで構成されている場合には、サブネットは付加されません。たとえば、ソース ゾーンの名前が scannet で、アドレス範囲 10.10.10.0 とサブネット 255.255.255.0 を持つとき、Cisco Anomaly Guard Module が IP アドレス 10.10.10.192 の内部範囲およびサブネット 255.255.255.252 に対して保護モードをアクティブにする場合、サブゾーンの名前は scannet_10.10.10.192_255.255.255.252 となります。サブゾーンの IP アドレスおよびサブネットは、Cisco Anomaly Guard Module が外部からの攻撃の兆候で受信したもの、または Cisco Anomaly Guard Module が保護モードをアクティブにする原因となったパケットの IP アドレスです。

サブゾーンの保護モードが終了すると、Cisco Anomaly Guard Module はサブゾーンを消去します。サブゾーンの保護モードは、通常のゾーンの保護モードを終了するときと同様に、アクティベーション方式および保護の終了のタイムアウトに基づいて終了します。

ゾーン テンプレートからのゾーンの作成

ゾーン テンプレートを使用して新しいゾーンを作成するには、次の手順を実行します。

ステップ 1　次のいずれかの方法で、Create Zone 画面を表示します。

- ナビゲーション ペインで **Detector Summary** をクリックして Detector モジュールの要約メニューを表示してから、次のいずれかのメニュー オプションを選択します。
  - **Zones > Create Zone** を選択する
  - **Zones > Zone list** を選択し、Zone list 画面で **Add** をクリックする
- ナビゲーション ペインで任意のゾーンをクリックしてゾーンのメイン メニューを表示し、そのメニューから **Main > Create Zone** を選択します。

ステップ 2　表 4-1 の説明に従って、ゾーンの設定のパラメータを設定します。

表 4-1　Zone Configuration Form のフィールド

フィールド	説明
Name	新しいゾーンの名前。先頭を英字にして、1 ～ 63 文字の英数字文字列を入力します。文字列にアンダースコア（_）を含めることはできますが、スペースを含めることはできません。
Description	ゾーンについて説明するテキスト。1 ～ 80 文字の英数字文字列を入力します。

表 4-1　Zone Configuration Form のフィールド（続き）

フィールド	説明
Operation mode	Detector モジュールが攻撃の進行中に動作する異常検出モード。Operation mode ドロップダウン リストから、次のいずれかを選択します。 • **Automatic** : Detector モジュールは、攻撃の進行中に作成する動的フィルタのすべてを自動的にアクティブにします。 • **Interactive :** ユーザは、Detector モジュールが攻撃の進行中に作成して Detector モジュールの推奨事項としてユーザに提示する動的フィルタを受け入れるか無視するか決定します。 ゾーンの検出モードの詳細については、第 9 章「異常の検出のアクティブ化」の「ゾーンの動作モードの変更」の項を参照してください。

表 4-1　Zone Configuration Form のフィールド（続き）

フィールド	説明
Zone Template	ゾーンの設定で使用されるデフォルト ポリシーを定義するゾーン テンプレート。Detector モジュールには、次のプレフィクスを持つ 2 セットのゾーン テンプレートがあります。 • **DETECTOR_** : Detector モジュールでのみ使用するために設計されたゾーン テンプレート。Cisco Anomaly Guard Module とゾーン設定を同期させない場合は、DETECTOR_ バージョンのゾーン テンプレートを選択します。 • **GUARD_** : Detector モジュールと Cisco Anomaly Guard Module で使用するために設計されたゾーン テンプレート。CLI を使用して Cisco Anomaly Guard Module とゾーン設定を同期させる予定の場合は、GUARD_ バージョンのゾーン テンプレートを選択します（『*Cisco Traffic Anomaly Detector Module Configuration Guide*』を参照）。 Template ドロップダウン リストから、次のいずれかを選択します。 • **DETECTOR_DEFAULT** : Detector モジュールのデフォルトのゾーン テンプレート。 • **DETECTOR_WORM :** ゾーンに対する TCP ワーム攻撃を検出できるようにするためのゾーン テンプレート。 • **GUARD_DEFAULT**:Cisco Anomaly Guard Module のデフォルトのゾーン テンプレート。Cisco Anomaly Guard Module は、パケットの送信元 IP アドレスを Cisco Anomaly Guard Module の TCP プロキシ IP アドレスに変更する場合があります。このテンプレートは、該当のゾーン ネットワークの着信 IP アドレスに基づく ACL（IP ベースのアクセス リスト）、アクセス ポリシー、またはロード バランシング ポリシーを使用しない場合に使用することができます。 • **GUARD_TCP_NO_PROXY** : Cisco Anomaly Guard Module を TCP プロキシとして動作させないゾーン用に設計されたゾーン テンプレート。このテンプレートは、インターネット リレー チャット（IRC）サーバ タイプ ゾーンなど、ゾーンが IP アドレスに基づいて運用されている場合に使用できます。

表 4-1　Zone Configuration Form のフィールド（続き）

フィールド	説明
Zone Template（続き）	• **帯域幅限定リンク テンプレート**：小規模なカスタマー（ゾーン）による大規模なネットワークに関係するアプリケーションを主な対象として、特定のサーバまたはサービスではなく、リンクに対する攻撃を検出するために設計されたゾーン テンプレート。リンク テンプレートをこの目的で使用するには、ゾーンを既知の帯域幅ごとにセグメント化できる必要があります。リンク テンプレートを使用して新しいゾーンを作成するときは、protect-ip state を **only-dest-ip** にしてゾーンを定義することをお勧めします（この表の *Protect-IP state* を参照）。帯域幅限定リンク ゾーン テンプレートは、128 K、1 M、4 M、および 512 K の各リンク用が用意されています。 — **DETECTOR_LINK_128K** — **DETECTOR_LINK_1M** — **DETECTOR_LINK_4M** — **DETECTOR_LINK_512K** — **GUARD_LINK_128K** — **GUARD_LINK_1M** — **GUARD_LINK_4M** — **GUARD_LINK_512K** リンク テンプレートで作成されるポリシーは、ゾーンでオンデマンドの保護が必要になった場合に使用できるように設定されます。リンク テンプレートを使用するときは、ラーニング プロセスのポリシー構築フェーズを実行することはできません。ただし、しきい値調整フェーズは実行できます（第 7 章「ゾーンのトラフィックのラーニング」の「ラーニング プロセスの実行」の項を参照）。 これらのゾーンについては、ステップ 5 で Activation extent パラメータを **IP address only** に設定することにより、攻撃されているサブネットまたは範囲に基づいて Cisco Anomaly Guard Module の保護モードをアクティブにすることをお勧めします。

表 4-1　Zone Configuration Form のフィールド（続き）

フィールド	説明
Protect-IP state	Detector モジュールがリモート Cisco Anomaly Guard Module をアクティブにするのに使用する Guard の保護方式。ここで選択する Guard の保護方式により、Cisco Anomaly Guard Module が特定のゾーン保護の要件に集中するようにして、Cisco Anomaly Guard Module のリソースを節約できます。状態を Protect-IP state ドロップダウン リストから選択します。 • **Entire Zone**：トラフィックの異常が検出されると、Detector モジュールは Cisco Anomaly Guard Module をアクティブにし、ゾーン全体を保護します。ゾーン全体が、まとめて保護する必要のある相互に関連したゾーンで構成されている場合は、この方法を使用します。 • **Only Dst IP**：Detector モジュールがゾーン内の異常の対象を判別できる場合、Detector モジュールは Cisco Anomaly Guard Module をアクティブにして、ゾーンの特定の部分に保護を適用します。貴重な保護リソースをゾーン全体に使用するのではなく、ゾーン内部の攻撃対象となるセクションにのみ保護を適用する場合は、このオプションを選択します。 • **Policy type**：トラフィックの異常が検出され、指定したゾーンが宛先になっていた場合、Detector モジュールは Cisco Anomaly Guard Module をアクティブにして、そのゾーンに対する保護を適用します。検出した異常トラフィックの宛先が指定ゾーンかどうか判断できない場合にも、Detector モジュールはすべてのゾーンにわたって Cisco Anomaly Guard Module 保護をアクティブにします。ゾーン全体が相互に密接に関連したゾーンで構成されているときに、ゾーン内部の攻撃対象となった領域がゾーン全体に損害を与える事態を避けるには、この方法を使用します。

表 4-1　Zone Configuration Form のフィールド（続き）

フィールド	説明
Protect-IP state（続き）	• **Only Dst IP by address**：トラフィックの異常が検出され、特定の IP アドレスが宛先となっていた場合、Detector モジュールは Cisco Anomaly Guard Module をアクティブにして、その IP アドレスを保護します。この IP アドレスは、Cisco Anomaly Guard Module に定義されているいずれかのゾーンのアドレス範囲に存在する必要があります。ただし、Cisco Anomaly Guard Module のゾーン名が Detector モジュールのゾーン名と同じである必要はありません。Cisco Anomaly Guard Module のゾーン名が Detector モジュールのゾーン名と同じでない場合、またはゾーン全体が関連性のないサブゾーンで構成されている場合には、この方法を推奨します。 （注）　攻撃を受けた IP アドレスに対してのみ Cisco Anomaly Guard Module が保護モードをアクティブにするようにするには、Cisco Anomaly Guard Module でゾーンのアクティベーション範囲が IP Address Only として定義されていることを確認してください。このように定義すると、Guard をアクティブにして攻撃の対象となる IP アドレスを保護できる一方で、ゾーン全体のトラフィックを Guard に宛先変更することを回避できます。
IP address	ゾーンの IP アドレス。
Mask	ゾーンのアドレス マスク。アドレス マスクを Mask ドロップダウン リストから選択します。

ステップ 3　次のいずれかのオプションを選択します。

- **OK**：新しいゾーン設定を保存します。ゾーンの全般ビュー画面が表示され、ゾーンの設定情報が示されます。

  （オプション）全般ビュー画面に表示される Attack Detection/Termination、Activation、および Packet Dump のパラメータを設定するには、**Config** をクリックして Config 画面を表示し、次のステップに進みます。

  - Attack Detection/Termination のパラメータを設定する場合は、ステップ 4（GUARD_ ゾーン テンプレートのみ）
  - Activation のパラメータを設定する場合は、ステップ 5（GUARD_ ゾーン テンプレートのみ）
  - Packet Dump のパラメータを設定する場合は、ステップ 6
- **Clear**：フォームの情報をデフォルト値に戻し、追加した情報をすべて消去します。
- **Cancel**：情報を保存せずに Create Zone 画面を終了します。Zone List 画面が表示されます。

ステップ 4　（オプション）GUARD_ ゾーン テンプレートを使用して作成するゾーンの Attack Detection/Termination のパラメータを設定します。この設定は、Cisco Anomaly Guard Module のゾーンにのみ影響します。表 4-2 の説明に従ってパラメータを設定します。

表 4-2　Attack Detection/Termination のパラメータ

フィールド	説明
Malicious-rate detection threshold	ドロップされるゾーン パケットの最小レート。レートがこのしきい値より低くなった場合、Cisco Anomaly Guard Module がゾーンの保護モードを終了することがあります。Cisco Anomaly Guard Module は、保護メカニズム（動的フィルタ、フレックスコンテンツ フィルタ、およびレート リミッタ）が攻撃の一部として識別したゾーン パケットをドロップします。ドロップされるパケットは、ゾーンの Dropped カウンタを使用してカウントされます。 Malicious-rate detection threshold のデフォルトは、10 パケット / 秒（pps）です。

表 4-2　Attack Detection/Termination のパラメータ（続き）

フィールド	説明
Protection-end timer	Cisco Anomaly Guard Module が保護モードを終了できる時刻。Cisco Anomaly Guard Module では、作成する動的フィルタをチェックすることで攻撃が終了したかどうかを確認します。使用中になっている動的フィルタがなく、事前定義されている期間内に新しい動的フィルタが作成されなかった場合、Cisco Anomaly Guard Module は保護モードを非アクティブにします。1 秒以上の値を入力します。無期限にすることもできます。
Filter-rate termination threshold	このしきい値は、Malicious-rate termination threshold とともに使用して、Cisco Anomaly Guard Module が動的フィルタを非アクティブにできるタイミングを指定します。このしきい値は、パケット / 秒（pps）単位で定義します。
Malicious-rate termination threshold	このしきい値は Filter-rate termination threshold とともに使用して、Cisco Anomaly Guard Module が動的フィルタを非アクティブにできるタイミングを指定します。このしきい値は、パケット / 秒（pps）単位で定義します。

ステップ 5　（オプション）GUARD_ ゾーン テンプレートを使用して作成するゾーンのアクティベーション範囲を設定します。この設定は、Cisco Anomaly Guard Module のゾーンにのみ影響します。表 4-3 の説明に従って、パラメータを設定します。

表 4-3　Activation のパラメータ

フィールド	説明
Activation interface	保護のアクティベーション方式。この方式により、外部からの攻撃の兆候を受信した場合に Cisco Anomaly Guard Module がゾーン保護をアクティブにするゾーンを特定する方法が決まります。デフォルトでは、Cisco Anomaly Guard Module は、ゾーン名に基づいてゾーン保護をアクティブにします。ゾーン名を使用せずにゾーンの保護をアクティブにするには、代替となる次のアクティベーション方式のいずれかまたは両方を選択します。 • **By packet** : Cisco Anomaly Guard Module は、受信パケットの宛先 IP アドレスに基づいてゾーン保護をアクティブにします。Detector モジュールはゾーンのデータベースをスキャンし、受信パケットの宛先 IP アドレスを含むアドレス範囲を持つゾーンをアクティブにします。 • **By IP address** : Cisco Anomaly Guard Module は、受信 IP アドレスに基づいてゾーン保護をアクティブにします。Detector モジュールはゾーンのデータベースをスキャンし、受信 IP アドレスまたはサブネットを含むアドレス範囲を持つゾーンをアクティブにします。 必要なアクティベーション インターフェイスの隣にあるチェックボックスをオンにします。**By packet** と **By IP address** の両方を選択すると、Cisco Anomaly Guard Module は IP アドレスまたはパケットのアクティベーション インターフェイスを使用します。どちらのチェックボックスもオンにしない場合、Cisco Anomaly Guard Module はゾーン名のアクティベーション インターフェイスを使用します。

表 4-3　Activation のパラメータ（続き）

フィールド	説明
Activation extent	Cisco Anomaly Guard Module が、外部からの攻撃の兆候を受信した場合に、ゾーン全体またはゾーンの一部のどちらに対してゾーン保護をアクティブにするかを定義します。 次のいずれかのオプションを選択します。 • **IP address only**：ゾーン内部の指定した IP アドレスまたはサブネットのみ保護をアクティブにします。これがデフォルトのアクティベーション範囲設定です。 • **Entire zone**：ゾーン全体の保護をアクティブにします。

ステップ 6　（オプション）表 4-4 の説明に従って、Packet Dump 領域のパラメータを設定します。

表 4-4　Packet Dump のパラメータ

フィールド	説明
Auto Packet Dump	次のいずれかのオプションの隣にあるチェックボックスをオンにします。 • **On**：自動パケットダンプをイネーブルにします。 • **Off**：自動パケットダンプをディセーブルにします（デフォルト設定）。
Max. disk space	Detector モジュールが自動パケットダンプに使用するディスク スペースの最大容量（MB）を入力します。

既存のゾーンからのゾーンの作成

既存のゾーンをテンプレートとして使用して新しいゾーンを作成するには、次の手順を実行します。

ステップ 1　ナビゲーション ペインで、ゾーン テンプレートとして使用するゾーンを選択します。ゾーンのメイン メニューが表示されます。

ステップ 2　ゾーンのメイン メニューの **Main > Save as** を選択します。Zone Save as 画面が表示されます。

ステップ 3　新しいゾーンの名前を定義します。Name テキスト フィールドに、ゾーン名を 1 ～ 63 文字の英数字文字列で入力します。この文字列は英字で始まる必要があり、アンダースコアを含むことができますが、スペースを含むことはできません。

ステップ 4　次のいずれかのオプションを選択します。

- **OK**：新しいゾーン設定を保存します。ゾーンの全般ビュー画面が表示されます。
- **Clear**：フォームの情報をデフォルト値に戻し、追加した情報をすべて消去します。
- **Cancel**：情報を保存せずに Zone Save as 画面を終了します。ゾーンの全般ビュー画面が表示されます。

ゾーンの設定の変更

ゾーンの設定のパラメータを変更するには、次の手順を実行します。

ステップ 1　ナビゲーション ペインでゾーンを選択します。ゾーンのメイン メニューが表示されます。

ステップ 2　ゾーンのメイン メニューの **Configuration > General** を選択します。ゾーンの全般ビューが表示されます。

ステップ 3　最初のテーブルの下にある **Config** をクリックします。Config Zone 画面が表示されます。

ステップ 4　目的のゾーン パラメータを変更します（パラメータについては、表 4-1 を参照）。

ステップ 5　次のいずれかのオプションを選択します。

- **OK**：新しいゾーン設定を保存します。ゾーンの全般ビュー画面が表示されます。
- **Clear**：フォームの情報をデフォルト値に戻し、追加した情報をすべて消去します。
- **Cancel**：情報を保存せずに Zone Save as 画面を終了します。ゾーンの全般ビュー画面が表示されます。

ゾーンの設定への IP アドレスの追加

ゾーンの設定に IP アドレスを追加するには、次の手順を実行します。

ステップ 1　ナビゲーション ペインでゾーンを選択します。ゾーンのメイン メニューが表示されます。

ステップ 2　ゾーンのメイン メニューの **Configuration > General** を選択します。ゾーンの全般ビューが表示されます。

ステップ 3　2 番目のテーブルの下にある **Add** をクリックします。Add Zone IP 画面が表示されます。

ステップ 4　次のアドレス情報を入力します。

- IP Address：ゾーンの IP アドレス
- IP Mask：ゾーンの IP アドレス マスク

ステップ 5　次のいずれかのオプションを選択します。

- **OK**：新しいゾーン設定を保存します。ゾーンの全般ビュー画面が表示されます。
- **Cancel**：情報を保存せずに Add Zone IP 画面を終了します。ゾーンの全般ビュー画面が表示されます。

ゾーンの IP アドレスまたはサブネットを変更する場合は、次のいずれかの作業を実施します。

- 新しい IP アドレスまたはサブネットが、ゾーンのネットワークに定義されていなかった新しいサービスで構成されている場合は、ゾーンで検出をアクティブにする前にポリシー構築フェーズをアクティブにするか、サービスを手動で追加します。詳細については、第 7 章「ゾーンのトラフィックのラーニング」の「ポリシー構築フェーズの開始」の項、または第 8 章「ゾーンのポリシーの管理」の「サービスの追加または削除」の項を参照してください。

- ゾーンの動作状態が Detect and Learn である場合は、ゾーンのポリシーを未調整としてマークします。ゾーンに対する攻撃がある場合は、ゾーン ポリシーのステータスを未調整に変更しないでください。これは、ステータスを変更すると Detector モジュールで攻撃が検出されなくなり、Detector モジュールが悪意のあるトラフィックのしきい値をラーニングするためです。詳細については、第 7 章「ゾーンのトラフィックのラーニング」の「ゾーンのポリシーに対する調整済みまたは未調整のマーク付け」の項を参照してください。
- ゾーンの動作状態が Detect and Learn ではなく、Detect and Learn 動作状態をアクティブにする予定もない場合は、ゾーンで検出をアクティブにする前にしきい値調整フェーズをアクティブにします。詳細については、第 7 章「ゾーンのトラフィックのラーニング」の「しきい値調整フェーズの開始」の項を参照してください。

ゾーンの設定からの IP アドレスの削除

ゾーンの設定から IP アドレスを削除するには、次の手順を実行します。

ステップ 1　ナビゲーション ペインでゾーンを選択します。ゾーンのメイン メニューが表示されます。

ステップ 2　ゾーンのメイン メニューの **Configuration > General** を選択します。ゾーンの全般ビューが表示されます。

ステップ 3　削除する各 IP アドレスの隣にあるチェックボックスをオンにします。表示されている IP アドレスをすべて削除するには、ヘッダーの IP カラムの隣にあるチェックボックスをオンにします。

ステップ 4　2 番目のテーブルの下にある **Delete** をクリックします。ゾーンの設定から IP アドレスが削除されます。

ゾーンの削除

1 つまたはそれ以上のゾーンを削除するには、次の手順を実行します。

ステップ 1　ナビゲーション ペインで **Detector Summary** をクリックします。Detector モジュールの要約メニューが表示されます。

ステップ 2　Detector モジュールのメイン メニューの **Zones > Zone list** を選択します。Zone list 画面が表示されます。

ステップ 3　削除する各ゾーンの隣にあるチェックボックスをオンにし、**Delete** をクリックします。表示されているゾーンをすべて削除するには、Zone の隣にあるチェックボックスをオンにし、**Delete** をクリックします。削除の確認画面が表示されます。

ステップ 4　次のいずれかのオプションを選択します。

- **OK**：ゾーンを削除して Zone list 画面を表示します。
- **Cancel**：ゾーンの削除要求を無視して Zone list 画面を表示します。