CHAPTER 10

ゾーンの保護

この章では、Cisco Anomaly Guard Module（Guard モジュール）の設定およびアクティブ化の方法について説明します。これらの手順は、ゾーン保護をイネーブルにするために必要です。

この章は、次の項で構成されています。

ゾーンについて

ゾーン保護をアクティブにする前に、Cisco Traffic Anomaly Detector Module（Detector モジュール）から Guard モジュールにゾーンのトラフィック パターンをラーニングするか、またはゾーン ポリシーを含めたゾーン設定を同期しておくことをお勧めします。ラーニング プロセスにより、Guard モジュールで各ゾーンのトラフィック パターンをラーニングし、ゾーン トラフィックの統計分析に従って推奨のしきい値のセットを作成することができます。ゾーンの IP アドレス範囲が重なっていなければ、複数のゾーンを同時に保護できます。

ラーニング プロセスを開始する前にトラフィックの宛先変更を設定するか、ゾーンのトラフィックを Guard モジュールに手動で宛先変更する必要があります。Guard モジュールのルーティング設定を使用して、ゾーンの宛先変更を設定してください。詳細については、第 5 章「トラフィックの宛先変更の設定」を参照してください。

ゾーンが攻撃を受けていなければ、保護およびラーニング機能をアクティブにして、Guard モジュールがゾーン トラフィックを常に宛先変更するようにし、ゾーン ポリシーのしきい値を調整できます。詳細については、P.6-15 の「Guard モジュールの Cisco Traffic Anomaly Detector Module とのゾーン設定の同期」を参照してください。

次の保護特性を定義できます。

- 動作モード：Guard モジュールがゾーン保護を実行する方法を設定して、Guard モジュールがゾーン保護手段を自動的に適用するか、またはインタラクティブな方式で適用するかを定義できます。
- アクティベーション方式：ゾーンをアクティブにするときに、ゾーン名、ゾーンのアドレス範囲、または受信トラフィックのいずれに従うかを定義します。ゾーン保護が外部デバイス（Detector モジュールなど）によってアクティブにされる場合は、アクティベーション方式を設定する必要があります。
- アクティベーション範囲：ゾーン保護を、ゾーンのアドレス範囲全体についてアクティブにするか、ゾーン内の特定の IP アドレスに限定してアクティブにするかを定義します。アクティベーション範囲は、ゾーン保護が Detector モジュールなどの外部デバイスによってアクティブにされる場合に限り、ゾーンに適用されます。
- 保護の終了のタイムアウト：Guard モジュールがゾーン保護を終了するまでのタイムアウトを定義します。

オンデマンド保護のアクティブ化

ゾーンが攻撃を受けている場合は、Guard モジュールによるゾーン トラフィック特性のラーニングをイネーブルにせずに、システム定義のゾーン テンプレートを使用してゾーンを保護できます。ゾーン テンプレートにおける定義済みのポリシーとフィルタにより、Guard モジュールに未知のトラフィック特性を持つゾーンを保護できます。これらのゾーン ポリシーのデフォルトのしきい値は、ゾーンのトラフィックに異常を発見した場合に Guard モジュールがスプーフィング防止機能をすぐにアクティブにするように調整されています。

Guard モジュールはゾーンのトラフィック パターンを認識しないため、定義済みポリシーでは、送信元 IP アドレスをブロック（ドロップ）するために使用されるしきい値が高く設定されています。オンデマンド保護では、スプーフィングされていない攻撃を軽減する場合にユーザの介入が必要です。正当なトラフィックと悪意のあるトラフィックのゾーンのレートを監視して、Guard モジュールの軽減アクションを確認する必要があります。

ゾーンに対する攻撃があり、次のいずれかの条件に当てはまる場合は、ゾーンのオンデマンド保護が必要になる場合があります。

- ゾーンがラーニング プロセスの実行中である。
- 保護およびラーニング機能がイネーブルになっているが、Guard モジュールは、ゾーンのトラフィック特性をラーニングしていない。
- ゾーンのトラフィックを表さないと考えられるポリシーのしきい値を受け入れている。

オンデマンド保護をアクティブにするには、次の手順を実行します。

ステップ 1　次のコマンドを入力して新しいゾーンを作成します。

zone *new-zone-name* [*template-name*] [**interactive**]

詳細については、P.6-6 の「ゾーン テンプレートからの新しいゾーンの作成」を参照してください。

ステップ 2　ゾーンの IP アドレスを定義するには、次のコマンドを入力します。

```
ip address ip-addr [ip-mask]
```

詳細については、P.6-10 の「ゾーンのアトリビュートの設定」を参照してください。

ステップ 3　次のコマンドを入力してゾーン保護をアクティブ化します。

```
protect
```

詳細については、P.10-16 の「ゾーン保護のアクティブ化」を参照してください。

ステップ 4　ゾーンのトラフィック パターンを分析します。詳細については、第 15 章「Guard モジュールによる軽減の分析」を参照してください。

Guard がゾーン保護を行う方法の設定

次のいずれかの方法で、Guard がゾーン保護を実行するように設定できます。

- 自動保護モード：動的フィルタはユーザの操作なしでアクティブになります。この動作モードはデフォルトです。
- インタラクティブ保護モード：動的フィルタは、インタラクティブ　モードにおいて手動でアクティブになります。動的フィルタは推奨事項としてグループ化され、ユーザの決定を待ちます。ユーザは、どの推奨事項を受け入れるか、無視するか、自動アクティベーションに切り替えるかを確認して決定できます。

詳細については、第 11 章「インタラクティブ保護モードの使用方法」を参照してください。

保護アクティベーション方式の設定

保護アクティベーション方式は、外部からの攻撃の兆候を受信したときに、ゾーン保護をアクティブにするゾーンを Guard モジュールがどのように識別するかを定義します。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。

Guard モジュールが保護をアクティブにするために使用する方式は、次のいずれかです。

- ip-address：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 Detector モジュールなどの外部デバイスからコマンドを受信した場合に、ゾーン保護をアクティブにします。
- packet：ゾーン宛てのトラフィックを受信したときにゾーン保護をアクティブにします。
- packet-or-ip-address：ゾーンを宛先とするトラフィック（パケット）を受信した場合、またはゾーンのアドレス範囲の一部である IP アドレスまたはサブネットで構成される Detector モジュールなどの外部デバイスからのコマンドを受信した場合に、ゾーン保護をアクティブにします。
- zone-name-only：ゾーン名に基づいたゾーン保護をアクティブにします。

パケットか、パケットまたは IP アドレスの保護アクティベーション方式でゾーンを構成する場合は、次の手順を実行します。

- 外部デバイスを使用してゾーン トラフィックを Guard モジュールに手動で宛先変更する必要があります。これを設定しないと、Guard はゾーンのトラフィックを監視できません。
- **protect-packet activation-sensitivity** コマンドを入力することにより、Guard モジュールがゾーン トラフィックをアクティブにするために必要とされる最小受信トラフィック レートを設定できます（詳細については、P.10-9 の「ゾーン保護をアクティブにする詳細度の設定」を参照してください）。
- 同一のアドレス範囲に 2 つ以上のゾーンを設定しないでください。複数のゾーンを設定すると、ゾーン保護は正しく機能しません。

保護アクティベーション方式が zone-name-only ではない場合、Guard モジュールは、ゾーンのアクティベーション範囲に従って、ゾーン全体または指定された IP アドレス範囲をアクティブにします（P.10-10 の「保護アクティベーション範囲の設定」を参照）。保護アクティベーション方式が zone-name-only である場合、Guard モジュールはゾーン全体をアクティブにします。

保護アクティベーション方式を設定するには、ゾーン設定モードで次のコマンドを使用します。

activation-interface {**ip-address** | **packet** [**divert**] | **packet-or-ip-address** [**divert**] | **zone-name-only**}

デフォルトは zone-name-only です。既存のゾーンを複製してゾーンを作成する場合、複製元になったゾーンの設定に関わらず、protection activation method は zone-name-only に設定されます。P.6-8 の「既存のゾーンの複製による新しいゾーンの作成」を参照してください。

表 10-1 に、**activation-interface** コマンドのキーワードを示します。

表 10-1　activation-interface コマンドのキーワード

パラメータ	説明
ip-address	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 Detector モジュールなどの外部デバイスからコマンドを受信した場合に、ゾーン保護をアクティブにします。Guard 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。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、Guard モジュールは、プレフィックスが最も長く一致するゾーン（受信 IP アドレスを含むアドレス範囲が最も限定的なゾーン）をアクティブにします。受信 IP アドレスまたはサブネットは、ゾーンの IP アドレス範囲に完全に含まれている必要があります。

表 10-1　activation-interface コマンドのキーワード（続き）

パラメータ	説明
packet	ゾーン宛てのトラフィックを受信したときにゾーン保護をアクティブにします。Guard 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 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 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、Guard モジュールは、プレフィックスが最も長く一致するゾーン（受信 IP アドレスを含むアドレス範囲が最も限定的なゾーン）をアクティブにします。受信 IP アドレスまたはサブネットは、ゾーンの IP アドレス範囲に完全に含まれている必要があります。 **（注）** パケットの保護アクティベーション方式でゾーンを設定する場合、Guard モジュールはアクティブなゾーンが宛先になっていないトラフィックを処理する方法を変更します。そのトラフィックへの注入を設定した場合、Guard モジュールはトラフィックをドロップする代わりに転送します。
divert	（オプション）BGP[1] 通知を隣接ルータに送信して、ゾーン トラフィックを元のパスから Guard モジュールに宛先変更します。Detector モジュールが BGP を使用して、Guard モジュールのゾーン保護をアクティブにする場合、**divert** キーワードを使用します。 詳細については、『*Cisco Traffic Anomaly Detector Module Configuration Guide*』を参照してください。
packet-or-ip-address	ゾーンを宛先とするトラフィック（パケット）を受信した場合、またはゾーンのアドレス範囲の一部である IP アドレスまたはサブネットで構成される Detector モジュールなどの外部デバイスからのコマンドを受信した場合に、ゾーン保護をアクティブにします。詳細については、この表の ip-address および packet 保護アクティベーション方式を参照してください。

表 10-1　activation-interface コマンドのキーワード（続き）

パラメータ	説明
zone-name-only	ゾーン名に基づいてゾーン保護をアクティブにします。Guard モジュールは、Guard モジュールが Detector モジュールなどの外部デバイスから受信するコマンドで呼び出されるゾーンのゾーン保護をアクティブにします。このアクティベーション方式はデフォルトです。

1. BGP = ボーダー ゲートウェイ プロトコル（Border Gateway Protocol）

次の例は、保護アクティベーション方式を設定する方法を示しています。これによって、ゾーンの IP アドレス範囲内のパケットを受信すると、Guard モジュールは保護をアクティブにします。

```
user@GUARD-conf-zone-scannet# activation-interface packet
```

（注）　アクティベーション範囲が ip-address-only で（P.10-10 の「保護アクティベーション範囲の設定」を参照）、アクティベーション方式が zone-name-only でない場合は、**protection-end-timer** コマンドを使用して、ゾーンに対する攻撃が終了したことを Guard モジュールが識別するためのタイマーを設定することをお勧めします（P.10-14 の「保護の無活動タイムアウトの設定」を参照）。**protection-end-timer forever** コマンドを入力すると、Guard モジュールは、攻撃が終了したときに、ゾーン保護を終了しません。また、特定の IP アドレスを保護するために作成したサブゾーンを削除しません。

受信 IP アドレスまたはパケットが他のどのゾーンの一部でもない場合に備えて、保護のための Guard モジュールのデフォルト ゾーンを作成することができます。デフォルトのゾーンを定義できるのは、ネットワークが同種であるために、同じゾーン テンプレートを使用できる場合だけです。デフォルトのゾーンに対してラーニング プロセスを実行することはできません。IP アドレスが 0.0.0.0 で、サブネットが 0.0.0.0 のゾーンを作成します。アクティベーション範囲を ip-address として定義します（P.10-10 の「保護アクティベーション範囲の設定」を参照）。

ゾーンのアクティベーション方式を表示するには、ゾーン設定モードで **show running-config** コマンドを使用します。

ゾーン保護をアクティブにする詳細度の設定

Guard モジュールがゾーン保護をアクティブにするために使用する方式が packet か、packet-or-ip-address の場合、単一 IP アドレスへの受信トラフィック レートがアクティベーションの詳細度よりも高い場合に限り、Guard モジュールはゾーン保護をアクティブにします。アクティベーションの詳細度はグローバルに定義され、すべてのゾーンに適用されます。

ゾーン保護をアクティブにするのに必要な最小パケット レートを変更するには、設定モードで次のコマンドを使用します。

protect-packet activation-sensitivity *min-rate*

min-rate 引数には、Guard モジュールがゾーン保護をアクティブにする原因となる、単一のゾーン宛先 IP アドレス宛ての最小パケット レートを定義します。デフォルトは 0 パケット / 秒（pps）です。

次の例は、アクティベーション詳細度を 10 pps に設定する方法を示しています。

```
user@GUARD-conf# protect-packet activation-sensitivity 10
```

保護アクティベーション範囲の設定

保護アクティベーション範囲は、Guard モジュール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ゾーン保護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。

Guard モジュールは、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：ゾーン全体についてゾーン保護をアクティブにします。Guard モジュールは、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、ゾーン保護をアクティブにします。
- IP アドレスのみ：指定した IP アドレスまたはサブネットに限定してゾーン保護をアクティブにします。Guard モジュールが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 Detector モジュールなどの外部デバイスからのコマンドを受信した場合、Guard モジュールは新しいゾーン（サブゾーン）を作成します。このアクティベーション範囲はデフォルトです。詳細については、P.10-12 の「サブゾーンについて」を参照してください。

アクティベーション範囲を設定するには、ゾーン設定モードで次のコマンドを使用します。

activation-extent {**entire-zone** | **ip-address-only**}

表 10-2 に、**activation-extent** コマンドのキーワードを示します。

表 10-2　activation-extent コマンドのキーワード

パラメータ	説明
entire-zone	ゾーン全体のゾーン保護をアクティブにします。
ip-address-only	指定した IP アドレスまたはサブネットに限定してゾーン保護をアクティブにします。このアクティベーション範囲はデフォルトです。

次の例は、**activation-extent** コマンドを使用して、ゾーン全体のゾーン保護のアクティベーション範囲を設定する方法を示しています。

```
user@GUARD-conf-zone-scannet# activation-extent entire-zone
```

ゾーンのアクティベーション範囲を表示するには、**show running-config** コマンドを使用します。

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）に対してゾーン保護をアクティブにした場合、Guard モジュール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ます。

サブゾーンの設定は、IP アドレスと名前が異なる場合を除いて、ソース ゾーンの設定と同様です。サブゾーンの名前は、ソース ゾーン名の最初の 30 文字と、アンダースコアで連結された IP アドレスおよびサブネットで構成されます。サブゾーンが単一の IP アドレスで構成される場合、サブネットは追加されません。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* を持つ場合に、Guard モジュールが 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* に対してゾーン保護をアクティブにすると、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、Guard モジュールが外部コマンドとともに受信したもの、または Guard モジュールがゾーン保護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。

ゾーン保護を終了すると、Guard モジュールはサブゾーンを削除します。Guard モジュールは、ソース ゾーンに対して設定されたアクティベーション方式と保護の終了のタイムアウトに従って終了します。**no protect** コマンドまたは **deactivate** コマンドを使用してゾーン保護を手動で終了した場合、Guard モジュールはサブゾーンを削除しません。

（注） ゾーン上の攻撃が終了したかどうかの識別に Guard モジュールが使用するタイマーを **protection-end-timer forever** コマンドを使用して設定する場合、Guard モジュールは攻撃が終了したときにゾーン保護を終了せず、サブゾーンを消去しません。

Guard モジュールがサブゾーンを削除しても、サブゾーンのログと攻撃レポートは消去されません。

Guard モジュールがサブゾーンを消去した後にサブゾーンのログおよびレポートを表示するには、次のコマンドを使用します。

- **show log** *sub-zone-name*：詳細については、P.13-5 の「Guard モジュールの設定の表示」を参照してください。
- **show reports** *sub-zone-name* [*report-id* | **current**] [**details**]：詳細については、P.12-14 の「攻撃レポートの表示」を参照してください。

ゾーンから作成されたサブゾーンのリストを表示するには、コマンドを入力して *sub-zone-name* 引数で **Tab** キーを押します。

次の例は、消去されたサブゾーンのログを表示する方法を示しています。

```
user@GUARD-conf-zone-scannet# show logs scannet_10.10.10.192
```

保護の無活動タイムアウトの設定

Guard モジュールは、ゾーンに対する攻撃が終了したことを識別したときに、ゾーン保護およびラーニング プロセスをアクティブまたは非アクティブにできます。Guard モジュールは、ゾーンを保護している場合、ゾーンが攻撃を受けなくなった時点でゾーン保護を終了します。保護およびラーニング機能がイネーブルの場合、Guard モジュールはゾーンへの攻撃を検出したときにラーニング プロセスを非アクティブにし、ゾーンへの攻撃がなくなったときにラーニング プロセスを再開します。

Guard モジュールは、ゾーンに対する攻撃が終了したかどうかを、無活動タイムアウトに従って確認します。このタイムアウトは、数秒から無限まで定義できます。

無活動タイムアウトを定義するには、ゾーン設定モードで次のコマンドを使用します。

protection-end-timer {*time-seconds* | **forever**}

表 10-3 に、**protection-end-timer** コマンドの引数とキーワードを示します。

表 10-3　protection-end-timer コマンドの引数とキーワード

パラメータ	説明
time-seconds	タイムアウト（秒単位）。61 以上の整数を入力します。
forever	無限のタイムアウトを設定します。

デフォルトは **forever** です。デフォルト値を変更しない場合は、ゾーン保護を手動で非アクティブにする必要があります。

次の例は、保護の無活動タイムアウトを設定する方法を示しています。

```
user@GUARD-conf-zone-scannet# protection-end-timer 300
```

Guard モジュールは、動的フィルタの無活動およびドロップされたトラフィックに基づいて無活動を測定します。事前定義された期間中に、使用中になった動的フィルタがなく、次の両方の条件に該当している場合、Guard モジュールはゾーンに対する攻撃が終了したものと見なします。

- 新しい動的フィルタが追加されていない：動的フィルタを削除するタイミングを Guard モジュールがどのように決定するかについては、P.7-41 の「動的フィルタの非アクティブ化」を参照してください。
- ドロップされるゾーン　トラフィックのレートが定義されているしきい値よりも低い：Guard モジュールは、動的フィルタ、ユーザ フィルタ、およびフレックスコンテンツ フィルタが攻撃の一部として識別するゾーン パケットをドロップします。また Guard モジュールは、**rate-limit** コマンドが使用されるときに、ゾーンに対して定義されたレート リミットを超過したトラフィックをドロップします。Guard モジュールはゾーンの Dropped カウンタを使用してドロップするパケットをカウントします（詳細については、P.13-8 の「カウンタを使用したトラフィックの分析」を参照）。デフォルトのしきい値は 1 pps です。ドロップ カウンタのしきい値を変更するには、ゾーン設定モードで次のコマンドを入力します。

  attack-detection zone-malicious-rate *threshold*

  threshold 引数には、ドロップされるゾーン パケットの最小レートを定義します。レートがこのしきい値より低くなった場合、Guard モジュールはゾーン保護を終了することがあります。レートがこのしきい値を超えた場合、Guard モジュールはゾーンへの攻撃を識別し、攻撃レポートを作成します。

ゾーンのアクティベーション方式が Packet である場合、Guard モジュールはゾーンを非アクティブにする前に、受信したトラフィックに基づいて無活動をチェックします。Guard モジュールが保護を非アクティブにするのは、前の条件が当てはまり、ゾーンへのパケットが受信されなかった場合のみです。

ゾーン保護のアクティブ化

外部デバイス（Detector モジュールなど）がゾーンへの攻撃を検出してから、ゾーンを保護するように Guard モジュールを設定することもできますが、ゾーンの設定が完了してから Guard モジュールをアクティブ化してゾーンを保護することもできます。Guard モジュールがゾーンを保護する場合、Guard モジュールはゾーンのトラフィックを自分自身に宛先変更し、その保護ポリシーを適用します。

Guard モジュールでゾーンのトラフィック特性をラーニングし終わる前にゾーンが攻撃中になった場合は、オンデマンド保護を使用してゾーンを保護します。新しいゾーンに対する Guard モジュールのデフォルトのしきい値を使用すると、効果的なオンデマンド保護を実行できます。詳細については、P.10-3 の「オンデマンド保護のアクティブ化」を参照してください。

（注） **activation-interface packet** コマンドを使用して、アクティベーション範囲を packet に設定している場合は、外部デバイスを使用して、ゾーンのトラフィックを手動で Guard モジュールに宛先変更する必要があります。このようにしないと、Guard モジュールはゾーンのトラフィックを監視できません。

ゾーン保護は、次の方法のいずれかでアクティブにできます。

- ゾーン全体を保護できます。
- ゾーンのアドレス範囲の一部である、IP が特定されたゾーンを保護できます。
- 対象の IP アドレスが含まれている IP アドレス範囲を持つゾーンの名前がわからない場合でも、その IP アドレスを保護できます。

ヒント Guard モジュールがゾーンのトラフィックを受信していることを確認してください。ゾーン保護をアクティブにしてから少なくとも 10 秒待ってから、**show rates** コマンドを入力します。レートのうち少なくとも 1 つの値がゼロより大きいことを確認します。すべてのレートの値がゼロの場合は、宛先変更に問題があることを示しています。詳細については、P.15-3 の「トラフィックの宛先変更の問題」を参照してください。

この項では、次のトピックについて取り上げます。

- ゾーン全体の保護
- ゾーンのアドレス範囲の部分である IP ゾーンの保護
- ゾーン名が未知の場合の IP アドレスの保護

ゾーン全体の保護

ゾーン設定モードで次のコマンドを入力することにより、ゾーン全体を保護できます。

protect [**learning**]

オプションの **learning** キーワードは、Guard モジュールがゾーンを保護してポリシーのしきい値を調整するように設定します。詳細については、P.9-11 の「ポリシーしきい値の調整」を参照してください。

次の例は、ゾーン保護をアクティブにする方法を示しています。

```
user@GUARD-conf-zone-scannet# protect
```

ゾーンのアドレス範囲の部分である IP ゾーンの保護

ゾーンのアドレス範囲の一部である、IP が特定されたゾーンを保護できます。この場合、Guard モジュールは新しいゾーンを作成します。新しいゾーンの名前は、元になるゾーンの最初の 30 文字と、アンダースコアで連結された特定の IP アドレスで構成されます。同じ名前のゾーンがすでに存在する場合、Guard モジュールは同じ名前の別のゾーンを作成せず、既存のゾーンに対するゾーン保護をアクティブにします。

IP が特定されたゾーンについてゾーン保護をアクティブにするには、グローバル モードで次のコマンドを使用します。

protect *zone-name ip-address-general*

表 10-4 に、**protect** コマンドの引数を示します。

表 10-4　ゾーン設定モードの protect コマンドの引数

パラメータ	説明
zone-name	ゾーンの名前。
ip-address-general	ゾーン アドレス範囲内の特定の IP アドレス。IP アドレスをドット区切り 10 進表記で入力します。たとえば、192.168.5.6 と入力します。

このゾーンを削除するには、**zone** コマンドの **no** 形式を使用します。

次の例は、ゾーン scannet の IP アドレス範囲に含まれている IP アドレス 192.168.5.6 のゾーン保護をアクティブにする方法を示しています。

```
user@GUARD# protect scannet 192.168.5.6
creating zone scannet_192.168.5.6
user@GUARD#
```

ゾーン名が未知の場合の IP アドレスの保護

対象の IP アドレスが含まれている IP アドレス範囲を持つゾーンの名前がわからない場合でも、グローバル モードで次のコマンドを入力することにより、その IP アドレスを保護できます。

protect *ip-address-general* [*subnet-mask*]

表 10-5 に、**protect** コマンドの引数を示します。

表 10-5　グローバル モードの protect コマンドの引数

パラメータ	説明
ip-address-general	ゾーンのアドレス範囲内の特定の IP アドレス。IP アドレスをドット区切り 10 進表記で入力します。たとえば、192.168.5.6 と入力します。
subnet-mask	（オプション）ゾーン保護をアクティブにするサブネットマスク。IP アドレスをドット区切り 10 進表記で入力します。たとえば、255.255.255.252 と入力します。

Guard モジュールは、IP アドレス アクティベーション方式に基づいて、その IP アドレスを含む IP アドレス範囲を持つゾーンに対するゾーン保護をアクティブにします。詳細については、P.10-10 の「保護アクティベーション範囲の設定」を参照してください。

次の例は、IP アドレス 192.168.5.6 のゾーン保護をアクティブにする方法を示しています。

```
user@GUARD# protect 192.168.5.6
```

複数のゾーンに対して同時に **protect** 関連のコマンドを入力できます。これには、グローバル モードで、ワイルドカードにアスタリスク（*）を使用してコマンドを発行します。たとえば、すべてのゾーンについてゾーン保護を停止する場合は、グローバル モードで **no protect *** コマンドを入力します。名前が *scan* で始まるゾーン（scannet や scanserver など）すべてについてゾーン保護を停止する場合は、グローバル モードで **no protect** *scan**** コマンドを入力します。

ゾーン保護の非アクティブ化

ゾーンに対する攻撃がなく、ゾーンのトラフィック異常の検出を他のソースに依存しているときは、ゾーン保護を非アクティブにして、Guard モジュールへのトラフィックの宛先変更を終了することができます。

ゾーン保護を非アクティブにするには、ゾーン設定モードで次のコマンドのいずれかを使用します。

- **no protect**：ゾーン保護を終了します。保護およびラーニング機能をイネーブルにすると、Guard モジュールはポリシーのしきい値のラーニングを継続します。
- **deactivate**：ゾーン保護と、ラーニング プロセスのしきい値調整フェーズの両方を終了します。

次の例は、ゾーン保護およびラーニング プロセスを非アクティブにする方法を示しています。

```
user@GUARD-conf-zone-scannet# deactivate
```