CHAPTER 4

ゾーンの作成と設定

この章では、Guard 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、Guard が DDoS 攻撃からの保護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）

Guard 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、複数のゾーンを同時に保護できます。次のアトリビュートを含むゾーン設定を作成して、新しいゾーンを定義します。

- 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：ラーニング プロセスを実行したときに Guard 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、Guard のスプーフィング防止機能またはゾンビ防止機能をトラフィックに適用することや、悪意のあるトラフィックのドロップに及びます。
- ゾーン フィルタ：ゾーンのトラフィックを必要な保護レベルに誘導し、Guard で特定のトラフィック フローを処理する方法を定義します。ゾーン フィルタを使用すると、特定のトラフィック フローをカウントすることや、Guard の異常検出機能をバイパスすることができます。デフォルトのフィルタ設定を変更して、独自のゾーン フィルタ設定を作成できます。この設定によって、どの異常検出機能を Guard がトラフィック フローに適用するかが決まります。

次の方法により、ゾーンを作成することができます。

- 事前定義されているゾーン テンプレートを使用する：いずれかの 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。各ゾーン テンプレートには、ネットワーク サービスおよびポリシーしきい値を定義する、あらかじめ定義された一連のポリシーがあります。これらのポリシーは、オンデマンド保護に使用されます。ゾーン テンプレートには、一連のポリシー テンプレートも含まれています。これらのテンプレートは、ラーニング プロセスでゾーンのトラフィックを分析して、検出した各サービスのポリシーを作成するときに Guard が使用します。Guard がラーニング プロセス中に作成する新しい各ポリシーは、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。トラフィック特性が 2 つのゾーン間で異なっている場合は、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があります。実行すると、Guard がゾーンのトラフィックを分析して、必要なポリシー変更を新しいゾーン設定に対して実行できるようになります。

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

ゾーンの設定を定義するときに、Guard がゾーン保護を自動的にアクティブにするためのトリガー、つまりアクティベーション方式を定義できます。また、Guard が保護する領域の範囲も定義できます。たとえば、ゾーン全体や、ゾーン内部の特定の領域のみを Guard で保護することができます。

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

Guard は、ゾーン名に基づいて、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 : Guard 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。これが、Guard がゾーン保護のアクティベーションに使用するデフォルトの方式です。
- IP アドレス : Guard 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。Guard 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 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 IP アドレスを含むアドレス範囲が最も限定的なゾーンがアクティブになります。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。
- パケット : Guard　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。Guard 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、Guard 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 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。

- IP アドレスまたはパケット：Guard は、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。詳細については、上記の「パケット」および「IP アドレス」の説明を参照してください。

ゾーン保護の範囲

アクティベーション範囲は、Guard 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。この兆候は、Cisco Traffic Anomaly Detector などの外部デバイスまたはゾーン（パケット）を宛先とするトラフィックからのコマンドで示されます。

Guard 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。Guard 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。Guard 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、Guard 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、Guard 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、Guard が外部からの攻撃の兆候で受信したもの、または Guard 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、Guard 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 ペインの **Guard Summary** をクリックして Guard の要約メニューを表示し、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	ゾーンの動作モード。Guard は、攻撃の進行中にこのモードで動作します。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**：Guard は、攻撃の進行中に作成する動的フィルタをすべて自動的にアクティブにします。 • **Interactive :** 攻撃の進行中に Guard が作成し、Guard 推奨事項として提示する動的フィルタを受け入れるか拒否するかについて、システム管理者が決定します。 ゾーンの動作モードの詳細については、第 9 章「ゾーン保護のアクティブ化」の「ゾーンの動作モードの変更」の項を参照してください。
Zone Template	ゾーンの設定で使用されるポリシーを定義するゾーン テンプレート。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。 • **GUARD_DEFAULT**：デフォルトのゾーン テンプレート。Guard は、パケットの送信元 IP アドレスを Guard の TCP プロキシ IP アドレスに変更することがあります。このゾーン 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 IP ベースのアクセス リスト（ACL）、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**：TCP プロキシを使用し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、カスタマー（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。帯域幅限定リンク ゾーン テンプレートは、128 Kbps、1 Mbps、4 Mbps、および 512 Kbps の各リンク用が用意されています。 — **GUARD_LINK_1M** — **GUARD_LINK_4M** — **GUARD_LINK_128K** — **GUARD_LINK_512K** リンク テンプレートで作成されるポリシーは、オンデマンドの保護を必要とするアプリケーション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 プロセスの概要」の項を参照）。 これらのゾーンについては、ステップ 4 で activation-extent パラメータを **IP address only** に設定して、攻撃されているサブネットまたは範囲に基づいて Cisco Traffic Anomaly Detector 上で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
Max. Rate	Guard がネットワークに再び注入できるトラフィックの量。帯域幅の値は、ゾーンへの送信で測定された最大の帯域幅に設定します。帯域幅の最大値が不明な場合は、Max. Rate フィールドおよび Burst フィールドをブランクのままにして、ドロップダウン リストから無制限の単位（**unlimit**）を選択します。 最大レートの整数を入力し、ドロップダウン リストから次のいずれかの測定単位を選択します。 • **unlimit**：Guard がネットワークに再び注入するトラフィックのレートを制限しない場合は、このデフォルト設定を使用します。**unlimit** を選択した場合、最大レート値を入力しないでください。 • **mbps**：メガビット / 秒。 • **kbps**：キロビット / 秒。 • **bps**：ビット / 秒。 • **kpp**：キロパケット / 秒。 • **pps**：パケット / 秒。
Burst	最大レートを超過する前に、Guard がゾーンに再び注入できる最大トラフィック バースト サイズ（上記の Max. Rate を参照）。バースト サイズ レートの整数を入力します。Guard は、最大レート（Max. Rate）の測定単位をバースト パラメータに対して使用します。
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、Guard がゾーンの保護モードを終了することがあります。Guard 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 4-1　Zone Configuration Form のフィールド（続き）

フィールド	説明
Protection-end Timer	Guard が保護モードを終了できる時刻。Guard 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、Guard 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	Malicious-rate termination threshold とともに使用して、Guard 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するしきい値。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	Filter-rate termination threshold とともに使用して、Guard 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するしきい値。このしきい値は、パケット / 秒（pps）単位で定義します。
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。

  全般ビュー画面に表示される 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。

  - Activation のパラメータを設定する場合は、ステップ 4
  - Packet Dump のパラメータを設定する場合は、ステップ 5
- **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　表 4-2 の説明に従って、Activation 領域のパラメータを設定します。

表 4-2　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。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 がどのように識別するかを定義します。デフォルトでは、Guard 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**：Guard 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。Guard 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**：Guard 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。Guard 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。 パケットまたは IP アドレスによる保護アクティベーションを選択する場合は、ゾーンが攻撃を受けたときに、トラフィックの宛先を手動で Guard に変更する必要があります。Activation interface のオプションの詳細については、「保護のアクティベーション方式」の項を参照してください。

表 4-2　Activation のパラメータ（続き）

フィールド	説明
Activation extent	Guard 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。 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。 Activation extent のオプションの詳細については、「ゾーン保護の範囲」の項を参照してください。

ステップ 5　表 4-3 の説明に従って、Packet Dump 領域のパラメータを設定します。

表 4-3　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	Guard 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を MB 単位で入力します。

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、次の項を参照してください。
  - 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
  - 第 8 章「ゾーンのポリシーの管理」の「サービスの追加」の項

- 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 Guard で攻撃が検出されなくなり、Guard 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。ゾーンの設定とゾーンの全般ビュー画面から 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 **Guard Summary** をクリックします。Guard の要約メニューが表示されます。

ステップ 2　Guard 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。