

## DDoS 攻撃の軽減対策

Distributed Denial of Service (DDoS; 分散型サービス拒否) 攻撃は、全世界で増加しており、企業にとっての深刻な脅威となっています。これらの攻撃は、現在一般的に使用されているツールでは検出できないように設計されているため、ターゲットとなった企業はたちまち営業不能に陥り、収益と生産性の低下によって、数百万ドルとはいかないまでも、数千ドルの損害を被ることになります。このような DDoS 攻撃からビジネスを保護し、事業活動を維持するためには、DDoS 攻撃を検出して撃退するために設計された新しい専用ソリューションが必要です。

DDoS 攻撃は広範囲の混乱をもたらす兵器です。セキュリティ境界を突破して情報を盗み取るアクセス攻撃と異なり、DDoS 攻撃は、偽のトラフィックによってサーバ、ネットワークリンク、およびネットワークデバイス(ルータ、ファイアウォールなど)の負荷を過剰に増加させてネットワークシステムを麻痺させます。

DDoS 攻撃は、ハッカー、政治的・社会的な動機を持つハッカー「Hactivist」、サイバー恐喝者、および国際的なサイバーテロリストが好んで使用する武器として台頭しています。DDoS 攻撃は、防御が不十分であれば簡単に仕掛けることができ、Web サイトなどのネットワークエッジにあるサーバだけでなく、ネットワークそのものに被害を与えます。実際、アグリゲーションルータ、コアルータ、スイッチ、またはサービスプロバイダーのネットワークにある Domain Name System (DNS; ドメインネームシステム)などのインフラストラクチャをターゲットとした攻撃が、すでに開始されています。2002年10月、その後の大規模な DDoS 攻撃を予告するかのような初歩的な攻撃が仕掛けられ、すべてのインターネット通信のロードマップとして機能する重要なシステムであるルートDNSサーバ13台のうち、8台がその影響を受けました。

サービスプロバイダー、企業、政府機関、教育・研究機関では、インターネットが業務に欠かせないものになるにつれ、DDoS 攻撃が成功した場合の影響が、コスト面でもその他の面でも、ますます深刻になっています。さらに、今後数か月から数年の間に、新しい DDoS ツールによってより破壊的な攻撃が仕掛けられることは確実です。

DDoS 攻撃は防御が難しい攻撃であるため、DDoS 攻撃に正しく効果的に対処することが、インターネットに依存しているサービスプロバイダー、企業、政府機関、教育・研究機関にとっての大きな課題となっています。ファイアウォールや Intrusion Detection System (IDS; 侵入検知システム)などの境界セキュリティテクノロジーは、セキュリティ戦略全体の中では重要なコンポーネントですが、DDoS 攻撃を包括的に軽減する機能はありません。インターネット利用を脅かす最新の DDoS 攻撃に対抗するには、ますます高度化、複雑化し、巧妙になっている攻撃を検出し、撃退する機能を特別に備えた専用のアーキテクチャが必要です。

このホワイトペーパーでは、以下の事項について説明します。

- 増大する DDoS 攻撃の脅威と、攻撃が成功した場合に組織が受ける深刻な影響
- 従来のルータおよび境界セキュリティテクノロジーだけでなく、DDoS 攻撃を軽減するソリューションが必要となる理由
- DDoS 攻撃を撃退するために必要な基礎要件

- DDoS 攻撃を防御するシスコの革新的なテクノロジーとアーキテクチャの仕組み

## DDoS 攻撃の脅威

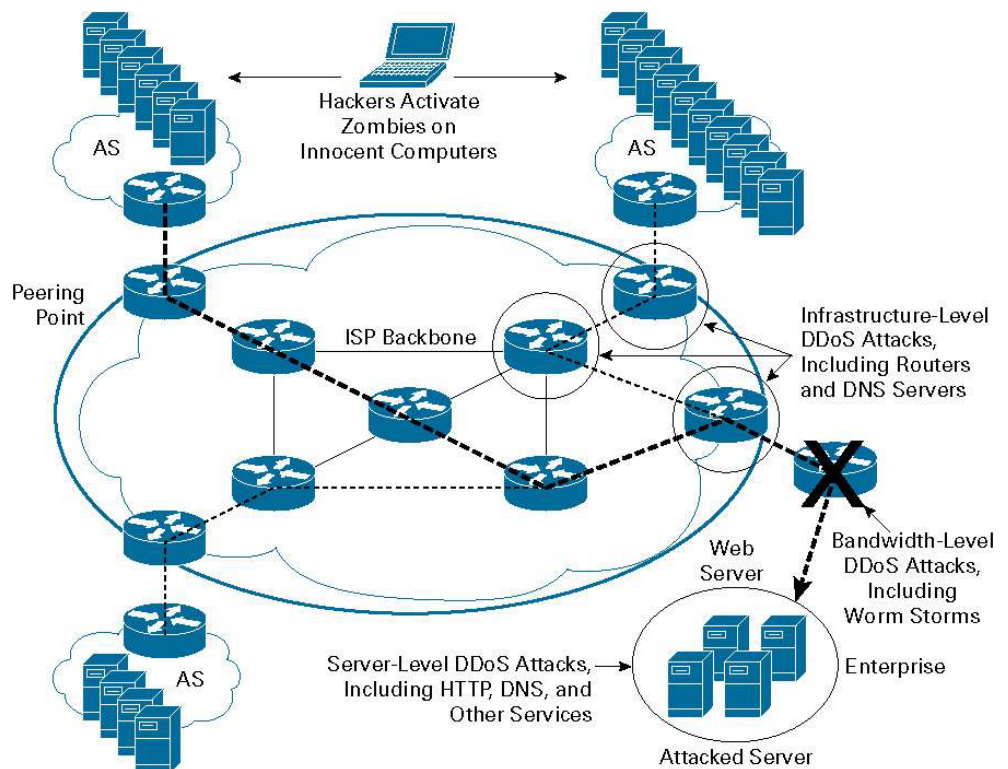
DDoS 攻撃は、数百または数千もの脆弱な「ゾンビ」ホストから、単一のターゲットに対して仕掛けられます。これらのゾンビ ホストは、高速な常時接続によってインターネットにアクセスしている数百万台の無防備のコンピュータの中から作り出されます。ハッカーは、これらのマシンに「スリーパー」コードを埋め込むことによって、DDoS 攻撃の開始命令を待機するゾンビの大群を編成します。ゾンビ ホストの数が多ければ、攻撃は驚くべき規模になります。

## DDoS 攻撃の影響

DDoS 攻撃が成功した場合の影響は、広範囲に及びます。サイトのパフォーマンスが著しく低下するため、顧客やその他のユーザのストレスが増大します。サービス プロバイダーでは、Service-level Agreement (SLA; サービスレベル契約) の違反により、高額の使用料金請求が発生する可能性があります。企業の評判に傷が付き、回復できない場合もあります。収益の減少、生産性の低下、IT 支出の増加、訴訟コストなど、損失は積み上がる一方となります。

損失額は膨大です。Forrester、IDC、および Yankee Group の評価では、大規模な e- コマース企業が 24 時間操業停止に追い込まれた場合のコストは、3000 万ドル近くに達すると予測されています。また Yankee Group の試算では、2000 年 2 月に相次いだ Amazon、Yahoo、eBay、その他の有名なサイトに対する DDoS 攻撃の累積損失額を 12 億ドルと見積もっています。さらに 2001 年 1 月には、サイトに対する数日間の DDoS 攻撃により、Microsoft がおよそ 5 億ドルの損失を被りました。企業がさまざまな脆弱ポイントにおいて防御を強化し、こうした悪意のある攻撃に対する保護措置を講じる必要があることは明らかです(図 1 を参照)。

図 1 さまざまな脆弱ポイントと障害ポイント



### DDoS 攻撃の仕組み

DDoS 攻撃は、どのような仕組みを使って被害を与えるのでしょうか。DDoS 攻撃の場合、任意のソースアドレスから任意の宛先に分け隔てなくデータ パケットが配信されるという、インターネット プロトコルの特性とインターネットの基本機能を悪用しています。

DDoS 攻撃と呼ばれるものは、これらのパケットの動作です。つまり、ネットワーク デバイスやサーバが処理できないほどの大量のパケットが送られること、あるいはパケットによってサーバリソースが急速に消費されてしまうことを意味します。DDoS 攻撃の阻止が困難な理由は、不正なパケットと適正なパケットの区別が難しいことにあります。IDS で使われているような「シグニチャ」によるパターン マッチングでは、DDoS 攻撃を防ぐことはできません。また、これらの攻撃の多くには偽造されたソース IP アドレスが使用されているため、特定のソースアドレスから送られてくる大量のトラフィックを検出するモニタリング ツールを使っても、攻撃元が特定できません。

DDoS 攻撃は、以下のような 2 つのタイプに分けられます。

- 帯域幅攻撃 — この種類の DDoS 攻撃では、大量のパケットを送り込むことで、ネットワーク帯域幅やネットワーク装置のリソースを消費させ、その機能を停止させます。ターゲットとなったルータ、サーバ、およびファイアウォールなどは、処理リソースの限界のために通常のトランザクションが処理できなくなり、過負荷が原因で障害を起こす場合もあります。

最も一般的な帯域幅攻撃は、パケット フラッディングです。この攻撃では、表面上は適正に見える TCP、UDP、または ICMP パケットを特定の宛先に向けて集中的に送り込みます。こうした攻撃では、検出を困難にするため、攻撃元を特定できないようにソース アドレスが偽造されることがあります。

- アプリケーション攻撃 — この種類の DDoS 攻撃では、TCP や HTTP などのプロトコルでの予想される動作を利用して、コンピュータ リソースに過剰な負荷をかけ、正常なトランザクションまたは要求の処理を妨げます。このようなアプリケーション攻撃には、HTTP ハーフオープン攻撃や HTTP エラー攻撃などがあります。

### ますます破壊的になる DDoS 攻撃の脅威

最近の DDoS 攻撃は、高度なスプーフィング技術によって攻撃元を追跡できないようにしたり、(ブロック可能な重要性の低いプロトコルではなく)ビジネスに必須のプロトコルを利用することで破壊力を増強させたりしています。これらの攻撃は、適正なアプリケーション プロトコルやサービスが利用されているため、識別して撃退するのが非常に困難です。パケット フィルタリングやレート リミットといった措置を施しても、適正なユーザも含めてすべてを拒否することになり、結果的には攻撃者の目的を達成させることになってしまいます。

### 現在の DDoS 攻撃防御に足りない機能

どのような種類の DDoS 攻撃であれ、現在のセキュリティ対策は、DDoS 攻撃の軽減とビジネスの継続性確保には不十分です。ブラックホール ルーティングやパケット フィルタリングなど、DDoS 攻撃への対抗措置として一般的に利用されているものも、ますます高度化する攻撃の処理には最適ではありません。IDS は、いくつかの攻撃には優れた検出機能を発揮しますが、DDoS 攻撃を軽減することはできません。ファイアウォールは、ブラックホール ルーティングやパケット フィルタリングなどの基礎レベルの保護機能を提供しますが、最近になって増えている高度な攻撃を阻止できるようには設計されていません。さらに、オーバープロビジョニングのような他の戦略も、攻撃の規模が大きくなれば有効な防御策とはならず、DDoS 防御の戦略としてはコストがかかりすぎます。

## ブラックホール ルーティング

ブラックホール ルーティングとは、攻撃のターゲットとなった企業宛でのトラフィックを、できるかぎり上流でブロックするサービス プロバイダー側での処理のことです。トラフィックはルート変更されて「ブラックホール ルータ」へ送られて廃棄され、プロバイダーのネットワークと他の顧客を保護します。悪意のある攻撃トラフィックとともに適正なパケットも廃棄されるため、ブラックホール ルーティングは DDoS 攻撃の軽減対策になりません。ターゲットとなった企業はすべてのトラフィックを失うため、ビジネスの停止という攻撃者の目的が達成されるからです。

## ルータ

ルータには、Access Control List (ACL; アクセス コントロール リスト) を使用して「望ましくない」トラフィックをフィルタリングする機能があります。これによって、DDoS 攻撃も防御できると多くの人が誤解しています。ACL を利用すれば、重要性の低い不要なプロトコルをフィルタリングすることによって、ping 攻撃などの単純な既知の DDoS 攻撃を阻止できることは事実です。

しかし、現在の DDoS 攻撃では、インターネットを利用するのに必須となるプロトコルが使用されることが多いため、プロトコル フィルタリングでは効果的な防御ができません。また、ルータでは無効な IP アドレス空間に属するパケットを阻止できますが、攻撃者は通常、有効な IP アドレスを偽のソース アドレスとして使っています。そのためルータの ACL は、確かに基本的な攻撃に対する最初の防御ラインとなりますが、以下のような高度な DDoS 攻撃に対する防御としてはうまく機能しません。

- SYN、SYN-ACK、FIN などのフラグディンク — ACL では、Web サーバのポート 80 に対するランダムな偽造ソース アドレスからの SYN 攻撃や ACK および RST 攻撃をブロックできません。この場合、偽造されるソース IP アドレスは常に変更されるため、個々の送信元をすべて特定するには手作業での追跡という事実上不可能な手段しかありません。そのほかの手段としては、サーバ全体をブロックすることがありますが、これは攻撃者の目的を達成させることになります。
- プロキシ — ACL では、プロキシを利用して同じソース IP アドレスから送られる適正な SYN と悪意のある SYN とを区別できません。そのため、ISP の大規模プロキシ サーバや、特定アドレスを指定した DDoS クライアントからの集中的なスプーフィング攻撃を阻止するには、そのアドレスをブロックする必要があります。
- DNS または Border Gateway Protocol (BGP) — ソース アドレスがランダムに偽造される DNS サーバまたは BGP ルータ攻撃が仕掛けられた場合、ランダムに偽造されるトラフィックの量が急速に変化するため、SYN フラグディンクの場合と同様に追跡が不可能になります。そのうえ、偽造されたアドレスと有効なアドレスを識別する方法もありません。
- **アプリケーション レベル(クライアント)攻撃** — 攻撃および個々の偽造されていない送信元を正確に検出できさえすれば、ACL を使って、HTTP エラーおよび HTTP ハーフオープン接続攻撃のようなクライアント攻撃をブロックすることはできます。ただし、ターゲットのクライアントごとに数百、場合によっては数千の ACL を設定する必要があります。

もう 1 つのルータ ベースの DDoS 対策機能に、Unicast Reverse Path Forwarding (uRPF) を使用して送信側でスプーフィング攻撃を阻止する方法があります。ただし、これは最新の DDoS 攻撃に対抗するうえでは無力です。uRPF の基礎的な原則は、IP アドレスがそのサブネットに属さない場合に送信トラフィックをブロックすることです。しかし、攻撃者は実在するアドレスと同じサブネットのソース IP アドレスを偽造できるので、こうした戦略は簡単に突破できます。さらに、uRPF を効果的に適用するためには、攻撃の可能性のあるすべてのサブネット上のルータに実装する必要があります。こうした実装を実際に行うことは、不可能ではありませんが困難です。

## ファイアウォール

ファイアウォールはあらゆる組織のセキュリティ ソリューションにおいて重要な役割を担っています。ただし、ファイアウォールは DDoS 対策専用のデバイスではありません。実はファイアウォールには、高度な最新の DDoS 攻撃に対抗するには不都合な特性があります。

まず設置される位置です。ファイアウォールは、下流から非常に離れたデータ パス上に設置されるため、プロバイダーから企業のエッジ ルータに至るアクセス リンクを保護することはできず、アクセス リンクは DDoS 攻撃に対して脆弱なままです。実際、ファイアウォールはインラインに設置されるので、セッション処理能力を飽和させて障害を引き起こそうとする攻撃者のターゲットとなることがよくあります。

第 2 は、アノマリ検出機能を備えていないことです。ファイアウォールの主な目的は、プライベート ネットワークへのアクセスを制御することであり、その点では優れた機能を発揮します。その方式の 1 つは、内部(「クリーン」な側)から外部のサービスに対して起動されたセッションを追跡し、そこから(「ダーティ」な)外部の送信元を予測して特定の応答のみを受け入れるというものです。しかし、一般に公開している Web、DNS、その他のサービスの場合、外部からの要求を受け取る必要があるため、この方式は役に立ちません。このような場合、ファイアウォールでは特定のサービスポートをオープンして、HTTP トラフィックを Web サーバの IP アドレスに伝送させます。こうしたアプローチは、特定のアドレス宛ての特定のプロトコルのみを受け入れるという意味では一定の保護機能にはなりますが、DDoS 攻撃の軽減対策としては不十分です。ハッカーは「承認された」プロトコル(この場合は HTTP)を使用するだけで攻撃トラフィックを送り込むことができるからです。ファイアウォールではアノマリ検出機能を備えていないため、有効なプロトコルが攻撃手段として利用された場合、検出が不可能になります。

ファイアウォールが DDoS 攻撃への包括的な保護機能を提供できない第 3 の理由は、スプーフィング防止機能を備えていないことです。DDoS 攻撃が検出された場合、攻撃に関連しているフローをファイアウォールでシャットダウンすることは可能ですが、パケットごとにスプーフィング検査を実行して適正なトラフィックと不正なトラフィックとを分離することはできません。偽造された IP アドレスを大量に使用した攻撃を阻止するには、こうした機能が不可欠です。

## IDS

IDS は、アプリケーション層の攻撃検出に優れた機能を提供しますが、有効なパケットを使用する DDoS 攻撃を検出できないという弱点があります。現在のほとんどの攻撃で使用されるパケットは、それ自身には異常がないため、IDS では検出するのが困難です。確かに IDS には、そうした攻撃の検出に必要なアノマリ ベースの機能がいくつか用意されていますが、専門家による相当な手動チューニングが必要であり、攻撃によっては識別できないものもあります。

DDoS 防御プラットフォームとしての IDS に関して考えられるもう 1 つの問題は、IDS は攻撃の検出を行うだけだということです。IDS には、攻撃による影響を軽減する機能がありません。IDS ソリューションによっては、ルータおよびファイアウォールでのフィルタリングを推奨していることがありますが、前述したように、これらは DDoS 攻撃を抑制するうえで効果的とはいえません。IDS に不足しているものは、特定の攻撃フローを識別する機能を提供し、ただちに對抗措置を実施する機能を備えた DDoS 軽減対策ソリューションです。

要約すると、IDS はシグニチャ ベースのアプリケーション層における攻撃の検出に最も適していません。高度な DDoS 攻撃はレイヤ 3 およびレイヤ 4 における異常な動作を引き起こすものであるため、現在の IDS テクノロジーは、DDoS 攻撃の検出または軽減に最適とはいえません。

### DDoS 攻撃への手動対応

DDoS 攻撃の防御方法として部分的に手動処理で対応することもできますが、処理に時間がかかり過ぎ、対応も不十分となります。DDoS 攻撃が仕掛けられると、通常、ターゲットとなったサーバの管理者は最も近い上流の接続プロバイダー (Internet Service Provider [ISP; インターネット サービス プロバイダー]、ホスティング プロバイダー、またはバックボーン通信事業者) に、送信元の特定を依頼します。これは、アドレスが偽造されている場合、多くのプロバイダー間の連携を必要とする長時間の面倒な処理となります。さらに、送信元が特定されたとしても、それをブロックすると、その送信元からの (適正なトラフィックも含めて) すべてのトラフィックをブロックすることになります。

### その他の対策

DDoS 攻撃の対抗策として、オーバープロビジョニング (必要以上の帯域幅または冗長ネットワーク デバイスを導入して、あらゆる要求の急増に対処する) なども考えられます。ただし、そうしたアプローチには、冗長ネットワーク インターフェイスやデバイスの追加が必要になるため、コスト効率に優れているとはいえません。さらに、当初は成果があったとしても、攻撃者は攻撃の規模を拡大して余剰のキャパシティさえ使い果たすことができます。

### アベイラビリティを確保する必要性

インターネットに依存したビジネスを展開している企業では、売り上げのためだけでなく、その他の理由のためにも、DDoS 攻撃の保護対策への投資が必要です。サービス プロバイダー、企業、政府機関、教育・研究機関などでは、インフラストラクチャのコンポーネント (Web サーバ、DNS サーバ、電子メールおよびチャット サーバ、ファイアウォール、スイッチ、ルータなど) を保護し、業務の完全性を維持して、技術スタッフの運用を効率化する必要があります。

### DDoS 攻撃防御の ROI モデル

DDoS 攻撃への包括的な保護対策には、当然それなりのコストがかかります。しかし、そうした実装に対する Return On Investment (ROI; 投資利益率) は、十分に説得力があります。

- e- コマース — e- コマース サイトへの DDoS 攻撃の保護対策コストは、DDoS 攻撃によって発生する可能性のある損失と比較すれば、数時間以内に採算が取れます。DDoS 攻撃によって引き起こされるダウンタイムがもたらす財務的影響を算出する場合は、e- コマース サイトのトランザクションの数、トランザクションあたりの平均収益、広告収益、無形の要素 (企業イメージの失墜や法的責任など)、攻撃されたサイトの復旧に必要な技術スタッフの工数などを、すべて考慮する必要があります。DDoS 攻撃への保護対策を施すことによって、より安価な帯域幅契約に変更できる可能性を含めれば、ROI の値はさらに向上します。
- サービス プロバイダー — サービス プロバイダーにとって、ネットワークの稼働状態を維持することで得られる ROI への波及効果は莫大です。プロバイダーのインフラストラクチャ (ルータ、DNS など) が攻撃を受けると、顧客へのサービスすべてに障害が起こり、SLA 違反が発生することになります。サービス プロバイダーにとって DDoS 攻撃への保護対策コストは、収益と顧客関係の悪化というビジネスの存亡にかかわるような破滅的な障害に対する保険です。

ホスティング、トランジット、およびサービス プロバイダーが包括的な DDoS ソリューションを実装する理由は、コストの問題だけではありません。これらのユーザの場合、DDoS 攻撃への保護対策は、新しい収益源を生み出し、競争上の差別化を可能にする付加価値サービスにもなります。

## DDoS 攻撃による脅威の軽減

DDoS 攻撃に対抗するには、ますます複雑化し、巧妙になる攻撃を検出するだけでなく、攻撃による影響を軽減し、ビジネスの継続性とリソースの可用性を保証できる新しいアプローチが必要です。

DDoS 攻撃への完全な保護対策を構築する場合、以下の 4 つのテーマが重要です。

1. 検出だけでなく、軽減する
2. 攻撃の存在を検出するだけでなく、適正なトラフィックと不正なトラフィックを正確に識別してビジネスの継続性を維持する
3. 上流に展開してすべての脆弱ポイントを保護できるパフォーマンスとアーキテクチャを装備する
4. 信頼性とコスト効率の高いスケーラビリティを保持する

こうしたコンセプトで DDoS 防御を構築すれば、以下のような特性を持つ保護対策を実現できます。

- 攻撃者の正体やプロファイルが常に変化するスプーフィング攻撃が行われても、組み込まれた検出およびブロッキングメカニズムによって、ただちに DDoS 攻撃に対応できる
- ルータによるスタティックなフィルタリングや IDS のシグニチャに比べて、完全な検証機能を提供する
- 振る舞い (behavior) ベースのアノマリ検出機能によって、正常に見えるパケットのなかから、サービス不能を目的に送信されたパケットを検出する
- 偽造された個々のパケットを識別してブロックし、適正なビジネストランザクションを保護する
- 保護されたリソースと同じコストをかけずに、大規模な DDoS 攻撃に対処できるメカニズムを提供する
- 障害ポイントまたはインラインソリューションのスケーリングコストを発生させることなく、攻撃の際にネットワークを保護するオンデマンド展開が可能である
- 不正なトラフィック ストリームのみを処理するインテリジェンスを備え、信頼性を最大限に高めて、スケーリングコストを最小限に抑えられる
- ネットワーク デバイスのリソースや設定の変更に影響を与えずに展開できる
- 標準的なプロトコルを使用してすべての通信を行うことにより、最大限の相互運用性と信頼性を確保できる

## シスコシステムズの DDoS 軽減対策ソリューション

シスコシステムズでは、総合的な保護機能を保証できるように、検出、ルート変更、検証、および転送という原理に基づく、DDoS 保護ソリューションを提供しています。シスコのソリューションが導入されていれば、保護されたターゲットに対して DDoS 攻撃が仕掛けられた場合、ビジネスの継続性は以下のようにして維持されます。

- **DDoS 攻撃を検出する**
- ターゲット デバイスに向かうデータトラフィックをシスコ機器へと**ルート変更**して処理できるようにする
- **トラフィックを分析**し、適正なトラフィック フローのパケットから不正なトラフィック フローをフィルタリングすることによって、悪意のあるトラフィックがパフォーマンスに影響を及ぼすことを防止し、適正なトランザクションを完了できるようにする
- 適正なトラフィックを**転送**してビジネスの継続を維持できるようにする

### シスコのソリューション セット

シスコのソリューションは、あらゆるタイプの DDoS 攻撃に対する完全な保護機能を提供し、まったく新しいタイプの攻撃にも対処できます。シスコのソリューションでは、迅速に攻撃を検出して悪意のあるトラフィックを適正なトラフィックから分離することで、アクティブに攻撃を軽減し、DDoS 攻撃に対して時間単位ではなく秒単位の迅速な対応を可能にしています。重要なルータやスイッチの近くに簡単に展開できるシスコのソリューションは、シングル ポイント障害の存在しない拡張性を備え、既存のネットワーク コンポーネントのパフォーマンスや信頼性には影響を与えないという特長があります。

シスコのソリューション セットには、Cisco Traffic Anomaly Detector XT と Cisco Guard XT という 2 つのコンポーネントが含まれています。これらのアプライアンスが連携することで、事実上あらゆる環境で DDoS 攻撃の影響を軽減します。

- Cisco Traffic Anomaly Detector XT — Cisco Traffic Anomaly Detector XT は、早期警戒システムとして機能し、最も複雑な DDoS 攻撃に対して綿密な分析を行います。Cisco Traffic Anomaly Detector XT では、ネットワークトラフィックのパッシブなモニタリングを行い、「正常」とは異なる動作、または DDoS 攻撃を示す動作を検出します。攻撃を識別すると、Cisco Traffic Anomaly Detector XT は Cisco Guard XT に警告を発し、攻撃に対して迅速に対応できるように詳細なレポートと具体的な警告を提供します。たとえば、Cisco Traffic Anomaly Detector XT では、全体としてはスレッショールドを超えていない場合でも、単一のソース IP アドレスからの UDP パケットが多過ぎるといった事象を確認できます。
- Cisco Guard XT — Cisco Guard XT は、シスコの DDoS ソリューション セットの基本要素であり、高いパフォーマンスを発揮する DDoS 攻撃軽減対策デバイスです。このデバイスは、上流側の ISP データセンターまたは大規模企業の境界に設置され、ネットワークおよびデータセンターのリソースを保護します。

Cisco Traffic Anomaly Detector XT または IDS やファイアウォールのような監視デバイスによって、攻撃されていることが Cisco Guard XT に通知されると、その攻撃のターゲットとなっているデバイス宛てのトラフィックは、関連付けられた Cisco Guard XT へとルート変更されます。次に厳密な 5 段階の分析とフィルタリング処理を通して、そのトラフィックから悪意のあるトラフィックが除去され、適正なパケットのみが伝送を続けます。

Cisco Guard XT は、ルータまたはスイッチに個別のネットワーク インターフェイスにて併設されるため、他のシステム宛てのデータトラフィック フローに影響を与えずに、オンデマンドの保護機能を提供できます。設置される位置にもよりますが、Cisco Guard XT は、ルータ、Web サーバ、DNS サーバ、LAN および WAN の帯域幅など、攻撃を受ける可能性のある複数のターゲットを同時に保護できます。

### シスコシステムズの MVP アーキテクチャ

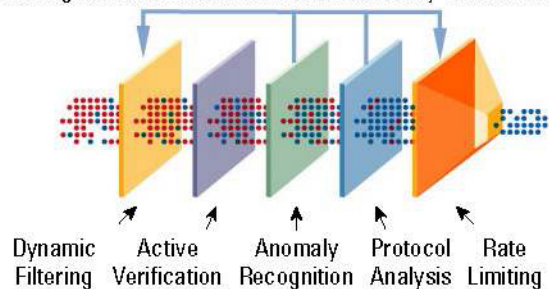
次世代の Cisco Guard XT DDoS 軽減対策ソリューションは、特許出願中である独自の Multiverification Process (MVP) アーキテクチャに基づいています。このアーキテクチャには、さまざまな検証、分析、および対抗措置の方式が組み込まれており、悪意のあるトラフィックを適正なトラフィックから識別して分離できます (図 2 を参照)。この浄化処理には、以下の 5 つのステップがあります。

- フィルタリング — このモジュールには、スタティック DDoS フィルタとダイナミック DDoS フィルタの両方が含まれています。スタティック フィルタは、必要性の低いトラフィックをブロックして、ターゲットが攻撃されないようにします。スタティック DDoS フィルタは、ユーザによる設定が必要で

すが、Cisco Guard XT の場合、デフォルト値がセットされた状態でシスコから出荷されます。ダイナミック フィルタは、トラフィック フローの観測と詳細な分析に基づき、他のモジュールによって設定が更新されます。ダイナミック フィルタはリアルタイムで更新され、疑わしいフローに適用する検証機能のレベルを引き上げたり、悪意のあることが確認された送信元やフローをブロックしたりします。

図 2 シスコシステムズの MVP アーキテクチャ

Anomaly Recognition and Active Verification Update the Dynamic Filtering and Rate Limiting Modules in Real-Time to Block Newly Identified Attack Traffic



- アクティブ検証 — このモジュールでは、システムに進入するパケットが偽造されていないことを確認します。Cisco Guard XT では、特許出願中の多数の独自の送信元認証メカニズムを使用して、偽造されたパケットがターゲットに到達することを阻止します。アクティブ検証モジュールは、適正なトラフィックを正しく識別するための複数のメカニズムを備えており、有効なパケットが廃棄されないようになっています。
- アノマリ検出 — このモジュールでは、フィルタまたはアクティブ検証モジュールを通過したすべてのトラフィックをモニタし、長期間にわたって記録された基準動作との比較を行うことにより、正常時とは異なる動作を検出します。このモジュールの基本原理は、送信元に存在する「悪玉」デーモンが生成するトラフィックのパターンと、適正な送信元が通常の動作で生成するパターンとが大きく異なるということです。この原理を利用すれば、攻撃の送信元とタイプを識別できると同時に、トラフィックをブロックしたり、疑わしいデータに対してより詳細な分析を実行したりする際の指針が得られます。
- プロトコル分析 — このモジュールでは、HTTP エラー攻撃のようなアプリケーションへの攻撃を識別するため、アノマリ識別モジュールで危険性が検出されたフローを処理します。プロトコル分析では、不完全なトランザクションやエラーを含めて、あらゆる不正なプロトコル トランザクションが検出されます。
- レート リミット — このモジュールでは、もう 1 つの対抗措置オプションを提供して、不正なフローによる大量のリソース消費を防止すると同時に、詳細なモニタリングを実行します。このモジュールでは、フローごとにトラフィック シェーピングを実行し、長期にわたって過度にリソース(帯域幅や接続など)を消費している送信元に対してペナルティを課します。

Cisco Guard XT は、攻撃と攻撃の合間には「学習」モードとなり、さまざまな保護リソースについてトラフィック パターンとフローをパッシブにモニタすることにより、正常な動作から基準プロファイルを作成していることに注目してください。この情報は、その後のリアルタイムのネットワーク活動のなかで、既知、および未知のまったく新しい攻撃を識別してフィルタリングするためのポリシー微調整に使用されます。

## シスコの DDoS 攻撃の展開

シスコの DDoS 軽減機能は、柔軟性のあるスケーラブルな展開シナリオに対応し、データセンター（サーバおよびネットワーク デバイス）、ISP リンク、およびバックボーン（ルータおよび DNS サーバ）を保護します。

### プロバイダー

サービス プロバイダーでは、ピアリング ポイントのようなプロバイダーのインフラストラクチャ内の戦略的ポイントに Cisco Guard XT を配置することで、コア ルータ、下流側のエッジ デバイス、リンク、および顧客を保護できます（図 3 を参照）。またエッジ ルータ側に配置すれば、特定の顧客を保護することもできます。検出メカニズムは、Provider Edge (PE; プロバイダー エッジ) 近くに配置することも、顧客の構内に配置することもできます。さらに上流側に展開することでネットワーク自体と複数の顧客データセンターを保護することが可能なので、プロバイダーの要件に適合します。

### 企業とデータセンター

企業のデータセンターでは、Cisco Guard XT をデータセンター内のディストリビューション層に展開することで、下流側の低速リンクとサーバを保護できます。Cisco Guard XT は、ディストリビューション スイッチに接続可能であり、冗長構成に対応しています（図 4 を参照）。

図 3 ISP 環境におけるシスコの保護ソリューション。ターゲット デバイスへ向かうトラフィックがルート変更されて Cisco Guard XT に送られ、クリーンなトラフィックはシステムに戻される。

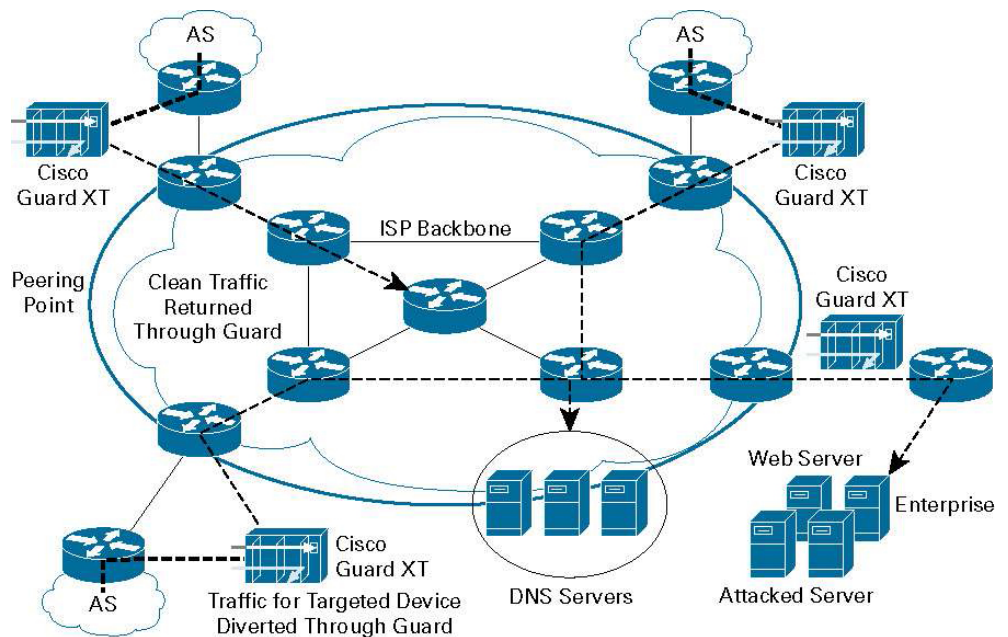
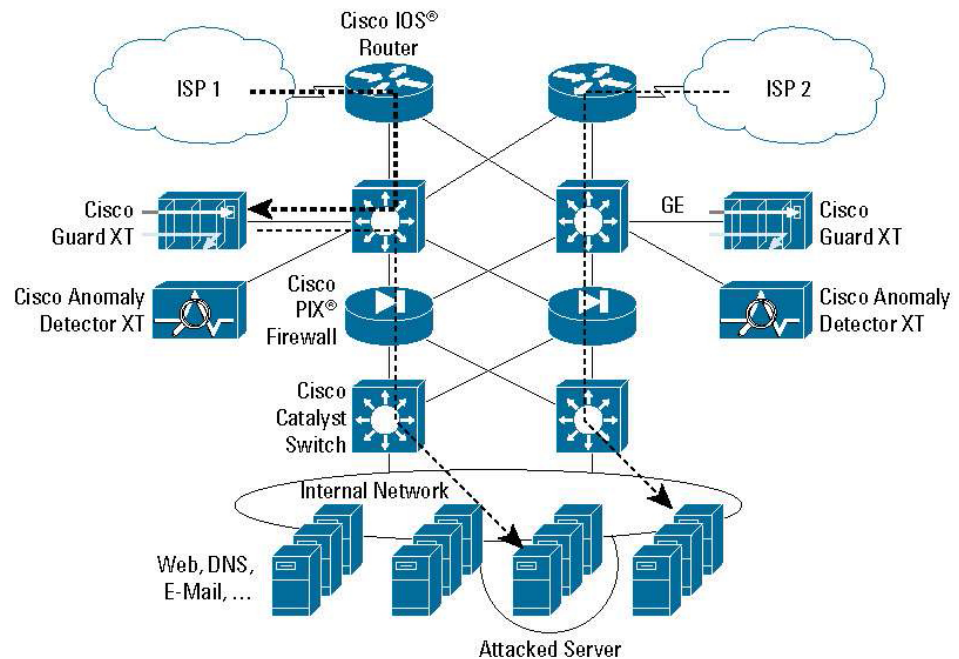


図 4 企業環境におけるシスコの保護ソリューション。ターゲット デバイスへ向かうトラフィックのみがルート変更されて Cisco Guard XT に送られ、「クリーンな」トランザクションはシステムに戻される。



## 結論

DDoS 攻撃は、今後も規模と深刻度が増大していきます。攻撃ツールがますます強力になり、誰でも簡単に入手可能になると同時に、さまざまな脆弱ポイントが存在するインターネットに依存するビジネスが増えているためです。これらの攻撃による被害コストが上昇するなか、プロバイダー、企業、政府機関、教育・研究機関では、投資、利益、およびサービスを保護するための対応を迫られます。

今後は、最も高度な DDoS 攻撃を検出するだけでなく、ますます複雑化し、検出が難しくなる攻撃トラフィックを、適正なビジネス トランザクションに影響を与えずにブロックするソリューションが必要になります。それは、ファイアウォールや IDS のような既存のセキュリティソリューションを補完する、新しいタイプのソリューションです。このアプローチには、従来のソリューションに比べて、攻撃トラフィックをより精細に検査し、分析できる機能が必要です。

シスコのテクノロジーとアーキテクチャは、トラフィックに対して現在使用できる最も詳細な検査を実施する革新的なアプローチを提供することにより、業務を停止させるという DDoS 攻撃の目的を達成させないようにします。シスコのソリューションでは、単純なフィルタリングを超えてデータの「浄化」を行い、悪意のあるトラフィックを除去するとともに適正なパケットを通過させ、ビジネスの継続性と完全性を確保します。

©2007 Cisco Systems, Inc. All rights reserved.

Cisco、Cisco Systems、およびCisco Systemsロゴは、Cisco Systems, Inc.またはその関連会社の米国およびその他の一定の国における登録商標または商標です。

本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。

「パートナー」または「partner」という用語の使用はCiscoと他社との間のパートナーシップ関係を意味するものではありません。(0701R)

この資料に記載された仕様は予告なく変更する場合があります。



#### シスコシステムズ株式会社

〒107-0052 東京都港区赤坂2-14-27 国際新赤坂ビル東館

<http://www.cisco.com/jp>

お問い合わせ先(シスコ コンタクトセンター)

<http://www.cisco.com/jp/go/contactcenter>

0120-933-122(通話料無料)、03-6670-2992(携帯電話、PHS)

電話受付時間：平日10:00～12:00、13:00～17:00

#### お問い合わせ先