

## Dos/DDoS 対策について

### 1 はじめに

DDoS(Distributed Denial of Service)という言葉が一般的に認知されたのは、1999 年後半であり、その後、2000 年 2 月頃に Yahoo, eBay, CNN, E\*Trade, ZDNet 等の有名サイトが次々とサービス不能に陥れられたことにより、DDoS の脅威が周知の事実となった。

最近では、イラク戦争中にカタールの衛星テレビ局アルジャジーラの WEB サイトや、英国のブレア首相の WEB サイトが DDoS 攻撃の標的となったとされている。

日本では、2001 年に、歴史教科書検定や小泉首相靖国神社参拝の問題により、関係機関の WEB サーバが DDoS 攻撃を利用した抗議デモを受けた。

このとき、各関係機関がとった対策は、ICMP パケットのフィルタリング、攻撃元ドメインからのアクセスの制限や WEB サーバのレスポンス向上などであったが、HP の閲覧が不能になるサイトが多かった。

この DDoS 攻撃とは、インターネットに接続されている多数のシステムを利用して、そこから攻撃先のサイトに対して大量のトラフィックを送信する攻撃である。言い換えれば、複数箇所から同時に DoS 攻撃を行う手法である。

このことから、当然 DoS 攻撃の防御対策を施す必要がある。その内容について以下に記す。

### 2 DoS 対策

ここでは、DoS 攻撃を大量のパケットを送信する Flood 攻撃タイプと、DoS のセキュリティホールを衝く脆弱性を狙った攻撃のタイプに大別して、個々の攻撃についてその防御対策を以下に記す。

#### (1) Flood 攻撃タイプの防御

このタイプの攻撃は、大量のパケットを送信することにより攻撃先のネットワークデバイスやサーバに負荷をかける攻撃であり、DDoS 攻撃でよく利用される。

##### ア SYN Flood 攻撃

SYN Flood 攻撃を受けた被害サーバは、各 SYN パケット送信元からの ACK パケットを一定期間（タイムアウトになるまで）待ち続けることにより、メモリが消費されたままになる。送信元アドレスは、詐称される場合が多い。対策手法は以下のようなものがある。

#### 【サーバ】

- ベンダからパッチが提供されていれば適用する
- 3way ハンドシェイク時のタイムアウトを短くする
- SYN Flood を防御できる機能を持つ OS を導入する。又はその機能を有効にする。

Linux: Syn Cookie, RST Cookie

Windows: SynAttackProtect 機能

Solaris: SYN Flood の防御機能を持ったカーネルを実装

【F/W】

- SYN Flood に対するプロテクト機能を持った F/W であれば、その機能を有効にする (Fw1 : SYNDefender、NetScreen : SYN Flood Protection 等)
- 3way ハンドシェイク時のタイムアウトを短くする

【ルータ】

- Syn パケットの帯域制限

#### イ UDP Flood 攻撃

コネクションレス型の UDP の特徴を利用するもので、いきなり非常に大きなサイズの UDP パケットを大量に送りつける攻撃である。逆に、極端に短いパケット長のデータを大量に送りつけることにより、ネットワークデバイス（特に F/W）に負荷を掛けることができる。対策手法は以下のとおり。

【サーバ】

- ベンダから提供されていれば、パッチを適用する
- 該当サービスの停止

【F/W】

- 該当ポートの拒否

【ルータ】

- 該当ポートのアクセス拒否又は、帯域制限

#### ウ Ping Flood 攻撃

UDP Flood 同様、ICMP の特徴を利用するもので、大きな ICMP パケット(ICMP P echo request)を大量に送りつける攻撃である。対策手法は以下のとおり。

【サーバ】

- ベンダから提供されていれば、パッチを適用する
- ICMP echo request に応答しないよう設定

【F/W】

- ICMP の拒否(タイプ、コード別に行ってもよい)

【ルータ】

- ICMP の拒否(タイプ、コード別に行ってもよい)又は、帯域制限

#### エ Smurf 攻撃

Smurf 攻撃は、送信元アドレスに攻撃先アドレスをセットした ICMP Echo Request をあるブロードキャストドメイン宛に送信することにより、そのドメイン全体から詐称されたアドレスに大量の ICMP Echo Reply が送られ、帯域を食いつぶす。対策手法は以下のとおり。しかし、router の外側の回線でトラフィックを抑えることはできず、抜本的な解決策はない。

- ルータで ICMP の拒否又は、帯域制限
- ルータでブロードキャストアドレス宛およびネットワークアドレス宛パケットの拒否 (踏み台防止)

#### オ fraggle 攻撃

Smurf の変種で、ICMP の代わりに UDP を使用する。echo、Chargen、daytime、qotd の各ポートが応答のトリガとして利用される。対策手法は以下のとおり。

- ルータで該当ポートの拒否又は、帯域制限
- ルータでブロードキャストアドレス宛およびネットワークアドレス宛パケットの拒否 (踏み台防止)
- サーバで該当ポートを閉じる

#### カ Connection Flood 攻撃

長い時間オープン状態を続けるコネクションを繰り返し行うことにより、ソケットを占拠する攻撃で、コネクション数に制限がない場合、サーバがクラッシュする可能性がある。これは、UNIX プロセス・テーブル攻撃とも呼ばれる。TCP コネクションを確立するため、送信元の詐称は難しい。対策手法は以下のとおり。

##### 【サーバ】

- リソースが許される範囲内で、ソケットオープン数を増やす
- リソースが許される範囲内で、TCP のキューの割り当てを増やす
- デーモンの timeout の値を短く設定する

##### 【F/W・ルータ】

- 攻撃元アドレスからのアクセスの制限

##### 【その他】

- 負荷分散装置の導入  
(アイドル接続時間超過や多数同時コネクションの拒否の機能)

#### キ リロード攻撃

WEB ページに大量のアクセスを行う攻撃で、WEB ブラウザで F5 キーを連続して押下することにより攻撃ができることから、F5 攻撃とも呼ばれている。Connection Flood 攻撃と同様、送信元の詐称は難しい。対策手法は以下のとおり。

##### 【サーバ】

- 標的となるページの容量を減らす。
- KeepAlive を有効にする

##### 【F/W・ルータ】

- 攻撃元アドレスからのアクセスの制限

##### 【その他】

- 負荷分散装置の導入  
(多数同時コネクションの拒否の機能)

### (2) 脆弱性を狙った攻撃の防御

このタイプの攻撃は、メモリリソースを消費するもの、プロトコルスタックのセキュリティホールに対して攻撃を行うものなど、DoS の脆弱性を狙ったものであるが、多量のパケットを送信するものではないため、DDoS 攻撃に使われることは考えにくい。

#### ア Ping of Death 攻撃

Ping of Death は IP 実装に関するバグを衝く攻撃で、RFC で定義された ICMP Echo パケットの最大サイズ(65536 バイト)より大きいサイズを送信する。このバグを抱えているホストは攻撃を受けるとフリーズする可能性がある。対策手法は以下

のとおり。

- ベンダから提供されているパッチを適用する
- ネットワークデバイスで ICMP の拒否

#### イ Teardrop 攻撃

Teardrop 攻撃は、TCP/IP の IP フラグメンテーションを再構築するコードの実装によっては、重複 IP フラグメントを正しく処理しないという弱点を衝く攻撃で、このバグを抱えているホストは攻撃を受けるとフリーズする可能性がある。対策手法は以下のとおり。

- ベンダから提供されているパッチを適用する

#### ウ Land 攻撃

Land 攻撃は、発信元の IP アドレスとポート番号を送信先のものと同じものに詐称した SYN パケットを送りつける。このバグを抱えているホストは攻撃を受けるとフリーズする可能性がある。対策手法は以下のとおり。

- ベンダから提供されているパッチを適用する
- ネットワークデバイスでソースアドレスが詐称されているパケットの拒否

### 3 DDoS 攻撃への対策

DDoS 攻撃は、攻撃者が標的に対して直接攻撃を行うのではなく、別の踏み台となるコンピュータから攻撃を行う。この踏み台は、非常に多数のコンピュータで構成される。DDoS 攻撃を受けた時の直接的な被害は、以下のようなものがある。

- 帯域の圧迫
- ルータや F/W の処理能力の低下
- ターゲットサーバの処理能力低下
- F/W やサーバのディスク資源の大量消費（膨大なログが発生）

現状では、DDoS 攻撃に対して根本的な防御手段はまだない。攻撃元のコンピュータ（エージェント）が不特定多数であり、送信アドレスを詐称することが多いため、追跡を行い攻撃元のコンピュータでエージェントを停止することも困難である。

DDoS 攻撃時に送信するプロトコルは、ICMP, UDP, TCP が利用される。有名な DDoS ツールが使用する攻撃は下表のとおり。

TFN (Tribe Flood Network)	ICMP flood( echo reply) SYN flood UDP Flood smurf
TFN2K (TFN2000)	ICMP flood( echo reply) SYN flood UDP Flood smurf MIX attack (Sen UDP, SYN and ICMP packets) ARGA3 attack (IP base の Random 形式)
Trinoo(Trin00)	UDP Flood

stacheldraht(barbed wire)	ICMP flood SYN flood UDP Flood Smurf
mstream	TCP ACK flood (stream attack)
trinity V3	udpflood fragmentflood synflood rstflood randomflagsflood ackflood establishflood nullflood
stacheldht1.666	NULL flood stream attack flood "HAVOC" flood (ICMP, UDP, SYN, TCP random flags and IP headers を送る) IRC flood
shaft	ICMP flood TCP SYN flood UDP Flood Randomize all three attacks

これらのツールが、全て Flood 系の DoS 攻撃を利用していることから、DoS 攻撃の対策（前項のとおり）を実施することが重要である。

通常のネットワークであれば、DNS で利用される UDP の 53 番ポート以外は必要ないので、ネットワークデバイスでフィルタリングや帯域制限を実施することにより、攻撃力を低下させることができる。

また、各機器においてパフォーマンス向上のチューニングを実施することにより、防御効果が期待できる。DDoS 攻撃に対する主な防御対策は以下のとおり。

- ソースアドレスが詐称されたパケットやブロードキャスト宛パケットを拒否する(RFC1918, RFC2827, RFC2644)
- 不必要な ICMP パケット、UDP パケットや SYN パケットの拒否又は、帯域制限を行う
- ブロードキャスト宛パケットのフォアディングの禁止
- 回線・ネットワークデバイス・サーバの負荷分散機能を含めたシステムの再構成を行う
- サーバ・ネットワークデバイスの処理能力を増強する
- 各種デーモンのチューニングを施すことによりレスポンスを改善する
- 踏み台にされないよう（エージェントを埋め込まれないよう）にコンピュータの脆弱性を解消する

## (1) ルータにおける対策

一般的に利用されている CISCO 社製のルータ (IOS) における対策を主に記す。

### ア トラフィックを制限

- 外部からの不必要な ICMP や UDP トラフィックを拒否する。
- 公開サービスへの UDP Flood 攻撃 (例えば、DNS Flood) に対しては該当ポートに割り当てる帯域幅を制限する。(rate-limit)
- SYN Flood 攻撃に対しては SYN パケットの転送レートを制限する。(rate-limit)
- 特定の場所からの大量なアクセス攻撃 (リロード攻撃、Connection Flood 攻撃) に対しては、ルータでアクセス元別に拒否する。

### イ IP スプーフィング防止

- パケットが到着したインターフェースから送信元アドレスへの経路が CEF テーブルに存在しない場合、拒否する。(Unicast RPF)
- 送信元アドレスにプライベートアドレス (RFC1918 で規定されているアドレス 10/8, 172.16/12, 192.168/16) や特定のアドレス (127.0.0.0/8, 169.254.0.0/16, 192.0.2.0/24, 0.0.0.0/8, 224.0.0.0/4) が設定された内向きのパケットを拒否する。
- 送信元アドレスに自ドメインのアドレスが設定された内向きのパケット、又は、送信元アドレスに外部のアドレスが設定された外向きのパケットを拒否する。

### ウ その他

- DoS に対する脆弱性を有しているならば対処する。
- ネットワーク機器の処理能力を増強する。
- ルータが攻撃対象とならないように不要なサービスを停止する。

## (2) F/W における対策

一般的に利用されている CheckPoint 社製の FireWall1 における対策を記す。但し、他の F/W でも同様のことが言える。

### ア 設定のカスタマイズ

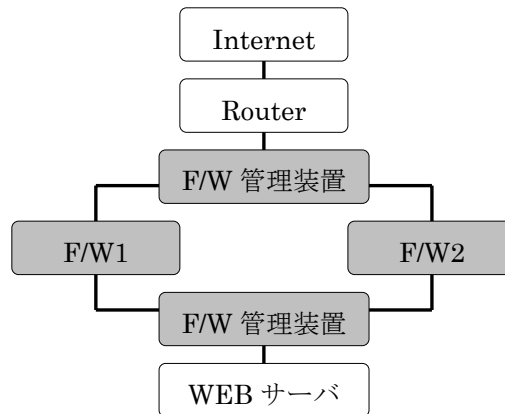
- ログの記録量を減らす。
  - Account ログを使用しない。
  - NBT packet のログは取らない。
- ルールの作成において F/W に負荷が掛からないようにする。
  - 頻繁に使用されるルールをルールベースの上のほうに作成する。(どのルール (クリーンアップ・ログ以外) のログが一番多いかをログで、確認するとよい)
  - ルール内では、できる限りワークステーション・オブジェクトではなく、ネットワーク・オブジェクトを使用する。
  - 同じセキュリティ・ポリシーを持つサブネット群は一つのネットワークとして定義する。
  - グループを使用して、ルールの数を減らす。
  - ドメイン・オブジェクトを使用しない。使用する場合は、ルールベースの下のほうにおく。
  - アドレス変換ルール内で、アドレス範囲オブジェクトの代わりにネットワーク・オブジェクトを使用する。
- SYN Defender 機能を有効にする。(SYN Flood 対策)
- 各種タイムアウト値を見直す。

#### イ 構成の見直し

##### □ F/W の 2 重化 (並列構成)

F/W を直列に接続した場合、2 台の内 1 台でもパフォーマンスの低下が発生すると、もう一台の F/W が正常であっても全体としてのパフォーマンスは低下してしまう。一つの手法としては、以図のように 2 台以上の F/W で平行して負荷を分散処理し、サービス停止のリスクを減少させる方法がある。

Ex)



- F/W 機器の処理能力を増強する。アプライアンス製品は、専用にチューニングされたカーネルやハードを使用しており、ハイパフォーマンスが期待できる。

#### (3)サーバにおける対策

##### ア 設定のカスタマイズ

- そのサーバに必要なサービス関連以外のポートは塞ぐ。
- 各種デーモンでロギングの際にリクエスト元の名前解決を行うことを禁止する。
- 3way handshake 時の timeout を短くする。(SYN Flood 対策)
- ハーフコネクション要求を受け付けるキューを大きくする。(SYN Flood 対策)
- 攻撃対象の該当デーモンの Time Out を短くする。(リロード攻撃、Connection Flood 攻撃)
- コネクション要求を受け付けるキューを大きくする。(リロード攻撃、Connection Flood 対策)
- SYN Flood 攻撃に対するプロテクション機能を有する OS を導入する。又は、機能を有効にする。

##### イ 構成の見直し

- サーバ処理能力を増強する。
- WEB サーバの負荷分散を行うなど、ネットワーク構成を再考する。

#### (4)その他

- 回線の増強を図る。
- 平素からトラフィックを把握する。  
諸対策を実施するためには現状把握が重要である。平素からトラフィックの統計情報を収集するなどして自サイトのネットワークについて把握しておく。
- サイト間連携  
サーバが高負荷状態になった時、一時的に別のサイトのサーバにリクエストを転

送する「サイト間連携」機能を持った機器を導入する。若しくは ISP で提供されている、この様なサービスを受ける。サイト間連携機能を使用することで、サイトのサーバが利用者のリクエストを処理できなくなっても、別のサイトでサービスを継続して受けることができるため、非常に信頼性の高いシステムを構築することができる。

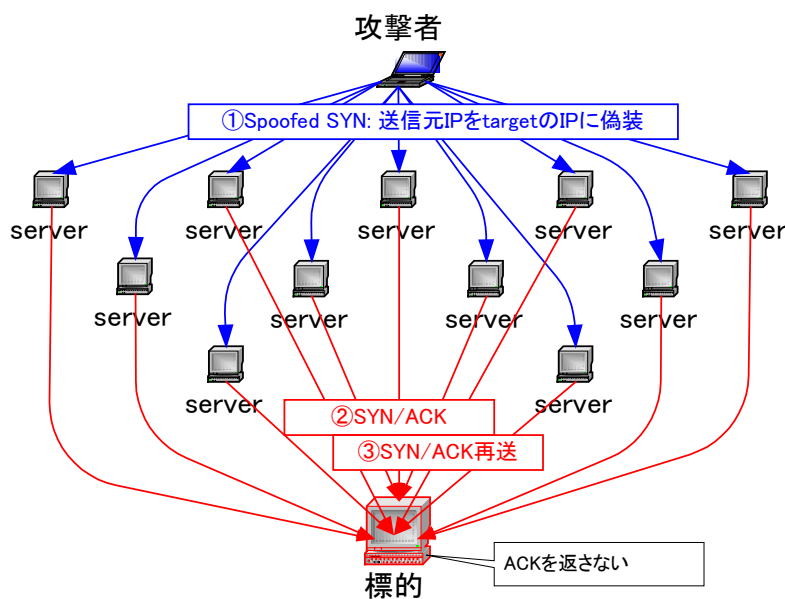
- 攻撃してきたエージェントにマスターを装い、攻撃停止命令を行うソフトウェアなども開発されている。場合によっては、この様なツールを利用する。

**ZombieZapper**： 攻撃してきたエージェントにマスターを装い、攻撃停止命令を行うツール。また、すでにアタックツール（マスター・スレーブ）が埋め込まれている場合は、それを除去せずその機能を停止させる。再度攻撃命令があれば、攻撃元の追跡が可能になる。Trinoo, TFN, Stacheldraht.に対応している。

[http://razor.bindview.com/tools/ZombieZapper\\_form.shtml](http://razor.bindview.com/tools/ZombieZapper_form.shtml)

#### 4 最近の DDoS 攻撃

従来の DDoS 攻撃では、エージェントを埋め込むためにそのコンピュータに侵入する必要があり、そのエージェントを多数用意することにより攻撃力を持った DDoS ネットワークとなっていたが、最近では、ワームによりエージェントを自動的に作るようになってきた。また、エージェントに侵入せずに、インターネット上に繋がっているコンピュータを利用して標的マシンにパケットを集中させる DrDoS(Distributed Reflection DoS)攻撃が出現している。(下図参照)



DrDoS 攻撃の攻撃手法は、以下のとおり。

- ① 攻撃者が SYN パケットの送信元アドレスに標的マシンのアドレスをセットして、インターネット上に繋がっている多数のコンピュータ(Reflector)に送信を行う。
- ② このコンピュータ(Reflector)は、SYN/ACK パケットを標的マシンに送信するが、標的マシンは、実際に SYN パケットを送信していないため、ACK を送信しない。
- ③ Reflector は、ACK パケットの返信がないため、SYN/ACK パケットを再送する
- ④ 標的サイトは多数の Reflector から SYN/ACK Flood 攻撃を受ける。

ほとんどのインターネットに接続されている機器を Reflector として利用できるため、今後脅威となり得る攻撃である。

DDoS 攻撃の手法は時間と共に洗練化され、膨大なトラフィックを送りつけることが容易にできるようになってきている。

## 5 参考資料

- 📖 Solaris Operating Environment Network Settings for Security - Updated for Solaris 8 Operating Environment  
<http://www.sun.com/blueprints/1200/network-updt1.pdf>
- 📖 Strategies to Protect Against Distributed Denial of Service (DDoS) Attacks  
<http://www.cisco.com/warp/public/707/newsflash.pdf>
- 📖 DrDoS  
<http://grc.com/dos/drDOS.htm>
- 📖 distributed attack tools  
<http://packetstormsecurity.nl/distributed/>
- 📖 ネットワーク上の攻撃に対するセキュリティの考察  
<http://www.microsoft.com/japan/technet/treeview/default.asp?url=/japan/technet/security/prodtech/windows/iis/dosrv.asp>
- 📖 不正アクセスの手法と防御 (ソフトバンク)
- 📖 詳解 TCP/IP Vol.1 プロトコル (ピアソン・エデュケーション)

(平成 16 年 3 月 24 日 一部改訂)