3.2 DoS/DDoS 攻撃対策（2）～高度化する DDoS 攻撃と対策 サイトの視点から～

倉上　弘（NTT セキュアプラットフォーム研究所）

サイトと DDoS 攻撃

DDoS（Distributed Denial of Service）攻撃は，複数の攻撃元からの大量通信により，インターネットサービスプロバイダ（以降，ISP）とのアクセス回線を輻輳させたり，サイトのサーバリソースを消費させたりする．それにより，Web サーバ等を収容するサイトの正常なサービス提供を不能にする．Web サーバの脆弱性を対象とした攻撃にはサイト側での対策が有効だが，DDoS 攻撃は ISP とのアクセス回線をも使用不能にすることがある．そのため，サイト側での対策だけでなく ISP が提供する DDoS 攻撃対策サービスが必要になる場合がある．DDoS 攻撃対策は，サイト側と ISP の DDoS 攻撃対策サービス利用の 2 つの視点で検討しておくことで，迅速かつ効果的に実施できると言える．

本稿では，高度化している DDoS 攻撃方法を示した上で，サイト側の対策と ISP 側の対策について紹介する．

アプリケーションレイヤ型に移行する DDoS 攻撃

DDoS 攻撃は，複数の攻撃元から大量の通信を発生させて攻撃対象サイトまたは回線に負荷を与え，サービス不能にさせる．DDoS 攻撃をパケット数や帯域に着目して分類すると，回線帯域の使用率を高める攻撃とサイトの負荷を高める攻撃に大別できる．

■ 回線帯域の使用率を高める攻撃

回線帯域の使用率を高める攻撃は，長いパケットを大量に送りつけ，サイトのアクセス回線を埋める攻撃で，サイトの正常な通信との判別が難しいパケット種別が使われることが多い（図 -1）．この攻撃の場合，サイト側だけでは対処できないことがある．このため，ISP が提供する DDoS 対策サービスの事前導入など，あらかじめアクセス回線を保護する施策を検討しておくことが望ましい．

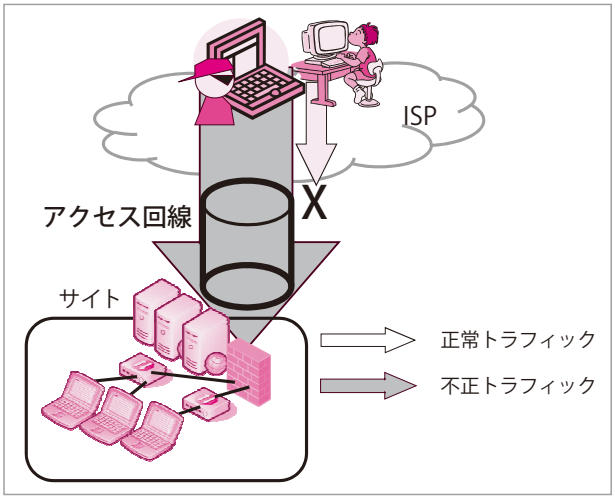

図 -1　回線帯域の使用率を高める攻撃

■ サイトの負荷を高める攻撃

サイトの負荷を高める攻撃は，プロトコルやサーバの実装を踏まえた上で，短いパケットを大量に送りつけることが多い．以前は TCP SYN Flood，IP Fragment 攻撃などのネットワーク／トランスポートレイヤ（以降，ネットワークレイヤ型）の攻撃が主であったが，最近は HTTP Get Flood 攻撃などのアプリケーション／セッションレイヤ（以降，アプリケーションレイヤ型）の攻撃に移行してきている（表 -1）．

回線帯域に余裕がある状態でサイトの負荷を高める攻撃が発生した場合には，ISP 側あるいはサイト側での対処が可能である．TCP SYN Flood 攻撃等のトランスポートレイヤ型の攻撃であれば，後述する SYN

レイヤ	攻撃手法
アプリケーション／セッション	HTTP GET Flood, HTTP POST Flood, Slow Read, Slowloris, Slow POST
トランスポート／ネットワーク	IP Fragment, TCP SYN Flood, ICMP Flood, UDP Flood, DNS Amp, Targa Flood, Wonk Flood

*）DNS Amp は回線帯域の使用率を高めるという点からトランスポート／ネットワークに分類している.

表 -1　DoS 攻撃のレイヤ分類

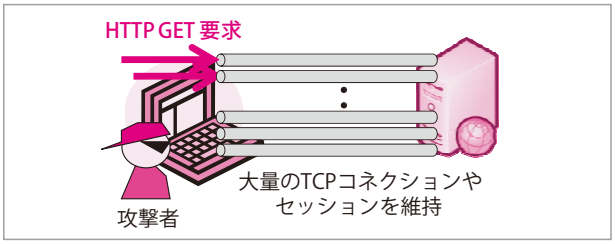

図 -2　サイトの負荷を高める攻撃

Cookies や IPS（Intrusion Prevention System）等での対策も可能である．ただし，大量の短いパケットや大量のセッションを張られる攻撃を受けた場合（図 -2），IPS が攻撃パケットを処理しきれなくなり回線全断になることがあるため，サイト側だけで処理しきれない場合を想定した対応策を検討しておきたい.

攻撃者に着目した攻撃方法の分類としては，人海戦術での攻撃，図 -3 に示すボットネットを用いた攻撃に大別できる．人海戦術での攻撃は，主に社会情勢に応じて社会的・政治的な主張のもと発生している．単純な F5 キーの連打による攻撃，TCP Connection Flood などのトランスポートレイヤ型の攻撃ツールや HTTP GET Flood などのアプリケーションレイヤ型の攻撃ツールを利用した手法が知られている[1]．一方，ボットネットを用いた攻撃方法はバリエーションが多く，攻撃方法も進化し続けている.

ボットネットによる DDoS 攻撃の変化

2002 年から 2003 年にかけて広まったボットに実装されている DoS（Denial of Service）攻撃手法を表 -2 に示す.

GTBot（Global Threat Bot）や SDBot には ICMP Flood や TCP SYN Flood 攻撃などのネットワークレイヤ型の DoS 攻撃手法は実装されているが，アプリケーションレイヤ型の攻撃手法は実装されていない．一

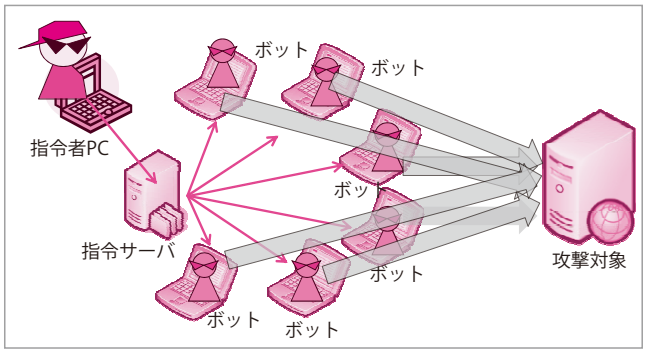

図 -3　ボットネットによる攻撃イメージ

ボットの種別	ボットに実装されている攻撃手法
GTBot（1998 年～）	ICMP Flood
SDBot（2003 年～）	TCP SYN Flood, UDP Flood, ICMP Flood
Agobot（2002 年～）	TCP SYN Flood, UDP Flood, ICMP Flood, Targa Flood (Random IP Protocol), Wonk Flood (SYN + 1023 ACK Packets), HTTP GET Flood

表 -2　ボットと DoS 攻撃手法

方，Agobot には Targa Flood や Wonk Flood 攻撃のようなネットワークレイヤ型だけでなく，HTTP GET Flood 攻撃のようなアプリケーションレイヤ型の DoS 攻撃手法が実装されている．Agobot は 2002 年 10 月に検出されたマルウェアだが，ボット生成キットやマニュアルが用意され，誰でも容易にマルウェアを生成できることから，600 を超える亜種の存在が確認されている．さらに，Agobot 以降，マルウェアを用いたビジネスが進み，ボットに実装される DoS 攻撃手法も高度化されてきている.

2012 年現在，攻撃活動にボットネットを用いることのできる DDoS 攻撃ツールキットとして，Dirt Jumper がある．Dirt Jumper は 2009 年に公開され，その当時は Russkill という名称で呼ばれていた．Dirt Jumper version 5 およびキットは約 800USD で売買され，HTTP GET Flood，HTTP POST Flood，Synchronous Flood，Downloading Flood などの DoS 攻撃手法が実装されていると報告されている[2]．このうち，Synchronous Flood 攻撃は，HTTP GET Flood 攻撃の一種で，同時に複数の TCP コネクションを設定する手法である．Downloading Flood 攻撃も HTTP GET Flood 攻撃の一種であるが，複数のファイルダウンロード要求を送信することで，攻撃対象のサイトや回

線帯域を消費させる．2002 年から 2012 年の約 10 年間の間に，ボットに実装されている DoS 攻撃手法も多様化していることが分かる．

このような攻撃手法の多様化に対処するため，IPS や Web アプリケーションファイアウォール（以降，WAF）では，発信元 IP アドレスごとかつ HTTP 要求のメソッドごとに IP パケットを分析して攻撃判定する機能が実装されるようになってきている．

高度化したアプリケーションレイヤ型の DoS 攻撃

DoS 攻撃手法は，ネットワークレイヤ型からアプリケーションレイヤ型に移ってきただけではなく，HTTP の仕様を踏まえた Web サーバ向けの DoS 攻撃手法へと高度化している．ここで紹介する Slow Read DoS，Slowloris，Slow POST DoS と呼ばれている攻撃は，Web サーバに特化した DoS 攻撃手法で，検出しにくい DoS 攻撃となるような工夫がされている．これらの攻撃手法の特徴は，時間をかけて少しずつデータ転送することで，リソースを消費したり負荷をかけたりするものである．

■ Slow Read DoS 攻撃

Web サーバに対して TCP プロトコルのウィンドウサイズを小さく通知し，HTTP 応答データを少しずつ送信させるよう制御することで時間をかけさせるという手法である．これにより，Web サーバ上のプロセス占有時間が長くなり，無駄なリソース消費が発生することになる．さらに，攻撃者は Web サーバの最大同時接続数（MaxClient 数）まで接続することで，Web サーバがほかの新しい接続を受け入れることができない状態を作り出す．

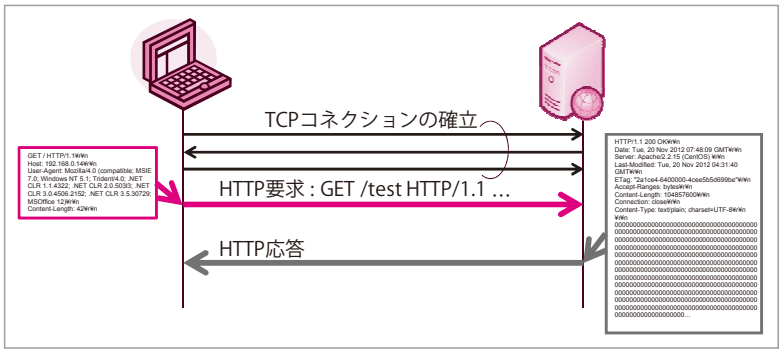

図 -4　通常の HTTP アクセス

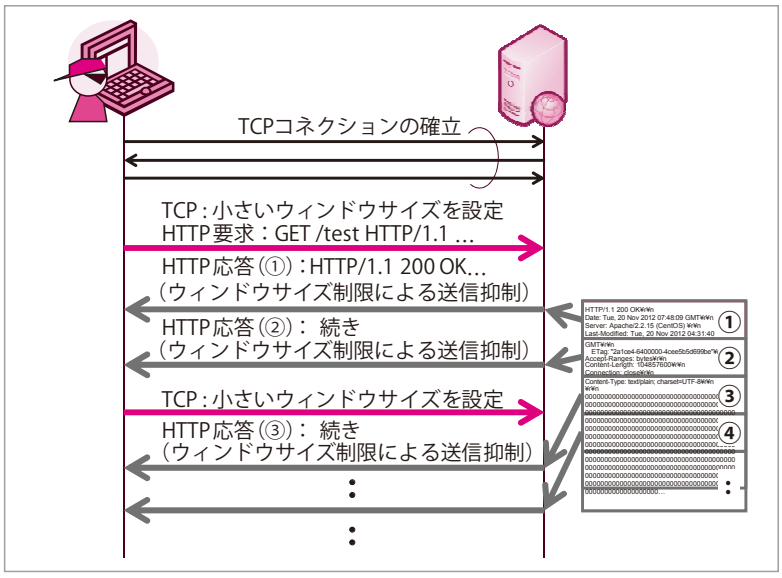

図 -5　Slow Read DoS 攻撃による HTTP アクセス

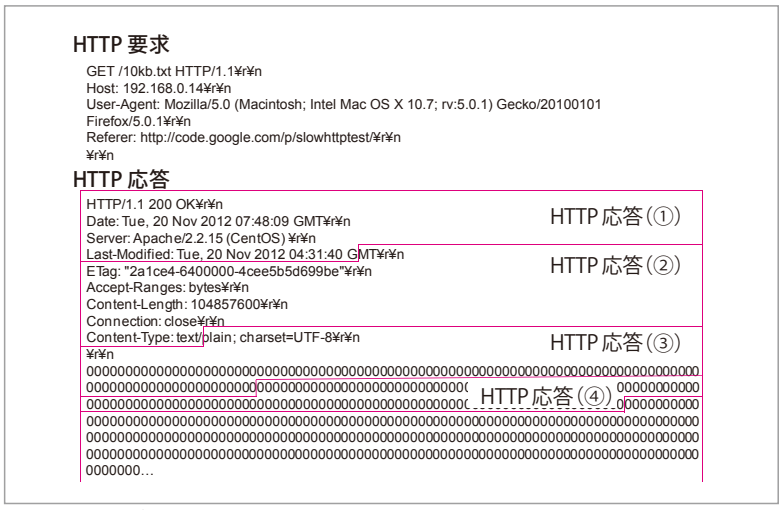

図 -6　HTTP データから見た Slow Read DoS 攻撃

図 -4 に通常の HTTP アクセスの流れを示す．これに対して，Slow Read DoS 攻撃による HTTP アクセスの流れを図 -5 に示す．Slow Read DoS 攻撃の場合，HTTP 応答が分割されながら少しずつ送信されていることが分かる（図 -6）．

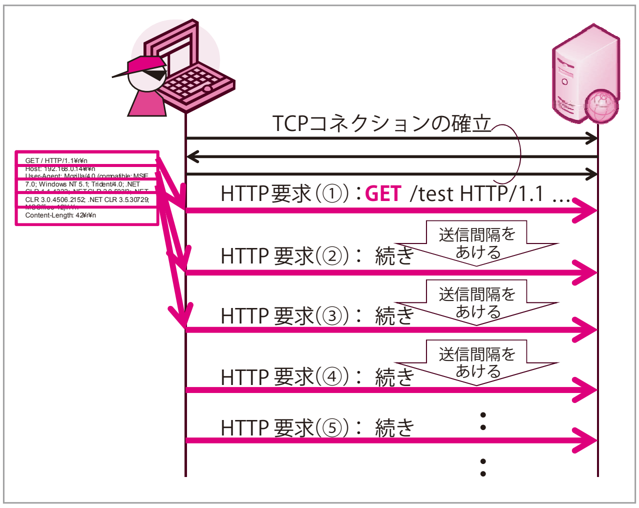

図 -7　Slowloris 攻撃による HTTP アクセス

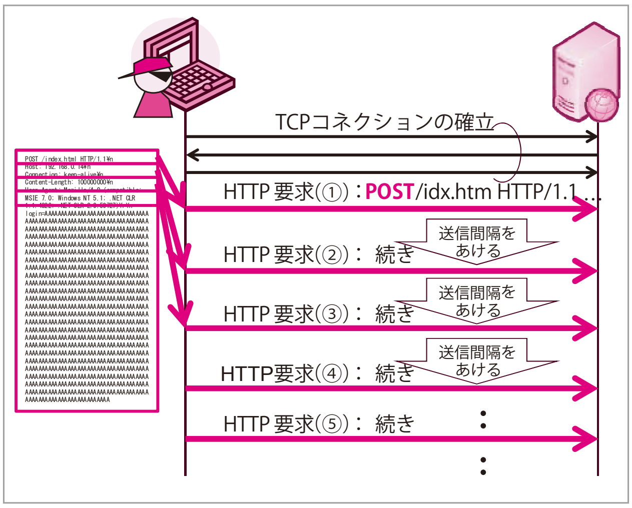

図 -9　Slow POST DoS 攻撃による HTTP アクセス

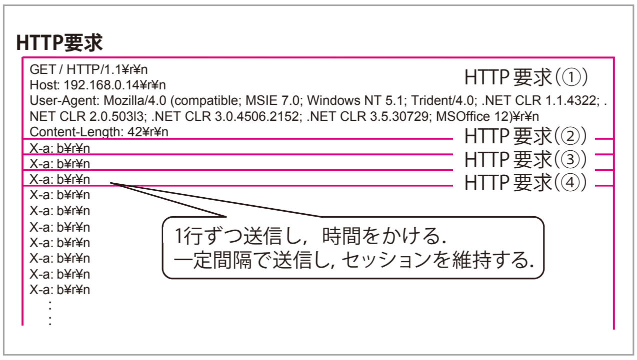

図 -8　HTTP データから見た Slowloris 攻撃

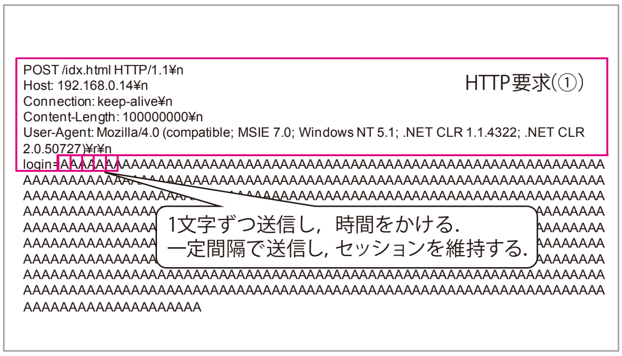

図 -10　HTTP データから見た Slow POST DoS 攻撃

■ Slowloris 攻撃

Apache Web サーバに対する攻撃手法で，HTTP GET 要求を少しずつ送信し時間をかけることで，Web サーバのプロセス占有時間を長くし，サーバに無駄なリソース消費を発生させる．Slowloris 攻撃の場合，HTTP GET 要求が分割されながら送信されていることが分かる（図 -7，図 -8）．

■ Slow POST DoS 攻撃

HTTP POST 要求を少しずつ送信することで時間をかけさせる手法である（図 -9，図 -10）．これにより，Web サーバ上のプロセスの占有時間を長くして無駄なリソース消費を発生させる．

Slow Read DoS，Slowloris，Slow POST DoS 攻撃のいずれも，少ないパケット数で Web サーバのリソースを消費させ，サービス不能にするものである．これらの攻撃コードは公開されていることから，ボットに組み込まれ DDoS 攻撃に使用される可能性も想定しておきたい．

DDoS 攻撃対策

ここまで，DDoS 攻撃がネットワークレイヤ型からアプリケーションレイヤ型の DoS 攻撃へ，さらに，アプリケーションレイヤ型の DoS 攻撃から Web サーバに特化した DoS 攻撃へと変遷していることを紹介してきた．ここからは，これら DDoS 攻撃の対策方法を概観する．

■ サイトでの対策

サイト側で対策可能な DDoS 攻撃は，アクセス回線の帯域使用率を高める攻撃以外で，サイトに設置した IPS，負荷分散装置，WAF などの機器性能を超えない範囲の攻撃となる．ここでは，IPS，負荷分散装置，WAF，Web サーバ，リソース分散による DDoS 攻撃

対策を示す.

IPS

IPS には TCP SYN Flood 攻撃などの DoS 攻撃手法を検出し廃棄する機能を持つ製品がある．使用している IPS が検出可能な攻撃で，パケット数やセッション数等で機器性能内であれば，IPS で不正パケットを廃棄することでサービスの継続が可能となる.

負荷分散装置

トラフィックを負荷分散させることで，不正パケットに対するサーバ負荷を分散し，サービスを継続させる．負荷分散装置の性能にもよるが，規模の大きな攻撃にも対処可能である.

WAF

WAF は，Web アプリケーションの脆弱性を悪用した攻撃から Web アプリケーションを保護するセキュリティ機構である．Web サーバに特化した DoS 攻撃も出現していることから，TCP SYN Flood 攻撃から，Slow Read DoS，Slowloris，Slow POST DoS 攻撃のような Web サーバのプロセスにかかわるリソースを占有する攻撃に対策可能な製品が存在する.

Web サーバ

TCP SYN Flood 攻撃の対策としては，SYN Cookies を有効にして攻撃パケットによるメモリ消費を防ぐ方法が挙げられる.

アプリケーションレイヤ型の DoS 攻撃に対しては，mod_security や mod_reqtimeout などが利用できる [3), 4)]．mod_security のような Web サーバ上で動作する WAF を導入することで同時接続数を制限でき，一部の Slow Read DoS 攻撃には有効となる．ただし，mod_security の動作によるサーバ性能への影響を考慮した上で導入を判断する必要がある.

mod_reqtimeout は Apache のモジュールで，HTTP ヘッダやメッセージボディの受信に対するタイムアウト時間を設定する．これにより，HTTP ヘッダやメッセージボディをゆっくり送信する Slowloris や Slow POST DoS 攻撃によるプロセス処理をタイムアウトさせ，攻撃を中断できる.

CDN (Content Delivery Network)

CDN は，コンテンツを配信するために最適化されたネットワークのことで，多くの場合，このような機能を提供するサービスの総称となっている．Web サーバのコンテンツをインターネット上の複数のキャッシュサーバにキャッシュし，さらに，ユーザからのアクセスをネットワーク上に分散させる (図 -11)．攻撃トラフィックも同様にインターネット上のキャッシュサーバに分散されることになる.

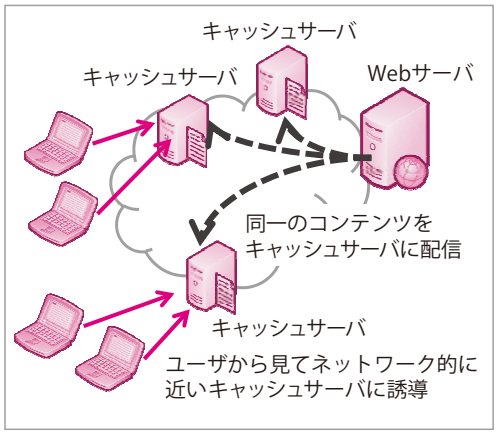

図 -11
CDN によるトラフィック分散

IP Anycast

IP Anycast は，IP アドレスを特定のサービスに対して割り当てるための技術で，この技術を利用することにより，複数サーバで同一 IP アドレスを利用できる．また，IP Anycast は経路制御技術との組合せにより実現され，同一 IP アドレスを持つ複数サーバの中から，ユーザから見てネットワーク的に近いサーバに誘導できる (図 -12)．このため，広域に分散しているサイトであれば，IP Anycast を用いて最も近いサイトにトラフィックを誘導することにより，DDoS 攻撃の負荷を分散可能である．ただし，利用上の制約があることから，主に DNS サーバでの導入が進められている [5)].

■ ISP での対策

回線帯域の使用率を高める攻撃やアクセス回線に設置した IPS 等の機器性能を超える攻撃に対しては，サイト側だけでは対策が難しい．この場合，ISP が提供する次のような DDoS 対策サービスにあらかじめ加入するなどを検討しておきたい.

DDoS 攻撃の軽減

事前に DDoS 攻撃の軽減内容を決定しておき，軽減内容に沿って，ISP のルータ・ファイアウォールでのアクセス制御 (図 -13) や，ISP が独自に導入している

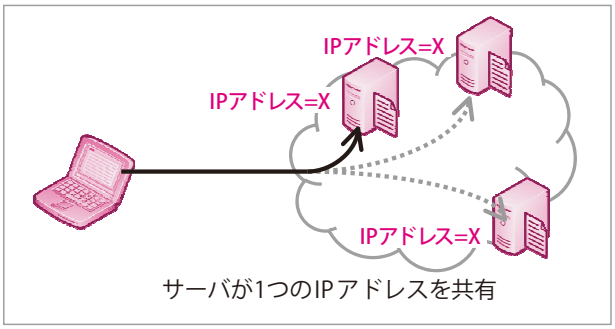

図 -12　IP Anycast によるトラフィック誘導

DDoS 対策装置において検知ならびに軽減を実施する．軽減内容としては，攻撃発生時には該当する Web サーバへの通信をいったんすべてストップさせる，攻撃パケットのみを破棄する，特定の発信元アドレスに対して帯域制御するなどがある．

DDoS 攻撃の可視化

トラフィックを解析し，ポータルサイト等でユーザが DDoS 攻撃の状況を確認したり，期間等の条件設定を行ってレポートを表示できるサービスがある．

DDoS 攻撃の監視

設定した閾値を超えるトラフィックが発生した場合に検知メールを送信する簡易のものから，マネージドセキュリティサービスのように，DDoS 攻撃対策サービスを包含したアウトソーシングなどもある．

サイト視点での DDoS 対策

DDoS 攻撃による被害を最小限にするためには，DDoS 攻撃の状況を迅速かつ正確に把握する必要がある．サイト側では，次のような項目を常時監視することで，DDoS 攻撃の発生や状況を把握できるであろう．

1) サイトに出入りするトラフィック量（pps/bps）
　可能であれば送信先 IP アドレスごとに量変動を監視する．
2) HTTP/HTTPS の応答時間
3) Web サーバごとの CPU/ メモリ使用量

2)，3) で設定した閾値を超えるなどの異常値を検出したときに，1) のトラフィック量から DDoS 攻撃の可能性を判断できる．ISP が提供する DDoS 対策サービスの攻撃検出通知に頼るだけではなく，Web サーバ

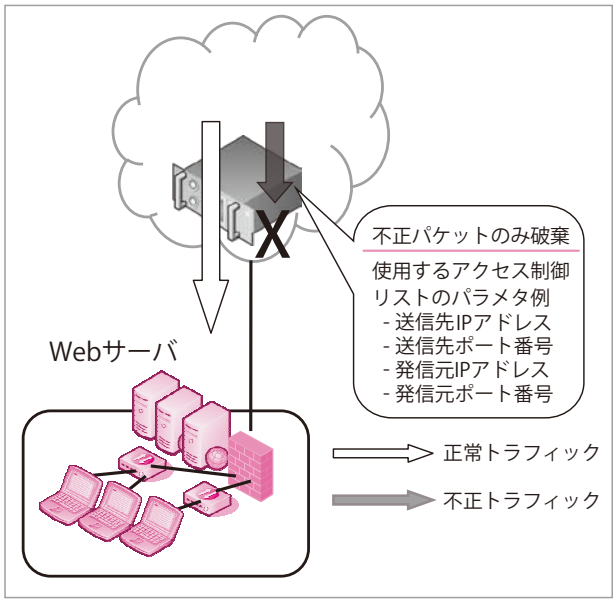

図 -13　ルータ・ファイアウォールでのアクセス制御

が通常通りに動作しているかをサイト側で監視しておくことは，サイトの安定運用という点でも有用であると考えている．

DDoS 攻撃に関しては，サイトの事業継続プランの中で，サイト側の対策だけでなく，ISP の DDoS 対策サービスの利用も検討しておきたい．また，DDoS 攻撃対策は，DDoS 攻撃の状況により攻撃を受けているサイトだけでは対処できない場合もあるため，事前に契約 ISP の相談先（故障連絡窓口や営業担当者）を確認し，相談できるようにしておくことも対策の 1 つに加えておきたい．

参考文献

1) Spyderlabs : HOIC DDoS Analysis and Detection, http://blog.spiderlabs.com/2012/01/hoic-ddos-analysis-and-detection.html
2) Radware：Dirt Jumper Ver.5 Technical Security Notes, http://security.radware.com/uploadedFiles/Resources_and_Content/Attack_Tools/research_DirtJ5.pdf
3) ModSecurity : Open Source Web Application Firewall, http://www.modsecurity.org/
4) Apache Module mod_reqtimeout, http://httpd.apache.org/docs/trunk/mod/mod_reqtimeout.html
5) JPRS : DNS のさらなる信頼性向上のために～ IP Anycast 技術と DNS ～, http://jprs.jp/related-info/guide/005.pdf

（2012 年 12 月 27 日受付）

■倉上　弘　kurakami.hiroshi@lab.ntt.co.jp
日本電信電話（株）セキュアプラットフォーム研究所主任研究員．ネットワークセキュリティの研究開発に従事．