一般

1 DoS/DDoS 攻撃とは

寺田真敏（(株) 日立製作所）

サイバー攻撃

ここ数年，報道などで「サイバー攻撃」という言葉を目にする機会が増えてきている．このサイバー攻撃を被害形態で分類してみると，大きく 3 つに分かれる．

- 官公庁系へのサイバー攻撃，パソコンが感染（2012 年 7 月）……クライアントへの標的型攻撃
- 官公庁系 Web サイトがサイバー攻撃被害（2012 年 9 月）……Web サイトへの侵入／改ざん
- 米金融機関を狙ったサイバー攻撃相次ぐ（2012 年 9 月）……Web サイトへの DoS/DDoS 攻撃

本稿で取り上げる話題は，サイバー攻撃の中の 1 つで DoS/DDoS 攻撃である．DoS（Denial of Service）攻撃は，サービス不能攻撃，サービス拒否攻撃，サービス運用妨害攻撃と呼ばれるもので，サービスそのものを使用できなくする攻撃である．また，DDoS（Distributed DoS）攻撃は，分散協調型 DoS 攻撃，分散 DoS 攻撃と呼ばれている．攻撃者の分身を多数準備し，その多数の分身から攻撃を仕掛けるとも言うべき手法で，多数のコンピュータに配備した DoS 攻撃用エージェントを制御しながら DoS 攻撃を仕掛ける．2004 年以降出現し始めたボットネットの原型と見ることもできる．

DoS という用語が普及し始めたのは，1996 年に米国コンピュータセキュリティ緊急対応チーム CERT/CC によって発行された注意喚起文書 "CA-1996-01 : UDP Port Denial-of-Service Attack（1996 年 2 月）" 以降である．前年 9 月に発生した TCP SYN Flood 型 DoS 攻撃（通称：PANIX ATTACK ☆1, 1)）により脅威が現実化したことも背景にあろう．現存するセキュリティ関連の文書を遡ると，1992 年 7 月に米国エネルギー省の下部機関であった CIAC（Computer Incident Advisory Capability）から発行された文書（C-28）の中で脆弱性の影響を記述するのに使用されている．また，DDoS という用語が使われ始めたのは，1999 年 10 月にワシントン大学から発行された DDoS ツール Trinoo の解析報告書の中である 2)．

その一方で，IETF 文書を遡ると，インターネットの世界で DoS という用語が使われ始めたのは，Jon Postel が作成したジャンクメール処理に関連する文書 RFC706（1975 年 11 月）からのようである．DoS という用語にはインターネットと同様にすでに長い歴史がある．

> In the ARPA Network Host/IMP interface protocol there is no mechanism for the Host to selectively refuse messages. This means that a Host which desires to receive some particular messages must read all messages addressed to it. Such a Host could be sent many messages by a malfunctioning Host. This would constitute a denial of service to the normal users of this Host. Both the local users and the network communication could suffer.

DoS/DDoS という用語の話題はここまでとし，以降の章では，本 DoS 攻撃特集を読み進める上で

☆1 1996 年 9 月 6 日午後 5 時 30 分頃から，ニューヨークエリアのインターネットサービスプロバイダ（ISP）である PANIX が保有する 3 台のメールサーバの SMTP ポートに対して，発信元 IP アドレスをランダムに詐称した 1 秒あたり 150 の SYN パケット（ホストあたり 50）ほどの TCP SYN Flood 型 DoS 攻撃が仕掛けられた事案である．

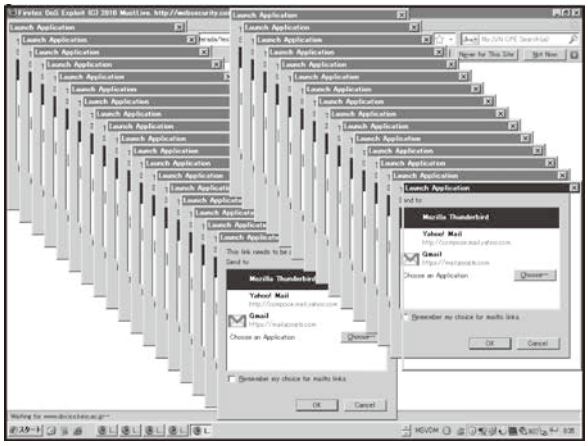

図-1　ブラウザへの動作停止 DoS 攻撃の例

役立つ，DoS 攻撃の関連用語を解説するとともに，DoS 攻撃の歴史について概観する．なお，マルウェアについては，本誌「情報処理」Vol.51, No.3（2010 年 3 月号）特集「マルウェア」を参照してほしい．

DoS 攻撃の関連用語

サイバー攻撃で使用される DoS 攻撃で思い描くのは，トラフィックが大量に押し寄せることで Web サイトが利用できなくなるというものであろう．しかし，Web サーバ装置の電源遮断，LAN ケーブルの切断などの物理的 DoS 攻撃，サーバ管理者に Web サーバの設定ファイルを変更させサービス不能状態に陥れるソーシャルエンジニアリング攻撃を併用した DoS 攻撃など，手法は多岐に渡る．そこで本章では，本特集を読み進める上で役立ついくつかの分類に絞って紹介することとする．なお，より詳細な用語解説や体系的な分類については文献 3），4）を参考のこと．

■ 資源利用に着目した分類

資源利用の視点から，量を増やし捌ききれなくなる状態を作り出す資源の利用消費型 DoS 攻撃と，仕様や環境条件の特性を逆用した資源の利用阻害型 DoS 攻撃に分類を試みる．

資源の利用消費型 DoS 攻撃

資源の利用消費型は，CPU，メモリ，ディスク，回線帯域などの有限なシステム資源を使い続けたり，使い切ったりすることを通してサービスを使用できなくする形態である．大量トラフィックを発生させて回線帯域を埋め尽くす（UDP/ICMP Flood 攻撃），高速に多数のプロセスを生成し OS のプロセスリストを埋め尽くす（Fork 爆弾），大量のログ出力を発生させることでディスクを溢れさせる，電子メールを大量送信する（電子メール爆弾，スパムメール），ユーザからの操作要求を受け付けない状態を作り出す（ブラウザへの動作停止 DoS 攻撃）（図-1）などがある．

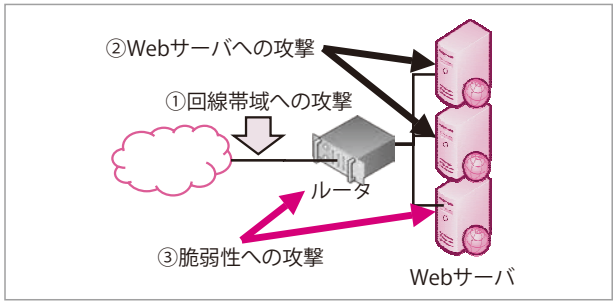

図-2　攻撃対象に着目した分類

資源の利用阻害型 DoS 攻撃

資源の利用阻害型は，有限なシステム資源を使い切るのではなく，仕様や環境条件の特性を逆用してシステム資源そのものを使えない状態を作り出すことでサービスを使用できなくする形態である．OS やアプリケーションログインの失敗を繰り返すことでログインのロックアウト状態を作り出す，ハードディスクのデータを破壊してしまうことで PC 自身を動作不能状態とする（W32/CIH，W32/Magistr），RST パケットや ICMP エラーパケットを用いて TCP コネクションを強制終了させるなどがある．

■ 攻撃対象に着目した分類

ここでは，インターネットを介して，Web サイトに DoS 攻撃を仕掛ける場面を想定し，攻撃対象に着目した視点で分類する（図-2）．

回線帯域への攻撃

回線帯域への攻撃としては，図-3 に示す大量トラフィックを発生させて回線帯域を埋め尽くす手法が挙げられる．

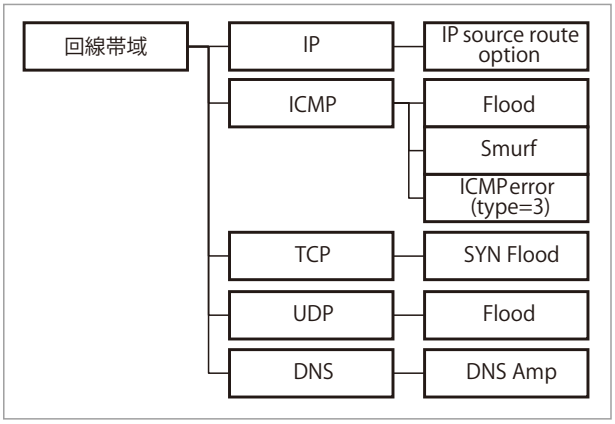

図 -3　回線帯域への攻撃手法

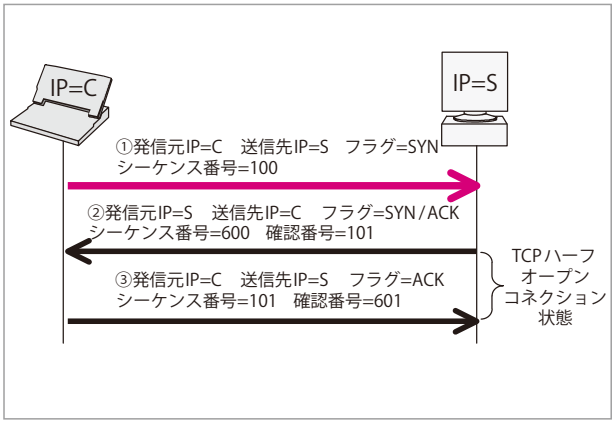

図 -5　TCP 接続の確立手順

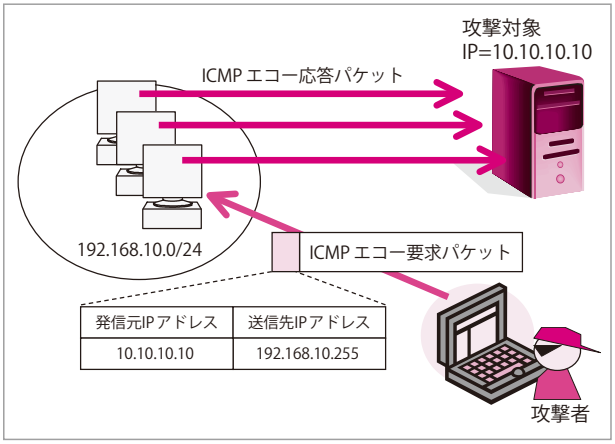

図 -4　Smurf 攻撃

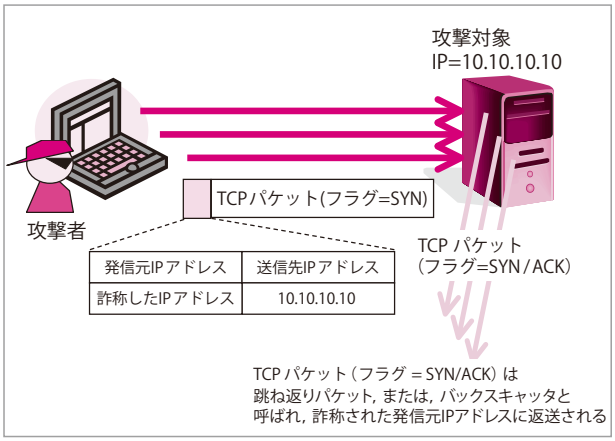

図 -6　TCP SYN Flood 攻撃と IP アドレス詐称

(1) Smurf 攻撃

ブロードキャストアドレスを増幅器として利用し，パケット数を n 倍化させる手法である（図 -4）．ICMP エコー要求パケットの送信先 IP アドレスにブロードキャストアドレスを指定し，発信元 IP アドレスに攻撃先となる IP アドレスを設定する．その結果，ICMP エコー要求パケットを受信した多数の PC（ブロードキャストアドレス先）は，一斉に詐称された発信元 IP アドレスに対して ICMP エコー応答パケットを返送することになる．詐称された発信元のネットワークでは大量の ICMP エコー応答パケット到着によりトラフィックが増大し，サービス不能状態に陥ってしまうことになる．

(2) TCP SYN Flood 攻撃

TCP 通信のコネクション確立要求を意味する TCP SYN パケットを大量に送信する手法である（図 -5 の①）．TCP 通信の場合には，3 ウェイハンドシェイクと呼ぶ 3 つのパケット交換を用いてコネクション確立を完了させる．ここで，図 -5 のパケット②と③の間を TCP ハーフオープンコネクション状態と呼ぶ．サーバはコネクション確立中であることを覚えているが，覚えられる件数は有限である．また，TCP SYN Flood 攻撃を行う攻撃者にとって，コネクション確立を完了させる必要はない．すなわち，攻撃者は，図 -5 のパケット②を受信する必要はなく，またパケット③を返送する必要もない．このため，TCP SYN Flood 攻撃には，発信元 IP アドレスを詐称した TCP SYN パケットが利用されている（図 -6）．

(3) DNS Amp 攻撃

DNS サーバを増幅器として利用し，データサイズを増加させる手法である（図 -7）．この攻撃では，DNS レスポンスが DNS クエリよりもデータサイズが大きいことを利用する．発信元 IP アドレスに

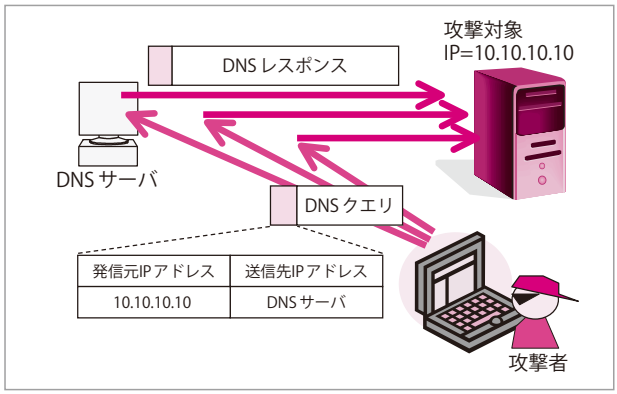

図 -7　DNS Amp 攻撃

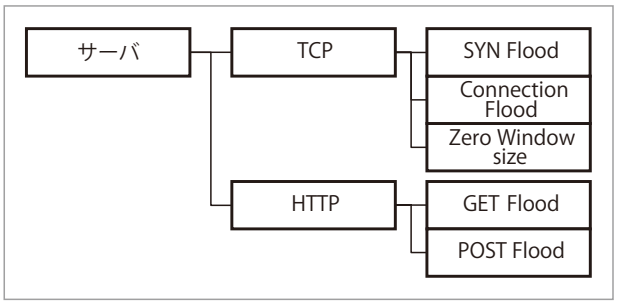

図 -8　Web サーバへの攻撃手法

攻撃先となる IP アドレスを設定して小さなデータサイズの DNS クエリを DNS サーバに送信すると，DNS サーバは大きなデータサイズの DNS レスポンスを返送することになる．この場合，詐称された発信元のネットワークには大きなデータサイズの到着によりトラフィックが増大し，サービス不能状態に陥ってしまうことになる．

Web サーバへの攻撃

Web サーバへの攻撃としては，システム資源を大量に使用する手法が挙げられる（図 -8）．

(1) TCP Connection Flood 攻撃

大量の TCP 通信のコネクション確立のみを行い，その後は，データ転送を行わない手法である（図 -9）．攻撃先のサーバには大量の確立済み TCP コネクションを維持させることで，システム資源の枯渇を誘発する．これにより，サーバでは新たな TCP コネクション確立を受け入れられなくなり，サービスを提供できない状態に陥ってしまうことになる．

(2) HTTP GET Flood 攻撃

Web サーバとの間で TCP コネクションを確立した後に，HTTP GET 要求を送信し，Web サーバにコンテンツを応答させる処理を大量に実行する手法である（図 -10）．コンテンツの応答は，Web サーバの負荷を上げるだけではなく，接続するネットワークに大量のパケット転送を発生させるためトラフィックが増大し，Web サイトがサービス不能状態に陥ってしまうことになる．F5 攻撃は，キーボードの F5 キーを連打することにより，コンテンツの再読み込みを発生させる手法で，手動による HTTP GET Flood 攻撃と言うことができる．

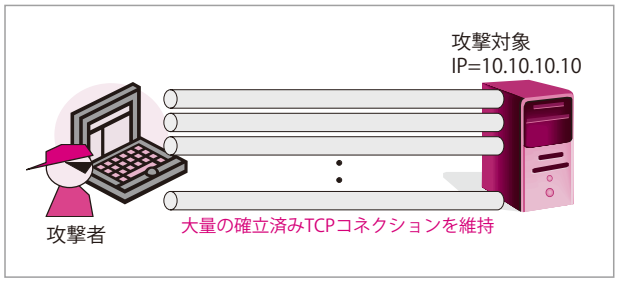

図 -9　TCP Connection Flood 攻撃

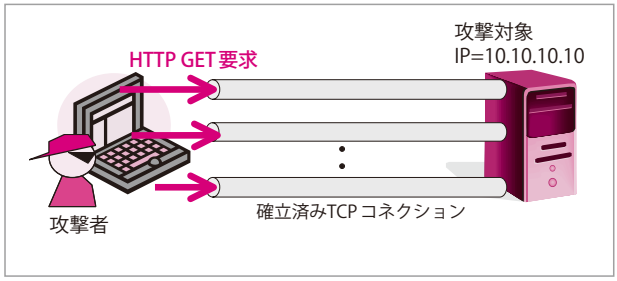

図 -10　HTTP GET Flood 攻撃

ルータやサーバの脆弱性への攻撃

権限を与えられていないユーザが，不正な方法でプログラムを実行したり，ファイルを読み書きしたりするなどの行為を無権限利用という．このような無権限利用を実現する手段として，安全性が考慮されていないプログラムのコーディングによって発生する脆弱性（ぜいじゃくせい）への攻撃がある（図 -11）．

(1) Teardrop 攻撃

分割した IP パケットがオーバラップするよう送信する攻撃である．受信側では，IP パケットを組み立てる際にパケットのオーバラップを適切に処理できない場合，ネットワーク通信機能の停止や再起動してしまうといった症状を引き起こすことになる（図 -12）．

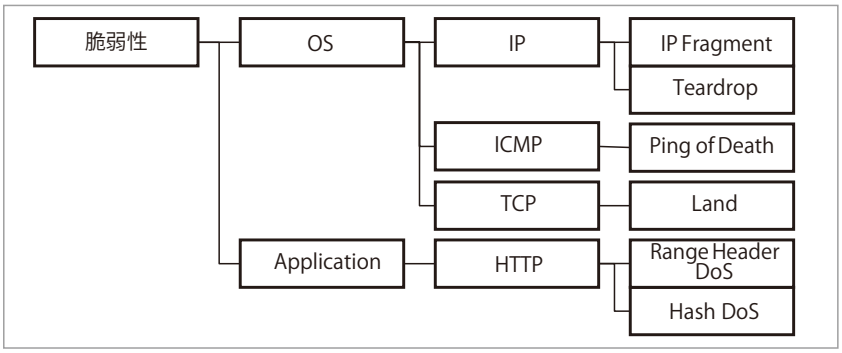

図 -11　ルータやサーバの脆弱性への攻撃手法

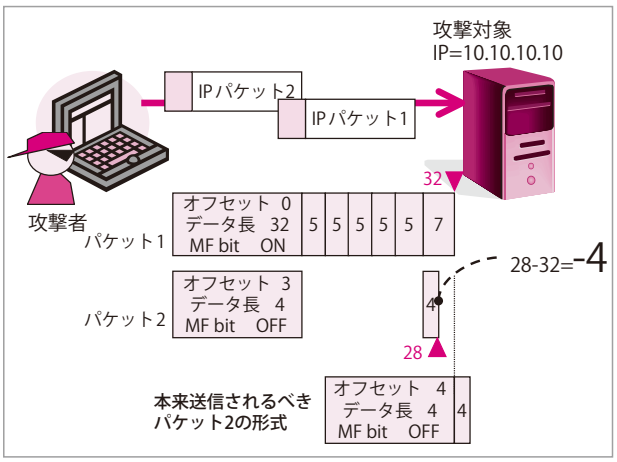

図 -12　Teardrop 攻撃

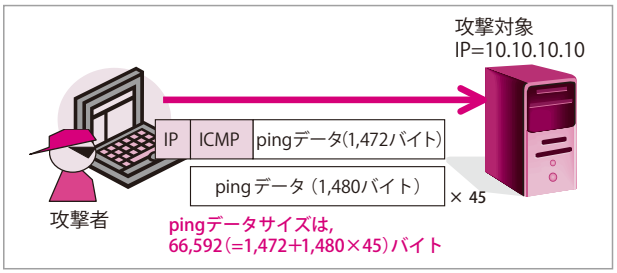

図 -13　Ping of Death 攻撃

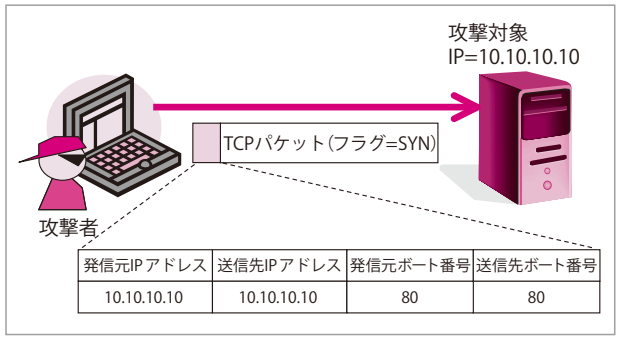

図 -14　Land 攻撃

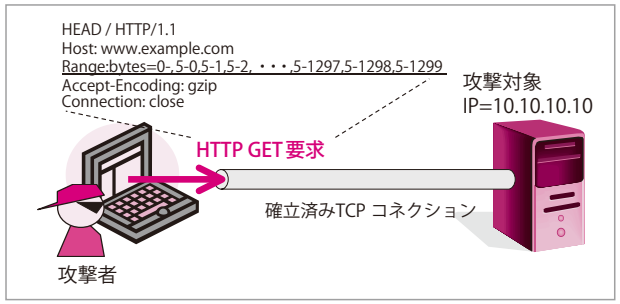

図 -15　HTTP Range Header DoS 攻撃

(2) Ping of Death 攻撃

規定外サイズの ICMP エコー要求パケットを分割して送信する攻撃である（図 -13）．受信側では，IP パケットを組み立てると，ICMP エコー要求パケットの ping データサイズの和（正確には，オフセットとデータサイズの和）が 65,535 バイト長を超えてしまうパケットを作成することになる．このような規定外サイズのパケットを適切に処理できない場合，ネットワーク通信機能の停止や再起動してしまうといった症状を引き起こすことになる．

(3) Land 攻撃

TCP 通信のコネクション確立要求を意味する TCP SYN パケットに，同一の発信元／送信先 IP アドレス，同一の発信元／送信先ポート番号を設定して送信する攻撃である（図 -14）．受信側では，このような不正なパケットを適切に処理できない場合，ネットワーク通信機能の停止や再起動してしまうといった症状を引き起こすことになる．

(4) HTTP Range Header DoS 攻撃

Range ヘッダはファイルの分割ダウンロードや，ダウンロード中断，再開などで利用されている HTTP ヘッダの 1 つでダウンロードを範囲指定する．この Range ヘッダに非常に多くの範囲指定を設定して送信する攻撃である（図 -15）．受信側では，このような HTTP 要求を適切に処理できない場合，

HTTP サーバが過負荷状態になるといった症状を引き起こすことになる．

DoS 攻撃の歴史

1994 年 12 月，IP アドレス詐称を広く知らしめた Kevin Mitnick 事件が発生した[☆2]．IP アドレス詐称は，1990 年代後半から DoS/DDoS 攻撃に利用されており，サイバー攻撃技術が年代とともに形を変え活用され続けている代表例といえる．本章では，DoS 攻撃の歴史を 4 つの世代に分けて概観する（図 -16）．

図 -16　DoS/DDoS 攻撃の進化

■ 1996 年～ 1998 年：発見の世代

1990 年代中盤の攻撃手法の流れとして，数多くのパケットレベルの DoS 攻撃を実現可能とする脆弱性が発見された．代表的な DoS 攻撃手法は，UDP Packet Storm 攻撃，TCP SYN Flood 攻撃，Ping of Death 攻撃，Teardrop ならびに Land 攻撃，Smurf 攻撃の 5 種類であったが，それ以降，パケットの組合せ方やデータサイズ変更などの変形による攻撃手法が流布した．このパケットレベルの DoS 攻撃は，やがて DDoS 攻撃へとつながることになる．

TCP SYN Flood 攻撃の手法については，1994 年頃に，Bill Cheswick と Steve Bellovin によって発見された[☆3]．この後，1994 年 12 月に発信元 IP アドレス詐称を広く知らしめた Kevin Mitnick 事件が発生し，1996 年 7 月には Phrack Magazine に "Project Neptune" として，TCP SYN Flood 攻撃の具体的な手法と発信元 IP アドレスを詐称可能な検証コードがリリースされた．1996 年 9 月，DoS 攻撃は PANIX ATTACK として現実のものとなる．TCP SYN Flood 攻撃がもたらす脅威については，米 CERT/CC から発行された注意喚起文書 "CA-1996-21 TCP SYN Flooding and IP Spoofing Attacks（1996 年 9 月）" によって世の中の人々が知ることになった．

■ 1999 年～ 2000 年：ツール世代

1999 年の後半に入ると，パケットレベルの DoS 攻撃は，多数のサイトにパケットレベルの DoS 攻撃用エージェントを分散配置し，さらにそれらのエージェントを制御しながら，攻撃を仕掛ける DDoS 攻撃へと進化した．DDoS 攻撃を実現するツールとして先陣を切った Trinoo（Trin00）は 1999 年 10 月に出現し，攻撃指令管理ホストから攻撃エージェントに対して，攻撃開始と停止を指示する機能，UDP Flood 攻撃機能などを備えていた．この後，UDP Flood，TCP SYN Flood，ICMP Flood，Smurf 攻撃機能，攻撃元を検知されにくくするための発信元 IP アドレス詐称機能を備えた TFN（Tribe Flood Network）が作成される．さらに，攻撃を検知されにくくするためのおとり（decoy）パケット送信機能を備えた TFN2K（Tribe FloodNet 2K）など，新たな DDoS 攻撃ツールが出回り，1999 年 10 月以降，DDoS 攻撃ツールのインストールを目的とした不正侵入が継続することになる．その後，2000 年 2 月，Yahoo!，Buy.com，eBay，Amazon.com，CNN，MSN，E*TRADE，ZDNet などの米国の大手サイトが次々と DDoS 攻撃によりサービス不能に陥っ

☆2 Kevin Mitnick 事件については，下村努による著作「TAKEDOWN」を参照のこと．
☆3 彼らの著書である Firewalls and Internet Security : Repelling the Wily Hacker に TCP SYN Flood 攻撃の存在を記載できる機会はあったらしいが，抜本的な対策がないことから，その記述を削除したとしている．

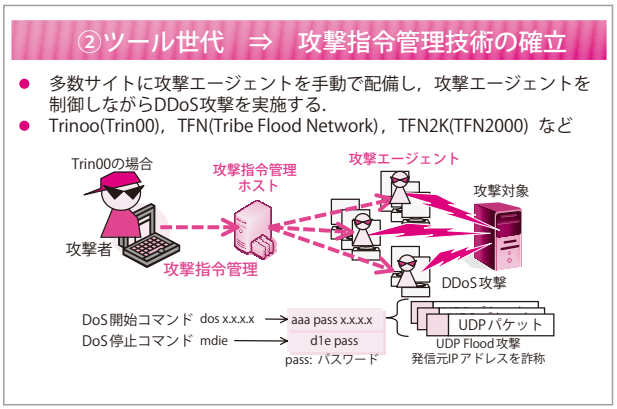

図 -17　ツール世代

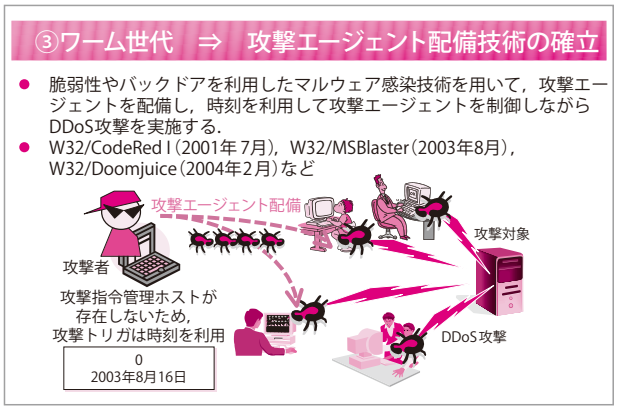

図 -18　ワーム世代

たことから，DDoS 攻撃の脅威が周知の事実となった．この一連の攻撃は，ハンドルネーム Mafia Boy と呼ばれていたカナダ人の少年が，75 台のコンピュータに侵入し，攻撃ツールを蔵置し，実行したと報告されている．

ツール世代において，DoS 攻撃用エージェントの配備は，主に攻撃者がサイトに侵入して DoS 攻撃用エージェントをインストールするという手動によるものであった．その一方で，多数の DoS 攻撃用エージェントを制御するという攻撃指令管理技術の基礎ができあがった世代であった（図 -17）．

■ 2001 年～ 2000 年代中盤：ワーム世代

2000 年，電子メールの添付ファイルとして，自己を複製しながら伝播する『電子メール型ワーム』が数十種類も発見された．この後，人手の介入を必要とせず自己を複製しながら伝播する方法として，Windows ネットワークのファイル共用を介した伝搬やリモートから操作可能なバックドアを介した伝搬などが利用され始める．さらに，2000 年代前半には，Windows や Windows サーバの脆弱性を狙う攻撃コードを用いて自己を複製しながら伝播する『ネットワーク型ワーム』の大規模感染が次々と発生した．『電子メール型ワーム』『ネットワーク型ワーム』は，新たな DDoS 攻撃活動形態をもたらすことになる．

2001 年 7 月 13 日に出現したワーム W32/CodeRed I（コードレッド）は，Windows NT/2000 上で動作するソフトウェア IIS（Internet Information Server）の脆弱性を攻撃する HTTP 要求をインターネット上に送出し，1 日で 30 万台を超える PC に感染した．さらに，W32/CodeRed I は毎月 20 日から 27 日に 198.137.240.91（ホワイトハウスの Web サイト）に向けて DDoS 攻撃を仕掛ける機能を備えていた．これに対し，攻撃目標に設定されていたホワイトハウスでは，事前に IP アドレスを 198.137.240.92 へ変更することにより攻撃を回避した．

2003 年 8 月 11 日に出現した W32/MSBlaster（エムエスブラスター）の場合には，2003 年 8 月 16 日にマイクロソフトの windowsupdate.com に DDoS 攻撃を仕掛ける機能を備えていた．8 月 14 日時点で少なくとも 33 万台が感染していたと言われており，マイクロソフトでは前日の 8 月 15 日に DNS サーバから windowsupdate.com の登録を抹消することで攻撃を回避した☆4．

ワーム世代は，攻撃指令管理を時刻に頼るしかなかったが，自己を複製しながら伝播する技術は，DoS 攻撃用エージェントのインストールを自動化する技術となった．その意味で，ワーム世代は攻撃エージェント配備技術ができあがった世代であった（図 -18）．

■ 2000 年代中盤～現在：ボット世代

2004 年頃から，マルウェアに感染している PC

☆4 2003 年 8 月 15 日以降，DNS サーバへの windowsupdate.com 登録は抹消されたままとなっている．

群が同期して活動する様子が世界中で観測され始めた．そして，翌 2005 年には，ネットワーク型ワームが終焉し，マルウェアの革新技術である「ボットネット」が台頭した．ボットネットは，ボットと呼ばれるマルウェアに感染した PC の集合体である．初期のボット（Agobot，SDBot，SpyBot など）はネットワーク型ワームを模しており，リモートからの脆弱性攻撃や，Windows ファイル共有などを利用して自己を複製しながら伝播する．2001 年～2000 年代中盤のワーム世代にできあがった攻撃エージェント配備技術の活用である．また，感染後は特定の IRC（Internet Relay Chat）サーバに接続して指令者からの命令を待ち受ける．これは，まさに 1999 年～ 2000 年のツール世代に考えられた攻撃指令管理技術の応用である．

ボットを利用した DDoS 攻撃としては，2007 年 4 月から 5 月にかけてエストニアで発生した事案，2009 年 7 月に米国，韓国で発生した事案，2011 年 3 月に韓国で発生した事案が記憶に新しい．2009 年 7 月に韓国で発生した事案では，攻撃にかかわったボットの総数は 115,044 台，政府，銀行，メディアなど計 36 サイト，また，2011 年 3 月の場合には，攻撃にかかわったボットの総数は 116,299 台，計 40 サイトが攻撃にあったと報告されている [5]．

ボット世代は，攻撃者の分身を増やす技術である攻撃エージェント配備技術と分身の活動を制御する技術である攻撃指令管理技術とが統合された世代であった（図 -19）．

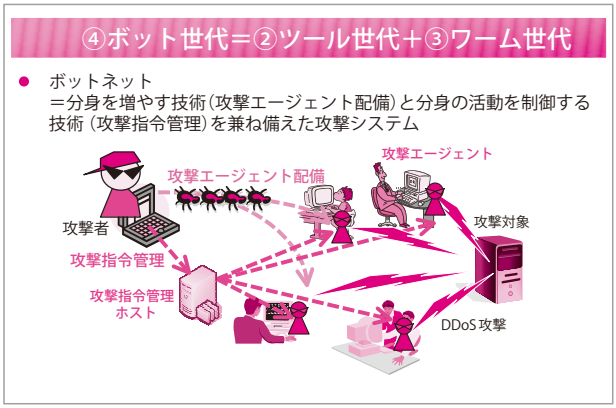

図 -19　ボット世代

DoS 攻撃との戦い

本稿では，DoS 攻撃の関連用語の解説，そして DoS 攻撃の歴史について概観した．DoS 攻撃の歴史は，サイバー攻撃における攻撃技術の進化の歴史である．DoS 攻撃との戦い，それは，サイバー攻撃との戦いの歴史と言えるかもしれない．本特集の以降の記事では，DoS 攻撃との戦いの現場や，DoS 攻撃と戦うための技術や活動について紹介されているので，ぜひそちらを参考とされたい．

参考文献

1) Public Access Networks Corporation : Panix Under Attack, http://www.panix.com/press/synattack.html
2) University of Washington : The DoS Project's Trinoo Distributed Denial of Service Attack Tool, http://staff.washington.edu/dittrich/misc/trinoo.analysis
3) IPA :「サービス妨害攻撃の対策等調査」報告書，http://www.ipa.go.jp/security/fy22/reports/isec-dos/index.html
4) IETF : RFC4732 : Internet Denial-of-Service Considerations, http://tools.ietf.org/html/rfc4732
5) Korea's Experience of Massive DDoS Attacks from Botnet, http://www.itu.int/en/ITU-T/studygroups/com17/Documents/tutorials/2011/ITU-T-ddos-tutorial-20110412-hyyoum.pdf

（2013 年 2 月 16 日受付）

謝辞　本原稿の執筆にあたり，有益な助言をいただいた Telecom-ISAC Japan の DoS 攻撃即応ワーキンググループの皆様に感謝の意を表する．

■寺田真敏（正会員）　masato.terada.rd@hitachi.com

（株）日立製作所横浜研究所 主管研究員／Hitachi Incident Response Team チーフコーディネーションデザイナ．コンピュータネットワーク，ネットワークセキュリティの研究開発に従事．JPCERT コーディネーションセンター専門委員，（独）情報処理推進機構研究員，Telecom-ISAC Japan 運営委員，日本シーサート協議会の副運営委員長を務める．