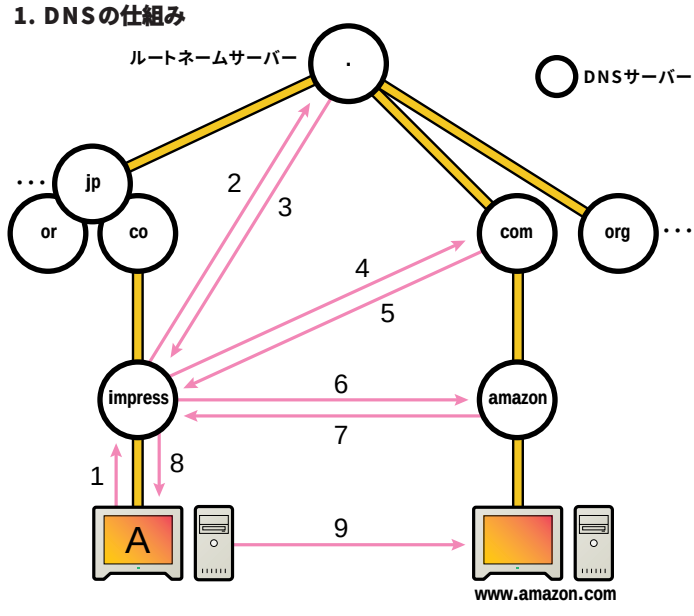
［追跡レポート］

ルートネームサーバーに何が起こったか？

「事件」からサイバーテロを考える。

1. DNSの仕組み



あるマシンAがwww.amazon.comと通信したいとき、Aで設定したドメインネームサーバー（ここではimpress.co.jpのDNSサーバー）に、www.amazon.comのIPアドレスを問い合わせる（1）。問い合わせを受けたimperss.co.jpのDNSサーバーは、まずルートネームサーバーに.comを管理するDNSサーバーのありかを問い合わせる（2、3）。次に.comを管理するDNSサーバーにamazon.comを管理するDNSサーバーのありかを問い合わせる（4、5）。これを順に繰り返し（6、7）、Aは最終的に最初に問い合わせをしたDNSサーバーから目的のマシンのIPアドレスを受け取って（8）通信する（9）。

サイバーテロの可能性がインターネット上でささやかれるようになった。去る2002年10月にはルートネームサーバーが一斉に攻撃される事件が起こった。果たしてこれはサイバーテロなのか、その警鐘なのか――。

text: **井上俊幸**

■攻撃された13のサーバー

日本時間10月22日早朝、世界中にある全13のルートネームサーバーに、過去最大規模の運用妨害攻撃が一斉に仕掛けられた。これはDoS（Denial of Service）攻撃と呼ばれるもので、AP通信によれば攻撃は約1時間続き、13あるルートネームサーバーのうち、9つに短時間の障害が起こっていたことが米国連邦当局によって明らかにされたと伝えている。ただ、今回のDoS攻撃による影響は重大なものではなく、ほとんどのユーザーが気づかなかい程度のものだったという。

ルートネームサーバーは、DNSサーバーからのクエリーに対して「impress.co.jp」といったウェブサイトのドメイン名から数字で表わされるIPアドレス（「202.173.173.**」など）へ変換するための重要な役割を担う。具体的には、階層構造を持つDNSの最上位に位置し、.comや.jpなどのトップレベルドメインを管理するDNSサーバーのIPアドレスを解決するのに使われる。すなわち、インターネットの根幹を成すサーバーだとも言える。

AからMまで名前が割り振られた13のルートネームサーバーのうち米国にあるのは10システム。それ以外はヨーロッパに2つと日本に1つが配置されている。それぞれのサーバーの管理・運用は別々の組織でなされており、東京にある「M」ルートネームサーバー（以下、Mサーバー）は、WIDEプロジェクトが管理している。

今回の攻撃について、Mサーバーを運用するWIDEプロジェクトの加藤朗氏は次のように語る。

「われわれが知るところによると13台に一斉に攻撃が仕掛けられたようです。ただ、今回に関しては大きな被害はなかったように思います。東京のMサーバーがもっとも影響を受けたうちの1つという報道もあったようですが、そうしたトラブル報告はないですね。Mサーバーのログを見ると確かに、攻撃されていた時間には、通常のクエリーに対して半分ぐらいしか応答できていなかったのですが、日本では早朝ということもあり、一般のユーザーに対する影響は軽微なものだったと思います」

被害が大きくなかったのには、DNSの仕組みによるところも多いようだ。

「DNSはキャッシュが命なんです。頻繁にアクセスされるドメイン名のデータは、実際にはDNSサーバーにキャッシュされているので、わざわざルートネームサーバーまで問い合わせることは少ない」（加藤氏）

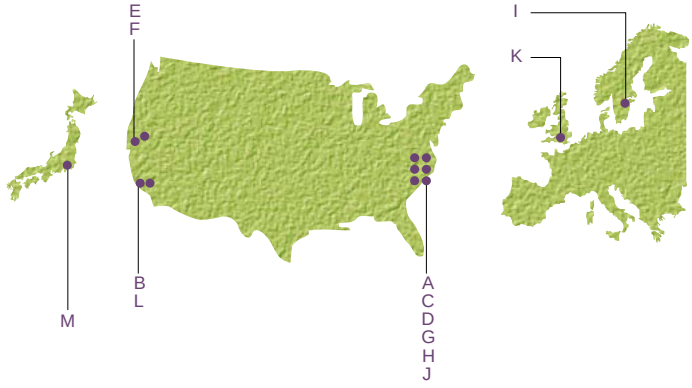
たとえ大打撃を受けたとしても、Y2K問題のときの検証で、問い合わせの量やサーバーの能力などを勘案した場合、13システムのうち3分の1が正常に稼動していれば通常のサービスには大きな影響はないと言われている。

だらかといって、この問題を軽視しているわけではないようだ。「今回のDoS攻撃

ルートネームサーバーは13あり、それぞれが世界中（そのほとんどが米国）に分散して運営されている。米国以外には、ストックホルム（I）、ロンドン（K）、東京（M）に存在する。13という制約はプロトコル上の問題で、今後、インターネット上のDNSサーバーすべてが新しいプロトコルを使うようなことになれば、さらに数が増える可能性がある。

名前	組織	場所
A	ベリサイン	ハードン（米バージニア州）
B	南カリフォルニア大学/ISI	マリナデルレイ（米カリフォルニア州）
C	PSInet	ハードン（米バージニア州）
D	メリーランド大学	カレッジパーク（米メリーランド）
E	NASA	マウンテンビュー（米カリフォルニア州）
F	ISC	パロアルト（米カリフォルニア州）
G	国防情報システム局	ビエナ（米バージニア州）
H	US Army Research Laboratory	アバディーン（米メリーランド州）
I	NORDUnet	ストックホルム（スウェーデン）
J	（ベリサイン）	Aと同じ場所
K	RIPE	ロンドン（イギリス）
L	ICANN	マリナデルレイ（米カリフォルニア州）
M	WIDE	東京（日本）

2. ルートネームサーバーのありか



はイタズラ程度」と片付けながらも、加藤氏は「サイバーテロのようなものが将来ある可能性は否定できない」と言う。ネットワーク上での攻撃もさることながら、物理的にコンピュータが攻撃される可能性も昨年の9・11を思い出せば「ない」とは言えない。もしすべてのルートネームサーバーがダウンしてしまったら、キャッシュにデータが残っていても2日程度でドメイン名からIPアドレスを割り出せなくなると言う。

■手法は古典的だが防ぐのは困難

ところで、今回受けたDoS攻撃とはいったいどのようなものなのだろうか。コンピュータ緊急対応センター（JPCERT/CC）によれば、DoS攻撃とは一般に「大量のパケットを送信してネットワーク資源を浪費させたり、サーバープログラムの弱点を悪用したりしてサービス自体を停止させ、サイトのネットワーク運用やホストのサービス運用を妨害する攻撃」と定義される。

インターネットなどの電子ネットワークを構成する機器（ルーター）が過負荷の状態になることでデータ通信に遅延が生じたり、サーバーがダウンしたりすることは、単に迷惑という以外にも具体的な経済的被害を発生させる。

今回の事件で用いられた手口は、DoS攻撃の典型的手法であるスマーフ攻撃（Smarf attack）が利用され、標的を一斉に複数の攻撃元から攻撃するDDoS（Distributed Denial of Service）攻撃だったと考えられている。ただ、DNSサーバーのシステム自体に弾力性があったことから前述のように大きな被害にはならなかった。だが、実際に13のルートネームサーバーをダウンさせることは理論的には可能であり、また攻撃犯の特定は非常に難しいという。

■「13」はプロトコルの制約

そもそもルートネームサーバーが13しかないという問題もある。13以上、たとえば100とかそれ以上のサーバーがあれば、このような懸念もなくなるはずだが――。

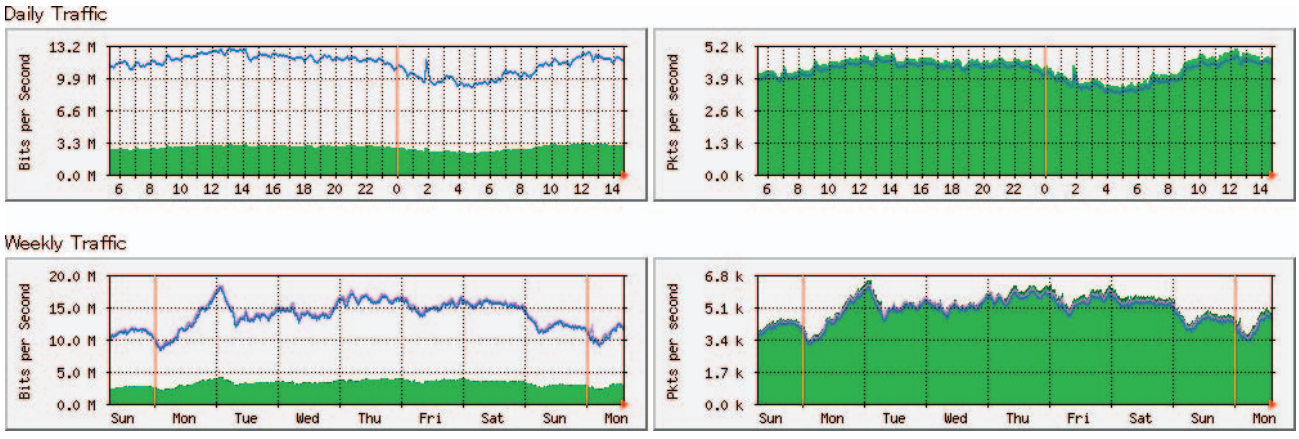
「13というのは、DNSのプロトコル上の制約なんです。DNSが使うパケットサイズの上限は“512バイト”というのに起因しています。このパケットサイズの制約で13までしかルートネームサーバーは増やせないんです。ただ、現在のプロトコルでは2048バイトのパケットを扱えるものもあって理論上は増やせます。ですが、インターネット上には古いDNSサーバーも多いので、すぐに実装するというわけにはいかないのが現状です」（前出の加藤氏）

だからといって手をこまねいて、見ているわけではない。Mサーバーでは、複数のサーバーに負荷を分散する体制を整え、セキュリティーに関しても対策を取っている。また東京地区での大災害時には、西日本に設置してあるサーバーが機能を代行できるようにしている。

■バラバラな管理体制の意味

ルートネームサーバーが世界におけるインターネットの中核的存在であるならば、「.jp」という日本のドメイン名の中核にあるサーバーも、日本という規模を見たときには大きな意味を持つ。では、.jpの管理体

3. ルートネームサーバーのトラフィック



ルートネームサーバーのトラフィックの様子。基本的には定常的にトラフィックが流れている。ただし、この約8割は不必要なクエリーだということだ。これを減らすためには、各DNSサーバー運用者の正しい管理知識が求められるという。

制はどのようになっているのだろうか。.jpの“ルートネームサーバー”に相当する.jpゾーンのDNSサーバーを管理するJPRSにも話を聞いた。

「われわれも、ルートネームサーバーと同じような危機があることは考えています。ただ、幸い過去にそのような攻撃はありません。また、ルートネームサーバーが13あるように、.jpゾーンにもDNSサーバーが6つあります。この6つはJPRS、JPNIC以外にプロバイダーや学術団体など別々の組織によって運営されています」(JPRSシステム部システムグループグループマネージャー・佐藤新太氏)。

もちろん、セキュリティー対策も考慮しており、ネットワークの輻輳を起こすような攻撃に対しては、比較的システムは堅牢だと言う。なによりも、ルートサーバーをはじめとして、主要なDNSサーバーがバラバラに管理されているのには、ちゃんとした理由がある。JPRSの佐藤氏が言う。

「管理する組織も、マシンの選定もそれぞれに異なるというのは、1つには多様性によってリスクをヘッジするという意味合いがあります。統一された考え方や方法で管理するのは効率良く見えるかもしれませんが、今回ルートネームサーバーが受けたような攻撃の場合、全部が同時に壊滅してしまう恐れも高くなる。その点、統一されていないとどこかがダメージを受けても、全体としては機能し続けられるのです」

ただ、このままバラバラで良いかというと、必ずしもそれがベストではないという意見もあるらしい。JPRSの佐野晋氏(代表取締役副社長)が続ける。

「非統一であるというのは、インターネット発展の歴史的経緯による部分も大きい。インターネットの世界では、元来がボランティアで役割を担うというのが不文律だった。しかし、裏返せば、リスクやコスト、ポリシーなどを誰がどのように負担し、決定するかということが不明確なままできてしまったのです。この点については議論が必要だとは思う。しかし、一方では、ボランティアベースで不明確なままでも実際にとても上手く機能しているので、その体制を変えていくのはとても難しいというのが現状です」

■ユーザーも大きな役割を果たす

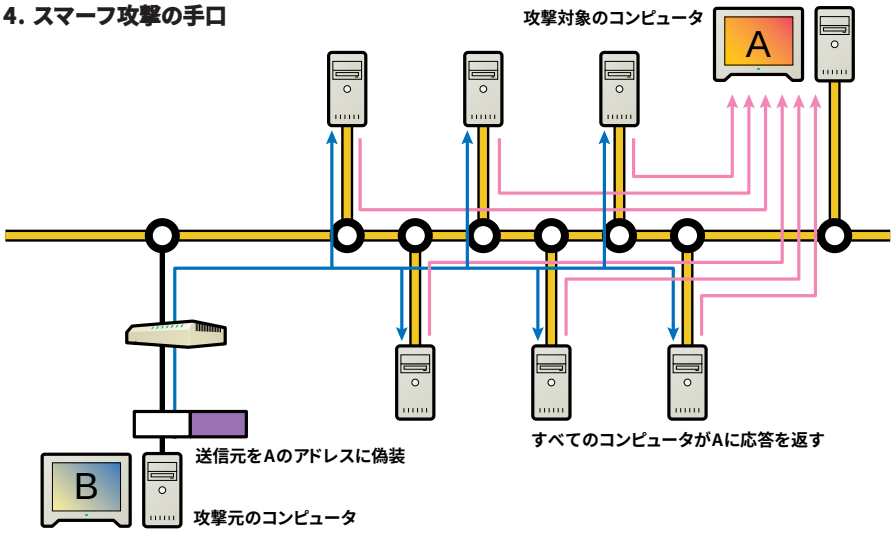
今回のルートネームサーバーへの攻撃は一部では大きな反響を持って迎え入れられ、サイバーテロの可能性もささやかれ始めている。だが、実のところこういった攻撃には、ユーザーとしてのわれわれにも大きな責任がある。DoS攻撃はそれぞれのユーザーが機器の設定やセキュリティー情報に気を配ることでかなり軽減できる。なぜなら、DoS攻撃は犯人の機器やアドレスから直接仕掛けられることはなく、ユーザーが使用している個々の機器を踏み台にして行われるからだ。そのために、パソコン上のソフトウェアを更新するなどして、セキュリティー上の弱点を塞いでおくことは当然のこと、ルーターのような周辺機器についても、設定を見直したり、必要に応じて最新のファームウェアにアップデートしたりする適切なセキュリティー対策が必要なのだ。それだけでも、知らぬ間にDoS攻撃の踏み台にされる確率を下げられる。

――サイバーテロが起こるのならば、それはわれわれの問題でもあるかもしれない。

スマーフ攻撃とは、ICMP Echoというネットワーク管理用のパケットを使ったDDoS攻撃の一種。ICMP Echoパケットを受け取ったコンピュータは、送信元のコンピュータにICMP Echo Replyパケットを送り返す。これを悪用して、不特定多数のコンピュータからICMP Echo Replyパケットを送り返すようにしたのがスマーフ攻撃というものだ。さらにブロードキャストというネットワークにつながったコンピュータすべてにパケットを送る方法がある。この2つの方法を組み合わせたのがスマーフアンプ攻撃である。

具体的には、攻撃元のコンピュータは、送信元のIPアドレスを攻撃対象のコンピュータのIPアドレスに偽装したICMP Echoパケットをネットワークにブロードキャストする。すると、ネットワークにつながったコンピュータがいっせいに、攻撃対象のコンピュータにICMP Echo Replyパケットを返す(1つのパケットが増幅される)。これによって攻撃されたホストは大打撃を受けるのである。攻撃元のコンピュータがあればあるほどネットワークの輻輳が増える。一般に攻撃元のコンピュータは攻撃犯によってクラックされたものである。

4. スマーフ攻撃の手口



［インターネットマガジン　バックナンバーアーカイブ］ ご利用上の注意

このPDFファイルは、株式会社インプレスR&D（株式会社インプレスから分割）が1994年～2006年まで発行した月刊誌『インターネットマガジン』の誌面をPDF化し、「インターネットマガジン　バックナンバーアーカイブ」として以下のウェブサイト「All-in-One INTERNET magazine 2.0」で公開しているものです。

http://i.impressRD.jp/bn

このファイルをご利用いただくにあたり、下記の注意事項を必ずお読みください。

- 記載されている内容（技術解説、URL、団体・企業名、商品名、価格、プレゼント募集、アンケートなど）は発行当時のものです。
- 収録されている内容は著作権法上の保護を受けています。著作権はそれぞれの記事の著作者（執筆者、写真の撮影者、イラストの作成者、編集部など）が保持しています。
- 著作者から許諾が得られなかった著作物は収録されていない場合があります。
- このファイルやその内容を改変したり、商用を目的として再利用することはできません。あくまで個人や企業の非商用利用での閲覧、複製、送信に限られます。
- 収録されている内容を何らかの媒体に引用としてご利用する際は、出典として媒体名および月号、該当ページ番号、発行元（株式会社インプレスR&D）、コピーライトなどの情報をご明記ください。
- オリジナルの雑誌の発行時点では、株式会社インプレス R&D（当時は株式会社インプレス）と著作権者は内容が正確なものであるように最大限に努めましたが、すべての情報が完全に正確であることは保証できません。このファイルの内容に起因する直接的および間接的な損害に対して、一切の責任を負いません。お客様個人の責任においてご利用ください。

このファイルに関するお問い合わせ先
株式会社インプレスR&D
All-in-One INTERNET magazine 編集部
im-info@impress.co.jp