# サイバーテロ――その動向と対策

宮脇 磊介●初代内閣広報官

## 不正アクセス対策だけに力を入れる日本の情報セキュリティ
## 国家安全保障の視点から、より幅広い技術対策が必要



### サイバーテロとは

サイバーテロとは何か。その定義はない。どこどこの政府機関や研究所のレポートではこのような定義をしている、といった捉え方で、一般に共通の定義はない。そもそもテロ（Terrorism）についても、その定義がないのである。技術の進歩のスピードが速く、社会システムへの展開がとめどもないエレクトロニクスが生む社会的・国家的脆弱性の拡大につけ込むサイバーテロは、そのもたらす脅威を受け止める立場や視点によっても大きく異なり、共通して納得する定義のしようがないのである。

あえてサイバーテロの定義を求めようとするのであれば、要素となるものは、まず、テロの名が示すように一般社会に恐怖を与える効果を狙うものであること。次に電子的に構築されたシステムに対して電子的な技術に基づく手法をもって攻撃し、情報を窃取したりシステムの機能を破壊したりするものであることであろう。

したがって、サイバーテロを考える場合には、定義から入るのではなくて、イメージを描いてみるのがよいであろう。

1995年、このような認識のもと、米国防総省の系統のランド研究所で「ザ・デイ・アフター」と呼ばれるシミュレーションが行われた。国民生活の基盤をなす電器、ガス、水道、交通機関、通信、警察・消防等緊急サービスなどの重要インフラに対するサイバー攻撃によって引き起こされるさまざまな事態を想定したものである。まず西海岸の電話が不通に。軍の基地でも電話システムもクラッシュ。次いで東海岸では高速列車の運航システムが機能を乱されて列車が衝突。英国では旅客機の電子機器が停止して地上に衝突。ワシントンでは携帯も含めた電話システムのすべてが機能を停止し、大統領が国家安全保障会議を緊急招集するが、メンバーに連絡がとれない。

### サイバーテロの現状と将来

平成12年（2000年）1月24日午後5時45分頃、科学技術庁（当時）のホームページが外部からネットワークに侵入してきた者によって書き換えられた。引き続き総務省、大蔵省、郵政省、運輸省（いずれも当時）、防衛庁、人事院や総合研究開発機構（NIRA）、毎日新聞社のホームページに中国語や英語で「日本人は負け犬だ」「日本政府は南京大虐殺を認めていない。日本人はアジアの恥だ」などと書き込まれたり、合計3万2,000回に及ぶ集中不正アクセスが行われたりした。警視庁麹町警察署に初めて設けられた捜査本部の発表によれば、被害届けが出された16件のうち12件が中国、1件が米国、2件が東大のサーバーからのアクセスであったとされる。日本の政府機関や言論機関が海外からの政治意図に基づく暴力的手法をとった攻撃によって実害が生じ、かつ、それらのセキュリティ対策の脆弱性が露呈され衝撃を与えたことは、サイバーテロないしサイバー戦争のはしりと受け止めてもよいものであった。

ちょうどその直後に米国のニューヨーク周辺で、eコマース（電子商取引）企業のヤフー、アマゾン・ドットコムなどが軒並みにサイバー攻撃に見舞われ、長時間にわたりサービスが停止した。これまでにない強力な破壊力を持つDDoS攻撃によるもので、被害額は最高の見積もりでは100億ドルに及んだとされ、急成長過程にあったeコマースに与えた心理的経済的影響は多大であった。

国家間で緊張関係が生じたとき、一定期間集中的に政府機関や特定機関に向けてサイバー攻撃が行われる。日本の官庁ハッカー事件は、中国が強調する南京大虐殺に否定的な日本の団体が大阪で中国政府の中止要求を無視して集会を持ったことへの反発であったことは、攻撃開始が集会の翌日であったことと書き込み内容から推察できる。その後も中国から再三にわたって集中攻撃が継続している。韓国からも教科書問題や竹島（独島）問題などに触発されたサイバーデモと称する集中攻撃が行われている。また、海外でも、インドとパキスタン、中国と台湾などの間で日常的にサイバー攻撃が交わされている。

国際的緊張に関連して、愛国心に燃えたハッカーなどのサイバー攻撃が敵対国の政府機関のウェブサイトにとどまらず、国民生活を支える重要インフラに向けられたり、人身に被害をもたらすような段階にいつ発展しないとも、限らないところにきているように思われる。また、国家が愛国的な行動を容認したり積極的にサポートするようなことも、なしとしない状況にある。日本周辺の複数の国の軍には、すでに日本の重要インフラを標的にしたサイバー部隊が編成され、研究や

演習が行われているという。また、中国人民解放軍の2名の現役上級大佐が著した「超限戦」は、これまでの限定戦争の枠を超えた「何でもあり」の戦争を行うというものであり、その中で重視されているのがコンピュータをハッキングすることである。

### 誰が、いかなる意図目的、手法で行うか

ハッカーの分類は、サイバーテロの定義が困難であり、まちまちであるのと同様に、さまざまである。ここでは、ナイーヴ・ノビス（無邪気な新参者）、プロフェッショナル・ハッカー、組織犯罪・テロリストグループ、外国情報機関の4種類を挙げたい。

2001年5月21日、世界のハッカーの誰ひとりとして知らない者はいないであろうウェブサイトが閉鎖された。アトリション・ミラード・サイトと称するそのサイトは、かつてカルトヒーローの名を持った著名なブライアン・マーティンが主宰する、世界のハッカーの戦果登録サイトであった。同氏の閉鎖にあたっての言によれば、サイト開設の頃の数年分に匹敵する数の報告が1日に寄せられるようになってさばききれない、とのことであった。侵入ソフトの高度化と大衆化は、アドバンスト・ノビス（高度な新参者）のカテゴリーをなくすことになったのである。

プロフェッショナル・ハッカーとは、カネ目当てにハッキングをする犯罪者である。企業の顧客情報を盗み出して売ったり恐喝したりする手合いで、最近は国際性を帯びてきているといわれている。

組織犯罪については、日本の暴力団が情報セキュリティの技術者を脅して不正侵入を試みさせ、企業情報を窃取したかどで逮捕された例は、氷山の一角にすぎないであろう。海外の麻薬マフィアは、取締当局に工作を仕掛けるための情報や取締りに関する情報を取るためにネットワークに侵入する。テロリストグループであるオウム真理教（現アレフ）の多くの信徒が、Y2K（2000年コンピュータ誤作動）問題の対策に日本の各企業が追われていた1999年、主要セキュリティ企業に入り込み、その大企業の名刺で100社にのぼる主要企業や治安と防衛をつかさどる官庁のY2K対策に従事していたことがあとで発覚した。悪意のないソフト技術者でも、のちにシステムトラブルがあった時のことを考えて、遠隔操作でシステムの状況を見るために自分だけしかわからないバックドアを付けておくのが通例である。次なるテロに活用できるバックドアがどこに残されているか、国家安全保障上ゆゆしいことであろう。

海外情報機関は、目的のためには何でもありで、「国営の組織犯罪」と考えるとその本質と活動が見えてこよう。ハッキングを最も高度にして洗練された技術をもって全世界に展開しており、サイバーテロやサイバー戦争の主体ともなるものである。

### 対策と今後の課題

日本は米国に次いで世界第2位の経済大国である。電気、ガス、水道、金融システム等々社会基盤の整備も、それらを支えるシステムの電子化もまた、米国に次ぐものがあろう。そのことは、とりもなおさず、日本が世界第2位のサイバー脆弱大国であることを意味する。それだけにサイバーテロ対策はこの国にとってとりわけ重要性が高い。

事実日本は、世界各国の中でサイバーテロ対策が米国に次いで進んでいるといえよう。Y2K問題対応で日本は政府はもとより民間中小企業に至るまで真剣に取り組んだことは、情報システムに対する脆弱性の認識の徹底に役立った。そしていまや日本モデルともいえる官邸主導型の情報セキュリティ対策は、1999年9月17日発足の関係官庁局長等会議で「ハッカー対策などの基盤整備に係る行動計画」の策定を目指すことに始まった。行動計画は、2000年1月21日、なんと官庁ハッカー事件の3日前に決定公表されたのである。

この時より今日に至るまで、「重要インフラに対するサイバーテロ対策に係る特別行動計画」はじめ警察のサイバーフォースの編成と活動など官側の対策の進展とあわせて民間各企業もISMSの資格認定を受けたりセキュリティポリシーを作成したりして、サイバーテロ対策の基盤が広く整備されてきている。

しかしながら、日本のサイバーテロ対策や情報セキュリティには、大きな欠陥がある。それは、ネットワークの正面玄関からの不正侵入ばかりに目が向いていることである。つまり、テンペスト（TEMPEST: The Electro-Magnetic Pulse Emanation Standard）のようにネットワークにまったく触れないで、アンテナでコンピュータなどから漏えいする電磁波を捕捉してIDパスワードや作動内容を窃視することや、逆に電磁波を外部から照射することによってコンピュータやシステムを誤作動や機能停止させたり、データを破壊したりすることを、知らないでいるか、知っていても対策が講じられていないことである。

その原因は、日本の指導者層が文系支配構造であることと国家安全保障の視点と素養に欠けていることにある。現在サイバーテロの司令塔である総理官邸も、情報セキュリティの体制が屋上屋を重ねるほど強化されながらも、この欠陥がなお存在していることが、今後に大きな課題を残している。


# ［インターネット白書ARCHIVES］ご利用上の注意

このファイルは、株式会社インプレスR&Dが1996年～2012年までに発行したインターネットの年鑑『インターネット白書』の誌面をPDF化し、「インターネット白書ARCHIVES」として以下のウェブサイトで公開しているものです。

http://IWParchives.jp/

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、データ、URL、名称など）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・図の作成者、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掲載されていない場合があります。
- このファイルの内容を改変したり、商用目的として再利用したり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される際は、出典として媒体名および年号、該当ページ番号、発行元（株式会社インプレスR&D）などの情報をご明記ください。
- オリジナルの発行時点では、株式会社インプレスR&D（初期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。

お問い合わせ先 | 株式会社インプレスR&D | ✉ iwp-info@impress.co.jp