追跡スクープ

日本も急襲!!
中国人民解放軍
サイバーテロの脅威

**中国発のサイバー攻撃が日本政府中枢を襲っている。
9月初旬、欧米諸国の政府中枢のコンピューターが
人民解放軍傘下のハッカー部隊によるものとみられる
侵入を受けていることが問題になったが、
本誌の取材で、日本での被害が在日米軍基地にも及び、
深刻なものとなっていることがわかった。**

本誌　藤原善晴

2005年6月に四川省成都で行われた中国人民解放軍の式典（Getty Images／AFLO）

上空から見た在日米軍横田基地（本社ヘリから＝小西太郎 撮影）

昨年5月、東京都内のコンピューター技術に詳しい教員のもとへ「第16駆逐戦隊」という奇妙な件名の電子メールが届いた。送信者名は、「防衛庁航空幕僚監部総務部」を偽装しており、航空幕僚監部（空幕）広報室の送信アドレスを表示してあった。「3週間を付属のファイルに見てください」と怪しい日本語で書いて

あったが、添付ファイルを開くとウイルスに感染し、パスワードなどの個人情報が流出する恐れがあった。メールはこの教員だけでなく、防衛庁（現防衛省）関係者を含む膨大な数の人々のもとへばらまかれた。

防衛庁標的のウイルス

「航空幕僚監部広報室」になりすましたのは、いったい誰だったのか。本物の広報室の説明はこうだ。

「中国のサーバーのIPアドレスが送信に使われていたことを確認しました。ただ、それだけでは中国が発信源だと断定するのは難しい状況です。警視庁に『業務妨害』事件として被害届を出し、その後、国際刑事警察機構（ICPO）に捜査が依頼されていますが、結果については聞いていません」

では、なぜ教員のもとにメールが届いたのか。この教員は、

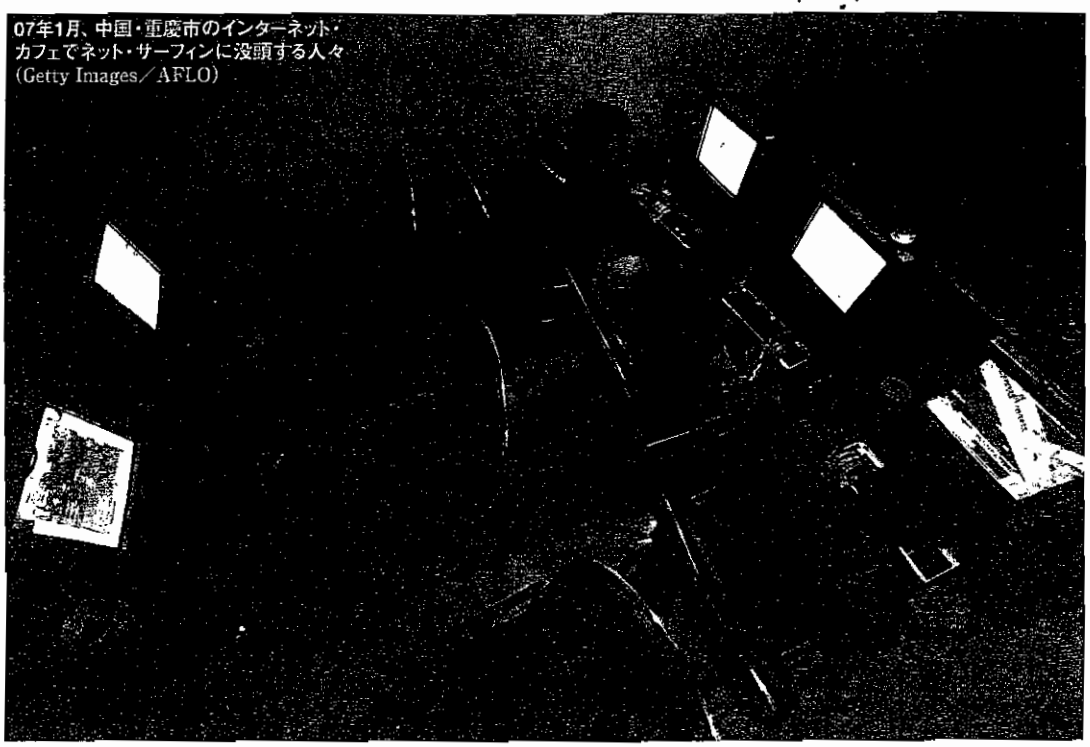
「防衛庁のメールニュースを受け取っていたことぐらいしか原因が思い当たりません」

といぶかしむ。サイバーテロに詳しい情報当局者は言う。

「問題は、犯人が、防衛庁やその周辺の人たちのメールアドレスをどのようにして大量に集めていたかです。くだんのウイルスメールを送信する以前の侵入で、防衛庁関係者から盗み取った情報からメールアドレスをごっそり取り出していた可能性があります。犯人は、さらに情報入手先を増やすためにウイルスをばらまいたのでしょう。発覚した事件以外に、気づかれずに行われた侵入がどれだけあったのか考えると恐ろしくなります」

同月、当時の額賀防衛庁長官からを装ったウイルスメールもばらまかれた。

送信者欄には、額賀長官の事務所が実際に使っていたアドレスが表示されていた。件名はなんと「海軍作戦計画」で、「付属のファイルに見てください」と書かれていた。ファイルを開くと、やはり、ウイルスに感染する恐れがあった。


07年1月、中国・重慶市のインターネット・カフェでネット・サーフィンに没頭する人々
（Getty Images／AFLO）

前出の情報当局者によれば、こうした情報入手を目的にしたウイルスばらまきは在日米軍基地も標的にしている。公表はされていないが、昨年、そして今年の春先にも、米軍横田基地のコンピューターで「トロイの木馬」型ウイルスなどが見つかっているというのだ。「トロイの木馬」は、ひそかに送り込まれるコンピューターウイルスの一種で、内部の情報を勝手に集めて送り出したり、外部からの操作を受け付けてしまう。

サイバー"民兵"を養成

9月5日付英ガーディアン紙は、「英国の外務省など主要官庁のコンピューター・ネットワークが、中国のハッカーによる不正侵入を受けていた」と1面トップで報じた。これと前後してゲーツ米国防長官室の電子メールに中国のハッカーが侵入し、完全復旧までに3週間かかったというニュースも流れた。8月下旬に訪中したメルケル独首相は、温家宝首相との会談で中国のハッカーがドイツの首相府などへのコンピューター攻撃を仕掛けていると抗議した。

これらの報道、抗議で共通して言及されているのは、中国人民解放軍の実行、または関与である。前出の情報当局者は言う。

「中国人民解放軍によるサイバー攻撃は、直属のハッカー部隊は直接手掛けず、別組織を使っているようです。関与の痕跡を残さないためでしょう。その内実は"民兵"というべきもので、欧米の情報機関では、『中国伝統の人海戦術で少なくとも数万人を動かしている』と推定しています」

中国のインターネット使用人口は約1億6000万人もおり、優秀なハッカーを探すのはそれほど難しいことではない。

破壊工作から情報入手へ

2003年、全世界で猛威を振るった「ウェルチアウイルス」で、中国のハッカーが注目された。このウイルスは米国政府の電算網を攻撃、ビザ発給業務を一時中断させる威力を発揮した。『ネットワーク時代のテロリズム』（三修社）の著者で大阪国際大学の安保克也准教授は、

「ウェルチアウイルスのプログラム内部に中国（china）という単語があったため、中国産だと推定されています」

と指摘する。

人民解放軍は03年、軍近代化の一環として、北京にハッカー部隊（情報化部隊）を創設したとされる。

韓国では04年7月、政府機関のコンピューター網への不正侵入事件で、中国人容疑者を特定し、中国に対し、捜査と再発防止を求めた。情報当局者は言う。

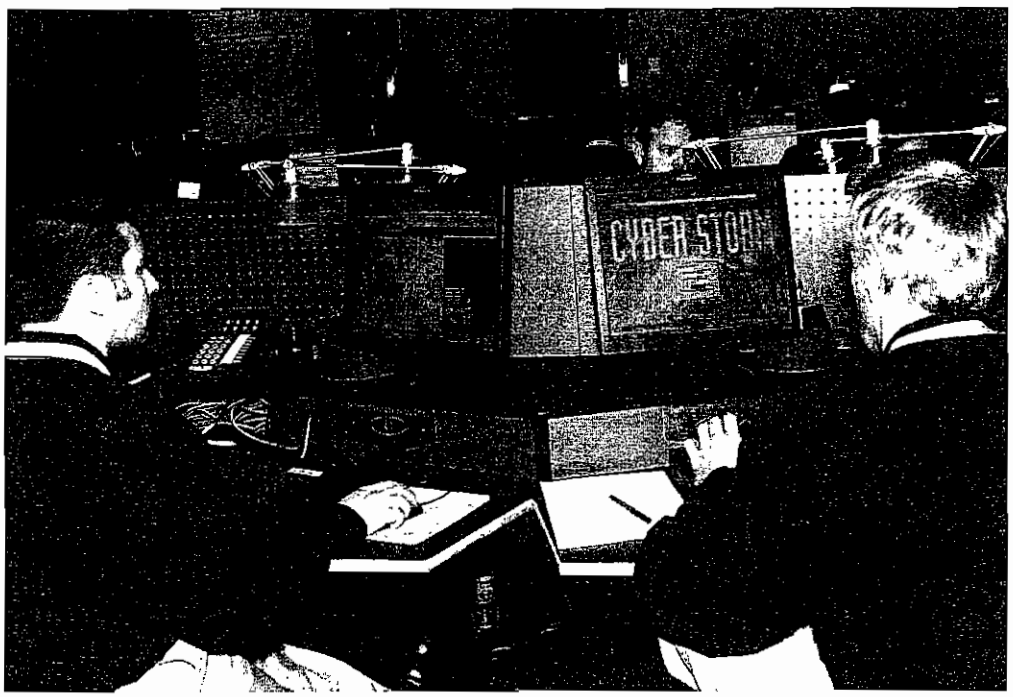
「韓国当局はメールのIPアドレスなどを追跡。容疑者は当時20歳代後半で、中国人民解放軍系の外国語学校で韓国語を勉強していた学生だったことを突き止めました。この学生が〝民兵〟の一人である可能性は十分あります」

IPアドレスを手がかりに容疑者を割り出した韓国に比べ、冒頭の防衛庁絡みでの事件での日本の対応は手ぬるいとの感は否めない。

情報当局者によれば、中国のハッカーたちは、従来から攻撃用ウイルスの開発、外国政府機関のホームページへのデータ大量送信などの破壊型のハッカー活動などを繰り広げてきた。その彼らが、ネットワーク侵入やなりすまし行為などによる、欧米、日本などからの機密情報入手に比重を移し始めたのは05年の後半からだという。これにより各国からどのような情報が盗み出されたかについては、コトが機密情報にかかわるだけに表面化していない。

危機感足りぬ日本

ドイツ有力誌「シュピーゲル」8月27日発売号は、憲法擁護庁が「約160ギガ・バイトの情報」が中国に流出するのを防いだと報じたが、「これまでに流出した情報がどんなものかは誰にもわからない」とのドイツ高官のコメントを掲載するにとどまっている。同誌によれば、中国発の「トロイの木馬」型ウイルスは、首相府、外務省、経済省、教育研究省のコンピューターで発見された。



06年2月、米国ワシントンの国土安全保障省で、サイバーテロを想定して行われた「サイバーストーム」演習（AP Images）

前出の安保准教授は、ドイツが狙われた理由について、

「北大西洋条約機構（NATO）の中枢でもあり、NATOのサイバー戦のレベルを試すとともに、ドイツの軍事技術（セキュリティー技術、情報技術）などを盗み出そうとしたのでしょう」

と分析する。また、欧米のマスコミが、中国発のハッカー攻撃と中国人民解放軍の関与について盛んに報道していることについては、

「中国のハッカーたちの情報入手のウイルス技術が高度化し、事態が深刻になっていることの表れ。日本政府はもっと危機感を持つべきです」

と警鐘を鳴らす。

このように、先鋭化する電脳空間の国際情報戦だが、一般市民も無関心ではいられない、と指摘する専門家もいる。コンピューターに詳しい軍事研究家の井上孝司氏は、

「サイバー攻撃の過程で、一般市民のパソコンにウイルスが忍び込み、乗っ取られてしまうことがあります。自分は関係ないとタカをくくり、セキュリティー対策をとらないでおくと、サイバー攻撃の〝踏み台〟にされて『共犯者』になってしまう事態もありえます」

と警告する。世界規模のネットワークが構築されたことで、一般市民はインターネットを利用することで、容易にさまざまな情報や知識を得ることができるようになった。井上氏は、

「便利さは、同時に一般市民がサイバー攻撃の戦場と隣り合わせに生きているということを意味するのですが、それを意識していない人が多いのです」

とも言う。

技術では米国が先行

欧米諸国での人民解放軍関与説について、中国外務省は「全く根拠がなく冷戦思考の表れ」と全面否定する。中国のメディア報道では、「海外のハッカーが中国のネットワークを脅かしている」と、「中国は被害者」と強調している。

もともとサイバー戦技術では米国が大きく先行してきた。中国側から見れば、米国への対抗措置としてハッカー技術の開発を進めているとの論理が成り立つかもしれない。

たとえば、1991年に米国を中心とする多国籍軍がイラクと戦った湾岸戦争で、米国はサイバー戦で大戦果を挙げている。イラクが戦争を準備している段階で、輸出品のプリンターに時限装置付きのウイルスを忍ばせた。そしてイラクの防空システムを麻痺させることに成功したのだ。安保准教授は訴える。

「近年、中国がサイバー技術を飛躍的に進歩させており、米国が絶対的に優位とはいえなくなっています。こうした急激に変化する情勢をにらみ、日本は、サイバー空間を守り、国家の重要な情報の漏洩を防ぐための法律や政府組織の整備、そして人材確保を急がなければなりません」 yw