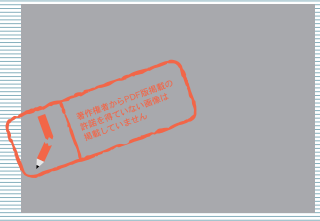
日本のインターネット危機管理はどこまで整備されたか



Text : 佐々木俊尚 (Press Archives)　　Photo : Hiroji Kazuo

これだけある社会生活に直結した危機

狙われている各国政府のシステム

平凡なウイルスが公共サービスを麻痺

2000年春、ちょっとしたコンピュータウイルス事件が米ヒューストンで起きた。

そのウイルスはパソコンに感染し、ハードディスクのフォーマットやシステムディレクトリーの削除を行う。これだけなら、きわめて平凡なウイルスの一変種でしかない。しかしこのウイルスは、もう1つ興味深い特徴を備えていた。アナログモデムを使い、米国の緊急通報電話番号である911番に電話をかける能力を持っていたのだ。

ウイルスはごく早期に発見されたため、実際の被害はほとんど生じなかった。米連邦捜査局(FBI)ヒューストン支局がいち早く捜査に乗り出し、容疑者と見られる男性の自宅を家宅捜索してコンピュータを押収するなど先手を打ったからだ。FBIは間もなく、ヒューストンの銀行に勤める技術者を逮捕した。宗教や政治的動機はなく、いたずら目的だったと見られている。

しかしこのウイルスは、実はかなり強力なパワーを持っていたのだ。プロバイダー経由で一度に2550台もの感染先のパソコンを見つけ出し、そして推定だが3日間で25万台ものパソコンに感染する能力があった。もしこのウイルスが爆発的に感染範囲を広げ、その結果、米国全土の無数のパソコンが911番に電話をかけ始めていたら——。被害が最小限に押しとどめられたのは、不幸中の幸いだった。もしこの強力なウイルスを、テロリストやカルト教団が入手していたとしたらどうなっていただろう。一定の日時に同時に911番へ通報するDDoS(分散型サービス拒否)攻撃を使い、凶悪なハイジャックテロや爆弾テロを起こすのと同時にこのウイルスを動作させたら、どうなっていただろうか。単一のテロ事件以上に、社会は大きな混乱を来す可能性は高かっただろう。

懸念されるハイブリッド型のテロ

同種の事件は、今年1月に全世界に蔓延したコンピュータワーム「SQL Slammer」でも生じている。このワームによって米シアトルの緊急通報番号が機能不全に陥ったのだ。シアトル郊外の警察と消防の911センターが事実上使えなくなり、スタッフは緊急電話に対して紙と鉛筆で対処する羽目になったのだ。

各国の政府関係者の間では、いまこうした「ハイブリッド型」とも言えるサイバーテロに対する懸念の声が高まりつつある。

かつてはサイバーテロと言えば、凄腕のハッカーが政府システムの中枢に侵入してデータを盗んだり、原子力発電所を勝手に作動させたり……といったイメージだった。しかし最近は、そうしたサイバーテロの可能性に対しては、懐疑的な見方も広がりつつある。日本政府のセキュリティー対策担当者の1人は「テロリズムは言葉のとおり、テラー(恐怖)を人々に与えるための手段。難しいサイバーテロで政府のコンピュータ技術者を惑わせるよりは、爆弾を投げて市民を殺害する方が簡単で影響力も大きい」と指摘する。「サイバーテロはこうした爆弾テロなどの補助的手段として使われる可能性の方が高いのではないか」と言う。

こうした可能性の1つが、冒頭に挙げたような緊急通報電話へのDDoS攻撃などの手口だ。こうしたハイブリッド型サイバーテロが行われ、市民が情報から隔絶されるような事態が生じた場合、社会に与える恐怖は何倍にも増加するだろう。

水道水が知らないうちに毒にも

とはいえ、重要なインフラに対するサイ

バーテロの危険性も決して否定はできない。たとえば「9.11同時多発テロ」を引き起こしたとされる国際的テロ組織「アルカイダ」は、米国の水道供給システムに侵入すべく準備を進めていた形跡があるのだ。

米国家インフラ防御センター(NIPC)は9.11テロから4か月後の2002年1月、アルカイダがSCADA(監視制御・データ収集システム)の情報を密かに収集していた形跡があると警告した。SCADAというのは、公共機関などが上水道や電力の供給、調整などに使われている遠隔機器制御システムの名称だ。このSCADAシステムに、もしテロリストが侵入できたら何が起きるのだろうか。米国の水道には、浄水場で塩素やフッ素が添加されている。この分量を変え、大量の塩素やフッ素が水道に流し込まれたら――。大きな被害が起きるに違いない。実際、SCADAの設計者の1人は米メディアの取材に「もし侵入者が十分な技術的知識を持ってSCADAに不正アクセスできれば、大惨事を起こすことも可能だ」と明言していたのだ。

政府のシステムに触れる者も注意

そしてサイバーテロは、決してネットワークを介した不正アクセスだけを言うのではない。最近問題として指摘されているのが、政府がシステムを導入する際、下請けや孫請けの業者として身元のはっきりしないエンジニアが政府施設に立ち入り、データの窃盗や改ざん、破壊工作などを行う可能性があることだ。9.11で過剰なまでにテロを警戒している米国では昨年、外国人が政府施設のコンピュータに近づくことを禁止する施策さえ打ち出している。人種問題からも批判の多いその施策の是非はおいておくとしても、米政府がいかにセキュリティーに対して強い意志を持っているかがわかるというものだ。

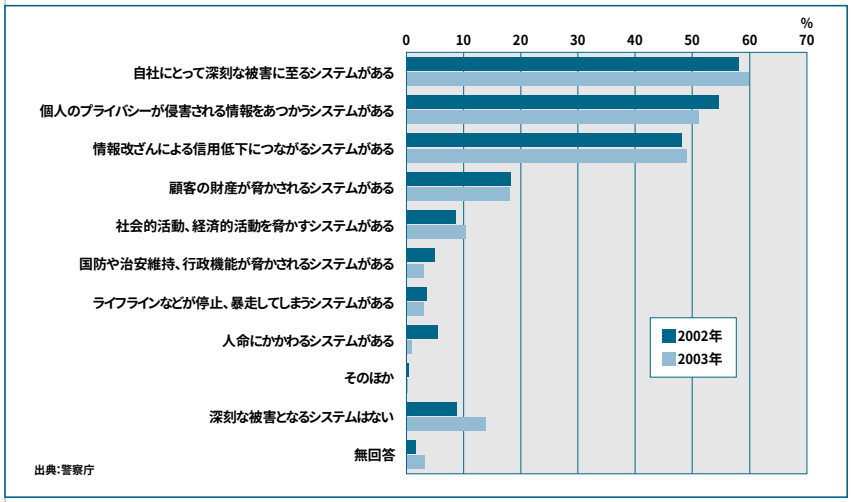
翻って、日本ではe-Japan戦略の例を見てもわかるように、政府や自治体がベンダーにシステム導入や運用を丸投げしてしまっているケースが少なくない。大手ベンダーは丸投げされた発注を下請けやさらには孫請けに出し、身元のはっきりしないスタッフが公共機関のシステムに接触している。

実際、すでに事件は起きている。2000年春、オウム真理教(現アレフ)の経営するソフト開発会社が、中央官庁のシステム開発を請け負っていたことが明るみに出たのだ。

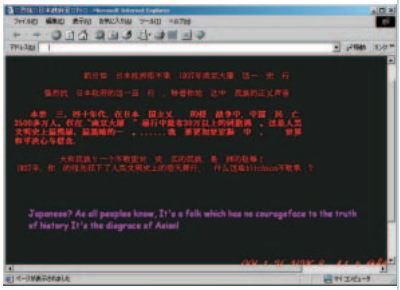
このうち防衛庁が発注したシステムは、自己資本額や実績などを審査した企業44社を対象に一般競争入札を行い、その中の1社と契約していた。だがこの会社が下請けに出し、そして下請け会社が孫請けに出して……というかたちで次々に仕事は下に回され、何と5番目に位置していたのがオウム真理教の会社だったのだという。実際に請け負っていたのは、庁内LANのルーター設置やファイアーウォールの導入などだったとされ、軍事機密にこそ近づいてはいなかったものの、オウム側がもし何らかの悪意を持っていれば、破壊行為も可能だった。事件は警視庁がこのオウム企業を別の事件の容疑で家宅捜索して発覚。防衛庁など中央官庁の側は警察に指摘されるまで、この事実にまったく気づいていなかったという。

このように緊急危機的に起こるサイバーテロは、あらゆる手法、あらゆる可能性をはらんでいる。政府がこれを防ぐのは、容易なことではない。「セキュリティーに完璧という言葉はない」とはセキュリティー業界の誰もが口にする言葉だが、国民の重要な財産と情報を握っている政府は「完璧はない」では許されない。果たして日本政府は、どこまで対策を進めているのだろうか。

社会的に深刻な被害を及ぼす情報システムの有無に関する調査結果



不正アクセス行為の禁止などに関する法律において、国家公安委員会はアクセス制御機能を有する特定電子計算機の不正アクセス行為からの防御に資するため、毎年少なくとも1回実態調査を行うこととなっている。調査対象は全国の企業、教育関連、行政サービス機関から偏りのないように1980件を抽出。調査結果の上位3項目は前回と同様の傾向にある。



日本では、2000年初頭に相次いで省庁のウェブサイトが改ざんされたが、これをきっかけにセキュリティー対策が本格化する。画面は中国語簡体字の文章に書き換えられた総務庁(現総務省)のウェブサイト。

もう省庁のウェブが改ざんされることはない？

危機の実体験から本気になった日本

幼稚な省庁が初めて受けた屈辱

このように、緊急対応が必要なネットワークを通じたサイバー危機の可能性は日本でも非常に高まっている。朝鮮半島危機が懸念される中ではなおさらだ。

日本政府のサイバーセキュリティー対策が大きく動くきっかけとなったのは、2000年初頭に起きた中央省庁のウェブサイト改ざん事件だった。最初に攻撃されたのは、科学技術庁（現文部科学省）のウェブサイトで、トップページを「日本人は負け犬だ」という英文に書き換えられた。1月24日に起きたこの事件を皮切りに、総務庁（現総務省）のサイトが南京大虐殺への中国語の抗議文に書き換えられる（前ページ参照）など、10以上の公的機関のサイトが改ざんされた。犯行は中国人の仕業だったと見られているが、それにしても日本の中央官庁が史上初めて、大規模な不正アクセスの被害に遭遇するという事態に、政府は大騒ぎとなった。

だがシステムの導入から運用まですべてをベンダーに任せきりだった省庁は、いきなりの事態にまともな対応もできず、右往左往するのみだった。総務庁ではパソコンに中国簡体字のフォントをインストールしていなかったため、中国語の抗議文が読めずに、文字化けしたままの画面を紙にコピーして報道陣に配布した。その程度のコンピュータリテラシーしか持ち合わせていなかったのだ。

いずれにせよ、この事件をきっかけに政府の対策が急に進むことになった。事件当時、あるセキュリティー企業の幹部は「事件発生後数日で、平年の数か月分の発注が来た」と笑みを浮かべ、「これから『ハッカー特需』がやってくるかも」と話していたが、そのとおりになった。

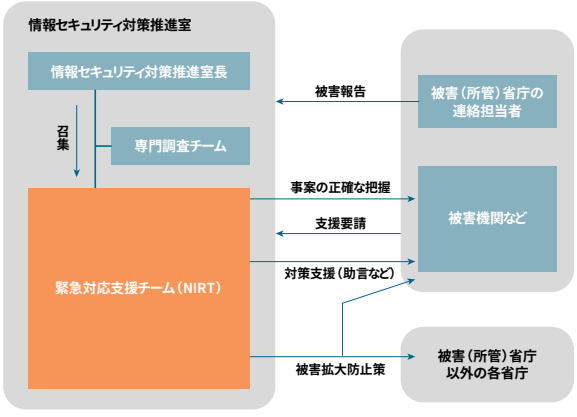
省庁を横断する組織を設置

政府対策の第一弾が内閣官房に「情報セキュリティ対策推進室」（以下、推進室）を新設したことだった。しかも、設立は事件発生からわずか1か月後の2月29日という異例の素早さだった。さて、推進室が最初にした仕事は、同年7月に各省庁に向けてセキュリティーポリシーのガイドラインを作ったことだった。

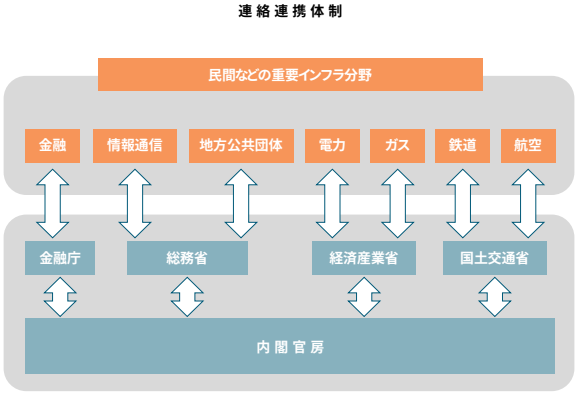
それまで各省庁はセキュリティーについては何もしていなかった。ポリシーなども当然なく、具体的な対策についてはベンダーに言われるがままにファイアーウォールを導入する程度だったようだ。職員の使うパソコンにアンチウイルスソフトさえ導入されていなかったとも言われている。推進室はこの態勢を改めるべく、①単にポリシーを策定するだけではなく、見直しを繰り返してポリシーをきちんと改善させていくこと、②セキュリティーの責任者を決めて、その下に委員会を作ること、③物理的セキュリティーと人的セキュリティー、技術的セキュリティー運用のそれぞれの観点から包括的な対策を行うこと、④ポリシーを徹底するために各部署で実施手順を決めること、という4点を指針とした。

また推進室はこの時期に中央省庁以外の重要な機関――電力やガス、通信、鉄道、航空、情報通信、銀行、地方自治体などのいわゆる「重要インフラ」をサイバーテロから守るための特別行動計画も作った。そして、政府がこれらのセキュリティー対策を推し進めることになった背景には、2つの大きな要因があった。

緊急対応支援チーム（NIRT）の活動概要



重要インフラを民間と連携して守る



1つは2001年9月11日に米国を襲った同時多発テロで、もう1つは今年あたりから具体化しつつあるe-Japan戦略の電子政府構想だ。前者は衝撃的なまでのテロリズムの実在を改めて政府に実感させるきっかけとなり、そして後者はそうした21世紀の状況の中で電子政府へと踏み出すことについての覚悟を政府関係者に再び植え付ける役割を果たした。

緊急に対応するチームを結成

その1つの結果が、緊急対応支援チーム（NIRT）の設立だった。昨年4月にスタートしたNIRTは推進室に置かれ、セキュリティー企業の関係者や各省庁の職員など非常勤のスタッフ17人で構成される。サイバーテロが実際に発生した場合は、関係省庁が推進室に連絡し、そこからスタッフに電話やメールで連絡が入る。

アラートのレベルは「情報収集」と「スタッフ一部参集」、「スタッフ全員参集」の3段階に分けられている。たとえばイラク戦争時などは、日本政府に直接のサイバー攻撃が行われる可能性は少なかったものの、米陸軍のウェブサーバーが侵入されたり、カタールの衛星放送アルジャジーラのウェブサイトがDOS攻撃を受けたりするなどの事件が発生していた。このためNIRTのアラートは「情報収集」のレベルだったという。もし今後、省庁のデータがごっそりと盗まれたり、大規模なDOS攻撃で電子政府のシステムがダウンしたりしてしまうような事態が生じれば、アラートは「全員参集」のレベルにまで引き上げられることになる。その場合には17人のスタッフが全員首相官邸に隣接する内閣官房に集まり、対策を検討するとともに、攻撃を受けた省庁などに出向いて現場を指導するなどの行動をとることになる。

現段階では、ここまでが政府の取ってきたおもなセキュリティー対策と言える。万全とは言えないかもしれない。ただ少なくとも、セキュリティーに対する理解度がゼロに等しかった2000年初頭の時点と比べれば、はるかに前進してきたのは間違いない。とりあえずは低レベルのサイバー攻撃に対しては対処する能力を備えるようになり、そして高レベルの攻撃に対しても緊急対応できる体制作りまではようやく整いつつあるということだろう。

情報セキュリティ対策推進室の吉原順二副室長に聞く 3年で日本はどれほどレベルを上げた？

政府のセキュリティー対策に大きくかかわる内閣官房の情報セキュリティ対策推進室の副室長を務める内閣参事官の吉原順二氏に現状などを聞いてみた。

対策室の設置から3年でセキュリティー対策はどのように進みましたか。

吉原氏：意識面、対策面ともに相当進歩している。今年初めにSQL Slammerというコンピュータワームが全世界に蔓延し、韓国などではたいへんな被害を出したが、日本ではほとんど被害が生じなかった。官公庁のウェブ改ざん事件も最近はゼロに近く、いたずらのレベルでの対策が相当に進んだ結果だと思う。最初のラウンドの仕事は終わったのかなという印象だ。

各省のセキュリティーポリシーをどう評価していますか。

吉原氏：対策室で実施状況をヒアリングして評価している。そこでいくつか課題が見えてきた。それはポリシーの運用が文書化されておらずに担当スタッフの力量任せになっていることや、同じ省内でも部署によってばらつきがあることなどだ。さらに職員に対する意識の醸成がもっと必要で、こうした論点をもとに昨年11月にはセキュリティーポリシーのガイドラインを改定した。

重要インフラについては、民間企業に対して官がどこまで介入するかという点も問題になりそうですが。

吉原氏：政府IT戦略本部の下に各省の局長級の情報セキュリティ対策推進会議がある。さらにその下に課長級のワーキンググループを作り、各省で管轄している重要インフラは大丈夫なのかを検討してもらっている。一部で心配されているダムや電力などの制御系システムについては、インターネットなど外部ネットワークには直接接続していないと報告されているようだ。

現状の問題点は。

吉原氏：セキュリティーポリシーのガイドラインも重要だが、きちんと技術基準も決めるべきではないかという指摘がある。たしかに海外の主要国を見ると、どの国も技術基準をしっかり作っているが、日本では各省庁に任せている。極論すれば、発注先のベンダー任せになってしまっているというのが現状だ。しかし、こうした技術基準を作ろうとすると専門家がたくさん必要で、予算の問題も生じてくる。さまざまなセキュリティー対策をどこまでやるかは、コストとの兼ね合いもあり、そしてまた政府がどこまで個人のプライバシーなどに介入するのかという問題もある。政治の問題になってくるのではないか。

米国では実地演習で評価や問題点を洗う

サイバーセキュリティー先進国に学べ

国防総省へアタックの実演習

冒頭に述べたように日本に比べて米国のサイバーセキュリティー対策は、圧倒的な深みと物量、そして歴史の長さがある。先進国から学ぶことは何であろうか。

サイバーセキュリティー対策の黎明期でもっとも有名なのは、1997年に国防総省が行った「エリジブルレシーバー」（資格がある応戦者）と呼ばれる演習だ。30人のエキスパートを選抜し、市販のPCと一般的なプロバイダーを使って国防総省のコンピュータに侵入できるかどうかをテストさせた。30人は3か月の準備期間を与えられ、その結果40回にわたって国防総省に侵入できた。

この衝撃的な演習の結果が、その後の米国のサイバーセキュリティー対策を大きく推し進める要因となった。翌1998年当時にはクリントン大統領が米国のシステムがサイバーテロに対してどの程度脆弱なのかを評価するように要請した。これに応え、国家安全保障会議（NSC）が国家計画を作り、そして翌1999年には議会に対して14億6,000万ドルもの巨額のサイバーテロ対策費の拠出を求めた。

こうした積極的な政策は、大規模な事件がきっかけになってさらに進められることになる。その最初のターニングポイントは、2000年2月に著名な企業サイトで起きたDDoS（分散型サービス拒否攻撃）事件だった。Yahoo!やeBay、CNNなどの大手ポータルサイトやニュースサイトが軒並み攻撃を受け、40時間以上にわたってシステムダウンした。この事件に米政府は大きな衝撃を受け、2001年度の予算案ではサイバーテロ対策費を前年比15パーセント増加して20億ドルが計上された。

「デジタルパールハーバー」防止へ

そして、第二のターニングポイントは9.11同時多発テロだった。この事件以降、サイバーテロに対する米国市民の関心は急速に高まったと言われる。「世界貿易センターに対する複雑で高度な攻撃を可能にしたアラブテロリストであれば、同時にサイバーテロを実行に移すこともあり得ない話ではない」という見方がマスメディアなどで頻繁に紹介された。米政府もこうした世論に押されるように、テロ事件直後の2001年9月末にサイバースペース安全保障担当大統領補佐官を新設した。初代補佐官に任命されたリチャード・クラーク氏は「太平洋戦争時の真珠湾奇襲に相当するようなサイバー攻撃が起きる可能性がある」と訴え、「デジタルパールハーバー」とぶち上げて危機感を煽った。

クラーク補佐官の政策で有名なのはガブネット（Govnet）構想で、米国内のすべての政府機関を専用回線網で結んでしまおうという計画だ。クラーク補佐官は、既存のインターネットはコンピュータウイルスやDoS攻撃に対して脆弱で、新たな専用網を作らなければならないと主張した。とはいえ、この意見に対しては「いくら専用網を作っても、たとえばフロッピーディスクからウイルスは侵入するし、攻撃を完璧には防げない」「新しい専用回線網を立ち上げるには莫大な費用が必要だ」などの批判も数多く出ている。

最近では、海軍大学が演習「デジタルパールハーバー」を実施している。約100人の参加者は、ロードアイランド州の海軍大に参集し、テロリスト役を割り振られたメンバーが重要インフラに対するさまざまなサイバー攻撃を計画立案し、かなりの成功を収めたという。だが同種の攻撃を実際に敢行しようとすると、数億ドルもの資金や長い準備期間がかかることも判明した。現実性の観点からはかなり疑問のある結果となった。

サイバーテロ対策に対するこうした疑問は最近の米メディアでも目立つようになってきている。システムに侵入するのはきわめて高度な技術が必要で、果たしてテロリスト側がそのようなややこしい方法を採用するだろうか。爆弾を投げた方が簡単で効果的ではないか――という見方だ。P120に挙げたように、今後は爆弾やハイジャックなどリアルなテロリズムの手口と、サイバーテロのハイブリッド型攻撃にどう対処するかが米国でもおもなテーマとなっていくのかもしれない。

米国のサイバーセキュリティー対策に関するおもな出来事

年	内容	
1997年	「エリジブルレシーバー」を実施	国防総省がエキスパートを選抜して省内のコンピュータにアタックをかけさせる演習を実施
1998年	サイバーテロ対策費の拠出	国家安全保障会議が議会に対して14億6,000万ドルもの巨額の費用拠出を求めた
2000年	大手企業ウェブサイトにDDoS攻撃	Yahoo!やeBay、CNNなどの大手ポータルサイトやニュースサイトが軒並み攻撃を受け、40時間以上にわたってシステムダウン
2001年	サイバースペース安全保障担当大統領補佐官を新設	リチャード・クラーク氏が初代補佐官に任命され、Govnet構想などを次々に打ち出す
2002年	演習「デジタルパールハーバー」実施	海軍大学に調査会社のガートナーが協力し、重要インフラに対してサイバー攻撃が行われた場合の対応策を考える演習を行った

どこまでセキュリティー対策を行えばいいのか

今後の日本における大きな2つの課題

人事異動とともにポリシーも変化

さて、こうした現況を踏まえて日本政府のセキュリティー対策を考えると、2つの課題が見えてくる。

1つは、セキュリティーポリシーをどう運用するかという問題だ。常に語られ続けていることだが、ポリシーは作っただけでは何の意味もない。中央官庁では人事異動でポリシーの運用が変わってしまう問題が起きている。

また「同じ省内でも部署によって対応がばらばらになっている」という指摘もある。最近はダウンサイジング化に加え、電子政府の効率的運用が求められるようになり、各部署が独自にサーバーを導入してシステムを構築、運用するケースが増えてきている。各省庁内にある膨大な数の部署がそれぞれきちんとセキュリティポリシーを運用しているかどうかを評価するのは、簡単なことではない。

情報セキュリティーアナリストの古川泰弘氏は「実効力があるサイバーセキュリティー政策がさっぱり見えてこないことに不安を覚える。積極的な情報収集や分析が不十分なため、脆弱性情報が海外のセキュリティー機関よりもワンテンポ遅れてアナウンスされているのが現状だ」と話す。情報収集にしても相変わらず「有識者」の名の下に、政府諮問機関に企業の経営者が呼ばれてセキュリティー対策を話すといったことが平気で行われている。古川氏は「生の情報が加工処理され、調理されたセキュリティー情報からハッカー対策を議論している。刺身を研究して魚の釣り方を検討しているようなものだ」と指摘する。「同時多発テロとイラク戦争を経験した米国は、政府から民間までセキュリティー意識が広まりつつある。日本でも今後はポリシーを策定するだけでなく、効果が見えるセキュリティーガイドラインを作って実践する段階に来ているのではないか」と訴えている。

安全保障との兼ね合いと巨費負担

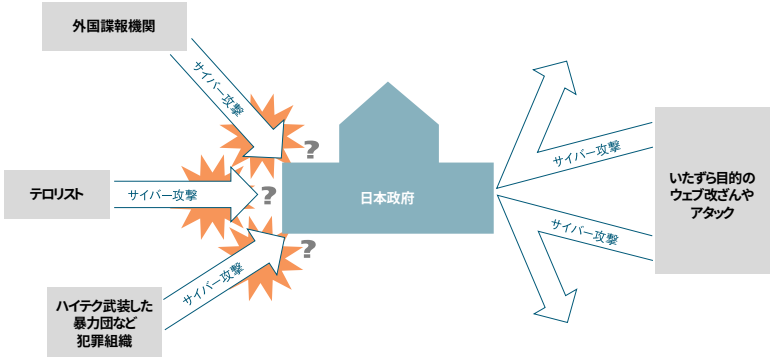
もう1つの課題は、サイバーセキュリティー対策と安全保障との関連をどう位置づけるのかという政治的な問題だ。

吉原参事官は「日本政府のセキュリティー対策は、一般的な役所のレベルという中では米政府とさほど遜色のない程度にまでなっている。だが機密情報を扱う部署などの対策は、レベルから規模から足下にもおよばないかもしれない」と言う。日本政府の現時点でのセキュリティーは、既存のハッカーツールを使ってウェブサイトの改ざんを行うようなレベルには対処できるが、組織化されたテロリストや外国の諜報機関が行う高度な侵入や攻撃には耐えられるレベルにはないということだ。

だが、こうした攻撃への対策を本気で進めようとすれば、巨額の予算と時間が必要になってくる。たとえば侵入技術を持っていると見られるテロリストや犯罪グループを24時間態勢で監視や盗聴するなど、公安当局が過激派などに行っているのと同じレベルの態勢が必要になってくるということだ。こうした対策を政府がもし進めようとすると、巨額の予算をどう捻出するのかという問題が生じるのと同時に、世論が果たしてどの程度にまでこうした対策を容認してくれるのかという問題も起きてくる。つまり、米国と同じような防諜機関を保有し、エシュロンやカーニヴォアと同じような方法で通信データを盗聴するのか。そして米国と同じような徹底的な監視社会化を進めるのか――大げさに言えば、そうしたことにまで議論は踏み込まなければならなくなる。本格的なサイバーセキュリティー対策はそうした政治的な議論と不可分だ。

プロフェッショナルな侵入や攻撃のリスクは少ないとはいえ、決してゼロではない。外国の諜報機関やテロリストが狙ってこなくても、暴力団などの組織犯罪がそうした行為に手を染める可能性もある。ある政府関係者は、こんなふうに語っている。「結局のところ、大きなサイバーテロ事件が実際に起きて初めて政策をどうするかという本格的な議論が始まるのかもしれない。正直に言えば、海外でそうした事件が起きてくれれば日本政府もそれを教材にできるのだが……」。

いろいろな攻撃にさらされる危険をかわせるか



［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