伊藤穣一の
フューチャースケープ

ROUND2　あのテロがつきつけたセキュリティーの意味

連載を始める前から「サイバーテロとセキュリティー」というテーマは取り上げる予定だった。今度の同時多発テロ事件が起きる前なら「放っておくとタイヘンな事件が起こるよ」と警鐘を鳴らしておけば済んだんだろう。だけど、実際に最悪の形で現実化してしまった今、どういうことが言えるだろう。『インターネットマガジン』に載るのだから、「サイバー」の面に集中したほうが適切なのかもしれない。でも今回はテロやセキュリティーについて、もう少し大きな流れの中で考えてみたいと思っている。

協力・関 聡司
構成・先田千映
Photo : Nakamura Tohru (mermaid)

まず結論から言うと、今僕がなにに違和感を感じ、なにを心配しているかというと、テロの後に来る反動だ。

あえて煽るような言い方をしてしまおう。今回のような事件はたいしたことじゃない。資金さえあれば、誰にでもできるだろう。

誤解しないでほしい。人道的に許されないことであるという事実を保留して、まず「あの行為」自体はそんなに難しいものではなかったということを、ここで再確認して話を進めたいだけだ。

あの行為をブロックすることは不可能だっただろう。現在考え得るすべてのセキュリティー対策を講じたとしても、本当に難しい。今回の事件を本当に回避できるようなセキュリティーというのは、そもそも存在するんだろうか？

サイバー領域のテロ対策として、着手しやすいところでは、暗号の規制があるだろう。テロリストのコミュニケーションを遮断する効果が期待できる。ただし、規制したらテロリストが暗号を使えなくなるかというと、当然ながらそんなわけはない。米諜報機関NSAの盗聴システム『エシュロン』(※1)は赤十字とかアムネスティーとか、およそテロリストとは関係ない組織のコミュニケーションも傍受して政治的に利用しているという話だけど、彼らのようなNGOは、たとえ暗号を使っていたとしてもごく弱いものだ。ビンラディンの組織のようなテロリストが使う暗号は、一説では画像データに情報を埋め込むステガノグラフィー方式のものだというし、一般的にもPGP(※2)のような強い暗号がすでに流通している。

今後、新しい暗号規制の動きが具体的に出てくるだろうけど、暗号規制自体はキーエスクロー(鍵預託)に関する議論が1997年ごろに終息を迎えた時点ですでに破綻しているともいえる。このとき、自由に暗号を復元する権限を政府に与えるキーエスクローまたはキーリカバリーは、誰がどうやって集中管理するのかという安全

性の面でも、それからコストの面でも非現実的で、時代錯誤な考え方として葬り去られている。

むしろ、デジタルデータによる通信傍受については、捜査機関の権限を強くすることが優先されるだろう。要するに「暗号を使ってもいいけど、こっちの力も強くなるよ」ということで、この動きを象徴するようなできごとがすでにアメリカで起きている。FBIがマフィアの構成員のコンピュータになんらかの仕掛けをつけ、打ち込まれるデータを盗聴して、裁判に証拠として提出したというケースだ。ところが、これは日本もそうだけれど、犯罪捜査においては証拠入手の手順を公開することが原則になっている。この場合、FBIは「デジタルデータはこの原則から外れる。なぜならその入手手段、つまり仕掛けが“国家機密”だから」と主張している。

物理的なテロ対策で真っ先に挙げられるのが空港のセキュリティーだ。

たとえば空港内で写真付きIDの提示を要求される。実はこれは主に航空券の流動性を阻害する目的、つまり他人のチケットを使えないようにするために航空会社がやってきたことだという人もいるぐらいで、ビジネスの一部でもあるわけだ。しかし考えてみれば資金力と組織力のある本物のテロリストなら偽造IDなんて簡単に手に入る。こんなことで乗客に架空のセキュリティー感覚を印象づけておいて、本来やるべきゲートでの身体検査はお客が面倒くさがるからまあほどほどにというのは、かなりお寒い状況だといえるだろう。

テロ対策は国も企業も一緒にやらなきゃいけないんだけど、政治的ニーズとビジネスのニーズが微妙に食い違っている。本質的に必要なことの周辺で、いろんな立場の人がそれぞれ自分の損得を考えている――現状はそんなところだ。

現実にテロ対策として形になってきているのは、まったく別のところだ。アメリカでもリベラルなほうの人たちが今いちばん危惧しているのは、さっきも言ったけど、米国内で捜査機関の権限が肥大化すること。盗聴も令状なしで可能、外国人の不当な拘留も正当化――アメリカの自由のためにアメリカの自由が失われるという皮肉な状況が予測されている。

これまでプライバシーをめぐっては、人権活動家と捜査機関（FBIやらCIAやら）がバトルを繰り広げてきたわけだけど、こんな事件が起きたせいで「ほら言ったでしょ」と捜査機関の意見がなし崩し的に通ってしまうかもしれない。

ともあれ、やはり国家レベルのテロ対策のメインになるのは、「情報」だろう。要注意リストに挙げられている主要なテロリストが、今世界のどこにいて、誰と話をしているのかという位置の把握、それから資金の流れの把握が最大の防御策になる。

テロにはお金がかかる。ただし、テロリストが資金を手にする手段は多様化している。だいぶ前に、eBayがDoS攻撃（※3）を受けて株価が暴落したことがあったけど、これも考えてみればテロリストの金儲けの手段になる。あらかじめ暴落を知っていれば株の空売りでひと財産作れるからだ。今回のテロ事件でも、すでに調査は始まっているけど、コストを回収するくらいのマネーゲームはできたはず。つまり、テロリストが脅迫や寄付ではなく金融市場で資金を得ることができるということだ。

テロリズムがビジネスになりつつあるというのはひとつの傾向かもしれない。フィリピンなどで起きている小さなテロ事件では、身代金目的にシフトしているケースが多いということだし。

これまでは「人を殺せる力がある」ということを誇示しながら、自分たちの要求を通していき、政治的な目的を達成するというのがテロの定義だった。そこには国家との駆け引きがあった。

デジタルデータは証拠入手の手順公開の原則から外れる。なぜならその入手手段が“国家機密”だから

今回は話が違う。要求貫徹のためのテロ行為じゃなくて、ただの仕返しだ。駆け引きもなにもない。イランをやっつけるためにイラクを軍事支援して、力をつけたイラクがクウェートを侵攻したら空爆して、というようなことを繰り返して、反米感情をどんどん浸透させていったせいで、ここまで事態がこじれてしまった——こうなると、最大のテロ対策は「嫌われないこと」だとしか言いようがない。

貿易センタービルやペンタゴンに旅客機が突っ込む。こんなことさえ可能なんだから、東京証券市場をダウンさせるとか、日本中停電にするとか、原発を爆破するとかだって、組織と資金のあるテロリストが本気になればできてしまうだろう。いろんな手段を講じてセキュリティーを高めても、「本気」の人間から守りきることはできないということだ。

繰り返しになるけれど、テロの時代、最大の自衛策は「嫌われないこと」に尽きる。嫌われるようなことをしても強いから大丈夫、ということはあり得ない。現に十分に強いアメリカがやられてしまったんだから。

サイバーテロに関しても同じことが言える。とはいえ、「嫌い」じゃないのに攻撃してくる人たち、つまりちょっとしたデータを盗んだりサイトを荒したりするクラッカーとかからシステムを守ることは十分可能だし、そういう金銭目的とか、自己顕示欲が強いだけの有象無象の犯罪者から100パーセント守りきれるようじゃなければ、そもそもセキュリティーとは言えない。

しかし、資金と組織をもつ「本気」の人間を完全にブロックするなんてことは不可能だ。ブロックしきれなかった時に受けるダメージを最小限に抑えるために、システムを分散したりレスポンスを効率化したりということが重要になってくる。

インパクト的には今回ほどの事態を引き起こすのは難しいとはいえ、サイバーテロでも人は殺せる。たとえばすでに起きている事件では、米国陸軍のデータベースに侵入して血液型のデータを改竄するということが起きている。これが戦争中にでも起きていればかなりの被害が出ているだろう。オーストラリアの病院ではカルテが改竄されて現実に人が死んでいる。

しかし現実面では物理的なテロの補助あるいはインフラとしてネットを使うというのが主流だろう。コミュニケーションの手段としてだけではなく、GPSのシステムをクラックしてミサイルの着弾を妨害するということも起きている。インパクトとしては物理的なテロに及ばないといっても、サイバーテロを甘く見るのは危険だ。その点で日本の対応はまだまだというところだろう。

日本はサイバーテロに関しても、物理的なテロに関しても、踏み台として利用される可能性が非常に高い国だ。経済的な豊かさがテロリストを惹きつけるわけじゃなく、情報に対する考え方の甘さだ。たとえば世界のほとんどの国では「スパイは死刑」が原則だけど、日本にはスパイ行為を裁く法律が実質的に存在しないから、スパイ業界の方には人気らしい。

テロの温床として利用されないために日本政府が取るべき対応には大きな壁がある。住民基本台帳法、一般的には「国民総背番号制」として受け止められているID制度に対する感情的な反発だ。しかしこの制度はテロリストや組織犯罪に対するデータマイニング、プロファイリング、トラッキングの面ではすごく有効なツールになるはず。資金の流れから人の流れまで、有効に追跡できる。

問題なのは、「背番号」に対する感情的な反発じゃなくて、自分が知らないうちに犯罪者候補や潜在的テロリストのリストに加えられる危険性だろう。借りてるビデオの趣味がヘンとか、携帯の番号を前に使っていたのがテロリストだとか、そんなドンブリ勘定で不審人物リストに名前を載せ

サイバーテロで人は殺せる。オーストラリアの病院ではカルテが改竄されて現実に人が死んでいる。

られて、それを孫の代まで引きずられるなんてたまったもんじゃない。しかもguilty by association――付き合いがあるゆえに有罪――の原則で、たとえば会社に1人テロリストがいれば、社員全員の経歴に大きく真っ赤なバツが付くことになる。

もうひとつ大きな問題が、ID盗難の問題。今度のテロ事件でも、FBIが犯人として公開したうち2人の名前が、過去にパスポートを盗まれた人のものだとわかっている。たとえ自分がやったことではなくても、自分の名前で爆弾の材料を買われたりすれば、いやおうなくテロリストの世界に巻き込まれてしまう。

今回の事件ではいろんな国でIDカード携行を義務づけるような動きがあるし、日本でも国民総背番号制を是認する動きが出てくるかもしれない。でも、こういうリスクの大きさを考えれば、そう簡単には結論の出る話じゃない。

テロ対策はプライバシー侵害と表裏一体。厳しく締めつければいいという問題じゃない。だから今確実に言えることで、本当に大切なのは、ネットワークセキュリティーをみんながもっと気にするとか、航空各社がそれぞれにセキュリティー体制を整備するとか、個々の企業や個人が意識することで、全体の危機管理レベルを底上げすることだ。その支援は、たとえば教育を通じて政府がやるべきことだろう。でも、政府がテロ対策をあたかも秘密プロジェクトのように進めるというのは危険だと思う。

この話の結論は出ない。やはり僕の中でも矛盾がある。テロリストから守ってほしいという気持ちと、プライバシーを守りたい気持ちと。ただ、僕に言えるのは、結局は「嫌われないこと」が最大の防御だということ。それから分散型の波状テロ攻撃への免疫を高めなきゃいけないということ。すべて受ける側の個々人がセキュリティー意識をもち、そしてそれをどう集約していくかにかかっている。

【用語解説】

※1 エシュロン
長い間その存在の有無がベールに包まれていた米国の国家安全保障局（NSA：National Security Agency）が開発した盗聴システム。全米でだけでなく、世界中の電話や電子メールなどの通信を盗聴しているといわれている。

※2 PGP
Pretty Good Privacyの略で、人権保護に強い関心を持つプログラマー、フィル・ジマーマンが開発した公開鍵方式の暗号を使った暗号化ソフトウェア。このソフトウェアの登場で、誰もが自由に暗号を使って通信ができるようになった。主に電子メールのやり取りに使われる。

※3 DoS攻撃
Denial of Service、つまりサービスの提供を不能にする攻撃。あるウェブサイトに非常にたくさんのリクエスト送りつけ、ウェブサーバーをレスポンス不能にさせる。昨年、米ヤフーや米eBayが攻撃の対象となった。

from Joi's Diary
Jump www.neoteny.com/jito/

【2001年9月10日】

ホテルオークラでDACの上場記念パーティー。懐かしい顔ばかり。一番最初に代理店の皆さんと一緒に会社を作るかどうか考えるためのFSプロジェクトに参加したとき以来会ってなさそうな人もいた。それから考えるとあっという間にこんなに大きくなったんだと感動しました。

※この記事に関するサイトへのリンクをJump www.neoteny.comに掲載します。

［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