“ 今月 ”を理解する

メディアレビュー MIX

9.11のテロからすでに2年が経ってしまった。その間、次には大規模なサイバーテロが起こるという緊張感は薄れてしまっている。はたしてサイバーテロなど永遠に起こらないのだろうか？ もしかしたら他人事のウイルス感染がサイバーテロなのか？ 今回は、リアリティーをもってサイバーテロを感じられるメディアを紹介する。

text: 松尾乗介（Press Archives）

今そこにあるサイバーテロの現実味を実感する

MEDIA REVIEW MIX

ハッキリと浮かび上がるサイバーテロのリアリティー

The copying-with method NO. 1

『ブラックアイス――サイバーテロの見えない恐怖』
9.11同時多発テロ以降のテロ環境の中で、サイバーテロの脅威に焦点を当てて「見えない敵」との戦いにどう対処すべきかを説いている。

著者：ダン・パートン著
訳者：星睦
インプレス

サイバーテロという言葉がリアリティーをもって語られるようになったのは、2001年の9.11同時多発テロがきっかけだった。航空機がマンハッタンの超高層ビルに激突するなどという絵空事が現実になるのなら、サーバーテロだって決して空想の物語ではない。

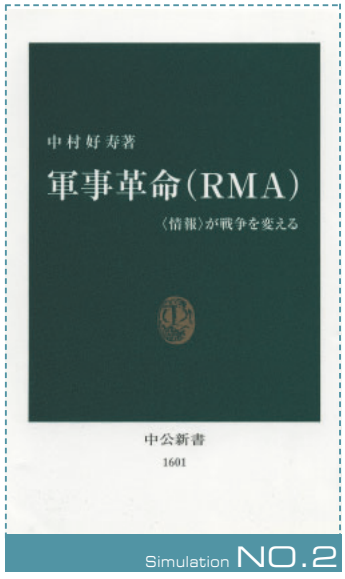
テロが起きた直後、ブッシュ大統領のサイバースペース安全保障担当特別補佐官に任命されたリチャード・クラーク氏の登場も、“ サイバーテロ狂騒曲 ”に拍車をかけた。クラーク氏は「デジタルパールハーバー」といったキャッチーな言葉を多用して危機を煽り、米国の世論を震撼させた。

しかし9.11から2年が経ち、サイバーテロの脅威はいつしか風化していく。深刻なコンピュータウイルス感染やウェブ改ざん事件は起きているものの、本来的な意味でのサイバーテロリズムが出現していない状況では、風化は仕方ないと言えるだろう。米メディアでは「サイバーテロの脅威は本当なのか？」と疑問を投げかける報道も現れ始めている。「テロリストがわざわざ面倒な不正アクセスに本当に挑戦するのだろうか？　困難きわまるテクニックを使って上水道システムに侵入するより、毒薬を浄水池に投げ込む方が簡単では？」というわけだ。

そんな状況の中で登場したこの本は、サイバーテロの現実的な危険を詳細かつ実証的に浮かび上がらせている。たとえば、かねてからその危険性が指摘されてきたSCADA（計測データ監視制御）。水道や電力、工業プラントなどのデータを一元管理し、遠隔制御するシステムの総称だ。全世界に数百万もの単位のSCADAシステムが存在するとされ、たとえば電力系だけでも市場規模は数千億円に達するとされている。SCADAが侵入され、乗っ取られれば、ダムの水位や電力、水道の供給などを自在にコントロールできてしまう。

「ブラックアイス」では、さまざまな関係者や専門家に取材したうえで、SCADAの脆弱性について詳細にレポートしている。SCADAについては、同時多発テロを引き起こしたとされるアルカイーダも注目していたとされている。米軍がアフガニスタンに進攻した際、首都カブールにあったアルカイーダのアジトからSCADAの資料が発見されたのだ。

アルカイーダがどのようにしてインターネットを利用し、構成メンバーがどの程度のスキルをもっているのか――そんな疑問にもこの本は答えてくれる。最新のサイバーテロの情勢を俯瞰することができる数少ない本だ。



Simulation NO.2

『軍事革命（RNA）』
相手を消耗させる戦いから、麻痺させる戦いへ——これからの戦争がどう変わっていくのかをシミュレーションによって描き出していく。

著者：中村好寿
中公新書

外国の軍隊が九州に侵攻 日本が一瞬で崩壊するシナリオが見える

米軍は1991年の湾岸戦争の直後から、サイバーテロを含む軍事のIT利用について本格的な研究を開始したとされる。その集大成がイラク戦争だった。開戦前の電子メールを使った攪乱工作や、実戦に投入された無人偵察機、電磁パルス爆弾などの“IT兵器”の登場は、ニュースに釘付けとなっていた世界の人々を驚かせた。

翻って、日本。ようやくここに来てサイバーテロに関する調査費が予算に計上されるようになったというものの、その実態はかなりお寒い。専門家がほとんど育っていないからだ。

筆者は97年にサイバーテロに関する取材を防衛庁に申し込んだことがある。だが防衛庁自体がサイバー戦争のことをよくわかっていない。関係者へのリサーチを繰り返し、ようやくたどりついたのが、自衛隊でただ1人のサイバーテロ研究者だった中村好寿一佐だった。中村一佐は当時、防衛研究所の主任研究員だった。

中村一佐はその後防衛庁を退官し、現在は軍事アナリストとして活動を続けている。本書は、9.11同時多発テロが起きる直前の2001年8月に発行された。

圧巻は、IT武装した外国の軍隊が九州に侵攻したらどうなるのかを想定したシミュレーションだ。自衛隊が九州沿岸に部隊を展開し、あくまで物理的な戦術に頼ろうとするのに対し、敵は東京証券取引所や東京駅の輸送司令センター、NTTの中継所などにサイバー攻撃をしかけ、日本の頭脳部分を大混乱に陥れてしまう。「現在の日本の防衛戦略は、工業化時代の戦争論に基づいており、情報化時代に適合したものではない」というのだ。

MEDIA REVIEW MIX

生物・化学兵器や麻薬密売と 並列の威力をもつサイバーテロ

9.11同時多発テロは「非対称戦争」だと言われた。米国という圧倒的な軍事力と戦うには、サイバーテロなど少人数によるゲリラ的な方法を採用するしかないという考え方だ。非対称戦争という概念が知られるようになったのは、この本がきっかけだ。「超限戦」は中国人民解放軍の現役の将校2人によって1999年に書かれ、中国大陸だけでなく、台湾や香港などでベストセラーとなった。米国でもワシントンポスト紙などで紹介され、軍事専門家の注目を集めた本だ。

そのコンセプトはあまりにも明快だ。超大国アメリカ合衆国との戦争に勝つためには、生物・化学兵器やサイバーテロ、麻薬密売などのありとあらゆる方法を動員しなければならない——というものなのである。グローバル化と技術の統合を特徴とする21世紀の戦争は、すべての境界と限度を超えた“超限戦”となる。あらゆる領域が戦争となり、軍人と非軍人、軍事と非軍事の境界は消滅するという。そして、それは超大国と戦うには、一般市民をも巻き込んだテロしかないという危険な思想でもある。

出版当時、米国と中国の間で緊張が高まっていたこともあり、中国は対米国軍事戦略としてサイバーテロを計画しているのではないか、という見方がこの本によって高まった。中国が実際に対米テロリズムを起こすことはなかったが、2年後に起きた同時多発テロによって、この本がさらに大きな注目を浴びるきっかけとなった。アルカイーダの指導者であるオサマ・ビン・ラディンが打ち出した論理は、『超限戦』の主張とほぼ同じ内容だったからだ。この本がテロリズムの世界に与えた影響は、はかりしれないと言える。

Military teaching materials NO.3

『超限戦——21世紀の新しい戦争』
中国人民解放軍の軍事教材として書かれ、その新たな戦争のあり方が世界に衝撃を与えた。

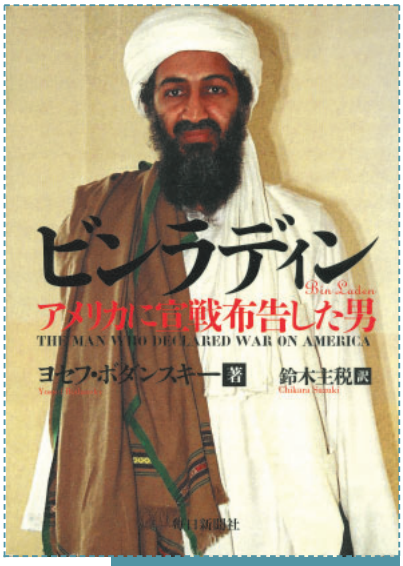
著者：喬良・王湘穂
訳者：劉琦
共同通信社

メディアレビュー
MIX

米国防総省の元顧問が語る テロリストのインターネット的つながり

オサマ・ビン・ラディン率いるテロリスト集団、アルカイーダ。その組織は特にロンドンを中心とするヨーロッパ全域にひそかなネットワークを張り巡らしているとされている。ビン・ラディンは当初、衛星携帯電話などを使って指示を出していたが、米国家安全保障局（NSA）がエシュロンを使って電話を傍受していることに気づいてからは、連絡手段をインターネットに移行させた。さまざまな暗号に加え、ウェブの画像や音声ファイルにメッセージを埋め込むステガノグラフィーなども多用しているとされている。同時多発テロの直後には、アルカイーダのキャンプで訓練を積んだ33歳のチュニジア人が構築していたテロリストネットワークの1つが暴かれ、捜査当局によってイタリア・ミラノのアジトが急襲されたこともあった。アルカイーダのこうした痕跡は、日本国内でもわずかながら確認されたことがあるという。テロリストのネットワークはきわめてグローバルな規模で展開されているのだ。

米国防総省の元顧問、ヨセフ・ボダンスキー氏が書いたこの本は、オサマ・ビン・ラディンを中心とするイスラム原理主義のテロリストたちがどのようにして各地にネットワークを張り巡らせていったのかを、豊富な機密情報をもとにして描き出している。源流は1979年に起きたソ連のアフガニスタン侵攻にあり、ここでゲリラ戦を勝ち抜いたイスラム教徒たちがその後、戦友のネットワークを形成してボスニア・ヘルツェゴビナやコソボ、チェチェンへと転戦していき、やがて巨大なテロ集団を作り上げていったのだという。圧倒的な迫力に満ちた本である。



Analyst report NO.4

『ビン・ラディン……アメリカに宣戦布告した男』
米ワシントンのシンクタンク、国際戦略研究協会（ISSA）研究部長を務めるアナリスト、ヨセフ・ボダンスキー氏がビン・ラディンという人物の全容に迫った。

著者：ヨセフ・ボダンスキー
訳者：鈴木主税
毎日新聞社

MEDIA REVIEW MIX

Analyst report NO.5

『21世紀の戦争――コンピュータが変える戦場と兵器』
英サンデータイムズでワシントン支局安全保障担当記者、支局長を務め、その後UPI通信のCEOになった著者が、ITと軍事がどう結びついていくのかを描き出す。

著者：ジェイムス・アダムス
訳者：伊佐木圭
日本経済新聞社

ITと兵器のつながり それがもたらす新しい国際“緊張”関係

ITと軍事が結びつき、戦争の世界に大きな革命を起こしている。サイバーテロと呼ばれる不正アクセスやコンピュータウイルスなどによる攻撃は、その“革命”の1つの表れでしかない。この革命はRMA（Revolution in Military Affairs）やIW（Information Warfare）といった言葉で呼ばれている。俗っぽい言葉で言えば、サイバーウォーだ。

RMAが最初に実戦に投入されたのは、1999年のユーゴスラビア空爆だったと言われている。米軍の爆撃機が在ユーゴ中国大使館を誤爆する事件が起き、米中間が一触即発となった。だが実は中国側が米軍のデータベースに侵入して中国大使館の位置とユーゴの軍事施設をこっそりと入れ替え、あえて自国の大使館を誤爆させたのが真相だった――そんなまことしやかな情報が流れたりもした。誤爆させることで、対米折衝を有利に進めさせようとした、というのだ。

1998年に書かれたこの本は、90年代の世界情勢の中でサイバーウォーがどのようにして実戦に導入されていったのかを克明に描いている。コンピュータ専門家の“遊び”のようなものだった不正アクセスを、米政府がどのように取り込み、国家の貴重なリソースとして扱い、軍事戦術として利用していったのか。米国家安全保障局（NSA）が暗号をどう使い、他国の暗号解読を進めていったのか。著者は「これは情報戦兵士、電子の騎士（サイバーナイト）の世界なのだ。戦場の優位を争うのは砲弾ではなく、ビットやバイトの力なのだ」と書く。

ITが軍事に与えたインパクトを、ジャーナリストらしい克明な筆でビビッドに描き出したノンフィクションである。

Cyber-criminal movie NO.6

『ソードフィッシュ』
政府の闇資金を奪おうと狙う元スパイ。それを手伝う元ハッカー。スピード感あふれるハリウッド・アクション。

ジョン・トラボルタ主演
ドミニク・セナ監督
ワーナーブラザース配給
2001年米国映画

ハリウッドが描く華麗なるサイバーテロは セキュリティー感覚までも麻痺させる

凄腕ハッカーだった主人公。捜査当局に摘発され、コンピュータに一切触れてはならないという裁判所命令を受け、隠遁生活を送っている。史上最強のハッカーと言われたケヴィン・ミトニックを彷彿とさせるこの主人公に、イスラエル・モサドの元スパイが米麻薬取締局（DEA）の裏資金を奪おうという計画を持ちかける――。

サイバーテロ的なプロットが登場する映画は数多いが、その典型が「ソードフィッシュ」だ。のっけから驚かされるのは、ジョン・トラボルタ扮する元スパイの前に、主人公が連れてこられるシーン。トラボルタは国防総省のログイン画面が表示されているデルのノートPCを主人公の目の前に置き、「凄腕ハッカーなら60分で侵入できると聞いたが、60秒以内で侵入してもらおう」と銃を突きつける。

主人公はあわててキーボードに向かい、ものすごい勢いでタイピングを始める。画面にはありとあらゆるIDらしき文字列が表れ……つまり、主人公は手作業で辞書アタックを仕掛けて突破を計ろうとしているようなのだ！　60秒後、ぎりぎりになって当てずっぽうのID、パスワードの1つがヒットし、無事主人公は国防総省にログインできてしまう。

おまけに、国防総省のログイン画面には麗々しく「DES 128 BIT ENCRYPTED SECURITY」と掲げられているのだ。ずいぶん侵入者に親切なインターフェイスではないか。

サイバーテロがこんな風に通俗的に描かれている限り、セキュリティーの本質をきちんと一般社会に理解されるのは難しいようにも思える。

ハクティビズムの嵐を インドとパキスタンの間からのぞき見る

サイバーテロの定義とは何だろう？　かつて自分の事務所のパソコンがコンピュータウイルスに感染してしまい、ウイルスメールをまき散らした挙げ句に「わが事務所がサイバーテロ攻撃された」と大騒ぎした衆院議員がいた。こんなケースは論外としても、どのレベルまでの攻撃をサイバーテロに含めるのかは、微妙な問題だ。狭義には、電力や水道、政府施設など重要インフラへの攻撃がサイバーテロと定義されている。この定義においては、日本でも頻繁に起きているウェブ改ざんなどはサイバーテロには含めない。

ウェブ改ざんは、テロではなくハクティビズムとしてとらえられている。ハクティビズムというのは、ハッカーとアクティビズム（行動主義）をかけ合わせた造語。政治的メッセージをアピールすることを目的に、不正アクセスによってウェブを改ざんする活動を指す。日本でも数年前、日本政府の南京大虐殺の扱いに抗議する中国人ハッカーたちが大挙して総務庁や文部省のウェブサイトを改ざんし、大きな騒ぎとなったのは記憶に新しい。

しかしこうしたハクティビズムがもっとも盛んなのは、インドとパキスタンだ。カシミールの国境紛争や核開発競争などを見ればわかるとおり、長年にわたって対立を続けている両国の間では、ウェブ改ざん攻撃も頻繁に起きている。その実態を克明にレポートし続けてきたサイトが、シンガポール在住のインド人が運営しているこの「Project India Cracked」だ。残念ながら新たな活動は休止してしまっているものの、印パ両国で激化するハクティビズムの嵐がどのようなものかを詳しく知ることができる。

The report of cyber-war NO.7

『Project India Cracked』
対立が続くインドとパキスタンの両国の間で続く“サイバー戦争”の実態を、日々追い続けている貴重なウェブサイト。

URL http://www.srijith.net/indiacracked/index.shtml

［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