NPO ISEF
Not-for-Profit Organization of Information Security Forum

特定非営利活動法人
NPO情報セキュリティフォーラム

NPO-ISEF 情報セキュリティレポート：2011-No.07

最近のサイバー攻撃と法的課題

情報セキュリティ大学院大学
林 紘一郎（Hayashi Koichiro）
湯淺 墾道（Yuasa Harumichi）

【著者経歴】

■林 紘一郎

1941 年生まれ。NTT アメリカ社長などを経て、1997 年慶應義塾大学教授。2004 年情報セキュリティ大学院大学の設立に参画。副学長を経て 2009 年から学長。『セキュリティ経営』（共著）など著書多数。

■湯淺 墾道

1970 年生まれ。青山学院大学法学部卒業、慶應義塾大学大学院法学研究科政治学専攻博士課程退学。2008 年九州国際大学副学長。2011 年情報セキュリティ大学院大学教授。九州大学大学院、中央大学大学院など非常勤講師。情報法、選挙制度などを専攻。

1． サイバー攻撃と APT

情報セキュリティのインシデントには、意図的なもの（例、意図的な侵入や破壊などの攻撃）と、意図せざるもの（例、過失による情報の流出）とがある。後者は、古くからあると同時に、技術が進歩してもゼロにすることは難しい。他方前者は技術に依存しているので、攻撃と防御の新しい手段が開発されて、年々様相を異にしている。

2010 年の初め頃からは、標的型サイバー攻撃という言葉が、ジャーナリズムを賑わしている。まず同年 1 月早々に「オペレーション・オーロラ」という攻勢がグーグルをはじめとした、多分野にわたる多数の企業に仕掛けられた。6 月には、それまで安全と信じられてきた制御システムでも、Stuxnet というコンピュータ・ウイルスがジーメンス社の SCADA（Supervisory Control And Data Acquisition）システムに侵入できることが判明した。そして 2011 年初春には、RSA 社を対象とした攻撃が明らかになり、9 月以降はわが国にも飛び火して、三菱重工を初めとした防衛産業が、軒並み攻撃されるようになった。

こうしたサイバー攻撃は、従来のものが即時的な破壊や情報の即時的な取得を目指していたのとは異なり、システム内部に深く進入し時間をかけて目標行動（情報の取得や遠隔操作など）を繰り返す点において異質である。そのため、APT(Advanced Persistent Threat)と名づけられ、①事前調査段階、②侵入段階、③攻撃準備段階、④攻撃実行段階という 4 段階を経るのが一般的であるとされる。

①の事前調査段階では、攻撃対象の組織やシステムの情報などを、外部から収集する。②の侵入段階では、①の情報を活用して、多岐にわたる手法を駆使してネットワーク内に侵入する。③では、攻撃実行のための準備として、システムの細部調査を行ない、外部との交信を行なう場合もある。そして、いよいよ④の段階で、最終的なシステムへの攻撃を実行する。

このプロセスを整理すると、取得する情報は 2 種に分かれ、情報Ⅰは①の段階で取得するもので、これが②や③の作戦に活用される。その後③の段階で新たな情報Ⅱが取得され、先のⅠとともに使われて、④の攻撃がなされる（以上は、この３月末に当大学院修士課程を修了予定の、岩崎正治さんの研究による）。

2． 情報資産（秘密と知的財産）の保護

このような前代未聞の攻撃に対して、法的な措置は十分と言えるだろうか。まずは、攻撃対象を、①情報資産、②情報システム、③社会秩序、④国家安全保障、の４つのレベルに分けて検討してみよう。まず、情報資産の保護から。

情報資産を守るとは、資産の CIA つまり Confidentiality（秘匿性）、Integrity（完全性）、Availability（可用性）を、所有者または管理者が望むレベルで維持することである。この点では、通常の ISMS（情報セキュリティ・マネジメント・システム）で求められる要件と変わらない。

APT でも、GPS（Global Positioning System）の誤動作が目的であれば完全性が狙われ、Stuxnet であれば可用性の破壊を目指していることになる。しかし APT の場合、攻撃者は、情報システムが通常通りに機能しており、相手に気づかれることなく執拗な攻撃を継続したい場合が多い。

つまり彼らが侵害しているのは、主として秘匿性である。そこで法的な観点から、これに対する防御が万全かと見ると、以下のように、はなはだ心許ない現状が明確になる。

① 情報の保護方式として「秘密型」と「知的財産型」があるが、その区分が明確に意識されていない（営業秘密は、保護形態としては前者であるが、通常後者と認識されている、など）。

② 知的財産型は法が整備されている（時に、整備されすぎている）が、秘密型の法体系には不備が目立つ。

③ 不備の代表例は、カバーされていない秘密があること、刑事罰の重さに代表される保護のレベル差があることである。

④ 前者の代表例は、国家機密である。現に法が整備されているのは防衛秘密だけであり、国家機密・外交秘密などの保護法がない（漏えいさせた本人は処罰され得るが、懲役１年以下である）。

そこで、尖閣諸島沖の中国漁船衝突事件を契機として、「秘密保全のための法制の在り方に関する有識者会議」が設置され、その答申（2011 年８月８日）を受けて、現在「秘密保全法」が検討されている。しかし現代のような技術革新が早い時代に、秘密を保護するのは容易なことではない。

一方、保護期間を定め、その間だけは秘匿するが、やがて「情報公開」することとセットで議論するという視点も重要である。電車や地下鉄の駅の構内で、よく「特別警戒中」という張り紙を見かける。本当に特別な警戒を要するようになったら、現時点でも既に「特別警戒中」なのであるから「超特別警戒中」とでもするのであろうか。秘密保護法制についても同様であり、秘密として保護する利益が薄れた情報は秘密から解除するということをセットにしないと、保護すべき秘密がどんどんふくれあがっていく。やがて秘密保全のためのコストも膨大となって、結局、秘密保護が不十分になる危険性が高い。

また、アメリカの秘密保護法制のように、国家安全保障情報と公開情報との間に、「機微であるが非分類の情報（SBU）」や「管理された非分類情報（CUI）」という中間的な保護の仕組みを取り入れることもあり得るだろう。

3． 情報システムの不正利用や破壊

APT というサイバー攻撃は長期間にわたるが、その突破口は情報システムの不正利用である。ただし稀には、破壊そのものが目的と思われる場合もあるし、攻撃者が情報システムを使い尽くしたと判断すれば、システム自体を破壊することがあるので、その備えも平行的に考えておかねばならない。

APT ほど大規模ではないにせよ、この種の攻撃はコンピュータのオンライン化とともに進んできたので、法的な対処も前よりは進んでいる。1987 年施行の刑法改正により「電子計算機損壊等業務妨害罪」が法定され（刑法 234 条の２）、併せて「電磁的記録」の「不正作出・供用」などの罪（同 161 条の２など）が整備されたのがきっかけである。これらに類似の規定は、2002 年には「支払い用カード」に関する犯罪にも適用されるようになった（同 163 条の２など）。また直近の改正では「不正指令電磁的記録（いわゆるウイルス）作成罪」（同 168 条の２など）が法定された。

この間、2000 年から施行されている「不正アクセス禁止法」においては、「ID・パスワードの不正な使用」や「そのほかの攻撃手法」によって、アクセス権限のないコンピュータ資源へのアクセスを、犯罪として禁止している。また認証を確実にするため、「電子署名・電子認証法」が定められ 2001 年から施行されている。

しかし現行の不正アクセス禁止法では、実在する銀行のサイトなどを装って、ID などの入力を求めるフィッシングのような行為が対象ではなかったので、こうした準備段階を含めて犯罪とする改正案が閣議決定され、国会で審議中である。その際併せて、「不正な手段」でなくても、不正目的であれば犯罪にするとか、フィッシング・サイトを開設しただけでも罪に問える（従来は、開設して誘導することが要件）などの改定が盛り込まれている。

4． 社会秩序の混乱

APT というサイバー攻撃の発信国は、大部分が中国だとする報告もあるが、もともと痕跡を残さないように仕掛けているのだから、即断することは難しい。しかし、これだけの攻撃を一人が片手間でやることは不可能に近いから、組織だった活動が行なわれていると見なければなるまい。

そうだとすると、かつてインターネット犯罪が愉快犯中心から、組織的犯罪に変化したように、サーバ攻撃もクラッカーによる個人ベースのものから、組織対組織の大規模なものに変化したと見るのが妥当であろう。それを裏返せば、効果として社会秩序の混乱を目的としている、ということになる。

この面では、法制度は整っているかに見える。刑法には「内乱に関する罪」（刑法 77 条以下）等が規定されているし、「破壊活動防止法」もある。また、「サイバー犯罪条約」を批准したことに伴って、「組織犯罪処罰法」も整備された。しかし、オウム真理教の一連の破壊行為に際しても、破壊活動防止法が発動されることはなかったし、「組織犯罪処罰法」を定めても、その実効性は地道な捜査や、息の長い裁判に依存している。

加えて、APT というサイバー攻撃の対象は、政府機関に留まらず「重要インフラ」と称される施設にも加えられている。否むしろ、重要インフラこそ一番のターゲットと言った方が当たっている。とすると、公的機関を念頭に置いた保護法制では十分でなく、民間部門も含めたより広いカバレッジを持ったシステムを考えねばなるまい。

5． 国家安全保障

前項の考えを推し進めると、平和憲法の下で自国の防衛をアメリカに依存してきたわが国も、そろそろ「国家安全保障」を真剣に考える時期に来た、と言わざるを得ない。平和憲法があまりに理想主義的に受容された結果、わが国はこうした機微に触れるテーマを「想定外」においてきたが、そのような時代は過去のものになりつつある。

サイバー空間が、陸・海・空と宇宙に次ぐ「第５の軍事領域」と呼ばれ、サイバー攻撃が交戦につながるものとされる現代である。アメリカはそのような理解で軍の再編成を行なっているし、それにふさわしい人材の登用も進めている。国防総省のリクルート案内でも、サイバー軍の入隊基準は陸軍などと違って、「行軍にどれだけ強いかなどは問題にしない」と明記している。戦争の形態そのものが変わってしまったのである。

こう言ったからといって、憲法９条を即時改正せよとか、自衛のためにも軍事力を強化せよ、と主張しているわけではない。言いたいのは、「国の存在は自分で守るしかないこと」と「戦争の内容がサイバー化していること」の２点だけである。

「国の存在は自分で守るしかないこと」についていえば、かつて、戦争は基本的には国家と国家（または、それに近い実力をもつもの）との問題であった。軍やスパイを部隊とした小説で知られる作家のフレデリック・フォーサイスが個人で傭兵を雇ってアフリカでクーデターを起こそうとしたという話もあるが、個人にできることは限られていた。しかし、いまでは金融商品への投機・投資を通じて巨万の富をえた個人が、クラッカーを雇って、ある国に集中的にサイバー攻撃を行なうということは現実的に可能である。その気になれば、個人でも戦争を起こせるのである。

「戦争の内容がサイバー化していること」についていえば、サイバー安全保障は、現時点では、サイバー・テロと似るところが多いので、日本の場合は安全保障の領域ととらえるか、警察活動の役割としてみるかは、微妙なところがある。

また国家安全保障としてのサイバー戦は、国連憲章 51 条にかかわる。国際的なテロ行為に関して自衛権を行使することの合法性については、国際法上、①テロ行為が国連憲章第 51 条で自衛権行使の要件とされている「武力攻撃」に相当するか、②テロ組織と国家の関連性として、当該国家がテロ組織に対し有効な統制（effective control）を有しているか、③自衛権行使としての武力行使が必要性かつ均衡性を充足するかどうか、から判断される。

これらの判断にあたっては、現時点では、サイバー戦で用いる技術的防御・攻撃手法（サイバー武器）に依存するというのが一般的な理解である 。したがって、これらのサイバー武器の内容を明確にしつつ、その使用についての合法性を確認していく必要があるだろう。

何代ものアメリカ大統領に仕えた、安全保障とセキュリティの専門家であるリチャード・クラークが、「サイバー戦争では攻撃力だけでなく、防御力がより重要になる。その点では、インターネットに依存したアメリカは、防御上の弱点を抱えている」と警告しているのは、日本にもそのまま当てはまるのではないか。因みに、インターネット依存度がゼロに近い北朝鮮は、攻守を総合しても世界で有数のサイバー戦力を保持していると懸念されている。

６．「平和だが有事」の対策

日本の場合、難しいのは、サイバー攻撃への対処について、その正当性に関するジレンマがあることである。

サイバー攻撃を「武力」の行使としてとらえ、それへの対処を自衛権の行使とするのであれば、憲法９条の制約を正面から受けることになる。それを「武力」の行使ではなく、単なる犯罪行為や違法行為ととらえるのであれば、それへの対処は通常の警察活動の範囲内で合法的に行なうしかない。しかしサイバー攻撃への対処のために、通常の法律では違法な行為が必要なときには、その正当性の根拠が必要である。そうしないと対処が違法となってしまうからである。ところが正当性の根拠は、最終的には自衛権の行使に行き着いてしまうのである。

このような現実を前にすると、いきなり国家安全保障を考えるのは日本人には酷で、まず「平和だが有事」というケースに慣れることから始めるのが、先決かもしれない。リスク管理の教科書には BCP（Business Continuity Plan）が必ず出てくるが、これは「いざという時にも業務が継続できる」ギリギリの備えを意味している。つまり「有事対策」である。

ところが、日本人は「平時と有事を分ける」ということにも慣れていない。先の東日本大震災に際して、「原子力緊急事態」宣言は発出されたが、「災害緊急事態」の布告はなかった。阪神・淡路大震災の初動ミスを教訓として、「災害緊急事態を布告しなければ、緊急災害対策本部を設置することができない」という規定を改正したため、平時のルールで有事に対応できることにしてあったからである。

これは一時しのぎとしては有効かもしれないが、いつまでも「平時と有事の切り替え」ができないことになってしまう。サイバー攻撃では、日本全体が非常事態に陥ることはないだろうが、目に見えないところで国の根幹が危うくなっているかもしれない。その意味では災害に次いで、「平和だが有事」の事例かと思われる。私たちは、望ましくない事態を「想定外」に追いやるのではなく、直視することに慣れていくしかないだろう。

2012 年３月２８日発行

特定非営利活動法人　NPO 情報セキュリティフォーラム
〒221-0835
神奈川県横浜市神奈川区鶴屋町 2-17　相鉄岩崎学園ビル
TEL(045)311-8777　　FAX(045)311-8747
E-Mail: isef@isef.or.jp　　URL: http://www.isef.or.jp