財団法人社会安全研究財団
2010 年度一般研究助成報告書

警察と軍におけるサイバーセキュリティ対策に関する国際比較研究

研究代表者
慶應義塾大学グローバルセキュリティ研究所
土屋大洋

共同研究者
慶應義塾大学総合政策学部
加茂具樹
慶應義塾大学総合政策学部
清水唯一朗
慶應義塾大学総合政策学部
神保謙
神戸大学大学院法学研究科
簑原俊洋

第１章　問題の所在

本研究の目的は、新たな治安上・安全保障上の問題として近年認識されつつあるサイバーセキュリティ対策について、警察と軍という視点から制度的な国際比較を試みることである。

サイバーセキュリティの問題は、これまでの治安上あるいは安全保障上の問題とはいくつかの点で異なる。第一に、不正アクセスや攻撃があったことすら分からないようにする形で相手に被害を与えられることである。例えば、ボットネットと呼ばれる手法を用いれば、世界中に分散したコンピュータから一斉に攻撃が行われることになるため、真の攻撃主体が誰で、どこにいるのかが分かりにくい。第二に、サイバー攻撃の主体は国家だけではない。高度な技術があれば、非政府組織や個人、テロ集団でもサイバー攻撃に参加することができるだろう。第三に、被害のレベルに大きな幅があることである。いたずら、中傷、迷惑・妨害行為、情報窃盗、不正アクセスといった個人的動機に基づくものから、重要インフラストラクチャの妨害・破壊といった国家安全保障上の危機に至るまで、さまざまな被害がありえる。

こうした特徴を有するが故に、不正アクセスやサイバー攻撃を犯罪として捉えるのか、あるいは戦争行為とするのか、テロなのかという点が難しくなる。言い換えるならば、主として警察機関が行ってきた犯罪捜査・法執行と、主として情報機関が行ってきたインテリジェンス活動との境界が分かりにくくなる。従来はそうした機関の間には、情報共有などを制限する壁が設けられてきたが、そうした壁が治安上・安全保障上の障害となりえる。

インターネットをはじめとする情報通信ネットワークがグローバルにつながっているため、日本もまたこうした問題に対策を講じなくてはいけない一方で、国際的な連携もまた必要になる。そして、諸外国のベスト・プラクティスを相互参照することも重要である。本研究は、こうした喫緊の課題に応えるべく、各国のサイバーセキュリティ対策について調査し、その際、主として警察組織が行う捜査・法執行活動と、情報機関が行うインテリジェンス活動の境界に注目することで、非伝統的な脅威に対応する枠組みを模索する一助としたい。

以下、次章では、近年のサイバーセキュリティの動向について概要を把握する。そして、こうしたサイバーセキュリティ問題の本質をつかむため、三つの章で事例研究を行う。まず、第3章では、歴史に範をとり、戦前の日米の情報戦を検討する。そこでは、情報を傍受するだけでなく、それをいかに解釈するかが外交・安全保障を有利に進めることにつながるという教訓を検討する。第4章では、2009年7月に米韓に対して行われた同時多発サイバー攻撃を取り上げ、それが日本のサイバーセキュリティ政策に与えた影響について検討する。第5章では、第4章で取り上げた韓国への攻撃に関連して、韓国がどのようなサイバーセキュリティ政策をとったのかを行政学的な点から検討する。第6章では、サイバーセキュリティに対応する組織について検討し、結論を述べる。

第２章　近年のサイバーセキュリティの動向

2011 年 9 月 19 日、読売新聞が一面で三菱重工が何者かからサイバー攻撃を受けていたと報じた[1]。三菱重工の全国 11 拠点にあるサーバーなど 83 台（サーバー45 台、パソコン 38 台）に、いわゆる標的型といわれる手法でウイルスが送りつけられ、感染したサーバーなどのうち少なくとも 20 台が社外に設置されているサイトに知らない間に接続していたことも明らかになった[2]。三菱重工の神戸造船所では原子力プラントや潜水艦を、長崎造船所では自衛隊の護衛艦を製造している。いわば防衛産業の一角を担っている。そして、同じく防衛産業に入る IHI や川崎重工業も、ウイルスに感染はしていないものの、同種の攻撃を受けていたことを明らかにした[3]。

この報道を皮切りに、さまざまなサイバー攻撃の被害が報告されるようになった。2011 年 10 月 25 日、朝日新聞は、衆議院のサーバーに不正侵入が行われ、パスワードが盗まれていたと報じた[4]。翌日には衆議院議員全員 480 人分のパスワードが盗まれていた可能性があるとも報じられた[5]。また、外務省の在外公館にも同様の攻撃が行われていると読売新聞が報じた。ウイルスに感染が確認されたのは、カナダ、カメルーン、韓国などにある在外公館であるという[6]。

実はこうした目に見えない、静かな「攻撃」は数年前からさまざまな標的に対して行われてきた（表 1）。サイバー攻撃というと、いわゆる DDOS（Distribute Denial of Service：分散サービス拒否）型の攻撃が思い浮かぶが、よりいっそう深刻なのは標的型の攻撃である。DDOS 攻撃はサーバーなどがダメージを受け、一時的にサービスができなくなるだけである。無論、金融サービスなどでは一時的とは言え、サービスが提供できなくなることは深刻な影響を与える可能性もある。しかし、そうした被害を受けたという事実は、信用問題に直結するため、なかなか公表されることはない。

こうしたサイバーセキュリティ問題の高まりに対し、どのような対抗策がとられているのだろうか。まず、国際的には、早くも 2001 年にサイバー犯罪条約が採択されている。これを発案したのは欧州評議会で、日米欧など主要国 30 カ国が署名したが、日本は 2011 年 6 月の刑法改正でようやく正式批准へ進む予定である。2011 年 5 月に開催された G8 のドーヴィル・サ

---

1 「三菱重サーバーに侵入」『読売新聞』2011 年 9 月 19 日。

2 「三菱重　感染サーバー、海外と通信」『読売新聞』2011 年 9 月 20 日。

3 「IHI・川重にもサイバー攻撃　防衛産業狙い撃ち」『日本経済新聞』2011 年 9 月 21 日。

4 「衆院にサイバー攻撃　議員のパスワード盗まれる」『朝日新聞（電子版）』2011 年 9 月 25 日
（http://www.asahi.com/digital/internet/TKY201110240606.html）。

5 「全衆院議員のパスワード盗難か　管理者権限で操作」『朝日新聞（電子版）』2011 年 9 月 26 日
（http://www.asahi.com/national/update/1026/TKY201110250740.html）。

6 「大使館にサイバー攻撃か」『読売新聞』2011 年 10 月 26 日。

ミットでは、首脳宣言のかなりの分量がインターネット問題に割かれ、サイバーセキュリティについても「インターネット上の犯罪・テロの防止のため協調が必要」とされた。

欧州では、2004 年 3 月に ENISA（European Network and Information Security Agency）が設立され、ギリシャのヘラクリオンに本部が置かれた。ENISA はネットワークセキュリティ及び情報セキュリティに関する予防・対応能力を促進することを任務とし、EU 加盟国および欧州諸機関へアドバイスや提言を提供するとともに、欧州諸機関、EU 加盟国ならびに民間企業・産業関係者との連携を促進している。2010 年 8 月に EU は「A Digital Agenda for Europe」と題する政策文書を発表し、七つの課題のうちの三番目に「サイバー犯罪の増加とネットワークの低信頼性のリスク」が入れられた。それを受けて同年 11 月には全加盟国が参加する初の演習「Cyber Europe 2010」が開催された。

米国では、ジョージ・W・ブッシュ政権の第二期末期である 2008 年に、国防総省の情報通信ネットワーク内で大規模かつ深刻なウイルス感染が見つかった。この事実は、ウィリアム・リン国防副長官が 2010 年に明かすまで明らかにされなかったが[7]、2008 年の大統領選挙に勝利し、2009 年に成立したバラック・オバマ政権では、政権成立当初から積極的にサイバーセキュリティ対策がとられた。

オバマ大統領は、政権成立直後に 60 日かけてサイバースペースに関する政策をレビューするよう支持し、2009 年 5 月に「サイバースペース政策レビュー（60 日レビュー）」として発表された。同年 6 月には、米軍の核兵器・宇宙軍を担当してきた戦略軍（STRATCOM）の下に、サイバー司令部（USCYBERCOM）の設置を命令し、この司令官は国家安全保障局（NSA）長官が兼務することになった。2010 年 2 月には、「4 年毎の国防計画見直し（QDR）」でサイバーセキュリティの重要性を強調し、2011 年 7 月には国防総省が「Strategy for Operating in Cyberspace」を発表した。

米国政府は、攻撃・侵入を食い止めるため、「アインシュタイン・プログラム」と呼ばれる侵入検知システムを開発している。これは、政府機関のネットワーク・ゲートウェイで不正なトラフィックを監視するもので、US-CERT（United States Computer Emergency Readiness Team）が開発した。これは政府関連の情報に限るが、中国政府が採用している「サイバー万里の長城」あるいは「金盾システム」と呼ばれる検閲システムと同種のものであるといわれている。

日本では、まず、2000 年 1 月 24 日午後、日本の科学技術庁のウェブページが何者かによって書き換えられる事件が起きた。同庁は 5 時間以上たった午後 11 時頃、首相官邸の危機管理室と警視庁ハイテク犯罪対策センターに被害を報告した。しかし、その後、被害は拡大し、総務庁、総合研究開発機構（経済企画庁の外郭団体）、運輸省のウェブページが書き換えられ、文部省、外務省、郵政省にも攻撃が行われた。

この攻撃の翌月、2000 年 2 月に内閣官房情報セキュリティ対策室が設置された。そして、それは 5 年後の 2005 年 4 月に内閣官房情報セキュリティセンター（NISC）として格上げされた。さらにその翌月の 2005 年 5 月には IT 戦略本部長（つまり内閣総理大臣）の決定により情報セキュリティ政策会議が設置された。

[7] William J. Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs*, September/October 2010.

以上のように、サイバーセキュリティはここ　　国はそのための対策を急いでいる。
数年で急速に政策課題として浮上してきた。各

表 1　近年のサイバー攻撃の例

年月	事例
2000 年 1 月	科学技術庁など政府機関サイトが改ざんされる。
2007 年 4 月	エストニアの政府機関や金融機関などに対し大規模な DDOS 攻撃。
2007 年	イスラエルがシリア国内を爆撃の際、シリア防空網操作の疑い。
2008 年	米国防総省の軍事機密を扱うネットワークがウイルスに感染し、他国のサーバーにデータが転送される。
2008 年	カナダの研究者が GhostNet と呼ぶ秘密の情報収集ネットワークが発覚。
2008 年	グルジアとリトアニアでロシアからと見られる大規模な DDOS 攻撃。
2009 年 7 月	米韓に大規模な DDOS 攻撃。
2009 年	油田情報などを標的とした、中国のグループによる「ナイト・ドラゴン」作戦。
2009 年	米グーグルなどのサービスを利用する中国や米国の人権活動家のメールが盗み見られるなど約 30 社が被害に遭う。
2010 年	イランの原発で制御系のシステムに影響するウイルス「スタックスネット」が発見される。
2010 年	経済産業省の職員にウイルス付きメールが送られ、省内のパソコン約 20 台が感染
2010 年 9 月	尖閣諸島問題に絡み、中国から日本の政府機関などに攻撃。
2011 年 3 月	米 RSA のシステムが侵入され、使い捨てパスワードの設計情報を盗まれる。
2011 年 3 月	欧州連合（EU）の欧州委員会や欧州対外活動庁に攻撃。
2011 年 4 月	ソニーの複数のネットサービスから合計 1 億件の個人情報流出。
2011 年 5 月	米シティグループのネットバンキングシステムから利用者の情報が盗まれる。
2011 年 5 月	米ロッキード・マーチンで外部から社内につなぐシステムを破られシステムに侵入される。
2011 年 6 月	国際通貨基金（IMF）が数ヶ月にわたり大規模なサイバー攻撃を受けていた事実を公表
2011 年 6 月	米グーグルの「G メール」利用者数百人のメール内容が見られる。
2011 年 6 月	米 CIA（中央情報局）の公式サイトが攻撃され、利用不能に。
2011 年 7 月	韓国 SK テレコムの子会社が運営する SNS などから 3500 万人分の個人情報が流出
2011 年 8 月	オランダのデジノターの電子証明書の発行システムに侵入され、500 を超える偽証明書を発行。米グーグルの利用者などに被害。

出所：以下の記事などを元に作成。「サイバー攻撃対策　強化」『日本経済新聞』2011 年 8 月 24 日。「三菱重サーバーに侵入」『読売新聞』2011 年 9 月 19 日。「相次ぐサイバー攻撃…政府ようやく『緊急会議』」2011 年 10 月 8 日。

第３章　歴史的観点からの戦前の日米情報戦

フランシス･ベーコンの有名な格言の一つに、「情報は力なり」というのがある。1941 年 12 月 8 日に、日米開戦の火蓋が切られるはるか前に、水面下では、こうした「力」の獲得を目指した激しい攻防線が展開されていた。それは、相手の腹の内を探ることを目的とした日米両国による暗号解読戦である。

情報をめぐるこの密かな戦いは、時として国家の命運を決するほど重要なものであった。そして、この前哨戦において、米国が日本に完勝したとするのが通説である。1941 年 8 月 1 日に発動された米国の対日石油禁輸によって、日米関係は一気に緊張しつつも、両国は和平へのラスト・チャンスであった日米交渉に望みを託していた。だが、この間、暗号解読に成功していた米国は、外務省の電信の内容をほぼ把握していたのである。他方、日本側について言えば、一般的に論じられている筋書きは次であろう。すなわち、国務省の暗号を最後まで解読できなかった日本は、暗中模索しながら対米交渉を進め、最後は相手の真意が分からずに手痛い敗北を帰した、とするものである。

こうした理解が、長らく日米情報戦で常識となっているが、相次ぐ新史料の発見によって、別の歴史像が次第に浮かび上ってきている。以上を踏まえて、本章では、この新たな日米暗号戦の実態について考証を与えることを目的とする。

米国の暗号解読の始まりとブラック・チェンバー

まず、一方的な勝利を収めたとされる米国の暗号解読の実態についてであるが、そもそも、歴史が浅い米国では、英仏などの暗号先進国と比較すると、解読の分野では随分と立ち後れていた。独立戦争の際には、英国の暗号を部分的に解読していたが、史料によって裏付けされる最初の大きな成果は、南北戦争時、北部諸州軍による南部連邦軍の暗号の解読である。他方の南軍は、北軍の暗号を最後まで解読できなかったが、その背景には解読から得られる情報そのものの重要性を認識していなかったことが挙げられる。皮肉なことに、北軍が使用していた暗号は、南軍と比べてかなり強度の低いものであり、身を投じさえすれば、解読は容易であった。

こうした暗号解読組織も、南北戦争の終結とともに閉鎖され、米国の解読ノウハウの維持・向上に対する関心も急速に失われた。米国が再び暗号解読の重要性に目覚めたのは、20 世紀となってからである。米国は 1917 年 6 月に、第一次世界大戦に参戦したが、それに伴って暗号解読に専念する最初の情報機関が創設されたのである。これが、MI-8（通称、ブラック・チェンバー）であり、同組織の中心人物が、アメリカ暗号解読の父と称されるハーバート・ヤードレーであった。こうした組織を運営するための予算の大部分は、国務省の機密費によって賄われ、その存在は議会にも伏せられていた。

最初は 3 人だけで始まったブラック・チェンバーは、大戦終結時には総勢 150 人の組織にまで成長し、その結果、メキシコなど中南米数カ国の外交暗号が解読できるまでになっていた。しかし、なんと言ってもその最大の功績は、日

本の外交暗号の解読に成功したことである。その結果、1921 年のワシントン会議時には、日本政府の外交電信の内容は全て筒抜けとなっていた。当時、国務長官であったヒューズの机上には、解読・翻訳されたばかりの外交文書が毎朝置かれていたが、これによって機密情報であった戦艦保有率対米 6 割という日本政府の最大譲歩ライン米国に漏れており、それによって軍縮交渉も有利に進めることに成功したのである。

政権が変わると、大きな政策転換が起きるのが米国である。そのため、1929 年に就任したスティムソン新国務長官は、「紳士たる者、他人の信書を盗み読みしてはならない」という言葉のもと、輝かしい功績を挙げてきたブラック・チェンバーを閉鎖したのである。その理由として、彼が倫理に反する行動に対して良心が痛めたからであるという理由がよく語られるが、実際のところそうした問題は関係なかった。それは、法律家であるスティムソンが、単に国際法と照らし合わせると、外交を行う国務省という組織が暗号解読に携わることは好ましくないと考えたという理由から端を発するものであった。ローズヴェルト政権下でスティムソンは後に陸軍長官に就任するが、その時の彼は、何ら躊躇なく日本の暗号解読文書に目を通しており、それがもたらす情報を重宝していたのである。では、ブラック・チェンバーが廃止された後の米国の暗号解読の行方はどうなったのか。

ブラック・チェンバー閉鎖後の米暗号解読

スティムソン国務長官によって閉鎖されたブラック・チェンバーであったが、米国の暗号解読力は致命傷を負うことはなかった。陸軍省が通信隊情報部（SIS）という新組織を設立し、「暗号の天才」と後に称されることになるウィリアム・フリードマンによって、米暗号解読組織の命脈を保たれたのである。

フリードマンは、現モルドヴァ共和国のキシニョフ生まれのユダヤ人で、2 歳の時にロシアによる迫害が強まったため、当時多くのユダヤ系移民のように米国へと渡った。大学院中退後、彼はリヴァーバンク研究所という民間の暗号研究所に就職し、同研究所の重要のプロジェクトの一つであった、シェイクスピアの作品中の暗号を解読し、真の作者を見つけるという仕事に携わった。こうした作業の傍らで、研究所が政府の非公式な外郭団体として請け負っていた外交電信の暗号解読も行ったのである。第一次世界大戦が勃発すると、研究所は陸軍省の依頼を基づいて暗号解読者の育成に専念し、対戦末期の 1918 年には、フリードマンも陸軍省に出向してドイツ軍の暗号解読に一役を買うことになった。

1919 年のパリ講和会議後、フリードマンはその才能を買われて暗号解読の専門官として SIS に転職することになる。しかしながら、当時、外交電信の暗号解読はブラック・チェンバーの管轄にあったため、フリードマンが所属する SIS は、それ以外の暗号解読を担うことになった。禁酒法成立後のアメリカでは、酒類の密輸が急増したため、SIS は密輸者が使用する暗号の解読に力を注ぎ、米国沿岸警備隊に協力しながら犯罪組織の撲滅に貢献した。

しかし、転機は突然訪れる。上述したように、スティムソンが 1929 年にブラック・チェンバーを廃止したことによって、暗号解読組織は大幅に改編され、国務省に取って代わって陸軍省が外交電信の暗号解読を担当することになったのである。こうして、ヤードレーが築いたブラック・チェンバーは、フリードマンによって引き継がれていくことになる。

米国の対日暗号解読の始まり

実は、米国にはもう一つの暗号解読機関があった。OP-20-G と呼ばれる海軍の解読機関である。第一次世界大戦後、海軍省は、ローレンス・サフォード中尉の下、陸軍とは別に日本政府の外交暗号の解読に取り組んだ。OP-20-G が得意とした手法は、「盗読」であった。工作員がニューヨークの日本総領事館に何度も侵入し、金庫に保管されていた暗号書を撮影したのである。史料によって確認できるだけで、こうした侵入は 11 回もあり、外務省の暗号書が更新される度に行われた。なお、陸海軍の間に協力関係はなく、それぞれが独自に傍受・解読を行っていたが、満州事変を契機に、両組織は協力体制を築いた。その結果、海軍は日本海軍の暗号を、陸軍は外交暗号を担当するようになり、日米関係に暗雲が立ち籠もった 1940 年冬以降は、共同で外交暗号の解読にあたるようになる。

このように満州事変は暗号解読組織に大きな転機をもたらしたが、その年、全く予期しなかった重大な危機に直面する。ブラック・チェンバーが閉鎖された腹いせとして、ヤードレーが『アメリカン・ブラック・チェンバー』を出版し、米国の暗号解読の実態を暴露したのである。日本の外交暗号の解読を中心に論じた同書は、日本政府に大きな衝撃を与えた。必然的に、暗号強化が焦眉の課題となり、日本は当時最高水準にあったドイツ製のエニグマ暗号機の導入を決定する。この暗号機に改良が施され、1934 年から外務省は解読不可能と考えられた機械暗号に移行するのである。

中国への侵略を拡大する日本に対して米国は強い懸念を抱いていたため、外交電信の解読は最重要の位置づけにあった。だが、機械暗号の導入によって、外務省の暗号はピタリと読めなくなり、フリードマンを中心とした SIS は、この新暗号の解読に全力を注ぐことになる。

通信諜報に関係する公文書の多くは、未だに国家機密指定となっているが、その中でも解読方法に関する情報は半世紀以上を経ても非公開が原則となっている。だが、日本の最初の機械暗号の解読方法については、徐々に解明されつつある。

機械暗号は、文章を暗号化する際に、反復がないため、パターンを確立しにくく、解読は複雑を極める。だが、言語と文章の特性はなかなか隠せない。例えば、ローマ字表記の日本語の場合、「Y」の後には高い確率で「O」か「U」が続く。この言語特性の解析に加え、解読者たちは外交電信の多くが、「極秘　官庁符号扱い」という語句で始まることに気づいたのである。こうしたヒント（お決まり文句）をもとに、機械暗号の組み方が次第に姿を現し、解読にこぎつけたのである。そして同暗号は、スペクトルに擬えて「レッド（赤）暗号」というコード名で呼ばれるようになった。

しかし、最も有名な暗号は、同様にスペクトルの色が用いられた「パープル（紫）暗号」である。97 式欧文印字機によって組まれたこの暗号は、レッドよりも格段に強度が高かった上に、暗号機自体もエニグマ機とは全く異なる形状であった。パープルの具体的な解読方法は、未だに非公開であるが、外務省による暗号の使用方法に大きな欠陥があったことが解読の発端となったことは疑いない。パープルの使用が、米国を含む 13 の在外公館に限られていたため、それ以外の在外公館との通信には従来の暗号が用いられていた。つまり、同一内容の文書が、新旧二通りの暗号で本省から送られていたのである。一方の暗号は解読できたため、双方を照ら

し合わせることによって（これを専門用語で crib と呼ぶ）、新暗号解読の手がかりを得たのである。

こうした人為的なミスにも助けられながら、米国政府は外務省の電信のほとんどを情報化することに成功し（魔法のようにすらすらと解読できたことから、通称は「マジック（Magic）」）、日米交渉において日本政府の手の内は米国側に筒抜けとなっていたのである。

ここで解読と対になる翻訳についても簡単に述べよう。日本語は難解な言語であるから、解読された電信から「情報」を取るためには、翻訳が重要である。しかし、電文自体がローマ字表記のため、日本人でもなければ同音異義語の判別は困難となる。「御前会議」が「午前会議」と訳されたのが、その好例である。もちろん、この程度なら許容範囲である。だが、日米交渉の最終段階において提出された乙案を「絶対的な最終提案（absolutely final proposal）」と訳したのは、重大なミスであった。こうした誤訳が相互不信を招き、最終的に日米交渉破綻の一因となったとする解釈はすでに指摘されているところである。

翻訳から見た情報戦

長らく機密指定されていた暗号解読に関する米軍の資料が最近になって相次いで米国立公文書館によって公開されたことにより、ようやく米国の対日暗号解読の実態の全貌がつかめるようになってきた。そこで、最も華やで、かつ注目度の高い「解読」にではなく、陰に潜んでいることが多い「翻訳」という側面に焦点を当てながら当時の情報戦の歴史の紐を解くことにする。

当然のことだが、暗号電信を傍受したのち、それを単に解読するだけでは情報としての価値は限られている。つまり、電信の内容を見極め、それを明瞭に理解できる媒体に変換しなければ（すなわち、情報化）、折角の解読文も有効に活かせないのである。そのため、解読者と翻訳者は車の両輪をなし、いずれが欠落しても電信から意味のある情報を抽出するのは不可能となる。そして、とりわけ日本語のような難解な言語の場合、有能な翻訳者は欠かせない。

ここで一つ留意しなければならないのは、日本の暗号電信はローマ字で組まれるという事実である。同音異義語が多い日本語の場合、翻訳者は文脈から意味を把握しなくてはならず、専門用語が頻出する文書の中で、それは卓越した日本語能力のみならず、文化・政治・経済・軍事の多岐の分野に精通してなければならないのである。

日本の外交暗号は、1917 年 12 月より米国によって断続的に解読されるようになったが、通信量がまだ少なかったころは、数人の翻訳者だけで十分間に合った。しかし、日米関係に暗雲が立ち籠めるようになった 1941 年以降から通信量は急増し、日本語が堪能な翻訳者の確保が焦眉の急となった。とはいえ、真珠湾攻撃前夜の時点でも、その肝心な日本語の翻訳者は僅か 9 人しかいなかった。このことからも、当時米国の主たる関心は日本ではなかったことが窺える。

当然、この状況は日米開戦後には一変し、米国は猛烈な勢いで対日戦時体制を整える。その一貫として、日本語の翻訳者を大幅に増やすことが決定され、その責を担ったのが、前述の米通信情報部（SIS）であった。SIS は、すでに 1930 年 5 月に言語課（日本語）を設けていたが、同課は 1935 年 3 月の時点でも本格的な翻訳作業を開始しておらず、それからの 2 年間で

も、300 通ほどの外交電信を翻訳しただけであった。翻訳作業がようやく軌道に乗り出したのは、1937 年 2 月以降のことである。

なお、外交暗号に限って言えば、1942 年 6 月まで米陸海軍ともにSISの下で解読に当たっており、提携が最終的に解消されるまでの間、新旧 49 種類の暗号の完全または部分解読に成功した。そして、この中には、当時外務省が最高強度の暗号と見なしていた 97 式欧文印字機による暗号も含まれていたが、同暗号による電信が SIS によって初めて翻訳されたのは 1939 年 9 月 27 日のことであった。

戦争勃発後、日本に関する暗号解読と翻訳作業は新設された SIS 内の B 課に移管されたが、驚くべきことに 1942 年 8 月の時点でも翻訳者は 16 人しかいなかった。その背景には、米国の各組織が日本語の翻訳者を競い合うようにして採用したため、人材確保が困難になったことが挙げられる。この深刻な事態を受けて、SIS は自前で翻訳者の養成を目的とする本格的な日本語学校を立ち上げることにし、その任に当時ハーバード大学教授のライシャワーが抜擢されたのである。彼の指揮のもと、エール、プリンストン、コロンビア、そしてハーバード大学で日本語を学習していた学生 30 人ほどが急遽集められ、陸軍管轄下の日本語学校（通称、アーリントン・ホール）が 9 月に発足した。

ようやく翌年の春にアーリントン・ホールの第一期生が卒業し、翻訳者不足は次第に解消されるが、逆に言えば、この時期まで解読とは対照的に翻訳作業は覚束ない状況にあり、米国の対日情報戦は必ずしも円滑には進んではなかったのである。とはいえ、日本語学校の設立は、アメリカの対日情報戦が最終的に成功を収めた大きな要因となった。このように情報戦では、どうしても「解読」の方が注目されがちだが、「翻訳」も引けを取らず重要なのである。そして、そのアーリントン・ホールが存続した 3 年間の間に、428 人の翻訳者が育ち、皮肉にもその一部が戦後、大学を舞台に日本の専門家として活躍し、アメリカにおける日本研究の礎を築くことになるのである。

ここまでは暗号解読において翻訳者がいかに重要であるかについて論じたが、米陸軍安全保障局（ASA）翻訳課の資料には、日本の外務省と陸軍の暗号をどの程度まで情報化できたかについても詳細に報告している。こうした資料によって、戦時中の日米情報戦がいかに一方的なものであったかが改めて浮き彫りとなる。そこで、ここからは米通信情報部（SIS、1943 年に ASA と改称）の翻訳課の活躍について検証する。

SIS が最も容易に解読できたのが外務省暗号であり、それがもたらした膨大な情報は極めて有用であった。その内容は、訓令に留まらず、日本が占領した地域の政治情勢や経済状況等、多岐に及んだ。第二次世界大戦は物量戦であったため、国家の総合的な経済力は重要であり、こうしたことから日本経済に関するデータは戦略上、欠かせないものとなった。実際、SIS は台湾・朝鮮両総督府、並びに日本の主な企業の暗号をも解読し、金融や工業に関する情報を積極的に収集した。外務省は、常時複数の暗号を使用していたが、SIS は 15 種類の主要暗号をほぼ全て解読していたため、同省の通信は筒抜け同然であった。なお、余り知られていない事実であるが、武官暗号（コード名、JAS）も解読されていたため、米国は複数のチャンネルから在外公館の機密情報を入手することができた。

例えば、スウェーデン公使館における小野寺信陸軍武官の和平工作や彼のスパイ網に関する情報も全て米国には周知の事実となっていた。その他にも本省暗号「トキ」（JBA）の解読に

よって、広田・マリク会談や佐藤・モロトフ会談、そして近衛文麿を特使としてソ連に派遣する案までもが ASA の翻訳課によって情報化されたのである。当然、ヤコブソン工作として知られる国際決済銀行（BIS）の北村孝治郎理事と戦略情報局（OSS）のダレス欧州局長とのベルンにおける秘密和平工作に関する日本側の態度も全て伝わっていた。こうした情報は、毎朝トルーマン大統領に送られ、ポツダム会議へ出席した時なども、翻訳文は専用機によって確実に大統領の手許に届けられたのである。

ここで挿話を一つ。ASA の資料は、ベルンの加瀬俊一とストックホルムの岡本季正両公使、そしてベルリンの大島浩大使がもたらした情報は超一級であったと賛辞しているが、その中でも特別な存在であったのがモスクワの佐藤尚武大使の情報であった。「ナゴヤ」（JAM）という高強度の暗号を使った彼の外交電信は、優れた知見と洞察力による極めて適切な状況分析がなされていたため、翻訳者たちはいつもその内容に感銘を受けた。そして、ソ連が中立条約の破棄通告を行った直後に大使から本省へ打電された悲痛の思いの電信は、翻訳者たちを佐藤という人物に惚れさせた。そのため、大使が失意の余り、東郷外相に辞意を申し入れた時、それを知った翻訳者たちは大いに嘆いたのである。

情報の金脈であった外交暗号だが、陸軍の暗号は果たしてどこまで情報化されただろうか。一般では、無限乱数表を用いた陸軍暗号は、解読不能であり、米国さえ解読できなかったと言われている。しかし、未公刊資料によると、陸軍の暗号も最終的には解読されていたのである。陸軍は、長文の電信や決まり文句を禁止するなど、機密保持には力を入れた。それ故、SIS も陸軍の主要暗号を数学的に解読するのは容易ではないという結論に至っていた。その結果、強度が低い陸軍の船舶暗号（JKK）は、1943 年 4 月に解読されたが、その他の暗号は破られないままでいた。しかし、1944 年 1 月 19 日に、東部ニューギニア戦線のシオにて日本陸軍の第 20 師団が保持していた暗号書と乱数表が地中に埋められた鉄製の箱から見つかったのである。それは、豪軍によって直ちに ASA へ送られ、解析された結果、陸軍の主要暗号（第 4 号）もついに解読された。同様に沖縄戦の首里城で、多くの暗号書が米軍の手に落ち、それによって航空暗号（JKC）などが解読できるようになった。資料によると、これによって特攻隊による被害をかなり軽減することができたとある。

このように、ほぼ完璧に情報化されていた戦時中の日本の暗号であったが、一つの大きな疑問が残る。果たして日本に対する解読はいつ頃まで続いたのだろうか。戦後を語る資料は少ないが、1951 年の講和会議の時まで解読されていたのは確かである。それ以降については、推測の域を出るものではないが、暗号技術の飛躍によって解読が困難となった 1970 年代までは続いたと考えるのが自然であろう。他方、ちょうどその頃に発足したエシェロンによって米国はより幅広い通信傍受能力を得、今では国際通話やｅメールまで傍受しているとされている。当然、米国の監視対象は政府だけでなく、民間企業もその範疇にある。昨今の個人情報に対する関心の増加を皮切りに、日本もそろそろ真剣に国家レヴェルで「情報保護」を考える時であろう。

第４章　日本のサイバーセキュリティ対策
――2009 年 7 月の米韓同時攻撃への対応を例に

本章では、2009 年 7 月の米韓に対する攻撃に日本政府がどのように対応したのかを検討する。関心は特にサイバーセキュリティ対策におけるインテリジェンス機関の役割に置かれている。米英韓などサイバーセキュリティに力を入れている国ではインテリジェンス機関が主導的な役割を担っている。サイバー空間における新しい脅威は、政府のシステムの変更を必要としている。それらの脅威は複雑で、不透明だからである。

日本では、2005 年に設立された内閣官房情報セキュリティセンター（NISC：National Information Security Center）がキー・プレイヤーである。しかし、NISC はインテリジェンス機関ではない。NISC は内閣府内の一機関であり、これまではサイバーセキュリティの技術的な手段に力点を置いてきたが、2009 年 7 月の米韓への攻撃の後、急速に国家安全保障の視点を取り入れつつある。NISC がインテリジェンスと法執行の交差するところであるとすれば、この協力システムは、将来の脅威に備えるための日本のインテリジェンス制度を再考する第一歩となる可能性がある。

サイバー攻撃は、しばしば攻撃されていることすら分からないという恐れがあるため、犯罪捜査を行う法執行機関、警察機関だけではなく、インテリジェンス機関の役割が重要になっている。特に、国家安全保障に関わるような攻撃は事前に阻止されなければならないため、インテリジェンス機関の関与が必要になる。

本章では、冷戦後の東アジアにおける情勢変化が、日本のインテリジェンス機関を活性化させるとともに、近年のサイバーセキュリティへの関心の高まりがインテリジェンス機関に新たな役割を付与し、特にその転機となったのが 2009 年 7 月のサイバー攻撃であるという立場を取りたい。

2009 年 7 月の米韓に対するサイバー攻撃

2009 年 7 月、米国の独立記念日の休日直後に何者かが米国の政府機関のサイトや商業サイトへの DDOS 攻撃を始めた。DDOS 攻撃は、ウイルスに感染した多数のコンピュータが特定のサーバーに同時に大量のアクセスを試みるもので、能力をオーバーしたサーバーは機能を損なわれる。しかし、個々のアクセス自体は正常のものにしか見えないので、回避するのが難しい。ホワイトハウスや国務省、財務省、国防総省、ヤフー、アマゾンなど少なくとも 20 以上のサイトが狙われた。

続いて 7 日から 9 日にかけて、韓国でも大規模なサイバー攻撃が行われ、国防部や国会、国家情報院、オークションサイト、銀行など 28 機関が被害を受けた。ウイルスで乗っ取られたコンピュータは韓国を中心に 19 カ国に及び、7 日の 18 時、8 日の 18 時、9 日の夜と波状的に行われる大規模な攻撃だった。韓国の権泰信・国務総理室長は 9 日の対策会議で「我が国の体制に対する攻撃であり、安全保障を脅かす挑発

行為だ」と語った（『朝日新聞』オンライン版、2009 年 7 月 10 日）。その後の解析で、米韓両国の攻撃には同じプログラムが使われていることが分かった。

当初、韓国のインテリジェンス機関である国家情報院は、はっきりした証拠を示さないまま一部の国会議員に北朝鮮の関与の可能性を説明したが（『朝日新聞』オンライン版、2009 年 7 月 8 日）、その後も首謀者を特定する証拠は得られなかった。韓国政府は 6 月 7 日の時点で「平壌が『南朝鮮の通信網を破壊しハッキングプログラムを開発せよ』との指示を出した」という情報を入手し、その約 2 週間後、韓国情報保護振興院と釜山の大学を標的にした「模擬訓練」の兆候を摑んでいたため、北朝鮮関与を疑ったという（『朝日新聞』オンライン版、2009 年 7 月 23 日）。ただ、一般のユーザーは、「つながるのが遅い」という程度の感覚で、感染したコンピュータが使えなくなった他は、深刻な被害が報告されたわけではなかった。誰が首謀者か、どこの国かを示すような痕跡はなく、北朝鮮の関与が濃厚とされているが、現在でも韓国政府は公式の判断を下していない[8]。

しかし、日本の同盟国である米国と、隣国である韓国が同時に大規模な攻撃を受けたことは、日本政府を動かすことになった。

サイバーセキュリティと日本の対応機関

2000 年頃を転換点とする日本のインターネット利用の拡大は、同時に前述のような省庁ウェブページ改ざん事件を引き起こし、「サイバーセキュリティ」という新たな問題の発生と拡大へとつながった。この新しい脅威に対処する政府機関としては、第一に警察が挙げられる。犯罪として考えられる行為があれば、容疑者を捕まえ、裁判にかけるために警察が捜査を行う。

しかし、第二に、単なる犯罪のレベルを超え、国家安全保障上の脅威として考えられるならば、対応するのは軍隊、日本の場合は自衛隊とそれを所管する防衛省になるだろう。ウェブページの書き換え程度なら犯罪のレベルだが、重要インフラストラクチャへの物理的な攻撃となれば、自衛隊による対応もあり得る。

そして、第三に、大規模な、あるいは深刻な攻撃を予測・防止するためには、インテリジェンス機関の働きが必要になる。原子力施設や交通網、金融システムへの攻撃などは、行われた後での対応では取り返しがつかなくなる。そうした攻撃を未然に防ぐためには、行政傍受などを含めたインテリジェンス機関による対応が必要となるだろう[9]。

日本の場合、これらの三つのタイプの機関はオーバーラップしており、厳密に区別することはできない。警察庁の警備局は有力なインテリジェンス機関であり、防衛省の情報本部もまた通信傍受機能を担うインテリジェンス機関という側面を持っている。公安調査庁は内外の過激派組織を監視している。日本のインテリジェンス・コミュニティの司令塔的役割を担う内閣情報調査室の歴代トップは警察庁出身であり、ナンバーツーは外務省出身で固定されている。

日本がそれまで受けたサイバー攻撃は政府省庁のウェブページの書き換えや人気掲示板への一斉アクセスによる妨害といったレベルであり、それほど深刻なものは報告されていなかった。

---

[8] 2011 年 1 月 27 日、韓国の KISA（Korea Internet and Security Agency）でのインタビュー。

[9] 行政傍受については以下を参照。土屋大洋「インターネット時代の通信傍受」『治安フォーラム』2007 年 12 月号、39―47 ページ。

しかし、2009 年 7 月に米韓への同時攻撃が行われたことは、それなりの衝撃を持って受け止められた。こうした変化の中で重要な役割を果たしつつあるのが NISC だが、警察庁、防衛省、NISC の米韓同時攻撃への対応を見ていこう。

警察庁

警察庁では、2009 年 7 月の米韓同時攻撃によって緊張感が高まった[10]。隣国が攻撃されたことで、サイバー攻撃が直接的な脅威と認識されるようになった。それに対応するための仕組みを日本政府内で作ることになり、この攻撃はそのための良い教材になったとの判断をしている。そして、3 月 19 日に日本政府全体の体制固めをした（図 1）。サイバー攻撃は自然災害と変わらないという位置づけで、いざというときには危機管理体制が動き出すようになっている。大規模サイバー攻撃は危機管理の対象であり、他の事案と同じように扱えるようになったことが大きな変化だという。

2008 年の春ぐらいから大規模サイバー攻撃への態勢を固めようという議論があったがなかなか進まなかった。しかし、2009 年の米韓での事件で一気に進んだという。

防衛省

2009 年 7 月の米韓への攻撃について、防衛省は管轄している情報通信インフラのほとんどがインターネットに依存していないため、大きな影響はなかったとしている[11]。ただし、米韓攻撃を受けて 2010 年 5 月に出された「国民を守る情報セキュリティ戦略」（後述）までは、システム・レベルのサイバー攻撃対処を考えてきた。しかし、2009 年 8 月の民主党への政権交代の影響もあって、安保・危機管理問題としてとらえるようになったと言うことはできるという。

防衛省にとっては、攻撃主体がどこかの国の政府であるかどうかはあまり問題ではなく、防衛という点ではあらゆる敵に対処しなくてはならない。攻撃主体を特定したり補足したりすることには防衛省としては関心がなく、防衛することが最優先である。

NISC

日本のインターネット利用者数が急増するのは 1999 年から 2000 年頃である。それに伴い、サイバーセキュリティ対策を進める必要性も意識されるようになってきた。それを受けて 2000 年 2 月に内閣官房情報セキュリティ対策室が設置された。そして、それは 5 年後の 2005 年 4 月に内閣官房情報セキュリティセンター（NISC）として格上げされた。さらにその翌月の 2005 年 4 月には情報セキュリティ政策会議が設置された。情報セキュリティ政策会議は、2005 年 5 月 30 日の IT 戦略本部長（つまり内閣総理大臣）の決定により設置された。2010 年 10 月現在の枠組みでは、議長は内閣官房長官で、議長代理は内閣府特命担当大臣（科学技術政策）がなっている。閣僚構成員としては国家公安委員会委員長、総務大臣、経済産業大臣、防衛大臣である。さらに民間からの構成員として企業人や学者 6 名が参加している[12]。NISC が情報セキュリティ政策会議の事務局となり、NISC のセンター長は官房副長官補（安全保障危機管理担当）が当たり、副センター長（内閣

[10] 2010 年 7 月 2 日に警察庁で行ったインタビューおよび公開情報に基づく。
[11] 2010 年 10 月 4 日に防衛省で行ったインタビューおよび公開情報に基づく。
[12] 筆者も構成員の一人である。

審議官）2 名、内閣参事官 5 名他、事務方のスタッフが数十名いる。

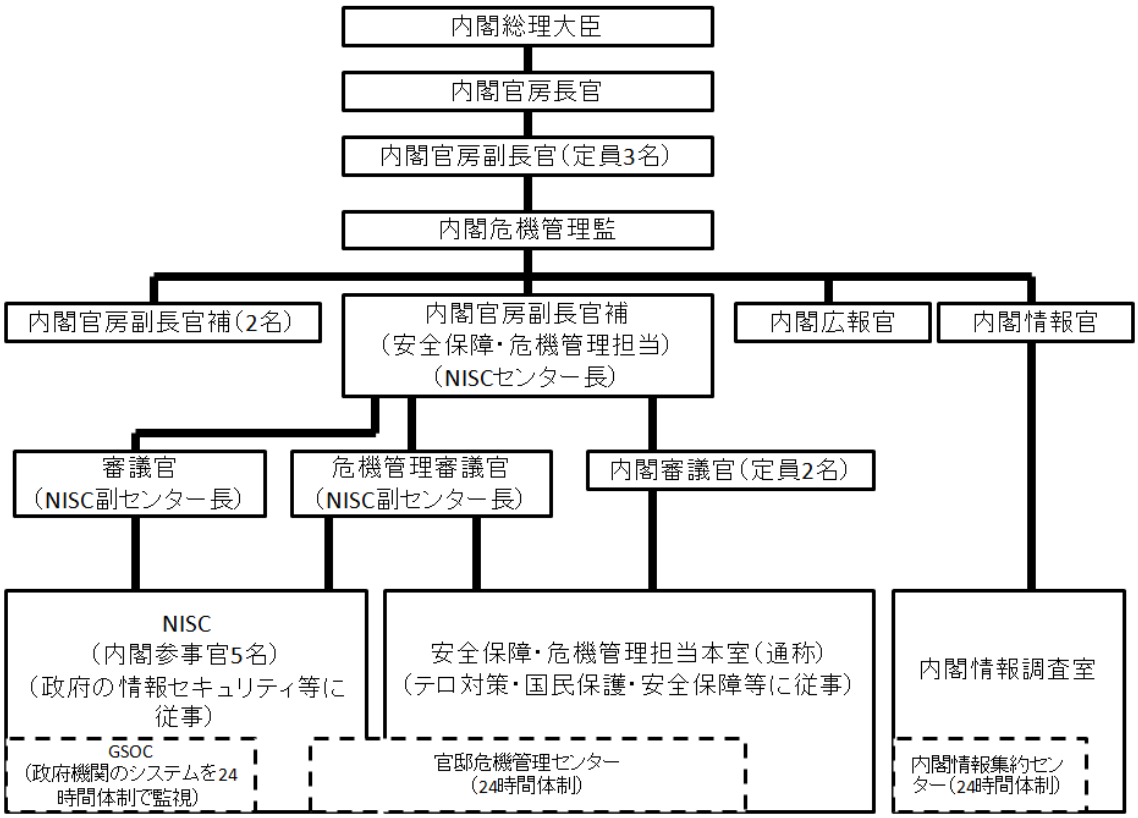

図 1　内閣官房の危機管理に関する組織

出所　警察庁資料に一部加筆

米韓同時攻撃への日本の対応

情報セキュリティ政策会議は 2006 年 2 月 2 日、「第一次情報セキュリティ基本計画―『セキュアジャパン』の設立に向けて―」を発表した[13]。この計画は2006年度から2008年度までを対象とする基本目標を提示し、2006 年度から年度毎の推進計画を発表することとした。そして、それを受け継ぐ「第二次情報セキュリティ基本計画―IT 時代の力強い『個」と『社会』の確立に向けて―」が 2009 年 2 月 3 日に発表された。これは2009年度から2011年度までをカバーするものである。

ところが、この第二次基本計画発表後の 2009 年 7 月、前述のような米韓への大規模なサイバー攻撃が起きた。また、同年 8 月の衆議院議員選挙において自民党が敗れ、民主党を中心とする連立政権が成立し、政権交代が実現した。そこで情報セキュリティ政策会議と NISC はこれまでの計画を見直し、2010 年 5 月 11 日、「国民を守る情報セキュリティ戦略」を発表した。この戦略は第二次基本計画を包含する 2010 年度から 2013 年度を対象とすることになり、毎

13 http://www.nisc.go.jp/active/kihon/pdf/bpc01_ts.pdf

年度の年度計画を作成することとした。「国民を守る情報セキュリティ戦略」の第1ページには以下のように書かれている。

> 「第二次情報セキュリティ基本計画」策定後、2009 年 7 月に米韓における大規模サイバー攻撃事態が発生したほか、大規模な個人情報漏えい事案の発生も後を絶たない。
>
> 特に、米韓における大規模サイバー攻撃事態は、経済活動や社会生活の多くの面において情報通信技術への依存が進む我が国にとって、情報セキュリティ上の脅威が安全保障・危機管理上の問題になり得ることを示す契機となった。

2009 年 7 月の米韓に対するサイバー攻撃は日本のサイバーセキュリティ対策の見直しに大きな役割を果たしたということである。

「国民を守る情報セキュリティ戦略」の基本方針は、第一に、サイバー攻撃事態の発生を念頭に置いた政策の強化及び対処体制の整備、第二に、新たな環境変化に対応した情報セキュリティ政策の確立、第三に、受動的な情報セキュリティ対策から能動的な情報セキュリティ対策へ、となっている。第一次基本計画、第二次基本計画でもサイバー攻撃は軽視されていたわけではない。しかし、「国民を守る情報セキュリティ戦略」ではそれが前面に出てきたことが注目に値する。

2010 年 9 月の最終週、米国の国土安全保障省が世界最大規模の官民サイバー演習「サイバーストーム」を実施し、これに日本の政府機関なども初めて参加した。参加国は 13 カ国 3000 以上になったという。日本からは NISC、警察庁、経済産業省からネット上の監視を委託された非営利団体 JPCERT／CC が参加した。JPCERT／CC は政府機関ではないが、実質的に最前線で日本のサイバー防衛を担っている組織と言って良いだろう[14]。サイバーストームはこれまで 2006 年 2 月と 2008 年 3 月に行われており、今回が 3 回目である[15]。

民主党政権の政策アジェンダの中でサイバーセキュリティはそれほど高い位置を占めているわけではない。例えば、2009 年 8 月に民主党政権が成立してから 9 ヶ月間、情報セキュリティ政策会議が開催されなかったことがそれを示している。当初、民主党は、自民党政権時代に設立された各種の閣僚が参加する会議を整理・廃止するとし、事業仕分けによってさまざまな政府予算も見直しを迫られた。そうした雰囲気の中で NISC の存在自体が仕分けの対象になるのではないかという懸念もあった[16]。しかし、他のさまざまな政策課題に埋もれて情報セキュリティ政策会議の存在自体が政府首脳には認識されていなかったというのが現実である。

「国民を守る情報セキュリティ戦略」を決定した 2010 年 5 月 11 日から約 1 ヶ月後の 6 月 8 日に鳩山由紀夫政権は終わりを告げ、菅直人政権が成立した。そして、新政権の下で 7 月 22 日に情報セキュリティ政策会議が開催され、年度計画である「情報セキュリティ 2010」が決定された。この中で「大規模サイバー攻撃事態への対処態勢の整備等」が最初に挙げられ、19 の施策が明示されている。

---

[14] 2011 年 3 月 11 日に JPCERT／CC で行ったインタビュー。

[15] 藤えりか「サイバー攻撃対策 13 カ国協調 米主導の訓練、日本初参加」『朝日新聞』2010 年 10 月 4 日。

[16] 実際、2009 年 11 月までに 18 の閣僚会議等が廃止された。
http://www.kantei.go.jp/jp/tyoukanpress/rireki/2009/11/17am_siryou.pdf

政策課題としてのサイバーセキュリティ

安全保障上の脅威を取り除くというインテリジェンス機関の役割の拡大は、冷戦後の東アジア情勢の変化に対処する上で、日本にとって重要な政策課題になっている。そして、近年のサイバー攻撃の可能性はインテリジェンス機関に新たな役割を付与することになった。インテリジェンス機関はその徴候を見つけ、未然に阻止することを目的としている。インテリジェンスの失敗は、大きな損害を生み出すことになる。未然に防ぐだけでなく、実際に行われた場合を想定した準備も必要である。

2009 年 7 月の米韓に対するサイバー攻撃は、日本のサイバーセキュリティ対策を進めることになった。民主党の政権交代という側面もあるものの、まだ残余期間の残っていた「第二次情報セキュリティ基本計画」を上書きする形で「国民を守る情報セキュリティ戦略」が決定されたことは大きな意味を持つだろう。

しかし、その中心的役割を担う NISC は、インテリジェンス機関としては定義づけられていない。警察庁や防衛省、あるいは本章では取り上げなかった内閣情報調査室、公安調査庁などが担うインテリジェンス活動を政策決定者につなげる役割を NISC は果たすことになる（図 1 にある通り、NISC センター長の内閣官房副長官補は、内閣情報調査室のトップである内閣情報官と、内閣危機管理監の下で並んでいる）。しかし、その役割は明白に定義づけされておらず、今後の課題となっている。

社会におけるインテリジェンス機関の役割の拡大は、プライバシー侵害などの面で別の問題を生み出す可能性がある。例えば、サイバーテロを防ぐために行政傍受（犯罪を未然に防ぐための通信傍受）を行わなくてはいけない可能性もある。しかし、日本の現行法制は犯罪捜査のための司法傍受は認めているものの、行政傍受は認めていない。計画倒れに終わらないサイバー防衛のための対策を NISC および関連機関は考え、実施して行かなくてはいけない。そして何よりも、情報セキュリティ政策会議、NISC、および関連機関をそうした対策の立案、実施、評価に向かわせる内閣の意志も必要である。

第５章　誰がサイバーテロ対策を担うのか
――行政機構の日韓比較から

日本のインテリジェンス機構に関する問題としてしばしば指摘されるのが、統合とガバナンスの不在である。インテリジェンスそのものの重要性は高く認識されつつあるものの、内閣官房、警察庁、防衛省、外務省などが個別に施策の精度を高める一方で、包括的なガバナンスの構築が欠落している。

ことサイバーテロ対策においては、これに加えて総務省、経済産業省が大きなアクターとして存在している。事案の性質も総合的な対策を必要とするものであることは言うまでもない。インテリジェンス機能の再編強化の過程のなかで、特に重要視されるべき分野であるといえるだろう。民主党政権は国家公務員制度改革、省庁再編に積極的な姿勢を見せていたが、インテリジェンス機構の再編に対する意識は決して高いとはいえない。サイバーテロ自体が通常は省庁のウェブサイト書き換え程度にしかイメージされない、勃発しないとわからない「見えない危機」であることもこうした対応の背景にあると考えられる。これは日本のみならず、各国の事例を一瞥しても同様である。

想定されうる事態に備えるのが危機管理の鉄則であるならば、先例に範を取って検討を進めていく必要があるだろう。そこで本章では、2009 年に大規模なサイバーテロ攻撃を受けた韓国を事例に、同事件以後の対応を中心にサイバーテロ対策機関の現状をまとめつつ、その長所と短所を明らかにしていきたい。

韓国のサイバーテロ対応機構

2007 年 7 月 7 日から 9 日にかけて、韓国はアメリカと同時に本格的なサイバーテロ攻撃に晒された。ゾンビ PC、ボットネットを利用した攻撃はきわめて広汎にわたり、その被害も甚大であったが、それ以上に精神的なダメージが大きかった。自らが一日の長を持つと自認している分野において大規模な侵入を許したことは、サイバー先進国を自負する韓国の自信と威信を大きく傷つけるとともに、「見えない敵」に対する脅威を現実のものとして認識させた。

その後、韓国はサイバーテロ対策の法的、行政的整備を急速に推し進め、「サイバーテロ対策先進国」となった。まずは同国の事例、とりわけ 2007 年以降の対応を見ていきたい。

その組織とガバナンス

韓国のサイバーテロ対応機構は、大きく政府部門、民間部門、軍事部門に分けて構築が進められている。サイバーテロ事態が同時多発的に起こり、かつ、ひとつの欠陥が大きなネットワークの被害につながることから、韓国ではこれら３つの部門を横断的に統治することの必要性が認識されるようになった。そのガバナンスを担っているのが国家サイバー安全戦略会議である。

図 2　韓国のサイバーセキュリティ体制

2004 年 3 月に大統領訓令（141 号）によって発足したこの組織は、きわめて実効的なガバナンス機能を有しているといわれている。同令には、以下のような規程がある[17]。

第 5 条

国家サイバー安全に関する政策及び管理については国家情報院長が関係する中央行政機関の長と協議してこれを総括・調整する。

第 6 条

1．国家サイバー安全に関する重要事項を審議するために国家情報院長に所属する国家サイバー安全戦略会議（以下、 戦略会議）を置く。

2．戦略会議の議長は国家情報院長とする。

3．戦略会議の委員は外交安保首席秘書官･放送通信委員会常任委員、金融委員会副委員長と戦略会議の議長が指名する関係中央行政機関の次官級公務員とする。

4．戦略会議は次の各号の事項を審議する。

1）国家サイバー安全体系の確立と改善に関する事項

2）国家サイバー安全に関する政策及び機関間の役割調整に関する事項

3）国家サイバー関連の大統領の指示事項に関する処置案事項

4）その他、戦略会議議長が付議する事項

5．戦略会議の構成、運営などに関して必要な事項は戦略会議の議長が別に定める。

議長となる国家情報院長にきわめて大きな権限と裁量が付与され、各部次官級によって会議を組織することでより実務的な統括が可能となっている。かつ、国家情報院次長（サイバーセキュリティ担当）を議長とし、戦略会議に関係する各省の室長・局長を議員とする「国家サイバー安全対策会議」が「戦略会議」の下部組織

17 「国家サイバー安全管理規定」大統領訓令第 141 号、2004 年。

として実務レベルで運用されている。周知のとおり、国家情報院はかつて中央情報院としてその圧倒的な存在感で知られたが、民主化以降、ひとたび安全企画部に格下げされていた。それがサイバーテロをはじめとする情報管理・保護の必要性が高まる中で、国家情報院と装いをあらためてふたたび独立した行政機構となったものである。

国家サイバー安全戦略会議が発足した同年には、国家情報院内に国家サイバー危機対応業務の総括・調整実務を担当する国家情報セキュリティセンターが新設され、みずからの手足も持つこととなった。さらに同院は政府部門電算網の保安点検、評価、情報保護の製品評価、認証制度なども担当している。その羈束が縦横に張り巡らされていることが理解できる。

この会議は定例ではなく、協議事項が生じた場合に召集される。2009 年の事件直後には国家サイバー危機総合対策をまとめ（8 月）、2010 年 4 月には国家サイバー安全管理規定の改定に取り組み、政府各部門にセキュリティ管理監視センターの設置を義務づけるなど、積極的で能動的な活動をみせている。

各分野を包括する法令整備も進められている。その代表的なものは 2001 年に制定された情報通信基盤保護法である。同法は重要施設を保護するために特に制定され、行政安全部が所管している。2009 年の事件を受けて、ゾンビ PC の跋扈を予防するための悪性プログラム拡散防止法案が放送通信委員会において策定、審議に付されたが、2011 年 7 月現在、制定を確認することはできない[18]。

政府部門

政府部門でサイバーテロに対応する主な行政機構は、行政安全部、国家安全情報課戦略室、国家情報院国家サイバー安全センターである。基本法である電子政府法（所管：行政安全部）を 2009 年以降 6 次にわたって見直したほか、「災難と安全管理基本法」（同）を改正し、「災害」の定義に「エネルギー、通信、交通、金融、医療、水道など国家基盤体系の麻痺」が入れられた。

個人情報の保護については、「公共機関の個人情報保護に関する法律」（行政安全部）が 2007 年につづいて、2011 年 9 月に大幅改正された。2011 年の改正は、個人情報の保護について、政府部門、民間部門を別々に取り扱うことの限界を認識した政府が横断的な立法に臨んだためである。その結果、韓国においても個人情報保護法（行政安全部、法律第 10465 号）が制定され、民間部門の「情報通信網知用促進及び情報保護等に関する法律」と政府部門の「公共機関の個人情報保護に関する法律」が横断的に結ばれることとなった。

行政安全部は、主に電子政府対応と個人情報保護を担っている。電子政府統合網及び政府統合電算センターの安全管理、個人情報保護及び各部署の情報保護、電子政府実現のための保安対策立案、施行が主な担当範囲であり、とりわけ李明博政権以降、拡大する人員・予算面での支援での役割が大きくなっているという。

これにくわえて、従来は旧放送通信部の職掌であった情報通信基盤保護委員会の運営など主要情報通信基盤施設の管理、電子署名ポリシーの立案、管理なども行政安全部に組み込まれることとなった。管理強化策の一環と言えるだろう。

国家情報院は、国家サイバー安全戦略会議・

18 韓国法制処の法令検索サイト（http://www.moleg.go.kr/main.html）による。

同対策会議を軸に国家サイバー危機対応業務の総括･調整を行うことが主な担務となっている。2004 年には国家情報セキュリティセンターが設置されている。そのほか、政府部門電算網の保安点検、評価や、情報保護の製品評価、認証制度などといったチェック・認証機能も有するようになってきている。

国防部門と捜査部門

国防部門は国防部の国防情報対戦対応センターが、国防電算網の安全と軍事機密へのハッキングの探知、予防、調査を担当している。ただし、今回の調査ではこの部分について詳細を知ることはできなかった。

事後における捜査態勢は、韓国においてもやや系統が入り乱れている印象がある。ネットワークを大規模に監視しているのは550 人のスタッフを有する KISA（後述）になる。ネットワーク上の異変については、ここを管轄する放送通信委員会が状況に応じて監視、注意、警戒と対応を行う。注意レベルに達した段階で対策本部が設置され、警戒レベルになると青瓦台への報告が義務づけられている。その後、事態は政府部門については行政安全部が、民間部門については放送通信委員会を中心に取りまとめ、同号調査段による協議を経て発表が行われる。

犯罪部分の捜査については、大検察庁・警察庁があたり、とりわけ警察庁サイバーテロ対応センターがその主軸を担うこととなっている。

民間部門

民間部門でのサイバーテロに対応する主な行政機構は、放送通信委員会（旧：放送通信部）、行政安全部の各部署、知識経済部となる。情報通信網知用促進及び情報保護等に関する法律（放送通信委員会）が基本的な位置づけとなり、近年の変化に対応して、電子金融取引法（金融委員会）、電子署名法（行政安全部）、位置情報の保護と利用等に関する法律(放送通信委員会)、産業技術流出防止法（知識経済部）、信用情報の利用と保護に関する法律（金融委員会）が整備されている。

放送通信委員会は、放送と情報通信網、民間分野のサイバー危機管理全般を所管し、保安業界と情報通信サービス提供者（ISP）の協力促進 、民間部門の情報保護政策立案、施行（情報保護技術開発、情報保護管理体系（ISMS）認証など）といったガバナンスから、民間分野のインターネット侵害自己対応、技術支援、サイバー攻撃の遮断、ゾンビ PC の除去、メディア対応 、平常時における全国的クリーン PC 運動など、現場に密着した対応を行う組織となっている。

同委員会は放送通信部から改組して発足した組織であるが、2009 年 7 月の事件を契機に予算は 4 倍になったという。電子商取引をはじめとして、民間部門で保護すべき情報は拡大し、現在はその 90%に到達すると言われている。それだけに現場に特化した対応を行う機動力のある機関になったと見ることもできるだろう。

放送通信委員会のもとで実際の対応に当たるのが韓国インターネット振興院（KISA） である。KISA では情報保護法制及び政策調査・研究、情報保護指針・ガイド開発・普及、法制度整備、情報保護の認証、評価などの実施支援（情報保護安全診断、ISMS 認証、情報保護システム評価･認証）情報通信網侵害のモニタリング、事故処理、原因分析及び事故対応など広汎な業務が行われている。550 人のスタッフの内 90 人はインターネット侵害事故対応センター（KISC）に所属し、リアルタイムの監視、対応に当たっている。個人情報侵害申告センター

などの運営も同院で行っている。

比較からみえてくるもの―日韓両国の抱える長所と短所

こうした韓国の対応機構の状況を見てくると、日本との比較で第一に挙げられるべきは統合とガバナンスの差であろう。韓国では国家サイバー安全戦略会議が極めて大きな権限をもち、国家情報院を中心としたガバナンスが機能しているように見受けられる。日本で同会議に対応する機関を求めれば情報セキュリティ政策会議とNISC（内閣官房情報セキュリティセンター）が該当すると考えられる。情報セキュリティ政策会議の議長は内閣官房長官が、議長代理は情報通信技術（IT）担当大臣が務め、国家公安委員長、防衛大臣、総務大臣、経済産業大臣などが構成員に充てられているが、活動はきわめて緩やかである。

政権の意向、意識に寄る部分も大きく、政権交代前は2008年12月、2009年2月、5月、6月と開かれていたものが、政権交代後は実に2010年7月まで会議は休眠状態となり、その後も2011年4月（持ち回り）、7月と政権の関心は薄い。実務レベルで主体的に動ける機能が必要とされる大きな理由となっている。

そうなると実質的な機能を期待されるのはNISCである。NISCはIT戦略会議以来の流れを継承し、内閣における総合調整の担い手となることが想定されている組織となっており、内閣官房に設置されている。しかし、センター長は官房副長官補、副センター長は内閣審議官であり、実質的な手足を持たない。このため、提言や対策の検討は民間有識者の協力を得ながら積極的に進められているものの、NISC自体が韓国の国家サイバー安全戦略会議や国家情報院のように主体的かつ能動的にサイバーテロ対策に動くことは想定されていない。周知のとおり、日本ではインテリジェンス機関が内閣官房（情報調査室）、警察庁、防衛省、総務省、経済産業省に分散し、統合されたガバナンスの不在が指摘されている。サイバーテロ対策についても同様に統合機関の設定が必要となっているが、分担管理原則の前提もあって、状況は前進していない。

しかし、韓国の側の問題もないわけではない。基幹となる国家サイバー安全戦略会議の設置根拠は大統領令である。2003年の事件を契機に早期に設立するためには大統領令による設置は合理的であったが、それが法制化されずに長期に亘ってそのまま存続していることには民主主義国家として疑問が呈される点であろう。事実、韓国国内では2010年1月に国家情報院が50周年を迎えるにあたり、同院の権限調整を必要という主張がみられるようになり、その議論の中で国家サイバー安全戦略会議の設置根拠を法制化する必要も指摘されている。

法制化されていない機関による統治は、既存の法制化されている機関の反発も招きかねず、早期の制度整備が必要であることは言を俟たないだろう。しかし、法制化に際しては機能調整の議論が再燃する可能性もあり、その結果によっては同会議によるガバナンス機能が低下することも考えられる。韓国政府がこの状況を放置している原因の一部はこのあたりに起因していると考えられるだろう。情報収集・管理の徹底と民主的な運用のバランスの難しさはここにも現れている。

もうひとつ、人材養成の観点からすると、韓国側の強い組織機構は歴史的に負の側面を内包している。近年、韓国でもサイバーテロ対応、情報管理に高い専門知識を有する人材を育成す

る必要が認識され、政府の支援により高麗大学に情報保護学専攻、KAIST に情報保護研究科知識保安プログラム（修士課程）が新設され、育成が進められている。暗号の解読には自然言語の知識・理解も重要とされ、とりわけ北朝鮮対応を考えるうえでは韓国人技術者の養成が急務となっているようである。

しかし、学生たちのあいだには国家情報院に対していまだ中央情報院時代の負のイメージを持つ者があり、彼らの父兄に至ってはよりその傾向が見て取れるという。歴史的に強い組織ゆえのガバナンスの成立は、ソフト面においてその強化と継続を困難にしている側面があることも否定できない。こうしたことから、KISA、KISC においても中途採用が主体となっており、採用時の身辺調査のコストも相当なものとなっているようである。

日韓間、もしくは日米韓間に視点を移せば、どのように同盟国間で情報共有、危機への教導対応をしていくかも課題であろう。サイバー犯罪自体はボーダレスに行われる一方で、対応側には国家と行政機構ごとの壁が存在している。日本の警察庁は国家情報院に対応する組織ではないため、同院に入ることすら叶わない。交流を行う場合の階級も総じて日本の側が低く、困難が多いと言われる。現状と危機の性質にかなった対応の必要性は日を増して高まっていることを前提にした組織改編が必要となっているように思われる。幹部職員のバスケット制を含んだ国家公務員法改正、インテリジェンス機関の再編を含む省庁改革の実施が待たれる。

第６章　結論

――サイバーセキュリティへの組織的対応

今後の情報セキュリティをめぐる問題は、「国家主権の衝突」という、より深刻な問題に向かっていくだろう。すでに国境を越えるサイバー攻撃が行われていることはこれまで論じてきた通りである。それは宣戦布告なき戦争だといっても過言ではない。しかし、その攻撃者のほとんどは捕まっていない。ネットワークの霧の中に隠れている攻撃者たちを捕まえるのは至難の業である。それを可能にするには、各国の法執行機関、情報機関、民間組織の協力が不可欠である。

それにもかかわらず、IT をめぐる法制度は各国でバラバラであり、越境して適用することはできない。そこに法管轄の壁が存在するからである。「国際協力、国際連携」という言葉を口にするのは簡単だが、相手が同盟国ではない場合、さらには敵対する国である場合、協力の可能性は著しく低下する。

もはや情報セキュリティは、コンピュータが動かなくなるというだけの問題ではない。国民の人権、財産、そして命に関わるようになってきている。「標的型攻撃」といわれる攻撃は、すでに政府の内部、企業の内部奥深くにまで達しており、看過できる状態ではない。そうした「見えない攻撃」の浸透が、将来のいっそう深刻な攻撃につながる可能性がある。

サイバーセキュリティ問題に日本がいかに対処していくかを考えていく際、どうしても避けられないのが、錯綜する権限の問題である。サイバーセキュリティ問題は、日本政府の中では、第一義的には経済産業省と総務省が対応すべき問題である。それは多くの場合、コンピュータや携帯電話といったデジタル情報通信機器を介するものであり、通信を用いるものである。コンピュータや携帯電話といった情報通信機器は経済産業省が所轄する産業であり、通信は総務省の所轄である。実際、経済産業省は商務情報政策局の下に情報セキュリティ政策室を持っている[19]。また、総務省は、情報流通行政局の下に情報セキュリティ対策室を持っている[20]。コンピュータ・ウイルスは通信を使って感染する場合が非常に多いので、両省の協力とイニシアチブが不可欠である。

実際のサイバーセキュリティ対応という点では、JPCERT コーディネーションセンターの役割も欠かせない。特定の政府機関や企業からは独立した中立の組織として、日本における情報セキュリティ対策活動の向上に積極的に取り組んでいる。さらに、各国の CERT（Computer Emergency Response Team）や CSIRT（Computer Security Incident Response Team）とも非営利ベースでつながり、協力を得ることができるのも JPCERT の強みである。

---

19 同室は「情報セキュリティ政策ポータル」というサイト（http://www.meti.go.jp/policy/netsecurity/）を運営している。

20 同室は「情報セキュリティホームページ」というサイト（http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/security.html）を運営している。

また、独立行政法人情報処理推進機構（IPA）は政府と民間の接点としてさまざまな支援業務を行っている。

しかしながら、ここまでの組織ができることは、サイバー犯罪の予防と被害対応である。一線を越えた犯罪の捜査と容疑者の逮捕、さらには軍事的な攻撃からの防衛やそれに対する反撃ということになると、警察や軍隊の役割になる（無論、日本の場合では、軍隊ではなく、自衛隊ということになる）。

米国ではUSCYBERCOMを設置し、軍事的な対応を明確にした。中国の人民解放軍にもサイバー攻撃・防衛を担う組織が設置されている。日本でも自衛隊の統幕にサイバー企画調整官のポストが設置された。それにも関わらず、依然としてどこまでが軍事的な攻撃で、どこからが違うのかという点については、はっきりした線引きができていない。国際法の研究者たちの間でも定説が固まっていない。

また、サイバー攻撃では、実際に攻撃が行われてからの対応では遅く、それを未然に防ぐことが重要性である。そこで必要になるのがインテリジェンス機関である。インテリジェンス機関については失敗がことさら取り上げられることが多い。しかし、インテリジェンス機関がテロやサイバー攻撃を未然に防ぐことができても報道されることはなく、一般の人々にもその成果は伝わらない。したがって、インテリジェンス機関の有効性がどれくらい実際にあるのかを判断するのは難しいといえるだろう。

それにも関わらず、事前にサイバー攻撃を察知し、首謀者をとらえたり、攻撃を回避できたりする可能性があるとすれば、インテリジェンス機関を使わないというオプションはないだろう。実際、米国ではインテリジェンス・コミュニティの一角を担うNSA（国家安全保障局）の局長がUSCYBERCOMの司令官を兼務するという形で、強くインテリジェンス機関とサイバーセキュリティは結びついている。韓国ではインテリジェンス機関の総元締めである国家情報院（NIS）の院長が議長となる国家サイバー安全戦略会議が設置され、サイバーセキュリティの中心となっている。日本では、公式な形では内閣情報調査室をはじめとするインテリジェンス機関が内閣官房情報セキュリティセンター（NISC）の活動には協力していない。しかし、非公式レベルでは協力が行われているようである。

日本のインテリジェンス機関は、内調の他にも、警察庁、防衛省、外務省、公安調査庁などに分散され、緩やかなコミュニティを形成しており、それぞれの省庁においてサイバーセキュリティは取り組むべきアジェンダとして急速に上昇してきている。内調とNISCの間の協力が、公式でも非公式でも拡大させることが必要になるだろう。諸外国とのインフォメーションおよびインテリジェンスの交換・共有のためにもインテリジェンス機関の関与拡大が求められている。

2011年9月以降の一連の報道は、日本のサイバーセキュリティ対策見直しのきっかけになるだろう。日本のこれまでの対策は2000年の大規模なウェブページ改ざんによって始まった。2009年7月の米韓への攻撃は日本政府の意識を変え、2010年5月に「国民を守る情報セキュリティ戦略」として結実したが、その本格的な実施・遂行が必要になっている。必要とあれば、戦略を見直すことも必要になるだろう。その上で、三つの点を指摘したい。

第一に、三菱重工へのサイバー攻撃が報道されるまでは、民主党政権は自民党時代と比べてこの問題にあまり関心を持ってこなかった。少

なくとも情報セキュリティ政策会議の開催頻度や時間設定は減ってしまっていた。2010 年以降は、政策会議が開かれるたびに情報セキュリティ政策会議の議長である官房長官が代わっており、毎回議論をやり直さないといけない状況になっている。

第二に、総理大臣決定だけで設置されている NISC は他の官庁と比べて基盤がどうしても弱くなり、人材も生え抜きではなく出向組でできているので、強力なリーダーシップを発揮しにくくなっている。報道では NISC のリーダーシップの欠如を批判するものが多いが、そもそもそれが不可能な体制になっていることを認識すべきである。

第三に、各国のサイバーセキュリティ対策は、インテリジェンス機関が主導している。日本ではインテリジェンス活動が広く 認知されているわけでもなく、政府・民間に覆い被さるセキュリティ・クリアランス（保秘制度）も整っていない。そのため、海外の政府との情報交換・共有がしにくい。政府は、2010 年の尖閣諸島問題のビデオ流出を受けて「機密保全法」の検討を開始したが、これは公務員による情報漏洩の罰則強化だけにとどまる見込みであり、本格的なセキュリティ・クリアランスの確立には至らない見込みである。

サイバー攻撃は各国共通の課題になりつつあることから、今後は国際的なフォーラムでの検討が進むことだろう。そこで、今後のシナリオとしては、三つ考えることができるだろう。

第一に、政府主導のサイバースペース規制の進展である。この場合、サイバー犯罪条約の厳格な運用が求められるようになり、国連等での議論も行われるようになるだろう。しかし、現実にはその運用は難しく、先進国と発展途上国、あるいはその他の対立軸が生まれる可能性がある。

第二に、非政府組織主導の秩序の形成である。政府主導の秩序形成がうまく行かない場合、非営利組織である CERT および CSIRT のネットワークを使ったコーディネーションやガバナンスがデフォルトの形で進む可能性がある。しかし、各国の CERT/CSIRT の運営形態はまちまちであり、簡単にはいかないかもしれない。特に国家主権、政府による管理を主張する国々ではうまくいかない可能性がある。

第三のシナリオは、国際的な協調が失敗し、対策が民間事業者にゆだねられる場合である。特に、通信事業者がネットワークの安全性に責任を負うようになり、いわゆる DPI（Deep Packet Inspection）の制度化が進む可能性がある。DPI は通信の内容に応じた制限を行うことであり、いうまでもなく通信の秘密に抵触する可能性がある。しかし、サイバー攻撃による被害が拡大すれば、通信の秘密の制限が社会的に合意される可能性もあるだろう。

外国からのサイバー攻撃は各国間の主権の衝突につながる難しい事態を作り出す。外国にいる攻撃者を特定し、身柄を拘束することはきわめて困難である。したがって、想定外の事態を想定する努力を行い、被害を未然に防ぎ、かつ最小化する措置をとるべきだろう。

サイバー攻撃はこれからも高度化を続け、知らない間に被害に遭っている、被害に遭っていることすら気がつかないというケースが出てくるだろう。対策を急がなければならない。