The 21st Century Public Policy Institute

21世紀政策研究所　研究プロジェクト

サイバー攻撃の実態と防衛

報 告 書

2013年5月

21世紀政策研究所

はじめに

さまざまな形でのサイバー攻撃はすでに 2000 年頃から広く認識されていた。日本でも政府の省庁を狙った大規模なウェブ書き換え事件が 2000 年に発生しており、それに対応する政策がとられた。2005 年には内閣官房情報セキュリティセンター（NISC）が設立され、ほぼ同時に内閣官房長官を議長とし、関係閣僚と民間有識者が参加する情報セキュリティ政策会議も設置されている。しかし、2000 年からの約 10 年間の認識は、サイバーセキュリティはあくまで技術的な問題であり、国家安全保障や危機管理の問題とはされていなかった。

2010 年頃からサイバーセキュリティは非伝統的安全保障の一環として急速に注目されるようになってきた。安全保障の文脈で「セキュリティ」という言葉を使うとき、そこには「防衛」だけでなく「攻撃」の意味も含まれる。そして、サイバーセキュリティではそこに「利己的な利用、搾取」という本来の意味から変化した「脆弱性の探究、悪用」といった意味での「エクスプロイテーション（exploitation）」も付け加わる。従来の兵器による攻撃や防衛は目に見える形で行われることが多かったが、サイバースペースでは目に見えない形でのシステムへの侵入や情報の抜き取りも重要な一部を占める。

2011 年秋からは、大々的にサイバーセキュリティがメディアを賑わせるようになった。特に注目を浴びたのは軍需産業の雄、三菱重工業への標的型メール攻撃であった。しかし、これは氷山の一角でしかない。「サイバー戦争」というとき、国家と国家の戦いというイメージが生じるが、実際には政府機関とともに企業も多くの被害に遭っている。2009 年の日本の事業所数は 588 万 6193 あったが、300 人以上の従業員を持つ事業所数は 1 万 1908（0.2%）しかない[1]。ほとんどすべてが中小企業である。中小企業だからといって傑出した技術を持っていないというわけではない。そうした企業の技術が狙われることもある。しかし、サイバーセキュリティ対策にまで資金が回っているかというと、その実態はおぼつかない。

政府が政府の情報通信システムを守らなくてはならないことはいうまでもない。国レベルでは、NISC がその司令塔の任を担っている。しかし、政府が企業の情報通信システムや情報資産を守ってくれるわけではない。基本的には企業の自助努力が不可欠である。情報通信技術（Information Technology：IT）に投資し、それを活用しようとするすべての企業は、その負の側面に留意し、対策をとらなくてはならない。

1　総務省統計局「産業、経営組織別事業所数及び従業者数」<http://www.stat.go.jp/data/nenkan/pdf/yhyou06.pdf>（2009 年）。

本報告書は、自らの責任としてサイバーセキュリティを企業が行う際に留意する点とは何かを検証し、いくつかの提言をまとめたものである。

第 1 章では、ある企業が受けたサイバー攻撃が、産業全体、社会全体に波及し、最悪の事態が起きる可能性を示した。

第 2 章では、サイバー攻撃を三つの手法に大別して概要を示した。

第 3 章では、サウジ・アラムコとコカ・コーラ、AP 通信の事例を検討する。

第 4 章では、サイバー攻撃をしている側として疑われている国の一つである中国の実態について、公開情報を元に迫る。

第 5 章では、こうしたさまざまなサイバー攻撃に対して、米国、英国、日本の各政府がどのような対応を取っているのかを示す。

そして、第 6 章では、企業経営者たちが、サイバー攻撃に対処するための方策について、10 箇条をまとめた。

本研究プロジェクトは、2012 年 7 月に活動を開始した。メンバー間による議論、ゲストを招いての議論、米国ワシントン DC（2012 年 12 月）および英国ロンドン（2013 年 3 月）での調査の結果をまとめたのが本報告書である。

2013 年 5 月
21 世紀政策研究所研究主幹
土屋　大洋

企業経営者のためのサイバーセキュリティ 10 箇条

【攻撃が起こる前】

1. 狙われないようにする
2. 専門家の話を聞く
3. 過去の経験は役に立たない
4. 情報セキュリティ投資は必要不可欠なコストである
5. 守れない規則を強要するな
6. 記録を残せ
7. 内部犯行の可能性を忘れない

【攻撃が起こった後】

8. 事実関係を承知してから判断をする
9. 対策の優先順位付けをする
10. 情報を共有する

目　　次

研究委員一覧

研究主幹

土屋　大洋	慶應義塾大学大学院政策・メディア研究科教授

研究委員

伊東　　寛	㈱ラック理事、サイバーセキュリティ研究所長
大澤　　淳	世界平和研究所主任研究員
加茂　具樹	慶應義塾大学総合政策学部准教授
野原佐和子	㈱イプシ・マーケティング研究所社長
早貸　淳子	JPCERT コーディネーションセンター専務理事
続橋　　聡	経団連産業技術本部長

オブザーバー

小野　雅史	第一生命経済研究所政策研究部課長（当時）

21 世紀政策研究所

篠原　俊光	21 世紀政策研究所主席研究員
泉地　賢治	21 世紀政策研究所研究員

第 1 章　最悪のシナリオ[2]

深夜、午前 2 時。電話が鳴り響いた。妻子を起こさぬように気遣って受話器をとる。情報セキュリティ担当者からだった。彼は、副社長と会議中だった。電話の理由は、開発部門のネットワークに接続されたプリントサーバーを介して大量のデータが盗まれたという情報を、情報セキュリティオペレーションセンターが受け取ったことを知らせるためだった。

情報セキュリティ担当者によると、会社が過去 10 年にわたって取り組んできた技術のほぼすべてに関する計画書や設計、販売用資料が社内のネットワークから盗まれたらしい。最新の技術も漏洩し、研究開発部門も同じ記憶装置を使用していたため、同部門が保存したデータもすべて漏洩した可能性がある。

何者による仕業かは分からないが、事故に対応した社員は一時ディレクトリに 500 個以上の暗号化圧縮ファイルを確認している。ファイルはすべて標準的な CD-ROM の容量ほどの大きさで、ネットワークを介して転送するために事前に一時ディレクトリに用意されていた。アウトソース先のセキュリティオペレーションセンターは、開発部門から営業部門のサーバーへファイルを大量転送している最中に、外向きのインターネット回線が危うく溢れそうになったことで、情報の窃盗行為を発見した。接続内容を監視する準備に手間取り、ようやくそれに着手した時、それに気づいた攻撃者は活動を中止したが、残されたファイルはすでにほんのわずかだった。

どのようにして起きたのか。攻撃してきたのは誰なのか。なぜもっと早い段階で発見し阻止できなかったのか。実際にどの位の量のデータが奪われたのか。正確なところ、われわれは何を失ったのか。

情報セキュリティ担当者の説明はこうだ。このような攻撃は APT（Advanced Persistent Threat：先進的で執拗な脅威攻撃）と呼ばれている。その攻撃は深く静かに行われるために、なかなか気づかれることがない。特に、最初の攻撃自体は、非常に巧妙な「ソーシャル・エンジニアリング」と呼ばれる手法によって事前に狙った相手の情報をよく調べた上で行われる。これは、悪意のあるコードを含むメールを送ってくるのだが、それがいかにも知っている人から届いたメールを装っているため、経営陣がこのようなメールを受け取ったとしても、何の疑問も抱くことはない。

2　本章の記述は、一般社団法人 JPCERT コーディネーションセンターによる「経営者が知っておくべきセキュリティリスクと対応について」<https://www.jpcert.or.jp/research/aptrisk.html>に加筆・改変したものである。

そして、受け取った電子メールを開いた際、またはメールの本文に記述してあるリンク先をクリックした際に、コンピュータに悪いソフトウェアがダウンロードされる。そのソフトウェアは、コンピュータの持つさまざまな脆弱性を利用して攻撃する。多くの場合、攻撃により内部で使われている認証情報が奪われ、遠隔管理ツールによって操作されるようになる。こうなれば、攻撃者はシステム内部でなんでも行うことができる。

こうした攻撃者はしばしば、企業が所有する機微な情報、競争優位性のある知的財産、事業やプロジェクトに関する経理情報、営業情報、および企業の合併・買収に係わる文書を狙って収集する。

今回のケースでは、攻撃者は当社が開発している内容を正確に把握しており、当社が開発した技術に関する極めて限定的な情報をシステムから収集したのだ。しかも攻撃者は当社の利用者全員の認証情報も取得している。彼らは再び攻撃してくると思われるが、その時には攻撃に気付くことはできないだろう。現在、セキュリティベンダーと共同で作業を行っているが、ベンダーも解決策を見出せないでいる。

「取締役会には何と報告すればいいのだ。」「顧客にはどのように説明しよう。」

社長は頭をフル回転させながら車を会社まで飛ばした。会社には少しやつれた顔をした情報セキュリティ担当者と副社長、そして彼らのスタッフたちが対応を検討していた。数時間後には市場がまた開く。このニュースをどう市場に伝えるか、株主に伝えるか。対応を誤れば、この会社は信頼を失い、存亡にかかわる事態になる。

その時、社長の頭の片隅で悪魔がささやいた。「この事実を知っているのはここにいる人間と、攻撃者だけだ。他に誰が知り得るだろう。いずれ誰かがしゃべるかもしれない。しかし、すぐに発表する必要はない。少なくとも対策を打ってから発表すべきだ。そうしなければもっと投資家たちから責められることになるだろう。」

社長はその場にいる全員に呼びかけた。「いいか、これは当面の間、極秘だ。絶対にしゃべってはいけない。ここにいるわれわれだけで解決するんだ。有効な対処法が見つかるまで、死に物狂いで対応するんだ。」外部のセキュリティベンダーから来ているエンジニアたちには守秘義務がある。彼らは漏らすことを許されていない。当面は漏れないだろう。

朝 9 時、市場は何事もなかったかのように開いた。株価は大きな変動を示してはいない。秘密は守られているようだ。通常の業務を続けるような振りをしながら、社長は、副社長と情報セキュリティ担当者からの連絡を待った。ログが改ざんされており、侵入経路がはっきりしない。一刻も早く各種のパスワードを変更し、その他の対応をとりたい。しかし、それでは異常事態が起きていることが、他の社員に知れてしまう。その前

に侵入経路を特定し、二度と同じことが起きないようにしなくてはならない。

確固たる対応がとれないまま、市場が閉まろうとしているとき、官邸記者クラブで働く大学時代の同期から電話がかかってきた。総理大臣がまもなく記者会見し、サイバーセキュリティについて触れるという。はたして、記者会見は多発するサイバー攻撃への対応を呼びかけるものだった。総理大臣は記者会見の中で次のように述べていた。

> わが国は急増するサイバー攻撃の脅威にも直面しなければなりません。今やハッカーたちが人々の ID を盗み、私的な電子メールにこっそり入り込んでいることが分かっています。外国政府や企業がわが国の重要な機密情報をかすめとっていることを知っています。敵はわれわれの電力網、金融機関、航空管制システムを破壊する能力も持とうとしています。何年か経ってから振り返り、われわれの安全保障と経済にとっての真の脅威に直面していたのになぜ何もしなかったのかと考えるわけにはいきません。政府は今般、新しいサイバーセキュリティ戦略をまとめました。わが国の国家安全保障、雇用、そしてプライバシーを守るために、情報共有を円滑に行い、さらに高度な態勢を整備することによってサイバー防衛を強化するものです。

社長は、総理大臣が自分たちの会社へのサイバー攻撃を知っているのではないかという錯覚に陥った。まさにこの会社は、重要インフラストラクチャの制御システムを開発している会社だったからである。したがって、自社にとって競争優位となる技術情報が盗まれたというだけではない。重要インフラストラクチャそのものが危機に陥る可能性が、盗まれた情報には秘められているのだ。もはやそれを取り戻すことはできない。情報はいったん誰かの手に渡ってしまえば、物のように取り戻すことはできないからである。

その週の後半、同業他社にも、密かにサイバー攻撃が始まっていた。最初に狙われた企業から盗まれた情報を元に、本物そっくりのメールが作成され、文法的にもまちがいのないメールが同業他社に送信されてきた。そのメールに添付されていたファイルにはウイルスが仕込まれていた。攻撃者は市場で手に入るあらゆるウイルス対策ソフトウェアを購入し、事前にそれらにひっかからないことを確認した上で、巧妙にメールは送られた。最初に被害にあった企業のメールを解析し、同業他社の社員ひとりひとりが使っているパソコンの OS とメールソフトウェアのバージョンをヘッダー情報の解析からつ

かんでいた。いとも簡単に、第 2、第 3 の被害企業が誕生し、サイバー攻撃の被害は、知らない間に業界全体へと広がり始めていた。

それから 2 週間、社長は、サイバー攻撃を知らせる電話を受けたときに感じた冷や汗を忘れてはいなかった。しかし、手口はいま一つはっきりしない。時間だけがじりじりと過ぎ、疲労とともに深刻感も薄れてきてしまっていた。

その時、ブーンという大きな音ともに、部屋の照明が一瞬消えた。机の上のデスクトップパソコンもダウンしてしまった。しかし、すぐに非常電源が起動したようだ。いろいろなものが順次起動していく。「停電か。」なにやら嫌な予感を感じながら、社長はデスクトップパソコンの電源スイッチを押した。ウイーンとパソコンは起動を始めたが、様子がおかしい。ブルースクリーンと呼ばれる青のデスクトップに白いコマンド文字が並ぶ画面になり、そこから進まなくなってしまった。画面の文字には、OS が入っていないので起動できないと書かれている。さっきまで動いていたパソコンの OS が消えるとはどういうことか。

社内が騒がしくなり始めた。同じようなことが会社の各所で起こっているようだ。副社長が部屋に飛び込んできた。「テレビを付けてください。電力網がおかしくなっているようです。」

テレビを付けると同時に携帯電話が鳴った。制御システムを納入している電力会社の幹部からだった。発電所の制御盤の計器は正常を示しているのに、実際の動作が不安定だという。対処方法が分からないのですぐに来て欲しいとのメッセージだった。しかし、その通話も最後まで聞き取れないうちに切れてしまった。何かが起きている。

テレビのニュースは、首都圏の各地で起きている異常を報告していた。電力だけでなく、それに連動して鉄道や空港などが正常に運行できなくなり、道路にも渋滞ができはじめている。

取引先の企業からの問い合わせを持った部下たちが次々と社長の部屋にやってくる。社長には事態が理解でき始めていた。そうだ。あのサイバー攻撃だ。あれが起点になり、連鎖的な攻撃が始まっているのだ。いや、そうではない。うちが最初ではない。そう信じたい願望が湧き起こってくる。しかし、いずれにせよ手遅れだ。

今度は情報セキュリティ担当者が飛び込んできた。「ようやく見つけました。こいつです。このノートパソコンのログを詳細に調べたら、わずかに異常な通信の繰り返しを見つけました。使っている奴に問い詰めたら、家に持ち帰ってネットにつないだそうです。SNS 経由か何かでマルウェアをダウンロードしてしまったんでしょう。あれほど口酸っぱく家に持って帰るなと言っておいたのに。」情報セキュリティ担当者は悔しそ

うだった。

官邸記者クラブの友人によれば、内閣危機管理監が緊急参集チームを招集しているようだ。テロの可能性が高まっているということだ。これまではネットワーク越しの攻撃だったが、物理的な攻撃が始まる可能性がある。

悪いニュースは続いた。もう誰も使わず、部屋の隅っこで忘れられていたファクシミリ機がガタガタと動き出した。出てきたのは最新のシステムを納入したばかりの原発からのメッセージだ。制御システムの様子がおかしいという。そこも狙われたのだろう。

さらに気の滅入る情報がテレビで報じられた。中国が艦船を台湾近海に集め始めたというのだ。北朝鮮もまた 38 度線近くに軍を移動し始めており、在日米軍、在韓米軍は警戒態勢に入るとともにワシントン DC からの指示を待っているとのことだ。もし、戦争になったりしたら、米国は助けに来てくれるのだろうか。そもそも、米国への攻撃は行われていないのだろうか。ひょっとすると米国でも混乱が起きているかもしれない。

以前、聞いた話では、米軍は商用ネットワークから回線を借り受けている。これはハワイを経由して日本と米国をつないでいる海底ケーブルに依存している。これが機能していないとすると大変だ。海底ケーブル陸揚げ局が狙われ、物理的に破壊されたりしたら復旧は簡単にはいくまい。その場合、政府の国際通信は一気に人工衛星経由に移行するのだろうが、使える回線数が少なく、会話にも遅延が生じる。これまで慣れてきたようなビデオ通話はできない。衛星経由による遅延にイライラしながら音声だけでやりとりしなくてはならないだろう。このような混乱時に意思の疎通が充分にできないことほど恐ろしいことはない。実際はどうなっているのだろうか。

中東の動きも徐々に不穏になっているようだ。イスラエル軍のネットワークにもサイバー攻撃がかけられているらしい。シリアやイランが探りを入れるように軍を動かし始めている。中東情勢が動けば欧米の市場も敏感に反応する。すでにロンドン市場では株価が全面安に転じていた。ユーロ危機で打撃を受けたヨーロッパ経済はどうなるのだろうか。

社長は自分の椅子にぐったりと座り、他人事のように成り行きを見守るしかなかった……。この事態が収拾されたとき、この会社はもはや存在を許されないだろう。自分はどのような責任を問われることになるのか。なぜあのとき、最初の攻撃を公表し、関係機関と情報共有をしなかったのか。しかし、誰と情報を共有できたというのだろう。ライバル会社だろうか。いや、少なくとも取引先の企業に警告はすべきだっただろう。警察にも協力を求めるべきだったかも知れない。警察がやってきて、会社のサーバーを洗

いざらい調べていくことになったかもしれないが、でもこの目の前の事態よりはましだったかもしれない。この事態は収拾されるのだろうか。この国は復活できるのだろうか。世界の国々はどんな混乱に陥っていくのだろうか……。

第 2 章　多様なサイバー攻撃の発生

2.1　韓国へのサイバー攻撃

3 月 20 日午後 2 時、韓国の報道機関や金融機関で、社内イントラネットにつながるコンピュータが一斉に動かなくなった。直接の引き金は各企業の社内ネットワークに広がったマルウェアで、このマルウェアが PC のハードディスクのマスターブートレコード（MBR）[3]を破壊した上で、ハードディスクを特定の文字列で埋め尽くし、PC を動作不能にした。このサイバー攻撃は、KBS、MBC、YTN といった放送局や新韓銀行、農協銀行の社内ネットワークの 4 万 8000 台の PC をダウンさせ、銀行の ATM が使用不能にするなど、大きな被害をもたらした。

この韓国へのサイバー攻撃は、北朝鮮によるものだと韓国政府は後に発表した。この攻撃は、朝鮮半島の安全保障上の緊張の高まりの中で発生している。2 月 12 日に行われた北朝鮮による第 3 回目の核実験が発端であったと考えられる[4]。北朝鮮の核実験に対して、国連安全保障理事会は 3 月 7 日に緊急の会合を開き、北朝鮮に対する制裁決議（安保理決議 2094）を全会一致で採択している[5]。この制裁決議は、従来中国の反対で要請にとどめていた金融制裁や貨物検査を加盟各国に義務づける厳しいものであり、これに対して北朝鮮は非常に激しく反発し、3 月 8 日に 1953 年の朝鮮戦争の休戦協定を白紙化すると宣言した。

さらに、韓国での大規模なサイバー攻撃が行われた 1 週間前の 3 月 15 日、北朝鮮のインターネットサーバーが「集中的かつ執拗なウイルス攻撃」を受けているとして、北朝鮮は米国と韓国を非難している。北朝鮮へのサイバー攻撃の犯人はアノニマスであるという指摘も見られるが、米韓による防衛的対抗措置だった可能性も、現時点では否定できない。韓国へのサイバー攻撃が起きたのは、米韓による示威的な軍事演習「キー・リゾルブ」の真っ最中であった。

北朝鮮の挑発的な態度が朝鮮半島情勢の緊張を高める中、国と国の対立が、戦場とい

3　起動時のハードディスクの読み込み先を記述したもの。

4　2013 年 2 月 12 日 11 時 58 分頃、北朝鮮は第 3 回目の核実験を実施したと見られる。米国地質研究所によれば、地震規模は M4.9 で、震源は北朝鮮北東部の同国核実験場付近、震源深度は約 1 キロ。今回の核実験の規模は、2006 年の第 1 回目、09 年の第 2 回目と同様数キロトンの規模と推定される。

5　United Nations Security Council, “Security Council Strengthens Sanctions on Democratic People’s Republic of Korea in Response to 12 February Nuclear Test,” United Nations Security Council <http://www.un.org/News/Press/docs/2013/sc10934.doc.htm> March 7, 2013.

う場所ではなく、サイバースペースという目に見えにくい場所で、ホットな戦いという形で行われていたのが 3 月の韓国でのサイバー戦争であった。

国際安全保障のつばぜり合いが、サイバー上でのホットな戦いとして浮上してきているのが、ここ 5 年のサイバー戦争の実情である。2007 年のエストニア、2008 年のグルジア、2009 年の韓国と米国、2010 年に表面化したイラン、2012 年のサウジアラビアにおいて、社会インフラストラクチャ／企業ネットワークを狙った大規模なサイバー攻撃が発生しており、背後には国と国の安全保障上の対立が見え隠れしている。また、そのような攻撃だけでなく、サイバースペースは今や、国や企業の秘匿されている情報を窃取しようという、サイバー・スパイ、サイバー諜報活動が激しく行われる場ともなっている。

幸いわが国では社会インフラを停止させるような大規模なサイバー攻撃は発生していないが、サイバー戦争のもう一つの側面であるサイバー諜報戦は、2011 年に明らかになった。防衛関連産業への攻撃、衆参両院への攻撃、政府機関への攻撃等がすでに大規模に発生している。また、諸外国においては、企業同士の競争の中で、サイバースペースを使ったスパイ合戦や相手のサービス／商品を貶めるようなネガティブキャンペーンも行われており、もはや、すべての企業が経営資源を割いてサイバーセキュリティに対応しなければならない時代に入っている。

米国大統領情報問題担当補佐官であったリチャード･A･クラーク（Richard A. Clarke）は、著書の中で、「サイバー戦争は現実であり」、「すでにはじまっている」と指摘し、サイバー戦争は「世界の軍事バランスや政治経済の関係を根底から覆す恐れ」があると述べている[6]。実際、サイバー戦争を見据えた各国の取り組みはすでにはじまっており、中国では、『超限戦』の中で現在のサイバー戦を見越した戦術が描かれており[7]、2002 年頃から人民解放軍は各軍管区傘下部隊に、情報戦民兵組織を設置し、民間の IT 企業、大学、人民解放軍のコンピュータ・ネットワーク作戦部隊の人間とも連携しているようである[8]。

---

6 Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do about It*, New York: ECCO, 2010. リチャード・クラーク、ロバート・ネイク（北川知子、峯村利哉訳）『世界サイバー戦争―核を超える脅威　見えない軍拡が始まった―』（徳間書店、2011 年）。

7 喬良、王湘穂（坂井臣之助監修、劉琦訳）『超限戦―21 世紀の「新しい戦争」』（共同通信社、2001 年）。

8 US-China Economic and Security Review Commission, “Capability of the People’s Republic of China to Conduct Cyber Warfare and Computer Network Exploitation,” <http://www.dodea.edu/Offices/Safety/upload/14_china_spy.pdf> p. 32.

北朝鮮でも、小学生の時から選抜・養成されたサイバー戦闘員からなるサイバー部隊が数千名いるとされている。

米国では、サイバー戦争の危機感の高まりを受け、「サイバー軍」が設置され、陸海空海兵の四軍に「陸軍サイバー軍」「第 24 空軍」「第 10 艦隊」「海兵隊サイバー軍」が編成されている。米軍はすでにサイバーを、陸海空宇宙にならぶ第 5 の作戦空間と位置づけている。すでに国際安全保障の戦場の一つとして、サイバースペースでの衝突が起こっている現実が浮かび上がってくる。その被害者は国家に限定されてはいない。多くの民間企業もまた攻撃に巻き込まれて被害に遭っている。

2.2 DDoS攻撃

「サイバー攻撃」と一般的にいわれるが、その手法は多様である。2000 年前後までのサイバー攻撃は、コンピュータ・ウイルスのように最初から不特定多数への感染を意図し、データの消去／PC のシステムの破壊／特定のメッセージの表示などを行う、愉快犯的な色彩が濃いものであった。代表的な例としては、1980 年代の Brain ウイルスや YankeeD、1990 年代の WMConcept や Happy99、2000 年代の W/Nimda、Toj/Banker、Gumbler などがある。こうした「ハッカー」行為[9]は、近年のサイバー攻撃には必ずしも含められない。

近年のサイバー攻撃には大きく分けて三つを挙げることができる。第一に、「分散型サービス拒否（Distributed Denial of Service：DDoS）」攻撃と呼ばれるものである。DDoS 攻撃の初期の例として有名なのが、2007 年のエストニアに対する攻撃である。エストニアには旧ソ連の影響が色濃く残っている。その象徴的な存在だったのが、首都タリン中心の広場に置かれていたブロンズ像であった（16 ページ図表 1）。エストニア政府がこのブロンズ像を郊外の戦没者墓地に移そうとしたところ、エストニアに対する DDoS 攻撃が始まった。

DDoS 攻撃とは、例えて言えば、自宅やオフィスの玄関に数千人、数万人が一斉に押しかけて呼び鈴をしつこく押すような状況に似ている。DDoS 攻撃の首謀者は、コンピュータ・ウイルスを不特定の人々のコンピュータに感染させ、感染したコンピュータが特定の日時になると標的となるコンピュータのサーバーなどに一斉にアクセスする。ウイルスに感染したコンピュータは世界中に広がっており、個々のアクセスは通常のア

9 「ハッカー」はもともと技術に精通した人々を指す言葉であり、不法行為を行う人々という意味ではない。ハッカーたちの技術が、門外漢にはある種の魔法のように見えるため、一種の魔女狩りのように「ハッカー」は悪者の代名詞となった。

クセスと見かけ上は変わらないため、ウイルスによる攻撃だけを止めることはできない。その結果、処理能力を超えたコンピュータは機能を停止せざるを得ない。ミリ秒を争う金融の世界では、ほんの少しの遅延も大きなダメージとなる。

エストニアを攻撃したのは、状況証拠からロシアだと考えられていたが、後にロシアの愛国者グループが関与を認めた。しかし、ロシア政府がそれに関与したのかどうかははっきりしていない。ネットワークの世界では、自分の痕跡を消すことができるため、攻撃者が誰なのかが分からないことが多い。これを一般的に「アトリビューション（帰属、属性）問題」と呼んでいる。

エストニアに対する攻撃と同様の DDoS 攻撃は、2008 年にリトアニア、2009 年には米韓に対しても同時に行われた。2010 年には日中間の尖閣諸島問題に関連して、日本に対する攻撃も行われた。

図表 1　エストニアのブロンズ像

注：2011 年 11 月撮影。

2.3　標的型電子メール攻撃

第二のタイプの攻撃が、「標的型電子メール攻撃」である。これはいわゆる「偽メール」や「乗っ取りメール」であり、電子メールを偽造して送りつけたり、本物の電子メール・アカウントを乗っ取ってしまったりする行為である。従来は、アカウントを乗っ取ること自体が目的の場合が多かったが、近年では密かにメールにアクセスし続け、標的の人

物に対するスパイ行為として使われることが多い。

2011 年 3 月 11 日に東北地方太平洋沖地震が発生し、大きな被害をもたらした。その直後から福島第一原発の放射線問題が深刻になった。地震から 20 日後の 3 月末になると、放射線に関する情報伝達を示唆する内容の電子メールが政府職員に送られ、添付されたファイルを開くと、コンピュータ・ウイルスに感染するという事例が見られた。

標的型攻撃では、攻撃者は「ソーシャル・エンジニアリング」を利用する。ネットワークへの不正侵入を達成するために、社会的な関係（仕事上の関係や会社内の上下関係など）を巧みに利用して、人間の心理的なミスにつけ込み、マルウェアを送り込んで PC やネットワークへのアクセス権などを不正に得る。被害者は、上司／知人または仕事に関係のある組織からのメールを受け取り、本物のメールと信じて添付されたファイルを開くが、開いた瞬間にシステムやプログラムの持つ未知の脆弱性を利用され（ゼロデイ攻撃)、バックドアを設置され、気づかないうちに遠隔監視のプログラムをパソコンにインストールされてしまう。このプログラムを通して、電子メールや機密ファイルへのアクセス、さらにパソコンの周辺環境への録音や撮影が可能となる。多くの場合、被害者は自分が被害に遭っていることにすら気付かない。

図表 2（18 ページ）は、偽メールの例である。内閣官房職員を装い、政府内部資料を転送してきたように見せかけている。おそらく、実際の電子メールを何らかの方法で入手し、その内容文を用い、ウイルス等のマルウェア（悪意のあるソフトウェア）を仕込んだファイルを添付したものである。しかし、このメールは差出人と返信先が無料メールになっており、転送に伴うメッセージが書き込まれていないなど、一見して偽メールと分かる低レベルのものである。本格的な作戦として標的型電子メール攻撃が行われる場合には、さらに高度な偽装を施すことになるだろう。

2011 年 9 月には、三菱重工業に対する標的型攻撃が報道された。この攻撃の結果、本社を含む 11 の事業所で 83 台のサーバーや PC が感染したことが明らかになり、防衛省の受注データ、戦闘機開発に関する過去の経緯、原子力発電所の設計に関する情報、パスワードなどの情報が漏洩した可能性があると報道されている。この攻撃は、該当企業だけでなく、他の複数の大手重工、電機関連企業にも行われたことが明らかになっている。

図表２　偽メールの例

2011 年に明らかになったサイバー攻撃は、氷山の一角であり、後に述べる米国の事例に見られるように、広範な企業がいまや、重要情報の窃取を狙う標的型攻撃の対象となっていることを認識する必要がある。

海外でも深刻な事例が報告されている。代表的なのが「スタックスネット（Stuxnet）」である。イランは、エスファハーン州ナタンズに核関連施設を持ち、イラン政府は平和利用だと主張しているものの、核兵器の開発が疑われている。イランのマフムード・アフマディーネジャード大統領は、当該施設をメディアに公開するなど、挑発的な言動を繰り返していた。

しかし、2010 年 6 月頃、核施設内の遠心分離機が異常な動作をするようになった。計器は正常を示しているのに、実際には異常な回転を見せるようになった。不審に思った技術者がコンピュータを自宅に持ち帰り、インターネットに接続したため、異常の原因となっていたコンピュータ・ウイルスがインターネットに流出し、世界各国に広がるようになった[10]。

「スタックスネット」と名付けられたウイルスを誰が作成し、どうやってイランの核施設に送り込んだのかが議論されたが、2 年後の 2012 年 6 月になって米ニューヨーク・

10　David Sanger, “Obama Order Sped Up Wave of Cyberattacks against Iran,” *New York Times*, June 1, 2012.

タイムズ紙が米国とイスラエルの共同作戦によるものと報道した[11]。イランに対するサイバー攻撃はジョージ・W・ブッシュ政権の頃から検討され、オバマ政権に引き継がれた。核開発を半ば公然と進めるイランは新たな懸念であったが、アフガニスタンとイラクの問題を抱えた米国にとってイランとも軍事的な衝突を始める余裕はない。そこで採用されたのが、核開発の遅延を狙ったサイバー攻撃であった。

2.4 わが国における標的型攻撃の現状

わが国では、2005 年頃から主に政府機関を中心に標的型攻撃が確認されている。情報処理推進機構の「標的型メール分析に関するレポート」（2011 年、20 ページ図表 3 参照）によれば、2005 年に実在の外務省員を詐称して、マルウェアを埋め込んだ MS Word ファイルが添付された標的型攻撃メールが複数の官公庁に届いたのが、標的型攻撃の皮切りであったと考えられる。翌年には、官公庁や新聞社の公務員や記者を詐称して、民間大手企業に対しても標的型攻撃が行われている。2007 年には、日本語環境でのみ使われる一太郎や圧縮解凍ソフトの脆弱性を利用した標的型攻撃が行われ、2008 年には比較的改ざんに対して強いと考えられていたアドビ社の PDF を添付ファイルに用い、Adobe Acrobat Reader の脆弱性を利用した標的型攻撃が行われている。

このような標的型攻撃は、年々進化して手口が巧妙になってきており、官庁のみならず民間企業でも社内ネットワークの感染が進んでいるものと思われる。今回、経団連 21 世紀研究所のサイバー攻撃研究グループが情報セキュリティ企業にヒアリングしたところ、個々の企業の名前は守秘義務の関係で明かしてもらえなかったが、「実際に調査に入ると多くの企業で標的型攻撃と見られる感染や感染の痕跡が発見できる」との話があり、また、個々の企業や情報部門の担当者が、自社の感染を対外公表することについて非常に後ろ向きである、ということを知ることができた。

経済産業省「サイバーセキュリティと経済研究会報告書」（2011 年）によれば、経済産業省が企業に対して調査したところ、2007 年に「標的型と思われるサイバー攻撃を受けた経験がある」と答えた企業が 5.4%であったのに対して、2011 年には 33%の企業が「受けた経験がある」と回答しており、相当多数の企業が標的型攻撃の対象となっていることが明らかになっている。

11 Ibid.

図表 3　国内における標的型サイバー攻撃の事例

年　月	事　例
2005 年 1 月	実在の外務省職員を詐称してウイルスを埋め込んだ MS Word ファイルが添付された標的型攻撃メールが複数の官公庁に届いた。
2006 年 5 月	官公庁を詐称してウイルスを埋め込んだ MS Word ファイルが添付された標的型攻撃メールが民間大手企業に届いた。
2006 年 5 月	新聞社を詐称してウイルスを埋め込んだ MS Word ファイルが添付された標的型攻撃メールが民間大手企業に届いた。
2006 年 8 月	ウイルスを埋め込んだ一太郎ファイルが添付された標的型攻撃メールが届いた。
2006 年 10 月	実行形式のウイルスが添付された標的型攻撃メールが届いた。
2007 年 4 月	一太郎の未修正の脆弱性を悪用したウイルスメールが届いた（ゼロデイ攻撃）。
2007 年 6 月	日本語環境の圧縮解凍ソフトの未修正の脆弱性を悪用したウイルスメールが届いた（ゼロデイ攻撃）。
2007 年 9 月	首相をかたる標的型攻撃メールが届いた。
2007 年 10 月	ウイルスを埋め込んだ PDF ファイルが添付された標的型攻撃メールが届いた。
2008 年 4 月	政府関係機関（IPA）を詐称してウイルスを埋め込んだ PDF ファイルが添付された標的型攻撃メールが官公庁に届いた。
2008 年 11 月	標的型攻撃メールに関する組織内の注意喚起メールを加工して、多数の従業員に標的型攻撃メールが届いた。
2009 年 5 月	新型インフルエンザ関連情報に見せかけた標的型攻撃メールが届いた。
2009 年 7 月	添付ファイルがついていない（html 埋め込み型）標的型攻撃メールが届いた。
2011 年 3 月	RSA の SecureID の情報摂取が標的型攻撃メールによって行われた
2011 年 3 月	東日本大震災や福島原発事故関連情報に見せかけた標的型攻撃メールが多数届いた。
2011 年 7 月	おれおれ詐欺を模倣した標的型攻撃メールによって情報流出が発生した。
2011 年 9 月	ネットバンキングの ID とパスワード情報を盗むウイルスが付いたフィッシングメールが届いた。
2011 年 9 月	防衛関連企業の複数箇所の拠点で、数十大のパソコンやサーバーにウイルスが感染していた。標的型攻撃メールの可能性がある。
2011 年 9 月	Mac OSX を標的としてウイルスが埋め込まれた PDF ファイルのウイルスが確認された。

出典：情報処理推進機構「標的型攻撃メールの分析に関するレポート」（2011 年）を一部改変

このように、多くの企業に対して標的型攻撃が行われ、かなりの企業で感染と情報漏洩が実際に生じていることが疑われるが、各企業の経営者がセキュリティ対策に危機感を持って対処しているとは言いがたいのが現状である。AIU 保険が 2012 年 12 月に実施した調査によれば、調査対象該当企業の約 8 割が「サイバー攻撃は受けたことが無い、

または無いと思う」と答え、情報漏洩に関するリスクを「非常に脅威」と感じている経営者の割合は 3 割、外部からのサイバー攻撃を「非常に脅威」と感じる経営者の割合は 2 割に満たなかった[12]。また、情報漏洩にある程度のリスク対策をとっていると答えた経営者が 7 割もいる一方、自社のリスク対策に自信が無いと答えた経営者が 9 割にも上る。なお、同調査においてサイバー攻撃の被害想定を聞いたところ、被害想定額の平均は 1 億 2000 万円であった。

わが国でサイバー攻撃に対するリスクへの認知が低い原因として、サイバー攻撃の実態がなかなか報道されないという点が挙げられる。これは、被害にあった企業も政府の側も、評判の低下を恐れて実態を外に出したがらないという実情を示している。

近年、金融機関や交通機関などでさまざまなシステム障害が起きていると報じられている。そのほとんどはシステム上の事故として処理されているが、実際には他者によるサイバー攻撃の被害である可能性もある。被害の実態を覆い隠すために事故として発表されていたり、原因が分からないままであったりする場合もある。

冷戦時代、ソ連が日本の防空体制やレーダーの性能を見極めるために、しばしば日本領空近くに爆撃機を飛ばし、航空自衛隊の戦闘機にスクランブルをかけさせるという現象が見られた。これは「東京急行」と呼ばれた。それはレーダーの周波数を探る等、日本の防空上の弱点を探るためだったと考えられている。現在見られるさまざまな「システム障害」もいわば「サイバー東京急行」であり、政府や企業のシステム上の脆弱性を探る動きだと考えることもできる。

政府へのサイバー攻撃が報道されたのは、2011 年 1 月 21 日の NHK テレビの報道「経済産業省にサイバー攻撃」が皮切りであった。同年 9 月には、読売新聞が防衛産業へのサイバー攻撃を報じた[13]。2011 年は、わが国政府機関へのサイバー攻撃が相次いで明らかになった年であり、10 月には、衆議院のコンピュータ・ネットワークへの攻撃が報道され、サーバー等数十台が攻撃によって感染させられたことが判明した。このような政府機関を狙った標的型攻撃は、すでに 2007 年頃より行われていたと見られるが、2011 年になってようやく被害の様子が報道され、広く世間に知られるようになった。

12　AIU 保険会社『経営者の情報漏洩リスクに対する意識調査』(2013 年 1 月) 調査は 2012 年 12 月に実施され、調査対象は従業員 100 人以上、資本金 5000 万円以上の企業の役員以上の経営者 200 名のサンプルアンケート調査。56 社が従業員 1000 人以上の企業で、上場企業が 1/4。

13　「三菱重サーバーに侵入　防衛・原発関連も　80 台ウイルス感染」『読売新聞』2011 年 9 月 19 日。

2.5　情報の窃取から制御システムを狙った攻撃へ

標的型攻撃は、官庁や企業のコンピュータ・ネットワーク内部に潜入し、機密文書などの情報を窃取することを目的としたものであった。しかし、それ以上に深刻な事態も進展しつつある。

2013 年 3 月の韓国のサイバー攻撃に見られるように、2000 年以降、通信、報道、金融、ガス、電気、水道といった社会の重要インフラの制御を麻痺させることを目的とした攻撃の前兆が見られるようになっている。

電力、ガス等の重要インフラが依存する産業用の制御システムは PLC（プログラマブル・ロジック・コントローラ）やアクチュエーター、バルブ制御装置などのフィールド制御機器、および状況の監視・計測に用いられるサーバーやクライアント PC など一群の情報機器から成り立っている。

制御システムは、常時ネットワークに接続されていないかファイアウォールを介してネットワークにつなげる等のセキュリティ措置が取られているため、サイバー攻撃の影響を受けづらいと言われてきた。また、事業者ごとにカスタマイズされた固有のシステムが使われているため、システム内部を熟知しなければ攻撃は難しく、一般的なコンピュータ・ウイルスの影響も受けないと考えられてきた。

しかし、実際のところ、そのような制御システムも PC などと同じ OS を利用しているケースが多く、外部からの情報入力も定期的に行われているため、サイバー攻撃を受ける危険性が高いことが最近明らかになってきている。

経済産業省の報告書によれば、日本プラント設備での端末の OS では約 9 割に Windows 系が使われており、そのうち 37%が外部ネットワークとの接続が行われている。また、接続が行われていないシステムにおいても、約 7 割で USB など外部メディアの接続口が設置されている[14]。

諸外国においては、図表 4 に挙げたように、制御システムに侵入されて被害が出た事例が 2000 年以降散見される。2003 年には北米東海岸（カナダを含む）で大規模な停電が発生している。停電の直接の原因は、オハイオ州の送電線が倒木によって接触し、電圧の異常が起きたためであるが、送電網への悪影響を防ぐシステム「監視制御データ収集システム（SCADA）」がマルウェア感染によって処理遅延を起こし、停電が連鎖していったと言われている[15]。そのような遅延を起こさせたのが、Slammer というマルウェ

14　経済産業省「工業用装置等における汎用 IT 技術応用に起因する脅威と対策に関する実態調査事業　報告書」（2009 年 3 月）。

15　Clarke and Knake, op.cit.

アであった。当時 SCADA システムは、米国の電力網の発電、変電、送電のあらゆる部分に使われており、そのほとんどが情報のやりとりにネットワークを利用していた。多くの機器はイントラネットで信号を送受信していたが、送受信先の機器の中にはインターネットに接続しているものが 2 割あったとされている。このような外部への接続を介して、マルウェアが電力制御システムに侵入したと分析されている。

図表 4　制御システムにおけるセキュリティ事故の事例

時　期	業　種	事故内容	原　因	影　響
2001 年	水道	オーストラリアのマローキー市の下水監視制御システムに不正侵入	アカウント管理不備による不正侵入	浄水装置に異常が発生
2003 年	電力	米国東海岸のファーストエネルギー社の電力管理システムでアラーム処理のアプリケーションに不具合が発生	不具合の背後にサイバー攻撃者の存在が疑われる。	東海岸、五大湖、カナダの広範な範囲で大停電が発生
2003 年	電力	米国の原子力発電所で、マイクロソフト SQL サーバーを狙ったウイルスが VPN 接続から侵入	Slammer ワームに発電所のコンサルタント会社の端末が感染	制御システムが 5 時間にわたって停止、他の電力施設との通信も遮断
2003 年	鉄道	米国東部の鉄道会社の信号管理システムがウイルスに感染	W32/Blaster ワーム	信号・配車システムが断絶。3 路線で半日にわたり通勤・貨物列車が運行停止
2005 年	自動車	米国の複数の自動車工場でウイルスが制御システムに感染し、プラント中に広がり、操業停止	Zotob ワーム	部品供給の停止など 1400 万ドルの損害
2007 年	電力	米国カリフォルニア州の電力データ管理センターへの不正侵入	アカウント管理不備による不正侵入	被害なし
2008 年	鉄道	英国で 14 歳の少年が鉄道の切り替え機をテレビのリモコンで操作	無線端末への不正侵入	列車が接触事故
2010 年	エネルギー	パイプライン、ウラン濃縮等の施設で使用されている制御システムにウイルスが侵入	Stuxnet	イランでは遠心分離機が停止。マレーシア、インドネシア、中国等でも感染拡大

出典：各種資料より作成。

2.6　通常兵器と組み合わせたサイバー攻撃

第三のタイプのサイバー攻撃は、通常兵器による攻撃と組み合わせたものである。この先駆的な例としては、シリアに対するイスラエルの空爆事件が挙げられる。2007 年、シリアの北東部に、北朝鮮の協力によるものと思われる核施設の開発が進められていた。ところが、この施設はイスラエルの戦闘機によって空爆されてしまった。しかし、シリアは全くこれに対抗することができなかった。事前にイスラエルがシリアのレーダー網を操作し、イスラエル機がレーダーに映らないようにしていたといわれている[16]。

2012 年 8 月、米海兵隊のリチャード・P・ミルズ（Richard P. Mills）中将は、米国内で開かれた公開カンファレンスで、米軍がアフガニスタンにおいて敵側のネットワークに侵入していたと発言した。それによって、自軍を利する情報を入手し、戦局を有利に進めることができたという[17]。また、アフガニスタンのタリバンのウェブサイトは何度も書き換えられ、米軍側を支持するメッセージを載せられている[18]。

通常兵器を使った現実の戦闘と組み合わせてサイバー攻撃が用いられることで、その威力はより一層大きくなる。今後は、重要インフラストラクチャを対象とした物理的な攻撃とサイバー攻撃の組み合わせを懸念しなくてはならない。敵軍の指揮通信システムをサイバー攻撃によって不能にした上で通常兵器による攻撃を行えば、容易に勝利を得ることができるだろう。

その意味で、将来的に懸念されるのが人工衛星の乗っ取りやその通信の妨害である。すでに韓国においては北朝鮮によって米国が運用する全地球測位システム（Global Positioning System：GPS）のジャミング（電波妨害）が何度も行われている。それによって空中、地上、水上にある軍用および民間の航空機、車両、船舶の位置把握が妨害される恐れが出ている。これまでのジャミングで事故は起きず、被害はなかったが、潜在的な脅威を認識させることになった。2012 年春のジャミングではソウルの仁川空港と金浦空港を使う 553 機が GPS に不具合を報告し、海上にあった船舶の多くも同様であった[19]。

16　Ibid.

17　Raphael Satter, “Afghanistan Cyber Attack: Lt. Gen. Richard P. Mills Claims to Have Hacked The Enemy,” Huffington Post <http://www.huffingtonpost.com/2012/08/24/afghanistan-cyber-attack-richard-mills_n_1828083.html> August 24, 2012.

18　Rob Taylor, “Taliban Website Hacked as Afghan Cyber War Heats up,” Reuters <http://www.reuters.com/article/2012/04/27/net-us-afghanistan-taliban-hacking-idUSBRE83Q09I20120427> April 27, 2012.

19　Sean Gallagher, “North Korea Pumps up the GPS Jamming in Week-long Attack,” Ars Technica

国際通信の多くはすでに海底ケーブルへ移行しつつあるが、それでも米国の軍用・政府用通信の多くはいまだに人工衛星を通じて行われているという。例えば、軍事作戦を展開しているアフガニスタンと米国との間の通信の 80%は人工衛星によるといわれている[20]。

実際、2007 年から 2008 年に深刻な事態が起きていたことが、2011 年 10 月に明るみになった。米国の航空宇宙局（National Aeronautics and Space Administration：NASA）の地球観測衛星「テラ」と地球資源調査衛星「ランドサット 7 号」が中国からと見られるサイバー攻撃を受け、テラは 2008 年 6 月と 10 月、ランドサットは 2007 年 10 月と 2008 年 7 月に、それぞれ数分から十数分間、制御を失った。攻撃はノルウェーの地上局を介して行われたと見られている。衛星の制御を乗っ取られたり、データが流出したりする被害には至らなかったものの、大事故につながりかねない攻撃であった[21]。

サイバー攻撃にもかかわらず、NASA の対応は不十分であった。2012 年 2 月 29 日に議会下院科学宇宙技術委員会で証言した NASA のポール・マーチン（Paul Martin）監察官は、2011 年度だけでも高度なサイバー攻撃を 47 回受け、そのうち 13 回で侵入を許したという。また、カリフォルニア州のジェット推進研究所（Jet Propulsion Laboratory：JPL）の主要システムが中国を発信源とするサイバー攻撃で乗っ取られ、攻撃側が完全にコントロールできる状態に陥った。さらに 2011 年 3 月には国際宇宙ステーション（International Space Station：ISS）に命令を送信するプログラムが入ったパソコンを盗まれるなど、2009 年～11 年にかけて 48 台のノートパソコンが紛失または盗難に遭ったという[22]。

人工衛星の制御システムにはそれほどバリエーションがないと言われている。地上の通信システムであれば電源そのものを落とし、ネットワークから隔離することができるが、人工衛星の場合はそうした電源スイッチはなく、すべての操作をリモート・コントロールで通信によって行わなくてはならない。誰かが操作できるということはそれが乗っ取られる可能性もあると考えなくてはならない。放送衛星、通信衛星、偵察衛星な

<http://arstechnica.com/information-technology/2012/05/north-korea-pumps-up-the-gps-jamming-in-week-long-attack/> May 10 2012.

20 Supriya Srinivas, “Governments/military Drive Growth for MSS Industry,” SatellitePro <http://www.satelliteprome.com/opinion/governmentsmilitary-drive-growth-for-mss-industry/> March 18, 2012.

21 「米衛星にサイバー攻撃　米議会報告書案　中国軍関与の可能性」『読売新聞』2011 年 10 月 29 日。「サイバー攻撃　中国の影」『読売新聞』2011 年 11 月 29 日。

22 「NASA 標的　サイバー攻撃」『読売新聞』2012 年 3 月 3 日。

どさまざまな用途の人工衛星が打ち上げられているが、そうした人工衛星のコントロールを失う可能性を想定した作戦を考えておく必要がある。空中、地上、水上、そして水中にある多様なビークルは、バックアップの通信システムを確保しておくとともに、それらを完全に失った場合にどう対処するかを想定しておかなければならない。

次章では、実際に起きた企業へのサイバー攻撃の事例を見ておこう。

第 3 章　企業に対するサイバー攻撃の事例

3.1　サウジ・アラムコ

2012 年 8 月 15 日、サウジアラビア国営石油会社のサウジ・アラムコ（Saudi Aramco）は、社内の情報ネットワークの一部コンピュータがウイルスに感染し、社内ネットワークを外部のネットワークから切り離したと発表した[23]。また同日「正義を貫く刀（Cutting Sword of Justice）」と名乗る集団が、「サウジ・アラムコの 3 万台のコンピュータを破壊した」との犯行声明[24]を出した。原油生産には影響が生じなかったものの、10 日後、サウジ・アラムコは、①社内のコンピュータ 3 万台が感染したこと、②感染の拡大を防ぐため、社内ネットワークをすべて切り離した上でマルウェアの除染したこと、③ウェブサイトが復旧していないこと、④犯行の背景は不明であることを発表した[25]。その後、カタール第 2 位の国営石油会社ラスガス（RasGas）でも同じマルウェアの感染が広がり、業務システムがダウンしたことが発表された[26]。

サウジ・アラムコを攻撃したマルウェアは、W32.Disttrack（Shamoon）と名付けられた。このマルウェアは、侵入先のコンピュータ上のファイルを破壊し、マスターブートレコードを書き換えるプログラムであった。その後の分析によって、マルウェアの中に同年 4 月にイラン石油省を攻撃した Flame というマルウェアのコンポーネントの一部が使われていること、破壊に成功すると攻撃者に完了報告を行うことが明らかになっている。

犯行声明を出した「正義を貫く刀」がいかなる集団かは判明していないが、犯行声明中の①サウジ・アラムコの 3 万台のコンピュータを、②15 日午前 11:08 に破壊した、という表現は、その後マルウェアの解析で明らかになった事実と一致しており、犯行を行ったグループに間違いないとされている。

米国は、一連の攻撃の背後にイランがいるのではないかとの疑念を表明している。レオン・パネッタ（Leon Panetta）国防長官（当時）は「Shamoon は民間部門を標的としたこれまでで最も破壊的なサイバー攻撃」であったと述べている[27]。また、ワシントン

23　2012 年 8 月 15 日リヤド発ロイター電。

24　PASTEBIN <http://pastebin.com/HqAgaQRj> August 15, 2012.

25　2012 年 8 月 26 日ドバイ発ロイター電。

26　Patrick Osgood, “Cyber Attack Takes Qatar's RasGas Offline,” Arabian Business <http://www.arabianbusiness.com/cyber-attack-takes-qatar-s-rasgas-offline-471345.html#.UXjTLStzd2A> August 30, 2012.

27　Leon E. Panetta, “Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City, October 11, 2012,” Department of Defense <http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136> October 11, 2012.

DC のシンクタンクである戦略国際問題研究所（Center for Strategic and International Studies：CSIS）のジェームズ・A・ルイス（James A. Lewis）上級研究員も、イランの犯行の可能性が高いと述べている[28]。その他、多くの専門家が、Shamoon 攻撃が 2010 年のイランの核関連施設に対するスタックスネット攻撃に対する反撃であるとの見方を披露している。

3.2 コカ・コーラ

米コカ・コーラは、2008 年 9 月、中国飲料メーカーの中国匯源果汁集団に買収を提案した。買収総額は 24 億ドルで、中国匯源果汁集団が香港市場に上場している発行済株式を 12.2 香港ドルで仏ダノン等の株主から買い付けるというものであった。しかし、中国の商務部は、この中国最大となる買収提案に対して、2009 年 3 月 18 日に、前年施行された独占禁止法をたてに、「競争力が損なわれる」として承認しなかった。

この判断の背後には、中国政府がサイバー攻撃で得た情報が使われたと報道されている[29]。米連邦捜査局（FBI）は 2009 年 3 月にコカ・コーラに対して警告を発したが、コカ・コーラの経営陣がサイバー攻撃による情報漏洩について発表することはついになかった。

一連のサイバー攻撃は、コカ・コーラ太平洋グループのポール・エッチェルス（Paul Etchells）副社長への 2009 年 2 月 16 日の標的型メール攻撃から始まったとされる。エッチェルス副社長は当時、匯源果汁集団買収の総責任者であった。メールの差出人はコカ・コーラの法務担当重役を詐称したもので、「エネルギー消費を減らして経費を節約しよう（CEO より）」というタイトルであった。当時、コカ・コーラでは、エネルギー消費軽減を経営課題としており、何の疑いも抱かなかったエッチェルス副社長はメールのリンクをクリックした。リンクは、マルウェアをダウンロードするサイトにつながっており、これにより、同副社長のコンピュータが乗っ取られ、最終的にはコカ・コーラ内部のネットワークへの侵入を許すことになった[30]。

一度コカ・コーラのネットワークに侵入したハッカーは、以後 1 ヶ月間に渡って、FBI

---

28 2012 年 10 月 22 日パリ発 AFP 電。

29 Ben Elgin, “Coke Gets Hacked And Doesn’t Tell Anyone,” Bloomberg <http://www.bloomberg.com/news/2012-11-04/coke-hacked-and-doesn-t-tell.html> November 5, 2012.

30 Jordan Robertson, “How a Coca-Cola Exec Fell for a Hacker’s E-mail Trick,” Bloomberg <http://go.bloomberg.com/tech-blog/2012-11-06-how-a-coca-cola-exec-fell-for-a-hackers-e-mail-trick/> November 6, 2012.

が警告するまで活動を続け、企業内の機密書類のほか、企業経営陣の送受信するメールを盗み見ていたと見られている。

実際に中国政府による匯源果汁集団の買収の可否の判断に、コカ・コーラから漏れた内部情報がどの程度影響したかは明らかではないが、結局大株主であった仏ダノンは2010年7月に、中国政府系の香港投資ファンドSAIFパートナーズにコカ・コーラが提示した額の半値の6ドル（総額2億ユーロ）で匯源果汁集団の22.98%を売却している。

米国では、政府と企業が総額60億ドル（約5400億円）を情報セキュリティに毎年費やしているとされている。また、情報セキュリティ市場全体の規模は2013年で258億ドル（2.11兆円）と予測されている[31]。コカ・コーラも米国企業の中では、セキュリティ投資を行ってきた会社である。しっかりと情報セキュリティ投資を行っても、最新の標的型攻撃が防げないというのが、直近のサイバー攻撃の現状をわれわれは理解すべきであろう。

3.3 米AP通信

2013年4月23日午後1時過ぎ（米国東部時間）、AP通信のツイッター・アカウントが、「速報：ホワイトハウスで 2 回爆発、バラック・オバマが負傷」というツイートを流した（30ページ図表5）。当然、多くの人の頭の中に、1週間前の4月15日に起きたボストンでの爆弾テロが浮かんだことだろう。株式市場もすぐに反応し、ダウ・ジョーンズ株価指数は午後1時過ぎに128ポイント下落した（30ページ図表6）。しかし、すぐに AP 通信も気づき、数分以内にこれがまちがったツイートであると別のツイッター・アカウントで指摘した。そして、アカウントが乗っ取られたこと、ホワイトハウスで爆発はなく大統領が無事であることも発表したので、株価はすぐ元に戻った。その数分後のホワイトハウスでのジェイ・カーニー（Jay Carney）報道官の記者会見の際、最前列に座っていたAP通信のジュリー・ペース（Julie Pace）記者は、AP通信のアカウントが乗っ取られ、まちがったツイートが行われたと説明した。報道官は「大統領は無事だ。さっきまで一緒に話していた」とこれに応じた[32]。

---

31 Gartner, Forecast: Security Software Markets, Worldwide, 2008-2015, 2Q11 UpdateForecast

32 Grace Wyler, “AP Twitter Hacked, Claims Barack Obama Injured In White House Explosions,” Business Insider <http://www.businessinsider.com/ap-hacked-obama-injured-white-house-explosions-2013-4> April 23, 2013.

図表 5　乗っ取られた AP 通信のツイート

出典：http://www.businessinsider.com/ap-hacked-obama-injured-white-house-explosions-2013-4

図表 6　AP 通信の偽ツイートに反応した株式市場

出典：Google Finance

AP 通信のツイッター・アカウントを乗っ取ったのは「シリア電子軍（Syrian Electronic Army)」と名乗るグループだった。このグループの実態は分かっていない。シリア電子軍は、その前の 1 週間に CBS ニュース、NPR（National Public Radio）のアカウントも乗っ取っている。さらには、国際サッカー連盟（FIFA）のヨーゼフ・

ブラッター（Joseph Sepp Blatter）会長のツイッターのアカウントもシリア電子軍に乗っ取られ、「汚職の責任を取って会長を辞任する」など偽の書き込みをされているとロイター通信が伝えている[33]。シリア電子軍はシリアのアサド政権支持者たちによるものと見られるが、その攻撃や主張に一貫した政治的メッセージは必ずしも見られない。

今回の AP 通信の乗っ取り事件は、短時間ではあるが株式市場に影響を与えている。もし株式市場がこのような反応をすることを想定し、何らかの方法で経済的利益を上げようとした可能性もある。ただし、短時間のうちに大量の売買注文を出して大きな利益を上げれば、米証券取引委員会（SEC）の調査を受けることになりかねない。取引を分散させ、組織的な作戦を練らなくてはならないだろう。

しかし、こうした虚偽の内容のツイートをすること自体を罰する米国の連邦法は存在しないという指摘もある[34]。そうなれば、犯人を特定することができても逮捕できないかもしれない。まして、シリア電子軍の構成員が米国外にいた場合には所在を確かめることも難しいだろう。

注目すべきは、AP 通信の本物のツイッター・アカウントで虚偽の情報が発信されても、すぐにそれを打ち消す情報が数多く発信されたことである。他のニュース・メディアの多くもツイッター・アカウントを持ち、ホワイトハウスの中にもメディアの記者たちがたくさん詰めている。同様の報道がなければ、ツイートの信頼性は急速に失われる。

まして、今回のツイートそのものが、AP 通信が通常使う文体とは違っていたという指摘もある。例えば、「速報」を意味する「Breaking」だが、通常であればすべて大文字の「BREAKING」になるところ、今回は最初の一文字だけが大文字になっている。また、オバマ大統領については通常は「President Obama」と書くところ、「Barack Obama」とだけ書かれているところも不信感を呼び起こした。

いずれにせよ、短時間であっても市場に影響を与えることができたということを示した点で、今回の事件は、今後の事件の先例となるかもしれない。これまでもインターネットでは虚偽の情報がたくさん流されてきたが、信頼される情報源としての通信社や大手

---

33 Reuters, “FIFA President Blatter's Twitter Account Hacked,” Yahoo! News <http://news.yahoo.com/fifa-president-blatters-twitter-account-hacked-184536218--sow.html> April 22, 2013.

34 “9NEWS legal expert: No law addresses AP Twitter hack,” 9News <http://www.9news.com/news/local/article/332440/222/9NEWS-legal-expert-No-law-addresses-AP-Twitter-hack> April 24, 2013.

マスコミのアカウントが乗っ取られることがあれば、その影響力は必然的に大きくなるということを示している。

第 4 章　中国におけるサイバースペースの安全

4.1　中国から米国への最近のサイバー攻撃

中国は、サイバー攻撃を行っている国として常に名指しされる国の一つである。しかし、中国政府は常に「中国は被害者である」と言い続けている。中国の国内の実態は必ずしも明らかになっていない。そこで、本章では、サイバーセキュリティ対策を練る前提として、中国国内の実態を公開情報に基づいて検討したい。

2013 年 1 月 30 日、米ニューヨーク・タイムズ紙は、中国から同社のコンピュータ・ネットワークに 4 ヶ月に渡って攻撃があり、すべての従業員のパスワードが流出したと発表した。2012 年 10 月 25 日に同紙が温家宝首相一族による数千億円の蓄財を報道した直後から、サイバー攻撃は始まった。同日、AT&T からの通報により、異常な通信が発見され、ネットワークから侵入者があることが明らかになった。

攻撃を分析したセキュリティ会社マンディアント（Mandiant）によれば[35]、攻撃の手法は過去に中国人民解放軍が関与していた手法と同様であり、攻撃者は、過去に人民解放軍から米国防衛産業へのサイバー攻撃に使われていた米国内の大学のコンピュータを踏み台として使用していた。また、攻撃者は、北京標準時の午前 8 時に仕事を開始し、深夜まで続いた。さらに侵入した攻撃者は、温家宝記事を書いたデービッド・バルボッサ（David Barboza）上海支局長およびジム・ヤードレー（Jim Yardley）前北京支局長のメール・アカウントに侵入していた。これらの証拠から、マンディアントおよびニューヨーク・タイムズ紙は、中国政府がかかわったサイバー攻撃であったと結論付けている。

このニューヨーク・タイムズ紙の報道以後、報道各社が中国からの攻撃を一斉に発表している。1 月 31 日、ウォールストリート・ジャーナル紙は、同社のシステムに中国のハッカーが侵入と発表。同紙を経営するダウ・ジョーンズは、中国による米国の報道の監視が目的とコメントした。2 月 1 日、ワシントンポスト紙が、過去 3 年間にわたり中国からと見られるサイバー攻撃を受けていたと発表した。

また、IT 企業もネットワークにサイバー攻撃があったことを明らかにしている。2 月 1 日、ツイッターが、同社のサーバーに不正アクセスの痕跡があり、25 万人分のメールアドレス、パスワード流出した恐れがあると発表した。2 月 15 日には Facebook が、同社従業員の PC がウェブサイトを通じてマルウェアに感染と発表した。さらに 2 月 19 日、Apple が、社内のコンピュータがマルウェアに感染と発表した。2 月 22 日にはつい

35　Madiant, “APT1: Exposing One of China’s Cyber Espionage Units” <http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf> March 2, 2013.

にマイクロソフトまでもが、不正侵入被害（Mac 事業部門を中心に複数のコンピュータが感染）を発表した。一連の IT 企業の感染源は、iOS アプリ開発者向けのサイト「iPhone Dev SDK」と見られ、同サイトが改ざんされ、Java 脆弱制を用いた不正スクリプトが挿入されていた。

また、2 月 21 日にワシントンポスト紙は、政府機関、報道機関、研究機関（シンクタンク）などワシントンのほぼすべての組織が中国からハッカー攻撃を受けていると報道している。

これらの一連の報道を受けて、米国政府はサイバー攻撃に対する対策を急速に進める一方、中国に対する警戒感をあらわにしている。2 月 12 日にオバマ大統領は一般教書演説でサイバー攻撃に対する危機感をあらわにして、次のように述べている。「われわれの敵は今まさに、電力供給システム、金融機関、航空管制システムの破壊を狙う能力を求めている」。一般教書演説に先立って、サイバー脅威に関する機密情報を民間企業と政府の間で共有し、重要なインフラを防護するサイバーセキュリティ強化に関する大統領令に署名した[36]。

3 月に入ると、トム・ドニロン（Thomas E. Donilon）国家安全保障担当大統領補佐官がニューヨークのアジア・ソサエティで講演し、「中国からの大規模なサイバー攻撃を通じて、企業情報や知的財産を窃取することが行われている」と指摘し、米中の二国間対話の中で、「中国政府がこうした行動を捜査し、これを阻止するために真剣に取り組むよう」、「サイバースペースにおいて許容される行為規範を確立するための建設的な直接対話をするよう」求めた[37]。また、オバマ大統領自身も 14 日に習近平国家主席との電話会談で、「対策強化」を求めた[38]。

米中の間では、長年にわたってサイバースペースにおいて、つばぜり合いが行われてきた。中国から米国に対する最初のサイバー攻撃は、今から 14 年前までさかのぼることができる。コソボ紛争中の 1999 年に、米軍はセルビア共和国の首都ベオグラードに

---

36 The White House, “Executive Order -- Improving Critical Infrastructure Cybersecurity,” <http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity> February 12, 2002.

37 トム・ドニロン「『2013 年の米国とアジア太平洋』―トム・ドニロン大統領補佐官（国家安全保障担当）によるアジア・ソサエティーでの講演（草稿）」米国大使館 <http://japanese.japan.usembassy.gov/j/p/tpj-20130326a.html>2013 年 3 月 11 日。

38 「オバマ大統領、サイバー攻撃停止促す　米中首脳が電話協議」『産経新聞』 <http://sankei.jp.msn.com/world/news/130315/amr13031509000002-n1.htm>2013 年 3 月 15 日。

ある中国大使館を「正確に誤爆」した[39]。これに対して、中国からホワイトハウスのウェブサイトに対してサイバー攻撃が仕掛けられた。その後の 2001 年には、米国の偵察機に中国の戦闘機が接触して墜落する事件が起きた。このときにも米中間でハッカーによる相互攻撃が生じている。2013 年に入り、中国側から民間企業の情報資産を狙った大規模な攻撃が行われていることも明らかになった。

4.2 マンディアント報告書

ニューヨーク・タイムズ紙への攻撃を分析したマンディアントは、2013 年 2 月に中国人民解放軍について分析した報告書を発表した。その中で、人民解放軍総参謀部第 3 部第 2 局（61398 部隊）を、中国におけるサイバー諜報活動を務めてきた最先端の組織の一つである可能性が高いと指摘し、同部隊が入っている建物として上海のビルを名指しした（36 ページ図表 7）。多くのメディアは、同報告書の内容について、中国が国家の意思としてサイバー攻撃を行ってきたことを示すものとして、大きく報じた[40]。

しかし、マンディアントの報告書は、写真を豊富に使うなど、耳目を集めるのに十分だが、その内容はすでに報じられていたものが多い。例えば、61398 部隊にしても、2011 年に米国の「プロジェクト 2049 研究所」が出した「中国人民解放軍の信号情報収集とサイバー偵察の基盤」と題するレポートで指摘されている[41]。それによれば、第三部には 13 万人の要員がいるという。第三部の第四局が日本を担当していると見られており、日本語の専門家が所属しているという。第三部は全体として中国の中で最も外国語に精通した人材のプールになっている。

---

39 米国政府は、誤爆であったとして中国に謝罪している。しかし、中国大使館の建っていた新市街地には、中国大使館以外の建物が周囲には無く、巡航ミサイルが正確に通信設備の置かれていた建物の地価を破壊していることから、当初から意図的な誤爆であったとの分析がたえなかった。

40 “Chinese Army Unit Is Seen as Tied to Hacking Against U.S.” New York Times, February 18, 2013. 「米国を標的に･･･　中国サイバー部隊の実力」『日本経済新聞　電子版』2013 年 3 月 18 日。山崎文明「解放軍ハッカー説と米国防予算　サイバー攻撃に関与―の真実はいかほど？」『日経ビジネス ONLINE』2013 年 2 月 27 日。

41 Mark A. Stokes, Jenny Lin and L.C. Russell Hsiao, “The Chinese People’s Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure,” Project 2049 Institute <http://project2049.net/documents/pla_third_department_sigint_cyber_stokes_lin_hsiao.pdf> November 11, 2011.

図表 7　マンディアント報告書で指摘された上海の建物

出典：Google Map

ちなみに、人民解放軍総参謀部の「第二部」は HUMINT と呼ばれる人間を使ったインテリジェンス活動、つまりスパイ活動を担っている。この第二部の下に第七局といわれる科学技術局がある。ここはコンピュータ・センターを管轄しており、早くからコンピュータを使ったインテリジェンス活動を重視していたようだ。

そうだとすると、なぜこのタイミングでマンディアントの報告書が出て、それが注目されたのかという点が問題になる。それに対する答えとしては、第一に、61398 部隊がプロジェクト 2049 研究所の報告書が出て以降、インテリジェンス・ソースとしての意味を失い、派手に取り上げても実害がなくなった可能性を指摘できる。総参謀部の組織改編も行われた可能性がある。逆にこの情報が報道されることで、米国側の能力を示す一つの材料になったということが考えられるだろう。第二に、2012 年 5 月のワシントンでの国防相会談で「協力しよう」といいつつ、なかなかサイバー攻撃をやめない人民解放軍に対する米国側からの警告の可能性もある。第三に、オバマ政権から米国議会に対するサイバーセキュリティ予算を要求するためのメッセージとも考えることができるだろう。

一方、2013 年 2 月 19 日に開催された中国外交部の定例記者会見において中国外交部報道官は、このマンディアントの報告書をどう評価するかとの質問を受けた。同報道官は、「サイバー攻撃はグローバルな問題であり、相互の信頼と尊重の基礎の上に建設的で国際的な協力の枠組みの下で解決を図るべきである」にもかかわらず、「サイバー攻撃に関する、根拠のない、無責任な批判は、問題の解決にはならない」とマンディアントの

報告書を批判した。

その上で、「中国は、サイバー攻撃の主要な被害国の一つである」という「被害者」としての立場をあらためて確認した。報道官は、近年、中国に対するサイバー攻撃やネット犯罪は急速に増加しているといい、CNCERT（国家互聯網応急中心）の報告を引用して、その被害の実態を説明していた。すなわち、「2012 年には、7.3 万の海外の IP アドレスから、トロイの木馬形ソフトウェアあるいはボットネットを介して中国国内の 1400 万台余りのホストコンピュータが操作され、3.2 万の IP アドレスを通じてバックドア型ウイルスを送り込まれて、中国国内の 3.8 万のネットワークが遠隔操作された」という[42]。そして報道官は、「中国が受けているネット攻撃は、米国のネットワークからの攻撃数が一番多い」とも述べ、マンディアントの報告書が指摘した中国「攻撃者」説に反駁した[43]。

同年 2 月 20 日に中国国防部が開催した記者会見においても、マンディアントの報告書に関する質問があった。これに対して国防部報道官は、中国は法律でインターネット環境の安全を破壊する行為を禁止していること、中国政府はインターネット犯罪に反対し、その取り締まりに積極的に取り組んでいること、中国軍はこれまで一切のハッキング活動に関わっていないことを確認した上で、マンディアントの報告書が中国軍はサイバー諜報活動を行っていると指摘したことを「根拠がない」と批判した。

そして、マンディアントの報告書について、三つの問題点を指摘した。第一に、IP アドレスについての分析結果を以て中国がサイバー攻撃を行っているという結論には技術的な不確かさがあるということである。第二に、「サイバー攻撃」という言葉の定義には未だ曖昧なところがあるということである。ネット空間を通じた日常的な情報収集はサイバー諜報活動でしかないかもしれないという。第三に、サイバー攻撃は国境を越えた攻撃であり、秘匿性が高く、攻撃者が誰なのかを明らかにすることは難しく、無責任な情報の発信は問題の解決に不利であるというものであった。

2013 年 3 月に開催された第 12 期全国人民代表大会において国務院総理に選出された李克強総理は、会議閉幕後の記者会見において、マンディアントの報告書を意識したと思われる質問（「中国はサイバー攻撃を行っているのではないか」）を受けた。これに対

42　CNCERT/CC「2012 年我国互联网网络安全态势综述」<http://www.cert.org.cn/publish/main/upload/File/2013032120120CNCERTreport.pdf> March 20, 2013. CNCERT の報告によれば、2013 年 1 月 1 日から 2 月 28 日までに間の 60 日間で、海外の 6747 のトロイの木馬形ソフトウェアあるいはボットネットを介して中国国内の 190 万台余りのホストコンピュータが操作され、そのうち米国の 2194 のトロイの木馬形ソフトウェアあるいはボットネットを介して、中国国内の 128.7 万台のホストコンピュータが操作された、という。

43　なお翌 20 日の定例記者会見でも同様の質問がなされており、報道官は同様の回答をしている。

する回答もまた、従来の公式発言を踏襲したものであった。それは、一つには中国はサイバー犯罪に反対であること、二つ目には中国はサイバー犯罪の最大の被害者であること、三つ目には根拠のない推測を以て中国を批判するべきではないということである。

4.3 「インターネット情報の保護強化に関する決定」の採択の二つの理解

2012 年 12 月 28 日に開催された第 11 期全国人民代表大会（国会に相当）の常務委員会（全国人民代表大会は、年 1 回、15 日程度しか開催されないため、その常設機関）において、「インターネット情報の保護強化に関する決定」（以下、「決定」）を審議し、賛成多数で可決した。

この決定の採択は、中国ウォッチャーの間で少なくない注目を集めた。それはこの決定が、第 6 項において、インターネットサービスの事業者はインターネットサービスの利用者に対して、身分を証明する情報の提供を要求することを確認したからである。

この決定は、その冒頭で目的として、サイバースペースにおける安全の保護、中国の公民や法人およびその他の組織の合法的な利益の保障とともに、国家の安全や社会公共の利益を保護することを確認していた。そのため、邦字紙は、この決定には当局がサイバースペースに対する管理の強化を目指すねらいがある、あるいは、同決定が採択されたことによって官僚の腐敗汚職の摘発に積極的な役割を果たしているネット言論を萎縮させる可能性があると分析していた。

また邦字紙は、「中国共産党の幹部などへの社会的監視が十分でない中国では、汚職追及や内部告発をする上でネットが最も有効な手段となっていること」や、同決定が採択された後に開催された記者会見において、インターネットサービスの利用者に対する身分照会を実施することによって「インターネットを使った汚職や腐敗の追及をしにくくなるのではないか」との質問が出たことに触れたたうえで、この決定を採択したのは、当局が「民主活動家らへの監視や言論封じ込めを狙っている」からとの分析をしていた。

中国共産党の新旧指導部が交代する過渡期というタイミングに、この決定が採択されたのはなぜか。その一般的な分析は、政治的な観点に基づくものである。中国共産党の指導部は、サイバースペースにおいて中国共産党や政府に対する不満が拡大していること、インターネットを通じて汚職や腐敗の告発が過激に、過度に行われていること、そして 2011 年末から 2012 年春の「アラブの春」運動において SNS が積極的な役割を果たしたことを憂慮している。そうしたことを踏まえて、中国当局はサイバースペースに対する警戒と管理の強化を目指して、このタイミングでこの決定を採択したのではないかと分析されてきた。

しかし、この決定の採択の意図には、中国における安全な経済活動を維持するためという経済的な理由も含まれているようである。すでに中国では、2000 年 12 月 28 日に全国人民代表大会常務委員会が「インターネット空間の安全を保護することに関する決定」を採択してサイバー犯罪の定義を明確にするとともに、「刑法」と「治安管理処罰法」の修正を通じてサイバー犯罪に対する罰則を明記した[44]。

こうしてサイバー犯罪に関する関連する法律法規が明確にされたにもかかわらず、その後も中国におけるサイバー犯罪件数の増加は著しかった。中国当局は、この事実を深く憂慮している。新華社などの主要メディアの 2007 年の報道によれば、2005 年の時点で全国のコンピュータとネットワークシステムの 80%が何らかのウイルスに感染し、また情報を盗み取ることを目的としたウイルスによる被害の件数が 2004 年の前年比 30%増から 2006 年の前年比 90%増へと急激に拡大し、2005 年の公式ウェブサイトが第三者によって改ざんされた事件の件数は 9100 件であり、このうち政府の公式ウェブサイトに対する攻撃が 2027 件であったという。中国当局は、こうした報道をつうじて、サイバー犯罪の蔓延に警鐘が鳴らし、社会に対して注意を喚起してきた。

2006 年 12 月から翌年 1 月にかけて、湖北省武漢市の青年が開発したコンピュータ・ウイルス「パンダの焼香（熊猫香焼）」が、猛威をふるった。「パンダの焼香」によって、わずか 2 ヶ月間で金融、税務、エネルギー部門を含む政府機関や企業を含む、100 万台のコンピュータが感染し、特に江蘇省はその深刻な被害を受けたといわれている[45]。また直近では、2011 年 12 月 12 日に、中国の主要なインターネットフォーラムやインターネット販売サイトである「CSDN 論壇」、「天涯社区」、「東京網」、「当当網」、「支付宝」、「騰訊」、「嘟牛」、「7K7K」、「多玩网」、「178 游戯網」、「多玩」、「世紀佳縁」、「珍愛網」、「美空網」、「百合」などのデータベースから、アカウントナンバーとパスワードを含む個人情報が漏洩する事件が発生している[46]。別の報道では、2011 年 2 月の春節以降、中国の主要な全国規模の銀行及び都市銀行などの中国の主要な金融機関において、フィッシング詐欺によって個人情報が流出したとされている。

44　新華網「全国人大常委会关于维护互联网安全的决定」<http://news.xinhuanet.com/it/2006-04/30/content_4495376.htm> April 30, 2006.

45　新華網「“熊猫烧香”案解密网络病毒产业链」<http://news.xinhuanet.com/legal/2007-02/16/content_5745932.htm> February 16, 2007. Sina「熊猫烧香病毒肆虐网络专题_科技时代_新浪网」<http://tech.sina.com.cn/focus/Worm_Nimaya/> Date Unknown.

46　CNTV「用户个人信息保护：一个民本网络环境的塑造」<http://jingji.cntv.cn/2013/02/28/ARTI1362056676973845.shtml> February 28, 2013. eNet.com.cn「网御星云：从应用安全事件谈安全服务」<http://www.enet.com.cn/article/2012/0322/A20120322985251.shtml> March 22, 2012.

図表 8　インターネット実名制に関連する法律法規

2002 年 11 月 15 日	「インターネットサービスを提供する空間における管理条例」[47]：インターネットサービスの利用者は、インターネットサービスを提供する場所の管理者に対して利用者の身分を証明する公的書類を提示しなければならないとした。事実上のインターネットカフェを利用する顧客に対する実名制の導入。
2004 年 12 月 28 日	「高等教育機関のキャンパスネットワークの管理の強化に関する意見」（国家教育部）[48]：高等教育機関のキャンパスネットワーク上に開設されている BBS を利用するにあたっての実名制の導入。
2010 年 9 月 1 日	工業情報化部の通達にもとづき、携帯電話の購入に際しての実名制を実施[49]。
2011 年 12 月	北京、上海、天津、広州、深圳の 5 都市において微博（マイクロ・ウェブ）を利用する際に実名制を導入。
2012 年 12 月 28 日	全国人民代表大会常務委員会、「インターネット情報の保護強化に関する決定」を採択。

中国のサイバースペースにおける情報の管理と保護、情報漏洩の防止のための当局による取り組みの歴史は、決して最近になってはじまったわけではない。その保護と管理のため、関係する法律法規の起草と修正が、過去 10 年の間、継続的に取り組まれてきた。サイバースペースにおける情報保護のあり方は、中国社会においても非常に重要な課題でありつづけた。例えば、中国においてインターネットサービスを利用する場合、利用者は身分を証明する情報をサービス提供者に対して提供しなければならない（これは「実名制」といわれる)。こうした実名制は、図表 8 のように 2002 年の時点から導入が図られてきたのである。

4.4　サイバースペースにおける情報保護の強化を求める要求

今日の経済活動においてインターネットは重要な役割を果たしている。安定した、安全なインターネット環境は、経済の発展にとって不可欠である。華字紙報道によれば、2011 年の上半期に、インターネットのアカウントやパスワードが盗み取られたインターネットユーザーは 1.21 億人であり、インターネットユーザーの 84.8%（4.56 億人）がインターネットを利用している過程で情報の保護の観点から危険を感じ、インターネット犯罪によって生じた直接的な経済損失は 200 億元に相当するという。

47　新華網「互联网上网服务营业场所管理条例」<http://news.xinhuanet.com/zhengfu/2002-10/11/content_593298.htm> Date Unknown.

48　吉林省教育文献資源庫「关于进一步加强高等学校校园网络管理工作的意见」<http://www.jledu.gov.cn/2012/0814/16294.html> August 14, 2012.

49　ChinaByte <http://telecom.chinabyte.com/zt/sjsmzss/> August 26, 2010.

こうした現状を反映するかのように、2013 年 3 月に開催された全国人民代表大会と中国人民政治協商会議全国委員会会議では、中国のサイバースペースの情報保護の安全性をめぐる問題が多く議論された。2012 年 12 月末に全国人民代表大会常務委員会において「インターネット情報の保護強化に関する決定」が採択されたことも、活発に議論された要因の一つであると考えられる。中国の主要メディアは、2013 年の全国人民代表大会と中国人民政治協商会議全国委員会会議における、一つのホットトピックであったと報じている。報道によれば、サイバースペースにおける情報の保護の強化を訴える議案や提案が、全国人民代表大会代表や中国人民政治協商会議全国委員会委員から提出された。つまり、中国は国外に対するサイバー攻撃を行っているだけではなく、国外から国内への、あるいは国内同士でのサイバー攻撃が日常化し、深刻になっているということである。その現状をいわば告発する形で代表や委員たちが問題提起している。

興味深いことに、サイバースペースにおける情報保護について発言した全国人民代表大会代表や中国人民政治協商会議全国委員会委員は、インターネットの管理を担当する国家機関関係者よりも、中国で活躍し、成功を収めている企業経営者が多い。図表 9（42 ページ）はその一覧である。

中国の公式メディアにおいて情報を発信することができる人物は、当局によって恣意的に選択され、また発言の内容も当局の意図に沿ったものに限られる。したがって、企業経営者および経済界関係者の発言者が多く、人民解放軍・人民武装警察・公安関係者やインターネット技術専門家や弁護士などの発言者が少数であることに留意すべきだろう。全国人民代表大会や中国人民政治協商会議全国委員会委員の中に、より多くの、より専門的な人民解放軍・人民武装警察・公安関係者が選出されていることは間違いない。しかし、実際に、サイバースペースの情報保護の管理を担当している人物を、マスメディアの前に露出させることはできないのだろう。

しかし、少なくとも注目しておくべきことは、情報通信分野で活動している企業経営者からのサイバースペースにおける情報をめぐる問題についての発言が少なくないという事実である。中国の民意機関である全国人民代表大会や中国人民政治協商会議全国委員会は、中国共産党や政府にとって社会が直面している諸問題の実情を把握するための重要なルートである。したがって、全国人民代表大会代表や中国人民政治協商会議全国委員会委員による、サイバースペースにおける情報をめぐる問題についての発言が多く報じられていることは、中国当局が、それを深刻な問題として認識していることの表れであると理解できる。彼らの支持を得て体制の政治的な安定性が確保されているのであるから、当局は、彼らの問題意識を無視することはできない。報道の多さは、問題の深

刻さと当局の問題解決に向けた強い決意の現れであるといって良いだろう。

中国政府は、組織的にサイバー攻撃を行っているのではないかとの疑いに対して、必ず、自らはサイバー攻撃の被害者であると発言している。その発言は、中国のインターネット環境の現実を、一定程度、正確に反映しているのかもしれない。中国国内の議論を観察すると、インターネット環境の安全に対する問題は深刻であり、その問題の克服に向けた当局の取り組みは、始まったばかりであることが分かる。中国における海外企業の経済活動もまた、そうしたインターネット環境の中で展開することはいうまでもなく、中国へ進出している企業にとっても、問題は深刻である。

図表９　中国のインターネット環境における情報保護の必要性を主張していた人物

企業経営者および経済界関係者
鐘天華　全国人民代表大会代表、中国移動浙江公司総経理
魏　明　全国人民代表大会代表、中国移動河南公司総経理
徐　龍　全国人民代表大会代表、中国移動広東公司総経理
雷　軍　全国人民代表大会代表、小米手機董事長・CEO
馬化騰　全国人民代表大会代表、騰訊 CEO
景新海　全国人民代表大会代表、中創軟件董事長・総裁
李東生　全国人民代表大会代表、TCL 董事長
楊　震　全国人民代表大会代表、南京郵電大学校長
孫丕恕　全国人民代表大会代表、山東浪潮集団董事長
辜勝阻　全国人民代表大会代表、中国民主建国会中央委員会副主席
李彦宏　中国人民政治協商会議全国委員会委員、百度 COE
孫歩新　中国人民政治協商会議全国委員会委員、北京市郵政公司海淀区郵電局局長
張近東　中国人民政治協商会議全国委員会委員、蘇寧董事長
賀　強　中国人民政治協商会議全国委員会委員、中央財経大学教授
人民解放軍・人民武装警察・公安関係者
戴紹安　全国人民代表大会代表、人民解放軍代表、前駐エジプト中国大使館駐在武官
李賢玉　全国人民代表大会代表、人民解放軍代表、第二砲兵装備研究院某研究所総工程師
李　晴　全国人民代表大会代表、江蘇省徐州市公安局網絡警察支隊政治委員（前徐州市公安局計算機監察科）
周俊軍　全国人民代表大会代表、江西省瑞昌市公安局肇陳派出所教導員
梁志毅　全国人民代表大会代表、広東省仏山市公安局高明分局荷城派出所社区警務中隊中隊長
インターネット技術専門家・弁護士
韓徳雲　全国人民代表大会代表、重慶市弁護士協会会長
閻保平　全国人民代表大会代表、中国社会科学院計算機網絡信息中心研究員
中国共産党・政府関係者
張春賢　全国人民代表大会代表、新疆ウイグル族自治区党委員会書記
郭声琨　全国人民代表大会代表、広西壮族自治区党委員会書記

第 5 章　政府の対応

5.1　米国政府の対応

頻発し、日常化しつつあるサイバー攻撃に対し、米国のオバマ政権は、2009 年 1 月の発足当初から積極的な対応をとってきた。それは、先述のように、ブッシュ政権時代から進められていたイランへのサイバー攻撃計画の間接的な影響があったとも考えられるだろう。自らサイバー攻撃の計画を進めている以上、米国側も自国を守るためのサイバー防御を進めなくてはならない。

オバマ大統領は､政権が発足するとすぐに､サイバースペースに関する政策のレビューを 60 日かけて行うよう指示し、それは 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。

その報告内容を受け、2009 年 6 月には米軍の統合軍（USSTRATCOM）の下にサイバー軍（USCYBERCOM）の設置をオバマ大統領は命令した。初代のサイバー司令官には、インテリジェンス機関の国家安全保障局（NSA）の長官であるキース・B・アレクサンダー大将が兼任する形で任命された。

さらに、同年 12 月にはホワイトハウス内に「サイバーセキュリティ調整官」のポストを設置し、米国政府内の全省庁を横断的に調整するよう命じた。そして、2010 年 2 月には「4 年毎の国防計画見直し（Quadrennial Defense Review：QDR）」が発表された。この中では、先述のように、陸、海、空に次ぐ第四の作戦空間として宇宙、第 5 の作戦空間としてサイバースペースが規定された[50]。

2011 年 7 月には、国防総省は初の「サイバー戦略」を発表した[51]。ここでは、必要ならサイバー攻撃による報復を行うだけでなく、通常戦力の行使も辞さない方針も打ち出した。そして、2010 年に設置されたサイバー軍に、陸、海、空、海兵隊の各サイバー部隊を横断的に統括する権限も与えた。

2012 年 10 月、レオン・パネッタ米国防長官は業界団体の会合で演説し、さまざまなサイバー攻撃の「集積結果は、サイバー真珠湾になり得る。つまり、物理的な被害と人命の損失を引き起こす攻撃である。実際、それは国を麻痺させ、衝撃を与え、新しく深

50　United States Department of Defense, *Quadrennial Defense Review Report*, Department of Defense <http://www.defense.gov/qdr/qdr%20as%20of%2029jan10%201600.PDF> February 2010.

51　United States Department of Defense, *Strategy for Operating in Cyberspace*, Department of Defense <http://www.defense.gov/news/d20110714cyber.pdf> July 2011.

遠な脆弱性の感覚を創出するだろう」と述べた[52]。

このパネッタ国防長官の演説の中でもう一つ注目されたのが、先述のアトリビューション問題である。パネッタ長官は、「過去 2 年間、国防総省はアトリビューション問題に対処するため、科学捜査（フォレンジクス）に多大な投資をしてきており、その投資から利益を得るようになってきている。米国を害しようとする行為に責任を持つ者たちを米国は見つけ出し、捕まえる能力があるということに潜在的な攻撃者たちは気づいたほうが良い」と述べた[53]。先述のように、アトリビューション問題はサイバーセキュリティにまつわる困難な課題と考えられてきた。しかし、米国はこれに対応する方策を見つけたことを示唆している。

実際に、米国防総省がどのような方策を見つけたのか、その詳細は分かっていない。しかし一つヒントになるのが、グルジアの事例である。先述の通り、グルジアは 2008 年にロシアからと見られる大規模なサイバー攻撃を受けた。チェチェンをめぐって武力紛争がグルジアとロシアで展開されている最中であった。その際、グルジアへのサイバー攻撃に携わったと見られる人物に、わざとウイルスが仕込まれたファイルを盗ませ、それによってウイルスに感染させ、この人物のコンピュータをリモート・コントロールし、写真を撮ることに成功した。この写真は広くインターネットで出回った。この人物はいまだ拘束されてはいないが、プライバシーを奪われ、実質的に国際的な移動の自由も奪われたことになるだろう（図表 10）。

パネッタ国防長官は、さまざまな情報を付き合わせ、組織間の協力を進めていけば、アトリビューション問題はそれほど深刻ではないということを示唆しているのかもしれない。

米国では、情報セキュリティ企業の育成にあたって、非常にユニークな方法がとられている。その一つが、軍や情報機関による積極的な企業育成である。先にニューヨーク・タイムズ紙のサイバー攻撃の調査を担当したマンディアントは、実は米空軍の情報技術将校の OB を中心に設立・運営されている会社である。同社は、2011 年、JP モルガン系私募ファンド ワン・イクイティ・パートナーズ（One Equity Partners）、ベンチャーキャピタルのクライナー・パーキンス・コーフィールド&バイヤーズ（Kleiner Perkins Caufield & Byers）、投資管理会社トレルス・マネージメント（Trellus Management）

---

52 Leon E. Panetta, “Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City, October 11, 2012,” Department of Defense <http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136> October 11, 2012.

53 Ibid.

より 70 億円の出資を受け、業容を拡大した。2012 年の売上高は約百億円、従業員 330 名である。

図表 10　グルジアへのサイバー攻撃に加担したと見られる人物の写真

出典：Avik Sarkar “Russian Hacker Behind Cyber Attack on Georgia Caught on His Webcam,” Voice of Grey Hat <http://www.voiceofgreyhat.com/2012/11/Russian-Hacker-Caught-on-His-Webcam.html> (posted on November 2, 2012; accessed on January 30, 2013).

同社は、2004 年にケヴィン・マンディア（Kevin Mandia）によって、コンピュータへの侵入への対処を目的とする IT セキュリティ会社として設立された。マンディア CEO（Chief Executive Officer）は、米空軍のコンピュータセキュリティ技術将校出身で、第 7 通信群、AFOSI でサイバー犯罪捜査を担当し、ロッキードマーチン、MacAfee でセキュリティコンサル部門の部長を歴任した。トラヴィス・リース（Travis Reese）COO（Chief Operation Officer）も、米空軍で 10 年にわたりカウンターインテリジェ

ンス、コンピュータ犯罪捜査に従事した。そして、国防総省、情報系の仕事を請け負う民間企業に従事した後、マンディアントに入社している。また、リチャード・ベトリック（Richard Bejtlic）CSF（Chief Security Officer）も、米空軍情報将校を皮切りに、GE の CIRT（コンピュータ事故緊急対応チーム）長を経て、マンディアントに入社している。

このように、米国では軍や情報機関が積極的に情報セキュリティ人材と企業を育成している。その一つの手法が、ベンチャーキャピタルの手法を利用した企業への出資である。米国では、軍や情報機関が有望な情報セキュリティのベンチャー企業に出資することによって、その企業に民間投資を呼び込む育成政策をとっている。政府の信用のお墨付きを得たベンチャー企業は、その信用を梃に、政府からの出資の約 10 倍の資金を民間から得ている。そのような効果によって、情報セキュリティ企業を急速に成長させることに成功している。

そのようなベンチャーキャピタルの一つが、IN-Q-TEL という投資ファンドである。IN-Q-TEL は、1999 年に非営利のベンチャー投資ファンドとして、国家情報会議（National Intelligence Council：NIC）が設立した。設立の目的は、米国のインテリジェンス活動に資する最新の情報技術開発を支援、商用技術開発と諜報組織が必要とする技術のギャップを埋めることとしている。開発された技術を中央情報局（Central Intelligence Agency：CIA）のみならず、国防情報局（Defense Intelligence Agency：DIA）など米国の諜報コミュニティに広範に提供しているのが特徴である。CIA のジョージ・テネット（George Tenet）元長官は、IN-Q-TEL の開発したデータマイニング技術により、テロリストの活動分析を行っていると証言している。提案評価型による投資（1 件あたり 100～200 万ドル）を行い、総投資額は数百万ドルである。

IN-Q-TEL は、現在約 60 社に投資をしているが、そのうち 9 社が情報セキュリティ企業である。その中には、標的型攻撃の検知と防御で、仮想システム環境を用いた非常にユニークなサービスを売り物にして成長著しいカリフォルニア州のファイアアイ（FireEye）や電子商取引に置けるセキュリティ技術を開発している同じくカリフォルニア州のシルバー・テイル・システムズ（Silver Tail Systems）、セキュリティデータの解析を行っているマサチューセッツ州のリバーシング・ラボ（Reversing Labs）等がある。

このように、官民一体となって情報セキュリティ技術の開発に取り組んでいるのが、現在の米国の現状である。その背景には、先に述べたように、10 年以上にわた

る中国とのサイバースペースにおける冷戦が、大きな影響を与えていることはいうまでもない。

5.2 英国政府の対応

英国も多様かつ大量のサイバー攻撃の対象となっているはずだが、実際の被害についてはあまり報道されていない。企業の名前が出て来ることもほとんどない。その中で、英国がサイバー攻撃を切り抜けた例として引き合いに出されるのが 2012 年のロンドン・オリンピックである。近年のオリンピックではコンピュータ・システムが多用されており、それに対する攻撃が行われれば、計時・計測や記録に問題が出たり、結果の通知がうまくいかなくなったりするのではないかと懸念されていたが、大きな問題を発生させることなく切り抜けることができた。英国政府関係者はサイバー攻撃対策の成果だとしている。

英国はこれまで数多くのサイバーセキュリティに関する文書を発している。2008 年、英国は最初の国家安全保障戦略（National Security Strategy）を公表し、「国家の安全の確保に関与する全ての省庁、部局、軍の目標と計画を統合する単一の包括的戦略」とした[54]。

しかし、国家安全保障戦略が、サイバースペースを重要な国家安全保障の領域と述べるのは 2009 年のことだった。それによれば、サイバースペースとは、「あらゆる形態のネットワーク化されたデジタル活動。これはコンテンツおよびデジタル・ネットワークを介して行われる全ての活動を含む」とされた[55]。

サイバーセキュリティに起因する脅威認識は広範にわたる。不道徳なコンテンツから詐欺的な犯罪行為、スパイ活動からインフラストラクチャに対する破壊的な攻撃までである。

> 敵対的な国家、テロリスト、犯罪者は、われわれの権益を弱体化させるためにサイバースペースを用いることができる。これは国家レベルで行われる可能性がある。例えば、われわれの不可欠なインフラストラクチャに対する攻

54 Cabinet Office, The National Security Strategy of the United Kingdom: Security in an Interdependent World <http://www.statewatch.org/news/2010/oct/uk-national-security-strategy-2008.pdf>, 2008, p. 3.

55 Cabinet Office, The National Security Strategy of the United Kingdom: Update 2009 - Security for the Next Generation, 2009, p. 102.

撃がある。しかし、サイバースペースにおける安全保障上の脅威は、企業や個人の利益を脅かすことにもなる。過去においては、国家安全保障とは国家と国益を守ることであると政府は考えてきた。これはいまだに重要ではあるが、しかし、今日の世界においてわれわれが直面しているリスクの本質は、国家安全保障へのわれわれのアプローチが個々の市民や企業を守ることにも同様に向けられなくてはならないことを意味している。したがって今日、この戦略の改定にあたり、われわれは、サイバーセキュリティに関する英国の最初の国家戦略を発表し、安全な方法でデジタル・ブリテンの恩恵を人々が受けられるようにする[56]。

英国政府は国家安全保障戦略とは別のサイバーセキュリティ戦略を発表するという告知を出した。2010 年の戦略は、サイバーセキュリティは「ティア 1」の脅威であり、人工衛星によって受信、送信、収集される情報への意図的な破壊が「ティア 2」の脅威であるとした。

これらの安全保障戦略とサイバースペースは内閣府主導によって作られたが、英国政府内における内閣府は、日本と比較して強い権限が与えられている。

2010 年に出た「戦略的防衛・安全保障レビュー（Strategic Defence and Security Review：SDSR)」は、可能性とインパクトの評価に基づいてリスクを三つのティアに整理している。この戦略においてサイバーセキュリティは「ティア 1」として位置づけられている。つまり、英国の国家安全保障にとって最も深刻な脅威の一つと見なされているということである。この戦略の公表にあたり、国家サイバーセキュリティ・プログラムへの資金拠出が発表された。この文書は、国防省に「サイバー作戦グループ（Cyber Operations Group)」の形成も発表している。

2009 年のサイバーセキュリティ戦略（Cyber Security Strategy：CSS）は、英国で初めて発表された統一的サイバーセキュリティ戦略である（ただし、以前に出された国家情報保証戦略［National Information Assurance Strategy］が同じ領域をカバーしている)。CSS は、国家、民間部門、一般市民を包含する広い安全保障枠組みによって構築された政府全体の戦略である。その目標は以下のように述べられている。

市民、企業、政府は、安全で回復力のあるサイバースペースの恩恵を全面的に

56 Ibid., pp. 3-4.

享受することができる。国内外でともに取り組むことで、リスクを理解して対処し、犯罪者とテロリストにとってのメリットを減らし、英国全体の安全と復元力を増進させるためのサイバースペースにおける機会をつかむことができる[57]。

2009 年サイバーセキュリティ戦略は、国家サイバーセキュリティ・プログラムの創設、および同プログラムの実施に当たる二つの組織の新設へとつながった。最初の組織は、「サイバーセキュリティ局（Office of Cyber Security：OCS）」であり、現在では「サイバーセキュリティ情報保証局（Office of Cyber Security and Information Assurance：OCSIA）」と呼ばれている。第二の組織は、「サイバーセキュリティ作戦センター（Cyber Security Operations Centre：CSOC）」であり、英国のサイバー・ネットワークへの攻撃をモニターするために設置された。これは通信傍受や暗号解読を担うインテリジェンス機関である「政府通信本部（Government Communications Headquarters : GCHQ）」に置かれている。

二つの組織以外に 2009 年サイバーセキュリティ戦略によって設定されたステップとしては以下が挙げられる。

- 英国のネットワークを守るための革新的未来技術の開発のための追加資金の供給
- クリティカルなスキル育成の促進
- 広範な公的部門、民間部門、人権団体、国民、国際的パートナーとの密接な協働[58]

2011 年の戦略は、以前のものと比べると、サイバーセキュリティにおける民間部門と市民の役割と責任をいっそう強調した点で異なっている。

英国政府の現在のサバイーセキュリティ戦略は、「国家サイバーセキュリティ・プログラム（National Cyber Security Programme : NCSP）」を中心に展開している。これは、先述の「2010 年戦略防衛・安全保障レビュー」の一部として発表された。これは、4 年間で 6.5 億ポンドをサイバーセキュリティのために政府機関に配分するというものであ

57 Cabinet Office, Cyber Security Strategy of the United Kingdom: Safety, Security and Resilience in Cyber Space <http://www.official-documents.gov.uk/document/cm76/7642 /7642.pdf > June 2009, p. 3.

58 Ibid., p. 5.

る。このうち約 60%は、インテリジェンスおよび安全保障機関（MI5、MI6、GCHQ）に割り当てられ、その次に大きいのが国防省である。2011 年から 2013 年の間に、インテリジェンスおよび安全保障機関は 1 億 7500 万ポンドを使うと見込まれている[59]。NCSP は、先述の OCSIA によって管理・調整されている。

原則的には、NCSP の成果物に責任を負っている政府機関が 15 存在する。しかし、実際に関与する組織・部門は官民でずっと多くなる。

NCSP は、サイバーセキュリティに関連して四つの戦略的目標を有している。

（1） サイバー犯罪に取り組み、ビジネスをするのに最も安全な場所の一つに英国をする。
（2） 英国とサイバー攻撃に対してもっと抵抗力のあるものとし、サイバースペースにおける英国の権益をより良く守れるようにする。
（3） 英国民が安全に使え、オープンな社会を支持するような、オープンで、安定的で、活力のあるサイバースペースの形成に資する。
（4） すべてのサイバーセキュリティの目標を支持するために英国の分野横断的な知識、技能、能力を構築する。

このうち、国防省とともにインテリジェンスおよび安全機関は、第二の目標を達成することが期待されている。

しかし、かなりたくさんの機関が第一の目標に従事しており、英国政府が広く定義しているサイバー犯罪は、サイバーセキュリティのリスクを広く捉えるならば、英国が直面する最もやっかいな問題といえるだろう。

サイバーセキュリティのための熟練人材を雇用・保持することは英国政府にとっても課題となっている。GCHQ のディレクターは、議会での証言で「大きな問題は、政府が必要な技術スキルを持つ人に魅力的な給与を提供できないということである。高給職は例えばグーグルやマイクロソフトで見つけることができる」と述べている[60]。GCHQ のディレクターはさらに「毎月、『申し訳ありませんが、3 倍の給料と車とその他をもらいにいきます』というようなことをいって辞めていく人材がいる」とも指摘

59 National Audit Office, The UK Cyber Security Strategy: Landscape Review <http://www.official-documents.gov.uk/document/hc1213/hc08/0890/0890.pdf> 2013, p. 22.
60 Intelligence and Security Committee, Annual Report 2010-2011, 2011, p. 20.

している[61]。

雇用・保持の問題に対処するためにパフォーマンスに応じたボーナスの導入も提案されている。

サイバーセキュリティに関連して現在および将来に必要なスキルや知識を満たすという問題は、英国政府に数々の戦略コミュニケーションや教育イニシアチブを導入させることになった。それによって、(1) 必要な技術的スキルを持っている人やその獲得に興味を持つ人がいるようにする、(2) その人たちが政府の仕事に興味を持つようにする、ことが期待されている。

GCHQ は、工学・物理学研究評議会（Engineering and Physical Sciences Research Council：EPSRC）とビジネス・イノベーション・スキル省とパートナーを組み、八つの「サイバーセキュリティ研究における学術研究拠点」を認定した。工学・物理学研究評議会はサイバーセキュリティ研究に研究する主要な英国の学術研究評議会である。毎年 4000～5000 万ポンドが使われる見込みで、サイバーセキュリティに関連する分野で 100 人の博士課程学生が修了すると期待されている。

別の枠組みとして、「国家暗号チャレンジ（National Cipher Challenge）」がある。これは英国の高校生がサウサンプトン大学でサイバースペースと暗号について教育を受けるというものである。さらには、コミュニケーション、セキュリティ、エンジニアリングなどの大学の多くで 2 年間の技術研修プログラムが提供されている。

いわゆる「Single Intelligence Account」と呼ばれる実習スキームもある。ここでは、インテリジェンス・コミュニティの仕事を毎年 100 人の学生に教えるというものである。

重要な戦略コミュニケーション・プログラムとしては「サイバー・セキュリティ・チャレンジ」もある。これは、サイバーセキュリティのキャリアに若い学生や職業人を誘うためにコンペティションやさまざまなイベントを行うというものである。

5.3 日本政府の対応

先述の通り、日本政府全体の情報セキュリティの司令塔的な役割を果たすのが NISC である。こうした日本政府の動きの背景にあるのは、情報通信技術を安心して利用できる環境の実現、つまり「情報セキュリティ先進国」の実現が、日本の持続的発展と情報通信技術を利用したより良い国民生活の実現へつながるという考え方で

61 Ibid.

ある。NISC はそのために情報セキュリティ政策会議の事務局として各種戦略を企画・立案し、官民連携により統一的・横断的な情報セキュリティ政策を推進することになった。

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。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、政権交代が行われた。

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。

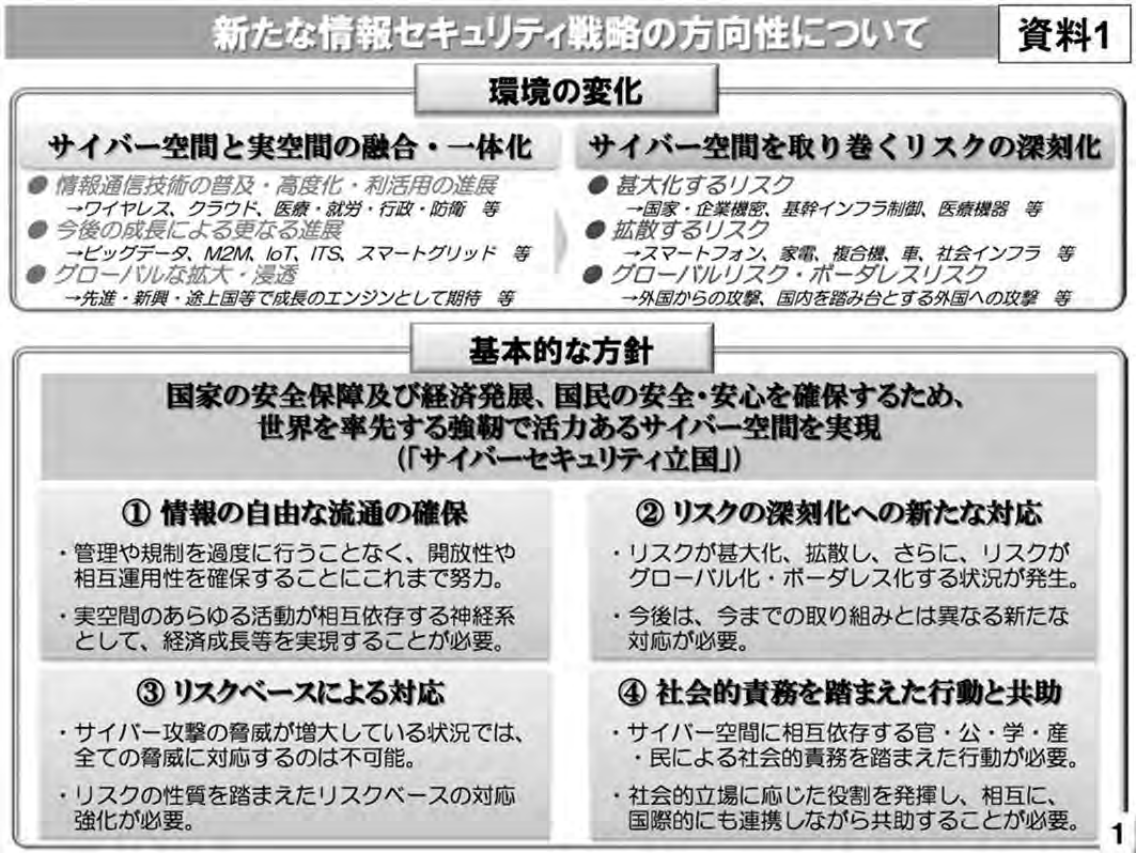
「国民を守る情報セキュリティ戦略」の基本方針は、第一に、サイバー攻撃事態の発生を念頭に置いた政策の強化及び対処体制の整備、第二に、新たな環境変化に対応した情報セキュリティ政策の確立、第三に、受動的な情報セキュリティ対策から能動的な情報セキュリティ対策へ、となっている。

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。

この戦略の下、「情報セキュリティ 2010」、「情報セキュリティ 2011」、「情報セキュリティ 2012」が作成され、毎年必要な対策が講じられてきた。

2012 年末、政権は自民党を中心とする安倍政権へと移った。そして、「国民を守る情報セキュリティ戦略」が期限を迎えるため、2013 年夏に向けて新しい戦略が策定中である。そこでは、これまで進められてきた政策を総括するとともに、サイバー攻撃の新しい局面に対応する「強靱で活力ある」サイバースペースを実現するための政策が検討されている（図表 11）。

図表 11　NISC による新たな情報セキュリティ戦略の方向性を示した資料



出典：http://www.nisc.go.jp/conference/seisaku/dai33/pdf/33shiryou0100.pdf

それでは、こうした政府の対策に加えて、企業ではどんな対策が必要とされているのだろうか。次章では、結論に変えて、企業経営者の視点から考えるべきサイバーセキュリティ 10 箇条を示すことにしたい。

第６章　企業経営者のためのサイバーセキュリティ 10 箇条

これまで見てきたように、サイバー攻撃による被害は経営を直撃するおそれがある。もはやこれは他人任せ、部下任せにできる問題ではなく、企業経営者自らが判断を下すべき問題であるという認識を持ち、常に自ら対応を考える必要がある。その際に留意すべき 10 箇条をここにまとめた。

【攻撃が起こる前】

1. **狙われないようにする**
2. **専門家の話を聞く**
3. **過去の経験は役に立たない**
4. **情報セキュリティ投資は必要不可欠なコストである**
5. **守れない規則を強要するな**
6. **記録を残せ**
7. **内部犯行の可能性を忘れない**

【攻撃が起こった後】

8. **事実関係を承知してから判断をする**
9. **対策の優先順位付けをする**
10. **情報を共有する**

【攻撃が起こる前】

1. 狙われないようにする

備えがあることを明示する。ただし、無限に投資することは現実的ではない。情報資産を分散したり、暗号化しておいたり、被害が甚大、致命的にならないよう準備しておく。対策を事前に講じて、被害を極小化しなければならない。いったん狙われたら逃げられない。担当者を責めても仕方がないことを覚悟しておく。コカ・コーラ社の事例では、同社はサイバーセキュリティへの投資で積極的だと見られていたが、巧妙な標的型電子メール攻撃で買収交渉の情報を盗まれていた。

2. 専門家の話を聞く

たくさんある経営課題の中で情報セキュリティも大事である。しかし、情報セキュリティだけを見ているわけにもいかない。専門家の話をちゃんと聞く必要がある。分からない言葉は説明を求め、分かった気になってやりすごしてはいけない。ただし、専門家は現状で一番良い対策を教えてくれるが、将来も正しいわけではないことを理解しておく。また、専門家を育て、長期的に産業を育てることも視野に入れておく。

3. 過去の経験は役に立たない

最新の情報に基づいて判断せよ。攻撃側は常に新しい脆弱性を探し、それにつけ込んでくる。過去に有効だった対策はすぐに十分ではなくなる。未知のウイルス、マルウェア、攻撃法が存在する可能性は排除できない。攻撃の技法は日夜進化している。

4. 情報セキュリティ投資は必要不可欠なコストである

投資すべき場所と量をまちがえてはならない。何をどこまでやればよいか。自社の規模や保有する量だけでなく、自社が持っている情報の質を勘案した情報セキュリティ投資をすべきである。専門家任せになるとセキュリティ投資が増大する一方になる可能性もある。経営者がリスク評価を行い、自らセキュリティ投資のレベルを判断しなければならない。

5. 守れない規則を強要するな

セキュリティの脆弱性は人間に由来する。人間にミスはつきものである。単なる言い

訳のための規則はいらない。セキュリティを強化するあまり、日常的な業務に過度の支障があるようではいけない。

6. 記録を残せ

さまざまな記録情報（ログ）を一定期間保持し、過去に遡って攻撃を解析できるようにしておく。攻撃者は痕跡を消そうとする。消えない足跡が残るようにシステムを設計しておかなければならない。

7. 内部犯行の可能性を忘れない

攻撃は外部からとは限らない。作為・不作為の内部犯行が攻撃の引き金になることは多い。自社の情報の出入りを監視するとともに、利用者の権限を限定し、むやみに使わせない。退職者の ID を削除し、アクセスを遮断する。

【攻撃が起こった後】

8. 事実関係を承知してから判断をする

攻撃者が悪いことを理解し、被害者や担当者を過剰に責めても仕方ない。法定伝染病と同じく、防衛と対策は一社だけの責任では担えないことを理解する。政府機関や他社などとの連携に二の足を踏まない。

9. 対策の優先順位付けをする

（1）日々のオペレーションの継続、（2）犯人探しのための証拠保全、（3）原因の究明と対策の設置、（4）対外的信用や株価との間で、優先順位を付けて対応を判断しなければならない。対応が経営全体に与える影響を考慮しなくてはならない。

10. 情報を共有する

一社でできることには限界がある。情報共有は他社を救い、長期的には自社を救う。目先の利益にとらわれず、大きな利益を追うべきである。名前を出さずにインシデント情報を共有できるシステムがある。他社などとの連携に二の足を踏まない。自社が自ら情報を共有することにはデメリットだけではない。

おわりに

東京都千代田区の神田明神では「IT 情報安全祈願」のお守りが人気になっているという[62]。2012 年にいわゆる「遠隔操作ウイルス事件」で誤認逮捕があったことから、一般にもサイバー攻撃の怖さが浸透してきているということだろう。

しかし、お守りは気休めでしかない。交通安全祈願のお守りは人気があるが、本当の交通安全につながるのは、日頃の自動車の整備と安全運転に他ならない。「IT 情報安全祈願」のお守りも、あらゆる手を尽くした後の気休めとして買うべきだろう。何も手を打たずしてお守りだけで対処できるはずがない。

どんな分野でもセキュリティへの投資は、無駄な投資に見えることがある。軍事力の整備は、軍事衝突が起きない限りにおいては、税金の無駄にも見える。軍事力の保持はときとして抑止力にもなるが、それでも戦争の火蓋が切られ、敗戦の憂き目を見ることもある。そうすると、最初からセキュリティへの投資をしなければ良かったという評価が出てくることもあるだろう。

サイバーセキュリティへの投資も同様である。いったい、いくら投資すれば完璧な備えになるのかは分からない。いくら投資しても、いったん狙われてしまえば、セキュリティは破られてしまうかもしれない。軍事予算の額を軍隊に尋ねれば、軍隊はよりいっそうの軍備の充実を求めるだろう。同じくセキュリティ予算の額をサイバーセキュリティ担当者に尋ねれば、よりいっそうの予算の割り当てを求めるだろう。適切な投資の水準が一意に決まらないところが、セキュリティの難しい点である。

したがって、どれだけの投資をサイバーセキュリティに行うかは、経営者の経営判断にかかっていることになる。全体的な経営状況を把握した上で、自社にとって絶対に失ってはいけない情報資産を特定し、優先順位を付けながら、対策を打っていくしかない。やはり、鍵もかけずにドアを開けっ放しにしている家よりは、何重にもセキュリティ対策を施している家のほうが、攻撃者にとってはやっかいである。みすみす情報資産やビジネスの機会を失うことがあってはならない。

本報告書の第 1 章「最悪のシナリオ」で示したように、サイバーセキュリティはそれぞれの企業の経営を直撃するとともに、一社だけにとどまらず、業界や社会全体に波及する危険がある問題だということを理解し、10 箇条をベースにして適切な経営判断を求めたい。

---

62 「冤罪防止ソフト、サイバー攻撃保険…お守りまで　インターネット犯罪対応商品が人気」『読売新聞』2013 年 4 月 7 日。

主要参考文献

- Arquilla, John, and David Ronfeldt, “Cyberwar is Coming!” *Comparative Strategy*, vol. 12, no. 2, Spring 1993, pp. 141-165.
- Clarke, Richard A., and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do about It*, New York: ECCO, 2010. クラーク、リチャード、ロバート・ネイク（北川知子、峯村利哉訳）『世界サイバー戦争―核を超える脅威　見えない軍拡が始まった―』（徳間書店、2011 年）
- Farwell, James P., Rafal Rohozinski, “Stuxnet and the Future of Cyber War,” *Survival*, vol. 53, no. 1, pp. 23-40.
- Lynn, William J., III, “Defending a New Domain: The Pentagon’s Cyberstrategy,” *Foreign Affairs*, vol. 89, no. 5, September/October 2020, pp. 97-108.
- Nye, Joseph S., “Cyber Power,” Harvard Kennedy School Belfer Center for Science and International Affairs, May 2010.
- Sanger, David E., *Confront and Conceal: Obama’s Secret Wars and Surprising Use of American Power*, New York: Crown Publishers, 2012.
- Tikk, Eneken, Kadri Kaska, and Liis Vihul, *International Cyber Incidents: Legal Considerations*, Tallinn: Cooperative Cyber Defence Centre of Excellence, 2010.
- 伊東寛『「第 5 の戦場」サイバー戦の脅威』（祥伝社、2012 年）。
- 情報セキュリティ政策会議「国民を守る情報セキュリティ戦略」（2010 年 5 月 11 日）。
- 土屋大洋『サイバー・テロ　日米 vs.中国』（文春新書、2012 年）。
- 西本逸郎、三好尊信『サイバー戦争の真実』（中経出版、2012 年）。

サイバー攻撃の実態と防衛

21 世紀政策研究所 研究プロジェクト
（研究主幹：土屋大洋）

2013 年 5 月発行
21 世紀政策研究所

〒100-0004　東京都千代田区大手町 1-3-2
経団連会館 19 階
TEL: 03-6741-0901
FAX: 03-6741-0902

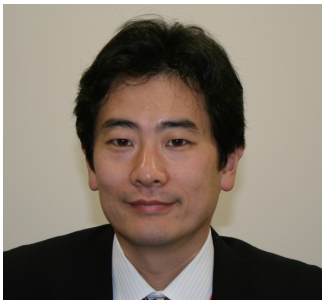
ホームページ：http://www.21ppi.org


21世紀政策研究所
The 21st Century Public Policy Institute

研究主幹に聞く

「サイバー攻撃の実態と防衛」プロジェクト

サイバー攻撃を止めることはできないのか



慶應義塾大学大学院 政策・メディア研究科教授
土屋大洋氏

2012年度の研究プロジェクト「サイバー攻撃の実態と防衛」の取りまとめをされている土屋大洋研究主幹に、サイバー攻撃の影響や対応の難しさについて聞きました（10月19日）。

――最近、公的機関や大学、特定の企業などに対するサイバー攻撃のニュースが報道されるようになりましたが、そもそもサイバー攻撃とは、どういうものですか。一般の企業や個人も攻撃の対象になるのでしょうか。

サイバー攻撃とは、コンピューターシステムやインターネットなどを利用して行う攻撃で、たとえば、①ウェブページの書き換え（ターゲットのパスワードを不正に入手してサーバーを操作し、ウェブページを書き換える）、②DDoS攻撃（多数のパソコンにコンピューターウィルスを感染させ、ターゲットのサーバーに対して大量のアクセスを集中させるように仕向けてダウンさせる）、③標的型電子メール攻撃（APT。ターゲットに電子メールで送って、ターゲット用にカスタマイズされたウィルス付きの添付ファイルを開かせたり、本文中に記載されたURL［ウェブサイトのアドレス］にアクセスさせたりして、ウィルスに感染させ、パソコンを乗っ取り、情報を盗んだり流出させたり、盗撮・盗聴したりする）、④ターゲットのコンピューターシステムにウィルスを感染させ（インターネットに繋がっていなくともUSBメモリなどを通じて感染する）、防空網やプラントなどを機能させなくする、などがあります（表１参照）。

イランの核施設（シーメンス社の遠心分離機制御プログラム）を使えなくしてしまった「スタックスネット」と呼ばれるウィルスは、その後、イランの技術者のパソコンからインターネット上に広まり、シーメンス社の制御プログラムを使っていた日本の水道施設も感染したと言われています。

マスコミなどでは報じられていませんが、こうした攻撃は、政府機関や特定の産業・個人に留まらず、既に、一般の企業や個人にも広がっています。その実態はなかなかつかめませんが、セキュリティサービス会社などに

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９月	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	リトアニアとグルジアでロシアからと見られる大規模DDoS攻撃。
2009年３月	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。
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12月	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６月	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DDoS攻撃。
2010年11月	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20台が感染。
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。
３月	欧州連合（EU）の欧州委員会や欧州対外活動庁に攻撃。
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。
５月	米シティーグループのネットバンキングシステムから利用者の個人情報が盗まれる。
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侵入される。
６月	国際通貨基金（IMF）が数カ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。
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盗み見られる。
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。
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。
８月	オランダのデジノター社の電子証明書発行システムに侵入され、500を越える偽証明書を発行。米グーグルの利用者などに被害。
2012年６月	「アノニマス」が日本のダウンロード違法化に抗議して政府サイトなどを攻撃。
７月	財務省のコンピュータ約120台が長期にわたりウイルスに感染し、情報が抜き取られていた可能性が発覚。

出所：土屋大洋著「サイバー・テロ　日米 vs. 中国」（文春新書）

は、かなりの相談があると聞きます。

――サイバー攻撃は、通常の攻撃や犯罪とどのように違うのでしょうか。それは、誰がどのような目的で攻撃するのでしょうか。

サイバー攻撃の第一の特徴は、攻撃者の特定が非常に難しいということです。サイバー攻撃の目的には、遊び・いたずら、金儲け、政治的攻撃などさまざまですが、攻撃される側から見ればどれも同じに見えます。しかも、攻撃者が、国内外のいろいろなルートを迂回して攻撃してきて、ウィルス感染の痕跡も消してしまう。たとえば、DDoS攻撃では、ウィルスに感染したたくさんの一般のパソコンが攻撃に使われます。また、中国などからの攻撃が多いと言われていますが、政府の指示によって統一的に行われているわけでは必ずしもありません。各部局がばらばらに攻撃したり、個人（民間人）や金銭でサイバー攻撃を請け負う「傭兵」が攻撃したりするなど、攻撃主体は多様であると言われています。さらに、他国が中国のパソコンを利用しているケースもあると言われています。

攻撃者の特定は非常に難しく、特定できなければ、反撃を加えることも、犯人を捕まえることも非常に困難になります。

第二の特徴は、攻撃されている側が、攻撃されていることに気づきにくいということです。特に標的型電子メール攻撃では、関係者からの正常な電子メールを装って送られて来ますので、添付ファイルを開いたり、URLにアクセスしたりしてウィルスに感染したことに気づかず、知らない間にサーバーやパソコンに蓄積された知的財産や情報が盗まれてしまうケースがあります。標的型ではありませんが、遠隔操作ウィルスに感染して、知らない間に脅迫メールの送信者に仕立て上げられた４人が、誤認逮捕されたケースも発生しています。

――それでは、わが国のサイバー攻撃への対応は、どうなっているのでしょうか。

日本政府は、サイバー攻撃に対して比較的早い段階から対策を取り始めていて、1999年８月の不正アクセス禁止法の公布を皮切りに、内閣官房情報セキュリティセンター（略称NISC。センター長は内閣官房安全保障・危機管理担当副長官補）と情報セキュリティ政策会議（議長は内閣官房長官）が中心となって、2010年５月に策定した「国民を守る情報セキュリティ戦略」に基づき、年度計画を立てて取り組んでいます。なお、これらの対応は、主に政府の重要施設や国の重要インフラを守ることを念頭に置いたもので、直接個々の企業や個人のシステムを守るものではありません。

また、警察庁の定点観測システム（全国の警察施設のインターネット接続点にセンサーを設置）がサイバー攻撃を24時間体制で監視しています。

自衛隊にもサイバー部隊「システム防護隊」がありますが、これはあくまでも自衛隊のシステムを守るためのものです。

国際的には、非政府組織ベースでは、JPCERT（Japan Computer Emergency Response Team）コーディネーションセンターが、各国のCERTとの間で連絡調整の窓口機能を果たしています。政府ベースでは、「サイバー犯罪に関する条約」が2001年に採択され、日本でもようやく関連の国内法を改正して、今年11月１日に発効しました。また、国際サイバー会議や国連でもサイバーセキュリティの問題が取り扱われはじめ、12月の国際電気通信連合（ITU）ではインターネットがITUの管轄に入るか否かが議論される見通しです。

いずれにせよ、抑止の対象となる攻撃者が誰だか分かりにくいので、完全に抑止することは難しい。

――企業や個人は、サイバー攻撃を回避することはできるでしょうか。攻撃を受けてしまったらどうすればいいのでしょうか。

企業や個人が、サイバー攻撃から完全に逃れることはできませんが、最低限自助努力で、ウィルスソフトの導入やOSのアップデート、メールの添付ファイルを安易に開かない、不要なアクセスはしない、などによってある程度は防げると思います。さらに、自分のパソコンでどのようなプログラムが動いているか、不正な動きをしていないか、モニタリングすることが重要です。自分でできなければ、プロバイダーやセキュリティサービス会社に依頼することになります。

特に企業の場合、弁護士や会計士を雇うのと同じ感覚で、情報セキュリティを確保するための専門家を雇う必要があると思います。国は、米国や韓国の先進事例を参考に、そうした人材の養成を急ぐ必要があります。

攻撃を受けてしまったら、セキュリティサービス会社などに相談して被害をできるだけ最小限に止めるしかありませんが、独立行政法人情報処理推進機構（IPA）などを通じて広く攻撃情報を共有し、日本社会全体のセキュリティレベルをあげることも非常に重要です。

インタビューを終えて

IT化の進展に伴い、サイバーセキュリティの確保は、非常に重要な課題になっています。当プロジェクトでは、一般の企業・個人にとって参考になるような報告書を取りまとめ、シンポジウムを開催したいと考えています。（主席研究員　篠原俊光）