経済広報センターポケット・エディション・シリーズ　No.134

我が国の
サイバーセキュリティ戦略

内閣官房情報セキュリティセンター　副センター長
内閣審議官

谷脇　康彦

一般財団法人
経済広報センター

インターネット環境が整備され、高度な情報端末が急速に普及するなど、情報通信技術が社会経済活動の重要なインフラとして定着してきている。一方、政府機関や企業、個人に対するサイバー攻撃は大きな社会問題となっており、情報漏洩などサイバー空間のリスクを防御するセキュリティ対策が喫緊の課題になっている。

そこで、経済広報センターでは、二〇一四年四月二二日、「我が国のサイバーセキュリティ戦略」について、内閣官房情報セキュリティーセンター（ＮＩＳＣ）の谷脇康彦副センター長・内閣審議官を講師に講演会を開催した。

講演では、サイバー空間におけるリスクについてご説明いただくとともに、政府が二〇一三年六月に策定したサイバーセキュリティ戦略に基づいて、ＮＩＳＣを中心に展開している具体的な対策や取り組みについてお話いただいた。

政府がさらされている脅威と、企業がさらされている脅威は、基本的には同じであり、本講演の内容は、民間企業におけるサイバーセキュリティの取り組みのヒントになるものと考え、本ポケット・エディション・シリーズとして発行することとした。

経済広報センター
ポケット・エディション・シリーズ

「我が国のサイバーセキュリティ戦略」

日　時　二〇一四年四月二二日（火）
　　一四時四五分～一六時

場　所　経団連会館　四〇一号室

講演者　谷脇　康彦　内閣官房情報
　　セキュリティセンター
　　副センター長
　　内閣審議官

【講師略歴】（敬称略）

谷脇　康彦（たにわき　やすひこ）
内閣官房情報セキュリティセンター　副センター長
内閣審議官

一九八四年	郵政省入省
二〇〇〇年	郵政省　電気通信局 事業政策課調査官
二〇〇二年	在米国日本国大使館参事官
二〇〇五年八月	総務省　総合通信基盤局 電気通信事業部　料金サービス課長
二〇〇七年七月	同　事業政策課長
二〇〇八年七月	総務省　情報通信国際戦略局 情報通信政策課長
二〇一一年七月	総務省　大臣官房　企画課長
二〇一二年八月	総務省　情報通信戦略局付
二〇一二年九月	総務省　大臣官房審議官 （情報流通行政局担当）
二〇一三年六月	内閣官房情報セキュリティセンター 副センター長

最初に、内閣官房情報セキュリティセンターについて紹介させていただきたい。英語で、National Information Security Center、略してＮＩＳＣと呼んでいる。職員は民間の方も含めて、今、八〇名体制で仕事をしている。情報セキュリティということで、当然インターネット上のあるいはサイバー空間の脅威に対して、守りを固めるという仕事をしているわけだが、非常にユニークな機関である。二つ役割を持っており、内閣官房として、各省庁のセキュリティ関係の政策を取りまとめ、国の戦略として推進していくという役目が一つ。もう一つは、霞が関の色々な情報システムを、二四時間、三六五日監視して、外部から霞が関に対して行われる攻撃を日々観測し、そして解析を行い、各省庁に警告したり、対策のお願いをしたりする役割である。要するに、政策の推進と日々のオペレーションを車の両輪としている職場である。

サイバーセキュリティと言うと、何かＳＦのような話と思われるかも知れないが、実はもう現実のものになってきており、その対策が喫緊の課題となっている。

まず、我が国が国家戦略として初めてＩＴ戦略を作ったのは二〇〇一年のe-Japan戦略であり、当時は、まさにインターネット普及の黎明期で、その戦略に基づいて高速大容量の光ファイバー網などが普及した。無線の世界でも今、３・９世代、つまりＬＴＥ（Long Term Evolution）が普及するなど、固定網、無線網を問わず、ブロードバンド網が整備されている。

安倍政権のＩＴ戦略「世界最先端ＩＴ国家創造宣言」は二〇一三年六月に閣議決定されたが、その中で、経済成長に必要な「ヒト」「モノ」「カネ」という基本的な要素に加えて、「情報資源」の活用こそが経済成長をもたらす鍵となると言っている。

最近よく、新聞や週刊誌などで、ビッグデータを活用した新しいビジネスを創っていこうと言われているが、これは、今までよりもＩＴに益々依存する社会になってきているということである。

さて、そのビッグデータにはどのようなものがあるのかと言うと、四つのカテゴリーに分けられると思う。

一つ目が、オープンデータである。国、地方公共団体等が持っている統計データや地理データなどをマシンリーダブル（機械判読可能、すなわちデータを容易にソフトウェアで加工できる状態）な形で公開し、こういったデータを使って新しいビジネスを創造してもらおうというものである。例えば、最近、国土地理院や気象庁が様々なデータを公開しており、そのデータを使ったビジネスが生まれつつある。

二つ目は、ナレッジ（知恵、ノウハウ）のデジタル化である。最近政府が健康データの活用を検討している。例えば、健康保険組合の組合員の方々が健康になろうと努力すれば、医者にかかる確率が下がり、健保組合の財政はよくなる。それならば、健康になるよう努力した組合員には健康ポイントを付与したり、あるいはそ

のデータを解析することで新しい薬を創ったり、新しい治療法を考えたりするなど、そういったデータの活用も考えられる。また、農業では、田畑にセンサーを置いて、日照量や風向きなど収集した外的なデータと、経験と勘を持つベテランの農家の方が作業した記録とを付き合わせることにより、農業のノウハウの形式知化も可能になる。さらに、社会インフラでは、トンネルや橋にセンサーを埋め込んで、それを解析することにより、老朽化したインフラをどこから直していけばいいのかといったメンテナンス作業の効率化が図れる。

三つ目が「M2M（マシントゥーマシン）」、つまりセンサーなどの機器やモノが感知したデータの収集・活用である。例えば、車が走ったり、停車したりしているデータを集め解析し、道路の混雑状況の把握や信号の間隔の調整など、街をスマートに運用することに生かせるのが「M2M」である。スマートメーターの導入などもこの類型に入ってくると思う。

四つ目が、個人のデータを活用したビジネスである。今、政府では現行の個人情報保護法の見直しをしようということで、データの活用とプライバシーを守ること、このバランスをどう取るのか検討しており、個人情報保護法の改正法案を二〇一五年の通常国会へ提出することを目指して検討を進めている。

このように多種多様なデータを使ってビジネスを創出することは、まさに成長戦略の中の大きな一つの要素になるわけであるが、こうして

我々の社会経済活動がＩＴに依存する比重が高まっていく中で、光の面だけではなく、影の面というものも今まで以上にクローズアップをされてきているという状況である。

具体的に、このサイバー空間、インターネット上において我々が直面しているリスクについて三点申し上げたい。一点目はリスクが従来よりも深刻なもの、甚大なものになってきていること。二点目は、サイバー空間の攻撃の対象範囲が拡大し、リスクが拡散してきていること。三点目は、インターネットには国境がないため、リスクがグローバル化してきていることである。

この三点について少し具体的に説明させていただきたい。サイバー攻撃は、十数年前位から登場してきたわけだが、最初は他人のホームページを改ざんし、自分の技術を誇示するような愉快犯的なものだった。それが最近では、特に金融機関をはじめとして、ＩＤやパスワードが漏出し、経済的な損害を被るケースが非常に深刻化してきている。

加えて、最近の事例として増えているのが、政府機関が持っている国の機微にわたる情報、あるいは民間企業の技術情報や知的財産といったものを標的に設定しピンポイントで攻撃をして、それを窃取しようという攻撃である。

冒頭申し上げたように、ＮＩＳＣでは、政府の情報システムを二四時間、三六五日監視をしているが、どのくらい不正な通信を感知しているかと言うと、霞が関の情報システムは一年間

で一〇八万回攻撃を受けている。一〇八万回といっても規模感が分かりにくいと思うが、一分間に二回攻撃を受けていると理解していただければよいと思う。二〇一〇年が四八万回、二〇一一年が六六万回であったので、倍々で増えているということが分かる。

サイバー攻撃を受けてシステムが停止してしまうことにより、社会経済活動に大きな影響を与えてしまう分野を重要インフラと呼んでいる。今までは、①情報通信（放送も含む）、②金融、③航空、④鉄道、⑤電力、⑥ガス、⑦政府・行政サービス、⑧医療、⑨水道、⑩物流の一〇分野を指定していたが、二〇一四年度からは、化学、クレジットカード、石油の三分野を追加し、一三分野を重要インフラと呼んでいる。

この重要インフラに対しても様々な攻撃が行われている。重要インフラ分野の事業者からの情報連絡によると、二〇一二年度には不正アクセスやウイルス感染などの報告は一一〇件あった。米国でも重要インフラを狙ったサイバー攻撃が増えており、二〇一一年から二〇一三年までの間に、攻撃が一七倍に増えたという非常に深刻な状況である。これが、リスクの甚大化、深刻化ということである。

二点目は、リスクが拡散をしているということであり、その一つがスマートフォンである。スマートフォンは、電話帳が入っていて、位置情報も取られており、カメラもついているなど個人情報の塊である。こういった情報が抜かれてしまうというケースが多々ある。それから、

自動車もある。自動車は、一台にコンピューターが一〇〇個以上積まれており、ソフトウェアでかなりの部分制御されている、いわばスマートカーとなっている。攻撃者が無線を使って車を勝手に操作することができてしまうということが、実はＳＦの世界の話ではなくなってきている。

また、電力各社はスマートメーターの導入を始めている。自宅の検針メーターがネットワークにつながり、需要家の電力消費量が通信ネットワーク経由で電力会社に知らされることになる。今まで電力ネットワークは、電力を融通するために存在していたわけだが、これがいわば通信のネットワークと融合することになってくる。従って、サイバー攻撃を仕掛けることによって、都内一円を停電させることも不可能ではなくなってきている。

三点目はリスクのグローバル化である。サイバー空間は国境がなく、いわば我々は一人で暗い部屋の真ん中に座っているようなもので、どこからぽかりとやられるか分からない。これがサイバー空間が今置かれている状況と言えるかと思う。

韓国の事例を紹介したい。韓国は、国連の電子行政ランキング（隔年ペースで公表）で二回続けて第一位であり、世界で最も電子行政が進んでいる国であるが、二〇〇九年と二〇一一年に、政府機関に対する大規模な攻撃が発生している。一つのサーバーに、色々なパソコンから集中してアクセスし、ダウンさせるＤＤｏＳ攻

撃が発生した。二〇一三年の三月には、金融機関全てのＡＴＭが一斉にダウンし、また、放送局、新聞社も業務用のシステムが全てダウンした。韓国当局は、これらは北朝鮮による攻撃であると発表している。実は、二〇一三年のこの韓国に対する攻撃に使われた不正プログラムが、同じ時期に日本でも発見されている。従って、日本でもこういった事態が起き得るということであり、脅威はすぐそこまで来ているということになる。

大規模なサイバー攻撃を最初に受けた国と言われているのは、エストニアである。エストニアもＩＴが非常に進んでいる国である。二〇〇七年に、世界で初めて大規模なサイバー攻撃を受け、三週間にわたり、政府機関、銀行、ＩＳＰ（インターネット接続業者）の機能が停止した。二〇〇八年にはグルジアがサイバー攻撃で麻痺をし、昨今でもＮＡＴＯ軍がサイバー攻撃を受けたという報道もされている。

このように、もはや、サイバー攻撃というものは非常に現実的なものになってきている。二〇一四年一月に世界経済フォーラムが出した『グローバルリスク報告書二〇一四年版』の中で、世界的な規模でリスクが発生する可能性が大きいものとして、トップ五に「サイバー攻撃」がランクインしている。社会経済システムがインターネットに依存する度合いが高まり、インターネットに繋がるデバイス（機器）の規模も極めて大きくなったことで、サイバー分野は、社会そのものまでも破壊してしまうほどのグローバルリスクであると広く認識をされるようになってきている。

また、リスクの影響度のトップ五には、「重要インフラの故障」が入っており、この重要インフラというものには、先ほど触れた通信、電力、金融、鉄道、といったものが含まれる。つまり、重要インフラは、サイバー空間において攻撃を受ける可能性が非常に高く、かつ攻撃を受けてシステムがダウンすると、社会経済に重大な影響を及ぼすということが広くグローバルに認識されている。

二〇一四年三月に政策投資銀行は、日本の企業と地方公共団体がどのようにリスクを捉えているのかについて意識調査結果を発表した。地方公共団体が、一番発生する可能性が高いリスクとして見ているのが、サイバー攻撃であった。その後に原子力災害、テロリズム、長期にわたるインフラ整備の遅れなどが続いた。民間企業についても同様で、大規模なデータの不正利用・窃盗、サイバー攻撃が発生する可能性が大きいと見ている。

一方、リスクが一旦破裂をしてしまうと与える影響が大きいものとして、地方公共団体の第一位はパンデミック、第二位が環境問題、第三位にサイバー攻撃が入っている。民間企業においても、原子力災害に次いで第二位にサイバー攻撃が入ってきている。従って、日本においても、サイバー攻撃は発生可能性が高く、影響度も大きいという認識が高まってきていると言えるかと思う。

サイバー空間がこれだけ大きくなって、我々が依存すればするほど、色々な問題が出てくる。その一つが、安全保障とサイバー空間とのかかわりである。二〇一三年一二月に、政府は国家安全保障戦略を閣議決定した。これは、今後一〇年間程度の国の安全保障の基本的な方向性をまとめたものであるが、その中で初めてサイバーという言葉が出てきた。海洋、宇宙空間、サイバー空間といった国際公共財（グローバルコモンズ）に対する自由なアクセス、およびその活用を妨げるリスクが拡散し深刻化していると指摘している。

また、この国家安全保障戦略の中で、サイバー空間というのは社会経済活動、軍事活動を含め、あらゆる活動が依拠する場となっていると述べている。そして、国家の秘密情報の窃取や基幹的な社会インフラシステムの破壊、軍事システムの妨害を意図したサイバー攻撃によるリスクが深刻化しつつあり、サイバー空間の防護というものは、日本の安全保障を万全とする観点から不可欠なものと位置づけている。

そもそも、サイバー攻撃について非常に難しいのが、誰が攻撃しているのか分からないということである。国の関与が深く疑われるけれども、国とは特定できない攻撃が来た場合、果たして日本政府としてどう対応するのか。これは非常に難しい問題である。サイバー空間には国境がない中、一体どの時点で私たちは自衛をするのか。専守防衛が当然基本ではあるが、実はまだ、国際的なコンセンサスづくりというものが必ずしも具体的には進んでいないという状況にある。

二〇一三年六月に、サイバーセキュリティ戦略を国として策定した。この戦略という設計図に基づいて個別の政策を、ＮＩＳＣを中心に現在展開している。サイバーセキュリティ戦略の構造を紹介したい。

一点目は、サイバー脅威に対して守りを固めるということである。守りを固める主体は三つに分かれている。一つ目は、国あるいは独立行政法人、二つ目が重要インフラ事業者、三つ目が一般のインターネットユーザーである企業や個人。これらの各主体の方々がサイバー防御をどう固めていくのかについて色々な施策が盛り込まれている。

二点目は、攻撃から身を守るための基礎体力（ファンダメンタルズ）が必要であるという点。具体的には、情報セキュリティ人材の育成や日本独自の強みを持つ技術開発などである。

三点目は、国際的な連携である。サイバー空間は国境がない中で、他の国々とどのように連携をしていくのかということである。この三点がサイバーセキュリティ戦略の柱ということになる。

次に、政府が具体的にどういう施策に重点的に取り組んでいるのかという点について説明したい。

まず、政府がどのようなセキュリティ対策を講じているのかについて述べたい。この話は、民間の企業でも取り組んでいただける内容では

ないかと思う。政府がさらされている脅威と、企業においてさらされている脅威は、基本的には同じである。政府の対応を一つのヒントとしてお聞きいただきたい。

現在、セキュリティポリシーは、各省庁で個別に決めている。

ただ、最低限守るべきベースラインとなるセキュリティの水準というものは、ＮＩＳＣが中心となって決めている。最低基準と言っても、脅威の高まりに応じ、これを段階的に上げていき、全体としてセキュリティレベルを底上げしていくという狙いがある。このセキュリティの基準を統一基準と呼んでいるが、この見直しを今、ＮＩＳＣで進めている（注：二〇一四年五月に情報セキュリティ政策会議で決定）。具体的な攻撃手法の中で、我々が最も対策を急ぐ必要があると考えているのが標的型攻撃と言われるものである。

具体的な事例をいくつか紹介したい。まず、標的型メールの特徴を説明する。差出人のアドレスで、@より右側のドメインが、省庁では“go.jp”であるが、“go-jp”のように非常に似た形で偽装しているものがある。また、件名で「重要」「緊急」などを付加し、開封を急がせるものがある。添付ファイルのアイコンをワードの文書のように偽装して送るものもある。拡張子が“exe”であるものは実行ファイルといって、これを開くと、不正プログラムに感染する。それからＵＲＬのリンク先を全く違うＵＲＬに偽装表示することも可能で、これを開くと攻撃者が用意したサイトに誘導されて不正なプログラムがダウンロードされ、パソコンが感染する事例もある。いったん感染すると、このパソコンは攻撃者の意のままに操れるようになってしまう。

この他、最近日本でも初めての事例として登場したのが、水飲み場攻撃というものである。攻撃対象組織が頻繁に閲覧するウェブサイトの脆弱性を見つけ、ここに攻撃者が不正なプログラムを仕掛けて、攻撃対象組織がアクセスした時のみ、これをダウンロードして感染させるが、一般の方がアクセスした時には何の影響も受けないといった、標的を特定してピンポイントで攻撃する水飲み場攻撃というものが日本でも発見されている。

標的型メールの件数は、非常に増えてきている。政府機関等への標的型メールに関するＮＩＳＣからの注意喚起の件数を見ても、二〇一〇年が一一八件、二〇一一年が二〇九件、二〇一二年が四一五件と、倍々で増えてきている。また、政府機関に限らず標的型メール攻撃に使用された不正プログラムの接続先であるが、日本国内はわずか三％であり、それ以外は全て外国のサーバーにアクセスし不正なプログラムが仕込まれてしまうという実態にある。

対策として、政府機関等では、標的型メール訓練をしてきた。ＮＩＳＣが作成した模擬の標的型メールを一二万人の政府職員を対象に送信し、どれくらい開封するかの訓練を実施している。二〇一二年度に二回実施した結果、開封率

は、一回目が一四・六%、二回目が一〇%であった。これは、一〇〇人いれば一〇人のパソコンが攻撃者に乗っ取られるということである。

標的型攻撃にどう対処するかであるが、政府機関や企業の情報システム内部の設計対策が効果的である。入口対策は今後とも重要であるが、もはや攻撃されシステム内部に侵入されることを前提として考え、攻撃者の侵入をいかに早く感知するか、被害をどのように最小化するかが重要になってきている。攻撃者は、まず管理権限から遠いパソコンに侵入し、中に潜んで内部探索をし、管理権限を持っているサーバーを乗っ取って情報を窃取しようとする。長いものでは二年から三年も攻撃者に中に入られていた事例もあり、攻撃者が中に侵入したことすら気がつかない企業も多くある。

そのような事例に対応するため、政府は、攻撃されたとき侵入範囲の拡大を防止するよう、内部探索がしづらいシステムを設計することや攻撃者の侵入を検知するためのトラップ（罠）を設置するなど、セキュリティ強化を図っている。防御を何段階にも固めていく多重防御が重要である。

ただ、多重防御するためには当然お金がかかる。予算の制約がある中でどうするかというと、重要な情報を扱う部署や情報システムを特定・選別するリスク評価を行い、システムを固めて守るべき情報には多重防御の仕組みを入れるなど、メリハリのあるセキュリティ対策をする。重点的に守るべき業務や情報がどこにあるかを

判断するのは、省庁では官房長等であり、企業では経営者であるので、彼らにセキュリティ対策の重要性を理解してもらう必要がある。従って、省庁では、官房長等がＣＩＳＯ（チーフ・インフォメーション・セキュリティ・オフィサー）として、現状の情報システムの対策状況や対策導入計画の内容・進捗状況について定期的に確認することができる仕組みづくりを始めている。

さて、ワンストップ型の行政サービスを実現するマイナンバーの導入に向けて、二〇一四年度から各省および各地方自治体のシステム改修が始まり、二〇一六年からマイナンバーを使った行政手続が始まる。サイバー攻撃というものは、つながっているシステムの中で一番弱いところを狙ってくる。マイナンバーができるということは、中央省庁と自治体のシステムが相互に連携し、必要な範囲で情報を互いにやり取りをするという仕組みになってくる。つまり、その弱いところを狙ってくる可能性があるので、このシステム改修にあたってはセキュリティの観点からも注意を払い、十分な措置を講じていく必要がある。

一方、政府としては、マイナンバーの利用範囲の拡大を検討しており、具体的には、民間企業との連携を検討している。企業においてもウェブサイトを持っていて、これにアクセスするための独自のＩＤやパスワードが設定されているが、アンケート調査によると、一般のユーザーが覚えられるＩＤは三つ位であると言われ

ている。そこで、信頼に足るＩＤ間の連携ができれば大変便利である。ところが、ＩＤは本当に正しい契約者のものであるのかどうか、ＩＤの認証を同じレベルの正確性や安全性の下で行っているのかどうかといった点についてお墨付きを与える仕組みが必要になってくる。ＩＤの連携に当たっては、マイナンバーと民間ＩＤの連携も考えながら、セキュリティを確保しつつトラストフレームワーク（信頼の枠組み）の構築を考えていくことが必要である。

先ほど、標的型攻撃を完全に防御するのは難しく、このためセキュリティのメリハリをつけることが大切であり、このため多重防御が必要だという話をしたが、霞が関全体の守りの体制ということで言うと、ＮＩＳＣの中にある政府機関・情報セキュリティ横断監視・即応調整（ＧＳＯＣ）チームが常に監視をしている。

各省庁においても、サイバー攻撃に即応できるような体制がある。例えば、ある省庁が大規模な攻撃を受けて、そこのスタッフだけでは対応が難しいという際には、ＮＩＳＣに応援要請が入り、情報セキュリティ緊急支援チーム（ＣＹＭＡＴ）が被害の確定や対策の強化に駆けつける。ＣＹＭＡＴは、各省庁のスキルを持っている約五〇名の職員で構成されており、定期的に訓練・研修を実施している。

また、重要インフラ一三分野について、ＮＩＳＣでは官民連携によるセキュリティ対策を強化しているところである。ある重要分野が大規模な攻撃を受けた際に、その情報を業界内、および業界を超えて他の業界と情報を共有することが必要であるため、特に情報共有体制の強化に努めている。他にも、各分野の事業者の方々の参加を得て大規模なＩＴ障害対応の訓練を定期的に行い、その中での気づきを次の対策に活かしている。さらに、重要インフラ各分野に横断的なセキュリティ対策の指針の策定と、それに基づく安全基準の整備などを官民連携で実施しているところである。

現在、重要インフラのセキュリティ対策の行動計画を策定しており（注：二〇一四年五月に情報セキュリティ政策会議で決定）、この中で、ぜひ伝えたいのは、セキュリティの重要性を経営者の方々にしっかり理解してもらうことが大変重要であるということである。サイバー攻撃を受けた場合の被害額の特定は難しい部分も正直ある。しかし、サイバーの世界でよく言われるのが、レピュテーションリスクである。サイバー攻撃を受けた企業の評判が、がた落ちになってしまう。これは計り知れないダメージになることをぜひ経営者の方々に理解いただきたい。

製造業あるいはガスプラント、石油プラントなどで使われているシステムは、いわゆる制御システムと言われるものであり、攻撃対象になりやすいという特徴が現れてきている。例えば、ある工場で使われているロボットは、従来は企業がそれぞれ独自に開発し運用していたものだったが、最近はコスト削減のため汎用型のＯＳを使うようになってきている。こういった

汎用製品を使うということは、つまり攻撃者もそれを知っているということであり、制御システムが攻撃される確率が高まってきている。

例として、ガスプラントを考えてみると、ガスタンクにどれくらい気圧があるかを遠隔監視によりパソコンで監視しているが、サイバー攻撃によって、実際のガスの気圧が高まっているにもかかわらず、監視モニター画面には正常であるという青信号が表示される可能性がある。政府としては制御システムのオープン化が進む中、どう防御するかということが非常に重要なテーマになってきている。

とりわけインターネットに接続されていないと思ったシステムが、実はインターネットに接続されているという状況が多々ある。複合機は、プリンターにも、コピー機にもファクスにもなる。これらはかなりの確率でリモートメンテナンスの機能がある。プラント設備においても、外部メディアの取り付け口があるものが七割以上ある。こういったところからウイルスが仕込まれる場合もある。

さて、一般の人は情報セキュリティについて、どのくらい認識を持っているかについてお話ししたい。二〇一三年夏の総務省の情報通信白書の中で、六カ国（日本、米国、英国、フランス、韓国、シンガポール）の意識比較をしたものがある。情報セキュリティ被害に遭ったことがあるかという質問に対して、受けたことがないという回答は日本が一番多く、六一・六％。ところが、インターネットを利用するときに不安を

感じるという人の数は、日本が飛び抜けて多く五〇・七％。ソーシャルメディアを利用する際が最も不安だと答えている。日本のインターネット利用者の約七〇％がウイルス対策を講じているにもかかわらず、不安を抱えている人が多いというのが日本の状況である。一方、標的型攻撃はウイルス対策ソフトでは防げないが、そうした特徴についての認知度は、米国、英国、フランスは五割以上の人が認知しているのに対し、日本の認知度は二四・五％と低い。従って、次々と登場する脅威に対して最新の情報をいかにわかりやすく伝え、普及啓発を図っていくのかという点が重要な課題である。

さて、防御能力を高めていく上で必要なのが、そのための基礎体力を強化する必要があるという点である。その一つがセキュリティ人材の育成の必要性である。

今、日本企業の中で情報セキュリティに携わっている方は約二六・五万人いる。しかし、経済産業省傘下の情報処理推進機構（ＩＰＡ）のデータによると、この二六・五万人の中で一六万人は能力不足で、さらに八万人の人材が不足しているといった結果が出ている。大学、大学院等で情報セキュリティのコースを卒業する人材は、年間一〇〇〇人なので、不足している八万人を埋めるためには今のペースでは八〇年もかかってしまう。

そこで注目しているのが、国内に一〇六万人いるＩＴ人材である。そのうちシステムエンジニアは八〇万人いる。こういった方々にセキュ

リティの知識も持っていただくことが大変重要になってきている。ただ、人材を育てても、就職先がなければどうしようもないわけで、他方、企業の方からすると、どこまでセキュリティ対策を行えばいいのか分からない部分もある。従って、政府としては、企業の経営層の意識改革を促すことを推進し、また各省庁の調達においては、情報セキュリティを要件化することによって、我が国のセキュリティ水準を向上させ、人材の需要喚起につなげることを考えている。

それでは、経営者の意識改革とは何かということであるが、米国の例で言えば、日本の有価証券報告書に当たる米国の証券取引委員会（SEC）に提出する報告書（10―K）の項目の中に、任意ではあるが、各企業のサイバー脅威がどれくらいあるのか、あるいはサイバー攻撃を受けた場合にどういう対応体制になっているのかについて書く欄があり、そのガイドラインをSECが作っている。

これを日本に当てはめて考えると、サイバーセキュリティへの備えや、あり得る想定被害を有価証券報告書に記載することになる。もちろん規制を導入するということは考えていないが、こうした情報開示の改善に向けた取り組みも今後重要になってくるのではないかと考える。経営者による株主への説明責任の中にサイバーセキュリティへの備えというものを位置付けることについて、現在、NISCと金融庁との間で議論を始めているところである。

セキュリティ関連の技術開発の在り方についても触れておきたい。今、国の成長戦略として重要視しているのは、医療・健康分野、スマートな都市機能の管理、ビッグデータの活用などである。日本でITの導入が進まない理由は、費用対効果の関係がよく見えないということと、セキュリティが心配であるという二点であると言われている。費用対効果についてはクラウドサービスの普及などに伴って費用が低下し、効果の大きさが明確になってきている。従って、残る課題であるセキュリティに対する懸念を払しょくするため、こういった発展分野でセキュリティ技術をどんどん開発していくことによって、ITの利活用も進むことが期待される。

さて、世界中で今インターネットをどれくらいの人が利用しているのかというと、世帯普及率は、先進国で七七・七％、途上国で二八・〇％であり、先進国と途上国との間の開きは依然として大きい。しかし、途上国の世帯普及率は今ぐんぐん上がってきている状況である。

これが何を意味しているのかというと、途上国でインターネットの普及が進むことによって、当然その国においてサイバー脅威が高まり、そのウイルスが、他の国に広がっていく可能性があるというのが一点。もう一点は残念なことではあるが、貧困を背景としてこういったサイバー犯罪に手を染める人たちが増える可能性も否定できない。従って、途上国のサイバーセキュリティ環境の底上げも、日本を含む先進国の責務だと思っている。

二〇一三年一〇月、政府は我が国のサイバー

セキュリティ分野におけるグローバルパートナーシップを強化するため、サイバーセキュリティに関する国際連携取組方針を策定・公表し、各国との政府間の政策対話を進めている。具体的には、米国や欧州といった先進国との間で政府間のサイバー協議を進めているが、昨今、我々がグローバルパートナーシップの観点から重視しているのがＡＳＥＡＮであり、二〇〇九年から様々な連携プロジェクトを展開している。ＡＳＥＡＮ各国と日本はいわばサプライチェーンで堅く結ばれており、経済的な結びつきが強い。しかも、ＡＳＥＡＮ一〇カ国の中でインターネットの普及率は、国によってまだ相当の格差がある。従って、これから成長、発展著しい国々のサイバーセキュリティを高めることに日本が協力していくことは、ＡＳＥＡＮ諸国にとっても日本にとっても利益があり、ウィンウィンの関係である。それ以外に最近では、エストニア、オーストラリア、ＥＵ、フランス、イスラエルなどの国々との間でサイバー協議の立ち上げに合意したところである。

さて、二〇二〇年、東京オリンピックが開かれる。私どもは今、二〇一二年のロンドンオリンピックの経験を、一生懸命勉強しているところである。実は、ロンドンオリンピックの期間中に、ロンドンオリンピックの公式サイトが、二億一二〇〇万件のサイバー攻撃を受け、中には大規模で集中的な攻撃であるＤＤｏＳ攻撃も受けていたということである。

そして非常に興味深い話だったのが、電力で

ある。ロンドンオリンピックの開会式当日の朝、サイバー攻撃によって電力がダウンする可能性があるという情報を政府が得て、開会式は全て電力設備をマニュアルで運用したということである。つまり、電力がなければオリンピックはできないという当たり前のことに気づかされたわけであるが、これは開催国の威信がかかっているので、レピュテーションリスクを狙った攻撃への対応が重要である。ダウンタイムは許されないことを原則として、政府機関はもとより重要インフラ事業者等と連携したセキュリティ対策が不可欠である。

二〇二〇年というと先のように思うが、実はその二八カ月前、二〇一八年の春には、情報システムは既に稼働していないといけない。そうすると、逆算すると二〇一五年頃にはシステム設計やセキュリティ対策について具体策を作っていく必要がある。

最後に、サイバー攻撃、サイバー脅威に対して、我々がまずやるべきこととして、情報の共有がますます必要になってきている。そのためにも、官と民が連携し、情報共有を促進することが大変重要であるということを述べたい。

本日、申し上げたかったことで最も重要なことは、まず、サイバー攻撃による被害を被ることを前提として、その被害を最小化するための対策が重要であること。二点目は、企業の経営層にサイバーセキュリティの重要性や緊急性を正しく理解していただくことが必要であるということ。三点目は、サイバー脅威から守りを固

めるためには、情報が各社の中にとどまるのではなく、いかに共有するかが重要であるということである。守るということが重要であるが、実は守っているつもりが、守りが弱いがゆえに攻撃者になっているということもある。自分のサーバーが攻撃されて攻撃者に乗っ取られ、別の企業へのＤＤｏＳ攻撃に知らない間に加担させられているという場合もあり得る。従って、それぞれの企業の社会的責務を果たしていただく上でも、守りというものは自分が攻撃者にならないためにも重要だということをぜひ認識いただき、それぞれの企業でセキュリティ対策に取り組んでいただければ大変有難い。

（文責　総務部主任　半田明美）

経済広報センター
ポケット・エディション・シリーズ

※当センターホームページでバックナンバー全文をご覧いただけます。（http://www.kke.or.jp/）

◆二〇一〇年発行

No. 112
「グローバル時代の英国の選択～日本へのヒント」
（英国ジャーナリスト・シンポジウムより）

No. 113
「持続可能な成長戦略を達成するための企業経営の課題」
（米国ビジネススクール教授招聘シンポジウムより）

No. 114
「二〇一〇年―日米関係の新たな扉」
（ライシャワー東アジア研究所との共催シンポジウムより）

No. 115
「東アジアのさらなる成長・発展に向けた日本ＡＳＥＡＮパートナーシップ」
（ＡＳＥＡＮジャーナリスト招聘シンポジウムより）

◆二〇一一年発行

No. 116
「台頭するアジアと日米の役割」
シンガポール国際問題研究所　所長
サイモン・テイ

No. 117
「世界金融危機後の経済体制と通貨制度はどうなるか」
英国王立国際問題研究所（チャタムハウス）
国際経済リサーチ・ディレクター
パオラ・スバッキ

No. 118
「日本の安全保障、経済と外交情勢―米シンクタンク研究者の視点―」
（米国シンクタンク研究者招聘シンポジウムより）

No. 119
「二〇一一年の米国の政治と政策見通し
―変化は起こるのか？―」

No. 120
「アジア・太平洋地域の発展とAPECの未来」
（日本経団連との共催シンポジウムより）

No. 121
「変化する世界における日英の役割」
（英国ジャーナリスト招聘シンポジウムより）

No. 122
「中国経済の行方」
野村資本市場研究所　シニアフェロー
関　志雄

No. 123
「アジア太平洋新時代における日印関係」
（インドジャーナリスト招聘シンポジウムより）

◆二〇一二年発行

No. 124
「成長する企業のためのイノベーションと創造性」
ブリガム・ヤング大学ハワイ校　学長
ハーバード・ビジネス・スクール　名誉教授
スティーブン・C・ウィールライト

No. 125
「二一世紀アジア太平洋時代と日印関係
～パートナーシップ発展への提言～」
（インド研究者招聘シンポジウムより）

No. 126
「ヨーロッパとドイツの現在と課題」

No. 127
「日韓新時代
～震災を越え、今後の日韓関係と
協力のあり方について考える～」
（韓国ジャーナリスト招聘シンポジウムより）

No. 128
「アジアの成長・発展と日本
～ASEANとのパートナーシップ強化に向けて」
（ASEANジャーナリスト招聘シンポジウムより）

No. 129
「政権移行期の中国経済の行方
―日本企業の対中投資戦略への提言―」
富士通総研経済研究所　主席研究員
柯　隆

No. 130
「ミャンマーの現状を知る
～日緬関係の発展に向けて」
（ミャンマージャーナリスト招聘シンポジウムより）

◆二〇一三年発行

No. 131
「日本のエネルギー安全保障を考える」
（エネルギー講演会より）

No. 132
「日中対立の経済関係への影響」
拓殖大学　政経学部　教授
朱　炎

No. 133
「ミャンマーの有識者に聞く
～経済・政治の改革～」
（ミャンマー有識者招聘シンポジウムより）

◆二〇一四年発行

No. 134
「我が国のサイバーセキュリティ戦略」
内閣官房情報セキュリティセンター　副センター長
内閣審議官
谷脇　康彦

経済広報センター
ポケット・エディション・シリーズの発刊に際して

経済広報センターは、土光敏夫氏（第四代経済団体連合会会長）のイニシャティブによって一九七八年に設立された財団法人です。当時国内では、企業の存在意義、あり方が厳しく問われ、また海外では、台頭してきたアジアの経済パワー、すなわち日本の動向に注目が集まっておりました。そこで、日本企業の考え方、行動、社会における存在意義などを広く内外にお伝えし、相互理解のチャネルとなるという志の下に、政府から独立した民間非営利組織として当センターが設立されました。

現在当センターは、経済界の政策提言や意見を社会にお伝えすることに力を入れております。そのような活動を支える基礎として、国内ではビジネスパーソン、消費者、ジャーナリスト、教育者、有識者との対話の機会を数多く設け、また、海外からは、多くのジャーナリスト、研究者、経済人、教育者を日本に招き、あるいは海外諸都市において日本の経済人、研究者による講演会やシンポジウムを開催するなどして、日本に関する理解の深化に努めております。

幸い、これら対話・講演・シンポジウムは、知識、情報、知見という観点からして深い内容となっており、会員各位から、当センター関係者のみが知るにとどめず、広く公共の財産として共有するに値するものであるとのご指摘をいただきました。

そこでこれからは、内外における対話や講演会やシンポジウムの記録をまとめ、「経済広報センター・ポケット・エディション・シリーズ」として、逐次刊行することといたしました。会員の皆様のみならず、各界の方々に広くご愛読いただければ幸いでございます。

このポケット・エディション・シリーズをより良いものとしていくために、各位のご教示を賜われば、幸甚に存じます。

一九九九年一二月

一般財団法人　経済広報センター

経済広報センターは、一般財団法人（二〇一二年四月一日に財団法人より移行）として三八業界団体、一六一企業の賛助を得て、経済界の広報活動を展開しております。

会長は榊原定征氏（東レ会長）、副会長は、岩沙弘道氏（三井不動産会長）、宮原耕治氏（日本郵船会長）、荻田伍氏（アサヒグループホールディングス相談役）、内山田竹志氏（トヨタ自動車会長）、佐々木則夫氏（東芝副会長）が務めております。

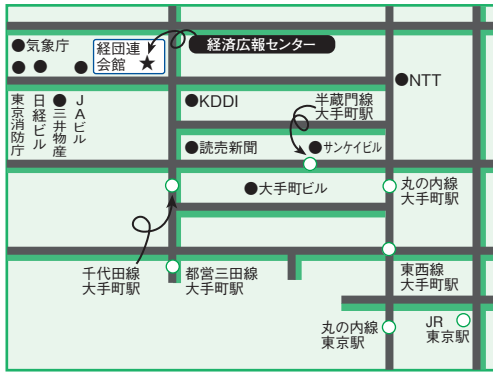
活動は次の四つの柱で展開しております。第一に、経済界の情報や提言を広く国の内外へ発信し、政策形成プロセスにおける議論を活性化するための広報活動、第二に、社会のメッセージを多角的に受信し、経済界の活動にフィードバックする広聴活動、第三に、豊かな知識社会を創造するための教育界との対話、第四に、会員企業・団体の広報活動の支援など、各種サービスの提供です。

これからも皆様方のご意見を伺いながら、各界の方々にご参加いただく活動を幅広く展開していきたいと考えております。

（本シリーズの緑色は国内広報活動、青色は海外広報活動に関するものです）

経済広報センター
ポケット・エディション・シリーズ No.134

発　　行	2014年7月29日
発 行 所	一般財団法人　経済広報センター 東京都千代田区大手町1－3－2　経団連会館 TEL：03(6741)0011　FAX：03(6741)0012
編集・発行人	中山　洋
印　　刷	株式会社　大巧



一般財団法人
経済広報センター
〒100-0004　東京都千代田区大手町1-3-2 経団連会館19階
webmaster@kkc.or.jp
http://www.kkc.or.jp/