情報通信の現在と未来を展望する

Vol.10
2012 Summer
ネクストコム

Nextcom

特集

情報セキュリティ

Feature Papers

論文
「情報セキュリティ」考：「防止」から「耐性と復元」へ
林 紘一郎 情報セキュリティ大学院大学 教授

論文
緊急事態と情報セキュリティ政策
湯淺 墾道 情報セキュリティ大学院大学 情報セキュリティ研究科 教授

論文
情報セキュリティガバナンス
—規制の情報セキュリティから戦略の情報セキュリティへ—
堀江 正之 日本大学 商学部 教授

特別論文
EUデータ保護規則提案と消費者プライバシー権利章典
石井 夏生利 筑波大学 図書館情報メディア系 准教授

Reports

学会リポート
「EEA-ESEM 2011」参加報告
馬場 弓子 青山学院大学 経済学部 教授

Articles

すでに始まってしまった未来について
期限付貨幣
平野啓一郎 作家

情報伝達・解体新書
偉大な微小脳
水波 誠 北海道大学 大学院理学研究院 教授

５年後の未来を探せ
池田英男教授に聞く
植物生理学・農学・ITが出会う「植物工場」の明日
船木春仁 ジャーナリスト

明日の言葉
何も言挙げせずとも
髙橋秀実 ノンフィクション作家

著書出版・海外学会等参加助成に関するお知らせ
論文公募のお知らせ

明日の言葉

Nullius in verba
言葉によらず
……王立協会のモットー

1660年にロンドンで設立され、現存する最古の科学学会である「王立協会」は、
そのモットーにラテン語の「Nullius in verba（言葉によらず）」を掲げている。
古代ローマの詩人ホラティウスの「Nullius addictus judicare in verba magistri
（何人も言葉に頼らず、おのれの目で見よ）」という言葉によるもので、
近代科学の客観性を強調している。

INDEX
summer
2012

Nextcom ネクストコム

特集
情報セキュリティ

オレゴン州ワロワ山地の氷河湖

すでに始まってしまった未来について ―― ⑩

文：平野啓一郎
絵：大坪紀久子

期限付貨幣

リタイヤ後の団塊世代の大量消費というのは、冷え込む内需の最後の望みのように久しく言われてきたが、どうも今のところは、さほどでもないらしい。私が読んだ新聞記事によれば、女性に比して男性の方が財布の紐が固いそうで、震災後の「いつ何時」という不安もあるだろうが、それが蓄財を促すのか、いっそ散財に向かわせるのかは人によって随分と違うだろう。恐らく、前者の方が多いだろうが。

楽しんで金を使うのは結構な事だが、消費しないのは悪である、というのは疲れる考え方である。私だって本を売って生活している人間だが、興味のない人にまで無理に金を出して買って欲しいと思った事は流石にない。

しかし、貨幣というものを、そもそも私的に、いつまでも所有し続けていていいのかという根本的な疑問もある。より多く消費する人は、結果として、より多くの人の生活を潤している。その上さらに消費税を徴収して社会福祉に当てるというのは本末転倒で、消費しない人からこそ〈無消費税〉――私の造語だが――を取って社会に還元させるというのは、一つのアイディアである。

もし貨幣が完全に電子化されて、税務署が所得と支出を全て把握できるような時代が来れば（ディストピア？）、貨幣に使用期限を設けて消費を促す、ということも考えられる。参考になるのは、ポイントである。

私は特にポイントマニアではないが、「年末までです」と期限の通知が来ると、やっぱり何かに使わなければという気持ちになる。

最近はますます寿命が延びて、90歳で亡くなった人の貯金を、相続するのが60歳の子供で、やっぱり死ぬまで貯金したままという笑うべきかどうかも分からない話がある。期限があれば、貨幣も安穏と銀行で眠っていることもなく、叩き起こされてまた社会に飛び出していくことにはなるだろう。

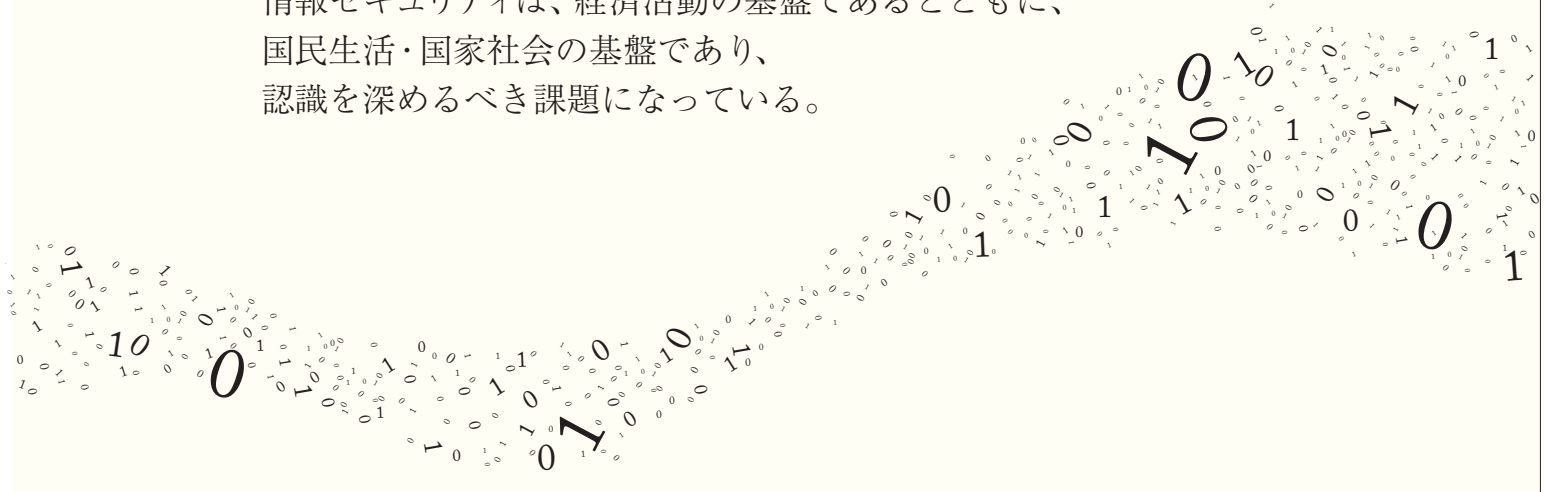
Keiichiro Hirano

小説家。1975年生まれ。1999年京都大学在学中に『日蝕』により芥川賞を受賞。
以後、『葬送』、『ドーン』、『かたちだけの愛』など、数々の作品を発表し、各国で翻訳紹介されている。
現在『モーニング』（講談社）にて 長篇小説「空白を満たしなさい」連載中。

特集

情報セキュリティ

情報セキュリティとは「機密性、可用性、完全性」が
維持されることと定義付けられている。
「真正性、責任追跡性、信頼性」と「否認防止」を加えることもある。
情報セキュリティは、経済活動の基盤であるとともに、
国民生活・国家社会の基盤であり、
認識を深めるべき課題になっている。



情報セキュリティ1

「情報セキュリティ」考：「防止」から「耐性と復元」へ

情報セキュリティ大学院大学 教授

林 紘一郎 Koichiro Hayashi

私は、2004年に開学した情報セキュリティ大学院大学の設立に参画し、
「情報セキュリティの法と経済学」を、学者としての最後の課題にすることに決めた。
その後約10年の試行錯誤を経て、やっと全体像を俯瞰できるところまできたとの感がある。
本誌への執筆依頼を機に、その直感をなんとか「形式知化」することを試みたい。
結論は、「セキュリティに決定打はない」「確率論やベスト・エフォートを所与とする気持ちが必要である」
「日本人が苦手とする『許すが忘れない』ことが大切である」といった常識的なものであるが、
若干目新しい知見として、「防止」から「耐性と復元」へという変化を、指摘したい。

キーワード
ディレンマ　トレード・オフ　ベスト・エフォート　耐性と復元　許すが忘れない

セキュリティのディレンマ1：残念ながら「否定的にしか定義できない」

セキュリティを追求するためには、克服しなければならない五つのディレンマがある[1)]。

第1は、「否定的にしか定義できない」ことである。『広辞苑（第六版）』によれば、セキュリティは、「① 安全。保安。防犯。② 担保。③ 証券。」とされている。このうち「安全」が最も近そうなので、改めて「安全」を引いてみると、「① 安らかで危険のないこと。② 物事が損傷したり、危害を受けたりするおそれのないこと。」となっており、結局「セキュリティ」の定義は「危険」や「危害」の定義に依存していることになる。

「セキュリティを絵にしてみなさい」という宿題を出したとすると、誰もがセキュリティが破られた状態、あるいは破られるリスクにさらされた状態を表現するだろう。こうして集められた「破られた状態」の陰にあって、何枚もの絵に共通の事象を集めたものが、セキュリティ対策になるのであり、リスクが「絵」で「地」の部分がセキュリティである。

セキュリティの定義については、他の国語辞典も同工異曲であり、「～（の状態）である」という肯定的な説明はなく、「～でない」という否定的な説明しかできないようである。これは、たかが定義の問題ということを超えて、社会的には意外に大きな差をもたらす[2]。

例えば、企業でセキュリティ投資を検討する際、いつも問われるのが「セキュリティを守るとこれだけの利益がある」と定量的に説明できないか、ということである。しかし、セキュリティが利益を生むのはその製品やサービスを売っている企業に限られ、一般のユーザー企業においては「セキュリティ対策を採れば、これだけの損失が防げる」という訴求しかできない。そして、売り上げ増という「プラス10%」も、同額の損失回避である「マイナス10%回避」も、会社に対する貢献度は同じなのに、なぜか前者が好まれる[3]。

この現象は、心理学者として初めてノーベル経済学賞[4]を受賞したカーネマンなどの研究成果を踏まえて、以下のように説明できる。彼らのプロスペクト理論によれば、人間は利得を得る場合よりも損失が生じた場合に、より強く刺激に反応する。賭け事において、損失を取り戻そうとして、リスクの高いビッドに走ってしまうのも、実質経済成長率が同じでもデフレよりもインフレが好まれるのも、この理論で説明できそうである。

とすると、その逆を行くのが企業として正しい戦略ではないかと思われる。つまり、100の利得がある計画と、100の損失を回避できる計画を比較するのは、人間心理を無視している。心理的効果も勘案すれば、「100の利得」と「80の損失回避」を同等と見ることで、初めて公平な評価が出来ると考えるべきであろう。しかし、これで説得できるほど、現在の企業環境は甘くないようだ。

ディレンマの２：守るより攻める方が楽

ディレンマの第2点は、セキュリティは守るよりも攻める方が格段に楽なことである。読者の多くは毎日スパム・メールに悩まされているであろう。メールの受信側は、スパムと判定されたメールの処理に毎日かなりの時間を取られているであろうから[5]、その社会的コストは馬鹿にならない。社会全体としては効用より費用の方が大きいから、何らかの方法でスパムを減らしてもらいたいところである。

しかし、発信者側のミクロのレベルでは、作業は機械化されていて何万通を送っても大したコストも時間もかからない。たとえ1万通に1通でも応答があって、それで何らかの商売（通常は詐欺などの非社会的なものであろうが）が成り立つなら、効用＞費用となるから止める理由はない。

このマクロとミクロ、送信側と受信側の非対称を是正する方法（送信側のコストを上げるか、成功率を下げる）は、今のところ見出されていない。つまり、パソコンやネットワークが、あまりに安価で使いやすくなったために、現時点ではセキュリティを破る方が圧倒的に優位に立ち、セキュリティを守る側を苦しめているのである[6]。最近のサイバー攻撃、それも標的型の攻撃についても、同じことが言えそうである。

ディレンマの３：トレード・オフが不可避

第3点として、より深刻なのは、「セキュリティ対策にはトレード・オフが不可避」なことである。代表的な事例として、DNA認証を取り上げてみよう。DNA情報は、地球上に現存する人間の間では重複する可能性が極めて低いことから、「究極の認証技術」として期

待する向きもある。しかし、照合するのもハードやソフトが関係するし、サンプリングの誤差もあるから、（他のセキュリティ技術と同様）100％ということはあり得ない。

そこで、「本人なのに他人と誤認され」たり（false negative、第1種の誤謬）、逆に「他人が本人と間違えられ」たり（false positive、第2種の誤謬）することが避けられない。図表1はこの状態を示しており、どこに閾値を設定して判定しても、誤りがゼロにはできない。できるのは、より安全サイドで行くか（この場合、利便性が犠牲になる）、より利便性を重視するか（この場合、安全性が犠牲になる）の選択になる。

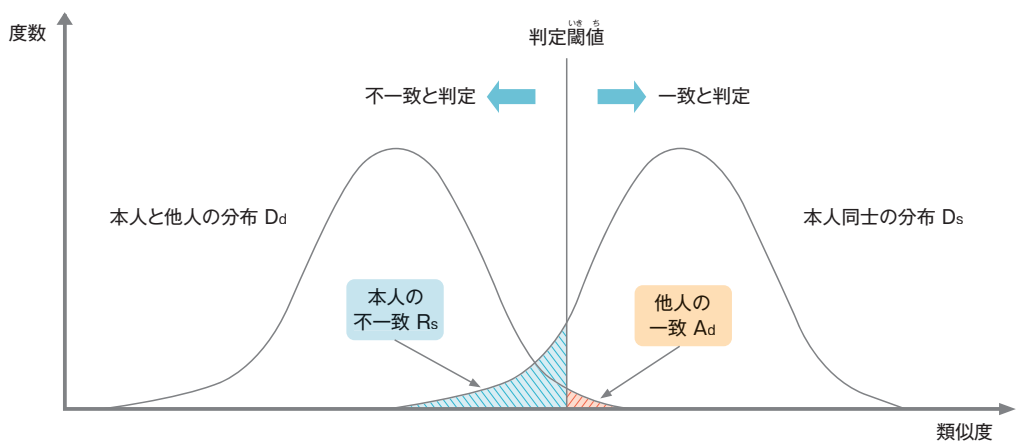
従来の科学法則の一般型は、「AならばBである」という形式で、これに当てはまらないものは、「例外」として切り捨ててきた[7]。今後は、トレード・オフを前提にした分析、100％はないという冷徹な眼、確率論や複雑系の科学などを積極的に取り入れる態度などが欠けると、セキュリティ分野における科学全体の寄与が、不可能あるいは僅少になるのではないかと懸念される。

ディレンマの4：リスク対策が別種のリスクを生むことがある

トレード・オフは同一の対策で「あちら立てれば、こちら立たず」の状態になることを指すが、「一つのリスク対策が別種のリスクを生む」危険性もある。医学的措置が良い例で、病気を治すために外科手術をすれば、一時的にせよ何らかの外傷は避けられない。薬を服用すれば、全く副作用のない薬は存在しない[8]。社会的な事象にも同じことが言え、農薬が農業の生産性を上げ、農作業を楽にしたことは間違いないが、かなりの薬害を生んだことも否定できない。何世代も後で、マイナスの効果が明らかになるケースもある[9]。

しかし、技術の進歩を止めることはできないし、人間は利便性に弱い。遺伝子組み換え植物や、IPS細胞などが期待通りの効果を上げれば、私たちの生活はより快適なものになると期待される。しかし、それに伴ってどのようなリスクが発生するかは、今のところ明確ではない。また、そのリスクを低減あるいは回避する

図表1 第1種と第2種の誤謬



出典：http://www.ipa.go.jp/security/fy15/reports/biometrics/documents/biometrics2003.pdf

技術が、別のリスクの種になることも考えられる。こうした新技術に対して、庶民感情として「漠然とした不安」があることは、むしろ健全な発想をしている人が多いことの証左かもしれない。

ディレンマの５：直接の被害者がいない場合が多い

最後に、情報セキュリティが他のセキュリティと違う点として、直接の被害者がいない場合が多いことを付加しておこう。情報セキュリティでも、被害者が存在し実害が発生することもある（例えば、営業秘密の漏洩）。しかし、スパム・メールや「いわゆる有害コンテンツ」[10]の拡大のように、社会全体としては損失を被っているのだが、個々の損害については僅少であるか把握しにくいため、対策が打ちにくいものが多い。

直接の被害者がいれば、被害者からの請求によって犯罪捜査や訴訟が開始されるなど、現存する社会制度を使って問題点が摘出され、しかるべき解決に導かれることが多い。しかし、被害者が特定されない場合や、母集団としては特定されても被害が広く薄く分布している場合には、問題が注目を集めないまま忘れられていく可能性が高い。どうやら情報セキュリティ・インシデントには、こうした傾向が避けられないようである。

ベスト・エフォート

このようなディレンマの中では、「セキュリティを維持するのは至難の業」という諦めも生じそうだ。現象の大部分は非線形で、しかも均衡がどこにあるか、それが単数なのか複数なのかも分からないことが多い。それに対して私たちが用いてきた手段は、主として線形的・要素還元的なもので、それでは捉えきれない事象がいくらでもある。

しかし世の中は不思議なもので、私たちが理論化できない、あるいはメカニズムが分からないということが、即「無秩序」を意味する訳ではない。複雑系の研究者たちが、一見秩序が無いかに見える事象の中から、自生的な秩序が生まれる「自己組織化」という現象を見出し[11]、インターネットが、その具体例であることが知られるようになった。

インターネットは元々、核戦争の下で多数ある戦略拠点が破壊されても、生き残った拠点間をつなぐことが可能な、ネットワークのトポロジー開発を目指していた。そのためにパケットという技術が考案され、宛先のアドレスだけを頼りに、なんとか目的地に到達することを最優先にしている。インターネットはやがて、大学間の超高速ネットワークへと変質し、折からのヒッピー文化とも相まって、政府から干渉されない「ネットワークのネットワーク」へと進化した（西垣（編著訳）[1997]）。

その思想は、従来の事前計画型のネットワークとは違って、全体を管理している人や組織はないし、ルート別に計画が立てられる訳でもないという点に端的に表れている[12]。IPアドレスという希少資源の割り当ては必要であるが、TCP/IPという標準に従ってネットワーク接続を果たせば、後は管理不要である。1990年代半ばの商用化後も、この構造は変わっていない。

インターネットでは、転送者がパケット化された元の情報をそのまま次のノードに転送するだけで、伝送品質や伝送速度を制御したり、誤りを正すことなどは期待されていない。従来のネットワークでは、通信事業者がこうした品質保証を行なっていた（そのためギャランティ型という）が、インターネットでは「できるだけの努力」をすれば良い（ベスト・エフォート型）として、中継者の負担やネットワークの重装備を軽減している[13]。

本来なら「重装備」「ギャランティ型」のレガシー・ネッ

トワークの方が堅牢で、「軽装備」で「ベスト・エフォート型」のインターネットは、信頼性に欠けると思われるかもしれない。ところが、2011年の東日本大震災においても、インターネットの方が生き残った部分が多かったのである[14]。

このように、時代は明らかに「ベスト・エフォート型」が中心になりつつある。情報セキュリティについては、元々「100％保証」の対策は無いのだから、「ベスト・エフォート型情報セキュリティ」が全てで、「保証型」は存在しないのかもしれない 。私たちは、インターネットがもたらした変化を、もう一度見つめ直す必要がありそうだ[15]。

「防止」から「耐性と復元」へ

かつての通信やコンピュータ・ネットワークにおける非常時対策は、ハードを中心にして二重・三重の備えをすることで、ProtectionとPreventionの二つのPが中心であった。当時の技術では、これには相当なコストがかかるので、redundancyという語が「冗長度」と訳され、「ムダ」だが「やらざるを得ない」ものと考えられていた。

しかし、その後コンピュータは「ムーアの法則」[16]で急速に安くなり、通信ネットワークも光ファイバとデジタル無線技術の進展によって、これに匹敵するほどコストが低下し、これまで貴重品であったコンピュータ・パワーと通信容量が日用品となった。またパケット通信が、ルーティングの柔軟化をもたらした。従来の回線交換では、特定の回線を物理的に一時占有せざるを得ないが、パケット通信では「バケツ・リレー式」に伝送するので接続はバーチャルになり、どのルートをたどっても宛先に届けることが出来る。

そうなると、ネットワークの事前完全防備を志すよりも、防備はある程度に抑える一方で、いざというときに全部機能が止まるのではなく、ある部分はインシデントに耐えて生き残り、かつ早期に復旧可能な方式が好まれる[17]。つまり「事前対応」（前述の二つのP）から「事後対応」の二つのR（ResponseとResilience）へと重点がシフトしつつある。しかも二つのRのうち、とりわけ後者がキーだと思われる。

レジリエンスは、アメリカの重要インフラ保護の基本概念になったばかりか（Homeland Security Advisory Council［2006］、Homeland Security Studies and Analysis Institute［2009］）、ダボスのWorld Economic

Forumでも注目されている（World Economic Forum［2012］）。私はこの語を「しなやかでしたたかな耐性と復元力」と訳したい。

今回の大震災においても、これに類する対応が見られた。日米間のインターネット回線については海底ケーブルの迂回路が有効だったし、携帯には衛星サービス、ウェブにはミラー・サイトが、ツイッターにはクラウド･サービスという支えがあった。要は、通信チャネルが「アバンダント」になった恩恵を享受できたのである。

1969年という早い時期に、林雄二郎氏等が「情報化社会」という新しい概念を提唱した際、その特色の一つとして「redundancy を見直す」と主張していたことが思い出される（林（雄）［1969］）。東日本大震災の教訓は、工業化社会の効率一辺倒を見直して、Just-in-Timeも良いが「ゆとり社会」も悪くないと、考え方を少し変えることかもしれない[18]。

間違えるは人の常

情報セキュリティが単なる技術問題ではなく社会問題でもある以上、人間行動を理解しないと、現象の一部しか理解していないことになってしまう[19]。そこで基本となるのは、「間違えることは避けられない」という認識であろう。細心の注意を払わねばならない立場の人でさえ、時として「うっかりミス」を犯す。

この点で「To Err is Human.」という報告書（Corrigan et al.［2000］）は示唆に富んでいる。これは、アメリカにおいて医療事故の解明に取り組んだ特別委員会の報告書であり、タイトルの「間違えるは人の常」という認識が、あらゆる事故対策の基本であるという強い注意喚起である。

単純ミスではなく、より根源的な「価値判断」を誤ったときの影響は更に大きい。特に、個人の判断と組織の利害が対立したとき、どのような調和を見いだし得るかは、はなはだ心もとない。我が国の企業社会にあっては、個人がカイシャの中に埋没して、独自の判断を回避してきた（回避せざるを得なかった）感がある。「性善説」でも「性悪説」でもない、「性弱説」を唱える向きがあるのは、このような「弱い社員像」と結び付いている[20]。

企業不祥事のケースでは、非違行為の存在が内部では知られていたのに、これが表面化することなく、長い年月が過ぎ去ることが多い。個人としては良識を持っ

ている人も、組織に属すると企業の論理に屈してしまうからであろう。しかし、独占禁止法違反の課徴金について導入された「リニエンシー制度」は[21]、実効性が疑われていたにもかかわらず、意外に機能している。このことから見ても、「誤りを正すに躊躇すべからず」という鉄則は、少しずつだが、確固たるカイシャ社会にも浸透しつつあるようだ[22]。

許すが忘れない

ところで、我々日本人はレジリエンスのような発想に馴染みが薄いようである。責任を追及する際、「厳罰主義」に走るか「寛容主義」に行くか二者択一に近く、前者は「あだ討ち・腹切り」を求め、後者は「水に流す」。しかも、「本音と建前」を使い分けて、「喉元過ぎれば熱さを忘れる」ことに期待しようとする。

そこで頭の体操をしてみよう。ある非違行為があったとして、これを許す（Forgive）か許さない（Never Forgive）か、忘れる（Forget）か忘れない（Never Forget）か、の2次元で考えるとする。F-F、F-NF、NF-F、NF-NFの四つの組み合わせができるが、情報セキュリティに適切な解はどれだろうか？

Forgive-Forget（許して忘れる≒水に流す）では経験が蓄積されないし、Never Forgive-Never Forget（許さないし忘れない≒あだ討ち・腹切り）は「間違える」動物には厳格すぎる。そこで、我が国で広く観察されるのは、誰かをスケープゴートにして「無かったことにする」仕組み、すなわちNever Forgive -Forget（許さないが忘れる）である。これは本来論理矛盾であるが、日本の組織では定型化している観さえある。

図表2 Forgive-Forget Matrix

	Forget	Never Forget
Forgive	水に流す	失敗学
Never Forgive	無かったことにする（論理矛盾）	あだ討ち・腹切り

私の経験では、Forgive-Never Forgetつまり「許すが忘れない」が最適で、それ以外の解はないと思われるが、この語は日本語の辞書になかったようで、失敗学（畑村［2000］）の新鮮さもそこにある[23]。私たちは、長期的な責任よりも「即効性のある責任」（例えば社長の辞任）を追及する傾向があり、冷厳な事実を見つめ続け「再発防止策」を講ずることが苦手なようである。マスメディアも今関心のあるテーマに群がり、10年間同じテーマを追いかけることはまれである。これは依然として、PreventionとProtectionの二つのPにこだわっており、Resilienceの大切さに気付いていない状態かと思われる。

しかし、少なくとも情報セキュリティについては、即効性よりも、事後類似の事件が起こらないようにすることの方が肝要で、「許すが忘れない」をデフォルト化することが必要だと思う。そして再発防止には、事故情報をデータベース化して、その後の備えをしておくことが必要である。検索技術が発達したので、データベースさえあれば、データを発掘し「過去に学ぶ」ことができるが、こうした「情報開示」の面でも我が国の課題は多い[24]。

［付記］

本稿は、以下の拙文の要点をまとめることを志したものであるが、「係長セキュリティから社長セキュリティへ」、「グローバル経営と情報セキュリティ」、「日本的組織風土と情報セキュリティ」といった視点は、紙幅の関係上割愛せざるを得なかった。関心を持たれた方は、直接以下の論文等に当たっていただけると幸いである。

・拙稿［2007］「『人間は間違える』ことを科学する」『Economic Review』Vol.11, No.4 富士通総研
・拙稿［2009］「巻頭言：セキュリタイゼーションとセキュリティ」『金融情報システム』No. 303（平成21年夏号）
・拙稿［2010］「係長セキュリティから社長セキュリティへ：日本的経営と情報セキュリティ」情報セキュリティ大学院大学紀要『情報セキュリティ総合科学』第2号
・拙稿［2011］「法学的アプローチ」松浦幹太（編著）『セキュリティマネジメント学』共立出版
・林紘一郎・田川義博・淺井達雄［2011］『セキュリティ経営』勁草書房

Koichiro Hayashi
林 紘一郎

情報セキュリティ大学院大学 教授
東京大学法学部卒業。日本電信電話公社（当時）入社後、NTTアメリカ社長（本社役員待遇）、Nextel（現Sprint-Nextel）社取締役などを歴任。慶應義塾大学メディア・コミュニケーション研究所教授を経て2004年4月より情報セキュリティ大学院大学副学長・教授。2009年4月から2012年3月まで同学長。現在、同教授。経済学博士（京都大学）。博士（法学、慶應義塾大学）。主な著書：『セキュリティ経営』（田川義博・淺井達雄氏との共著、勁草書房、2011年）、『引用する極意・引用される極意』（名和小太郎氏と共著、勁草書房、2009年）.『倫理と法ー情報社会のリテラシー』（矢野直明氏と共著、産業図書、2008年）など。

補注

1）政治学や国際関係論の分野では、「国王に権力を集中するとナショナル・セキュリティは高まるが、基本的人権の面でのセキュリティは低下する」ことをもって、セキュリティのディレンマと呼んでいたようである（土屋［2000］）。
2）否定的な定義しかできない状態は、少なくとも学問的な対象の確定に至っていないことと近似である。私のNTTでの経験でも、電話の次に出現するサービスについて「非電話系」と呼んでいた時代には、現在のインターネット・サービスの概念をつかみきれていなかった。
3）かつて大阪ガスの常務であった永田秀昭氏は、社内の保全部門の業績評価として「損失を回避したことを数量化して表彰する」という制度を設けて成功したが、このような事例はまれであろう（永田［2004］）。
4）厳密に言えば、アルフレッド・ノーベル記念スウェーデン国立銀行賞で、ノーベル賞と同格に扱うことに反対する意見もある。なお「プロスペクト理論」はトベルスキーとの共同研究から生まれた概念だが、同氏は既に故人であったため、ノーベル賞は受賞できなかった。
5）スパム・フィルターを入れても後述の二つの誤謬は避けられないから、最終的には受信者が受信メール全体をチェックせざるを得ない。
6）このことは、インターネットの特質とされる「信頼の原則」「問題先送りの原則」に遠因がある、という見方もある（ジットレイン［2009］）。
7）法学の世界も同様で、古くから「例外のない規則はない」という法諺（ほうげん）があったにもかかわらず、原則論の追求に集中してきた嫌いがあった。
8）副作用ゼロの薬は、文字通り「毒にも薬にもならない」。
9）私たちの世代はDDTに対して、シラミなどの防虫剤としてプラスのイメージを持っていたが、1980年代以降発がん性があるとして使用禁止になった。
10）世間では有害コンテンツという言葉が氾濫しているが、それが「青少年にとって有害」なものを意味するなら、そのように表記すべきである。さもないと違法コンテンツとの差がなくなり、憲法で保障された「言論の自由」に悪影響を及ぼす。私は一貫して「いわゆる有害コンテンツ」と表記している。
11）カオス理論やフラクタル現象として、目に見える形でその存在を明らかにした。
12）インターネットの父の一人と言われるカーンが提起した原則は、①個々のネットワークが自己責任でインターネットに接続する際、何らの変更を要さない、②通信はベスト・エフォートの原理に基づく、③通信を媒介するルーターは単に交換するだけで、パケットの中身にタッチしない、④運営をコントロール

する仕組みは不要である、というものであったとされる（クラーク［2011］）。
13）もっとも、このような説明は「通信屋」のもので、「システム屋」からすれば、「ソフトにバグが付き物のように、ベスト・エフォートが全て」ということかもしれない。両者のメンタリティの違いについては、坂井［2012］参照。
14）もちろん、利用者宅から基地局までの加入者線や無線接続が切れれば、インターネットも使えなくなったが。
15）インテリジェンスの担当者が、こうした考えを受け入れることができないのは、当然とも言える。アメリカで歴代大統領の顧問を勤めたクラークは、インターネットに五つの内在的脆弱性があるというが、その彼でも有効な対抗策を提示できない（クラーク［2011］）。
16）コンピュータの心臓部ともいうべき半導体チップの価格が、1年半ないし2年で半分になるという経験則。インテルの創業者の一人であるゴードン・ムーアが言い出したので、このように呼ばれる。
17）コンピュータの世界で、fail safe という概念がかなり早くから提唱されていたが、これがネットワークをも包摂した概念になったのが、resilienceと考えることもできる。
18）もっとも金融が中心の社会になると、産業社会のような物理的制約がない分、行動の自由が広がり、バブルとバブル崩壊を繰り返す危険も高まる。この辺りの按配（あんばい）は、未だ人類が習熟していない領域に属する。
19）ただし人間を考察する学問は、事物を観察する学問に比べれば科学としての展開が遅く、また観察者と被観察者がともに人間であることから、常に客観性についての検証を必要とする。実験に適さないケースもあり、再現性に乏しい場合もあり、ある情報を与えるとそれが事後の行動に影響を与えることもある。
20）学問の世界でも遅ればせながら、このような事象を分析し始めている。その中間的成果が「組織的逸脱行為」という概念である（本間［2007］など）。
21）違反行為について、最初に通報した企業には課徴金を免除するなどの特典を与える制度。
22）もっとも「公益通報者保護法」の実態は、期待外れとの声もある。
23）一時バズワードになった「想定外」も、我が国では、「忘れて良いもの」に近いニュアンスを持っているが、これに該当するresidual riskは「さしむき対策外とするが、消し去ることのできないリスク」という意味である。ここにも「忘れない」ことの大切さが浮き彫りになっている。
24）アメリカでは「税金で集めた情報は納税者のもの」という意識が強く、CIAの情報でさえ時間が経てば開示されるため、その後のセキュリティ対策に役立つ場面がある。一方我が国では、政府の情報はもちろん、企業の情報も、「永久保存」（その実、永久に謎）になっていることが多い。東日本大震災関係の行政行為も、議事録がないことで済ませてしまう国と、1年を経ずしてNRC（米原子力規制委員会）の膨大な記録を公開する国では、危機管理能力に圧倒的な差が出るのは必定である。

参考文献

クラーク,リチャード（北川知子・峯村利哉訳）［2011］『世界サイバー戦争』徳間書店。原著は、Clarke, Richard A., with Robert K. Knake［2010］"Cyber War," HaperCollins
坂井修一［2012］『ITが守る、ITを守る：天災・人災と情報技術』NHK出版
ジットレイン, ジョナサン（井口耕二訳）［2009］『インターネットが死ぬ日』早川書房。原著は、Zittrain, Jonathan［2008］"The Future of the Internet, and How to Stop It," Yale University Press
土屋実男［2000］「セキュリティ・ディレンマ」『政治学辞典』弘文堂
永田秀昭（監修）・大阪ガス実践的MOT研究会［2004］『技術者発想を捨てろ！―実践的MOTでキャリアが変わる』ダイヤモンド社
西垣通（編著訳）［1997］『思想としてのパソコン』NTT出版
畑村洋太郎［2000］『失敗学のすすめ』講談社
林雄二郎［1969］『情報化社会―ハードな社会からソフトな社会へ』講談社
本間道子［2007］『組織性逸脱行為過程―社会心理学的視点から』多賀出版
Corrigan, Janet et al.［2000］"To Err is Human―Building a Safer Health System," National Academies Press
Homeland Security Advisory Council［2006］'Report of the Critical Infrastructure Task Force'
Homeland Security Studies and Analysis Institute［2009］'Risk Analysis and Intelligence Communities Collaborative Framework, Final Report'
World Economic Forum［2012］'Partnering for Cyber Resilience: Risk and Responsibility in a Hyperconnected World'

情報セキュリティ2

緊急事態と情報セキュリティ政策

情報セキュリティ大学院大学 情報セキュリティ研究科 教授

湯淺 墾道 Harumichi Yuasa

現行の日本の緊急事態に関する法制度には、災害対策基本法における「災害緊急事態」と
原子力災害対策特別措置法における「原子力緊急事態」という２種類が存在する。
両者は、共に内閣総理大臣に相当に強力な権限を与えるものであるが、
3.11の東日本大震災の後に採用されたのは、首相が行政機関、地方自治体の組織を経由しつつも
「指示」という形で直接強い命令権を持つ後者であった。
このような緊急権について、日本の憲法学界は一般に否定的であったが、
個人による嫌がらせや愉快犯的な次元を越えた多様な手段・態様による国際的なサイバー攻撃が多発する現在、
緊急時の情報セキュリティの確保に関する法制度を検討するべき時期にきている。

キーワード
災害対策基本法　原子力災害対策特別措置法　緊急事態宣言　国家緊急権

1. はじめに

本稿執筆の時点で、2011年3月11日の東日本大震災からちょうど1年が経過しようとしている。

当初、東日本地域で発生した大規模な地震とその後に襲来した津波の影響は、他の地域では被災地を中心とした地域に限定されるものと認識されていたかもしれない。しかし、各地の原子力発電所の運転停止により全国的に節電が求められ、企業活動や人々の生活に大きな影響を与えた。近時の報道によれば、福島第一原子力発電所の事態の収束に失敗した場合、首都圏の3000万人の住民が避難せざるを得なくなるという「最悪シナリオ」すら政府に存在していたという。その意味で、東日本大震災は、局地的大災害という次元を越えた戦後日本最大の緊急事態であったと考えられる。

このような動きを受けてか、自由民主党の憲法改正推進本部が2012年3月2日の役員会で了承した憲法改正原案では、現行憲法には無い武力攻撃や大規模自然

災害に対処する「緊急事態条項」も新設されたとのことである。

ところで、現行の日本の法制度においても、2種類の「緊急事態」が用意されていることは、案外と知られていない。本稿では、まずこの2種類の緊急事態について内容を概観した後で、緊急事態が実際に発生した場合において求められる情報セキュリティ政策の方向について検討してみることにしたい。

2. 日本の緊急事態法制

災害対策基本法

1961年に制定された災害対策基本法は、全国で死者4697人、行方不明401人、浸水36万戸という大被害を与えた1959年の伊勢湾台風を契機として、それまでに応急的に制定されていた災害関係の法律を整理し、災害対策の基本を定めたものである。災害に関係する法律は非常に多く、基本法グループ、災害予防関係法グループ、災害応急対策法グループ、組織法グループ、災害事後対応・復旧法グループに整理されるが[1]、災害対策基本法はこれらの中で最も基本となる。

災害対策基本法105条によれば、非常災害が国の経済及び公共の福祉に重大な影響を及ぼす異常かつ激甚なものである場合、内閣総理大臣は「災害緊急事態」の布告を発することができる。災害緊急事態の布告が行われると、緊急災害対策本部の設置（107条）、一定の緊急措置を行うための政令の制定権限（109条1項）、他の法律の規定によって海外からの支援を緊急かつ円滑に受け入れることができない場合に必要な措置をとる政令の制定権限（109条の2）が可能になる。特に、緊急措置政令を制定することによって、生活必需物資の配給等の制限（流通・販売の統制）、災害復旧または生活に必要な物品・役務の物価統制、金銭債務の猶予等を実施することが緊急措置として可能になるので、これは相当に強力な権限である。

では、なぜ今回は災害緊急事態の布告が行われなかったのか。国会では小滝晃・内閣府参事官が「政令の布告は国会閉会中に限られること（今回は国会開会中だった）、国民の権利義務を大きく規制する非常に強い措置で適切な判断が必要である」と理由を答弁したが、恐らく理由は別のところにもあるだろう。その一つが、原子力災害対策特別措置法における「原子力緊急事態」である。

原子力災害対策特別措置法

原子力災害対策特別措置法は、1999年に起きたJCO臨界事故の教訓などから、原子力災害対策を強化するために1999年に制定された。特殊な危険性をもたらす原子力災害の性質にかんがみて、迅速な初期動作の確保、国と地方公共団体の有機的な連携の確保、国の緊急時対応体制の強化、原子力事業者の責務を定めている他、15条2項では、原子力緊急事態が発生したと認められるときは、主務大臣の報告を受けて内閣総理大臣は原子力緊急事態が発生した旨、及び原子力緊急事態宣言の公示を行うとしている。

原子力緊急事態が公示されると、対象地域を管轄する市町村長及び都道府県知事に対し、内閣総理大臣は、避難のための立ち退きや屋内への退避についての勧告または指示を行う。今回は3月11日に原子力緊急事態が公示されたので、福島原発の周辺地域の住民への避難指示や、立ち入り禁止の措置は、この権限に基づいているわけである。さらに、その他の緊急事態応急対策に関する事項についても対象地域を管轄する市町村長及び都道府県知事に指示するとされている。

また、原子力緊急事態宣言をしたときは、内閣府に首相を長とする原子力災害対策本部を設ける。原子力災害対策本部長は、主務大臣に対し、必要な命令をするよう指示することができるとされている。野菜の出

荷制限や摂取制限は、この権限に基づいて行われた。

二つの法律の違い

災害対策基本法に基づく災害緊急事態も、原子力災害対策特別措置法に基づく原子力緊急事態も、どちらも相当に強力な効果を持つ。それでは、今回はなぜ政府は後者を選択したのであろうか。

それには多くの理由があると考えられるが[2]、一つには原子力災害対策特別措置法が既存の行政組織を活用しつつ、直接的に強力な権限を首相に与えているからだろう。

災害対策基本法に基づく政令の布告は、国会開会中はできないことになっており、閉会中の場合は事後に国会の承認が必要である。また、日本の緊急事態法制の特色として、緊急事態とは何かの定義を欠き、個別の法律に対応すべき領域が明示されているに過ぎないこと、緊急時と平時とで行政の権限の区別が行われていないことが指摘されている[3]。緊急時における行政のマニュアルとなるべく策定された「南関東地域震災応急対策活動要領」においてもそれは顕著で、緊急時における対応は、行政が民間事業者等に要請して「協力」を得ることが基本となっている。一般の災害による緊急事態法制は、できるだけ平常時の枠組みで事態への対処を行おうとしているように見える。

これに比べると、原子力災害対策特別措置法では、首相は原子力災害対策特別措置法による権限を国会の関与なしに行使できる。その上、「内閣総理大臣は（中略）市町村長及び都道府県知事に対し、（中略）事項を指示するものとする。」とか、「主務大臣に対し、（中略）必要な命令をするよう指示することができる。」、「関係指定行政機関の長及び関係指定地方行政機関の長並びに前条の規定により権限を委任された当該指定行政機関の職員及び当該指定地方行政機関の職員、地方公共団体の長その他の執行機関、指定公共機関及び指定地方公共機関並びに原子力事業者に対し、必要な指示をすることができる。」として、首相が行政機関、地方自治体、電力会社等に対して「指示」という形で直接命令権を持つ構造になっている。

とかくリーダーシップの不在やトップダウン型の意思決定の欠如が指摘される日本の行政ではあるが、実際には、原子力緊急事態に限っていえば、首相には全権が集まっており、リーダーシップが発揮できるような仕組みにはなっているのである。ただし、これはあくまで既存の縦割り組織を活用することが前提になっているから、そのラインでは有効に機能するが、組織縦断的な対応が必要とされる場面では原子力災害対策本部長である首相がすべて調整しなければならないことになっており、実際には機能しない。例えば人が食べ物や水の摂取を通じて取り込んでしまう放射能の問題については、畑や田んぼに植えられている段階では農林水産省だが、それが食品になると厚生労働省、一級河川の水は国土交通省だが水道として供給されると

きは自治体という具合である。

この相違が、アンバランスな事態を生んでいると思われる。大津波で大きな被害を受けた地域では、流されてきた持ち主不明の自動車の残骸の所有権を尊重しなければならないというので、処分もままならない。そうかと思えば、福島原発の周辺地域では周辺住民はいまだに家に戻ることもできず、かつ家屋や土地の所有権や平穏な生活を送る権利がこれだけ侵害されたというのに、その私権を強く制限したままで救済・損害賠償が遅々として進まない。日本に緊急事態法制を本格的に導入するとすれば、この二つの緊急事態法制の相違点について、その効果と問題点を詳細に比較検討する必要があるだろう。

3. 緊急事態と情報パニック

今回の東日本大震災とその後の福島原発の事故の際にも、政府が多くの「情報隠し」を行っていたことが明らかになってきている。公的な意思決定の場（かつ、相当程度に重大な意思決定を行った場所）において議事録が作成されていなかったり、前述したような最悪のシナリオを無かったことにしたりというのは、その一例であろう。

このような情報隠しについて、当事者の間から異口同音に釈明の言葉として聞かれるのは「パニックを起こす恐れがあった」「混乱をもたらす恐れがあった」というものである。

確かに、行政には一般的にパニックを防止する責任が無いとはいえない。この点では、政府・自治体側の言い分もわからないではない。緊急事態におけるパニックは、古くは関東大震災のときの例があり、最近では2001年に発生した明石花火大会歩道橋事故（歩道橋の上で花火見物の客の群衆雪崩が発生して11名が亡くなるという痛ましい事故）があった。この事故は、民事訴訟においては自治体、警察、警備業者の責任を認める損害賠償訴訟の判決が確定しており[4]、刑事訴訟においては当時の警察署の副署長を被告とする訴訟が継続中である。

しかし、今回の東日本大震災と福島原発に関する政府の情報発信については、皮肉な結果になったといえる。東日本大震災（東北地方太平洋沖地震）を契機として、各種のソーシャルメディアが行政の広報広聴手段として高く評価されるようになり、特に震災の後には自治体の利用が増えた。しかし、ソーシャルメディアにおける情報に対する人々の信頼度は、誰からの発信かという点に大きく依存するといわれる[5]。市民が情報の信頼性を判断する際に「主に見ているのは、情報の中身ではない。見られているのは『発信者が信頼に値するかどうかである』」という[6]。野村総合研究所が実施した「震災に伴うメディア接触動向に関する調査」によると、発信者の身元が政府・自治体であることが明確であったものは、逆に国民に信頼されなかったこ

とが明らかになっている[7]。「原子炉そのものであることは確認されていないが、何らかの爆発的事象であると報告されている」（2011年3月12日枝野官房長官の記者会見発言）とか、「今回検出された放射性物質濃度のホウレンソウを摂取し続けたからといって、直ちに健康に影響を及ぼすものとは考えられない」（2011年3月20日同）などという説明も、事態をある意味で正確に伝えているのかもしれないが、何かを隠すために曖昧に言っているのではないかという疑いを招くだけであった。国民は、政府・自治体が発信する情報だからこそ、信頼に値しないと考えるようになったであろう。

情報隠しによってパニックを防止することはできたかもしれないが、政府や政権与党は国民からの信頼を失った。政府・行政への信頼感の喪失は、直接的な国民の権利侵害は発生させないかもしれないが、国家の体制全体の危機をもたらす。このことはファシズムの勃興という歴史が教えているし、現在も多くの先進民主主義諸国においては既存政党・既成政治権力への不信が政治の混迷をもたらしている。それと引き替えにしてまで、情報パニックは絶対に防止されなければならないのだろうか。むしろ、ある程度のパニックの発生を想定し、それをコントロールする手法を導入すること、それに関する行政責任の一定の免責を検討することが求められているのではあるまいか。

4. 緊急事態と情報セキュリティ政策

日本国憲法と緊急事態

緊急事態の情報セキュリティ政策について検討する場合、避けて通ることができないのは、サイバー攻撃を受けて重要インフラが機能しなくなるような状態に陥ることを防止する対策である。この問題は、サイバー戦争や有事法制の議論に結びつきやすいが、冷静な議論をすべき時期がきているようである。

憲法学の研究者の間では、従来、「緊急事態」という観念を導入することには一般に否定的であった。

立憲主義的な憲法秩序において、外敵の侵入、内乱、激甚な災害等が発生して平常の手段をもっては対処し得ないような緊急事態が発生し、それによって国家の存立そのものが脅かされたとする。このとき、国家はこれに対処して憲法秩序それ自体を維持するために、非常例外的な手段によって対処することがある。近代憲法は基本的人権の保障とそれを確保するための権力分立を構成要素としているが、一方で憲法によって基本的人権を保障するには立憲主義的体制自体が維持される必要があるので、憲法秩序それ自体が破壊されるような事態に至った場合は、憲法による人権の保障を実現するために憲法秩序それ自体を維持しなければならない。

そこで、緊急事態に関して何らかの措置を設け、憲

法自らの存立を保障する仕組みが必要である。これを憲法保障というが、それには国家が存立していなければならないとして、行政権に権力を集中し財産権や表現の自由などの人権を制約して国家を護(まも)る非常例外的な手段をとる権利を国家に与えるものが緊急権である。他方で、国民自らが憲法秩序を破壊するものに抵抗し、憲法秩序を維持・防衛・回復する権利を抵抗権という。

日本国憲法は、緊急事態や緊急権、抵抗権に関する明文規定を欠く。このことから、緊急権そのものを否定する立場と、逆にそれを憲法の欠陥・欠缺(けんけつ)として消極的に評価する立場に分かれることになる。また中間的なものとしては、緊急権そのものは理論的に「不文の法理」として肯定しつつも、それを具体的に発動するための立法については慎重な見解をとり、緊急権を謙抑的に理解しようとする立場もある[8]。

戦後の日本の憲法学における緊急権に関する議論の特色は、本来は憲法保障の一つであり抵抗権と表裏一体に語られるはずの緊急権が、抵抗権よりも憲法9条との関係において議論の対象となり、緊急権を認める立法がいわゆる有事立法と同義のものとしてとらえられることが多かったという点である。このため、憲法保障の一つとしての理論的次元における国家の緊急権に関する議論を行おうとする場合にも、「有事」に踏み込む射程を持っている限り、9条の問題を意識せざるを得ない。逆にいわゆる有事法制に関する議論においては、文面上は徹底した平和主義を採用していると解される日本国憲法の原理を純粋に尊重しようとして、外国からの武力攻撃やテロ等によるわが国の立憲体制に対する挑戦があり得るという想定自体を排除しがちになった。

ところが、有事立法へのアレルギーがもっぱら再軍備への危惧から発生しているとしても、「憲法が停止される」事態、または社会経済が大きな影響を受けて大混乱に陥るような事態は、戦争だけによって引き起こされるとは限らない。国家緊急権は一般に「戦争・内乱・恐慌・大規模な自然災害など、平時の統治機構をもっては対処できない非常事態において、国家の存立を維持するために、国家権力が立憲的な憲法秩序を一時停止して非常措置をとる権限」[9]として理解されている。換言すれば、本来、国家緊急権は戦争や内乱の場合に限って発動されることを想定されているものではない。3月11日のような事態が発生した場合にはどのように国家が緊急権限を行使することができるのかについては、もっと論じられてもよかったはずなのである。

にもかかわらず、国家緊急権の問題が9条との関係でだけ論じられてきたのは、要するに、緊急時の枠組みを厳格に定義しようとすることは不可能に近いが、だからといって緊急権の発動が許されるような事態を正確に定義しないで一般的抽象的に緊急権を肯定することは、緊急事態の予防という観点から緊急事態法制が逆に平常時の法制の中に侵入してくる可能性を生み、緊急権がかえって憲法保障の機能そのものをないがし

ろにする恐れがあるという懸念を憲法学者が共有していたからだろう。

サイバー攻撃への対処

2011年5月、アメリカ政府のホワイトハウス及び国防総省は、それぞれ「サイバー空間国際戦略（International Strategy for Cyberspace）」[10]、「サイバー空間作戦戦略（Department of Defense Strategy for Operating in Cyberspace）」[11]を公表した。

前者は、アメリカ政府のサイバー空間の運営・防護・利用に関する包括的な政策パッケージを提言するものであり、後者は、前者を受けて国防面での具体的な戦略を明らかにしたものである。国防総省のサイバー空間作戦戦略としては初めて公表されたものであるが、サイバー空間における敵対行為に対する自衛権及び軍事力行使の可能性を表明したものとして多くのメディアから注目された。

上記のアメリカ政府の政策においては、サイバー空間国際戦略では、国家の固有の権利である自衛権は、国連憲章を遵守（じゅんしゅ）する限りにおいてサイバー空間に対しても適用されるので、国家はサイバー空間において自衛のための軍事力を展開する権利を有するとしている。それは、新たな法的規範の定立に関する理論の構築を必要とするものではなく、伝統的な国家の自衛権と同様にサイバー空間における自衛権も「固有の（inherent）」ものであり、「サイバー空間における国家の役割を支持する既存の原則」の中に含まれるという。その一方で、サイバー空間国際戦略では国防の領域で優先されるべき政策を掲げており、その中には「集団安全保障の強化のために、同盟国及びパートナーとのサイバー空間における協力を拡大すること」という一文も含まれる。日本も今後アメリカから「サイバー空間における協力」を求められるであろうことは、ほぼ確実である。

個人による嫌がらせや、愉快犯的な次元を越えた多様な手段・態様による国際的なサイバー攻撃（それをAPT、サイバー戦争、サイバーテロ、それとも単なる脅威・攻撃と呼ぶかはさておくとして）が頻繁に発生するようになっているのは事実であり、これらのサイバー攻撃によって日本の社会システムが現実に大きな被害を受ける恐れが顕在化している。

しかしここでは、我々は大きなジレンマに直面している。サイバー攻撃を「武力」の行使としてとらえるならば、それへの対処は憲法9条や伝統的な戦争に関する国際法の制約を受ける。「武力」の行使ではなく、単なる犯罪行為や違法行為としてとらえるのであれば、それへの対処は自衛権の行使とはいえないから、通常の法律の枠内でこちら側が違法にならない程度に行うしかない。サイバー攻撃への対処のために、通常の法律では違法と評価され得る行為を特に行う場合、それが違法とならないようにするには、その正当性が問われることになるが、その正当性の根拠は最終的には自衛権の行使に行き着いてしまう。

ここで思い出されるのは、インターネットの利用が急速に進むようになった1990年代にアメリカの法律学者の間で争われた「馬の法律」論争（インターネット上のサイバー空間という新たに現れた領域において法秩序を実現するためには、この領域を規律・統制する新たな法規範が必要とされるかどうかの論争）であった。上記のジレンマを解消するためには、サイバー空間という新たな領域に関する緊急事態の法体系を構築するしかないのであろうか。

サイバー空間を管理するために、既存の法体系に代わる新たな法体系を探求することは重要であり、構想を具体化していくことが求められているかもしれない。しかし現時点においては、サイバー攻撃への対処やサイバー攻撃によって重要インフラ等が大きな被害を受けて経済社会が大きな混乱に陥ったときの情報セキュ

リティの確保については、対処策や緊急セキュリティ対策の具体的な技術的形態・運用的形態に即し、刑法や不正アクセスの防止に関する法律その他の情報セキュリティに関する法律が規制・禁止している事項に抵触しないかどうか、構成要件に該当している場合はどのように違法性を阻却するかについて、想定され得る事例や事案を精査し、法的に検討することの方が先決であるように思われる*。

さらに、既存の法体系に代わる緊急事態法制を導入するとすれば、災害対策基本法と原子力災害対策特別措置法という二つの既存の緊急事態法制の比較を通じて、どちらの型の緊急事態法制の方が緊急時には有用であるのか、あるいはどちらでもない全く新しい緊急事態法制を構想すべきであるのかを冷静に検証することから始めるべきであろう。

Harumichi Yuasa

湯淺 墾道

情報セキュリティ大学院大学 情報セキュリティ研究科 教授

青山学院大学法学部卒業、慶應義塾大学大学院法学研究科政治学専攻博士課程退学。九州国際大学法学部専任講師、准教授、教授、副学長を経て2011年4月から現職。2012年4月から学長補佐併任。九州大学、中央大学、横浜市立大学、愛知学院大学、神奈川工科大学非常勤講師。著書に『電子化社会の政治と制度』（オブアワーズ、2006年3月）、共編著『憲法学へのいざない（第2版）』（青林書院、2012年3月）など。論文に「電子投票法制の近時の動向」『情報ネットワークロー・レビュー』10巻（2011年）、「自治体における個人情報保護 ―定額給付金・子育て応援特別手当の給付事務を中心に―」『九州国際大学社会文化研究所紀要』64号（2009年）、「被選挙権の法的性質をめぐる近時の議論」日本選挙学会年報『選挙研究』24巻2号（2009年）など。

補注

＊この点において、日本はアメリカよりも相当の後れを取っていることは否めない。しかしそのような法的な観点からの検討は各方面で始まりつつあり、例えば海上自衛隊幹部学校では、その成果をとりまとめ、紀要『海幹校戦略研究』などで公開する予定であるという。http://www.mod.go.jp/msdf/navcol/SSG/SSG.html

引用文献

1）野口貴公美・幸田雅治（編）（2009）『安全・安心の行政法学』ぎょうせい

2）湯淺墾道・林紘一郎（2011年）「『災害緊急事態』の概念とスムーズな適用」『情報セキュリティ総合科学』第3号、32-53頁

3）林 敏彦（2011年）『大災害の経済学』PHP

4）神戸地方裁判所平成17年6月28日

5）藤代裕之（2011年）「ソーシャルメディアの登場で風評の広がり方が変わった」『宣伝会議』814号、28-30頁

6）三上直之（2011年）「専門家の伝える『正しい知識』はなぜ市民に信頼されないのか」『宣伝会議』814号、50-51頁

7）野村総合研究所（2011年）「東北地方太平洋沖地震に伴うメディア接触動向に関する調査（概要）」http://www.nri.co.jp/news/2011/110329.html

8）佐藤幸治（1995年）『憲法（第3版）』青林書院

9）芦部信喜（高橋和之補訂）（2011年）『憲法（第5版）』岩波書店

10）The White House, International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World (2011), http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

11）Department of defense, Department of Defense Strategy for Operating in Cyberspace (2011), http://www.defense.gov/news/d20110714cyber.pdf.

情報セキュリティ3

情報セキュリティガバナンス

―規制の情報セキュリティから戦略の情報セキュリティへ―

日本大学 商学部 教授

堀江 正之 Masayuki Horie

情報セキュリティリスクは、技術のリスクとして業務の現場でスペシャリストが対処すれば済むというものではない。
当該リスクへの組織的な対処いかんによって、企業の競争基盤が有利にも不利にもなったり、
企業価値や企業のレピュテーションを高めたり損ねたりと、経営の舵取りに決定的な影響を与える可能性がある。
それゆえ経営者の関与が不可欠なのである。
経営者は、情報セキュリティリスクをダウンサイドリスクでしか捉えない規制的ガバナンスだけでなく、
推進的ガバナンスも発揮することで、戦略的な情報セキュリティを目指す必要がある。

キーワード
情報セキュリティガバナンス　情報セキュリティ戦略　規制的ガバナンス
推進的ガバナンス　情報セキュリティガバナンスの成長ステージ

1. はじめに

情報セキュリティ対策は、情報システムの機能停止や情報漏洩（ろうえい）などに起因する損失を回避・低減するための手段となることに誰も異論はない。しかし、方針を持たない情報セキュリティ対策だと「場当たり的なつぎはぎ対策」となってしまい、非効率なだけでなく効果を削ぐ結果ともなりかねない。情報セキュリティにも戦略が必要なのである。

情報セキュリティ対策の効果には、損失の回避・低減といった「ブレーキ効果」（規制的効果）だけでなく、企業価値を高める「アクセル効果」（戦略的効果）も無いとは言い切れない。ブレーキを踏むことだけを考えていたら事業や組織は後退してしまう。それゆえ、情報セキュリティ対策のアクセル効果にもっと着目する必要がありそうである。

そこで本稿では、情報セキュリティ対策への経営者のコミットメントを求める情報セキュリティガバナンスに着目して、情報セキュリティの規制的効果だけでなく戦略的効果も視野に入れた提案をしてみたい。

2. 情報セキュリティガバナンスの意義

情報セキュリティガバナンスという用語は、2000年初頭から中頃にかけて、ITガバナンスという用語の登場から少し遅れて使われ始めた。いずれの用語もコーポレートガバナンスのアナロジーであり、米国からの輸入モノである。

我が国では、経済産業省が組織における情報セキュリティ対策の実効性を向上させる意図を持ってこの用語を使い始めた―もちろんその背景には2002年に起こった都市銀行の大規模障害もある―。

経済産業省は、情報セキュリティガバナンスを「社会的責任にも配慮したコーポレートガバナンスと、それを支えるメカニズムである内部統制の仕組みを、情報セキュリティの観点から企業内に構築・運用すること」と定義した[1)]。

その後、情報セキュリティガバナンス概念の具体化が図られ、国際規格ISO/IEC38500：2008“Corporate governance of information technology”（企業のITガバナンス）を参考にして、「方向付け」、「モニタリング」、「評価」、「監督」、及び「報告」からなる五つの経営者層の活動をもって情報セキュリティガバナンスのフレームワークとした[2)]。

当該フレームワークでは、情報セキュリティガバナンスの明確な定義が示されていないので、筆者独自の考え方を織り交ぜて定義すれば、次のようになる。

情報セキュリティガバナンスとは、「経営者層が組織の抱えるリスクに見合った情報セキュリティ戦略を立案し、リーダーシップによって組織全体としての情報セキュリティへの取り組みを確立し、さらには経営者層としての取り組みの適切性を担保するために、組織の内部及び外部からする規律付けが適切に行えるような仕組みまたは機能」をいう。

情報セキュリティガバナンスは、情報セキュリティマネジメントと次の2点において異なる。

第1に、情報セキュリティガバナンスは経営者層を対象としたものであるから、管理者層及び従業員層が主体となる情報セキュリティマネジメントと区別される。

第2に、情報セキュリティガバナンスは外部ステークホルダーとの関係を含むものであるから、組織内活動として完結する情報セキュリティマネジメントと区別される。

3. 情報セキュリティガバナンスの活動と構造

情報セキュリティガバナンスは、上記の定義からも明らかなように、内容的には次の二つの活動―推進的活動と規制的活動―からなっている。

第1は、経営者が情報セキュリティ戦略を立案し、組織全体としての取り組み体制を確立し、それらを有効に働かせる活動である。推進的活動としてのガバナンスである。組織全体として調和がとれていない情報セキュリティ対策では、組織間連携がうまくゆかず、組織全体として見たときの効果が大幅に低減してしまう。また、経営者が自ら進んで行動しなければ組織の末端まで浸透しない。

全社的な情報セキュリティ行動規範が策定されたり、大規模な組織では情報セキュリティを組織横断的に統括する役員や部署が置かれることがあるが、これらは組織全体としての取り組み体制の具体的な表れといってよい。

第2は、上で述べた情報セキュリティ戦略の立案と組織全体としての取り組み体制の確立が適切に行われるように経営者を規律付ける活動である。規制的活動としてのガバナンスである。「事故が起こらないように（あるいは事故の再発防止に向けて）ガバナンスを強化せよ」と言われることがあるが、その場合この活動内容を指すことが多い。

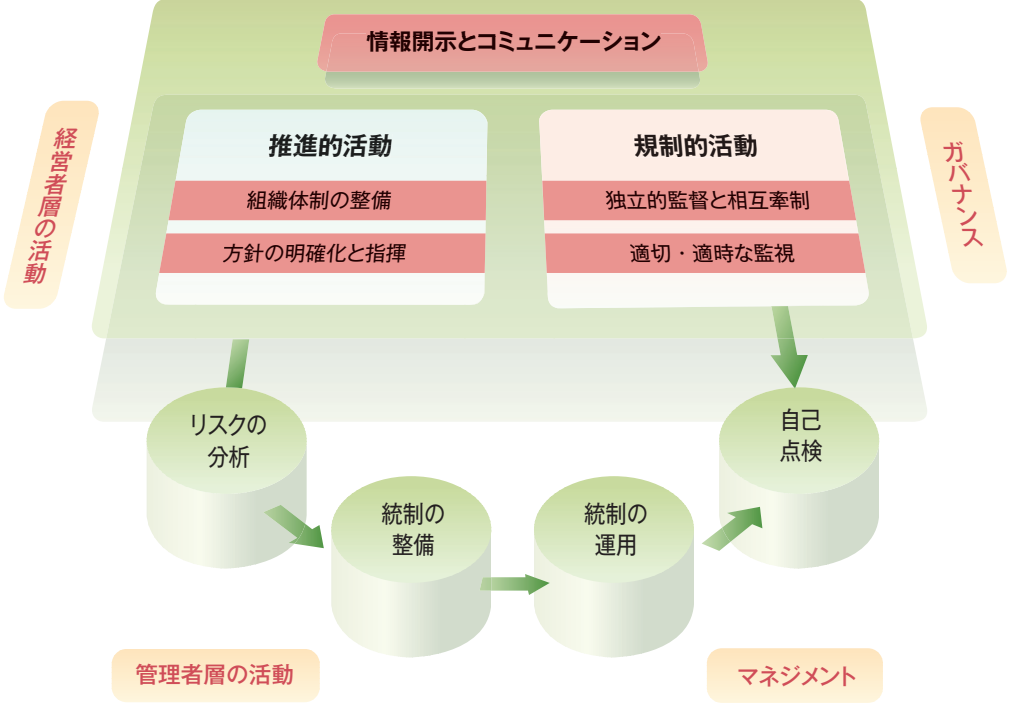
具体的には、取締役同士の相互監視、社外取締役による客観的な監視、外部ステークホルダーに対する説明責任の履行を通じた牽制（けんせい）、監査役または監査委員会による独立的な監督・監視を通じて達成することが期待されている。

図表1は、上記二つの内容を盛り込んで、情報セキュリティガバナンスの構造を表したものである。

4. 情報セキュリティガバナンスの実際

情報セキュリティ報告書を開示している企業では、1、2社の例外を除いて、情報セキュリティガバナンスについての情報開示を行っている[3)]。各社の特徴が浮き出るように整理すれば次のようになる。

図表1 情報セキュリティガバナンスの構造



［**グループ管理機能型**］ NEC：2010年報告書

情報セキュリティガバナンスをもって、グループ全体の情報セキュリティレベルの維持・向上のための仕組として位置付けている点に特徴がある。グループ全体の目標に基づいて各組織で行われるマネジメントシステムへとブレークダウンする視点を明確にしている。

［**対外的責任重視型**］ キヤノンマーケティングジャパン：2011年報告書

情報セキュリティガバナンスをもって、顧客満足度の向上というビジネス目標と併せて、セキュアな社会の実現という社会的責任の視点を取り込んでいる点に特徴がある。その枠の中で、企業グループの情報セキュリティ成熟度向上のための仕組みという社内的視点を組み込んでいる。

［**特定機能強調型**］ 日立：2011年報告書

情報セキュリティガバナンスをもって、情報漏洩を強調したダウンサイドリスクへの対応として位置付けている点に特徴がある。このことから、予防体制の整備と事故発生時の迅速な対応、及び社員の倫理観とセキュリティ意識の向上を重点的な取り組み課題として示している。

［**組織体制型**］ 富士ゼロックス：2011年度報告書

情報セキュリティガバナンスをもって、組織体制として捉えている点に特徴がある。具体的には、全社を統括する情報セキュリティ推進体制と、部門や関連会社ごとの情報セキュリティ推進体制からなる二層構造として、情報セキュリティガバナンスを捉えていることが重点的に説明されている。

［**組織体制・機能組合型**］ NTTデータ：2010年報告書

情報セキュリティガバナンスをもって、その活動と組織体制との組合として捉えている点に特徴がある。情報セキュリティガバナンスとして行われる活動（評価、方向付け、モニタリング、報告、監査）を示し、それぞれの活動をどのような組織が担っているかを対応付ける工夫が凝らされている。

［**個別的課題型**］ 富士通：2011年報告書

情報セキュリティガバナンスを、個別的課題に組み込んでいる点に特徴がある。グループとしての取り組みはコーポレートガバナンス体制として説明されており、情報セキュリティガバナンスはクラウドコンピューティングと、ソリューションビジネスグループの体制として取り上げられている。

5. 情報セキュリティガバナンスの内部的効果

情報セキュリティガバナンスには、組織に与える内部的効果と、外部ステークホルダーの視点を取り込んだ外部的効果が期待できる。

このうち内部的効果とは、経営者による経営活動（戦略策定と体制整備）、及び管理者による管理活動（上職者による指揮・制御・調整）に与えるプラスの効果である。

JohnstonとHaleは、北米と欧州を主な対象に、情報セキュリティガバナンスを導入している組織と導入していない組織との比較調査分析を行っている[4)]。それによれば、情報セキュリティガバナンスを導入している組織はそうでない組織に比べて、経営者による経営活動、管理者による管理活動のいずれについてもプラスの効果があることが確かめられている。

経営者による経営活動への効果については、経営者の情報セキュリティに対する認識や具体的な支援活動の質を調査項目としている。すなわち、①情報セキュリティ導入についての理解、②情報セキュリティプロ

グラムの積極的な支援、③情報セキュリティプログラムへの包括的準拠、④情報セキュリティの責任についての理解、⑤情報セキュリティを実施しないことの責任についての理解などを調査したところ、情報セキュリティガバナンスを導入している組織の方がそうでない組織に比べて、いずれの項目についても進んでいる。

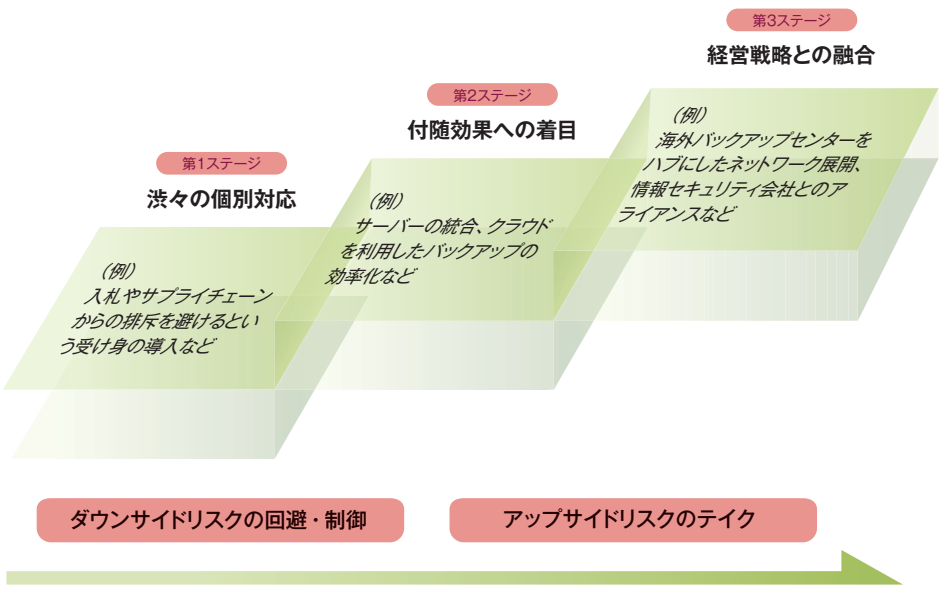
管理者による管理活動への効果については、「業務活動と情報セキュリティとの関連性」及び「情報保護体制の質」に関する調査項目の中に見ることができる。すなわち、①ビジネス目標を達成するためのセキュリティ投資の最適化、②ビジネスプロセスオーナーのセキュリティ代替案評価への関与、③ビジネスプロセスオーナーによる情報セキュリティに対する説明責任の履行、④組織内で使われている全ての情報の棚卸し、⑤情報に対するオーナシップ責任の割り当てなどについて、いずれも情報セキュリティガバナンスを導入している組織の方がそうでない組織に比べて進んでいることが確かめられている。

一方、我が国の実例に目を転じたとき、経済産業省・産業構造審議会の報告書において、いくつかの内部的効果が紹介されている[5]。例えば、情報管理サーバーのセキュリティ対策を導入する過程でその台数を大幅に削減でき、また不要な個人情報を削減することで、電力消費量や管理コストを画期的に削減できたとか、事業継続計画の一環として設置した海外バックアップセンターを国際的ハブ拠点として海外グループ企業との効率的なネットワーク構築に結び付けたといったケースである。

これらの実例を踏まえて情報セキュリティガバナンスの内部的効果に着目したとき、図表2に示すような成長ステージが識別できそうである。

第1ステージは、場当たり的対応によるコスト増加

図表2 情報セキュリティガバナンスの成長ステージ



や、セキュリティ対策の形式化、マンネリ化を招く。第2ステージは、情報セキュリティ対策の導入と、システムの最適化や業務改善の同時達成を狙うものである。第3ステージは、ITの戦略的活用に関わるアップサイドリスクへの対応として情報セキュリティを捉える考え方になる。

6. 情報セキュリティガバナンスの外部的効果

一般に、情報セキュリティ対策は、外部ステークホルダーの観点からみた企業価値向上に結び付くとは考えられていない。

情報セキュリティ事故が企業価値を毀損（きそん）することは多くの国内外の研究によって実証されている。企業価値を総合的に測る客観的な物差しがないため、株価の反応を調べる限定的な調査であるが、情報流出・漏洩では株価下落が確認されている。

これらの調査研究の中で、情報セキュリティガバナンスとの関係で興味あるのは、情報流出に関わるリスク情報が事前にステークホルダーに開示されている場合（有価証券報告書の「事業等のリスク」への記載）とそうでない場合とでは、リスク情報を事前に開示している会社の方がそうでない会社に比べて、株価の回復が早いとする調査結果である[6]。事故報道後15日において、リスク情報事前開示会社の株価は約0.1%上昇しているのに対して、非開示会社の株価は約3.0%下落していることが確かめられている。

情報セキュリティガバナンスは、情報セキュリティ管理とは違って、外部ステークホルダーからの影響を取り込む概念である。その意味で、情報セキュリティガバナンスとしての情報開示機能は、企業価値毀損の幅を小さくする効果があるといってよいであろう。ただ、今のところ、情報セキュリティガバナンスの向上が企業価値向上と結び付いているという調査研究は残念ながら寡聞（かぶん）にして見当たらない。

また、情報セキュリティ事故ではないが、不祥事が起こったときの会社の対応と株価反応との関係を解明する興味ある調査研究がある[7]。この研究では、株価の下落現象を会社が採った行動と重ね合わせることで、会社が「根本的な問題解決よりも経済性を優先する意思決定を行った」こと、そして「内部の自発的対応ではなく、事件に対する外部の認識と要求に従う形で意思決定を行った」ことに着目して、会社の事故対応のまずさが投資家の意思決定にマイナスの影響を与えたことを実証している。事故処理の経済性を優先したり、組織内部の自発的対応ができなかったことは、ガバナンスの欠陥といってよい。

これと全く逆のケースがジョンソン・アンド・ジョンソン（J&J）のタイレノール事件である。鎮痛剤タイレノールへの毒物混入の原因もつかめぬまま、徹底した回収作戦で1億ドル以上をかけて3,100万個の瓶を回収した。顧客第一主義を貫き、経済性を犠牲にした迅速かつ徹底的な対応で、企業価値を高めることとなった事件である[8]。

これらは食品会社で起こった食中毒事件、製薬会社で起こった毒物混入事件であるから、一般事業会社の個人情報の流出事件にそのまま重ねて考えることはできない―ただし個人情報の流失が会社の信用に致命的なダメージを与える性質を持つ組織では大いに参考となるであろう―。しかし、いずれもガバナンスの機能によって明暗を分けることとなった点に注目すべきである。

このコンテクストで行くと、情報セキュリティガバナンスを「予防→事故対応→回復」からなる事故対応プロセスとして把握することが重要となる。情報セキュリティガバナンスは、情報セキュリティ事故の未然防止のための組織機能として限定的に捉えられるこ

とが少なくない。けれども、事故対応がその後の経営戦略に大きな影響を与える以上、事故発生時の対応とその後の回復機能の事前の備えはガバナンスとしてカバーすべき重要な領域である。ガバナンスが効果的に機能しているかどうかは、情報セキュリティ事故が起こったときの経営者の対応に表れるといってよいかもしれない。

7. むすびにかえて

情報セキュリティガバナンスは、目で見て確かめることが難しい。その効果を客観的に測定することもできない。経営者は情報セキュリティを技術の問題と捉えがちで、とりあえず組織の形を整えることだけが自分の仕事だと思いやすい。

情報システムは経営や業務を支援するためのものであったり、新しいビジネスを創出するための武器である。それゆえ経営者は、「情報セキュリティ＝防御的対応」と狭く考えるべきではない。情報セキュリティは情報システムの目的達成を左右するものであるから、経営者による戦略が必要であり、また業務の効率的運営という観点から業務プロセスの在り方とも密接に関係している。

情報セキュリティは、外部環境、経営戦略、事業目的、業務プロセスなどの要因をトータルに取り込んだ一つの戦略でなければならない。その意味で、組織全体としての取り組み（推進的ガバナンス）とその適切性の担保（規制的ガバナンス）を通じて、情報セキュリティを組織のバリュー・プロポジションに組み込むことが求められるのである。

Masayuki Horie
堀江 正之

日本大学 商学部・同大学院 商学研究科教授。博士（商学）
カリフォルニア大学ロサンゼルス校（UCLA）客員研究員を経て、1996年から現職。専門はIT監査及びITリスクマネジメント。現在、日本セキュリティマネジメント学会理事、システム監査学会理事、内部統制研究学会理事、非営利法人学会理事、情報処理技術者試験委員、金融庁・企業会計審議会臨時委員、金融庁・予算監視効率化チーム外部委員などを兼任。また、日本監査研究学会理事、日本情報処理開発協会・企業のIT統制に関する調査検討委員会委員長、金融情報システムセンター・システム監査指針検討部会座長、経済産業省・企業のIT統制に関する調査検討委員会委員、経済産業省・情報セキュリティガバナンス研究会委員、公認会計士試験委員などを歴任。
主な著書に『IT保証の概念フレームワーク―ITリスクからのアプローチ』（森山書店、2006年、太田・黒澤賞受賞図書）、『システム監査の理論』（白桃書房、1993年、青木賞受賞図書）、『ITリスク・統制・監査』（編著：同文舘、2009年、日本監査研究学会課題別研究部会研究叢書）などがある。

補注

1）経済産業省「企業における情報セキュリティガバナンスのあり方に関する研究会報告書」（2005年）、9ページ。
2）経済産業省「産業構造審議会 情報セキュリティ基本問題委員会中間とりまとめ―企業における戦略的な情報セキュリティガバナンスの確立に向けて」（2008年）を経て、同「情報セキュリティガバナンス導入ガイダンス」（2009年）において、情報セキュリティガバナンスの全体像が示された。
3）早い会社ではすでに2008年の情報セキュリティ報告書において情報セキュリティガバナンスについて触れているが、ほとんどは2010年の報告書からこの用語を積極的に用いるようになった。これは経済産業省が情報セキュリティガバナンスを推進し始めた時期と重なっている。
4）この調査はISACAのCISMの資格を有する経営者、情報システム管理者、セキュリティ担当者、コンサルタント、監査人を対象にしたWeb調査である。A.C.Johnston & R.Hale, “Improved Security through Information Security Governance”, Communications of the ACM, Vol.52 No.1, 2009, pp.126-129.
5）経済産業省、上掲「中間とりまとめ」、9ページ。
6）金 紘玉「リスク情報の事前開示が投資家の意思決定に与える影響―情報流出リスクの顕在化ケースを用いて」『一橋商学論叢』Vol.2 No.2、2007年、102-113ページ。
7）朴 英元・大塚裕子・丸元聡子「不祥事に対する企業の対応とステイクホルダーへの影響－食中毒事件以降の雪印乳業の対応に関するイベント・スタディ分析」『科学技術社会論研究』第4号、2006年、75-88ページ。
8）J&Jについては本文に書いたような点が賞賛されるが、その後、この事件をうまく乗り切ったがゆえの成功の落とし穴にはまってしまったという厳しい見方もある（I.I.Mitroff, 上野正安・大貫功雄訳『危機を避けられない時代のクライシス・マネジメント』徳間書店、2001年、37-41ページ）。

EUデータ保護規則提案と消費者プライバシー権利章典

筑波大学 図書館情報メディア系 准教授

石井 夏生利 Kaori Ishii

本稿では、最近のプライバシー・個人情報保護に関する欧米の動向を取り上げる。
欧州連合では、2012年1月25日、データ保護規則提案が公表され、
アメリカでは、同年2月23日、消費者プライバシー権利章典を提案する政策大綱が発表された。
プライバシー・個人情報保護を人権ないしは基本的権利と捉えるヨーロッパと、
消費者保護の一環と捉えるアメリカの間には、根本思想に顕著な差が存在しており、
保護内容にも多くの相違点が存在する。
ここでは、「個人データ」の概念、「コントロール」の理解、執行の枠組みに焦点を置いて検討を加え、
日本におけるプライバシー・個人情報保護の在り方を考察するに当たっての課題を提示する。

キーワード
EUデータ保護規則提案　消費者プライバシー権利章典　コントロール　Do Not Track　忘れてもらう権利

1. EUデータ保護規則提案と消費者データプライバシーの公表

2012年1月25日、欧州連合（European Union, EU）は、「個人データの取扱いに係る個人の保護と当該データの自由な移動に関する欧州議会及び理事会の規則（一般データ保護規則）提案」（以下「EUデータ保護規則提案」という。）[1] を公表した。

その約1カ月後の2012年2月23日、アメリカ合衆国のオバマ大統領は、「ネットワーク社会における消費者データプライバシー：グローバル化したデジタル経済において、プライバシーを保護しイノベーションを促進するための枠組み」（以下「消費者データプライバシー」という。）[2] と題する政策大綱に署名した。

いずれの文書においても、インターネットが経済発展の中枢を担っており、消費者の信頼を構築することがデジタル経済を発展させる鍵となること、そのためには、強力な執行体制と個人のコントロールが必要で

あることについて、考え方は共通している。しかし、その根本思想は大きく異なっている。EUの個人データ保護については、基本的権利ないしは人権であるという発想が根付いており（EUデータ保護規則提案第1条2項）、「欧州連合の機能に関する条約（Treaty on the Functioning of the European Union）」第16条1項や、「欧州連合基本権憲章（Charter of Fundamental Rights of the European Union）」第8条1項では、全ての者は自らに関する個人データを保護する権利を有する旨の定めが置かれている。また、「人権及び基本的自由の保護のための条約（Convention for Protection of Human Rights and Fundamental Freedoms）」第8条1項では、「全ての者は、その私的な家庭生活、住居、及び通信を尊重してもらう権利を有する」と定められており、同条項はプライバシー権の根拠規定に位置付けられている。他方、プライバシー権の提唱国であるアメリカでは、カリフォルニア州の著名な裁判例において、プライバシー権を州憲法の定める「個人の幸福追求の権利」に基礎付けたものはあるが[3]、プライバシー・個人情報の保護に関して、ヨーロッパのような基本的権利ないしは人権であるとは認識されていない。とりわけここ数年では、連邦取引委員会（Federal Trade Commission, FTC）において、2009年2月12日付「オンライン上の行動ターゲティング広告に対する自主規制諸原則（Self-Regulatory Principles For Online Behavioral Advertising）」や、2012年3月26日付「急変する時代の消費者プライバシー保護（Protecting Consumer Privacy in an Era of Rapid Change）」などの報告書を公表しており、消費者プライバシーの保護を推し進める動きが強まっているようである。

2.「個人データ」概念の拡大

アメリカ及びEUでは、最近、「個人データ（personal data）」[4]の概念を拡大させる動きを見せている。1980年9月23日採択の「OECDプライバシー・ガイドライン（OECD Privacy Guidelines）」を始めとして、個人情報を保護するための国際文書や各国の法制では、個人データは、従来から「識別された、または識別され得る個人に関連する全ての情報（any information relating to an identified or identifiable individual）」であると定義されてきた。

しかし、FTCの「オンライン上の行動ターゲティング広告に対する自主規制諸原則」では、オンライン上の行動ターゲティング広告の文脈において、PII（personally identifiable information）とnon-PIIを区別する考え方が意味を失っていると指摘されている。消費者データプライバシーでは、個人データは「集積されたデータを含むあらゆるデータであって、特定個人と結びつく（linkable）もの」であれば良く、「特定のコンピュータまたは他の装置と連結されるデータを含む」と定義されている。それによると、例えば、スマートフォンの識別子、使用履歴（usage profile）を築き上げる家庭用コンピュータなどが該当する。また、FTCは、1998年児童オンラインプライバシー保護法（Children's Online Privacy Protection Act of 1998, COPPA）に基づく規則の改正を進めている。そこでは、個人情報（personal information）の概念を拡大し、クッキーが保有する情報、機器番号、IPアドレス、位置情報、写真、ビデオ、音声ファイルなど、消費者のインターネット活動を追跡するための情報を含めることが予定されている。

さらに、FTCの前記「急変する時代の消費者プライバシー保護」では、「本枠組みは、特定の消費者、コンピュータ、または他の装置と合理的に関連付けられ得る消費者データを収集または利用する全ての営利事業者に適用される。ただし、当該事業者において、1年間に5000人よりも少ない消費者のセンシティブでな

いデータを収集する場合であって、第三者と当該データを共有しない場合に限って、適用を除外される」と記されている。

1995年EU個人データ保護指令[5]は、「個人データ」を「識別された、または識別され得る自然人（データ主体）に関する全ての情報をいう；識別され得る自然人とは、とりわけ、個人識別番号、またはその人の肉体的、生理的、精神的、経済的、文化的、若しくは社会的アイデンティティに特有な一つ以上の要素を参照することよって、直接または間接に識別することができる者をいう」（第2条(a)号）と定義し、1980年OECDプライバシー・ガイドラインとほぼ同内容となっている。しかし、EUデータ保護規則提案を見ると、「個人データは、データ主体に関連するあらゆる情報を意味する」（第4条(2)項）という定めに変更されている。同規則提案では、「データ主体」は「識別されたまたは識別され得る自然人」と定義されていることから、識別性を前提としているようにも読める（第4条(1)項）。他方、この定義の対象範囲の中には、氏名、写真、電子メールアドレス、口座情報、ソーシャル・ネットワーキングサイトへの投稿、医療情報またはコンピュータのIPアドレスが含まれると説明されている[6]。

EUデータ保護規則提案の読み方は慎重に行うべきであるが、「個人データ」の範囲の拡大を容認していると読むことができる。

3.「コントロール」に関する考え方

EU及びアメリカでは、「個人データ」の概念が拡大し、個人識別性は決定的要素としての地位を失いつつあるようである。一方、「コントロール」に関する両者の捉え方は大きく異なっている。なお、日本では、プライバシー・個人情報保護の文脈で「コントロール」という時は、いわゆる「自己情報コントロール権」を想

図表1 消費者プライバシー権利章典

第1原則 **個人のコントロール**	消費者は、企業が消費者からいかなる個人データを収集し、どのように利用するかについて、コントロールを行使する権利を有する。
第2原則 **透明性**	消費者は、プライバシー及びセキュリティの実務について、容易に理解できアクセス可能な情報を得る権利を有する。
第3原則 **状況の尊重**	消費者は、企業において個人データを収集し、利用し、そして提供する際には、消費者がデータを提供する状況に適合した方法によることを期待する権利を有する。
第4原則 **安全性**	消費者は、安全かつ責任を持って個人データが取り扱われる権利を有する。
第5原則 **アクセス及び正確性**	消費者は、データの機微性及びデータが不正確な場合に消費者に不利な結果をもたらすリスクに適した態様において、利用可能な書式によって、個人データにアクセスし、訂正する権利を有する。
第6原則 **制限的収集**	消費者は、個人データを収集及び保有する企業に適切な制限を課す権利を有する。
第7原則 **責任**	消費者は、企業が個人データを取り扱う際に、消費者プライバシー権利章典を確実に厳守するための適切な措置とともに行わせる権利を有する。

起することが多いが、同概念は長きにわたり百家争鳴の状態が続いており、統一的な理解には至っていない[7]。

アメリカの消費者データプライバシーは、「プライバシー権利章典」と題し、次のような七つの諸原則を掲げて立法化を提案している（図表1）。

いずれも1970年代以降の公正情報実務諸原則（Fair Information Practice Principles）[8]から発展してきた重要な原則ではあるが、アメリカの考え方が最も顕著に表れているのは、第1原則及び第2原則といえる。

消費者データプライバシーによれば、第1原則の「個人のコントロール」について、次のように記されている。「企業は、消費者に対し、消費者が他者と共有する個人データに対し、また、企業が個人データを収集、利用、開示する方法に対する適切なコントロールを与えるべきである。企業は、企業が収集し、利用し、開示する個人データの規模、範囲及び機微性に対応するとともに、個人データに関する利用の機微性にも対応する形で、容易に利用されアクセス可能な仕組みを消費者に与えることによって、これらの選択を可能にするべきである。企業は、消費者に対し、個人データの収集、利用及び開示に関する意味のある決定を下せるような時期及び方法を提示し、明確で簡明な選択を与えるべきである。企業は、消費者に対し、最初に同意を付与する方法と同様に、同意を撤回し、または制限するための、アクセス可能で容易に利用できる方法を示すべきである」。この説明によると、個人データの収集、利用、開示に関する意味のある決定を「選択」と表現しており、そのための容易かつアクセス可能な仕組みを提供すべきことが求められている。同様に、同意の撤回または制限も「選択」に含まれる。

そして、個人のコントロールには二つの側面が存在すると説明されている。第1は、企業によるデータの収集時に、データの共有、収集、利用、及び開示に関する「選択」を提供することである。オンライン行動ターゲティングの場面では、第三者による個人データの収集が行われるが、このような第三者も「選択」を提供しなければならない。

アメリカでは、「選択」のための仕組みとして、「追跡拒否（Do Not Track, DNT）」の導入が進められている。これは、恒久的なクッキーに似た設定を消費者のブラウザに取り入れ、ブラウザが訪れたサイトにその設定を伝え、消費者が追跡されたりターゲティング広告を受け取ったりするのを望むか、そうでないかの信号を送信することを伴うものである。この仕組みは、オプト・アウトではあるが、「統一的（uniform）」かつ「恒久的（persistent）」に選択を与えることが特徴とされている。また、DNTには強制可能な要件が必要とされている[9]。

DNTの仕組みは、具体的には、ブラウザがウェブサーバーに送信するHTTPリクエストのヘッダに「DNT:1」を追加することなどにより行われる。Googleなど約400社が加盟するデジタル広告アライアンス（Digital Advertising Alliance）は、2012年2月23日付のウォール・ストリート・ジャーナルの記事の中で、9カ月以内にDNTをサポートする旨を公表した。

コントロールの有するもう一つの側面は、選択に対する消費者の責任である。消費者データプライバシーによれば、消費者は、個人データの利用や共有に対する自らの選択を評価し、その選択に責任を負うべきと記されている。その際、共有に関する最初の決定が重要となる。

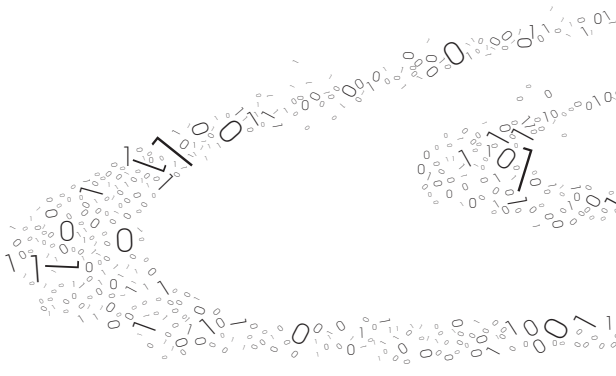
第2原則に関しては、次のように説明されている。「消費者がプライバシーのリスクを意味ある形で理解し、個人のコントロールを行使できるようにするために、企業は、自らがいかなる個人データを収集し、そのデータがなぜ必要であり、どのようにそれを利用し、そのデータをいつ消去し、または消費者のデータを匿名化するか、及び、第三者と個人データを共有する可能性

の有無及び共有する目的について、最も有用な時及び場所において、明確な説明を提供すべきである」。これは、個人がコントロールを行使する前提として求められる必要的原則といえる。第1及び第2原則が相まって、消費者の信頼を得るためのコントロールの仕組みを提供することが可能となる。

一方のEUデータ保護規則提案においても、前文の中でデータ主体によるコントロールの重要性がうたわれており、強力な執行を背景に、強固でより一貫したデータ保護の枠組みが強調されている[10]。規則提案は、加盟国の立法措置を必要とする「指令」から、立法措置なくして直接適用される「規則」への変更、域外適用の可能性、「忘れてもらう権利及び削除権」及び「データ・ポータビリティの権利」の創設、「データ保護・バイ・デザイン」、「個人データ侵害の通知/連絡制度」及び「データ保護影響評価」の導入、第三国への個人データ移転に当たっての「十分な保護レベル」を認定する際の独立監視機関の必要性、第29条作業部会から欧州データ保護委員会への改組、全世界の総売上2%を上限とする制裁金の措置など、極めて多くの改正事項を含んでいる。これらの制度は、全体的に、データ主体によるコントロールを強化し、データ保護制度を厳格化することを意図している。

特に注目されているのは、「忘れてもらう権利及び削除権（Right to be forgotten and erasure）」（第17条）である。この権利については、1995年EUデータ保護指令第12条（b）号において、データ主体に対し、データが不完全または不正確な性質を有していた場合の修正、消去又はブロックの権利が保障されていた。「忘れてもらう権利」は、同指令の権利を精緻化・具体化したものと説明されている[11]。第17条は、データ主体に対し、自らに関する個人データを削除させる権利、及び、当該データのさらなる拡散を停止させる権利を付与している（1項）。併せて、管理者が当該個人データを公開していた場合、管理者は、当該個人データを取り扱っている第三者に対し、全てのリンク、コピーまたは複製の削除をデータ主体が要請している旨を通知しなければならない（2項）。

以上のように、アメリカでは、消費者データの「コントロール」は、個人データの取り扱いに対して、「十分な情報提供を受けた上での選択権」を付与することであるが、EUでは、個人データの取扱規制の全般が、コントロールを実現するものであると考えられる。ただし、EUは、「拘束的企業ルール（Binding Corporate Rules）」による第三国移転（第43条）やデータ保護シールなどによる認証制度（第39条）なども導入していることから、厳格化一辺倒ではないことにも注意が必要である。



4. 執行の枠組み

アメリカでは、民間部門のプライバシー保護は、原則として自主規制に委ねられており、機密性の高い分野では、分野ごとに個別法が制定されるというセクトラル方式が採用されている。FTCは、分野別の個人情報保護法に関して、消費者保護の権限を担う独立監督機関としての役割を果たしてきた。特に重要なのは、FTC法第5条の定める「不公正または欺瞞的行為または実務（unfair or deceptive acts or practices）」である。FTCは、同条項に基づき、児童オンラインプライバシー保護法（COPPA）、1970年公正信用報告法（Fair Credit Reporting Act of 1970）、1978年金融サービス近代化法（Financial Services Modernization Act of 1978）といった個別法に基づくFTC規則に違反した事業者に対し、差止請求、排除命令、違反行為ごとに1万ドル以下の民事制裁金などの監督権限を行使してきた[12]。しかし、FTC法第5条を発動できない事業分野も存在していることから、共通的な基盤を提供する消費者プライバシー権利章典の立法化が提案されるに至った。消費者データプライバシーでは、FTC及び州の司法長官による直接的法施行が予定されている。例えば、FTCは、消費者プライバシー権利章典違反に対する民事的制裁金を求める訴訟に関して、司法省に書面による通知を発し、45日以内に司法省が提訴しない場合は、直接に提訴権を行使できるといった制度が提案されている[13]。

これに対し、次のようなセーフ・ハーバーの制度も検討されている。複数利害関係者[14]が策定手続きに参加した実務規範（Codes of Conduct）について、FTCは、それを消費者プライバシー権利章典に照らして審査・承認する権限を有する。しかし、実務規範を承認すれば、それに準拠している企業に対する法執行は制限される。一方、実務規範の採用を拒否した事業者、または、FTCの審査を受けない実務規範を採用している事業者に対しては、法に基づくプライバシー権利章典が適用される。

このように、アメリカでは、実務規範に基づく自主的な取り組みをベースとした上で、FTCの法執行を背景に遵守を担保するという方針が採用されている。

EUデータ保護規則提案では、前記のとおり、数多くの保護策の導入が予定されている。法執行との関連では、個人データ侵害を起こした管理者による監督機関への24時間以内の通知義務（第31条）、規則違反を犯した事業者に対する全世界の総売上2%を上限とする制裁金（第79条6項）などが話題となった。加えて、個人データの第三国移転を認めるための「十分な保護レベル（adequate level of protection）」を欧州委員会が認定する際の考慮要素に、「データ保護ルールの遵

守を保証する責任を負う独立監視機関に関する効果的な機能の存在」が明記された点は注目される（第41条2項(b)号）。EUの方針は、事業者に課すルールをより具体的に定め、独立監視機関の設置を第三国にも求めるというものである。

5. 終わりに

アメリカとヨーロッパでは、インターネット上の消費者の信頼構築がデジタル経済を発展させる鍵となること、そのために、強力な執行体制と個人のコントロールが必要であること、個人情報の識別性はメルクマールとしての機能を失いつつあることにおいては共通的であるが、プライバシー・個人情報保護に関する根本的思想、「コントロール」の理解、執行の枠組みにおいては、対照的な方向性を見せている。

日本の個人情報保護法制は、個人情報を「生存する特定個人を識別できる情報」であると定義しているが、スマートフォンのアプリを巡る昨今の問題にも見られるように、「個人識別性」の制約に捉われると、識別性の有無が明確ではない情報について、保護を及ぼすことができないという問題が発生する。また、個人情報保護法が目的とする「個人の権利利益」は人権としてのプライバシーであるのか否か、自己情報コントロール権のいう「コントロール」の捉え方に関しても、コンセンサスは形成されていない。

執行の枠組みに関して、個人情報の保護に関する法律では、主務大臣制による緩やかな監督が行われてきた。国会審議中のいわゆる「マイナンバー法案」が制定されると、「個人番号情報保護委員会」が新たに設置され、日本初の独立監視機関が日の目を見ることとなる。しかし、マイナンバー法案は、主に行政機関の保有する個人情報の保護に関する法律及び独立行政法人等の保有する個人情報の保護に関する法律の特別法であり、個人情報保護法制全体の枠組みに影響を与えるものではない。

アメリカの消費者データプライバシーは、実務規範に基づく国際的な相互認証にも言及しており、EUデータ保護規則提案への対抗策を意識したものと考えられる。2012年3月19日、EUとアメリカは共同声明を発表し、2000年に締結されたセーフ・ハーバーを再確認する旨を明らかにし、妥協の方向性を明らかにしたが、日本としては、個人情報保護法の世界的潮流がどこへ向かっていくのか、あるいはこれまでとは異なる第三の道が登場するのか、十分に見極める必要がある。少なくとも、プライバシー・個人情報保護の根本的思想、保護策の在り方について、欧米では自らの方針を明確に打ち出している現状を十分に踏まえつつ、日本においても、個人情報保護法制全体を改めて見直す準備を進めておく必要がある。

Kaori Ishii
石井 夏生利

筑波大学 図書館情報メディア系　准教授、博士(法学)。専門はプライバシー権・個人情報保護法
内閣官房「電子行政に関するタスクフォース」構成員、同「社会保障・税に関わる番号制度　個人情報保護ワーキンググループ」委員、総務省「利用者視点を踏まえたICTサービスに係る諸問題に関する研究会　スマートフォンを経由した利用者情報の取扱いに関するWG」委員、行政書士試験委員、神奈川県個人情報保護審議会委員などを歴任。著書は、『クラウドコンピューティングの法律』民事法研究会（共著）(2011)『プライバシー・個人情報保護の新課題』商事法務（共著）(2010)、『個人情報保護法の理念と現代的課題―プライバシー権の歴史と国際的視点』勁草書房(2008) など。

補注

1）European Commission, *Proposal for a Regulation of The European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data* (*General Data Protection Regulation*), http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf (last visited Mar. 10, 2012).

2）White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy,* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf (last visited Mar. 10, 2012).

3）Melvin v. Reid, 297 P. 91 (Cal. Ct. App. 1931).

4）日本の個人情報保護法制では「個人情報」に相当する。

5）Council Directive 95/46, 1995 O.J. (L 281) 0031-0050 (EC).

6）Data protection reform: Frequently asked questions, http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/12/41&format=HTML&aged=0&language=EN&guiLanguage=en (last visited Mar. 10, 2012).

7）アメリカでは、情報プライバシー権とも言われている。*See* Alan F.Westin, Privacy and Freedom (1967); Arthur R. Miller, The Assault on Privacy：Computers, Data Banks, and Dossiers (1971). 日本で自己情報コントロール権を急速に普及させる契機となった論文は、佐藤幸治「プライヴァシーの権利（その公法的側面）の憲法論的考察（一）－比較法的検討－」法学論叢第86巻5号（1970年）1頁以下、同「プライヴァシーの権利（その公法的側面）の憲法論的考察（二）－比較法的検討－」法学論叢第87巻第6号（1970年）1頁以下である。

8）合衆国保健教育福祉省（United States Department of Health, Education, and Welfare＜当時＞）の「自動個人データ・システムに関する長官の諮問委員会（Secretary's Advisory Committee on Automated Personal Data Systems）」による「記録、コンピュータ及び市民の権利（Records, Computers, and the Rights of Citizens）」（1973年7月）において、「公正情報実務に関する法」の制定が勧告された。

9）2010年12月1日付「急変する時代の消費者プライバシー保護」（中間報告書）63-69頁、及び、2012年3月26日付同最終報告書52-55頁参照。

10）前文第6項及び第55項参照。

11）EUデータ保護規則提案解説メモ9頁「3.4.3.3　第3条－訂正及び削除」参照。

12）15 U.S.C. § 45 (a) (2), (b) (m) (1) (A).

13）15 U.S.C. § 56 (a).

14）個別の企業、事業者団体、プライバシー擁護者、消費者団体、犯罪被害者、学者、国際的パートナー、州の司法長官、連邦の法執行官その他関連団体。

彼らの流儀はどうなっている？

執筆：水波誠　絵：大坪紀久子

昆虫の脳は神経細胞わずか100万個の微小脳。しかし昆虫は極めて優れた学習能力を持つ。
その脳の精妙な仕組みが明らかになりつつある。

偉大な微小脳

昆虫の脳は**小型・軽量・低コスト**

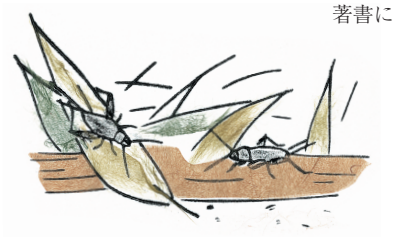
「昆虫にも脳がある」と言うと驚く人もいるかもしれない。昆虫の行動は一見すると単純に見えるので、昆虫の頭部にある神経細胞の集合体を「脳」と呼んでいいのか、それとも単に「頭部神経節」と呼ぶべきか、専門家の間でも議論があった。実際、昆虫の「脳」を構成するニューロン（神経細胞）は数十万個に過ぎず、人間の脳が1000億個ものニューロンから成るのに比べて10万分の1以下である。

しかし最近、この小さな脳には、複雑な記憶を司り、行動を組み立てる巧妙な仕組みがぎっしりと詰まっていることが分かってきた。

私は、昆虫の小さな脳を、哺乳類の大きな脳と対比して、微

Makoto Mizunami　北海道大学 大学院理学研究院 教授

1957年生まれ。九州大学大学院理学研究科修士課程修了。東北大学大学院准教授などを経て2009年より現職。
著書に『昆虫―驚異の微小脳』（中公新書）、『動物は何を考えているのか？：学習と記憶の比較生物学』分担執筆（共立出版）など。



小脳という概念でとらえることを提唱している。昆虫の脳は、その小さな体での生活に適合した、小型・軽量・低コストの情報処理装置の傑作ではないかと提案したのである。

コオロギの学習

昆虫の行動の多くは反射や生まれながらの本能に基づくというのが従来の定説であった。しかし私たち生物学者は、昆虫が匂い、模様、色などを記憶する優れた能力を持つことを明らかにしてきた。私が調べているフタホシコオロギの匂い学習を例に挙げよう。

数日間絶水させたコオロギに匂いをかがせ、その直後に報酬である水を飲ませる訓練を行う。するとわずか１回の訓練で、匂いと水とを結びつける学習が成立した。３回の訓練で成立した記憶は４日間保持された。幼虫の初期に５日間連続で匂い学習の訓練を行うと、その記憶は成虫になり老熟してもまだ保持されていた。匂いの記憶は一生涯保持されるのだ。

また14種類の匂いを７組に分け、一方を報酬である水と、もう一方を罰である高濃度の塩水と結びつける訓練を行った。するとコオロギは、いずれの組の匂いを嗅がせても水と結びつけた方の匂いを選んだ。コオロギは14種類の匂いを同時に記憶できたのだ。

またコオロギには「状況依存的学習」と呼ばれる高度な学習能力があった。例えば明るいときにはバニラの匂いを水と、ペパーミントの匂いを塩水と結びつけ、逆に暗いときにはペパーミントの匂いを水と、バニラの匂いを塩水と結びつけて覚えることができた。

コオロギは、学習獲得の素早さ、記憶保持期間の長さ、記憶容量の大きさ、高度な学習をこなす能力、そのいずれをとってもラットやマウスなど哺乳類とほとんど引けを取らない。哺乳類の巨大脳と昆虫の微小脳で、その基本原理には共通点があるのかもしれない。

昆虫の脳から人間の脳へ

現在、人間の脳科学が脚光を浴びているが、もし昆虫と人間の脳の原理が似ているとすると、昆虫の脳の解明が人間の脳を解明する突破口になるかもしれない。昆虫の脳の設計図を手に入れ、人間の脳の理解の助けとすること。この目標を達成すべく、私たちはコオロギやゴキブリ相手に奮闘を続けている。

リポート

5年後の未来を探せ

池田英男教授に聞く
植物生理学・農学・ITが出会う「植物工場」の明日

取材・文：船木春仁　撮影：菊地英二

土を使わず、養液で野菜を育てる植物工場。膨大な条件下における植物成長の変化をITを駆使して探り、かつ成長を制御するための研究開発が進められている。日本農業の在り方を根底から変える力を秘めた植物工場の先端研究を聞いた。

養液栽培を基本とする省資源型農業

千葉県柏市の北部に在る、つくばエクスプレス「柏の葉キャンパス駅」。駅前のショッピングモールを囲むように高層マンションが立ち並ぶが、５分も歩けば千葉大学環境健康フィールド科学センターの広大なキャンパスが控えている。ここは、日本の植物工場の最先端技術の研究の地でもある。

農林水産省の補助事業に採択され、千葉大学と企業が共同で研究する八つのプロジェクト（コンソーシアム）が進行中だ。研究の推進役でありアドバイザーでもあるのが池田英男特任教授（大阪府立大学名誉教授）。日本の植物工場研究の先駆者である。

植物工場とは、「養液栽培を基本とし、生育環境の全てを制御して植物を育てる技術と施設」のこと。土を使わず、少ない資源で効率良く、無農薬で植物を育て、環境への負荷も少なくする。太陽光を一切使わない「人工光型」と、光源は太陽光として、室温や光強度、湿度、二酸化炭素（CO_2）濃度制御なども併せて行う「太陽光型」の二つのタイプがあり、八つのプロジェクトも両タイプに分かれるが、中でも注目されるのが太陽光型の「統合環境制御による生産性向上プロジェクト」だ。

育てるのは、オランダで植物工場用に改良されたトマト。2011年９月から栽培を始め、2012年７月いっぱいまでの10カ月間、ありとあらゆる生育環境を制御して10アール（1000㎡）当たり50トンの収穫を目標としている。取材で訪ねたのは４月上旬だが、既に目標達成のめどがついたという。これは補助事業が求める開発目標のレベルを超えるもので、1kg 200円で販売しても、10アールで1000万円の粗収入となる。

ちなみに同じ面積での露地栽培の収穫量は8トンから10トンほど、温室栽培でも20トン程度が多い中で、植物工場の収穫量は図抜けている。また４月10日の東京青果（株）における千葉県産トマトの相場は１kg当たり603円で、植物工場の生産量ならば、生産者の出荷価格次第とはいえ、大きな利益を得ることは可能だ。

しかし池田教授は、「植物工場では世界で最も先行するオランダでは、65トンから70トンが当たり前で、まだまだ満足できるレベルではない」と厳しい。

Hideo Ikeda
池田 英男

千葉大学 環境健康フィールド科学センター 特任教授
大阪府立大学農学部助手、筑波大学農林学系助教授、大阪府立大学大学院生命環境科学研究科教授を経て2009年に退職、同大名誉教授。同年、千葉大学客員教授に就任。この間、日本養液栽培研究会会長、各種政府系研究会委員長などを歴任。

600個のセンサーを駆使して リアルデータを収集・解析

統合制御研究の植物工場は、軒高が5mを超える大きなハウス。天窓や室内ファンもある。ハウスには、光合成の原料となるCO_2を灯油を燃やして発生させる装置、その排熱でお湯を沸かしてハウス内を温めるための装置、液肥を調整し送り出す装置などがある。外からの雑菌や害虫の侵入を防ぐために入り口は3重で、訪問者は靴を履き替え、特殊な作業衣を着なければならない。まるで半導体の製造工場だ。

トマトの栽培法は、年1作・長期多段採りといわれるもの。トマトの茎を天井からのひもで吊しながら上へ上へと30～40段にまで伸ばす。多段になればなるほど多くの花房（果房）がつき、収穫量を増やせるからだ。ハウスの天井高が高いのも、この栽培法のためだった。ハウス内には受粉のために蜂が放たれている。

トマトは、幅20cm、長さ91cm、高さ7.5cmのロックウールの“ベッド”に根を張る（ロックウールとは、玄武岩や石灰などを高温で溶解して作る人造鉱物繊維）。一つのロックウールに3株が植えられ、10アール当たり2400株が育てられている。このベッドに自動的に液肥が施されていく。2400株の全てに同じ品質や濃度の液肥を等量施す。これは土の畑では絶対にできない。またベッドは、高さ1mほどの所に設置されている。腰を曲げなくてもよい作業性の良さも植物工場の大きな特徴だ。

そして、「キャンパス内の工場全体には600個を超える数のセンサーが設置され、間断なくデータを収集している」。植物は、様々な環境の影響を受けながら成長している。環境要因の主なものだけでも地上部環境では光・湿度・気温・風・CO_2濃度、地下部では温度・水分・液肥のpHや濃度・溶存O_2濃度・無機要素の組成と濃度、植物自身では葉温・光合成や炭水化物などの転流・蒸散速度・浸透圧・根温・根圧・呼吸量等々。

「しかも、どこで計測するかによっても測定結果は大きく変化する。例えば光合成に利用される光は植物体の上部では強いが、下へ行くほど弱くなり、1.5mほど下になると最上部の10分の1にも満たない。そうしたことも考慮しながらセンサーを配置してデータを多面的に収集している」

植物生理の知見と農学の技法が絡む膨大なパズル

統合制御では、環境の制御法を見つけ出せさえすれば、欲しい収穫物が得られるように栽培できると考える。ひたすらに収穫量を多くしたければ、そのための制御法を探り、収穫量よりも味や甘みを優先したければ、そのための制御法を探り、カルシウムやビタミンが豊富な野菜を採りたければ、そのための制御法を探る。

同じ種類の植物でも、条件を変えれば育ち方は全く違う。これは人間とて同じ。植物の場合は、「生殖成長」と「栄養成長」という二つの成長があり、両者のバランスをうまく取ることで多収となる。またトマトでは、根が吸収する水分量を減らしてやるなどのストレスを与えると、細胞の分裂や伸長が抑制されて葉や果実は小さくなるが、葉から果実への糖の転流は抑制されにくいので、甘い果実が収穫できることになる。またストレスは、うまみの主成分であるグルタミン酸を増加させることも知られている。幹や側枝を伸ばしたりするのは栄養成長だが、こればかりに栄養が回っては実が充実しない。

制御法の探索はつまり、膨大なデータをいかに読み解き、実際の成長との相関性を突き止めるかにある。ビッグデータの解析と活用、つまりマイニングにほかならない。これまでの日本の農業に欠けていたのは、栽培環境を理解するためのデータである。

同じ気温でも、春と秋では光の量が違う。だとするならば、光量の差に代わる別の環境要因を制御できれば収穫は安定するのか。飽差*が適当な範囲にあると、植物は葉の裏側にある気孔を開けて、より多くのCO_2を吸収する。また、CO_2を供給し、葉からの蒸散を促すには風が必要である。ならば風をどれぐらいの強さで、どういう条件下で制御すべきか。さらには生殖成長と栄養成長のバランスを取るために、ストレスをどうかけるか等々。植物生理学の知見と農学の技法が複雑に絡み合う膨大なパズルである。

だからという訳ではないだろうが、池田教授も「植物生理学の基本と植物の環境応答を理解した上で、コンピューターを上手に使える人ほど収穫量が多いね」と笑う。

IT 活用によるビッグデータ解析の有用さを改めて知らされるが、それを強調するのは遅きに失しているかもしれない。植物工場の先進国であるオランダの例を見れば明らかだからだ。

オランダは、総人口が日本の16%、耕作面積が20%しかないのに農産物輸出額はアメリカに次いで世界２位だ。労働生産性（就業者１人当たりの国内総生産）は、OECD30カ国の中で８位で1980年の倍以上になった（日本は20位、2008年ベース）。その原動力がIT活用による農業、つまり植物工場技術の構築だった。大規模な植物工場で各種管理のシステム化やロボット化を進め、農業に工業的な手法を駆使する1.5次産業化に成功した。池田教授は、植物工場の有用性を次のように強調する。

「コンピューターを駆使した植物工場は、人工的に気温や光、風などを制御するが、それは何らかの形で燃料を使った制御であり、燃料ベースで生産計画を立てることを意味している。そうするとコ・ジェネレーションとか創エネなどの周辺技術の開発と活用にも目が向けられ、さらに低コストで環境を制御できるようになる。オランダでは日照時間が日本より少ないのに、実験的には、2008年に1㎡当たり100kgのトマトの収穫に成功している。これは今、我々が実証しようとしている量の２倍だ」

統合環境制御システム

機械室

機械室では、ハウス内外の環境情報に基づき、コンピューターが設備・機器を動かしている。





①統合環境制御専用のコンピューター、マキシマイザー。換気、遮光、保湿、CO_2濃度、気温、給液などの制御をしている。
②エンジニアがモニタリングしている画面。蓄積したデータを分析し、制御値の修正を行っていく。
③CO_2発生装置と温湯暖房装置。オランダでは当たり前のCO_2施用は、日本ではこれまであまり普及していない。
④養液装置。成長段階と代謝の状況に応じて、水やりと肥料成分の調整を行う。
⑤排液循環システム。廃液による環境への負荷を抑える。

制御指示

環境測定値

栽培室

半閉鎖式、高エネルギー高効率ハウス内では、高収量トマト品種のハイヤーワイヤ式栽培、ロックウールの使用などによって、長期多段栽培を行っている。トマトのつるの長さは10ｍを超え、収穫できる果房の数は30～40にもなる。



⑥センサーが随所にあり、常時、測定情報が収集されている。
⑦カメラ画像は千葉大学の研究室に送信されている。
⑧一つの株から何段もの実をならせている。
⑨植物工場に「土」はない。床には温水パイプが、栽培ベッドには給液装置がある。
⑩床の温水パイプは、高所作業車のレールにもなり、腰を屈めて作業する必要がなく、労働が軽減できる。
⑪ロックウールに根を張るトマト。養液パイプが差し込まれ、１株ずつ管理される。


食糧安保につなげていけるか

農業市場の対外的な開放は、戦後一貫した貿易対立のテーマだった。TPP（環太平洋戦略的経済連携協定）参加を巡る議論も従来の流れの中にある。しかし、オランダのように農業が国富の源泉となるならば、植物工場をためらう必要があるだろうか。韓国では国策として植物工場を輸出産業にしようとしている。輸出、つまり外貨獲得を目的にした植物工場の建設が大規模に進んでいるという。

池田教授が学生時代に指導教授から「レタスの水耕栽培法の研究」を勧められたのは45年前、1960年代半ばの高度成長期のことだ。既に当時から、「工業に学ぶ農業、1.5次農業」という発想はあったのだ。そして今、日本でも植物工場は増加している。農林水産省の調査では、1ヘクタール（10000㎡）以上の植物工場は全国で80カ所を数える。養液栽培の総面積は2000ヘクタールで、ハウス栽培５万ヘクタールの４％ほど。市場調査会社の矢野経済研究所は、2009年の植物工場の野菜出荷金額は約138億円で、2020年度には640億円にまで拡大すると予測している。

農林水産省では、生産コストを３割削減した栽培管理技術の実用化と植物工場の設置数を150カ所、つまり倍増させることを目標としている。補助事業自体の実施が若干遅れているので、この目標は４～５年後の達成を目指していると解釈してよいだろう。

しかし、それほどバラ色でもない。池田教授が強く指摘するのが、「農業は土作りから」という日本農業の“土壌信仰”の強さだ。土を使わない農業は認められず、消費者も植物工場で栽培された野菜は、「何か人工的で嫌だ」などと言う。この国土は栄養豊かで、オランダのように耕地面積が少なく土地も豊かでなかった所での“必要は発明の母”を生まなかった。しかし現状は、土作りとは大量の土壌改良材を投入したものであり、土地活用型農業の経済生産性は低く、決して明るい未来を描けているわけではない。IT の力をバネにするケースも少ない。

興味深いのは、補助事業の名称が「モデルハウス型植物工場実証・展示・研修事業」となっていることで、実際、千葉大学をはじめ補助金を受けている団体は、展示会や研修会を定期的に開いている。つまり、植物工場の実態を知ってもらい、人の意識から変えていかないとダメだというのである。

池田教授はまた、「1億円プレーヤーを増やす会会長」を自称している。農家収入をもっと増やし、農業を魅力と誇りに満ちた産業にしたいと願ってである。ある研究によれば、所得500万円を得るための作物の栽培面積と労働日数は、例えばホウレンソウは40日で栽培できるが、1.8ヘクタールの土地で568労働日数が必要だという**。これに対して植物工場ではトマトなら30アール、ミツバやホウレンソウなどなら20アールで年間売上高は2000万円程度になり、1000万円程度の実所得になる。「植物工場こそが環境負荷も少なく、持続的で、楽しく収益を確保できる道である」

19世紀に植物生理学という学問分野を確立したのはドイツ人のJ.ザックスだが、彼が植物学や農学の発展に大きく寄与したのは、水耕法の発明にあった。様々な無機塩類を溶かした水溶液に根を浸し、どのような植物がどのような無機塩類を必要としているのかを調べたのである。今まさに千葉大学で展開されているのは、ザックスの検証方法を、対象を環境という大きな世界に広げ、ITを駆使して究めることである。

*その時の葉温における飽和水蒸気分圧と実際の大気の水蒸気分圧の差。飽差が大きいほど，空気が乾いていることを意味する。
** 小沢聖『農業及園芸』第72巻３号1997年

取材･文 船木春仁 Haruhito Funaki
1956年、北海道生まれ。東京タイムズ社総合デスクを経て独立、編集工房PRESS Fを主宰。ものづくりや情報通信等について執筆活動を展開。著書に『時代がやっと追いついた』（新潮社刊）等。

蛍光灯を使った人工光利用型施設の一つ。低コストでカット野菜並みに衛生管理がされたレタス栽培を実証している。（左）

研究室の一部。野菜の成分分析などを行い、環境と生育・代謝の関係を分析し続けている。（右）

2012年度著書出版・海外学会等参加助成に関するお知らせ

本誌では、2012年度も公益財団法人KDDI財団が実施する著書出版・海外学会等参加助成に、候補者の推薦を予定しております。

【著書出版助成】

助成内容：情報通信の制度・政策の研究に関する著書出版への助成
助成対象者：過去5年間にNextcom誌へ論文をご執筆された方*
助成金額：3件、各200万円
応募受付期間：2012年8月1日～9月10日

【海外学会等参加助成】

助成内容：海外で開催される学会や国際会議への参加に関わる費用への助成
助成対象者：Nextcom誌に2頁程度のレポートをご執筆いただける方*
助成金額：北米東部　最大40万円　北米西部　最大35万円
ハワイ　最大30万円
その他地域　別途相談（総額100万円以下）
応募受付期間：2012年6月以降偶数月の1日～20日

推薦方法：監修委員会において審査・選考し、KDDI財団への推薦者を決定します。
応募方法並びに詳細は、下記「Nextcom」ホームページをご覧ください。
*常勤の国家公務員（研究休職などを含む）、KDDIグループ関係者は応募できません。

論文公募のお知らせ

本誌では、我が国の情報通信制度・政策に対する研究活動の活性化を図るため、新鮮な視点を持つ若手研究者の方々から論文を公募します。

【公募要領】

申請対象者：45歳以下の研究者（大学院生を含む）で、日本に在住する方
*常勤の国家公務員（研究休職などを含む）、KDDIグループ関係者は応募できません。
論文要件：情報通信の制度・政策に関する未発表論文（日本語に限ります）
*情報通信の制度・政策の参考となる内容であれば、情報通信以外の公益事業に関する論文も含みます。
*技術的内容をテーマとするものは対象外です。
選考基準：刷り上がり10ページ以内（およそ10,000字）
情報通信分野における制度・政策に対する貢献度を基準に、監修委員会が選考します。
（査読付き論文とは位置づけません）
公募論文数：毎年若干数
公募期間：2012年4月1日～8月31日（掲載は2012年12月または2013年3月を予定）

応募方法・詳細については「Nextcom」ホームページ
http://www.kddi-ri.jp/nextcom/index.html をご覧ください。

「EEA-ESEM 2011」参加報告

馬場 弓子
青山学院大学 経済学部 教授

**2011年8月25日から29日まで、オスロ大学にてEEA-ESEMが開催された。
今回は、最先端の研究発表を通じた、理論、実証、実験の融合の場となった。**

EEA-ESEMとは

財団法人KDDI財団の海外学会等参加助成を受け、筆者は第26回EEA（European Economic Association）に参加して研究発表を行う機会を得た。

今回は、第26回EEAと第65回ESEM（Econometric Society European Meeting）との共同開催として、2011年8月25日から29日まで、オスロ大学にて行われた。EEAはヨーロッパで年1回国際学会を開催している。ESEMは名称から自明なように、Econometric Societyのヨーロッパ支部の学会であり、Econometric Societyは、世界6地域で定期的に国際学会を開催している。内訳は、北アメリカ地域で半年ごとに、ラテンアメリカ、ヨーロッパ、オーストラリア地域で毎年、極東、南及び東南アジアで隔年、となっている。さらに、5年に一度世界大会が開催される。EEA、ESEM共催の学会が対象とする研究分野は、ミクロ、マクロ、ゲーム、計量経済学の純粋理論から、教育、財政、金融、労働、環境、産業組織、国際経済、開発などの応用分野、そして近年、理論、実証に加え、第3の分析方法として注目を浴びている実験経済学や行動経済学、関連分野としての、移民、政治経済、法律まで多岐にわたり、今回は六つの招待講演とノーベル賞セッション、17の招待セッション、315の一般セッションなどから構成され、1500人余りが参加した。参加者は主に大学、研究所に所属する研究者であった。

理論、実証、実験の融合に向けて

各分野の第一人者からなる六つの招待講演は、Randall Wright（ウィスコンシン大学）、Per Krusell（ストックホルム大学）、Christopher Pissarides（ロンドン・スクール・オブ・エコノミクス）、Daron Acemogulu（MIT）、Susan Athey（ハーバード大学）、Bengt Holmstrom（MIT）の各教授によって行われたが、その中でも、純粋理論から応用まで幅広い研究対象に対して、理論、実証、実験の全ての研究手法で最先端の研究成果を出し続けている、気鋭のSusan Athey教授の講演が特に印象に残った。Susan Athey教授は自らの主要業績である、木材やインターネット広告のオークションを例に、理論、実証、実験の3分野の融合の重要性を強く説いていた。

筆者自身は、第26回EEAのContract and Auction Theory Ⅰというセッションにおいて、“An Alternative Position Auction Mechanism”というタイトルで論文発表を行い、サーチ・エンジンによる広告枠のオークションに対して、既存のものとは異なる方法で効率性、売り手の期待収入最大化を両立できることを示した。同

オスロ大学Blindern キャンパスの図書館

Contract and Auction Theory Ⅰセッションの議長と筆者（左）

じセッションで、外部性を導入したオークションや筆者の研究成果の一部を応用した発表が行われるなど、活発な意見交換が行われた。さらに、産業組織論、オークション、調達、ネットワークなどのセッションに出席し、売り手によるコミットメントがない場合のオークション、ネットワークの外部性下でのサーチ・エンジンの寡占性、二位価格封印入札における売り手の広告投資、オークションにおける売り手の情報開示、調達オークションと破産問題、企業と消費者の仲介者としてサーチ・エンジンが果たす役割、ネットワークの外部性下での通話料金体系などについて、知見を得た。

この学会は全体として、Susan Athey教授が強調したように、理論、実証、実験の三つの手法の融合を強く感じるものであった。5日間集中して最先端の知識に触れることで得ることのできた知的財産を、今後は研究、講義を通じて、広く還元していくことが義務であると考えている。このような貴重な機会を提供して頂いたことに対し、財団法人KDDI財団に深謝する。

Yumiko Baba

馬場 弓子

青山学院大学 経済学部 教授

慶應義塾大学経済学部卒業、スタンフォード大学大学院修了（Ph.D.）、東京大学大学院経済学研究科助手、青山学院大学専任講師、准教授を経て現職。専門はオークション、コンテスト、行動経済学等。訳書にMilgrom, P.（2004）Putting Auction Theory to Work, Cambrifge University Press（川又･奥野監訳　計盛･馬場訳（2008）『オークション理論とデザイン』東洋経済新報社）。著作に、"Three Essays on Auctions and Bargaining," UMI press, 1997、"Post Modern Manufacturing System," The Aoyama Journal of Economics, 55（4）, 2004、"An Alternative Position Auction Mechanism," paper presented at EEA 2011など。第1回Nextcom情報通信論文賞受賞（対象論文：「4G周波数オークション導入に向けて」）。

Nullius in verba
言葉によらず
……王立協会のモットー

何も言挙げせずとも

髙橋秀実

ロンドンの王立協会（The Royal Society）の設立は1660年。世界で最も歴史の古い学会で、科学者たちの学会というより、今日の「科学」そのものを生み出した権威ある学会なのだが、そのモットーは――

「言葉によらず（Nullius in verba）」。

古代ローマの詩人ホラティウスが記した一節。なんでも「言葉に頼らず、おのれの目で見よ」という戒めらしいのだが、言葉によって生計を立てている私などには耳が痛い。

言葉によらずして何によればよいのだろうか。協会の注釈によると、実験で得た事実のみに注目せよということだが、その「事実」も言葉で説明されるものではないのだろうか。数式なども広い意味では数学の言葉だし、人間は言葉なしでは物事を考えられないわけで、大体、この「言葉によらず」も言葉ではないか。

などとぼやいているうちに、ふと気が付いた。

私たちはよく「言葉にならないこの気持ち」などと言う。これも言葉には違いないが、言葉によらずして気持ちを表現している。「申し訳ありません」もよく使う。言い訳ができないということで、言葉にできないと言って謝罪するのである。そういえば、古くから日本人は言葉にすることを「言挙げする」という。「言挙げせずとも稔（とし）は栄えむ」（万葉集）という具合に、物事はわざわざ言葉にすることはない、あるいは言葉にしてはいけないと忌み嫌ってきたのである。

若者などがよく使う「○○っていうか」などもその伝統といえるかもしれない。「美人っていうか、かわいいっていうか、なんか、こう、普通っていうか、ブスっていうか……」などと次々と言葉を否定して、語尾を濁す。物事を言葉で断定しようとしない。むしろ言葉を否定することで会話をつなげていくのだ。

考えてみれば、欧米では聖書に「初めに言葉ありき」とあるように、言葉が神として世界を

article：**Hidemine Takahashi**
ノンフィクション作家。1961年生まれ。東京外国語大学モンゴル語学科卒業。
著書に『にせニッポン人探訪記』『からくり民主主義』『やせれば美人』『趣味は何ですか？』など。
『ご先祖様はどちら様』で第10回小林秀雄賞受賞。最新刊は『結論はまた来週』（角川書店）

分別していくが、日本の古事記は序文に「ひたたけたるもの既に凝りて」（混沌としたものがすでに固まっていて）と書かれており、なんだか分からないができちゃっていたものが全ての始まりで、それは「名もなく」とわざわざ明記されている。言葉に先行してヘンなものがあったというわけで、私たち日本人は最初から言葉によっていないのである。

毎年のように流行語が生み出され、同じことでも次々と言い換えていく。言葉によらないことが日本人らしさとも言えるわけで、だから日本は科学立国になり得たのかもしれない。

背景

「聖書や古典などに頼らず、実験や観測によって事実を確定する」という近代自然科学の客観性をモットーとして、1660年に設立されたロンドン王立協会。会員には、ロバート・ボイル、ロバート・フック、ジョン・ウォリスなど、17世紀後半の著名な科学者が名を連ねている。ニュートンは後に協会理事長になった。

編集後記

今号の特集テーマは、「情報セキュリティ」としました。いかがでしたでしょうか？

特集するテーマの検討を進めるにつれ、当初の想定以上に奥深い分野であることが分かりました。ページ数の都合から、一部しかご紹介できておりませんので、今後も折りに触れて同様のテーマを取り上げたいと思います。

次号は、「震災と情報通信（仮称）」を予定しています。発行予定日の9月1日は、ちょうど防災の日になります。（しのはら）

Nextcom（ネクストコム） Vol.10 2012 Summer
平成24年6月1日発行

発行　株式会社KDDI総研
〒102-8460 東京都千代田区飯田橋3-10-10 ガーデンエアタワー
TEL：03-6678-6179　FAX：03-6678-0339
URL：www.kddi-ri.jp

編集協力　株式会社ダイヤモンド社
株式会社メルプランニング
有限会社エクサピーコ（デザイン）
印刷　瞬報社写真印刷株式会社

●本誌は当社ホームページでもご覧いただけます。
http://www.kddi-ri.jp/nextcom/index.html
●宛先変更などは、株式会社KDDI総研Nextcom（ネクストコム）編集部にご連絡をお願いします。（Eメール：nextcom@kddi-ri.jp）

株式会社 KDDI総研　http://www.kddi-ri.jp