JSSM25　社会への提言

日本セキュリティ・マネジメント学会
創立 25 周年記念事業

理論と実務を統合するセキュリティマネジメント
次代を担う CIO/CISO の育成

2012 年 2 月

日本セキュリティ・マネジメント学会理事会有志

目次

０．エグゼクティブサマリー

複雑化し相互依存を高める種々のシステムが互いに連携する現代社会では、幅広い分野の協調した対応が求められるが、そこには様々なファクターが複雑に絡み合った解決の難しい問題がある。現実に起きている問題には、企業の取り組みの不備が原因のものに加えて、個々の企業の枠を超えて、技術と法の連携にかかわる社会システムとしての検討不足という深刻なものもある。企業の経営環境は、グローバル化に加えて情報技術の急速な発達がバーチャル化を急加速させており、バーチャル社会のリスクを十分に理解して取り組んでいかなければならないことを、これまでの種々の事件が示している。

このような課題に取り組みセキュリティを確保するのがセキュリティマネジメントである。セキュリティマネジメントは情報セキュリティ技術と経営技術の両方の組み合わせであり、実務に深くかかわるとともに、効果的に実施するには自然科学や人文・社会科学の成果を必要とする。つまり、この分野では実務と学をつなぐ知識の循環が形成される必要があるが、まだその出発点で足踏みをしている状況にある。

一方、問題解決の中心的役割を期待されている CIO/CISO は、まだ本質的な解決に向けての役割が十分には果たせていない。米国などに比較すると、日本の組織には学位取得者が少なく科学的アプローチに基づく理論的手法を取り入れようとはしていない。企業の人材育成も、組織外にも通用する普遍的・客観的価値観で問題解決にあたることができるいわゆる目利きが育ちにくい環境にある。

そこで、理論と実務を統合するセキュリティマネジメントの実践に向けた産官学連携の共同作業を提言するのが本提言の趣旨である。実務に基づく本質的な課題設定と、学の抽象課題から理論解を見つける普遍的方法論とを本質課題を通して連結することが産官学連携の一つの重要な解決の糸口になる。さらに、理論解を現場に合わせて適用し効果を上げるには理論解を現実解に解釈しなおす力が求められる。ここがもう一つの連携の重要ポイントである。これらのポイントを押さえた産官学連携を実現するには、実務の側の CIO/CISO が自らの課題を抱えて学のアプローチの習得に取り組む必要がある。学においては複眼的な目利き人材を育成するダブルメジャー化を推進するとともに、実務においてはセキュリティマネジメント思想を経営の中核に植え付けるとともに本質課題に取り組む人材の育成に力を入れる必要がある。

具体的には、6 つの分野について提言する。

第 1 は、政策である。「情報セキュリティ」とそのマネジメントに関する法的諸概念を整理し、情報セキュリティの法的定義を確立することが望ましい。法を取り巻く環境は急速に変化している。何らかの形で、基本法的な性質を持つ法律を制定するか、既存の法を改正することによって、セキュリティマネジメントに関係する法の体系性を構築することを提言する。第 2 は投資である。セキュリティマネジメントは実務界と学界とが共同して体系を作りあげて行かなければならない理論と実務を融合すべき分野である。このような分野を確立するには、関連組織を束ねて引っ張っていく

センター機能が必要であり、その推進に国のリーダーシップが不可欠である。同時に、実務を担う産業界からのセキュリティマネジメント研究への投資も不可欠である。第 3 にコース開発がある。実務の持つ暗黙知を体系化・定式化してセキュリティマネジメント体系の中に位置づける産官学連携の枠組みを作り上げる必要がある。第 4 は官界および産業界の育成キャリアパスである。実務教育と企業文化中心の人間教育とで忠誠心をはぐくむとともに、複眼的に社外において客観的普遍的な価値観を身に着けた人材が今後の企業発展に必要であると位置付けてもらいたい。第 5 は産・官・学をまたがる人材循環の仕組みである。社会全体を視野に入れた人材の適正配置の視点から、産・官・学をまたがる人材循環を可能にする仕組みを構築し、同時に専門的人材確保についての各主体の考え方を転換していかなければならない。第 6 は経営改革である。組織経営はセキュアな社会基盤の一角を担うという明確な認識の下、セキュリティマネジメント思想を組織経営に取り入れ、CIO/CISO が CEO をはじめとする経営陣と連携して取り組んでもらいたい。

日本セキュリティ・マネジメント学会（JSSM）は、起点機能、交流機能、集積機能の 3 つの機能でこの中心的な役割を果たす覚悟である。

1．セキュリティマネジメントは現代社会を象徴するテーマ

高度情報化が進む現代社会では、情報の価値の相対的な高まりとともに、情報セキュリティの確保は組織の社会的責任とみなされるようになり、場合によっては組織の存在意義にもかかわるような重要な意味合いを持つテーマとなった。様々な分野で急速に進む IT 化の進展と、それに伴なって発生してきた種々のトラブルなどから、IT 化されたシステムのコンセプトの中核にセキュリティマネジメントの思想が必要なことが明らかになってきた。現代社会の抱える様々な課題をみると、それらの多くに情報セキュリティに帰着する課題をみることができる。

複雑化し相互依存を高める種々のシステムが互いに連携する現実の中で発生するセキュリティ課題への対応には、様々なファクターが複雑に絡み合った解決の困難さが内在しており、本質的に幅広い分野の協調した取り組みが求められる。このような情報セキュリティ課題を解決することは、現代社会が直面する多くの問題の解決につながると考えられる。

セキュリティマネジメントは、自然科学の成果を踏まえたハードウエアやソフトウエアの設計や機能開発などを必要とするとともに、そこで行われるリスクの評価は様々な価値観に基づき、あるいは対策の現実への適用面では困難な調和が求められるなどで人文・社会科学の成果も必要とする。

日本が科学技術立国として発展を続けるには、科学技術にかかわるリスクの解明とその対応策も併せて科学していくほかに道はない。新たな技術が内包するリスクはもとより、その技術を適用したシステムが社会に及ぼすリスクも評価し適切な対応策をとることで、新技術の恩恵を社会で享受できるようになる。

情報セキュリティにかかわるリスクについても、的確なリスクアセスメントに裏付けされたセキュリティマネジメントを理論と実務の融合した体系として構築することにより、次なる発展につなげていかなければならない。セキュリティマネジメントは高度情報化が進む現代社会を象徴するテーマであり、日本社会がいままさに取り組まなければならないテーマである。

２．現代社会が抱えている課題

2.1　種々の発生している問題

発生している問題に、日々マスコミをにぎわせている個人情報漏洩等の関連事犯の続発がある。その背後にはセキュリティマネジメントの不備という共通の原因が存在する事が多く、高度情報社会の深刻な問題となっている。

少し遡りこれまで発生した問題の幾つかを見ると、初期の頃は対象をモノ（媒体）に絞ったものである。代表例は、コイン／紙幣偽造・テレフォンカードにはじまる各種カード偽造・情報無断持ち出し・改竄等々である。これらの共通点は、モノ（媒体）の印刷・鋳造技術並びに関連する情報の暗号化のみを注視し、使用機材の配置・保管や廃棄等を考慮したライフ・サイクル全体に及ぶ運用管理が徹底されていなかったことに起因する。その証拠に、アタック対象となる機材を内部者並びに外部者が不正入手し、これを使用し偽造並びに流用が行われた。特に、カード偽造では、媒体と機材は管理体制が別々であり、機材は事業体内部に設置するものと認識し、アタックを受けることを想定していないという事実である。また、カード内に格納さている情報の暗号化はなされていたが、当該カードをコピーするのみで偽造カードができ、不正利用できることから暗号解読等の技術を必要としなかった。また、装置廃棄処分も外部事業者に委託し、最終処理段階の確認を行っていなかった。

しかし最近はモノ（媒体）ではなく、先に触れた大規模な個人情報漏洩問題が発生している。この問題も当初はモノ（媒体）と共通の事実が存在する。それは、内部者（退職者を含む）が情報を外部に持ち出すとは想定されていない点である。これは運用システムの稼働記録であるログは自動的に記録されるが、外部へ持ち出された痕跡の調査までログ解析等の対処はなにも為されていないことも事例から伺い知れる。この事実は、企業・組織において情報を経営資源として捉えていなかったことを明白に物語っている。しかし最近は内部関連者ばかりではなく、外部からの組織的な攻撃技術が進み、コンピュータウィルスによる被害等も後を絶たず、情報を許可なく改竄・悪用・流用する問題へと進んでいる。

特に最近発生した社会安全確保を主務とする検察当局が押収した証拠書類を改竄し、自身の主張を立証しようとした行為までも発生している。これは情報に対する不正改竄・不正利用であり、組織存続にも大きな影響を及ぼす問題である。事犯に利用されたツールは市販品であり自由に入手でき、対象となる情報がどのように管理・運用されているか、即ちセキュリティマネジメントをどのように実践するかが根本的問題といえよう。

また、情報の可視化（見える化）が進められると共に、リアルからバーチャルへと大きく変化し、ネットワークを主軸とするソーシャルメディアの展開が進んでいる。そのため、情報に対するアクセス者は内部者のみと限定されず、アクセス者を特定できない環境での運営を想定し対応する事が重要であり、これが事業継続（BCP：Business Continuity Plan）に直接結び付く。特に、2003 年頃アメリカにてサービスが開始された交流サイト SNS（Social Networking Service）や 2006 年サービスを開始したツイッター（Twitter）等は、国の存続にまで影響を及ぼす力を持っている。これらへの参加者は不特定であり、匿名をベースに情報を発信し、社会風評に結び付いている。これ

にもまして、内部公文書を公表するウェブサイト・ウィキリークスも登場し、内部告発がオープンな環境で為されていることにも注意点が存在する。これがまさしく高度情報社会の中枢を担うネット経済社会なのであろう。

これらとは異なり、企業・組織から市場へ発信される各種商品（サービス・製品等）が、日常社会においてどのような位置を占めるかという社会への影響、特にもたらされる各種のリスク等について事前検証が為されていない。法・制度を含め、ほとんどが“コト（事）”が起きてからの対処である。例として、日常生活に大きく関与している携帯電話にからむ各種問題点が散見される。その一つが普及当初、自動車運転中に利用することが黙認され、事故多発により本格的対応は 2004 年の道路交通法改訂という事実である。また、軽車両に属する自転車については現在も黙認状態で、歩道を歩いている時の恐怖感は誰もが経験し、いまだ解消されていない。これらは道路交通法の問題であるが、背景には当該商品の利用場面を十分に設定できなかったことがあり、販売開始時に利用市民への注意喚起や啓発活動も十分には行われていない。

このように種々発生している問題は、技術問題のみではなく、企業・組織から発信される各種商品（サービス・製品等）が社会に及ぼす変化を予測し、各種リスク等を事前に充分に検証し、生活環境の変化からもたらされる影響にも配慮することが求められる。これまで日本文化の根底となっていた性善説を基本とする社会構築では対応できず、ここで生きる環境整備の充実が急がれる。その一つの取組みが「技術と法・制度の連携」であり、“コト（事）”が起きてからの対応ではなく、社会の先を読み、企業・組織活動で想定されるリスクとセキュリティを基軸とし、表現の自由並びに通信の秘密を踏まえた法・制度整備への取組みであろう。

2.2　学の現状

図 1 は、我が国における情報セキュリティ関係の論文発表の概況を示す。調査対象は、情報セキュリティ論文の主要な掲載先である情報処理学会論文誌コンピュータセキュリティ特集号、電子情報通信学会英文論文誌の暗号と情報セキュリティ特集号および本学会誌である。３誌の全論文について、タイトルと概要、著者リストを調査し、セキュリティマネジメントの論文、そのうち企業や官公庁と大学との共著論文（産学共著論文）を抽出した。なお、産学共著論文の抽出においては、論文に掲載された著者リストの中に、広い意味の産（官公庁、監査法人等を含む）の著者と広い意味の学（国公立研究機関等を含む）の著者の両方が含まれていることを条件とした。2006 年から 2010 年までの平均では、調査対象の論文総数は 59.2 件/年、うちセキュリティマネジメントの論文数は 6.0 件/年、うち産学共著の論文数は 1.4 件/年である。このことから、

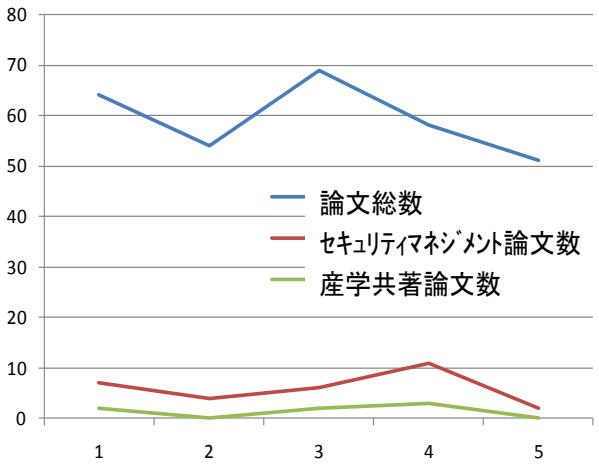


図 1　日本のセキュリティ論文発表の概況

情報係のセキュリティマネジメントについて、産学連携が順調であるとは必ずしも言えないことがわかる。

この問題に関連して、セキュリティマネジメントに関する学側の教育研究状況を把握するために、全国の国立大学８８校の大学院における情報セキュリティ関係の科目数を調査した。各大学の公開している Web ページにおいて、「情報セキュリティ」というキーワードで検索可能な科目を洗い出した。その結果、88 校の大学院における情報セキュリティ関係科目総数は 122 であり、1 大学あたり 1.4 科目であった。さらに、122 科目の内容を調べたところ、「情報セキュリティ論」といったセキュリティ全般に係る科目や「暗号理論」などの基礎理論に係る科目が多かった。これらの科目では、セキュリティマネジメントや IT リスク管理が中心にはなっていない。以上から、国立大学において、情報セキュリティ特にセキュリティマネジメント関係の科目は少ないことが分かる。また、科目が少ないということは、この分野の専門教員が少ないことを意味している。

セキュリティマネジメントの研究は、情報セキュリティ技術と経営学の手法の両方を必要とし、さらに、個々の企業の実務に深く関与することが多い。そのため、学だけで研究を深めることが難しく、産学連携を必要とする分野である。産から学に現場の問題意識や経験が提供され、学から産に分析や解決策が提供されるといった知識の循環が期待される。しかし、現実には、セキュリティマネジメントの産学共著論文が少なく、学における専門科目、専門教員も少ない。そのため、期待される知識の循環は、残念ながら足踏み状態から抜け出せないでいるのが現状かもしれない。文部科学省「先導的 IT スペシャリスト育成推進プログラム」に基づく ISS square[1]や IT Keys[2]のように、すでに取り組まれている例もあるが、全体として順調であるとは言い難い。

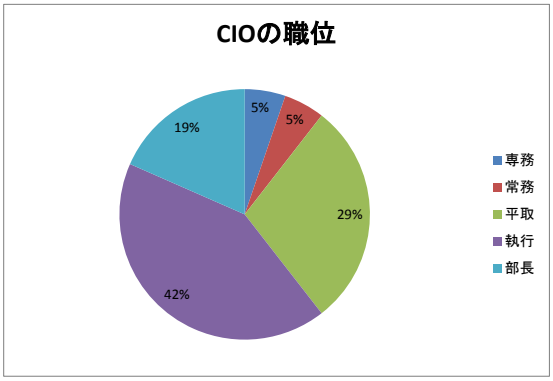
[1] ISS square: Integrated special scheme for information security specialist cultivation, http://iss.iisec.ac.jp/

[2] IT Keys: IT specialist program to promote key engineers as security specialist, http://it-keys.naist.jp/.

2.3　産の現状

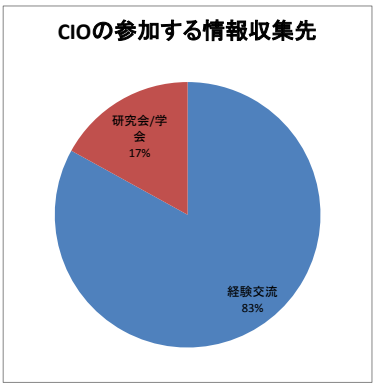
2.3.1　CIO/CISO の参照型アプローチ

産や官での現実のセキュリティマネジメントへの取り組みについては、正確に実情を示すデータは見つからなかったが、日経情報ストラテジー「CIO 登場[1]」に出ている 38 人の CIO の実態から分析すると、概ね二つのことがわかる。一つは、CIO/CISO は根本的な課題に取り組むための権限を持ちうる地位にすでにあるということである。全体の 8 割を超える CIO が取締役あるいは執行役員の地位にあり、残りも部長以上の職位にあること



がわかる。情報セキュリティの知識がありやる気があればセキュリティマネジメントの課題に本格的に取り組むには十分な地位にすでにあると思える。

もう一つは、CIO や CISO は経験交流に熱心で、お互いに体験談や成功例の共有に努めているということである。CIO/CISO がセキュリティマネジメントに取り組む際の知識や情報の収集もとは 83%が部長会や IT ユーザー会あるいはセミナーなどの経験交流であり、学会や研究会などへの参加は 17%にとどまっている。しかし、経験交流を趣旨とするセミナー等からだけでは、セキュリティ課題の根本的な解決には至ることは難しかろう。



CIO/CISO は、現実に直面している課題の本質を見抜き、理論的な裏付けのある手法を適用し、現場に即した客観的で合理的な解決策を見出す努力をしなければならないはずである。しかし実際には、課題の本質を見抜くのは難しく、さらに問題を抽象化し理論的な解を見出すには学問的なアプローチの鍛錬が必要であり、それを現場に即して応用するには豊富な実務経験が必要である。これらの一つあるいはいくつかに欠ける状態では、他のうまくいった事例を探して適用を模索するという参照型アプローチにならざるを得ないことは想像に難くない。

IT 製品の取捨選択には熱心に取り組むが、システム全体のリスクの把握や情報セキュリティマネジメントの科学的アプローチにはあまり取組めていないのが実情であろう。しかし CIO/CISO は経験交流などの参照型アプローチだけでは現代のセキュリティ問題に対処できない。現実に発生している様々な問題の背景には、このような参照型アプローチの限界があると思われる。

[1] 日経情報ストラテジー「CIO 登場」に出てきた 38 人の CIO
http://itpro.nikkeibp.co.jp/article/COLUMN/20090803/335057/　2011/02/02 アクセス

2.3.2　組織における学位取得者の日米比較

セキュリティマネジメントは複合的かつ包括的な枠組みであるから、CIO/CISO は単に技術的観点のみならず、経営・組織・人事・法律等の高度で専門領域横断的な専門知識が必要とされる。その意味で、大学院において高度な専門知識を習得し、セキュリティに関係する諸問題について高度な知見を専門領域横断的に活かして対処することができるような CIO/CISO が求められている。

しかし、一般にわが国の組織においてはいわゆるライン職に求められる素質として総合性が重要視され専門的な知識や知見は必ずしも重視されない傾向があるといわれている。セキュリティマネジメントに関わる組織的な地位にあり組織における権力を有する幹部における修士や博士の学位取得者の割合は、必ずしも高いとはいえない。

総合性が重視される典型的な例としては中央官庁がある。中央官庁に関しては、課長職以上の幹部職員について氏名が公表されるのみであるため正確な略歴等のデータの入手が困難であるが（このこと自体も問題である）、各種の職員録等の資料集等を参照する限りでは、中央官庁の幹部職員

において博士号を取得しているケースは希である。技官を除いては、大学院修了者が採用されている例も少ない。

高度情報通信ネットワーク社会推進戦略本部には各府省の情報化統括責任者（CIO）が構成員となる各府省情報化統括責任者（CIO）連絡会議が置かれているが、多くの府省では前述の幹部職員である官房長や官房審議官が CIO として出席しており、政府の CIO の中には学位取得者は少ないのが現状である。2003 年 7 月、各府省情報化統括責任者（CIO）連絡会議において情報化統括責任者補佐官（通称：CIO 補佐官）を各府省に置くこととされた。各省庁において部局横断的に情報セキュリティ施策を推進する必要があるところから、通常は事務官のポストである官房長等が CIO に充てられることが多い。CIO 補佐官の場合は情報セキュリティに関する専門家が任命されることが多いが、その反面で国家公務員法上はあくまでも非常勤であることが多く、技術補佐員として「時間雇用」で雇用されることもある[1]のが実情である。

これに対して、アメリカにおいては 1970 年代以降学位取得者が増加した結果、企業幹部が英米圏の専門職学位である MBA や JD 以上の学位を取得することは半ば常識となっており、連邦政府職員や軍幹部においても学位取得者の割合は高い。政府 CIO については、CIO 評議会[2]のサイトに各省庁 CIO の一覧が掲載されているが、学部卒業のみという人材は見当たらない。この点では、わが国の政府 CIO とは対照的である。付言すれば、わが国の CIO は圧倒的に男性が多いが、女性が進出していないのはなぜなのかも検討する必要がある。

2.3.3　企業の人材育成の課題

企業の人材育成は、一般に、企業活動における業務能力(スキル)を高めるための教育と精神面(企業文化)を高めるための教育があるが、我が国においては、終身雇用制度と大きく係わりを持ちながら発展してきたため、後者に重きを置いてきたといっても過言ではない。

これの意味するところは、各企業によって異なる企業文化を人材育成プログラムの中に取り込み、これを中心に据えて、その企業でのみ使われる仕事のノウハウを教育するということによって、その企業に対する忠誠心とその企業特有の仕事のやり方による効率化の実現である。このような我が国の人材育成においては、冒頭述べた終身雇用制度と相まって、高度成長期からバブル崩壊時期までは非常にうまく機能していたと思われる。

しかしながら、バブル崩壊後の我が国においては、グローバルな競争環境を背景に欧米の流動性のある雇用制度が広がりを見せてきたにもかかわらず、企業の人材育成は相変わらず今まで通りのプログラムを中心に行われているのが現状である。転職後、転職先企業の企業文化を身につけるまでに時間がかかる問題はもちろんのこと、スキルにおいても転職先企業特有の仕事のやり方があり、それに慣れるまでに相当な時間がかかるようである。

また例えば、ある代替案の検討において必ずしも理論的な最適解は探求されず、企業内の価値観に基づいて意思決定が行われる。このような風土においては、理論的な最適手法に長けた人材は

[1] 文部科学省の場合。http://www.mext.go.jp/b_menu/saiyou/hijyoukin/1302372.htm
[2] http://www.cio.gov/

むしろ出る杭として排除されやすく、客観的・普遍的価値観に基づいて様々な課題に対応できる「目利き」が育ちにくい環境にある。

これでは、国際競争力を考えた場合に、我が国においては汎用性を持った総合力を備えた人材を育てることはなかなか難しいと言わざるをえない。我が国における縦割りの弊害と言われる所以でもある。

2.4　環境変化

急速に進歩する情報技術によって、「リアル」に加えて「バーチャル」へと高度情報社会は大きく広がり、且つ複雑なものとなっている。この環境変化において、そこで行動する個々人の立ち位置の明確化が極めて重要となる。

「リアル社会」では、対面し相互に相手を認識した上で情報が取り交わされる。そこで取り交わす情報のレベルに応じて、日本では印鑑が使用されている。しかし「バーチャル社会」においては、相手を認識する情報はネット上にのみ存在し、実名のみではなく匿名・ハンドルネーム・シュードネーム等々のもとで情報が取り交わされる。このような環境において情報を正しく扱うためには、新たなルール制定が必須となる。

そこで「バーチャル社会」構造を改めて見た時、次のように行動領域区分を定義できる。

① 匿名をよしとする万人参加領域
② 記名が前提で権利・義務を伴うビジネス領域
③ 権利・義務に加えて責任を保持し信頼・安全を持つセキュリティ領域

この 3 領域は現在営んでいる「リアル社会」での印鑑文化と同じで、新しいことではない。「バーチャル社会」においては①のみを有効とし、②③を否定する意向が散見されるが、これは如何なものであろうか。安心・安全に加えて信頼できる「バーチャル社会」を構築する際に、印鑑に代わる手段の制定が急がれる根拠がここにある。これは利便性の追求ではなく、今後の社会をどのように描くか、国策としての大きな問題であり、国民共通番号制度の上で企業・組織はもとより、個人も行動基盤を十分に理解することが重要である。ここに参加する各個人をはじめ企業・組織は、どの領域で行動しているかを自覚すると共に、その領域選択の責任も求められる。

また、社会環境はこのように大きく変化し、技術進歩と共に、これに対峙する集団の存在も理解し、バーチャル社会の中の「ネット経済社会」の「情報・情報資産」に取組むことが求められる。特に、取組む際、利便性のみを追求するのではなく、取り巻く社会のリスクへの配慮が極めて肝要である。“コト（事）”が起きてからの対処ではなく、抱える“リスク”を充分に理解し、配慮・展開する対応である。これが「技術と法・制度の連携」であり、「学と企業・組織の連携・調和行動」を求める根拠でもある。

3．課題解決への提言

3.1　産官学連携の共同作業

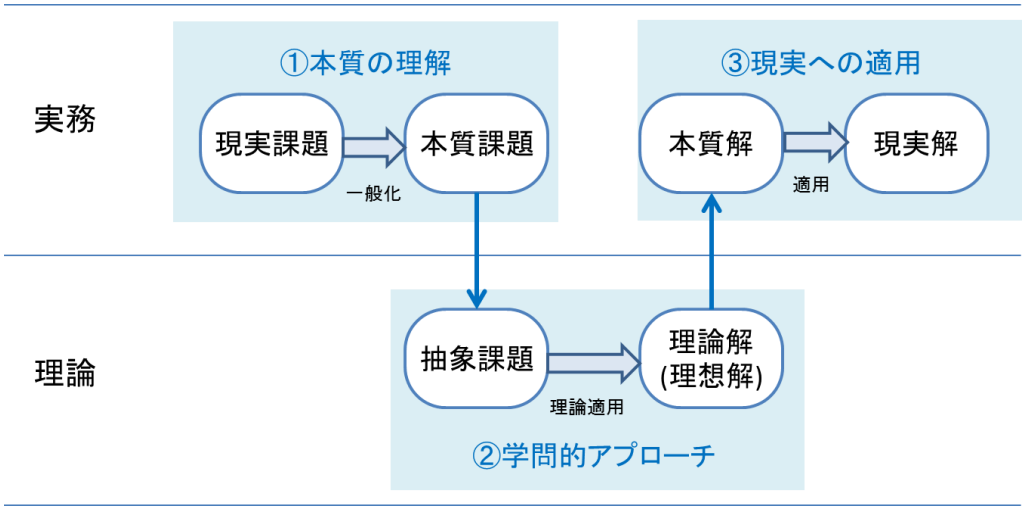
セキュリティマネジメントを総合科学として発展させるためには、理論と実務を統合したアプローチが不可欠である。学のみのアプローチでは、現場の実務課題を見つけ出しその課題の本質を見抜くのは難しかろう。仮に学のアプローチで理論的な解が見つかったとしても、それを現場に適用して効果を上げるには鍛え抜かれた現場力が必要である。

産や官のアプローチだけでも難しい。現実課題の本質を見抜き、普遍的な課題設定に持っていくこと、その課題を学のアプローチで理論的最適解を見つけること、などがなければ本質的な解決にはなるまい。

産や官の実務に基づく本質的な課題設定と、学の抽象課題から理論解を見つける普遍的方法論とを本質課題を通して連結することが産官学連携の一つの重要な解決の糸口になる。さらに、理論解を現場に合わせて適用し効果を上げるには理論解を現実解に解釈しなおす力が求められることになる。ここがもう一つの産官学連携の重要ポイントである。

これらのポイントを押さえた産官学連携を実現するには、産や官の側の CIO/CISO が自らの課題を抱えて学のアプローチの習得に取り組むのがベストであろう。また、学の側も本質解の解釈とそれが現実階となるうえでの現場力を理解し、理論適用の幅を広げる努力が不可欠であろう。

このような産官学連携を進めることが解決への大きな力になるに違いない。



3.2　学の取り組み提言

今日の情報化社会においては、情報セキュリティの概念自体が専門化かつ多様化しており、最狭義の情報セキュリティに関する技術が進歩していると同時に、社会全体のセキュリティマネジメントを適切に行うにはエネルギー供給や物流、国民への情報提供や世論形成のあり方等、多くの側面から検討を行うことが必要となっている。

わが国においては、専門領域における単能家的な専門家は多く存在するが、専門家相互の交流に乏しく、多元的な議論の形成が妨げられてきた傾向がある。このため、2 つ以上の専門領域を有する複眼的な専門家の育成が望まれるが、現実には日々深化する最新技術動向や社会変化を 1 つの領域においてフォローすることも容易ではない。

またセキュリティマネジメントの現場においては、暗号技術等の最先端のセキュリティ技術はすぐれて自然科学的であるのに対して、セキュリティに係わる価値判断や意思決定は人文・社会科学的知識を背景として行われており定量化が困難であるという実態がある。ある領域において専門的に深い学識と知見を有すると同時に、各領域における種々の議論や主張について、その適切性や正確性を見極め、社会における情報セキュリティの確保全体の重要性の見地から諸施策の優先度や緊急性を合理的に判断することができる複眼的な「目利き」力を有する人材を養成することが必要となっている。

そこで、学においては、総合的かつ多面的な能力を有する人材を養成できる仕組みを確立し、具体的にはセキュリティマネジメントに関わる人材（CIO/CISO 等）のダブルメジャー化を推進することを提言する。

ダブルメジャー化に関しては、情報セキュリティ政策会議が 2011 年に公開した「情報セキュリティ人材育成プログラム（案）」[3]でも「一つの分野の専門家ではなく、様々な専門分野の知見を総合できる文理融合型の『ハイブリッド型人材』」、「鳥瞰図的な視点で、ダイナミックに変化する情報セキュリティリスクに対応した問題発見・解決能力を有する『問題発見・解決型人材』」が求められているとされている。

ダブルメジャー化は複数学位の取得に限られず、CIO/CISO を養成する教育プログラムの中で複数の専門性を育成する手法（たとえば複数校の連携によりいわゆるダブル・デグリーを付与する方法）によっても実現することができよう。また近時、社会の国際化と人材の国際的流動化が従前にも増して進展していることを考えると、ダブル・デグリーについては、国際的な連携の枠組みの下に推進することも検討するべきであろう。

さらに、セキュリティマネジメントに関わる人材を養成するプログラムに求められているカリキュラムについて、社会と産学のニーズを適切に把握し、産学官の連携の枠組みを活かした標準的なカリキュラムを策定することも学の役割である。その際、座学だけではなく実習・実務、就業経験等についても意義と効果を検討する必要がある。

もとより「目利き」力を有する人材を養成するには、自らが単能家的な専門家から脱するための努力が必要であり、学自身が多領域の専門家との協働作業に積極的に参画して自己の専門的知見を複眼的に深化させるだけではなく、実務と積極的に交流して産学官連携を推進することが求められる。さらに、日々深化するセキュリティ技術と産学官連携においてフォローしつつも、各種のセキュリティに関わる事象に対して多元的な観点から考察を加え、体系化を図ることも学の役割である。

セキュリティマネジメントは総合科学であり、多種多様な構成要素に対して一定の体系性を与えて理論的根拠を提供することが学には求められている。

3.3　産の取り組み提言

情報社会においては、産業界が作り出すさまざまの製品やサービスが社会の安全に直接間接の影響を与えることから、企業活動の中核にセキュリティマネジメント思想をしっかりと植えつけるこ

[3] http://www.nisc.go.jp/active/kihon/pdf/jinzai2011.pdf

とが肝要である。これはさらに、これまでの企業内の価値観や人間関係を主体とする企業文化に、セキュリティリスクの認識をトリガーとした客観的普遍的価値観を取り込まなければならないことをも意味している。

企業経営者には、これらのことをしっかりと受け止めて経営方針に取り込むとともに、人材育成にも工夫を盛り込んでもらいたい。特に、経営のトップである CEO は、今後の情報社会において自社が勝ち組となるためには、如何に CIO/CISO の育成が重要であるかを自覚し、これからの企業の存亡に関わる重要なポジションになるとの認識の下、経営に携わっていただきたい。

産学連携の共同作業に鑑みて、産としては先ずはしっかりと実務の原理原則とその内容がわかる人材を育てることが重要である。この実務が分かれば、次にその実務を通して本質的な問題設定ができる人材の育成が必要となるが、ここまでは、産の現場で行うことである。

次に、問題設定ができたならば、この問題の解決策を考えるわけであるが、ここからは学の力を十二分に活用して、論理的に問題解決を行うのが最も効率的であり、解決策を間違えることも少なくなると考える。したがって、産の取り組みとしては以下をあげたい。

1. 実務の原理原則とその内容がわかる人材の育成
2. 実務の問題選定ができる人材の育成
3. 学の力を借りて問題解決を的確にできる人材の育成

上記の提言を実現するためには、産で何年か実務経験を積んだ人は、必要に応じて学に来て、普遍的方法論を身につけると共に最大限に活用することを望みたい。こうすることで、CIO/CISO になるためのスキルが身に付くと考える。

もう一つは、「目利き力」を有する人材の育成を積極的に行うことである。これは世の中の動向を的確に把握し、かつ最先端の技術を常にウォッチしている人材である。専門性と汎用性の両方を備えた人材をいかに育てるのかが、今後の我が国の人材育成を高めるための重要な点であると考える。

3.4　具体的提言

3.4.1　政策

情報通信技術（ICT）が社会の重要なインフラとなっていることはすでに周知の事実であるが、ICT の根幹に係る情報・通信とそのセキュリティに関しては必ずしも法制度の対応が十分ではない。

情報セキュリティの領域では、「情報」そのものに関する明確な定義は存在せず、法の正統性の根源である国家の支配能力が低下したために、アーキテクチャやセキュリティに関する各種の国際規格、ISMS のような一種のマニュアル類からなるソフトローによって情報セキュリティが担保されている部分が大きい。その原因としていわゆるドッグイヤーで進化する諸技術に対して、既存の権利義務関係の解釈の見直しや立法等の対応が常に後追いとなっていることが挙げられる。

法が最新の技術環境に柔軟に対応することは必要であるが、その一方で情報化社会における公序の基礎となる法の安定性の担保のために「情報セキュリティ」とそのマネジメントに関する法的諸概念を整理し、情報セキュリティの法的定義を確立することが望ましい。

これについては困難も予想されるが、長年、法制化が困難といわれてきたコンピュータウィルス（マルウェア）作成の可罰化が 2011 年の情報処理の高度化等に対処するための刑法等の一部を改正する法律の制定で実現したことに象徴されるように、法を取り巻く環境は急速に変化している。何らかの形で、基本法的な性質を持つ法律を制定するか、既存の法を改正することによって、セキュリティマネジメントに関係する法の体系性を構築することを提言する。

セキュリティマネジメントに関わる法の体系化にあたっては、情報セキュリティの CIA（Confidentiality、Integrity、Availability）とわが国の法体系における枠組みとの整合性や、プライバシーの概念とその範囲、プライバシーと個人情報の異同、「通信」の定義と「放送」との異同等についても一体的に再検討することが必要である。そもそもわが国の法体系の下では、「電磁的記録」（刑法第 7 条の 2）という定義は存在するが、「情報」とは何か、「情報セキュリティ」とは何を指すのかという明確な規定が存在しない。情報セキュリティを法的にどのように位置づけることができるのかの検討を、産学官連携の下で諸領域における知見を総合して行うべきであろう。

また、平成 6 年に高度情報通信社会推進本部が内閣に設置されて以降、組織としては高度情報通信社会推進本部と IT 戦略本部、主な法律としては高度情報通信ネットワーク社会形成基本法、戦略としては e-Japan 戦略、IT 新改革戦略、デジタル新時代に向けた新たな戦略～三か年緊急プラン～、i-Japan 戦略 2015、重点計画としては e-Japan 重点計画（同 2002、2003、2004、2006、2007、2008）等が推進されてきた。また平成 17 年に内閣官房情報セキュリティセンター（NISC）が設置されているが、これらの組織・法律・戦略相互の関係は複雑であり、国民にとって政府が推進する情報セキュリティ政策は必ずしもわかりやすいものとはいえない。

新たに出現する種々の脅威に柔軟に対応できるよう留意しつつ、政府が推進するセキュリティ諸施策を見直し、再編できるものは一元的に推進するように務めるべきである。これによって、政府が情報セキュリティ政策に重点的に取り組む姿勢が国民にとって可視的になると期待される。

3.4.2　投資

複雑性の増す現代社会において、日本が科学技術立国として世界の先端に立ち続けるには、単に個々の技術に投資するだけでなく、それらの技術が社会にもたらすリスクの解明と対応策の科学的な研究、なかでもセキュリティマネジメントの研究に国として応分の投資をすべきである。

セキュリティマネジメントは先述のごとく総合科学であり、かつ実務界と学界とが共同して体系を作りあげて行かなければならない理論と実務の融合分野である。このような分野を確立するには、関連組織を束ねて引っ張っていくセンター機能が必要であり、その推進に国のリーダーシップが不可欠である。

同時に、実務を担う産業界からのセキュリティマネジメント研究への投資も不可欠である。この研究の成果を最も享受するのは産業界にほかならず、CIO/CISO 候補人材の育成のみならず、直面している様々のセキュリティマネジメントにかかわる課題についての普遍的な解決策の枠組み利用できるようになり、さらなる企業発展の糸口につながるなどの効果が期待されるからである。

企業からは、CIO/CISO 候補人材の育成のみならず、実務で直面している課題を自社固有の条件下だけでとらえるのではなく、より抽象化・一般化された課題として具体的な課題提示が求められ

る。その解決のための制約条件も一般化して整理することにより、自社の課題解決はもとより、産業界全体にとっての普遍的な解決策として活用できるようにすべきである。そのためには、産業界からの学界への協力の形で、共同研究などの投資を促進することが望ましい。

3.4.3　コース開発

CIO/CISO の機能向上に向けた産学連携について、学側でどのような取り組みが可能かを述べる。民間企業や中央省庁・地方自治体などの機関では CIO/CISO が実際に活動し、実務課題に直面している。したがって、CIO/CISO 機能の向上に必要な研究教育の材料は、これらの機関の側にある。 また、2.3.1 節で述べたように、CIO や CISO は経験交流に熱心である。そのような状況下で、学が貢献できるのは、民間企業や中央省庁・地方自治体などの機関が経験を通じて見いだした課題と知識・技術を体系化・定式化することである。この結果、一つの事故・事例から得られた経験を、企業にまたがってより多くの案件に適用できるようになる。また、新たな経験をセキュリティマネジメント体系に中に位置付けることで、その重要性や波及効果を判断することが可能となり、経験から得られる知識・技術の効果的な蓄積が可能になる。

セキュリティマネジメントのような複雑な現象を体系化・定式化できるのだろうか。過去を振り返ると、経済活動という複雑な現象も、経済学、経営学、金融工学といった分野で体系化され、一部は数学的に定式化されている。また、データの活用についても、データ工学、データベース工学の分野で体系化され、一部は定式化されている。セキュリティマネジメントが経済やデータ活用に比べて格段に複雑であるとは思えないので、一定の努力によって体系化できるのではないだろうか。

上記に例示した分野の体系化、定式化は、民間企業や中央省庁・地方自治体などの機関単独ではなく、産学の連携を通じて進められてきた。セキュリティマネジメントの材料は民間企業や中央省庁・地方自治体などの機関の側にある一方、学の研究者は体系化・定式化を生業にしていることを考えると、この分野の体系化・定式化も産学連携によって進める必要がある。

体系化・定式化というフレームワークで産学連携ができれば、リスク分析手法や情報セキュリティの投資最適化といった個別の手法についても、学から民間企業や中央省庁・地方自治体などの機関への知識貢献が進み、産学間の知識の好循環へと向かうことが期待できる。このような産学連携は、これらの機関の人材育成にもつながる。前述した日経情報ストラテジー「CIO 登場」によると、CIO/CISO の多くは、もともとセキュリティマネジメントを専門にしてきたわけではない。産学連携によって、セキュリティマネジメント学を修めることで、ダブルメジャー化が可能となる。たとえば、CIO/CISO の候補者が、社会人大学院の学生として、経験の体系化・定式化を含むセキュリティマネジメント学を研究することは有意義であろう。

3.4.4　育成キャリアパス

我が国においては、専門性を重視するあまり、あれもこれもと手を出すことが人事的に評価されない傾向がある。これが学際的な領域の人材がなかなか育たない所以でもあるように思われる。今後は、複数の専門領域を持つ人材の育成にかじを切る必要がある。多様化する社会において、新たな価値を生み出すとともにセキュリティを確保するには、様々な分野の英知を集めて製品やサービ

スを実現しなければならない。複数の専門分野を持つ人材の活用の場は確実に広がっている。さらに、多くの分野にまたがる課題を解決するには、普遍的な解決方法論を身に着けることが必須であり、直面している課題の客観的な理解ができなければならない。

企業では、実務教育と企業文化中心の人間教育とで忠誠心をはぐくむとともに、複眼的に社外において客観的普遍的な価値観を身に着けた人材が今後の企業発展に必要であると位置付けてもらいたい。

そこで、育成キャリアパスとしては、次のようなことを提案したい。まず、企業に入社後しばらくは実務経験を積み、その実務経験も 1 か所だけではなく、複数個所を経験した後、例えば企業における昇格や資格等のタイミングで大学に戻り、理論的かつ普遍的方法論を実務経験に基づき勉強させることを産学連携で実現する。この育成キャリアパスを人事制度に導入し、CIO/CISO になる人材は必ず経験することとし、我が国に定着させることが必要であると考える。

つまり、次の三段階の育成パスを明確にキャリアプランに位置付けることを提案する。第一段階は、複数の分野で実務経験を積みながら現場の課題を理解しそれらの背後にある本質課題が認識できるまで、第二段階は、本質課題をテーマに関連する学問分野の研究に取り組む。この過程では、社会人博士課程などを考慮することが望ましい。そして第三段階では、この科学的アプローチの成果である理論解を解釈し現場に適用する、そして的確な方法で効果測定を行い学へのフィードバックに努める。この第三段階で、CIO/CISO の職責が果たせるようになることを人材育成指針などで明確に位置付けてもらいたい。

3.4.5　産・官・学の人材循環の推進

社会全体の視点で見ると、セキュリティマネジメントに卓越した能力を持つ CIO/CISO、あるいはその候補者たちの数は限られている。教育コースを開発し、育成キャリアパスを明確にしても、当面は限られた人材で社会全体のセキュリティマネジメントのレベルを高めていく工夫が求められる。さらに、個々人のセキュリティマネジメント能力の向上や、セキュリティマネジメント学全体の進化に向けては、ダブルメジャーの促進とともに、様々な組織でのセキュリティマネジメントの経験を積んだ人材の輩出と、それらの人材が次にまた活躍の場を得てさらに成長していける枠組みが必要である。

企業内の育成キャリアパスに沿って、学位も得て理論武装し成長した人材が成果を上げた暁には、他の企業や官への転出、あるいは学に地位を得て研究や後進の指導にあたるなど、あるいは、学で教育・研究に取り組んだ人材がまた産・官で陣頭指揮を執るなどが、スムースに実現するような環境にしていかなければならない。

組織から組織への CIO/CISO 人材の異動はこれまでもそれなりに行われてきた。しかし、当然ながら社会全体を視野に入れた人材の適正配置の視点は欠如している。どこにどのような人材ニーズがあり、どこにどのような人材がいるかを的確に把握したうえで、好ましい人材循環を推進しなければならない。そのためには、産・官・学をまたがる人材交流・人材循環を可能にする仕組みが必要である。

同時に、各組織の人材囲い込みの戦略や人事評価における減点主義的な考え方など、専門的人材についての基本的な考え方を転換していかなければならない。また、このような人材循環の対象となる候補者個人の専門家としての倫理や責任の問題などにも取り組まなければならない。

このような課題を解決できる、産・官・学をまたがる人材循環の仕組みを構築するべきである。

3.4.6　経営改革

今後の企業・組織経営は、国内はもとより国際的にも通用する経営姿勢と経営スタイルを整備することが求められる。特に企業・組織は、「セキュアな情報通信社会基盤」の一角を担う主体となることが求められる。そのため企業・組織の活動において、対象となる「情報：企業・組織が作り出す商品（製品・サービス）、社会における当該商品の及ぼす影響、並びに当該組織内の情報処理」を坦務する CIO 並びに CISO が緊密な連携のもとで、CEO をはじめとする経営陣と連携し行動することが必須となる。特に、経営トップである CEO をはじめとする経営陣は、“コト”が起きてからの取り組みではなく、また「想定外」的発想を立ち切り、“コト”が起こる前の取り組みが重要であることを再認識する必要がある。

また CEO は、「情報」分野を担当する CIO/CISO の任命権を行使するだけではなく、坦務内容を十分に理解し、当事者となる人材の適格性判断も重要な視点であることを再認識する必要がある。このためにも「情報」の構成・目的・運用、そしてそれらの価値を明確にすると共に、ライフ・サイクルについても明確に定義し、経営基盤を確立する事が求められる。この一連の行動が戦略的 IT への取り組みであり、経営改革の第一歩となる。この行動が情報攻撃並びに風評被害に対しても確固たる姿勢が維持でき、日々の経営を営むことに結び付く。

これら一連の「情報」が企業・組織にとって、「情報資産」となる。この為、CIO 並びに CISO の坦務（権限・責任）を明確にし、対象となる「情報」を十分に分析し、要求事項を自企業・組織側で描き、「情報資産」の運用基盤を構築する流れを創り出すことである。

これらを実務と理論の裏付けの下で実践することとなるが、対象となる各種分野の最新情報を「知る」ことへのチャレンジが極めて重要となり、自社内に閉じた思考ではなく、広く理論に裏付けられていることが重要となる。この行動を経営トップはじめ経営陣全員が理解し、「学」との結びつきを明らかにし、体制整備にも結びつけたい。この体制を確立するためにも、社員育成として実務へ着いた後の「学」の習得に取り組むことを提言する。Dr.や MBA を習得する「学」の場面と、その後の「学」との人脈構築も極めて重要な意味を持つ。

この展開において注意すべきことは、これまで「マーク取り」行為と総称できる形だけの受け入れ、即ちマネジメント・システムの確立と維持向上となる本来の意義を二の次とし、第三者認証のマーク取得のみを目的とした形骸化する行為を反省する必要がある。

この「産」と「学」の連携活動を継続することは、「学」にとっても現場情報が理解でき、「企業・組織」と「学」の連携が建設的思考に結び付くこととなる。この取組みは、これまで内に閉じていた自社流に固執した企業文化や価値観を、社会の普遍的なものへと昇華させ、新たなリスクに対し、科学的に取り組む経営への脱皮を可能にする。これが経営改革の重要な視点のひとつであり、

① 社員育成プログラムの確立

② 結束力の確立
③ 国際間で通用する行動規範構築
となる。

以上の流れを CEO 中心に、CIO/CISO と他の役員・管理者と共に“コト”が起こる前に充分に連携し進めることにより、経営改革に結び付く。これが安心・安全を基盤とする信頼される企業・組織活動となり、企業・組織内活動も活性化し、BCP（事業継続）に結び付くものとなろう。

４．まとめ

産や官の実務に基づく本質的な課題設定と、学の抽象課題から理論解を見つける普遍的方法論とを本質課題を通して連結する産官学連携によって、本質課題を解決し現場の実情に合わせて解釈しなおす力を持つ CIO/CISO を育成し、日本社会が直面している様々のセキュリティ課題を解決しようというのが本提言の骨子である。

その実現に向けた 6 つの具体的提言が産官学の各主体に受け入れられ、これからますます進む情報社会の本格化に日本社会が主体的・能動的に取り組めるようになることを切に望む。

日本セキュリティ・マネジメント学会(JSSM)は、この提言の実現に向けて中心的な役割を果たす覚悟である。具体的には以下の 3 機能を果たす。

① 起点機能・・・産や官と学の間を取り持つ仲介機能、産や官からの連携要請を学に仲介する。
② 交流機能・・・CIO/CISO 並びにその候補者が互いに交流し、学とも出会い、セキュリティマネジメントのコミュニティに参加するとともに、組織内価値観にとらわれずに客観的な価値観でものを見る心構えなどを養うことができる。研究会活動や全国大会、学術講演会などの場を活用する。
③ 集積機能・・・・・産官学連携の成果を研究論文や研究ノートとして発表していただく。さらにはその前後の、論文にまでは至っていない課題検討や本質解の現場への適用経験なども集積する

産官学のそれぞれの関連する主体は、これら 3 機能を活用しつつそれぞれの役割に応じた活動に取り組まれることを期待する。

提言起草委員

大木榮二郎、　手塚　悟、　　平松　雄一、　湯淺　墾道、　吉浦　裕

賛同理事

淺井　達雄、　飯塚　久夫、　井上　克至、　内田　順一、　大内　　功、
大曽根　匡、　小川　文雄、　小倉　久宜、　喜入　博、　　橘高　弘武、
小林　健、　　佐々木健美、　佐々木良一、　澤田　栄浩、　椎原　正次、
清水　惠子、　力　利則、　　能勢　豊一、　橋本　純生、　浜谷　卓美、
林　紘一郎、　藤本　正代、　堀江　正之、　松浦　幹太、　若梅　裕子、
渡辺　研司

(いずれもアイウエオ順に記載)