セキュア社会実現へ向けての７つの提言

－安心と信頼に支えられた IT 社会実現のために－

2003 年 9 月 15 日

黒川　信弘[Ψ]

－目　　次－

[Ψ]技術士（情報工学、総合技術監理）、情報セキュリティアドミニストレータ、システム監査技術者、ISMS 審査員

セキュア社会実現へ向けての７つの提言

－安心と信頼に支えられた IT 社会実現のために－

セキュリティコンサルタント
黒川信弘

要　旨

経済不況に自然災害、地域紛争にテロといった過って無い社会不安が蔓延している。併せて高度ネットワーク社会と言えば聞こえはいいが、無法地帯と化したサイバー世界も様々なリスクに満ち満ちて来ている。このような状況では、我々のＩＴ業界の景気回復はもとより、健全なＩＴ社会の到来は望むべくも無い。本稿では、セキュリティコンサルタントの立場から、これらの現状を打破し、安心と信頼に支えられた IT 社会実現のための７つの提言を行う。

1．はじめに

入社後すぐにソフトウェア開発の職場に配属され、AVCC[1]システム、ニューメディアシステム、ファームウェアシステム、マルチメディアシステム、コンテンツ配信システム、デジタル情報家電システムなどの多くのシステム開発を 20 年間担当してきた。マルチメディアシステムを担当していた'90 年代中ごろから暗号処理や電子透かしなどのセキュリティリクワイアメントが出始め、以来、セキュリティに関連した仕事を担当するようになった。コンテンツ配信システムではコンテンツデータの改竄防止の仕組み作りや耐タンパー技術の活用なども経験した。直近では、ネットワークシステム事業展開に向けて顧客からの信頼を勝ち得るためのセキュリティ認証を取得したところである。これらのセキュリティ技術開発、セキュリティ基準作り、セキュリティポリシー策定やセキュリティ認証取得支援などの 8 年間の経験をベースにセキュリティコンサルタントとしての活動を 3 年ほど続けている。

リアルな世界では、不況による社会不安やテロや災害などでリスクの非常に高い状況である。同時に昨今の IT 関連の市場動向や技術動向を見るにつけ、或いはセキュリティコンサルタントとしての顧客との商談活動の中で、現在の社会環境においてはセキュリティ面での不安要素があまりに多いと感じる。セキュリティインシデントが頻発する現在のような状況では、健全なネットワーク社会実現へ向けて黄色信号が灯っているも同然であり、我々の IT 業界の先行き不安も感じる。本稿では、先行き不透明な 21 世紀と言う新たな時代を、安心して暮らせる社会にするために、そして我々の業界活性化のために、情報セキュリティに関する７つの提言を行う。

2．情報セキュリティとは

さて、ここで翻って情報セキュリティとは一体何であろうか。あらためて問われると多くの方が躊躇する。教科書的に言えば、「情報資産の機密性・完全性・可用性を確保すること」となるが、一般化するには少々難解である。

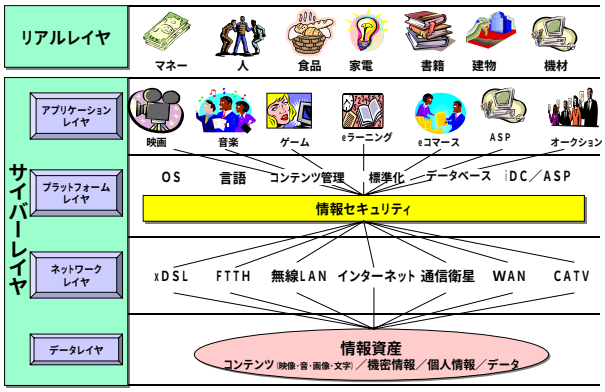

図1．情報セキュリティの位置付け

[1] Audio Visual Communication & Computer　映像・音響を駆使したコンピュータシステムアーキテクチャ

もっと分かりやすく言えば、図 1. のように貴重な情報資産を様々な用途に安全に活用できるようにするためのプラットフォームであると言える。
また情報資産をもっと詳しく見れば次のようになる。

①顧客から預かった情報
　機密情報、個人情報、環境情報など
②組織のコアコンピタンス
　製品、サービス、ソリューションなど
③自組織内の情報
　経営情報、技術情報、人事情報、情報環境設備など

それらは図 2. のように組織内にあまねく散在する。

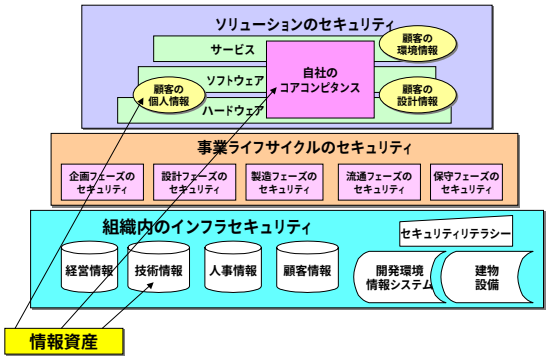

図2. 企業における情報セキュリティの概念

現代社会における情報資産は、ハードウェア、ソフトウェアを問わず益々複雑性を帯び、その組織のコアコンピタンスを支えるナレッジ（知識）と言うことになるかもしれない。電子情報は勿論､紙媒体やメディア媒体､人の記憶や話、メモまでありとあらゆるものが情報資産と言えよう。結局、情報セキュリティとは、これら多様化した情報資産の健全性を確保するための取り組みを言うのである。それだけにその取り組みは複雑かつ巨大化、多様化し、一つの切り口からではなく多面的な取り組みを必要とするものになってきた。だからこそ、本稿で示す７つの提言にあるような多面的な取り組みや社会的基盤整備、教育などが重要になって来る。

3. 情報セキュリティの現状と課題

3.1 情報セキュリティの現状

6 万種を超えると言うコンピュータウィルス、それでも次から次へと新種が出てくる。不正アクセスでは逮捕者まで出るご時世になったし、ネット掲示板での誹謗中傷合戦にインターネットオークション詐欺、パスワードクラッキングによる銀行預金の窃盗などサイバー犯罪の侵攻が続く。そして何と言っても続発する個人情報の漏洩は益々大規模化し、大きな社会問題化してきた。最近では、ウィルスのためにニューヨーク近郊の列車が止まったり、カナダの航空では旅客機が飛ばなくなったという市民生活における実害まで出るようになった。この騒動はいったい何時まで続くのだろうか。

3.2 情報セキュリティの課題

(1) もぐら叩き

これら日々巧妙化するサイバー犯罪技術に対抗して､その場しのぎの防衛策を実施しても、もぐら叩きの域を出ない。現在のソフトウェアアーキテクチャが続き、セキュリティホールが存在する限り、セキュリティインシデントは無くなりはしない。このようなイタチゴッコを永遠に続けるのだろうか。今までのように莫大なお金と人と時間をかけて、いつまでもこのようなインシデントにお付き合いするほど、現代社会に余裕があるわけでもない。思いつきや場当たり的な対応でお茶を濁すことを止め、そろそろ社会的に抜本的な対策を考えるときではなかろうか。

(2) 海外メーカへの依存度の高さ [5)]

現在のセキュリティ製品の殆どが米国製やイスラエル製であり国内製品は皆無といっていい。それだけこの分野のビジネスはブラックボックスとなり日本国内では手も足も出ない状況となりつつある。しかし、セキュリティという製品の特質上、自分たちの生活の安心を守ってくれる製品がすべて他国の技術で出来上がっているということは多少の課題があるといわざるを得ない。自国の安全を他国に頼っていては不安で仕方ない。日本国内の重要な情報資産の多

くを特定のセキュリティプロダクトで守るという事は、特定の国や団体の監視のもとにさらされているという状況に他ならない。日本とその国や団体との関係が悪化した場合には、我が国の意志とは無関係に多くの重要な資産、例えば国防関連の設備や空港や交通設備、金融システム、或いは電気・水道・ガスなどの生活インフラシステムが他国の監視状態に置かれることだって十分にありえるのだ。他国や特定のメーカが我が国を監視したりチェックしたり、或いは監視システムを一斉にシャットダウンなどすれば日本はその国に簡単に乗っ取られてしまう。あるいは特定のベンダーが事業的に立ち行かなくなったとき、現在、稼動中のセキュリティ製品の動作や保守サポートは誰がどう対処してくれるのだろうか。このような面からも国産のＩＴインフラ、セキュリティインフラの整備・充実は大きな課題として存在している。

(3) 既存 IT アーキテクチャへの疑問

パソコンの OS である Windows3.1 のプログラムソースコードは 300 万行であったが、Windows2000 になると 5,000 万行にまでなっているという。このように巨大化したプログラムを管理していくことは並大抵のことではない。従来からWindowsなどのOSには多くのバグが内在していることが指摘されている。Windows2000 は 63,000 ものバグを内在したまま出荷されたとも言われている。言わば、商品の欠陥である。多くのセキュリティインシデントは､セキュリティホールの存在が原因である。不思議なことにコンピュータ業界では、このような商品の欠陥があるということを認めたうえでのビジネスが慣習化されている。おまけにセキュリティホールのパッチあての責任はユーザに押し付けられている。ウィルスに感染したのはパッチを当てていないのが悪いのだという論調だが、その前にセキュリティホールを作った責任は誰も追求しない。その反面、何千万行のプログラムを一つのバグも無しに完璧に仕上げるということは神業に近いと認める。それはある面、現在のノイマン式コンピュータアーキテクチャの限界と考えるべきであろう。

(4) 犯罪捜査しにくい状況

2003 年 8 月に猛威を振るった MS ブラスタは今までに無い新たなワームとして記憶に新しい。米国 FBI は MS ブラスタを作成した 18 歳の犯人を逮捕した。しかし、このような例はまれであって、通常はウィルス作者や不正侵入やデータの破壊・改竄をした犯人を捕まえることは容易ではない。攻撃技術の巧妙化と検知・探索技術の高度化のイタチゴッコが永遠に続く。また、プライバシーや通信の秘密の権利などがサイバー犯罪捜査の行く手を阻む。不正行為と表裏一体の個人の権利が存在する。或いは犯罪捜査により ISP 事業者などの事業面に悪影響が出てくる。IT 市場隆盛に向けて水を差すことになってもいけない。被害算定の難しさ、秘匿性などが絡まって犯罪としての立件が難しい。サイバー犯罪捜査はこれらによって殊更困難を極めているのが実情であろう。

このように現状の情報セキュリティには多くの課題が存在する。いずれも一朝一夕に改善できるものではないが、今のまま放置しておくことはさらに深刻な事態を招きかねない。官民総力を挙げての対策が急がれる。

4．IT 化の方向性

4.1 社会インフラ化する IT

世界初のコンピュータ ENIAC[2]は 1946 年に産声を上げた。当時、高さ 3 メートル弱のキャビネットが 40 個、真空管 18,000 本と何マイルものワイアーがぎっしりと詰まった消費電力 174KW､重量 30 トンの巨大なコンピュータは、それが一体何に使えるのかさえ分からないような真空管のお化けであった。約半世紀かけて僅か数ミリ角のチップに進化したコンピュータは、電気・水道・ガス・電話などのライフラインはもちろんのこと、交通、金融、流通、医療、製造など市民の社会生活から企業の基幹部分まで

2 「エニアック」スコット・マッカートニー　パーソナルメディア株式会社による

多くの分野で無くてはならない存在になって来ている。もはやコンピュータは、それ無くしては社会生活が立ち行かないほどに市民生活の中に深く入り込み、社会経済や産業構造をしっかりと下支えしているのである。

4.2 ユビキタスネットワーク社会の到来

国内においてはインターネットが'90 年代中ごろから爆発的に広まった。このことは企業における業務を革新的に変えたと言える。企業内の LAN に止まらず、会社の外ともオープンなネットワークでつながったということは、何時でも誰とでも簡単に情報のやりとりが可能になったということであり、業務やビジネスの進め方の飛躍的な改革につながったと言える。所謂ビジネスモデルを検討できるようになったのはインターネットのおかげであり、eビジネスと言われて従来の商売のやり方をスピード､効率､レスポンス、テリトリーの観点から大幅にその障壁を取り去ったものであった。

さらには携帯電話に代表されるモバイルの進展がある。いまや 8,000 万台[3]に近づこうとしている国内の携帯電話は車の台数を上回った。今までのサーバ／クライアントコンピューティングの延長線上に有線、無線のネットワークの充実が進む。これは、もはや地理的な規制を外す画期的なインフラ革命であり、物理的距離や時間的制約などのハンディキャップの解消につながる。通信技術・ネットワークの発展により社会に広まったコンピュータは、より密接に相互連携し合うようになる。

ADSL[4]、CATV、FTTH[5]を始めネットワークはブロードバンド化の道を辿っている。まだまだ、全ネットワークがブロードバンド化されているわけではないが､2010 年には動画をやりとりしてもストレスのない時代がやってくると言う。いつの時代も早すぎる技術展開に懐疑的な人たちはいる。例えば、ニューメディア時代のキャプテンしかり、CD-ROM から DVD への移行についてもそうだった。キャプテンのような情報提供を誰が必要としているのか、誰が情報提供主体者になるのかということがその当時論議されていたと思う。情報自体の貧弱さやアナログ方式による問題、データ更新性の課題、通信速度の問題があって、結局キャプテン自体はすたれてしまったが、それに変わってインターネットによるホームページや携帯電話によるｉモードでの情報提供に現在のような大規模な市場ができあがった。或いは、CD-ROM に変わって DVD を生み出した当時、こんなに大きな容量のメディアを何に使うのかと言う論議が起きた。CD-ROM で十分だと言うことだったが、今では映画やゲーム、マルチメディアデータの入った DVD の売れ行きは絶好調であり、既にビデオテープの市場を凌駕しつつある。だから、FTTH 構想で光ファイバーを敷設しても何に使うのかが見えないので敷設しないのだと言う論理が通用しなくなっている。すでに ADSL の爆発的ヒットで結論が出ていると思うが､市場(ユーザ）はブロードバンド化を望んでいるのである。

さて､ネットワークがブロードバンド化され、縦横無尽に張り巡らされると、何時でもどこでも誰でも簡単にネットワークに入れると言うユビキタスの時代になる。既に携帯電話ではその予兆が表れている。コンピュータ系よりも電話系から市場がブレークした PDA[6]は、携帯電話をベースにして多くの機能が充実してくるとともに、軽薄短小の日本人特有の商品開発能力により益々小さく軽くなりウェアラブルコンピューティングの世界へと進むであろう。

また、家庭に浸透したコンピュータは、それらをまとめるホームコンピュータの出現へとつながる。それはデジタルテレビの流れと合流し、ノン PC と言われるコンピュータの進化したネット家電として多くの家庭に浸透していく。(図

[3] 2003 年 7 月末現在　電気通信事業者協会による

[4] Asymmetric Digital Subscriber Line 電話回線を使って双方向高速データ伝送できる非対称デジタル加入者線

[5] Fiber To The Home　電気通信事業者の事業所から利用者の各家庭までを高速･広帯域の光ファイバーケーブルで結ぶこと

[6] Personal Digital Assistance　個人の情報管理を行うための携帯端末

3．参照）

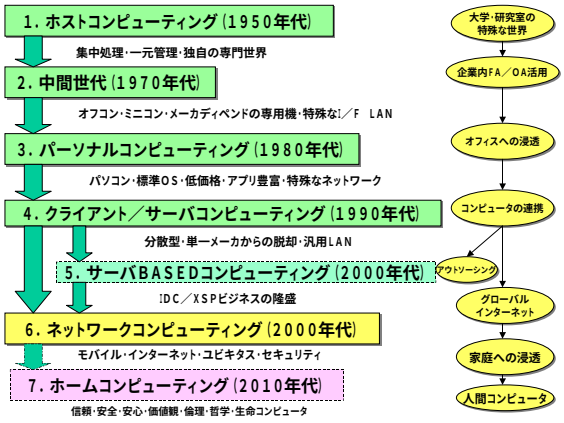

図3．ITの進化

テレビ文化はアナログからデジタルテレビ時代へと移りつつあり、はるか宇宙からの電波送信を行う衛星通信時代となっている。21 世紀はこれら BS/CS 衛星波や地上波デジタル放送が主流となり、デジタルテレビセットが家庭内のコントローラ的な位置付けで AV 家電や白物家電など様々なデジタル情報家電をネットワーク経由でコントロールできる世界に移る。出先から携帯電話で自分の家の中の様子を見ることができる。心配なら玄関の鍵もロックできるし、帰宅前に風呂の水を入れたりエアコンや炊飯器のスイッチを入れることもできる。

特に最近、セキュリティチップという超小型 IC の活用が始まりつつある。一番小さなもので 0.4 ミリ角と言うから肉眼では何かの粉末のようにしか見えない。ここに 512 ビットの情報の書き込みが行なわれ、スーパーの買い物カゴ、食堂の食器、書籍類、家電、チケット、物流のケース、衣類、車などありとあらゆる物に埋め込まれていく。それにより商品管理、人物確認、物流の効率化などその応用用途は限りなく広がる。工場、倉庫、病院、図書館、学校、食堂、家庭、遊園地、鉄道、高速道路、空港、ホテルなど活用される場面も様々に多い。まさに繊細で器用な日本人向きの先端技術であり、一人ひとりに対するきめ細かいサービスを可能とする事例とも言える。耐タンパー性を具備して紙幣やコイン、包装紙や雑誌、さらには日本のお家芸である携帯電話や DVD ディスクになどのデジタル情報家電などに埋め込めば、個人認証と組み合わせた様々なサービスの授受が考えられる。後ろ向きや暗い面の多かった今までの情報セキュリティ市場の未来は、そのようなユビキタスネットワーク社会の実現を目指して限りなく前向きで明るいものに変貌していく。[6)]

このように市民生活を広く深く下支えするコンピュータシステムは「安全と安心」がキーワードになっていく。これらの信頼おける IT によって社会・経済が安定する世界となる。情報セキュリティは、空気と同様に無くてはならないが、あって当たり前の存在になっていく。

5．セキュア社会実現へ向けての７つの提言

情報セキュリティにはどれだけお金がかかるか分からないから不安だという声をよく聞く。確かに日々巧妙化する攻撃技術に対する対策を打つにもイタチゴッコの面がある。企業によっては、ファイアーウォールやアンチウィルスソフトの導入などネットワーク面の技術対策にばかり偏ってしまって、ログ解析も含めた運用面がまったく野放しになっている状況もよく目にする。せっかく作った情報セキュリティポリシーも神棚の上に飾ってあり、社員の殆どはその存在すら知らないと言う会社もある。また、何時発生するかも分からないインシデントに対して、予めお金をかけて準備しておくと言うのも多くの企業経営者には納得いかない部分かも知れない。

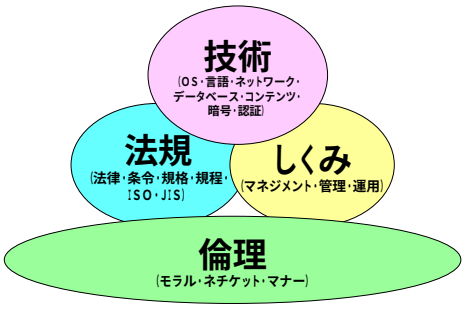

図4．情報セキュリティの4つの要素

結局、情報セキュリティを確保するには、マ

ネジメント、管理などのしくみ面、法律・規格・条令などの法規面、ファイアーウォール・暗号・認証などのネットワーク技術面、モラル・ネチケットなどの倫理面にバランスの取れた対策を取ることが重要である。そうすることで効率的・効果的な情報セキュリティ対策が実行できるのである。人・物・金・情報と言う経営資源投入のバランスが最も重要ということである。（図 4. 参照）そういった多面的な取り組みが必要と言う意味も込めて 21 世紀のセキュア社会を創出するために次の７つの提言を行う。(図 5. 参照)

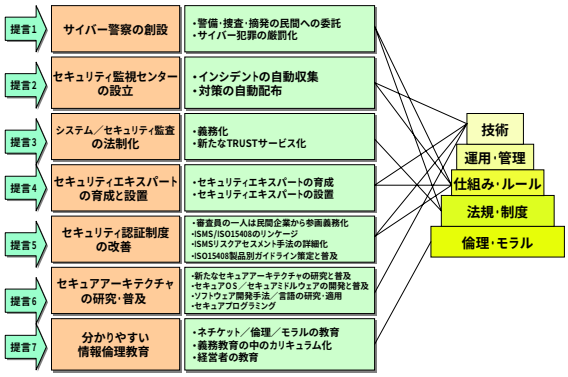

図5．7つの提言

提言１

5.1 サイバー警察の創設（しくみ面・法規面）

(1) 警備・捜査・摘発の民間への委託

サイバー犯罪を取り締まる警察組織として 2001 年 4 月にサイバーフォースが組織化されている。しかし、名前が先走っている面が多々あり、実効的な活動ができていないように感じる。なぜなら警察組織におけるセキュリティの専門家の絶対数が大幅に足りないからだ。セキュリティなどのサイバー犯罪防止には抑止効果も含めて警察力の強化が必須である。そのためには専門的スキルを必要とする警備、捜査、摘発などを民間に委託することが考えられる。リアルな世界でもイベント警備や巡回警備などに民間の力を借りようとしている状況である。サイバー世界では警備や捜査のために肉体的な損傷を受ける危険性も無いのでリアル警備よりも実現の可能性はもっと高い。ただ、特定の団体に偏った性格になってはいけないので様々な企業の専門家で構成される中立的な組織にする必要がある。徹底した専門家によるサイバー犯罪対策を実施することでサイバー犯罪を許さないと言う強い国家意志を示すことが重要である。

(2) サイバー犯罪の厳罰化

現行の法制度はサイバー犯罪を取り締まる面で不備が非常に多い。2000 年 2 月に不正アクセス禁止法、2003 年 5 月に個人情報保護法が成立したとは言え、まだまだ抜け道も多く腑抜けの法律ともいえる。おまけに現行法では情報を盗んでも窃盗罪にはあたらない。そしてなんといってもサイバー犯罪は罪が軽い。例えば、不正アクセスをした場合の刑事罰は 1 年以下の懲役または 50 万円以下の罰金である。また、ウィルスを作成または提供した者は 3 年以下の懲役または 50 万円以下の罰金となる模様だ。一方、米国では、Melissa ウィルスを作った犯人への刑事罰は最高で懲役 10 年、罰金 5,000 万円ということであるから、日本の罰則が如何に軽いかが分かる。いずれにしてもウィルスが原因で人命や財産に被害が出てもこの程度の罰則である。ネットワーク社会においては僅かな悪戯心がどんな結果をもたらすか予想もできないところが怖い。もっと厳罰化を持ってあたらないとこの種の愉快犯的な面の強い犯罪は無くならないと思える。既にウィルスで列車が止まったり航空機が止まったり市民生活に直接に影響する被害が発生している。もっと深刻な事態が発生しないうちに抑止効果を狙って厳罰化を図ることが急務である。

提言２

5.2　セキュリティ監視センターの設立(しくみ面・技術面)

(1) インシデントの自動収集

ウィルスの IPA への届出件数は、2001 年が 24,261 件、2002 年が 20,352 件、2003 年は 8 月までで 10,791 件、不正アクセスは 2001 年が 550 件、2002 年が 619 件、2003 年は 8 月までで 286 件ということである。一見、増加傾向と

も思えないし、数字的にも大したことが無いように思える。しかし、これは IPA に報告された件数のみであり、実際のウィルス被害や不正アクセス被害は、このように数字として表に出ている 10 倍以上あると言われている。ほとんどの企業や個人は、その対応に手を取られて IPA などにいちいち報告をしている暇はないということである。人手を煩わさずに自動的に申告できるしくみを構築すれば、正確な市場の状況や被害状況を把握することができる。既に公共性の高いネットワークシステムについては、ネットワークインシデント監視センター設立の動きがある。センターの機能としては、インシデントの早期発見と公表、その対策実施であろう。メーカの協力と利用者の理解を得て、企業や個人利用者のアンチウィルスソフトの中にセンターへの自動通報機能を導入しておけば、インシデントの実体を詳細に把握することができる。同時に適切かつタイムリーな対策を打つことができる。（図 6. 参照）

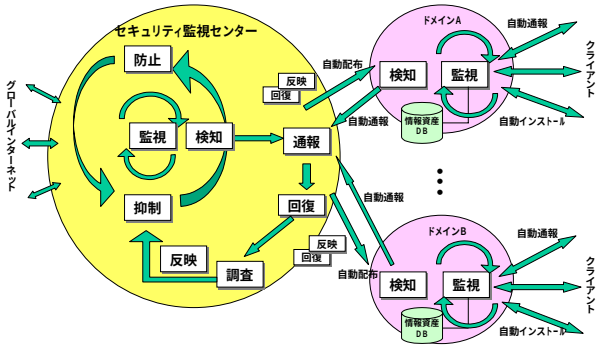

図6. セキュリティ監視の流れ

最近、リアル世界でも犯罪防止と早期発見のために監視ビデオ設置の動きがある。2003 年 7 月に発生した長崎幼児殺人事件は商店街の監視ビデオのおかげで犯人の逮捕につながった。その他にも銀行 ATM や駅の監視ビデオのおかげで凶悪犯の逮捕につながった事例は多い。そのことが犯罪の抑止効果にもなる。プライバシー問題もあるが、安全で安心な生活が保障されてのプライバシーである。優先順位を間違えてはいけない。サイバー世界でも同様であろう。安全で安心な世界であればこそ、プライバシーや通信の秘密が確保できることを忘れてはいけない。利用者の賛同を得て、インシデント自動通報制度を開始したい。

また、インターネットにより世界はシームレス化しており、日本国内だけの監視ではあまり意味が無い。セキュリティ監視センターは国際的な連携のもと、地球規模の運営管理を目指して欲しい。

(2) 対策の自動配布

上記の早期発見システムにより、ウィルスを検知したという報告があがれば、そのワクチンや対策をメーカと一緒になって早急に徹底する。問題は、その対策がいつも後手に回ったり、ワクチンソフトインストールやセキュリティホールのパッチあての手順が煩雑であることだ。どこのメーカのどの URL を見て、その説明を読んで、それぞれの状態に合わせたソフトをダウンロードして、などととても時間と手間のかかるのが現状である。IT のプロフェッショナルである筆者でも、煩雑で憂鬱に感じてしまう。素人にも簡単にすぐ対応できるように自動的にワクチンを散布するとか、先の自動通報ソフトと連動した自動対策インストール機能を装備することができないであろうか。事前の予防も含めて、もっと簡素でシンプルかつ迅速な対策手法をユーザは必要としている。一部のメーカで取り組んでいる面もあるが、公共性や負担度合いを考えると官民の協力のもと、推進すべき事項である。表 1. にセキュリティ監視センターの機能をまとめる。

表1. セキュリティ監視センターの機能

セキュリティ監視センターの機能	ドメインサーバの機能	クライアントの機能
・グローバルな セキュリティインシデントの監視 ・インシデント予測と予報 ・自動通報の受信とインシデント分析 ・対策の立案 ・対策ソフトの自動配布 ・効果把握と インシデント予報への反映 ・マルチベンダー対応	・情報資産の自動収集と自動アップデート ・セキュリティインシデントの監視 ・インシデント検知時、センターへの自動通報 ・対策ソフトの自動配布 ・効果の報告	・情報資産の自動申告 ・セキュリティインシデントの監視 ・インシデント検知と自動通報 ・対策ソフトの自動インストール・ アンインストール

・リスク分散の意味合いで
特定企業に依存しない
・公共的な性格を維持
・負担の大きさから公共投資とする

具体的な
情報資産の例

・ソフトウェア（OS，IEなど）・・・・バージョン、更新情報
・ハードウェア（CPU，HDD，メモリ、追加デバイスなど）
・ネットワーク情報（IPアドレス、MACアドレスなど）
・ネットワーク機器（config、セグメント構成、接続構成など）
・利用状況（ポートの使用状況、帯域など）

提言３

5.3　システム監査／セキュリティ監査の法制化（法規面）

(1) 義務化

2002 年 4 月のみずほ銀行のシステム統合におけるトラブルでは、口座振替の処理遅れ、ＡＴＭ障害、二重引き落とし、振込みの遅延などが発生し、多くの顧客に迷惑をかけ、同時に莫大な被害が発生した。また、2003 年 3 月 1 日に東京航空交通官制部で発生したシステム障害は航空機の欠航や遅れによって約 27 万人の利用客に大きな影響を与えた。さらには厚生年金の 220 億円の未払いと 24 億円の過払いという前代未聞のトラブルも発覚し、役所は市民への謝罪と回収に走り回っている。これらの事故はコンピュータプログラムのバグが起因していると思われる。

コンピュータシステムが社会構造のインフラと化した現在、本番稼動前にプログラムテストを実施するのは当然のことであるし、システム監査というものを定期的に実施するしくみを構築することが社会的要請としてある。つまり IT が社会経済を支えるインフラ化した現在、市民生活に深く関連する特定の分野や業種においてはシステム監査を法制義務化することが急務である。もはや IT インフラはそれほど社会的に信頼性を求められるものになったのである。既にサイバーフォースによってある程度の監視をされているようではあるが、定期的な監査は監視とは別次元で必要な機能である。以下のような分野や業種においては、システム監査／セキュリティ監査を義務付けることを要望する。

①公共機関：官公庁・防衛庁・地方自治体・警察

②法人／企業：金融・交通・通信・医療・ライフライン（電力・水道・ガス）

これにより、社会生活や経済活動も安定するし、国民の不安が解消され IT 業界活性化にも寄与することと思う。

(2) 新たな TRUST サービス化

現在のシステム監査（セキュリティ監査[7]）にも若干の課題がある。監査を受ける側からすれば、単なる監査だけでは不備を指摘されるだけで、現状改善のための具体的な方策が分からない。システムの信頼性・安全性・効率性確保のためにする監査であるから､考え方からすれば､次のような手法が用いられるべきであり、実際に市場においてもこのような分かりやすいサービスが提供され始めている。

①現状を知る（今の自分を知る）
②あるべき姿を想定する（目標を立てる）
③目標へ向けての進み具合を定量的に測る
④アカウンタビリティ（状況の公開）

上記のようなステップを繰り返して、らせん状に成熟度を向上して行くことが求められる。特に監査結果とその効果を公表することが、このしくみの市場への浸透に大きく影響する。最近の社会的な価値観からすれば、隠すことよりも公表することが当事者のインセティンブにつながっている面が強いことを企業は既に学習している。このような観点からそれぞれの分野、業界ごとにコンサル面に重心を置いた適切で分かりやすいシステム監査（セキュリティ監査）が求められる。市場にとって分かりやすい監査機能を提供することが監査側の責務である。

提言４

5.4　セキュリティエキスパートの育成と設置（しくみ面・技術面）

(1) セキュリティエキスパートの育成

セキュリティの専門家としては、既に国家資格としての情報セキュリティアドミニストレータやシステム監査技術者資格が存在する。その他に ISMS 審査員や CISSP[8]などの海外資格も多い。これ以上新たな資格を創設し市場を複雑にするよりも、今ある資格人材を有効活用することを切に望む。問題は、セキュリティの専門家としてどのような制度のもとでどのような教

[7] セキュリティ監査の場合は、情報資産に対する機密性・完全性・可用性の観点からの監査になる

[8] Certified Information Systems Security Professional 国際的なセキュリティ専門家資格

育をするかである。その詳細なカリキュラムについては多くの関係機関で論議されているのでそちらに譲るとして、ここでは資格制度に対する考え方を提起したい。

情報処理事業の奨励と振興のために昭和 44 年から情報処理技術者試験が開始された。以来、30 年の長きに渡って継続されており、既に累積 1,000 万人の応募者と 100 万人の合格者[9]を輩出している。とは言え、我が国の情報処理分野の国際競争力はどうであろうか。未だに IT 製品のコア部分は他国に頼っており、日本製の OS／DB／ブラウザ／ミドルウェアなどメジャーなものは殆どない。ましてや後発国の中国やインドなどにソフトウェア分野の技術者の優秀さでは大きく水を開けられた状態である。つまり IT 分野の人材はこの 30 年間育っていないのである。それは次のような情報処理技術者試験の制度に原因があると思う。

・実務経験を問わないペーパー試験
・継続教育の義務がない
・一度合格すればずっと有資格者

これらの点を勘案して既存の有資格者をセキュリティ専門家として次のような考え方をベースに新たに認定することを提起する。

①実務経験重視

今までのようなペーパードライバ的な面を廃し、実際に実務としてセキュリティ業務を経験してきたことを認定の必須条件とする。セキュリティ商材の開発・販売、セキュリティサービス、セキュリティコンサルなどを 3 年以上経験していることが望ましい。

②継続トレーニング教育の受講義務

情報処理技術者資格のように、一度試験に合格すれば永遠に有資格者として認められる時代は既に終わった。特に IT は時々刻々と進歩しており、その技術スピードに付いていくには、日々の研鑽が求められる。最近の有用な資格では継続教育義務が常識となっており、セキュリティ分野においても継続トレーニング制度を導入したい。例えば、年間 30 時間以上の公的教育の受講を義務化すれば、新たなセキュリティ技術や動向を確実に普及徹底することができる。

③資格更新制度の導入

資格を維持しようと思ったら、一定期間ごとの更新手続きを必要とする制度としたい。資格更新の要件は、例えば上記のような継続教育を規定分以上受講した証拠を示すことである。自動車運転免許でも更新制度があるので、こういった変化の激しい技術資格では更新制度は当然のことである。3 年ごとに必要な継続教育と実際の実務を経験したということでその資格を更新維持できる。それで初めて有用で信頼されるセキュリティ専門家に育って行くと考える。

(2) セキュリティエキスパートの設置

5.3(1)で指定した分野や業種、及び一定規模以上のシステム設備保有者には、上記のセキュリティエキスパートの設置を義務化する。セキュリティエキスパートは、常に組織のセキュリティインシデントに気を配り、システムや設備を監視し、積極的にシステムの健全化を図り、組織内の徹底・啓蒙を図ることをミッションとする。インシデントが発生すれば前記のセキュリティ監視センターと連携をして、可及的速やかにその対処を行う。金融や電力などの公共性の強い企業や団体のシステムインフラなどでは社会的義務としてそのような専門家を設置して、システムの健全性を確保する責任がある。例えば、1,000 万円以上のシステム設備、或いは 10 人以上の情報処理担当者に 1 人の割合でセキュリティエキスパートを設置するくらいのことは必要であろう。そうすることで雇用面の経済的波及効果も見込める。

提言 5

5.5　セキュリティ認証制度の改善（しくみ面・技術面）

(1) 審査員の活性化

例えば ISMS 審査において審査員が 3 名構成だとすれば、その 3 名のうち 1 名は、一般企業から参画させることを審査機関に義務付ける。

9 情報処理技術者試験センター 統計情報による (http://www.jitec.jp/1_07toukei/oubo_gokaku.html)

そうすれば、民間企業のセキュリティ能力も上がるし、課題や事例を共有できる。緊張感をもって適切な審査が行われる。ひいては我が国全体のセキュリティレベルアップにつながる。審査料などのキャッシュの流通が進み、ある程度の経済効果も見込める。

また、日本社会の悪い慣行であるが、審査員という職種は社会経験豊かなベテランが多いが、裏を返せば定年退職者やリストラ組の色合いが強い面がある。監査技法は体得しているが肝心の情報セキュリティや IT のスキルは皆無だと言う審査員も多い。このような風潮が蔓延すれば情報セキュリティや IT 業界に決していい影響はない。審査や監査という職種にも最先端の IT スキルを保有した若手ばりばりで有能な人材が集まってくれるような性格のものにすることで、さらに日本の情報セキュリティレベルも大きく向上するものと思う。

(2) ISMS/ISO15408 のリンケージ

現在の組織セキュリティの ISMS と製品セキュリティの ISO15408 の相互関係は全くないと言っていい。[1)4)] 行政の縦割り組織の反映そのものである。制度自体も双方無関係であるし、要求事項の中身もつながりは見えない。そこが市場には理解しにくいところであるようだ。双方とも広く見れば同じセキュリティ認証制度であるので、制度面の連携や要求事項の相互参照や同一手法の活用などもっと密接なリンケージが欲しい。(図 7.[1)4)] 参照)

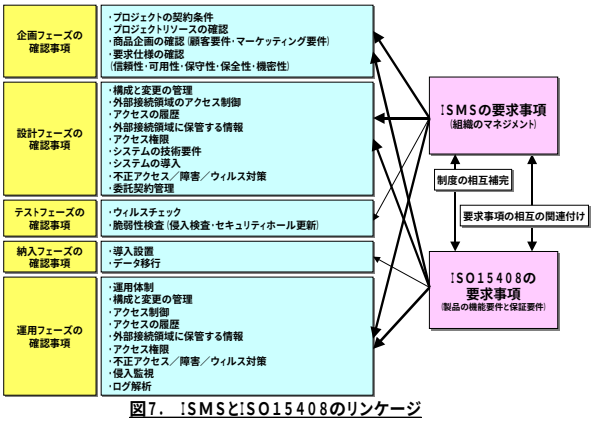

図7. ISMSとISO15408のリンケージ

例えば、ISO15408 の保証要件などは ISMS と同質な面が多い。しかしながら、ISO15408 はマネジメントシステムではないので、対象の商品のセキュリティさえ確保できれば、同じ会社の他製品への適用には無関係であるし、対象商品のサービスが終了すればそのしくみなり環境は不要になる。しかし、現実の企業はそうはいかない。お金と人と時間をかけて構築した保証要件に該当するしくみ・機能は、自社内の他の組織へも活用したい。それはまさに ISMS の要求事項そのものではないか。そういった部分のリンケージをもっと強く出したい。ISMS 制度（ISMS 適合性評価制度)、ISO15408（IT セキュリティ評価・認証制度)、情報セキュリティ監査制度など同じ情報セキュリティ関連の制度が無関係に並立している。情報セキュリティの確保をテーマとしている現場では、それらは全て一つの同じ情報セキュリティである。考え方の統一と制度の連携がこれら制度の普及のポイントであるし、それによって我が国のセキュリティレベルは格段に上がるはずである。

(3) ISMS リスクアセスメント手法の詳細化

ISMS 認証においてはリスクアセスメントが重要な位置付けを占める。[1)2)] しかし、現状は、このリスクアセスメントが認証取得者に多大の負担を要求している。ISMS 認証取得の作業工数の大半はリスクアセスメントに費やされる。膨大な作業となる情報資産管理フェーズの自動化まで含めてリスクアセスメントフェーズをもっと簡素化できればコスト的、時間的な問題も縮小され、企業の負担も軽減し、その結果、認証取得もさらに広まるであろうと思える。そのためには、ツールの整備も含めてリスクアセスメントの手法を詳細化したい。つまり抽象的な事例紹介 [3)] ではなく、個々の組織で悩む余地の無いほどに客観的で定量的な手法の開発普及と作業部分の自動化、ツール化を推し進めたい。

(4) ISO15408 の市場普及

ISO15408 には課題が多い。審査員や企業内技術者を多数育成する必要があると言われているが、それは二次的な話である。本質的な問題は、内容が ISMS 要求事項のように一般的では

ないことである。[4] 現場において採用されている IT 商品の設計・開発・テスト手法と大きな隔たりがある。さらにそういった親和性の無い要求事項の上に重たい制度が乗っているので、実際に市場・業界がこれで回るかどうか不安視されている。この制度を普及させるためには、ISO15408 の内容と現場の開発手法との整合性を取ったディフォルメしたガイドラインを作成し、市場に対して分かりやすくアピールすることが重要である。前記(2)のリンケージもその方策の一つである。

また、例えば EAL3 レベル[10]の取得で数千万円のコストアップになる負担を企業に被せるのは現実的ではない。まだまだ国内の取得例が少ない現状であるので、国の負担で商品ごとの PP[11]評価、ST[12]確認や TOE[13]認証の具体的サンプル事例を多く作り、それをベースに市場普及していくことがベターである。

提言 6

5.6　セキュアアーキテクチャの研究・普及（技術面）

現在の Windows 寡占状態を解消しなければならない。市場が特定のアーキテクチャに過度に集中しているからサイバー攻撃のターゲットになるし、問題が起きたときに被害が大きくなる。そろそろ Windows 以外のセキュアな環境構築に手を付ける時期であろう。既に関係省庁を中心にそういう動きもあるが、以下のような点について研究・開発・普及が急がれる。

①新たなセキュアアーキテクチャの研究と普及

―量子コンピュータ[14]、DNA コンピュータ[15]など

②セキュア OS の開発と普及

―LINUX・TRON などをセキュア OS として機能向上

③セキュアミドルウェアの開発と普及

―サーバソフトやブラウザなどミドルウェアソフトのセキュア化

④セキュアソフトウェア開発手法／セキュアプログラム言語の研究・適用

―開発手法／環境／プログラム言語／ツールなど

⑤セキュアプログラミング

―セキュアプログラミングを一部のオタク文化にしないで、徹底した公開教育と啓蒙でメジャー化を図る

提言 7

5.7　分かりやすい情報倫理教育（モラル面）

(1) ネチケット・倫理・モラルの教育

法律遵守を求めることも重要であるが、リアルな世界とは異なるサイバー社会の到来にあたり倫理面の普及・啓蒙が急がれる。ネットワーク上のエチケットとしてはネチケットということで有志レベルでのボランティア的普及活動があるが、既にそのような生ぬるい手法では限界を感じる段階まで来ている。三菱自動車のリコール隠し、東京電力の原子力発電所トラブル隠し、東海村 JCO 臨界事故、雪印の集団食中毒事件、同じく雪印と日本ハムの牛肉偽装事件などトラブル隠しやリスク対応不備など多くの企業で不祥事が発生している。その結果、企業のコンプライアンス（法令遵守）とアカウンタビリティ（説明責任）重視の経営と言う透明性確保の取り組みは急ピッチで進んでいる。同時に、技術側の倫理を問う声も高く、あらためて技術者倫理教育も進められている。同様にサイバー空間における倫理面の教育も求められているところであろう。これからはサイバー世界の特異性と情報倫理を市民一人一人に理解を求め、文化として醸成することが重要である。

(2) 義務教育におけるカリキュラム化

10 Evaluation Assurance Level 評価保障レベル

11 Protection Profile ユーザの立場から作成するセキュリティ要求仕様書

12 Security Target システムや機器を提供するベンダー側からの立場から作成するセキュリティ基本設計書

13 Target of Evaluation 評価対象

14 量子力学の原理に基づいて動く、現在とは全く異なる動作方式のコンピュータ

15 DNA の 4 種類の塩基を素子とした現在とは全く異なる生物的なコンピュータ

新たなサイバー世界での常識やマナー・ルールは、子供時代から修得した方が効果が高い。義務教育の段階から子供たちに情報倫理を教育し、健全な倫理感を持った人材を早期に育成することが求められる。情報セキュリティはマネジメント面や技術面など非常に広範囲かつ専門的な部分が多い。しかし、どんなに良いしくみを作ろうが、どんなに優秀な技術を応用しようが、それを活用するのは人である。人の意識が低ければどんな対策をとっても無駄な結果に終わるのである。サイバー社会の常識とは、モラルとは、マナーとは、まだ手探り状態の面があるが、現在の情報倫理教育をベースに未来の若い人たちが新たに作って行くものかも知れない。

(3)経営者の教育

情報セキュリティを普及するためには、企業の経営トップが情報セキュリティについての認識を新たにすることが重要である。既に情報セキュリティは、技術課題ではなく経営課題として認識すべき段階になっている。そして、企業防衛、企業責任の観点から一歩踏み出て、自社コアコンピタンスのコアスキルとして市場へ提供するソリューションの中に盛り込むべきものである。そのためにも情報倫理を中心とした社会における情報セキュリティの位置付けを経営者へ教育・啓蒙することが急がれる。

(4)製品の倫理認証

IT の進化とともにコンピュータは益々ブラックボックス化して行く。Windows Update や Cookie が一体裏で何をしているか不安になったことはないだろうか。パソコン内部の通信ソフトやＬＡＮボードが何処へどんなデータを送っているか目に目えないだけに不安は尽きない。ましてや最近の IT プロダクトはグローバル化し、ソフトウェアやボードは海外の名も知れぬ中小企業で簡単に作れる。町の電気屋で買ってきた PC カードや通信ソフトが、入力したクレジット番号やパスワードをひょっとして何処かへ横流しする機能を持っているかも知れない。

もはや技術はスペック的に正しく動作することは当然のことであり、それ以上に、法的、倫理的な正当性を実証すべき時代に入っている。製品ごとに法的・倫理的に問題が無いことを認証局が保証する取り組みが必要である。PC、ネットワーク機器、メモリデバイスなどが反社会的な動作をしないとか、倫理的に正しいということを保証する倫理マークが必要である。

6．おわりに

昭和 60 年に制定されたシステム監査基準にも、情報セキュリティという考え方は存在していた。その当時に比べると現在の情報セキュリティ管理基準は、ネットワーク面や人的側面が大きくクローズアップされている。その結果、セキュリティ問題は企業にとって手間、コスト、時間のかかるとてもやっかいなものになってきた。恐らくどこの組織も本業の基幹業務を支える IT インフラの信頼性確保のためと社会的な企業責任を果たすために情報セキュリティの確保に注力せざるを得ない状況と思える。そのために所謂利益を生まない後ろ向きな業務として色づけされ、セキュリティ担当者への成り手がいないという状況にまでなっていたほどである。このような状況では、決して情報セキュリティは向上も進歩もしない。後ろ向きな後追い対策としてではなく、先進的な技術を駆使し、企業・組織のコアコンピタンスの付加価値作りに貢献すると言う明るい前向きな情報セキュリティにして行きたい。その結果、優秀な人材も多く集まり、熱意を持って新たな取り組みや多くのノウハウが蓄積され、益々市場のセキュリティレベルは上がっていく。そして、安全と安心に囲まれた信頼のおける健全な IT 社会が創出されるのではないだろうか。

以上

＜参考文献＞

1)（財）日本情報処理開発協会　「ISMS 情報セキュリティマネジメントシステム適合性評価制度　－ISMS 認証基準（V2.0）－」(平成 15

年 4 月 21 日)
2) British Standards Institution「Information security management system –Specification with guidance for use」 (2002.9.5)
3)（財）日本情報処理開発協会 「ISMS ガイド V1.0」(平成 14 年 4 月 1 日)
4) 情報処理振興事業協会「情報技術セキュリティ評価のためのコモンクライテリア」(2001/1 第 1.2 版)
5) 黒川信弘 情報セキュリティのビジネスモデル「月刊セキュリティ研究」2003 年 3 月号 p29-32
6) 黒川信弘 情報セキュリティのビジネスモデル「月刊セキュリティ研究」2003 年 9 月号 p45-49