情報セキュリティ問題とその進化

辰巳　憲一*

1　はじめに

情報セキュリティは技術、機器、思考、アーキテクチャー(1)のいずれもが、今、統合管理の方向を向いている。この「統合」とは、複数のセキュリティ機能を１つの機器に収めること、あるいは１つのセンターから一括してすべての機能を達成すること、を指す。後述の、セキュリティ・ゲートウェイやUTM（Unified Threat Management、統合脅威管理）などが目標としていること、に近いのである。

当然、これまでも何らかの管理はあった（管理するかどうかの検討の結果管理しないと決めた、管理するべき事柄なのかどうかわからずに検討項目にあがらず検討もしていない、ことも含めて）。今はそれに効率と管理コストの双方に視点が移ったという言い方もできる。これまでばらばらに存在し、それぞれ個別に運用コストが必要だったセキュリティ対策を１つにまとめて、管理性を高め、運用コストを下げるのが「統合」の目指すところである。

これらを統合セキュリティ管理と総称し、情報セキュリティが起こった理由、情報セキュリティの進化の過程、それが問題にする情報システムとは何か、の観点から考察してみよう。

2　情報セキュリティとは

2−1　情報セキュリティ問題が起こるわけ

情報セキュリティ問題が起こるわけ、大きな問題となっている原因をあげてみよう。

＊　学習院大学経済学部教授。Information Security and its Development: A Critical Survey. 内容などの連絡先：〒171-8588豊島区目白１－５－１学習院大学経済学部、TEL（DI）：03-5992-4382、Fax：03-5992-1007、E-mail: Kenichi.Tatsumi◎gakushuin.ac.jp（ご送信される場合◎は@に置き換えてご利用ください。）

本稿は後藤　允准教授（北海道大学）との2010年度共同研究の一部（辰巳・後藤（2010）をも参照）である。また、多くの方に議論に付き合っていただき、ヒントをいただいた。特に、辰巳（2011）作成時でも貢献いただいた、木谷一彦、西端恭一、永岡春夫、などの各氏に感謝したい。コカ・コーラの挿話は、随分前に、どこか記事、HPかブログで見たことを思い出して書いたもので、所在と日時が不明のため、引用不可能である。

(1) 情報システムにおけるアーキテクチャーとは、情報システム設計者の発想のことをいい、設計者が「情報システムにおける目的をどのような構造で実現しようか」と発想し、発想によって見いだされた構造が適切かどうかを検討したうえで、最適と思われる構造を決めること、である。それゆえ、情報システムにおける目的が正しく設定されていることを前提すれば、情報システムの良しあしはアーキテクチャーで決まる。主要部分は松山（2011）から引用。

(1) 情報システムの大規模化と複雑化

情報システム[(2)]が大規模化、複雑化するに伴い、攻撃を受ける可能性やシステム障害発生の可能性が高まる。つまり、システム化の範囲が拡大するにつれ、システム接続先も増加する。その結果、悪意の攻撃者の標的になりやすくなるだけでなく、わずかな「うっかりミス（これはシステム障害発生の最大原因である）」の影響が、広範囲に及び、しかも大きくなるのである。

企業が対処すべきセキュリティ対策の領域は実に広範囲に及び、その項目も多岐にわたっている。例えば、外部／内部ネットワークの境界、エンドポイント、PCやモバイル・デバイス内のデータに至るまで、ネットワークのあらゆる個所においてセキュリティ上の脅威に悩まされている（シュエッド（2008））。

これらは経営を揺るがす大事態を引き起こしかねない。異なる複数の情報システムを統合した組織では、当然、システム障害発生のリスクも高くなる。そして、ひとたび障害が発生すると、その影響はひとつの組織に止まるだけでなく社会全体に及ぶことになる。

(2) 情報のデジタル化・処理速度高速化と情報の価値の増大

情報のデジタル化が進み、複製・蓄積や加工・編集が非常に容易になり、大量のデータもコンパクトになった。これらのことが情報を盗み易くなったことに直接結び付いている。容易にしかも大量に情報を送ることができるようになり、情報の流通が容易になった点も重要である。

そもそも、超大量のデータや画像などの複雑な情報も簡単に情報処理できるようになり、それまで処理できずに等閑にされてきた情報にまで価値が生まれるようになったことが、根本的に影響している。

うっかりミスも多いが、部内者による情報漏洩（ろうえい）が無視できない位多い。その原因は情報が売れるからである。これは企業内部から発生するセキュリティの脅威である。

(3) 愉快犯だけではないサイバー攻撃の多様化

サイバー攻撃や迷惑メールが増えた。それらは、多種多様な形態をとる。また、いつも愉快犯はいる。過去の一部の攻撃方法の例をあげてみると、

> USBメモリーをパソコンに挿すとウィルスが自動的に起動する「オートラン（Autorun）」、パソコンの基本ソフト（OS）の脆弱（ぜいじゃく）性を突いて感染する「ダウンアドアップ（Downadup）」、

がある。多種多様な攻撃に対して、また攻撃側が攻撃の的を絞り確実になっている攻撃に対して、さらにまた多様化した攻撃や進入の経路に対して、複合的に対応しなければならなくなった、ということである。

高いセキュリティ意識を持つ企業さえも攻撃のターゲットとなっている。2009年後半に登場した石油、エネルギーや製薬会社を狙ったNight Dragon、あるいは2010年に登場したGoogleなどを狙ったOperation Auroraが例としてあげられる。

---

(2) システムとは、ある目的のために構成要素が互いに関連し合い達成に向かっている仕組みである。情報システムとは、組織における意思決定や、調整、管理、分析などを支援するために、構成要素が互いに関連し合って協働することにより、情報を収集し、処理し、貯蔵し、伝達するシステムである。アーキテクチャーとは、構成要素、構成要素間の関係、そして設計思想（なぜそこにその要素が存在し、他の要素となぜそのような関係になっているかの理由であり、企業文化などその組織の持つ土壌や風土によって規定される）を指す。

(4) ネットワーク拡大

ビジネス・チャンスを広げるため、企業は広く様々なネットワークを求めてきた。独自の専用ネットワークを使う場合は、比較的安全であるが、ビジネス・チャンスが限られるからである。この動きのなかに、様々な提携、業務の外部委託（アウトソーシング）がある。アウトソーシングが進む中、仕事を請け負う外部企業を通じた情報漏洩の心配がある。

(5) ITコスト削減とセキュリティ

不況になると、プロセスの自動化や標準化、集中化など、より一層可能なかぎり効率化に取り組む必要があり、ITコストを削減する傾向が生じる。

ITに関連する経費を削減する方法はたくさんある。例えば、サーバー**仮想化**、**オフショアリング**、オープンソースへの移行、サプライヤーやインフラの整理統合、**クラウド・コンピューティング**への移行などである。しかしながら、そうした方法の多くは、経費削減の代わりにセキュリティ関連の負担を増やしてしまう。

(6) 事なかれ主義

人々や企業の態度も要因にあげることができよう。事なかれ主義がセキュリティ問題を大きくする。事例は複数あげられる。

「自由と安全が両立しないならば大衆は安全を選ぶ。」ドイツにおいて、ファシズムの台頭という危機に対して、人々がとる行動と経済社会的背景を考察したドラッカー（1997）は、こう考えた。多少不自由でも、安全がよい、という態度が危機をさらに大きくしたのである。

同じような傾向は、漏洩にあたっても、指摘できる。データの漏洩により、企業買収や新製品の市場投入を中止した企業があると報道されている。また、データの漏洩発生を隠蔽する企業が増えてきている。そこまで極端でなくても、漏洩事件をすべて報告するのではなく、漏洩事件の情報を選別した上で報告するケースもある。

2−2 情報セキュリティの進化

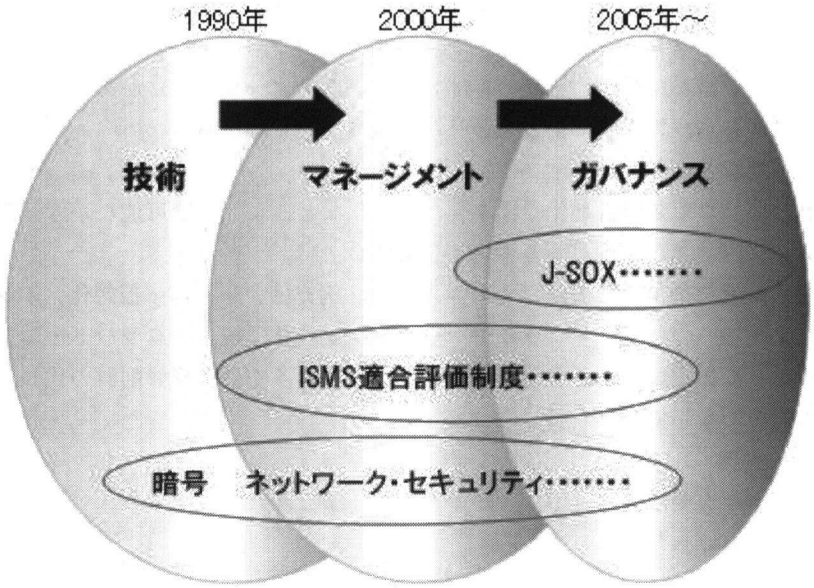
2−2−1 情報セキュリティのソフト化

情報セキュリティは、図1のように、技術が絶えず進歩しているだけでなく、管理、ガバナンスとソフト面でも発展は目覚ましい。

また、別の見解では、企業のセキュリティ投資は、対策優先の第一段階、費用対効果に基づく整理・統合の第二段階を経て、現在では、より積極的な業務効率の向上とそれによるコスト削減が求められる第三段階にある、といわれる。サーバー統合管理に代表されるような、管理を統合して効率を向上させ運用コストの削減を図る、**仮想化**といわれる技術が第三段階の代表である。

ちなみに、セキュリティのアウトソーシングは当該組織にとって必ずしも進歩ではない。このアウトソーシングに関しては慎重を要すると言われる。セキュリティのアウトソーシングが可能なものはいくつかあるが、思慮を欠いたままセキュリティ業務を外部に丸投げし、外部の人間に処理を任せっきりにするアウトソーシングは一般的に間違いである、と言われる。

図1　情報セキュリティの進化



出所）林（2009）

2−2−2　情報セキュリティの技術進歩

(1) セキュリティにおけるSaaS

セキュリティSaaSとは“Security as a Service”のことで、“Software as a Service”のセキュリティ版である。セキュリティSaaSのメリットは主に、単体の機器などでは実現できないパフォーマンス、セキュリティ専門家の管理下にあるという安全性、そして直接管理する必要がないという管理効率、の3つである。セキュリティ・システムにおいては、効率化のためにあらゆる重複を排除する必要がある。インフラとサーバーにかかるコストを回避するために、単なるアウトソーシングを超えたセキュリティにおけるSaaS採用も考慮に入れるべきである、と言われている。

(2) Endpoint Security

例えばイスラエルの会社Check PointのPCセキュリティ製品「Endpoint Security R71」には、ファイア・ウォール、プログラム制御、ネットワークアクセス制御（NAC）、アンチウィルス、アンチスパイウェア、リモートアクセス、フルディスク暗号化、ポート制御／メディア暗号化のクライアントセキュリティ機能を、単一のエージェントによって管理する統合機能がある。

(3) UTMやファイア・ウォール

現在の一般的なファイア・ウォールは、**ポート**や**プロトコル**によって通信を判別して制御する。しかし現在では、さまざまな攻撃手法が確立され、この方式だけではセキュリティ対策が不足してしまうことが知られている。そこで、アンチウィルスやIPS、メール・フィルタリングといった機能を追加したUTM製品が登場した。

UTMアプライアンスを導入すれば、複数のセキュリティ機能が1つにまとまり、機器の統合や

管理の簡素化によるコスト削減効果が目に見えやすくなる。

しかしながら、UTM[3]は、既存のファイア・ウォールに幾つかの機能を後付けしたものに過ぎない。その結果、パフォーマンスや制御に限界がある。ファイア・ウォールに他のテクノロジーを追加するのではなく、ファイア・ウォール自体にそれらの機能を持たせた、必要なファイア・ウォールをゼロから作った製品もある。従来のものと区別して、これを次世代ファイア・ウォールと呼ぶ業者もある。

(4) 統合管理の環境

シュエッド (2008) によると、今や複数のセキュリティ・コンポーネントを統合環境で管理できるようになっている。これが2008年段階での話である。

1つのエージェントで複数のセキュリティ・コンポーネントを管理できる。その上、1つのコネクションですべての状態を把握できるようになっている。例えば、他社のウィルス対策ソフトが導入済みであれば、その管理だけをエージェントで行うことも可能となっている。

2−3 情報セキュリティ概念の要約

様々な情報セキュリティ技術が導入された後、ここで一度、情報セキュリティを定義し直す必要があるようにみえる。**情報セキュリティとは、許可された者のみ情報にアクセスが可能な状態(機密性)、情報が改ざん・消去されない状態、許可された者が必要な時に情報にアクセスできる状態 (可用性)、を維持できるようにすることである。**

情報セキュリティは、企業にあっては、ほぼ常時進入を試み、生産活動を妨害するウィルスなどの攻撃を阻止し、生産におけるリスクを軽減しコストを低減する、ことになる。

2−4 ネット攻撃の進歩

(1) ネット攻撃の分業化

既述のように、ネット攻撃の主流は、愉快犯から、金銭目的になっている。商用サイトを狙ってデータベースの中身を盗み出したり、特定のユーザー向けに専用ウィルスを送り込んで情報を盗み出したりして、営利に結び付ける手口がはやっている。

ネット攻撃の方法も、個人や小規模グループによる攻撃から進歩し、攻撃者は広がってきた。まず、能力があるクラッカーが攻撃ツールを開発して闇サイトで販売するようになった。そして、攻撃者はそれを購入して攻撃に使う。さらに、単純な攻撃ツールだけでなく、拡張可能な攻撃ツールやウィルス開発用ツールキットも登場した。そして、攻撃者はそれを購入して自己の目的に会う様拡張・開発して攻撃に使う。

(2) ネット攻撃の闇市場

ネット攻撃は、さらに分業化が進み、それぞれのスキルを持つ犯罪者の間で、金銭をやりとりする闇市場が生まれることで発達してきた。

こういったネット攻撃の分業化の究極の形態といわれるCaaS (crimeware as a service) は、悪意のある人向けに提供する、インターネット上の攻撃代行サービスである。CaaSを利用すると、

(3) UTM (Unified Threat Management 統合脅威管理) は、複数の情報セキュリティ機能を統合的に管理することで、人材やコスト面での投資最適化に対して導入すれば効果がある。しかし、実際上、その定義はベンダーによって大きく異なる。同じUTMでも、必要な機能が不足していたり、逆に不要な機能まで搭載されているため無駄なコストが発生することがあると言われている。

ターゲットを攻撃し、狙った情報を手に入れてくれる。これは、いわば、ソフトウェアをネットワーク上のサービスとして提供するSaaS（software as a service）のネット攻撃版である。

3　情報システムと情報セキュリティ

3−1　情報システムの特性

情報システムは業務に必須だが投資に見合った効果が出るとは限らない。しかも、他の設備投資に比べて専門的で難解でもある、といわれる。情報システムの特性、あるべき姿を要約してみると次のようになる。

①情報システムとは、組織の意思決定と情報伝達についての何らかの仕組みである。

②組織は、その規模の大きさと複雑さに係わらず、情報システムを必要とする。

③情報システムは作られる、作られなければならない。放っておいて自然発生的に生まれる情報システムは必ずしも効率的ではない。

④情報システムは効率的に作られねばならない。情報の取得／分析／伝達にはコストがかかる。そのため、情報システム構築の最適なデザインが必要になる。そのために情報システムの標準化が必要になる。階層（ハイアラキー）の下層で収集された情報が要約されて上層へ向かい、上層での意思決定に活用される。そして、その意思決定結果が実行に向けて下層まで伝達される、というピラミッド型指示系統がとられることが多い。

⑤情報システムは情報取得／分析／伝達のコストを引き下げ、組織内のより広い範囲に十分な情報を行き渡らせることを可能にする。その結果、下層においても意思決定に必要な情報を入手できるようになる。

⑥構築された情報システムは活用されなければならない。情報システムを運営する際にもピラミッド型指示系統（これも情報システムである）が必要で、そのリーダーの能力不足で、情報システムが十分に活用されない場合がある。雇用慣行、取引先との関係、などを維持するために、十分に活用されない場合もある。活用するツールも情報システムである。

⑦情報システムは外部環境などの変化に応じて改善されなければならない。過去の成功体験に固執して新しい技術・環境に敏速に対応できない場合が往々にしてある。これを避けなければならない。

⑧情報システムは規模が大きくなる、あるいは複雑になるほど、内部でのミスによって壊れやすくなる、あるいは外部からの侵入・攻撃によって壊れやすくなる、つまり情報セキュリティが脆弱になる。

⑨情報システムは複数集まって一つの組織になる。つまり組織は情報システムの集合体である。それを複合情報システムと呼ぼう。企業は複合情報システムの１つである。他の例として、市場などがある。市場は複合情報システムである。

⑩組織のリーダーが交代し経営を変えようとしている組織は情報システムが変わる。むしろ積極的に情報システムを変える必要がある。

⑪情報システムには、該当業務に精通していなくてもシステムを作れ、外部からシステムの構造を推察できる普通のレベルから、それらができない非常に複雑で高度なレベルまである。

⑫情報システムの目的は、明確でなければならない。普通のレベルの情報システムでは、これ

は比較的明確である。例えば、電子帳票システムなどの書類の電子化（ちなみに紙の情報をデジタル化する作業を効率化しなければ、しかも情報セキュリティも高くなければ、情報システムを導入してもコストや時間の削減は実現しない。）、受発注の電子化、在庫のデータベース化、全国ネット化、顧客情報の一元管理、などのようである。

高いレベルの情報システムの場合、例えば業務・仕事を新しいやり方に変えていく、これまでできなかったことを実現するといった事柄が情報システムの目的になる場合、その目的を組織自身が十分把握し解析し詳細を決めなければならない。情報システム構築にあたってはシステム作成者が十分理解し、作成しなければならない。複数のシステム作成者がいる場合十分協議する必要がある。

⑬情報システムには金銭の出費が伴う投資が必要になる。しかも、情報システムは、工場新設のように商品を直接生み出すことはなく、投資を増やしても売上や利益が直接目に見えて伸びない、コスト・センターである。それゆえ情報システムの目的が何だったかを省みず、コスト削減が大きな目標になりがちになる。

⑭情報システム投資額は、その技術が効率化しようとしている、企業の期待価値を超えることはできない。

⑮複合情報システムにおいては、分散する情報システムを統合・連携させ効率化させていくアーキテクチャーが必要になる。

⑯個々の情報システムの目的・目標は、それを作成し管理する上位組織（情報システム）の目的・目標と矛盾することは許されない。一般に、これは組織の大原則である。

⑰情報システムは使いやすく便利になるほど、情報セキュリティが脆弱になるというリスクを負う。

⑱情報システムと物理的な物品・機器・構造物との間には、代替的か補完的な関係がある。

⑲情報システムを危険に晒すものに、「内部の脅威」「脆弱性の悪用」「サイバーテロ」「産業スパイ」などがある。

3−2　情報システムの経済的価値

コカ・コーラは、保存料や合成香料を使っていないと宣伝するだけで、一般に製造方法は知られていない。特許を取得すれば、原液の成分が公開されてしまうことを恐れている（と関係者は指摘する）ため、コカ・コーラは原液の特許を取得していない。そうまでして、秘密は保持したいと考えているようである。昨今の農産物や資源価格の上昇に際して、原材料価格の上昇を理由にコカ・コーラは販売価格の値上げを打ち出したから、自然食品が原料であるようだ。1886年に誕生して以来、コピー商品は出ていない。つまり、製法のセキュリティは守られてきた。

しかしながら、現ダブリン・ドクターペッパー・ボトリングによって1891年から売り出されている、同じく米国に古くからある炭酸飲料であるドクターペッパーとシェア争いを行ってきた。さらに、ペプシもこのシェア争いに途中から参戦し強力な競合商品になってきた。これらの超類似の商品だけでなく、類似商品の炭酸飲料はたくさん開発され、コカ・コーラが炭酸飲料に占めるシェアは確実に低下している。類似商品はコカ・コーラのシェアを侵してきた。それゆえ、類似商品に過ぎないことをもって、コカ・コーラの製法情報は守られてきたと考えない方がよいだろう。

一般的に考えて、セキュリティ対策として守るべきものとは、商品や組織それ自体ではなく、機能そのものなのである。コカ・コーラが炭酸飲料に係わる周辺技術の特許を取らなかった（取れなかった）こともセキュリティが万全でない（なかった）証拠である。守る（べき）ものとは何なのか、セキュリティ対策にあたって十分考える必要があるのである。

その結果、守る（べき）ものの価値をどう測るか、という大きな問題を提起する。しかしながら、この点は本稿で取り扱わない。

3−3　情報セキュリティの特性

商品を購入する際あるいは取引を始めようとする際、一体何に関心をもつだろうか。企業の財務体質や販売している商品の安全性だけでなく、情報システムのセキュリティ・レベルも、顧客選択の重要な指標となってきている。セキュリティへの投資は、一見、売上アップに直接つながらないと考えられがちだが、昨今のビジネス環境では、競合優位性を構築する重要な投資になってきた。また、セキュリティ・コストの削減や効率化に貢献するツールやソリューションも続々登場している。

情報セキュリティの特性を順不同であげてみると次のようになる。

①情報セキュリティは組織・企業の情報システムの期待価値を守ろうとする技術である。

②情報セキュリティは、技術的な対策のみならず、組織内のルールや対外的な説明責任など、いわばソフトを含めたトータルなリスク管理を含む。

③情報セキュリティは、攻撃によって劣化する場合がある。

④情報セキュリティ技術は新しい投資に体化して進歩する。社員に対するセキュリティ教育では社員に体化する。

⑤過去に行った投資（箱）に新しい情報セキュリティ技術（ソフト）を注入しても効果は限られる場合が多い。情報セキュリティについては、過去に行った情報セキュリティ投資は現行の情報システムに役立たないと見なさなければならない。

⑥情報セキュリティは、多面な局面（侵入口）を持つ。それゆえ、すべての面でバランスよく対策をとり、向上させることが重要である。企画・設計情報、在庫・人事・資材情報から生産情報など、組織・企業で扱うすべての情報を対象にしてセキュリティを高める必要がある。共通のルールを決め、一定のセキュリティ水準を目指すベースライン・アプローチがある。

⑦情報セキュリティの様々なツール・技術は一般に相互に補完的である。しかしながら、一部に代替性がある。

⑧情報セキュリティ投資の額はその技術が守ろうとしている組織・企業の情報システムの期待価値を超えることはない。

⑨情報セキュリティ対策には「システム的」「物理的」「管理的」「人材育成」の４本柱がある。

⑩情報セキュリティのシステム的対策には、ウィルス、ファイア・ウォール、不正侵入検知、などの対策がある。

⑪攻撃者は、攻撃して獲られる価値に比較して情報セキュリティの弱い企業をターゲットにする。高い価値の情報システムを持つ組織・企業はより多くの情報セキュリティ投資が必要になる。

⑫情報セキュリティ強化は、従業員のプライバシーや情報システムの利便性が犠牲になっていくことが往々にしてある。

⑬情報セキュリティにかかわるさまざまな問題は情報化がもたらす負の側面である。

⑭組織・企業の情報セキュリティは、これまで３段階に進化してきた。「まず、初期においては被害に遭わないための技術、たとえばファイア・ウォールやワクチンプログラムといったテクノロジーが中心となってきた。次の段階では事故や不正が起きたときにどう対処するか、応急処置としてのインシデントレスポンスの概念が取り入れられてきた。そして現在は応急処置にとどまらず、事後にどのような対応をするべきか、あるいは証拠を集めるデジタルフォレンシックなどの法律的な対策等、情報セキュリティをマネジメントとしてとらえるべき段階に入った（東京電機大学情報メディア学科佐々木良一教授HP)」。

⑮情報セキュリティ対策は、企業内で費用対効果が見えにくい。どれだけ投資したからこれだけ売り上げが上がった、というような計算はすることができない。何も起きないのがベストの状態だからだ。

費用対効果が見えにくいところでどのようにして予算を捻出するか、経営陣や株主を納得させるにはどうしたらよいのだろうか。佐々木教授は、被害と費用を定量化し、いくつかの基準ポイントを決めることで予算を計算することを提唱する。「情報セキュリティはリスクだから、発生確率×損害額を算定できます。年に何回くらい起きるだろうとか、そのときの被害額とか。個人情報漏洩であれば何件くらい漏れるだろうか、１件１万円で計算しようか、３万5,000円にしようか、6,000円にしようか、などの数値を取り込んで計算するのです」（東京電機大学情報メディア学科佐々木良一教授HP)。

4　統合管理の必要性

4−1　統合管理が必要なわけ

情報セキュリティには統合管理が必要な理由は複数ある。順不同で説明していこう。

(1) 複合的な攻撃に対応

既に一部見たように、攻撃者側の技術進歩が進み、複合的リスクが増している。複合的な攻撃に対しては、ばらばらな対応をしても対策として有効ではなく、複合的な対策が必要になる。

例えば、2001年９月に登場したネットワーク・ウィルスであるニムダ（PE_NIMDA. A）は、複数のセキュリティ・ホール攻撃によるダイレクトアクション（ネットワーク・ウィルス活動)、ファイル感染、マスメーリングワーム活動、ネットワークワーム活動を行う多機能型ウィルスの一つである。Webを閲覧しただけで、メールをプレビューしただけで、またエクスプローラでフォルダを表示しただけで、ニムダが実行され活動を開始してしまう(4)。

2008年11月ころから世界中で感染被害が続いたコンフィッカー（Conficker）は、ユーザー・パスワードに対する総当たり攻撃（ブルート・フォース攻撃）で感染する仕組みを備えるほか、ネットワーク・ドライブ経由での感染、USBメモリー経由での感染（機能を利用)、さらにピア・

(4) ニムダはこの活動により、2001年当時最速規模と言われたコードレッド（Code Red）の感染被害をさらに上回る世界的な大規模感染を巻き起こした。コードレッドは基本的にWebサーバーが攻撃対象だったが、ニムダはすべてのコンピュータに感染を広げる。ちなみに、MSVistaには免疫がある。

ツー・ピアの通信機能を使って自分自身をアップデートする仕組みを持つ。一つひとつの仕組みは既に過去に例があり、それらが組み合わさっている。

また、最近のマルウェアはどれも様々な解析対策が施されており、以前と比べて防御者側の解析がやや面倒になっている。攻撃者はマルウェアの発見を困難にさせたり、セキュリティ・ベンダーらによる解析を遅らせたりするため、エンコーディングやゴミコード挿入などによる難読化、コンポーネントや実態の多段化、**デバッガ検出**[5]などの様々な解析対策を実装している。防御者側でも、このデバッガ検出を無効にする方法が考えられている。このように、攻撃者側と防御者側の間で技術の攻防がある。

(2) ランダムな技術進歩

セキュリティの技術進歩が体系的に進んでこず、ランダムな技術進歩であり[6]、順不同で開発出来る所から、いわばランダムに進歩してきた、と思われる。それゆえ、これまで導入してきた情報セキュリティ技術を、ここで見直し、最適に統合整理するべき時期にきているように思われる。

このような技術進歩観については、技術者から異論がでることが予想できるが、セキュリティ技術の進歩の有様を体系的に分析した文献はないようである。それは、あたかも、個人は癌を治す医療技術や医薬の発展を望んでいるにも係わらず、また医療・医学研究者もそれを目指して日夜研究しているにも係わらず、実際は技術発展は目覚ましく進んでいない、とさえ患者から思われるのと同じである。

---

(5) デバッガ検出とは、ウィルス対策プログラムやデバッグ・ソフトウェアなどの、バックグラウンドで実行されているプログラムを検出することを指す。プログラムの不具合をバグ（bug）、バグを取り除くことをデバッグ（debug）、バグの原因を突き止める作業をデバッギング（debugging）、デバッギングの手助けをするツールをデバッガ（debugger）、ついでにデバッギングされるプログラムのことをデバッギ（debuggee）という。

ウィルスには、プログラムのなかのデバッガ検出部分を巧妙に隠すなど、デバッガ対策を施しているウィルスが少なくない。

(6) 技術革新のタイプは、いくつかに分類される。分類方法としては、

クリステンセンの「破壊的イノベーション」、

チェスブロウの「オープン・イノベーション」、

など、いくつか提案されている。

クリステンセン（Clayton M. Christensen）は、技術進化軌道の延長線上にあるか、その軌道を断ち切るかで、技術進歩をそれぞれ持続（sustaining）技術と破壊（disruptive）技術に分類した。この概念分類は、ハードディスク業界の研究から生まれたもので、イノベーションとコントロールの相克を従来意味していた「イノベーションのジレンマ」という言葉が、既存技術がまったく異なる新規技術によって駆逐されてしまうことを意味するように変えてしまった。

この2つの概念を、もう少し丁寧な日本語で表現して、積み上げ型と飛び越し型と言う研究者がいる。文献紹介は略。

技術の発生、普及、影響の範囲の広がりに注目した技術概念であるチェスブロウのオープン・イノベーションは、1つの組織内で起きるクローズド・イノベーションと対峙され、技術のネットワーク性とビジネスモデルの創出効果に着目している。

情報セキュリティ技術の進歩は、今後は破壊的でオープンなイノベーション型になるだろうが、これまでは、全体として持続的で、各コンポーネントの技術進歩が足並みを揃えていない、と表現できるのではないかと思う。これをもって、本稿ではランダムな技術進歩と呼んだ。

(3) 対応するべき環境の変化

技術進歩面だけではない。対応するべき経済等環境の変化でも問題が起こっている。銀行へ応用を念頭に説明してみよう。市場リスクや信用リスク、システム障害といった事務リスクなど、銀行が抱えるリスクは注目される重点が次々と移行してきた。それとともに、都度それぞれの個別案件を集中的に管理する部門が様々な部署に作られてきた。同様にそれぞれのシステムも構築されてきた。今や、分散していたリスク管理機能を集約し、リスクの一元的な管理体制の構築を目指す必要があるのである。

(4) 機能の高度複雑化

ユーザーが必要としている機能は、多岐にわたる。例えばノートブックPCのセキュリティ対策を考えてみると、ウィルス対策ソフト、スパム対策ソフト、パーソナル・ファイアウォール、データ暗号化、リモートアクセスVPN（virtual private network、仮想閉域網）などのセキュリティ・コンポーネントが必要となる。しかし、それらを異なるベンダーから購入すると、当然、全体の初期投資は大きくなり、管理作業も煩雑となる。また、何らかのセキュリティ侵害が発生した場合にも、原因の究明に時間がかかってしまう。これらがコストとして跳ね返ってくる（シュエッド（2008）参照）。

また、ベンダーの販売する商用ソフトウェアだけではカバーしきれなかったという歴史的事実がある。セキュリティ分野では、商用ソフトの隙間を縫って多くのオープンソース・セキュリティ・ソフトウェアが活躍している。これは企業が直面しているセキュリティ上の問題がベンダーの販売するセキュリティ・ソフトウェアだけでは解決できないからである。

(5) 分割、セキュリティと統合管理

分割が情報などのセキュリティに有効である場合が多いことは、辰巳（2011）が多くの事例を挙げ、説明した。そのような形で分割された後のシステム全体の管理に必要なものは、言ってみれば、統合管理である。

4−2　統合管理が必要となる具体的な例（小項目）

統合管理が必要となる具体的な例のいくつかを、重複を恐れず、解説してみよう。

①シュエッド（2008）によると、主要なセキュリティ・ベンダーは世界に15社ほどある。それぞれから製品を購入し、個別にライセンス契約を交わした上で、別々に運用管理するのは複雑で非効率である。

②クラウド・コンピューティングが2008年から話題のITテーマであるが、すべての業務がクラウドで行われるわけではないし、行えるわけではない。将来は、クラウドと非クラウドは混合する。クラウド・コンピューティングとは、アプリケーションがインターネット上の中央サーバーで稼働するシステムである。

5　まとめ

著者は先に、情報セキュリティの分割やバックアップの戦略（辰巳（2011））を纏めた。それでは、本稿で入門導入編を展開した情報セキュリティの統合戦略とは具体的にどのようなものなのか、稿を改めて、詳しく論じたい。

参考文献

ドラッカー、P. F. (Drucker, P. F.)、上田 惇生訳 (1997)『「経済人」の終わり』ダイヤモンド社、1997年５月。

Gersbach, H. and Schmutzler, A., (2003), "Endogenous spillovers and incentives to innovate," *Economic Theory*, Springer, vol. 21(1), pp.59-79.

林 誠一郎 (2009)「「情報セキュリティの10大潮流」～プロローグ～「脅威を前提としたシステム」とは」ScanNetSecurity、2009年４月21日、28日。

飯島淳一 (2008)「システム統合の着眼点と考慮点—求められるのは「ビジネスとの統合」と「アーキテクチャの統合」」『月刊Computerworld』、2008年９月号。

岩井博樹 (2009)「オンライン・バンキングを狙った次世代型サイバー攻撃」2009年11月５日。

松山貴之 (2011)「アーキテクチャーとは「エンジニアの発想」のこと」『日経SYSTEMS』、2011年４月19日。

Messmer, E. and Bort, J., (2009)「セキュリティ・コストを削減に導く「３つのキーワード」：統合／SaaS／セキュリティ・サービス」*NETWORKWORLD*米国版 (Computerworld)、2009年４月６日。

Shwed, G., (ギル・シュエッド) (2008)「単一エージェントでセキュリティ管理を簡素化する」『月刊Computerworld』、2008年12月５日。

辰巳憲一・後藤 允 (2010)「情報セキュリティとその投資の分析～研究報告書～」『学習院大学計算機センター』2010年12月、pp.49-62。

辰巳憲一 (2011)「金融・経済活動における情報などの分割、バックアップと情報セキュリティ～金融セキュリティの経済学入門(Ⅰ)～」『学習院大学経済論集』、2011年１月、pp.301-321。