『学習院大学　経済論集』第49巻　第１号（2012年４月）

情報セキュリティの階層型統合管理に関する経済分析（Ⅰ）

辰巳　憲一*

1　はじめに

2011年には，特に注目される，サイバー攻撃が世界各地で頻発した。国内ではソニーや三菱重工業，そして衆議院をはじめとする官公庁への攻撃が，一般の人にも大きな衝撃を与えた。また海外では，2010年にイランの原子力発電所システムを標的として送り込まれたウィルスが発見される事件が起き，その驚きが治まる暇もなく，2011年には電子証明書を発行するDigiNotar の情報漏洩などが，明るみになった。攻撃の事例はこれだけに留まらないから，関心は否が応に高まるのである。

様々な情報セキュリティ対策をとっている筈のグローバル企業ソニーがサイバー攻撃を受け，同様に比較的堅固と思われる米国大手銀行が内部情報の漏洩に恐れ慄く，状況を2011年われわれは目の当たりにしたのである。誰もが何が起こっているのか不審に思った。一般顧客向けへのプレスリリースなどでは，対策として様々な情報セキュリティ技術の導入について言及されている[1)]が，それらをどう構成するかなど，詳細がうかがい知れない，ところがある。

---

*）　学習院大学経済学部教授。Integrated Stratified Strategy of Information Security: An Economics Approach（Ⅰ）.
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。）
本稿は多くの先行文献，ネットでの用語解説や研究者の口頭での発言に依存している。体系的でない記述をしている文献は引用できない，引用しなかった。それゆえ，ここで謝辞に代えたい。

1）　2011年５月プレステのデータベースに不正侵入を受けたソニーは，サービス再開後，個人情報保護に関する取り組みを充実する策について，プレスリリースで，次のように述べた。「より高度なセキュリティ技術の導入や，システムへの侵入および脆弱性をモニタリングするソフトウェアの追加，暗号化方式の強化，ファイア・ウォールの増設などデータセキュリティシステム強化を含む安全管理措置を講じました。また，不審行為の恐れのある行動パターンをより早い段階で警告し，ネットワークへの不正侵入の動きを検知するシステムの導入など，お客様の個人情報をより高度に保護する対策を実施しました」。
他の事例としては，米国国務省の機密外交公電を公開したWikiLeaks は，さらに，米国大手銀行の極秘社内文書をまもなく暴露する見込みという予想を受け，世界中の政府機関や企業がデータ・セキュリティに関する懸念を募らせた，ケースが存在する。
これに対しては「機密情報にはアクセス権の制御や区分レベルの導入はもちろん，効果的な監視といった対策が欠かせない。例えば，機密情報にタグつけ，審査もしくは許可を受けていない人物が保護ドメイン

その関わりでみると，情報セキュリティは技術，機器，思考，アーキテクチャ[2] のいずれもが，統合管理の方向を向くようになっている，ことに気付かされる。「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。当然，これまでも何らかの統合管理はあった。それが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名付けることができる。新しい情報セキュリティ技術を構成するのは，多層防御や多層管理である。

以下では，様々な情報セキュリティ技術を多面多層に備え管理する，いわば情報セキュリティの階層型統合管理を，システムや機器の代替性・補完性，相関分析，様々な環境での最適化，その一例としてポートフォリオ理論，産業構造の分析，などの経済学やファイナンスの基本概念を使って，経済学的に考察することにしよう。

なお，攻撃者は様々な動機で行動していることが予想できるが，本稿では攻撃者の動機を問うことはしない。また，セキュリティ・ベンダーの製品とその機能は解説することになるが，その製品名は CM になるのでできるだけ挙げるのを避けたい。そして，エンジニリング上の技術用語を使うのも避けることにしたい。

２　情報セキュリティ

２－１　情報セキュリティの機能

情報セキュリティ問題は，①情報システムの大規模化と複雑化，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，などの複数の要因からもたらされたが，③愉快犯だけが目的ではなくなったサイバー攻撃の多様化，という攻撃者側の要因に対応しなければならなくなった，という点も大きな比重を占める。しかも，④ネットワーク拡大と⑤ IT コスト削減，という経済や技術が要求した複数の要因のために，セキュリティ関連の負担が大きく増えてしまった面を否定できない。

（１）セキュリティ機能いろいろ

いろいろな局面とレベルで情報などの防御，制御が行われる。ドロボー等の侵入の被害を防ぐためにわれわれが現在取っている次のいろいろな方法や手段を参考にして考えてみよう。われわれは，

侵入を防げる家の構造にする，

家のドアや窓の鍵を頑強なものにする，

外からこれを移動させられないようにするといった措置が必要だ」という感想・意見が主流である。

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。
情報システムを構成する要素は，サーバー，ストレージ，ネットワーク装置，OS，データベースソフト，ミドルウェアなどである。アーキテクチャとは，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。

現金などを守るための金庫を備える，
ガードマンによる警備を依頼する，
各種の盗難予防センサーを付ける，
ＴＶモニターによる異常の監視を行う，
等々の防犯対策技術を設置してきた。アウトソーシングには，
現金を，安全と考えられている銀行に預金として預ける，
銀行の貸金庫に貴重品を保管する，
等の方法がある。

以下では，このような事例を参考にして，いろいろなセキュリティ機能を分類してみよう。後述の，侵入防止や侵入阻止と侵入被害防止の間にはHTS（ハザード・トレラント・システム）という考え方がある。 HTSとは，たとえ侵害等の脅威（ハザード）が発生しても，実際の損害となるまで結びつかせない，もしくは損害を極小化する，ハザード（脅威）に寛容なシステム確立に必要な技術を指している。

いくつか前提としている事柄を前もって述べておけば，例えば，防災用に避難ハッチを取り付ける，など（避難）経路を増やすことが大きな建造物では行われる。しかしながら，脅威から効果的に防御するためには，逆に攻撃を受ける経路の数を減らすのが有効である。それゆえ，以下では防御する組織の行動目的に照らして，最適な経路数になっており，これ以上経路の数は減らせないとして議論を進めよう。

また，根本的な問題として，まず，解析できていない（解析できない），つまり分からない攻撃には対応できない，ことを前提にしておかねばならない。いわばドロボー等が侵入したかどうかわからない場合は分析対象にならない。

（2）情報セキュリティ機能の特徴

情報セキュリティを，ユーザーつまり企業や人を中心に対策をとるか，情報データつまり物を中心に対策をとるかの２つに分けて考えるとわかり易い場合もある。

また，守るものが情報である場合，情報を消滅されればふつうの財の盗難と同じであるが，**改ざん**されたり，一部だけ消去されてしまうと情報の価値がなくなる，というその他の財にない特徴がある。

さらに，PCのなかにある情報については，コピーを取れば，あるいは呼び出して閲覧すれば，そういう行為をしたという記録が残る。しかしながら，紙に書かれた情報は，**書き写し**たとしても，あるいは**写真を撮**っても，何の変化も起こさない。その盗んだ情報を使って何か行動をとることにより，盗みが発覚する可能性が生じるが，盗んでも使用・悪用しなければ，あるいは行動しなければ発覚もしない。このような特徴もあるので，情報に関しては，攻撃者の侵入にはとりわけ注意が払われてきたし，注意を払わなければならない。

２－２　セキュリティの機能とその手段

セキュリティの機能とその手段を，まずは伝統的方法から展開してみよう。同じセキュリティ手段でも，内容によって程度が異なる，ことに注意して分類しておきたい。

２－２－１　セキュリティの機能と伝統的手段

（1）侵入口検知機能

侵入者の入り口を検知する伝統的方法としては，コンサル等の専門家や警察からアドバイズ

を受ける，などがある。現在，警察は「防犯診断」をおこなっている。

（2）侵入者調査

侵入を簡単に検知するには，眺めの良い場所に高い構築物や櫓[3] を作って陣取ればよい。武士の時代には天守閣から見張る，近年には門番，受付，監視カメラ・TV モニター・熱センサー，などを置く，方法がある。現代の民家では，透けて見える生垣にし，庭にはジャリを敷く方法などがある。

（3）侵入防止

不正な侵入を防ぐ伝統的方法としては，土塁・堡塁（bulwark, earthwork fortification），堀（canal, ditch）・外濠（moat, foss），切岸，堀切，防波堤・防潮堤（breakwater），などがある。侵入経路を少なくするために，門の数を少なくする。道をつけない，道を狭くする，などは戦国時代の方法である。（小）山の上に城などを築けば，侵・進入は防げるが，いろいろ不便はある。

昔の大きな城では外堀・外堀土塁・内堀土塁・内堀と何重にも防御している。堀・外濠については，攻撃手段の進歩に応じて，距離が狭い「薬研堀」から矢や鉄砲を防ぐため距離が長い「箱堀」へと変化している。

塁堡・堡塁などと呼ばれた城塞・要塞（redoubt）では，大砲が主要防御武器として進歩して，多数の大砲が互いの死角を補い合うように設計された，日本では幕末に五稜郭などの城で著名な，「稜堡（りょうほ）」など，がある。海堡や野堡は設けられた場所による分類である。他に，円形の砦を陵堡と表現する場合もある。

広域にわたる物理的な囲いによって安全を確保するゲイティッド・コミュニティもある。最近の欧米の高級住宅地で見られる方式である。最近の日本の団地にも取り入れる動きがある。過去の例として，ヨーロッパの城壁に守られた旧市街，砦がある。

民家では，門・玄関，最新の鍵，をつける，鉄条網を張り巡らす。「監視カメラ作動中」のシールを玄関に貼る。警備員，警備保障会社と契約[4]，「セコムしている」ことを知らせるためにシールを玄関に貼る，などがある。その他様々な自己防衛策がある。商店ではレジの現金引き出しに，引き出した際に音が鳴るように，鉦（かね）などを付けるという方法が昔とられていた。食堂や外食店舗では，レジによる現金の取り扱いを避け，券売機をおくという方法もとられている。玄関・窓には，人が来ればライトが付くあるいは警報音（ブザー）が鳴るセンサーをつけたのはここ20年くらいのことである。高圧電流フェンスにする，レーダーを設置する，などは特殊な施設の防御方法である。

---

3) 櫓（やぐら）とは，城郭などに防御用あるいは物見用に建てられた仮設または常設の建築物である。後代には，礎石の上に建てられ，防火と防弾を考慮して厚い土壁が塗られ，屋根は瓦で葺かれるなど，している。大坂城本丸東面の三重櫓と多門櫓は堅固なこと，名古屋城の辰巳隅櫓は南東の隅に造られ，櫓の役割を果たしていること，をそれぞれの言葉が示している。
大型の櫓の構成は，中央に身舎（もや）を設け，周囲に入側・武者走（いりかわ・むしゃばしり）を廻らし，その構成は天守に近い。熊本城の五階櫓のように身舎の内部に壁を設けていくつかの部屋に区切ることもあった。櫓は時代が下がる毎に進入防止の役割の方に重点が置かれるようになってきていることが窺われる。

4) いくつか違いを記しておこう。ふつうの警備員は常駐するが，セコムなどとの警備保障会社契約では連絡を受けて警備員が駆けつけてくる。

（4）侵入阻止

侵入を阻止する伝統的方法としては，凶暴な番犬，強力な武器での自己防衛，などがある。内部から迎撃・攻撃するために土堀や櫓に設けられた小窓である佐間（さま）は，封建時代の城に設けられ，石落としや油落としなどを行い，火縄や弓矢を射り，鉄砲を打つ，所である。鉄砲佐間や弓佐間などの区別がある。

車に忍び寄る窃盗犯がドアをこじ開けた衝撃やエンジン始動などを感知して大きな警報音を発し退治してくれる盗難警報器の例もある。窓に補助錠をつける，などもこの分類に入れられるだろう。

（5）侵入被害防止・被害局所化

侵入されても被害を受けないようにする伝統的方法としては，金庫に貴重品を保管する，などがある。カムフラージュ（金庫を隠す）や要素分割（金庫を複数おき分散して保管する），などもある。他分野の例をあげれば，災害対策において減災と言われている様々な方法がある。あるいは，発病対策には，細菌が身体に侵入しても発病しないよう免疫機能を利用する療法がある。

被害局所化の伝統的な方法としては，金庫を複数備え，脆弱な金庫には，あるいは危険な場所に置かざるをえない金庫には小額の現金しか置かない。各部屋を個別にロックする，などの方法がある。工場を分散化するねらいの１つは，自然災害の影響を小さくすることであったが，最近は電力会社の同一管轄地域に設備を集中するべきではないという要因が加わった。

（6）漏洩被害防止

伝統的方法としては，金庫の管理方法がある。複数の責任者を決め，相互の承認がなければ開錠できない仕組みにする，などがある。

（7）漏洩被害阻止

従来，方法は特に多くない。商品に鎖を付ける，商品にタグを付け出口に検知装置を置く，方法が商店あるいは図書館ではとられている。

（8）外部アクセス防止阻止

伝統的方法は，金や貴重品を持ち歩かないようにする，しかない。

（9）駆除

侵入し居座っている攻撃者やその手先が罪を犯さないように駆除する。具体的には，ドロボー等を縄でぐるぐる巻きにする，手錠をかける，等などである。

２－２－２　セキュリティの機能と様々な新しい手段

現代の新しい手段には，それでは，何があるのであろうか。

（1）侵入口検知機能

どこが侵入者の入り口になりうるかを検知する脆弱性検査（Penetration Test：ペンテスト）があるが，これは擬似ハッキング検査，擬似アタック検査とも言う。昔はファイア・ウォール検査サービスなどと呼れた。技術としてはファジング（fuzzing）[5] がある。

5）　ファジングは，ファザーとも呼ばれる，ソフトウェアや機器の脆弱性を探す技術である。検査対象のソフトや機器に対して，それらの開発者が想定していないような，非常に長い文字列や大きい値などのデータを入力し，その応答から脆弱性を探し出す。応答として異常な結果を返したり，動作が異常終了したりした場合は，その処理をした箇所を詳細に調べる。

（2）侵入者調査

まず認証があげられる。IC カード認証，手のひら静脈の認証，歩いている人の顔を自動認証する「ウォークスルー顔認証システム」などがある。

システマテイックには，これらは IDS（Intrusion Detection System 侵入検知システム）やレピュテーション・システム[6] と呼ばれるものになる。機密情報の程度に応じてアクセス制限（入退室管理システム。顧客，パートナー，ベンダーにも適用）を変えるシステムの導入，トラフィック・モニタリング（異常な通信量があるかないか等の調査）などの様々なアクセス制御の一部，もこの概念に含まれる。

さらに，業務委託先に対しても同様な管理（業務委託先の過失で情報漏えいが発生した場合の損害賠償請求など法的な手段をとることなどを含む）を行う。あるいは情報セキュリティ格付けを活用して下請け企業と取引する，ことなども現実味を帯び出している。

かつては大きな問題にならなかった現代的要素もある。それは，対策が採用されるかの視点として，脅威の発見を早める，という時間的要素が挙げられるであろう。発見が早ければ早い程，対策も早く採れるようになり，対策は効果的になる。

（3）侵入防止

伝統的な方法であった，道を狭くするという対策は現代では，不正アクセスを防ぐ「ファイア・ウォール」や「IPS（Intrusion Prevention System 侵入防止システム[7]）」が該当する。二重に土塁を設ける過去の方法に該当するのは，スクリーンサブネット型のファイア・ウォール[8]，などである。

様々な具体的な方法を順不同で説明すると次のようになる。マルウェア（悪意のあるプログラム）侵入を防ぐ「アンチウィルス」を導入する。セキュリティ・ソフトのパターンファイル（定義ファイル）を常に最新の状態にする。OS などの修正ファイル（パッチ）を頻繁に適用する。パスワードによるユーザー認証を行う。「ワンタイム・パスワード」と呼ぶ使い捨てのパ

6） 侵入検知システム IDS（Intrusion Detection System）は，常時，パケットの中身を監視して攻撃を検知する。監視したパケットの中身と，すでに登録してある攻撃パターンのパケットとを照合して，一致すれば攻撃とみなして管理者に知らせるシグニチャ型が１つのタイプである。また，通常状態のプロフィールを IDS に登録しておき，通常状態とは異なる大量のトラフィックが流入した場合，異常とみなして管理者に知らせるアノマリー型が第二のタイプである。
レピュテーション・システムとは，（一般にはリアルタイムで）送信者の評価を行うシステムで，評価値を出すなどの方法がとられる。これを行うと既知のスパムはもちろん，未知のスパムやウィルスの送信者を評価し防御する事が可能になると言われる。フィッシング対策としても有効である。また，スパムやウィルスを，最初から，ブロックし，切り取ってしまえば，システム本体への負荷を，あるいはスパム対策ソフトへの負荷を小さくできる。

7） 侵入防御システムの IPS（Intrusion Prevention System）は，侵入を検知するだけでなく，攻撃を検知すると自動的にその攻撃パケットの破棄，通信の遮断などの防御を実施する。例えば，機密情報を格納したデータベース（DB）に出入りするデータすべてをストレージ（外部記憶装置）に記録して，大量の顧客情報を取り出すなど疑わしいデータの流れを検知し，必要に応じてアクセスを遮断する。侵入を管理者に知らせ，管理者が対策を施すまで一般に時間がかかってしまうが，自動化によって，対策が後手になることを避けることが出来る。

8） スクリーンサブネット型のファイア・ウォールとは，インターネット側に１台，プライベートネットワーク側に１台のパケットフィルタリング・ルーターをそれぞれ設置し，それらの間に非武装地帯（DMZ, de-militarized zone）を置く構成である。DMZ には，要塞ホスト（十分なセキュリティ対策を施したホスト）を設置する。これには構成が複雑になるデメリットがある。

スワードで不正なアクセスを防ぐ。パスワードの生成と利用方法にも工夫を凝らし，数秒に一度の頻度でユーザーを認証する。ウェブサイトへの悪意のある書き込みなどを防ぐ「WAF（web application firewall）」を導入する。コンテンツを改ざんし悪意あるサイトへ誘導するための攻撃を防止する方法もある。脆弱な囮（ハニーと呼ばれる）を置き，それを攻撃させ，攻撃者先や攻撃方法から危険を探る方法もある。

（4）侵入阻止

ユーザーの高度認証を行えば侵入を阻止できるが，それには，ホワイトリスト作成，公開鍵，電子署名検証，発行者署名付電子チケット（セキュリティトークン）などがある。最新の方法には，バイオ認証があり，すでに一部では普及している。攻撃者に超多大な計算量を課し断念させる難文化という方法もある。

（5）侵入被害防止・被害局所化

情報を暗号化しておけば，仮に情報が盗まれても読み取れないようにできる。これが強固な暗号が求められる理由である。

スパム・メールからの感染を防ぐ「アンチスパム」がここに含まれるであろう。さらには，リモートでのロック・アンド・ワイプ（端末を無くしたときに遠隔からロックを掛けたり，データを消す）がある。一定時間後メモリーが消滅する USB もある。

カムフラージュ（情報を隠す）や要素分割（情報を複数に分割保存），表示の難読化・記号化などのブラックボックス化，などがある。ワンタイム・パスワード[9]（フィッシング詐欺で銀行口座の番号を奪われたとしても，ワンタイム・パスワードを採用していると奪われた情報はまったく役に立たない[10]）。

被害局所化にはシステムを分散化，ブロック化，するのが有効な方法になる。情報資産を遠隔地に保管するデータレプリケーションが該当する。

（6）漏洩（被害）防止

限られた者だけにわかる暗号化を情報に施す。シンクライアント専用端末（シンクライアントは PC ではなくサーバーに PC で使うデータを保存することでセキュリティを高めることができる仕組みである）を使う，等の方法がある。従業員のパソコン操作を監視するのも１つの方法である。社員にわざと偽のメールを送り，無意味に開封しないように訓練するサイバー訓練は最近の日本で多く行われるようになっている。

9） ワンタイム・パスワードは，刻一刻と変化する暗証番号を発生させる IC チップを利用する。利用者に予め，IC チップを組み込んだカードや USB 等のデバイス（媒体）を配布する。デバイスは，発行時に設定したデバイス所有者番号と利用する時刻がパラメーターとなった特殊関数により暗証番号がランダムに発生する仕組みになっている。例えば一分おきに６桁の暗証番号をランダムに発生させる。
利用者は，ログオンする時，この媒体に表示された暗証番号をインプットする。その結果，ログイン ID，利用者の決めた暗証番号，一定時間ごとにランダムに変化するワンタイム・パスワードの３つが一致しなければ，ログインできないというシステムを構築することが可能となり，例え ID 番号と暗証番号が盗まれても，ワンタイム・パスワードは刻一刻と変化しているので，このデバイスも同時に盗まれない限りセキュリティは保たれる。

10） しかしながら，Man-in-the-browser（MITB）攻撃によって攻撃者はワンタイム・パスワードを回避できる。MITB 攻撃とは，標的 PC がオンライン・バンキングなどのサイトにアクセスしたタイミングで，不正プログラムを動作させる攻撃を指す。サイバー犯罪者は，この手口を使うことで，現状のオンライン・バンキングの認証機能を回避できる。技術的な内容については岩井（2009）を参照のこと。

（7）漏洩（被害）阻止

社内や自宅のPCの管理（メールに機密情報などが含まれていないか監査するフィルタリング。システムの利用状況を記録するログ管理。）や盗難・紛失時にノートPCのデータを遠隔消去する技術がここに含まれる。PC持ち出し禁止措置はいろいろな意味で厳しい方法である。

メールの誤送信による情報漏洩事故が予想外に多く，それを防止することが必須になる。それには「送信メールの保留」「添付ファイルの暗号化」「メール本文と添付ファイルの分離」「送信拒否」の４段階がある。

後述の出口対策で比較的詳しく触れるように，バックドア通信の抑止と遮断ができれば究極の方法になる。

（8）外部アクセス防止阻止

外部アクセスを防止・阻止する必要があるのは，ユーザーが悪意ある添付ファイルを開いたり，有害なWebサイトのリンクをクリックすれば，それらに仕込まれたマルウェアがソフトウェアの脆弱性を悪用してマシンを乗っ取る，というようなことが起こるからである。

不正サイトへのアクセスをブロックする「URLフィルタリング」「コンテンツ・フィルタリング」，Webサイト上で個人情報などを登録する際に安全性を確認できる認証（機構）制度，などが対策になる。

（9）駆除

侵入し居座っている攻撃者やその手先が罪を犯さないように駆除する。

２－２－３　セキュリティの機能と様々な手段のまとめ

このように見てくると，減災や堅牢化という概念は，古くから存在するが，これらがセキュリティ機能のどの概念に相当・該当するのか，分類に迷ってしまう程かなり広い概念であることがわかる。情報セキュリティ技術は，その多くのものが，多方面に多段階に分類できる，どこかの分野に所属していることがわかる。しかも，それぞれの方面に複数のツールが存在することがわかる。

また，（1）から（8）までは，予防と調査（ただし，（4）では一部は実力行使を含む）に限られている。そして，従来のセキュリティ・ソフトの多くは，攻撃発生を抑止する機能（脅威低減機能）ではなく，発生した攻撃が成功しないよう防御する機能（脆弱性低減機能）である，ことがわかる。

２－３　情報セキュリティのその他の具体的対策

２－３－１　組織継続の視点

防止や阻止などという侵入対策だけでなく，侵入が起きてしまった際に被害を少なくするという視点をさらに掘り下げ，①なるべく早く回復する，②再発を防ぐ，③補償，などの視点も採る必要がある。言ってみれば，組織の継続を考慮した情報セキュリティ対策が必要なのである。

取引所のシステム・ダウンに対して，５年間を目途に99.999％の信頼度・安定性（数年に一度のダウンに止め，ダウン時間は10分以内）を目標にする，ように仕組まれる，などが事例となる。

（10）早期回復

回復するにはバックアップしておくことが必要である。既述の一定時間後メモリーが消滅す

るUSBだけではダメでUSBの内容はバックアップをとっておく必要がある。

早期に回復するとしても，闇雲に早いというのは現実的ではない。どこまで復旧するかというポイントと復旧にどれくらい時間を掛けて良いか，の視点を持たなければならない。事業やプロジェクト単位ごとに目標復旧ポイントと，可能な限り迅速かつ効率的にオンライン状態に戻る目標復旧時間を設定するのが具体的な方法になる。

失ってもよいデータの量はどの程度かの視点がRPO（目標復旧ポイント（Recovery Point Objective））で，失うことを容認できるデータの量を，時間を単位として測定する。これは不都合なイベントが発生した瞬間から，直前のバックアップポイントまでを遡った時間で表現される。例えば，RPOを１時間とする場合は，イベントまたは災害の発生後に，イベント発生１時間前までの全データが復旧されなければならない。発生前の１時間の間に処理されたデータは，失われたものとみなし，諦めるのである。

何時間以内に復旧できれば組織や会社は生き残ることができるかの視点がRTO（目標復旧時間（Recovery Time Objective））で，災害発生後システムがダウンしていても影響しない時間の最大長を表す。RTOは，災害からの復旧に要する時間に，業務の再開に要する時間を加えた時間となる。RPOは災害発生時から直前のバックアップまでさかのぼって測定するのに対し，RTOは災害発生時から全データが復元されていなければならないある時点までの時間である。

これらとは別に追加するべき問題がいくつかある。バックアップ・システムも同様に起動しないことが考えられ，新システム導入に際しては旧システムも残し（library holdback），ダウンに備えて稼働できるようにしておくことも必要になる。さらにはシステムの三重化あるいは多重化によって切り替え時間を短縮する。また，視点を変えて，間違いを探しやすくするためにシステムを複雑にしない，という観点もありえる。

バックアップについてであるが，それが小額の物品で在庫流通量に心配がないなどの理由があれば，急いで再購入するという方法がある。多額にのぼる物品であれば短期リースするという方法もあり，米国ではそのようなサービスを提供する会社が存在する。

（11）再発防止

悲惨な出来事が起こるたびに再発の防止が誓われるのが常である。しかし残念ながら，現実には，一度起きたことは二度三度起こる。イベントが起こるたびに，原因を探り，その対策をとっていくことによって再発を防ぐことができるケースもある。そして，このプロセスをシステム化することが必要である。セキュリティ監査という業務のねらいは再発防止である。

（12）補償

被害の額を事前に評価し，補償の仕組みを広く公表しておけば，内に対してはセキュリティ意識を高める役割が期待される。外に対してはセキュリティの高さを誇示できることになる。

しかしながら，セキュリティ・イベントのタイプごとに被害の額を測定する評価モデルを構築するような作業は，なかなか難しく，緒に就いたばかりである，といってよいように思える。また，プライバシー侵害賠償の判例がいくつか存在するが，経済学的根拠が明瞭でないため，筆者の考えでは，将来的に課題を後送りしているように思える。

２－３－２　事後検知とその対策

上記の情報セキュリティ機能の例外となる事例があるので説明しておかねばならない。侵入者検知がまったくできず，侵入防止や阻止も有効にできない場合がある。

（1）被害発覚とその時点

既述のように，磁気記録された機密情報ファイルやパスワードのようなデジタル・データは，侵入者が盗んでも原本は消滅しない。侵入犯は情報を「コピー」したに過ぎず，複写された側には，被害の痕跡は残らないのがふつうである。その結果，被害は直ちには発覚しない。

被害は，例えばクレジットカードに係わる犯罪の場合，出金が記帳され預金口座残高が減る時点までわからない，ことがある。あるいは，企業極秘情報の盗難については，競合企業が強力な新商品を売り出し，その仕様などが公表され明らかになる時点までわからないことがある。場合によっては，被害額さへわからない場合が存在する。

預金口座からの出金を止める，あるいは新商品が生産されるまでに競合企業を告訴する，ことが必要である。

（2）その原因

クレジットカードでそのような犯罪が起こる原因は，端末の管理が他の組織あるいは他人任せになってしまっており，制御不能である，からである。それにも拘わらず，対策はこちらが採るしかない。しかしながら，コストをいくらかけても，制御不能は減らせるが，完全には制御できない。

（3）速やかな事後検知～対策例

１つの事例はクレジットカードにみられる。クレジットカードの管理は個人が行い，オーソリイゼーションはオフラインで持ち込まれたクレジットカードで行う場合，被害発覚は遅れ，セキュリティ・イベントの発生は避けることができなくなっている。被害発覚も即時でなくなっている。即時検知でなく，事後検知になってしまっているからである。その対策としては，事後検知を速やかに行うしかない。

２－３－３　情報漏洩問題の詳細

（1）情報漏洩問題とは

情報漏洩に対しては，ユーザーを中心に対策をとるか，データを中心に対策をとるかの２つに分かれる。前者には，「ユーザーのアクセス権限」を設定して機密データの流出を防ぐものが多い。例えば，「正社員はすべてのデータにアクセスでき，USB メモリーなどでの持ち出しも自由とする」が「契約社員は経理のファイルにはアクセスできない。USB メモリーなどでの持ち出しを禁止する」といったルールを作る対策である。

これに対して後者は，その企業にとって機密であるデータと機密でないデータを区別し，機密データだけを外部に漏えいさせないようにする。このデータ中心型の漏洩防止システムは DLP（data loss prevention あるいは data leak prevention ）と呼ばれる。

さらに大きな問題は，社員の脳と筋肉に記憶され蓄積された情報はアクセス権限設定だけでは漏洩を防げない点である。社員の転職によって情報は漏洩する。逆に，新人転職社員の途中入社によって情報がスピルオーバーしてくる。これが情報スピルオーバーという研究分野でモデル化される概念で，情報漏洩が合法的にどの様に起こるかを分析しており，その研究分野では情報漏洩をいかに防ぐかは直接議論の対象にはなっていない。有能な社員が退職しない，インセンティブのある雇用システムや賃金体系が情報セキュリティ対策の手段の１つとして入ってくる。その分析の例として Gersbach and Schmutzler（2003）などがある。

（2）情報の持ち出し阻止

外からの攻撃に備える，進入防御（Outside/In defense ）あるいは防衛境界線防御（perimeter

defense ）が従来の防御の基本であった。

しかしながら，泥棒が家から出て行く時，物も人も一切出させないようにすれば，犯人は捕まえることができ，被害はなくなるわけだ。それができない場合は，盗んだ物だけは置いていってもらう，ことができれば盗難の被害は実際上なくなってしまう。

伝統的には，進入者の逃走を防ぎ，物の持ち出しを阻止するための手段が，数多く考え出され，用意されているわけではない。そのための有効な手段もなかった，と言ってよいように思う。不審者の進入さえ防げば，その退出は考えなくてもよいと，警察は考えないが，一般の人はそう考えてしまったのかもしれない。

現代の持ち出し阻止（Inside/Out defense ）は次のように行うべきである。攻撃者は，ＲＡＴ（remote administration tool ）と総称される遠隔管理ツールをシステムに偲び込ませて情報を盗み出す。それゆえ，進入するのは賊ではなくＲＡＴで，なるべく早くその進入に気付き，気付けばなるべく早くＲＡＴを隔離する，必要がある。

（３）出口対策

新しいタイプの攻撃に対処するには，「もしウィルスに感染しても情報を流出させない」という，感染を前提とした対症療法的な考え方も必要となっている。入口対策をしておくことは大前提とした上で，従来の入口対策とは反対の「出口対策」である。今後のセキュリティの考え方として，入口と出口はペアで考える必要が出ている。課題は，入口で何を遮断し，出口で何を遮断するのか，になっている。

ウィルスは侵入しただけの状態では具体的な活動を行わないのが，これまでのところ，普通である。ウィルス自体の機能強化だったり，システム最深部への侵攻，システムの破壊といった行動は，すべて外部からの指示で発動する。このとき，ウィルスと外部の攻撃者を繋ぐのがバックドアを使った通信である。このバックドアを経由した，ウィルスと外部の攻撃者の連絡を絶ち切ることが，窃取や破壊というウィルスの活動を停止させる最も有効な手段となる。つまり出口対策の最終的な目的は，バックドア通信の抑止と遮断である。相馬（2011）はこの技術を比較的詳しく展開しているので参照のこと。

出口対策にはいくつかレベルがある。インターネットへ向けてのアウトバンドの通信を，SOC（セキュリティオペレーションセンター）で有人監視をする，のが初歩段階の対策である。サイバー攻撃やマルウェア対策としての出口対策機能を搭載した Web フィルタリングソフトは既に提供されているので，それを導入するのが普通の対策になりつつある。企業の根幹をなす機密情報をインターネットから切り離すのが究極のセキュリティ対策になるが，機能的にネットが不便になる恐れがある。

（４）ユーザー自身が持っている脆弱性に対する対策

攻撃者は，政府機関からの（誤）送信を装い，ファイルを開けてみたくなる心理を狙う新手を使うようになっている。また，ユーザーの心理を付いたり，善意を利用する，いわゆるソーシャル・エンジニアリングを巧みに用いて攻撃するようになっている。それゆえ，ソーシャル・エンジニアリングに対する対策が情報セキュリティのなかでも大きな比重を占めるようになっている。情報システムの脆弱性だけでなく，ユーザー自身つまり人間が持っている脆弱性に対する対策が必要になってきているのである。

そのため，心当たりのないメールが来て添付ファイルの閲覧を求めていても，社員や組織構成員がむやみにファイルを開かないよう，また不用意に会社や組織の情報や個人（の貴重）情

報を入力しないよう，に注意する動きが日本企業にある。それは，わざと添付ファイルを送ったり，偽の上司や偽の人事部からメールを送り，個々の社員や組織構成員の不注意度を確認し，注意を喚起するような活動が行われている。

それらが，予防接種（inoculation あるいは vaccination ），や避難訓練（refuge training ）あるいはサイバー訓練（cyber drill ）と呼ばれる活動である。

攻撃者によって狙われる情報は会社や組織にとって秘密性の高いものである上，攻撃を受けること自体が会社や組織のイメージ悪化につながるとの恐れがあるという考え方が根強くあり，攻撃を受けても被害はもちろんのこと，攻撃があったこと自体が公表されることはほとんどない，とみられている。このため，このような訓練は，攻撃を防ぎ，被害をなくすだけでなく，秘匿性をも維持できる。そのため，日本企業で広く行われるようになっているのである。しかしながら，攻撃の実態を益々つかみにくくしているのが実情である。

２－４　情報セキュリティの進化

２－４－１　情報セキュリティのソフト化

情報セキュリティは，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進歩ではない。これ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もいくつかあるが，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。

２－４－２　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，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，と言われる。

最近では，現状回復（リカバリー）機能をアウトソーシングする RaaS（Recovery-as-a-Service）という段階までに達しており，専門会社などもある。RaaS は，いわばリカバリーのクラウドであるので，クラウドのメリットを享受できるとともにその欠点も共有する。RaaS のメリットとしては，①初期コストの低減を図れる，②リカバリー全体の一貫性が確保できる，③最新の専門的なノウハウを活用して複雑な構成（何をいつ，どのような頻度で行うか）を的確に判断し対処できる，などがあげられる。

（2）Endpoint Security

例えば，一例（良い製品という意味で示すわけはない）をあげれば，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。

このように複数のセキュリティ機能をシステムとして統合するソフト・機器が生まれている，ということである。

（3）UTM や次世代ファイア・ウォール

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。しかしながら現在では，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・フィルタリング等などといった機能を追加した UTM 製品やサービス[11] が2000年代前半に登場した。

UTM（Unified Threat Management，統合脅威管理）は，複数のセキュリティ機能を1台のきょう体に詰め込んだ，企業向け装置の総称で，企業の LAN とインターネットなど外部ネットワークとの境界に設置し，セキュリティゲートウェイとして使用する。UTM 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 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，と批判される。その結果，パフォーマンスや制御に限界がある。当初の UTM は，ファイア・ウォール装置ベンダーが製品化していたからである。

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。これを，従来のものと区別して，次世代ファイア・ウォールと呼ぶ業者もある（これは名称だけの問題で誤解を産みかねないが，）。それゆえ，現在では，IDS/IPS 装置ベンダーやセキュリティソフトベンダーが UTM 製品をラインアップする一方で，ルーターベンダーは UTM の機能を搭載した企業向けルーターを出している。小規模拠点向けの機器から大規模拠点 / データセンター向けのハイエンド機器まで，多数の UTM 製品がある。

最近は特に，アプリケーションの利用に注目したファイア・ウォールが必須の機能になっている。

（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。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上に，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管理することも可能となっている。

11） 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導入効果がある。しかしながら，その定義はベンダーによって実際上大きく異なる。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。

最後に，情報セキュリティの目的を要約しておくと，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。**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，常時侵入を試み，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。

２－５　サイバー攻撃の進化

攻撃者も攻撃手法を進歩させている。また，防御者が新しい防御技術を実装した場合にはそれに対応した手段を選ぶ。例えば，小売店が防犯用に熱センサーを導入したとわかると，侵入者は防火服を着こんで店に忍び込んで熱センサーをかいくぐる，という具合である。

（１）ネットワーク・インフラを狙う攻撃

最近のマルウェアは，メールを大量に送り付ける感染拡大策をとらず，多くのユーザーが使っているソフトウェアの開発元を狙うようになってきた（Zaytsev (2009)）。

攻撃者が手っ取り早く多くの標的に攻撃を仕掛けるには，ネットワークそのものを狙う方が効率的である。その結果，インターネット接続事業者（ISP）やソフトウェア・ベンダーへの攻撃も増えた。

様々な攻撃手法が登場し，セキュリティ対策を施すべき場所はサーバーやネットワークなど多岐に渡り，企業の情報システム全体に拡散するようになってきた，のである。

PC のすべてにセキュリティ・ソフトが実装されていても，不正アクセスの経由はありえる。サイトに接続可能な PC をウィルスに感染させ，サイトへの FTP 接続情報を不正に取得すればよい。その結果サイトの一部ファイルに対して改ざんが行え，サイトにアクセスしたユーザーを無関係の外部サイトに誘導できる。

対策としては，すべてのファイルに対して改ざんの有無を都度チェックし，改ざんされたファイルに対しては復旧・回復を行う。また，FTP アクセスについても停止措置を行う，ことなどが必要になる。

（２）ソーシャル・エンジニアリングを使う攻撃

ソーシャル・エンジニアリングとは，再度簡単に要約すると，盗み聞き，盗み見などが潜在的に好きな，人間の心理や行動の隙を突くことで情報を不正に取得する手段の総称である。人間の本能や本性，あるいは善意を巧みに利用する攻撃である。上司，監督官庁，友人名でメールを送り，開封させるように仕組むことなどが事例になる。

（３）自動化された攻撃ツールによる大量無差別型攻撃

サイバー攻撃は，当初，無差別（indiscriminate）攻撃で，徐々に大量化したという認識が持たれてきた。しかしながら，最近は形態が変わってきた。

一例はリモート・ファイル・インクルード（RFI）攻撃である。RFI 攻撃は，まず，検索サイトを利用して，攻撃者の設定した条件に該当する標的サーバーをリストアップする。このようにしてまず攻撃できる標的サーバーを選ぶ。そして，Web アプリケーションの脆弱性を利用して標的とするサーバーに，外部のサーバーから悪意あるファイルを読み込ませる攻撃である。標的サーバーのシステム情報を取得するなどの行為を行う。

（4）標的型攻撃

特定のユーザーや組織を狙った標的型攻撃は，海外では Targeted Attack と呼ばれ，スピア攻撃（Spear Attack）とも呼ぶことがある。

攻撃対象を絞ると，攻撃対象に即した工夫を仕込むことが出来，詐欺などの成功率を高められる（攻撃を検出されないような工夫を凝らせるので，攻撃されていることに気付かないケースが多いと考えられている。）と同時に，無駄に多くばら撒かないのでスパム対策技術による監視の目から逃れることができる。

レピュテーション・システムとは，（リアルタイムで）送信者の評価を行うシステムで，評価値を出すなどの方法がとられる。これを行うと既知のスパムはもちろん，未知のスパムやウィルスの送信者を防御する事が可能であり，フィッシング対策としても有効である。

無料 Web メール・ホスティング・サービスを使って少数の特定ユーザーあてにメールを送り，スピア攻撃を仕掛ける詐欺が最近急増している。無料 Web メール・サービスの使用によって，防御側が設けているレピュテーション・システムの効果が薄れてしまう。

（5）サーバー攻撃の分業化

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流行っている。

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よう拡張・開発して攻撃に使う。

（6）サーバー攻撃の闇市場

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（Zhuge-Holz-Song-Guo-Han-Zou（2008）などを参照）。

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，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。

（7）益々ソフト技術化

今後は，サイバー攻撃はハード技術ではなく，あるいはハード技術の構成，ソーシャル・エンジニアリングなどでもなく，アプローチなどのソフト技術化の方向への進歩が益々進むだろう。

3　統合管理の必要性

3－1　統合管理が必要なわけ

まず統合管理が必要な卑近な例をあげてみよう。PC などの立ち上げや会員サイトへのログ

インに際して，例えば，パスワードを用途毎に変えるとか，長い文字数あるいはアルファベットが複雑に入ったものにするなど，予想できない難しいものにすればよいとの考えで，このような対策をとってしまう。しかしながら，これが覚えきれなくて，往々にしてメモ紙やポストイットに書いたり，携帯電話に記録しておいたりして，かえって無防備になる。結局，セキュリティは弱体化してしまう。

「セキュリティ対策は強くすればする程よいと考えてしまうのが間違い」なのではなく，無駄に強くしていることが間違いなのである。より重要なのは，メモ紙やモバイルなど関連するツール・機器などとの管理と統合したセキュリティ対策が必要であるということである。

統合管理が必要になる原因・理由は数多くあげられる。そもそも，「人を見分けることは限りある身の人間に与えられた力ではない（ドラッカー（1991））」から，人間以外の力を借りなければならないのである。また，得てして場当たり的になる対策は有効でない。戦略的な視点を持たなければならない。個別戦略はサイロ型と呼ばれる。統合戦略は，まず全体を見て部分に掘り下げることができる戦略である。監視などのセキュリティ対策はサイロ型から統合型へ向かいつつある，といえる。

考えられる固有の要因を列挙すれば次の各小節のようになる。

（1）複合的な攻撃に対応

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[12)]。

例えば，2001年９月に登場したネットワーク・ウイルスであるニムダ（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・ウイルス活動），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った[13)]。

2008年11月頃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・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・

12） 統合管理が必要となる具体的な例として，さらに２つあげておこう。
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，当時，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年から話題となっている IT のテーマであるが，すべての業務がクラウドで行われるわけではない，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。その意味でも，統合管理が必須になる。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。

13） 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，MS Vista には免疫がある。

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**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は進んできたのは事実であるが，それが体系的に進んでこず，ランダムな技術進歩であった[14] ため，順不同で開発出来る所から，開発者が考え付ける所から，いわばランダムに進歩してきた情報セキュリティ技術の導入を，ここで見直し，最適に統合整理するべき時期にきている。

この点については，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。あたかも，個々の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大いに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（と患者あるいは癌を恐れる人は感じる），のと同じである。

（3）対応するべき環境の変化～増改築が繰り返されたシステム

技術進歩面だけではない。対応するべき経済等の制度と環境の変化でも問題が起こっている。情報通信技術の飛躍的な進歩で多くの産業や企業で同様なことは生じているが，銀行へ応用すること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。つまり，程度の差があっても，ほとんどの銀行で増改築が繰り返されたシステムになっている。この点は多くを説明するまでもないであろう。実はこれらのリスクは相互に関連を持っており，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。

14） 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。
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。

（4）機能の高度複雑化

ユーザーが必要としているセキュリティ機能は，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，管理作業も極めて煩雑となる。個人にとって管理はできない状況になってしまう。

また，何らかのセキュリティ侵害が発生した場合にも，統一的な管理でないと，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））。

また，ベンダーの販売する商用ソフトウェアだけでは対策として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）企業の管理問題

メーカーが違うとone stopの運用・トラベルシューティング・修理を行ってもらえない。端末やサービスを跨いだ情報の一元化ができず現状把握と管理が短時間に低コストでできない。また，企業は情報などのセキュリティ機能の統合化によって管理負荷を軽減し，余力を残すことを重視し始めている。

様々な意味での「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，統合管理なのである。

（後半の（Ⅱ）に続く）

参考文献

Computerworld「海外からのWeb攻撃がセキュリティ・パラダイムの変化を促す」『月刊Computerworld』，2009年３月16日。

ドラッカー，P. F.（Drucker, P. F.），現代経営研究会訳『変貌する産業社会』，ダイヤモンド社，1959年。

ドラッカー，P.F.（Drucker, P. F.），上田惇生・田代正美訳『非営利組織の経営』，ダイヤモンド社，1991年７月。

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

ドラッカー，P. F.（Drucker, P. F.），上田 惇生訳『新しい現実』，ダイヤモンド社，2004年１月（旧訳1989年）。

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「「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「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「オンライン・バンキングを狙った次世代型サイバー攻撃」『ITpro』，2009年11月５日。

Messmer, E., and Bort, J.,「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。
相馬基邦「情報を流出させない「出口対策」を重視しよう」『ITpro』，2011年10月４日。
Shwed, G.,（ギル・シュエッド）「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。
山下 眞一郎「防衛産業企業を狙った標的型攻撃が発覚，「多層防御」を考察する」『ITpro』，2011年９月28日。
Zaytsev, V., “W32/Winemmem - Know Your Enemy,” *McAfee Avert Labs Blog*, April 9, 2009.（「「W32/Winemmem」がファイル改ざん検査をすり抜ける仕組み」，2009年５月20日。）
Zhuge, J., Holz, T., Song, C., Guo, J., Han, X., and Zou, W., “Studying Malicious Websites and the Underground Economy on the Chinese Web,” WEIS2008.（Johnson, M. E., Ed., *Managing Information Risk and the Economics of Security*, Springer, December, 2008.）