『学習院大学　経済論集』第49巻　第２号（2012年７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（Ⅱ）

辰巳　憲一*

本稿は表題に関連する事柄の経済的背景や基本の概念，そして問題意識を展開した辰巳（2012）の後編であり，関連する理論や戦略を易しく詳しく，図表などを用いて，経済学的に展開する。節番号や脚注番号は，それに続くものである。本稿では，もっぱら，定量的ではなく，定性的な枠組みの解説に集中する。

４　統合管理の手順の素描と基本原理

管理というものは，大規模化すれば，生産効率などとは違って，管理コストは加速度的に増える。大規模化だけでなく，小規模でもむやみに複雑化すれば，逆に管理コストは増えることがある。複雑な構成のためにセキュリティを保証できなくなる，こともある。それゆえ，統合管理の仕組みは十分考察されなければならない，のである。

企業の情報セキュリティ責任者（ＣＩＳＯ）は，「企業内情報の漏洩」から「外部からのサイバー攻撃によるシステムの停止」まで，情報セキュリティにかかわる事業リスクを評価し，リスクをどこまで許容し，どのリスクへの対策に重点的に投資するか，企業のトップに判断材料を提供する役割を担う。彼／彼女が，統合管理する重要性を十分に認識しても，それだけでは不十分である。統合管理には逐次管理していく方式と一括導入管理する方式の２つが考えられ，どちらにするか決定しなければならない。以下では，それぞれの原理を考察してみよう。

４－１　タクティックス

まず簡単な軍事戦略を例に基本原理を考えてみよう。防御線上の異なる場所で同時に２つの大規模なトラブルが勃発した場合に，対応するタクティックス（tactics）は二正面戦略と二段階対応戦略の２つがある。

---

*）　学習院大学経済学部教授。Integrated Stratified Strategy of Information Security: An Economics Approach（Ⅱ）.
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。）
本稿は辰巳（2012）の後編であり，節番号や脚注番号は，それに続くものである。

（1）二正面戦略

これら２つのトラブルに対して同時に対処し，沈静化を図るという戦略が前者である。もし資源が限られていれば，資源をそれらの規模（跳びぬけた攻撃技術である場合，質を規模に変換する必要がある）に応じて割り振ることになる。それぞれに対して必要最小限の資源量を投入できない，という問題も起こりえる。

（2）二段階対応戦略

主力は１ヵ所のトラブルに対応しつつ，２ヵ所目の戦線にはトラブルの拡大（あるいは侵入を意図している者の侵攻）を阻止するだけの戦力を投入し，かつ１ヵ所目での勝利の後に主力を２ヵ所目に振り向けるという戦略が後者である。二段階対応戦略の遂行には，二正面戦略より，一般に，少ない資源，小額の資金で済む。

４－２　逐次管理の原理

さて，二正面戦略は一括導入管理法と解釈でき，時間差で行動する二段階対応戦略は逐次管理法であると解釈できる。以下では，順番として後者から，考えていくことにしよう。上の４－１は，同時に二方面でトラブルが発生したが，トラブルの緊急度は同じであるが規模だけが異なることを前提にした議論である。現実的にするには，これらの前提を外した考察を行う必要がある。

逐次管理の原理とは，最終的に完全システムにするが，限られた資金のなかで，さしあたり導入の優先順位をどう考えていくか，という問題への１つの解決法である。

（1）脆弱性基準

脆弱性の高いところから防御を始める方式がまず考えられる。どのITサブシステムにも同じレベルでセキュリティ・リソースやコストを投じるのではなく，セキュリティ上の重要度に応じたレベルでセキュリティ・リソースやコストを投じる方式である。有効に実行するためには脆弱性を知る必要がある。脆弱性を知るために情報セキュリティ格付けを利用するのも１つの方法である。

（2）コスト基準

セキュリティ・コストの低いところから，あるいは（同じ意味であるが）企業価値を高める箇所から，管理を始める方式が次に考えられる。

地域銀行のシステム共同化の動きがシステム業界では長らく注目されているが，それを事例として解説してみよう。地方銀行システム共同化の動きのなかでこのコスト方式をとるのは，当初，千葉銀行（千葉県千葉市），第四銀行（新潟県新潟市），北國銀行（石川県金沢市），中国銀行（岡山県岡山市），伊予銀行（愛媛県松山市）の５行から成ったTSUBASAプロジェクトのサブシステム先行方式である。ちなみに北國銀行の新システム開発のベンダーが2011年秋にTSUBASAプロジェクトからの脱会を発表したため現在の参加は４行である。

このサブシステム先行方式とは，銀行基幹系システムに先行して，共同化可能なサブシステムについて，合意できた銀行間から共同化を進める形態を指す。費用がかさむ勘定系システムを後回しにして，小さな投資で大きな効果が得られる周辺システムの共同化を先行させる，ことがなされた。

サブシステムの更改時期が同時に到来する銀行同士から共同化できるメリットもある。さらに，ハードウェアの更新とアプリケーションの寿命は一般に同期しないケースが多い。このよ

うな場合コスト基準はメリットのある共同化方式になるかもしれない。

この方式をセキュリティ管理に応用する場合，メリットもあるが，いくつか問題を生じさせる。例えば，共通の攻撃に対しては効率的に対応できるが，グループ内の他メンバーの脆弱性から悪い影響を受ける。

企業や銀行の内部でも同様な問題が生じる。ユーザーは，セキュリティ・ベンダーが販売しているセキュリティ製品を，当然必要に応じて，無秩序に導入してしまっているのが実情である。結果としてネットワーク全体でセキュリティの一貫性を保つことができず，管理不能の状態に陥ってしまっている場合もある（シュエッド（2008））。それゆえ，セキュリティ・コストの低いサブシステムから管理を始めれば，この状態を改善できなくなってしまう。脆弱性の高いサブシステムから情報セキュリティ投資を始める必要がある，のである。セキュリティのためには，脆弱性基準を必須な条件として採用しなければならない，ということである。

（3）攻撃側の事情を考慮したまとめ

攻撃側の技術進歩がランダムで，しかも攻撃側の相手先選びと攻撃の頻度がランダムであるとすると，コスト基準での導入でもほぼ安全である。

しかしながら，攻撃者たちは2008年，膨大な数のWebサイトから脆弱性のあるものを自動的に検出し，侵入できるワームのコードを開発することに成功した，と言われる（Source Boston Security Showcaseコンファレンス（Computerworld（2009）参照）でのバーネット（Ryan Barnett）の報告，など等を参照）。それゆえ，セキュリティのためには，脆弱性基準を採用する必要がある。

緊急医療などの分野では，トリアージュ[15]などの優先順位が付けられ治療されることが知られている。脆弱性基準は一見概念的にトリアージュに近い。しかしながら，この緊急医療分野では医療組織全体が破壊される攻撃はない（現実に該当するのは，医療スタッフ全員が掛かり切りになってしまう超重症患者の到着である）のが前提であり，致命的なサイバー攻撃が日常的にある情報セキュリティ分野ではそれに対処することを断念してしまっているので，トリアージュは情報セキュリティ分野には直接適用できない。

また，影響度などを無視した，やってきた順に対応するという単純な管理方法もあるが，多数のサイバー攻撃があれば処理が追いつかなく，未処理案件が蓄積していくので，適切な管理方法ではない。

４－３　一括導入管理の環境と原理

次に統合管理を考えてみよう。

４－３－１　一括導入管理の環境

いくつかの観点から，統合管理しやすい技術的なエンジニアリングの環境は整いつつある。

15）緊急医療の現場で，処理能力をはるかに超える傷病者が到着することがあるので，傷病者の優先順位をつけて，救える命を最大限にするための治療を行うことを，フランス語で「選り分ける」という意味の，トリアージュ（triage）という。この優先順位付けは，「治療すれば助かる可能性の大きい」傷病者の治療を優先する。しかしながら，失礼な言い方であるが，「どうせ死んでしまう」傷病者に貴重な医療資源を使わない方針である。ネットワーク内企業や企業内サブシステムの場合には，そのうち，激しいサイバー攻撃を受けたところは切り捨てるということである。それゆえ，厳密にはこのトリアージュという方針と言葉を情報セキュリティ分野に適用するには問題がある。

エンジニアリングの用語を使って要約すると次の２小節のようになる。

（１）統合管理ツール～エンジニアリング・アプローチ

Messmer − Bort（2009）が指摘するように，セキュリティ機能を１つ１つ導入するのは面倒であり，設計も複雑になりやすい。また，個々のセキュリティ機能が別々のベンダーの製品から構成されていると，その管理には大きな手間がかかる。さらには，個々の製品の保守費用をベンダーや SIer（エスアイヤー。システムインテグレータのこと）に支払う必要もある。セキュリティ対策が複雑かつ高コストなのは，こうした手間と管理による。そこで，複数のセキュリティ機能を１つの機器にまとめることで管理性の向上を図れる。

既述のように，セキュリティ管理において必要となるすべてのコンポーネントを１つの統合コンソールで管理することが技術的に可能となっている。ポリシー定義やログ管理，ユーザー管理，トラフィック・モニタリング，ソフトウェアの自動アップデートをはじめとした各種セキュリティ機能やルール定義が完全にモジュール化されているのである（シュエッド（2008）などを参照）。

ちなみに，エンドポイント・セキュリティ（Endpoint Security）は，極秘の内部情報を持っている組織が内部情報を一切外部に漏らしたくない場合にセキュリティをアウトソーシングするには確かに適したセキュリティ管理方法である。しかしながら，内外のセキュリティ管理をどう統合するかが，残された大きな課題になり，完全な統合管理ではないのである。

（２）仮想化とクラウド・コンピューティング～エンジニアリング・アプローチ

仮想化とクラウド・コンピューティングによって容易く統合化できる環境は整ったといえるのではないかと思う。仮想化によって，単一サーバーで複数の OS を稼働でき，仕事（ワークロード）の要求が移り変わるにつれて物理的な１台のマシンから別のマシンにソフトウェア群を柔軟に移動できる。それゆえ，仮想化は，ハードウェアとソフトウェアの結び付きを断ち切り，サーバーとより高度なソフトウェアの間に，サードパーティーのテクノロジーが入り込めることになる。更に，アプリケーションをインターネット上の中央サーバーで稼働するクラウド・コンピューティングでは，各拠点間の統合化はしやすいのである。

４－３－２　様々な統合管理の方式

（１）システム統合の方式

統合管理の方式を考察するために，一般のシステム統合の方式をまずみておこう。システム統合には，飯島（2008）などによると，次のようにいくつかの方式がある。

システム統合の典型的な型の一つは，「片寄せ型」あるいは「巻き取り型」と呼ばれる，一つのシステムに合わせて統合する方式である。そのシステムにその他すべてを吸収する「吸収型」と呼ばれる方式もこの分類に含めて考えることもできる場合がある。

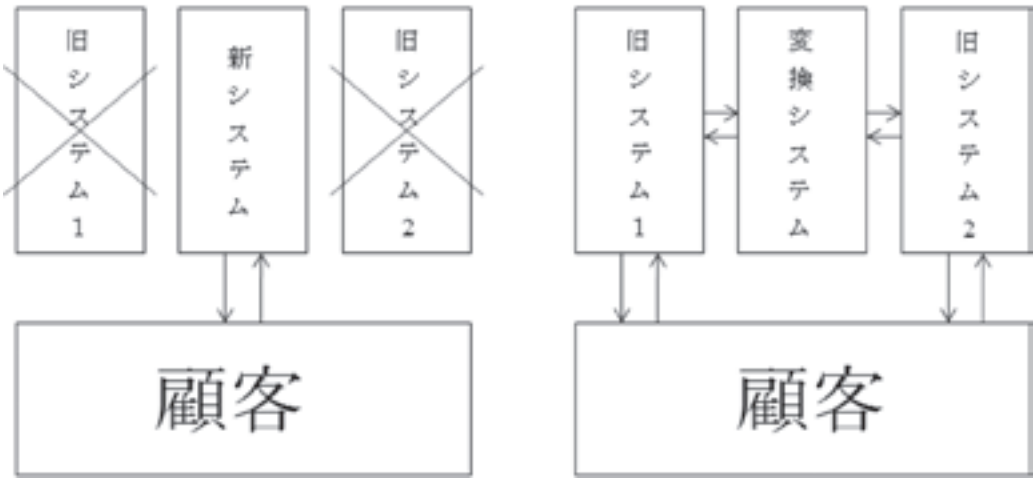
他方で，もう一つの極端では，まったくの「新規開発型」と呼ばれる方式が採用されるケースがある。

それらの間に，中間型の折衷案がいくつかある。コンポーメント（部品）ごとにすべてのシステムから“いいとこどり”をする「組み合わせ統合型」と呼ばれるアプローチがある。あるいは，「併存型」と呼ばれる，統合を行わずにおのおののシステムを別個に走らせ，必要なものだけを外付けの形で新たに付加するというアプローチもある。

東京三菱銀行（現三菱東京 UFJ 銀行），三井住友銀行，みずほ銀行のメガ銀３行が誕生した時には，合併が優先された結果，システム統合が間に合わず，旧来のシステムを平行稼働させ

て，単一のシステムのように見せかける「リレー統合」がなされた。「リレー統合」とは，システムを一本化することなく各行のシステムを新たに設置したメインコンピューターに接続して運用する形態である（図表１参照）。

図表１．新規開発システムとリレー統合



図表１中右の，変換システムとは，コーディングされた情報を相互に変換するシステムであり，前述の各行のシステム間に新たに設置したメインコンピューター・システムである。図表１中の矢印の数からわかるように変換システムがある場合には，通信回数は新システムを構築する場合の数倍になる。

リレー統合を，片寄せするまでの，繋ぎとするケースもある。2009年10月泉州銀行が池田銀行に吸収合併され，合併後の池田泉州銀行ではリレー接続による並行稼働を経て池田銀行のシステムである NTT データ地銀共同センターへ片寄せされた（移行時期は2012年１月であるが，両行のシステム統合が完了したとしてプレスリリースされた）。

いずれにしても，リレー統合は新規開発あるいは片寄せまでの暫定的な繋ぎの方式である，と解釈されるのが普通になっている。

（２）ポートフォリオ理論的からみたアプローチ

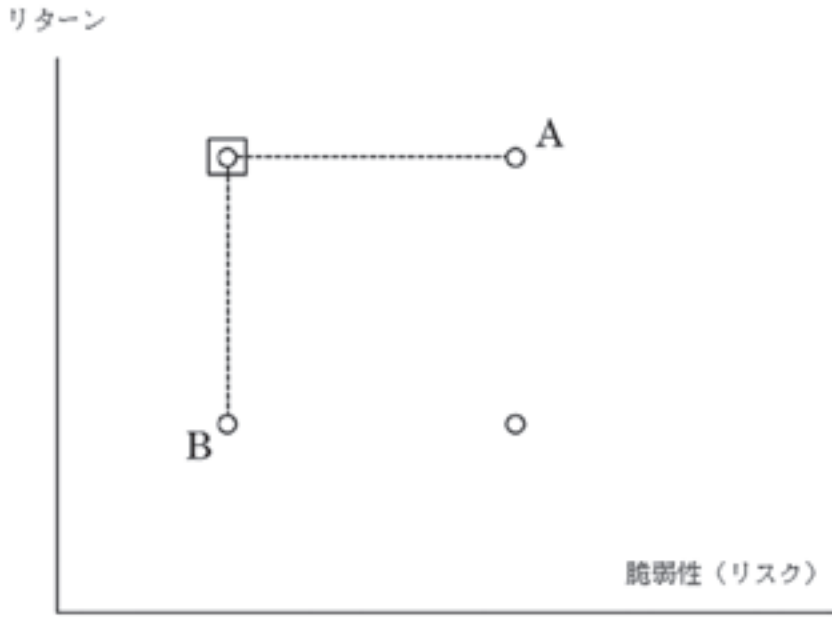
ポートフォリオ理論は，リスク（本稿では，脆弱性が該当することになる）というマイナス要素とリターン（本稿では，システムのパフォーマンスが該当することになる）というプラス要素から成る２次元の特性を持つ複数の銘柄（本稿では，システムとなる）を最適に組み合わせる最適化の理論である。ポートフォリオ理論は応用範囲の広い一般的な最適化理論である。一般にシステムは，多次元多機能なコンポーネントから成るので，２次元のポートフォリオ理論より複雑で，ある。それゆえ，ポートフォリオ理論は簡単であるが，サブシステム（銘柄）間のパフォーマンス（リターン）の相関関係を考慮できる点が１つの利点になる。

先のシステム統合方式をポートフォリオ理論に応用してみると，図表２のようになる。脆弱性（リスク）とリターンの２次元で示される２つのサブシステムＡとＢを統合する場合，いい

とこどり解は左上の四角でマルを囲ったコーナーになる。ポートフォリオ理論は理論上モーメントの数を３次あるいは４次まで増やせ，しかもソフトが完備している実務的なポートフォリオ戦略モデルは銘柄（サブシステム）の数は数万までになっても取り扱えるので，いくつかの統合管理問題を解決できそうである。

ポートフォリオ理論では，銘柄の最適保有比率をきめる。これは，各サブシステムの構成比率が該当する。サブシステムが分割可能な最少単位にあるとすると，ひいては，それが，いいとこどりを示していることになる。サブシステムが分割不可能であるとすると，変数が整数であることを条件にした２次最適化法を適用できる。

図表２．いいとこどり解



（３）管理コストとサブシステム間接続コストの観点とセキュリティの観点

１つの組織内に２つの基幹サブシステムを置くケース（図表３の右）と２つの基幹サブシステムを２つの組織に分けて設置するケース（図表３の左）では，管理コストに差が出てくる。後者の分散設置の方が，２つの組織に跨る分だけ管理コストは高くなる。ちなみに，２つのケースにおいて，他組織内のサブシステムから基幹サブシステムに繋ぐコストは共通である。図表３中の点線でそれを示しており，この場合各２回線ある。

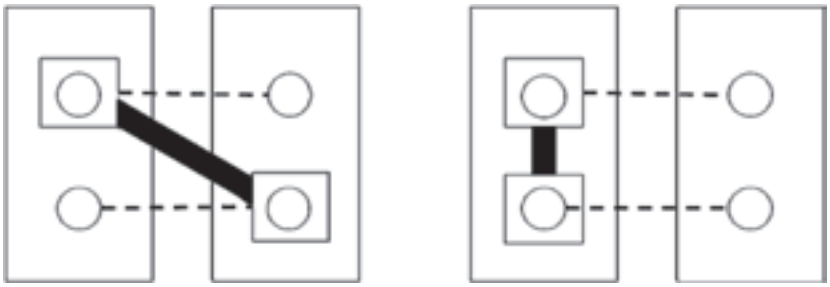
一般に，サブシステム間を接続するコストは，違った組織にあるサブシステムを結ぶ方が，同じ組織内にある２つのサブシステムを結ぶ場合より，高くなる。２つの基幹サブシステムを結ぶ接続はいわば動脈である。基幹サブシステムから端末を結ぶ接続はいわば静脈である。この喩えは科学的には必ずしも適切ではないが，重要さをあきらかにしている。あるいは，違った組織にあるサブシステムを結ぶ前者は外線，同じ組織内にある２つのサブシステムを結ぶ後

者は内線，による接続であり，前者の外線の方が接続コストは高くなる。

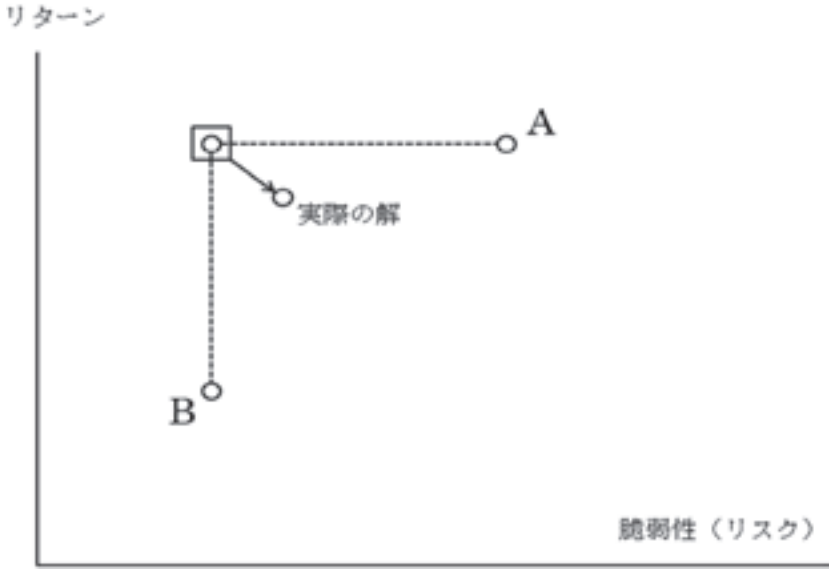
複雑な統合化はセキュリティ問題を引き起こす。直前の図表３からわかるように，外線と内線では，セキュリティの程度が違う。外線は，内線と比較すれば，サイバー攻撃に対してより脆弱になる可能性がある。

以上の理由から，「いいとこどり」解は，実際上，これらのコストを考慮し斟酌した点まで，パフォーマンスが退化する可能性が高い，ことが予想される（図表４を参照）。

図表３．基幹サブシステムの分散配置と集中配置



図表４．ポートフォリオ理論から見たいいとこどり解



（４）統合方式の選択

企業がＭ＆Ａを実施した際に，問題となるのは情報システムの統合である，と考えられている。それは，企業が提供する財・サービスが複雑になってきているので，一つひとつの案件やシステムはそれぞれ特性が違う，からである。それを新しい情報システムで統合しようとすると，かなり大変になる。システム統合は，同じ組織内にすべてのサブシステムを収める片寄

せでなければコストは非常に高くなると思われる。サービスや業務プロセスを，今動いているシステムに合わせる形で標準化して，その後にパフォーマンスを追求するというやり方にするしかない。

既述のように，それぞれ独自の情報システムを持つ複数の企業・組織が統合する場合の，現実的な情報システムの統合方式は「片寄せ型」，「新規開発型」，「いいとこどり」をする組み合わせ統合型，の３つが考えられるのである。しかしながら，現実には，多くの場合「片寄せ型」が採用されてきた。

「片寄せ型」の場合，図表２のＡあるいはＢのうち，どれを選ぶかは，ポートフォリオ理論によると，右下方向に向かって凸の無差別曲線を用いるべきである，ということになる。リスク回避型の企業はＢ点を選ぶかもしれない。つまり脆弱性のもっとも無いシステムＢに片寄せする，ようになるだろう。

形式的な無差別曲線を用いなくとも，選択肢の数は限られているので，社内で十分検討すれば，同様な結論に到達できるものと思われる。

（５）拡張の可能性

ポートフォリオ理論においては，運用対象資産の価格や価値の変化率がリターンであり，その標準偏差がリスクであると解釈される。

ポートフォリオ理論がセキュリティ問題に適用される際には，それゆえ，まず守られている物やサービスの，貨幣額で測られる，価値が明らかにされる必要がある。情報であれば，情報の経済的価値である。次に，特定のセキュリティ機器・ソフトが守っている比率を推計しなくてはならない。これらの作業自体大きな研究テーマであるので，ここでは指摘するだけで，立ち入らない。

これが，ポートフォリオ理論をオーソドックスに適用する際の手順である。この場合，脆弱性は，物やサービスの価値の変動性を測っていることになる。それゆえ，価値の変動性を低減する，つまり価値の安定性を増大するセキュリティ機器・ソフトが存在し，そしてそれが当該資産やサービスの脆弱性を意味するとすれば，ポートフォリオ理論をそのまま適用できることになる。

しかしながら，資産やサービスの価値の増大ではなく，もっぱらその低下が，当該資産・サービスにとっての脆弱性である場合もあろう。セキュリティ機器・ソフトの機能がその価値の低下を防ぐことになる。資産やサービスの脆弱性がその価値の低下を意味し，価値低下を止めるセキュリティ機器・ソフトへの最適投資理論が必要であるとすれば，適用するべきはポートフォリオ理論ではなく，ポートフォリオ理論形成の過程で提起された，バリュー・アット・リスク（VaR，Value at Risk）の理論であろう。この理論は，ファイナンス分野では，広く知られ，実際にも使われている。Hull and White（1998），Jorion（2000）や Choudhry and Tanna（2006）以外にも，新しい研究が多数ある。

VaR は，統計学的手法を使って算出された，市場リスクがもたらす予想最大損失額をいう。株価・金利・為替などが予想と反する動きをした場合に，現在保有している資産に金額としてどれ位の損失が出るかを，一定の期間と信頼区間のもとで，統計学的に算出している[16]ので，

16） 現在保有している資産（あるいはポートフォリオ）を，将来のある一定期間保有すると仮定した場合に，ある一定の確率の範囲内（つまり信頼区間）で，マーケットの変動によって，どの程度の損失を被る可能

市場リスクの管理手法の一つとしてよく使われるようになっている。

例えば，ある資産・ポートフォリオについて，その保有期間を１日，信頼区間を99％としてVaRが計算されると，その保有期間中に，このポートフォリオの損失がVaRの金額を越える確率は１％となる。100日の内99日は日次損失がVaRの範囲内であるが，100日の内１日はVaRを超える可能性があることを意味する。

VaRは，被害･損害や損失の予想額が計算できるだけでなく，補償額算定にも係わる。また，VaRは，予想損失額などの計測に限られるわけではなく，最適化問題の目的関数として捉え，最小化問題にすることが不可能ではないので，応用範囲は広い。資産やそのポートフォリオのリターン分布のパラメターなどを変えることによって，VaRの確率分布が得られ，様々に活用できる。

しかしながら，いくつか欠点がある。VaRは過去のデータから求めた資産価値の予想変動率（ボラティリティ）を用いるため，継続的にデータを取得できないような資産には適用できない。

また，1987年のブラックマンデーや2008年のリーマンショックのような異常時には一般に適用できない。ストレス・テストを定期的に施して異常時でもどこまで使えるか，を知っておく必要がある。

５　情報セキュリティの階層型統合管理

５－１　多層多面の管理

日本の大手通信２社のトップが2011年５月31日世界ICTサミット2011で次のように述べている。ＫＤＤＩは，仙台までの海底ケーブルに加え，東北自動車道沿いと送電用の鉄塔上に回線を設け，三重化していたが，東日本大震災ではそのうち２つが使えなくなった。それで日本海側にも回線を新設し，四重化を進めた。ＮＴＴグループでは，米国とつなぐ５本の海底ケーブルのうち，４本が切れた。残ったのは伊勢志摩から出ている回線だけだった。国内でも仙台への中継ケーブルが切れたが，途中に原発事故の立ち入り禁止地区があり，修復が困難になった。日本海側の中継網を太くするなど迂回ルートの確保を急いだ。

これらの発想は，同じ場所あるいは近辺に二重三重の回線を設けるのではなく，位置・場所を大きく変えて通信回線を設置するので，多層防御（Defense In Depth）に通じる方法である。防御は，多層多面でなされなければならない，のである。

残念ながら，防御だけでなく，攻撃も多層多面でなされる。このような環境の下でその管理はどのような統合管理であるべきであろうか。いくつか考察するべき要因を，まず，あげてみよう。

情報セキュリティの個々の機能を幾つかの層に分けること（これは本稿の前編（I）で既に行なった），守るべき企業内部情報をその重要度で分類することが，まず必要であろう。それだけでなく，それらを取り扱う人間を内外，職階，などいくつかの局面で分けることも重要で

性があるかを計測したものである。保有期間には１日をとって測定し，それを月単位で合計し，平均値を算出する，などの操作を行う。

VaRは，1990年代から欧米の金融機関で利用され始め，1993年に発表された第２次BIS規制において金融機関の市場リスク管理手法として採用が推奨され，日本でも急速に普及した。

ある[17]。同じように，攻撃や情報漏洩を幾つかのタイプに分けることができる。攻撃アクセス数の多小，攻撃頻度（時間当たりの攻撃アクセス数），当該セキュリティ・イベントの現状回復スピードの速さ遅さ，緊急度，などで分けれる[18]。

５－２　多層多面で防御する戦略の基盤

最近，情報セキュリティ・ベンダーの新商品は統合管理の視点がとられている。しかしながら，限られたリソースで情報セキュリティ投資する企業などにとって，多額にのぼる情報セキュリティ統合管理ツールの導入は一朝一夕には決断できるものではない。考察するべき事柄は多い。情報セキュリティ機能の統合管理について考慮するべき経済学的要素としては，概略次のように考えられる。

５－２－１　代替性と補完性

情報セキュリティのソフト・機器，防御者の企業が保有する複数の資本設備やソフト，攻撃者行動の３局面のいずれにも，代替性と補完性がみられる。

（１）セキュリティのソフト・機器～機能分析の必要性

様々な情報セキュリティの機器や商品がセキュリティ・ベンダーから提供されるようになっている。いくらでも無限にある機器や商品を全て採用するわけには行かない。しかも，それら情報セキュリティの機能は，技術的に，さらには経済効果からみて，複数のグループに分けられるが，ほとんどの情報セキュリティのソフト・機器は相互に補完しあうだけでなく代替している。

もう少し正確に述べれば，情報セキュリティ機能を複数のグループに分けた場合，セキュリティ・レベルは相互に異なるが，それらソフト・機器はグループの中で機能は代替的である，ということである。代替的な情報セキュリティのソフト・機器は，結局どれか１つを採用することになっても，それらを目的に応じて順序付けすることが必要になる。この順序付けのプロ

17）人的構成をどうするべきかについては，いくつかの参考になる事例がある。例えば，店舗において深夜に従業員が一人体制で就業するのが恒常化すれば，それが知られてしまうことが要因となり，強盗事件が高頻度で発生する。それを避けるためには，他の防犯策もあるが，深夜の複数従業員制を採用するのが１つの対策である。強盗事件にお客様が巻き込まれる可能性が低くなる。
セキュリティ部門の要員数が少なければ，この事例と同様に，サイバー攻撃に晒される危険が増えるだろう。

18）RSA Conference Japan 2010（2010年９月９日）の基調講演で，米 EMC のセキュリティ部門である RSA のプレジデントのコビエロ（Coviello）氏は，「その多くが連携せずに個別に動作しているのが現状」と次のように指摘した。
IT インフラにはマルウェア対策やファイア・ウォール，認証，暗号化といった製品が多数導入されているが，それらがカバーするのはそれぞれ単一の側面のみ。しかも，複数のベンダーにまたがって管理を行う必要があり，ログやレポートも個別に吐き出されてくるという混乱した状況だ。
コビエロ氏は，３つのレイヤからなるセキュリティ・アーキテクチャを提唱した。まず一番下には，ポリシーを実行に移す「コントロール」層がある。そして次に，それらを監視し，ログの収集やプロビジョニングを実施する「コントロールの管理」層がくる。そのさらに上に，ガバナンスやコンプライアンス，リスク管理といった観点からポリシーを定める「ガバナンスとモニタリング」層が位置するという構図だ。そして，包括的な管理を実現するには，「ボトムアップではなく，まず高いレイヤから取り組むべき」（コビエロ氏）。
山下（2011）なども多層防御を考察している。

セスは，それゆえ，情報セキュリティ機能を多層で統合管理することに繋がるのである。

（2）企業のシステム・資本設備～カスタマイズされた情報セキュリティ

攻撃者の侵入に備えて対策しておくには，まず，情報セキュリティ機能の逐次導入と一括導入のメリットとデメリットを考える投資理論が必要であると考えられる。

例えば，ある業種に属するある企業が保有する複数の資本設備間で，生産における補完性が高いとしよう。補完性が高ければ，たった一つの設備が攻撃され被害にあっただけで，他のすべての資本設備は動かなくなる。このような場合，情報セキュリティ機器を一括導入するしかない。他方，すべてのシステム・設備が代替的であれば，情報セキュリティ機器導入は一部で済ませることができる。４つの代替的なサブシステムには，そのうち，例えば２つだけに情報セキュリティ機器を導入する，という方法も非現実ではない。

この例でわかることは，個々の企業にとって，所属する業種，構成されている企業組織の形態などに応じた独自の個別情報セキュリティ対策が存在するということである。技術やノウハウあるいは組織の構造などの企業・組織のソフトな面についても，同様である。

（3）攻撃者の攻撃～相関分析

ある単一の情報セキュリティ機能を実現するためには，度々既述のように，複数の類似の機器・手法・システムが存在する。このような情報セキュリティ機能は複数存在する。複数ある情報セキュリティ機能を有効に活用するには，相関分析という方法がある。

攻撃者は，都度ドメインを変えるなどして，自身が特定化されないようにしている。あるいは複数の攻撃方法をとったり，複数の攻撃先を狙ったり，して攻撃を確実なものにしている。いわゆる複合化戦略を採っている。防御者はそれに対して，攻撃者の身元（ウィルスや迷惑メールの送信元）情報や攻撃内容（ウィルスや迷惑メールの送信内容）情報などの手に入れることができる情報から，可能な限り多面的に対応する必要があるわけである。

相関分析の１つには，複数のセキュリティ機器が蓄積するログデータを相関的に分析する手法がある。例えば，日々高度化する不正アクセスの手法の中には，時には各種セキュリティ機器が検出できない（あるいは攻撃者が攻撃に利用するのを辞めた）ようなものも存在するが，この事実を確認し，正確な判断を下すには，複数のセキュリティ機器のログデータから分析を行う必要があることもある。また，コンプライアンスを強めることが要求され，それを受けてセキュリティ対策が求められるようになった，ことなどがこのような技法が注目されるようになった理由でもある。

相関分析によって検出したセキュリティ・インシデント情報とその他のアナログ監視情報を結びつけることによって，例えばサーバーダウンの原因が，ハードウェア障害なのか，あるいはワーム感染等のセキュリティに起因した現象なのかを区別できる，切り分けから原因調査まで可能となる。さらには，攻撃パターンの認識までできるようになる。セキュリティ・イベント相関分析（SEC, Security Event Correlation）は企業ネットワークなどのセキュリティを保護する防御的かつ包括的な手法になるのである。

不正請求・不正利用などの発見では，繰り返し起こるユーザーの利使用パターンを見いだすことで，このパターンから外れた利使用を不正請求・不正利用として突き止め追究する[19)]。こ

19） パターン認識による方法の例はいくつもある。クレジットカードの不正利用発見では，繰り返し起こるユーザーの利用パターンを学習することで，そこから外れた利用を追究できる。保険金の請求などにおい

れも相関分析の一部であり，クレジットカード，保険などの不正請求摘発に適用される。

ある特定のセキュリティ・イベントが，どのセキュリティ機能を突く攻撃であるか，およそ推定できるケースが多いであろう。それを確率的に捉えることができれば，さらに，数量的な分析に役立てることができる。防衛する企業が自社にはどのような攻撃が多いかを把握しておれば，どのセキュリティ機能をどれだけ重視するべきか，が確率的にわかるようになる。

５－２－２　いくつかの課題

（１）相関分析の課題～計測上の問題と共同戦線

相関分析には，いくつか欠点がある。ウィルスには，そのプログラムの一部を変えるだけで無数の亜流ウィルスが作られる。それゆえ，パターン分析を基本とする相関分析では十分に対応できない，と考える専門家が多い。亜流ウィルス同士は別のウィルスにカウントされてしまう危険性があるからである。

また相関分析には，攻撃側の攻撃先（攻撃者がある攻撃先を打ち破れない時他のどのような攻撃先を攻撃するか。）や攻撃機能の相関性（攻撃者がある機能を打ち破れない時他のどのような機能を攻撃するか。攻撃手法を次々と変えて複数個所を攻撃するのか。）という面と防御側の技術としての情報セキュリティ機能の相関性（上で既述）という面の２つがある。これが示唆するのは，相関をどのように測るべきか，の計測上の問題が存在することである。

攻撃被害は，攻撃側と防御側の両者が攻防した結果であり，両者の要因が複雑に絡み合い，単純な比較では意味がない。計量経済学ではこの現象を早くから気付いており，価格と取引数量のデータ系列だけから需給の両曲線を計測できないというような識別性を問題にしている。

公表された攻撃データから相関分析する場合さらに別の問題がある。被害は，ほんの一部しか報告されない。ほとんどは被害事態が極秘にされる。それゆえ，サンプルセレクション・バイアスがある。専門の業者が相関分析する場合においても，攻撃は自動的に報告され詳細が明らかになる（当然外部には非公開）が，業者がカバーするのはすべてのサンプルではないので，やはりサンプルセレクション・バイアスがある。

そして，相関の高い情報セキュリティ・ツールの間では，投資額をともに増やす（一方を増やした時他方も増やす）必要があるのか，あるいはともに減らすのか。それでは，より相関の低い情報セキュリティ・ツール間ではどういう対応をするべきなのか。このような問題も検討すべきテーマになる。

さらに，攻撃者は攻撃を横断的に行う可能性がある，ということは，複数の防御者同士が共同して防御するのが有効になるということである。この可能性があるという事実を鑑みると，どのような共同戦線を誰（企業）と組めるのか，も重要な検討対象になる。攻撃者が特定の企業や組織の防衛線を打ち破れない時，他の誰（企業）をどのように決めて（特定化して）再攻撃するのか，攻撃手法を次々と変えて複数の個所を攻撃する場合はどうなのか，などを分析することも重要な研究テーマになるだろう。

（２）標的型攻撃と相関分析

標的型攻撃では，数少ない攻撃者が特定のいくつかの攻撃先を度々，目的を達成するまで，攻撃する。攻撃者は，攻撃ごとにカスタマイズ（特定の企業や組織を狙うためだけに作成され

て，請求の内容だけでなく，地理的時間的データなどを組み合わせることで，繰り返し起こるパターンを見いだし，不正請求者を突き止めることができる。

る）したウィルス（悪質なプログラム，マルウェア），それゆえ世界中に１つしか存在しないウィルスを使っている。その結果ウィルスは広範には出回らないため，対策ソフトメーカーがサンプルを入手できず，対応が遅れる。

標的型攻撃では，１つの企業・組織に送信される標的型メールの数はそれほど多くない。怪しまれないようにするためであると理解されている。2011年に起こった世界の防衛産業サイバー攻撃の場合には，潜水艦，誘導弾などの防衛部門，そして原子力プラント関連の開発拠点が攻撃先になったが，多いケースでもおよそ500通の標的型メールが送られたに過ぎない。相関分析にはサンプルサイズが小さすぎる。

標的型攻撃では，攻撃を受けたり，感染する検体・被害者が都度違い，検知された攻撃者名が感染時期やユーザーによって異なる傾向がある。それゆえ，報道されたり警告されている情報だけを参考にして，個々の企業・組織がセキュリティ対策をする，あるいは（報道を信じ切ってしまって攻撃対象業種ではないと勝手に判断してしまって）まったくセキュリティ対策しない，ことが起こる。攻撃データは集中し偏っており，サンプル数が集まっても，有効な相関分析はできない可能性がある。これではセキュリティ対策としては十分でない。

ちなみに，標的型攻撃への対策の一環として，①サーバー，クライアントPCで実行できるアプリケーションを固定化してしまう（ダウンロードを自由にさせない）方法，②ホワイトリスト機能によってアプリケーションを実行できる人間を制御してしまう方法，そして，③誰が，いつ，どのファイルをどのように変更したかの証跡を取得し保存（システム変更改ざん検知・保護）する方法，への関心が高まった。

（３）日本的慣行の弊害

横並びの日本的経済慣行から，ある会社の製品が良いとなれば，他の企業も同じものを導入する傾向が日本にはある。その結果，国内では数の極めて限られたセキュリティ技術が普及（良いものでなければ蔓延という言葉を使う方がよいだろう）するようになる。導入する企業にとっては相互によく知ったセキュリティ・ツールなので便利な場合もあるが，他社製に切り換える誘因も生まれてこない。これを，不正侵入する側から見れば，一国全体が破りやすいシステムになっていく。一つ破れば，すべて破れる，というわけだ。

この現象を相関分析から表現すると，破られる時は皆同時で，導入されたセキュリティ技術の相関度は極めて高いということである[20)]。

（４）防衛の共同戦略

さらに，共同防御が望ましい場合が存在するという議論は，情報セキュリティは公的に行うべきであるという，考え方に導かれる。攻撃経路が多数に及んでいる，あるいは攻撃規模が大きくなると，セキュリティ対策は個人や個々の企業ではできない。

過去においては，多くの国で都を城壁で囲んで防御した，ことが共同防衛戦略の一事例にな

---

20) テーマは遡るが，日本企業に独特な問題をもう１つ，ここであげておこう。日本では，経営トップの正しい認識と企業としての取り組み方針をトップ自ら示す必要がある。上から指示がないかぎり，日本企業には強い現場主義があるので，セキュリティ・イベントが起きたら，まず現場で何とか解決しようとする。そして現場ではどうしようもなくなるまで上には報告しない傾向がある。その結果対応の遅れが生じることになる。
被害が拡大し，情報セキュリティの専門家が駆けつけても手の打ちようがない状態に至る最悪の場合を避けるために，未然に報告マニュアルなど対応策を決めておくべきなのである。

る。城壁のことを羅城，土を固めて作れば築地塀（ついじべい），と呼ばれた。そして羅城に開けた門を羅城門と呼んだ。

どの範囲まで，どの程度まで，情報セキュリティの整備を公的に行うべきだろうか。政府自身が大きな情報セキュリティ・センターを作り，国をあげてサイバー攻撃に対峙することが，まず一方の極として考えられる。他方の極の，政府部門はなにもしない，というケースをおいておくと，中間には，いくつかのケースが存在しうる。政府調達において調達先に一定のセキュリティ要件を義務付ければ情報セキュリティは普及するだけでなく，情報セキュリティを半ば義務化させることになる。少なくとも政府ができる事柄には，政府が攻撃の情報を企業と共有したり早期警戒態勢で企業と連携したりする方法など，が含まれる。

５－３　階層型情報セキュリティ統合戦略

それでは具体的な多層防御（Defense In Depth）を体現した階層型情報セキュリティ統合戦略とは具体的にどのような原理なのだろうか。

侵入口検知，侵入防止から侵入阻止さらに侵入被害防止まで多層に及ぶセキュリティ機能をどう管理すべきだろうか。すべての局面で，各層毎に防御するべきか，あるいはその他の方法をとるべきなのだろうか。既にみたように，同じレベルの情報セキュリティ機能を実現するための機器・手法・システムは複数存在し，しかも，それらの機能は多段階に及ぶ。それゆえ，階層化戦略も必要になる場合がある。経済的な理由で安価な機器を第一層においたというわけではなく，技術的な理由で脆弱な機器をおくしかなかった場合には，それをカバーする機器を第二層におかねばならないだろう。

卑近な例を使って，統合戦略の機能間配分問題の一局面を説明してみよう。東日本大震災の後起きた津波に関して東北地方のある地域では，巨大防波堤があるからと過信して逃げなかった住民がいると報道されている。防波堤と安心な高台に逃げるという対処方法は機能の全く違う津波対策である。もし前者が完全であれば，確かに後者は不用かもしれない。前者が１％でも完全でなければ，全体として完璧を目指して後者を準備しなければならない。効果の点からみれば，前者をほどほどにして，後者を徹底するという方策も，ありえる。ここでいう前者とはセキュリティの第ｉ層が該当すると考えると後者は第（ｉ＋１）層である。

さらにもう一つ論点がある。被災地では大震災直後の早い段階から，今後は高台に移転するべきだという声があがり，実際にも，時間はかかったが，その方向に進んだ。著者は誤解しているのかもしれないが，高台移転はこれだけで津波は今後100％安心ということだろうか。これでは，巨大防波堤がかかえていた問題と同じ轍を踏む恐れがある。サイバー攻撃においては，１つの機能だけに集中して多額のお金をかけて防御していこうという一点集中戦略が該当する。一点集中戦略も１つの解答ではあるが，攻撃者が今後どう変貌するか，不明ななか不確かな戦略であると言わざるをえない，ということになる。

５－３－１　階層型統合戦略の概略

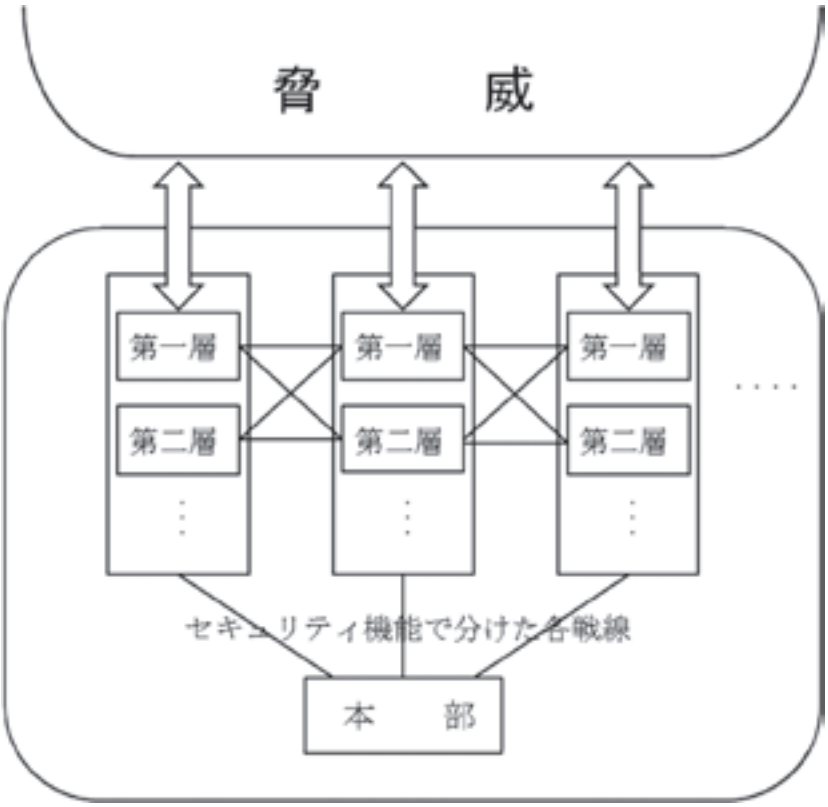
この階層化戦略に関しては，１つのアプローチとして，攻撃アクセス数の多小，攻撃頻度，などに基づいた，次の図表５のような階層化戦略という考え方が取りえる。

ちなみに，いくつか事前に説明しておくべき事柄があるので，まずそれらを述べておこう。先に解説したポートフォリオ理論やVaRは，この枠組みのなかの一部に使える，ことを頭において以下を理解して欲しい。そして，第二に，異なるセキュリティ機能のそれぞれを達成す

る様々な機器を統合しようとする際には，それらの互換性[21] が担保されていることが最小限の条件になる。本小節でもそれが前提になる。

フロントの第一層が破られた時に備えて，第二層のカバーとかバックアップをどのように行うか，さらには第三層についてはどうする（例えば，第三層は対応しない，つまり防備しないなどの決定）か，などが論点である。どの機器・手法・システムを第一層に置くか，そして第二層に向く機器・手法・システムは何か，なども重要な決定事項になる。さらに，これらの検討結果を技術進歩に応じて定期的に見直していくことも必要である。

図表５．階層型統合管理の概念



（1）脆弱性とコストの基準

１つの原理が考えられる。まず，肝要なのは，攻撃アクセス数の多い，攻撃頻度の高いデータ・情報や部門は，侵入防止の早い段階から，高度なセキュリティ機能を持つ機器・ソフトで守る，ことである。そして，攻撃アクセス数の少ない，攻撃頻度の低いデータ・情報や部門に対しては，後段の侵入阻止・侵入被害阻止段階で，低価格な機器・ソフトで守る，という脆弱

21）非互換排除が達成されない場合には，並列的に繋ぐしかない。ある１つのセキュリティ機能を達成するために複数の機器が例えば第一層に設置され，それらが繋がれる，非効率な構成になる。

性とコストによる原理である。

これらを決めることによって，各セキュリティ機能をどれ位のレベルまで達成するかも，結果として，決められることとなる。

情報を取り扱う人間を内外，職階，などいくつかの面で分ける方式については，例えば具体的に，詳細な財務情報を閲覧できる権限を課長以上の経理担当者に持たせる，そのための方式を考える，などである。ちなみに，閲覧者を制限できる暗号方式は既に存在している。

（2）自動化

また，防御の階層化を自動的に実行することも考えられる。攻撃発生量の推移を元に，セキュリティ機能の移動を自動実行する。より多く（少ない）の時間当たり攻撃数になれば，高（低）機能機器・ソフトへ自動的に移動するわけだ。セキュリティ機能をクラウドで利用できれば，つまり機器・ソフトを所有するのではなく，借りることができるならば，防御の階層化を自動的に実行することも可能になる。

５－３－２　階層型統合戦略のその他の論点

現状回復スピードの遅さ，緊急度などの観点から階層化戦略をとることも考えられる。これらの観点も幾つかのレベルに分けられる。場合によって，これらの観点はさらに次元の高い議論を惹起するかもしれない。

多層防御には，これまで述べてきた，いわゆるエンドポイント・セキュリティだけでなく，ネットワーク・セキュリティ，サーバー・セキュリティといった多岐の分野での対策が求められる。このリストにさらに項目を追加すれば，ストレージ・セキュリティ（データ・情報を重要度・利用頻度，機密度に応じてカテゴライズし，それぞれに応じた保護を適用する階層型ストレージが注目される），ソフトウェア・セキュリティ，などがあろう。これらに関しては，それぞれ利用する技術が異なり，エンジニアリングの視点がさらに含まれる。

2011年３月に起こった東日本大震災は，リスク分散を広域的に行うべきことや，バックアップは三重でも足らなかったことに加え，様々な個々人や企業あるいは公的機関が持つ様々なノウハウや情報の共有化が必要なことを浮き彫りした。社会システムとして新しく構築する際に忘れてはならない観点になろう。

最後に根本的な問題として，情報セキュリティが何よりも上位の行動目的になることがあってはならない，という点がある。コスト削減は当然のこととし，組織本来の目的（企業であれば，例えば，利益）と矛盾しない形で，行われなければならないのである。しかし，利益優先で安全無視というわけでもない。

６　まとめ～要約と残された課題

情報セキュリティの統合管理が，どのような階層形態であろうと，導入された暁には，セキュリティ・インシデンスの発見や調査は円滑に進む，可能性は高まる。ネットワーク全体で何が起きているかを監視し，異常な出来事の発見は早くなり，調査も体系的に行える，ようになる。

情報セキュリティ統合管理の原理に基づけば，セキュリティ製品を異なるベンダーから購入するのではなく，包括的なセキュリティ・ソリューションを提供する総合ベンダーから購入したようがよい。総合セキュリティ・ベンダーは広範な製品ラインアップをそろえている上に管

理環境も統合している（シュエッド（2008））ので，セキュリティ管理を簡素化・効率化できる。それゆえ，情報セキュリティのコストの削減ができる。

デバイスの機能や働き方が多様化し，クラウドの普及によって企業の内と外を分ける境界線も曖昧になった。その結果，従来のような防衛線がはっきり存在することを前提にした情報セキュリティ管理は時代遅れになった，と言われる。情報セキュリティの統合管理には新しい課題が突きつけられている。

クラウド，ネットワーク，ストレージや時間軸に関しては，本稿の議論を拡張できる。一つずつ簡単に要約しておこう。セキュリティ機能の一部を，しかもそれだけをクラウド[22]化する（つまり，購入したり構築するのではなく，賃料を払って使用するだけにする）場合も含めた状況で階層型統合戦略を考慮する必要がある。

情報システムの一部である，ネットワークやストーリッジについては触れることができなかったが，これら自体にも階層構造をとりえる。しかも，これらを含めた，階層型統合戦略が考察される必要がある。

さらに，時間軸も階層型統合戦略に取り入れる必要がある。ちなみに，時間の経過ということに関しては，ビルや会社への入出舘に際して，それぞれの時間を記入してもらう（記入する，記録する）方式は，現代のタイムスタンプの仕組みに取り入れられているが，単なる認証（侵入検知，侵入防止）を超えて，不審行動の直後発見や被害箇所の特定・発見，などに役立ち，セキュリティに対して大きなメリットがある。

攻撃者の行動については本稿で体系的に分析していない。攻撃対象については，それが無差別である事例から，標的を定めて攻撃する事例まで，様々である。本稿で展開したように，主流は前者から後者に移りつつある。また，攻撃者は非合理的な誘因で攻撃する場合だけでなく，あるいは経済的な合理性を持ちつつ行動する場合もあるだろう。前者はコストを無視しているが，後者では限られたリソースのなかで合理的に攻撃行動をとっているだろう。このように攻撃者は様々な動機で様々に行動している。現象上は，その結果，複合した様相を示すことになるだろう。非合理的な攻撃行動は，合理的な行動を分析した後でないと，その特徴は明らかにならないだろう。このような分析は，次の機会に譲りたい。

参考文献

Choudhry, M. and Tanna, K., *An introduction to value-at-risk*, John Wiley and Sons, 2006.

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

22） クラウド・セキュリティについて１点だけ述べておきたい。ある特定の攻撃の有る無しが明瞭である，比較的安定的な攻撃サイクルがある場合，あるいは予想不可能な攻撃増加がある場合，クラウド・セキュリティを導入するべき環境であり，奨められる。

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。
Hull, J., and White, A., “Incorporating Volatility Updating into the Historical Simulation Method for Value at Risk,” *Journal of Risk*, １, 1998, pp. ５－19.
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。
Jorion, P., *Value at Risk: The New Benchmark for Managing Financial Risk*, McGraw-Hill, 2000.
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。
辰巳憲一（2012）「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）」『学習院大学経済論集』，2012年４月，pp.３－21。
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.）