JSD の 2004 年 5 月の月例研究会

JSD では、2004 年 5 月の月例研究会として、「SD とセキュリティ（安全）研究 Security and System Dynamics Approach」をテーマに、2004 年 5 月 15 日（土曜日）午後 1 時から 4 時半まで、学習院大学で、IT セキュリティの状況や IT セキュリティに関し、SD を使った研究の紹介を行いました。

1. 5 月の月例研究会の開催主旨

情報社会は進んだ今日、セキュリティ（安全）の確保がかってとは違った様相となっている。セキュリティにはいろんなレベルや分野があり、国家レベルでは、安全保障などが、社会レベルでは防犯社会などが、そして企業レベルや個人レベルでは、個人情報や企業情報の漏洩防止などが問題となっている。SD 学会は、セキュリティの重要性に注目し、学会内にセキュリティ研究分科会を設立している。

SD と軍事に関する研究の一部は、昨年 9 月の例会で少し紹介しているので、今回は、非軍事の分野に関するセキュリティを取り上げ、まず、システムのセキュリティに関する基本的な考え方を紹介し、続いて、SD を使ったセキュリティの研究を紹介する。

2. アジェンダ

13:00-13:10 (1) セキュリティ（安全）の概要（あずさ監査法人、末武）
13:10-14:40 (2) IT におけるセキュリティ（オージス総研、猪上 謙吾様）
・タイトル：「情報セキュリティの最新動向」
・講演者： オージス総研　東日本営業部クロス営業チーム（兼）システム技術部インフラ技術第一チーム、猪上 謙吾様
・講演主旨：相次ぐ個人情報流出事件、相変わらずのウィルス流行など、情報セキュリティに対する世間の関心は高いものの、情報セキュリティに関連する事件、事故が続発し、世間を賑やかせています。法律や情報セキュリティ関連規格の整備はどのように進んでいるのでしょうか？情報セキュリティにどう取り組むべきなのでしょうか？
情報セキュリティの規格類を有効に活用するために気をつけないといけないことは何でしょうか？ツールの選択はどうすればよいのでしょうか？
事故が起こってからあわてないために、情報セキュリティへの取り組み指針を、最新動向を交えてご紹介いたします。
14:50-15:20 (3) SD とセキュリティ研究（あずさ監査法人、末武）
15:20-16:00 (4) 活動報告
－日本衛生学会総会でのミニシンポの活動報告
（大賀英史様＋池田 誠様）
－研究分科会活動報告（松本様）

3.発表内容概要

(1) セキュリティ（安全）の概要

1) SD セキュリティ研究分科会

セキュリティは、国家レベルでは国防や安全保障、企業レベルではビジネス・システムに対する攻撃や情報流出などいろんなレベルで考えることができる。SD 研究との関係では、前者は SD 国際会議などでも軍事研究として成果が発表され、また、ミリタリ・ラウンド・テーブルなど関係者が議論を行うが場が用意されてきた。今回の月例会でも、最初は、この軍事関係を中心としたセキュリティを取り上げることを考えていた。

後者に関しても、近年、注目が高まり、2003 年の国際会議において、セキュリティ研究分科会設立の呼びかけがなされ、IT を含むビジネス・システムを中心としたセキュリティを研究する、セキュリティ研究分科会が設立された。

2) セキュリティ対策の動向

ビジネスに関するセキュリティ対策、特に IT システムが関係するビジネス・システムに対するセキュリティは、かっては、ネットワークを介した外部からの攻撃が問題だったが、近年では、社員や業者などの内部関係者による情報流出や悪意ある妨害、破壊が問題となっている。これらの、システムに対する攻撃や情報漏洩などのセキュリティに脅威を与える要因への対策は、①技術的コントロール、②公式的なコントロール、③非公式的なコントロール に分けられるが、従来は、技術的コントロールと公式的なコントロールが中心の静動的議論で終結し、動的にはあまり取り上げられてこなかった。また、③に関しても、あまり取り上げられてこなかった。例えば、筆者の勤務先であるあずさ監査法人も、情報システムの監査サービスや関連会社を通じての情報セキュリティ確保のためのアドバイザリー・サービスを提供しているが、上記①及び②の内容が中心となっている。そして、アドバイザリーの内容としては、情報セキュリティが確保できるような情報システム・セキュリティ管理技術の確保や、それを運用管理できるような体制、制度の確立や整備を薦め、さらには、その整備レベルを確認し、外部に提示することができるという意味で、BS7799 や JIPDEC の ISMS 適合性評価制度などの情報システム・セキュリティ・マネジメント・システムの認証取得を推薦している。

こういった認証制度で定められた技術的コントロールや制度などによる公式的コントロールはもちろん必要条件ではあるが、しかしながら、この 2 つのコントロールを整備すればセキュリティ対策が完璧になるとは言えない。筆者などがしばしば見聞しているところであるが、情報システム・セキュリティ管理のために、いくら立派な規定や会議体を設置しても、水面下での制度の形骸化が進んでいて、いわゆる目標のなし崩し現象が発生し、隙をついて問題が発生することが多い。①技術的コントロールや②公式的なコントロールだけでなく、こういった③非公式的なコントロールに含まれる問題について、その発生メカニズムや対策の効果を SD の観点から研究し、対策に応用することは極めて有効であると、セキュリティ研究分科会の関係者は考えている。

3) SD でセキュリティを研究する意義

SD では、すでにピーター・センゲを中心とする学習する組織の研究や実践成果を上げることに成功している。セキュリティ関係の問題が発生する前に、顕在化しなかった問題があり、それを見逃したために事故になったという例が多い。そこで、顕在化しなかった事故をきちんと認識し、分析し、対応し、その発生構造を分析し、根本的な対応を取ると共に、事故記録を蓄積し、それを仮想体験学習に活用し、事故体験を常にフレッシュに体験する、さらには、自分達以外の企業や組織が経験した事故に関しても、他山の石として、あたかも自分達の経験と考え、事故から学び続ける学習組織の構築が有効であることが知られている。（学習する組織）

また、最近では、エージェント理論などで、仮想の従業員や IT システムの利用者などを 1 人 1 人の行動として把握し、1,000 人程度の利用者が関係してくるシステムの様相を把握することも可能となっている。こういった、SD での研究成果を活用し、③の非公式的なコントロール、特に人間の心理的な面（メンタル・モデル）も含めてモデル化し、総合的に捉えることで、従来とは違った側面からセキュリティを分析してみることが期待できる。

また、従来の技術的コントロール及び制度的コントロールだけでは、よくある、制度の形骸化現象をうまく説明できなく、また、それに対する有効な対応策が考えつかなかった。セキュリティ関係の事故を SD モデル化により表現し、ST のアーキタイプの中の、目標のなし崩し現象が起きる様子を再現し、どのような対応策が有効かをシミュレーションで検討することなども有効であると考えられる。（システムの動的振る舞い）

(2) IT におけるセキュリティ

1) 情報セキュリティの動向

近年、ネットワーク会社の個人情報流出事件など、IT セキュリティに関係する事件が多発している。このようなセキュリティに係る事故が発生すると、顧客へのお詫びや株価下落、損害賠償やビジネス機会損失など膨大な被害が発生し、場合によれば組織の存続をあやうくする事態まで発生する。かっては、インターネットなどからの外部者による攻撃やウィルスがセキュリティ対策の中心課題であったが、近年は、委託先を含む内部関係者からの漏洩、事務所からの盗難、廃棄物からの顧客情報流出、置き忘れなどにより情報が漏洩し、顧客からのクレームで発見するなど、内部関係者による事件が多くなり、こちらの対策に重点が置かれるようになってきている。

政府も、刑法、著作権法、不正アクセス行為の禁止等に関する法律や個人情報の保護に関する法律の制定、経済産業省による情報セキュリティ監査制度の設立など、法制度の整備を進めている。このうち、2003 年に成立し、2005 年より施行が決まっている個人情報の保護に関する法律では、トレーサビリティという、情報漏洩を自己解決できるしくみ及び責任の所在を明確にする仕組みの確立、内部の不正に対する責任と義務、公に発覚する前に察知し、問題の公表、開示、原因究明、善後策の提示、苦情の適切かつ迅速な処置を求める企業責任と義務の明確化を要求している。

2) 情報セキュリティ・マネジメント・システム認定制度

そして、このような法律の整備に対応し、それを遵守するしくみとしての制度の面からは、企業内の情報セキュリティ確保のための情報セキュリティ・マネジメント・システムの認証のための制度が設置されている。セキュリティ認証制度は、最初に英国の BS7799 が設置され、これが ISO に取り入れられ、ISO/IEC17799 となっている。この日本版が JIS に取り入れられ、JIS X5080 となっている。ISO も JIS も基準で、これを守ることが推薦されるという制度である。従って、その基準を遵守していることを評価し、認定するという制度が必要となってくる。この認定制度では、情報処理開発協会(JIPDEC)の ISMS 適合性評価制度があり、企業の情報セキュリティ・マネジメント・システムの整備状況が評価され、認証される。現在、日本では金融機関、情報通信企業、病院、自治体、学校など 422（2004 年 5 月 13 日時点）の企業・団体・組織がこの認証制度で認定を受け、基準を満たしていることの認証を取得している。政府機関などでは、応札要件に認証取得を義務付けている所もある。

3) 情報セキュリティ・マネジメント・システムで保護するもの

情報セキュリティ・マネジメント・システムは、情報の機密性、完全性、可用性を保護することを目的としている。これを、計画－実施－チェック－改善の PDAC サイクルで継続的に運用管理する。また、情報セキュリティ・ポリシーを定め、ポリシーを実施するセキュリティ・スタンダードを定め、スタンダードに沿ってプロシジャーやマニュアルを整備し、それに従って業務を実施する。また、各部門のセキュリティ責任者などから構成される情報セキュリティ委員会などのモニタリング組織を設定し、セキュティ計画に沿って実施された内容についてレビューする。このようなしくみで情報セキュリティ・マネジメント・システムは運営される。

4) ISMS 適合性評価制度

ISMS 適合性評価制度に基づき、この認証を取得ための ISMS 認証基準が公表されている。この認証基準では、認証取得までは以下のような流れで進められる。

①ISMS の適用範囲を決める：コアとなるビジネスや重要な業務を対象に、自組織内でコントロールできるものに絞り、適用範囲の明確な線引きを行う。
②情報セキュリティ基本方針を定める
③リスク・アセスメントを行う：情報資産の洗い出しを行い、重要性を評価する。
④実施すべき管理目的及び管理策を選択する

⑤適用宣言書を作成する
⑥試験運用
⑦予備審査
⑧本審査
　基本的には、全ての情報資産の保護をするのではなく、投資対効果を勘案し、体系にもとづいた組織的な取り組みを継続しながらセキュリティ対策を行っていく。

(3) SD とセキュリティ研究

1) From Modeling to Managing Security – A System Dynamics Approach 概要

　SD 学会で、セキュリティ研究分科会設立が提案され、その提案に際して、セキュリティに関する論文をまとめた小雑誌、From Modeling to Managing Security – A System Dynamics Approach, ed. by J. Gonzalez が発刊された。この中から、2 つの研究を取り上げ、SD のセキュリティ研究の具体例として紹介したい。掲載されているのは以下の 5 本の論文である。

1. A System Dynamics Model of an Insider Attack on an Information System by C. Melara, J.Gonzales, A. Sawicka, et .al.
2. Choice Under Risk in IT-Environments According to Cumulative Prospect Theory by A. Sawicka, and J.J. Gonzalez
3. Learning from Incident , by D. L. Cooke
4. The Role of learning and Risk Perception in Compliance by J. Gonzalez, A. Sawicka
5. Emergency Management Simulations – An Approach to the Assessment of Decision-making Processes in Complex Dynamics Crisis Environment by K. Breuer and U. Satish

　このうち、2 は CPT: Cumulative Prospect Theory を適用した SD モデルを構築し、このモデルでバックアップ頻度などを変数にしてセキュリティの有効性や影響を IT のセキュリティをシミュレーションしてみたという内容で、理論的な話が中心である。4 は、人間的要因が存在し、どのように完璧と思われるシステムや制度を構築しようとも、おおかみ少年（ゴールのなし崩し）などが起きてしまうという現象を研究している。人間的要因（人間はリスクを正しく理解できない）という問題からこの現象が発生するのだが、
1)人間のリスク認知のやり方に問題（欠陥）がある。（完璧ではない）
2)人間のたましにしか発生しないものに対しての対応のやり方に問題（欠陥）がある。（完璧ではない）
3)コンピュータに依存しすぎる。しかも、その危険性に対する対応に問題（欠陥）がある。
4)情報セキュリティに関する意思決定に問題（欠陥）がある。そもそもこういったことを人間にさせることに無駄がある場合もある。
5)悪意を持っているかも知れない内部の人間を従事させなければならない。
6)ソーシャル・エンジニアリグ的問題。守秘しなければならない情報を簡単に攻撃にさらしてしまう。（例：ガードが固すぎると利用者からクレームが来る。クレームが多いとゴールのなし崩しが起きる。）
という大きく 6 つの原因からこの問題が起きる。この論文では、最後の部分に焦点を当て、その様子をモデル化し、シミュレーションしたものである。
　また、最後の 5 の論文では、戦略管理システム(Strategic Management System)に危機管理のシミュレーション要素(Emergency Management Simulation)が含まれているものもあり、中には 30 年以上使われているものもあり、これらは、危機管理の評価や危機管理の疑似体験によるトレーニングに使われてきたという経験を踏まえ、この危機管理シミュレーション的要素を含んだ戦略管理システムに SD 思考を組み込み、より高度化できるということを主張している。

2) A System Dynamics Model of an Insider Attack on an Information System

この論文は、1996 年に起きたオメガ・エンジニアリング社の事件を事例に取り上げ、SD でモデルを構築し、この事件の発生をトレースし、セキュリティ・レベルの強化や学習組織の組み込みの有効性をシミュレーションで検証したものである。

オメガ・エンジニアリングは米国ニュージャジー州にあるハイテク計測機器メーカーで、当時、グローバル戦略を採択し、世界規模の企業に脱皮しようとしていた。この中で、効率性や売上、利益が重視され、これらに直接結びつかない情報セキュリティ業務などは軽視されていった。

ティム・ロイドは同社電算部門に 11 年以上勤務してきたベテランで、同社のネットワーク・システム設計に従事し、その後、ネットワーク・システムの運用管理を任されていた。ティム・ロイドは、そろそろ自分も昇進すると思っていたが、結果は、会社から解雇され、彼のネットワーク・システム運用管理業務は外注先に引き継ぐことを指示された。そして、1996 年 7 月 10 日、ティム・ロイドは正式解雇された。

1996 年 7 月 31 日、オメガ・エンジニアリング社のコンピュータは一斉に稼動停止した。この知らせを受けて、自宅から会社に呼び戻された工場長のジム・ファーガソンは、バック・アップ・ファイルを探したが、どこにも見あたらなかった。次に、単独で稼動し、データやプログラムが残っている PC を探したが、会社の中にあるどの PC やサーバーにも、データ及びプログラムは全て消去されていた。オメガ・エンジニアリングは、この事件での逸注、生産活動中断などの被害を受け、その総額は 1 千万ドル（約 11 億円）にも上った。

この事件発生前に、ティム・ロイドは同社の効率性重視の姿勢や電算業務作業環境悪化に不満を述べていた。また、彼は、ちょっとしたシステム・ダウンを引き起こしていた。こういった初期兆候を見逃し、ティム・ロイドをネットワーク運用管理担当者として使い続けたばかりか、さらに、オメガ社は、ティム・ロイドにバックアップ・ファイル管理の業務までも兼任させるという内部牽制機能破壊を行っていた。さらに、オメガ社は、ティム・ロイドを解雇する際に、外部業者に業務引継ぎを指示したが、引継ぎを受ける者の確認もしなく、引き継いだということの確認（バックアップ・ファイルの内容、保管場所の確認、コンピュータ内部の変更プログラムの確認等）も行なわなかった。

うすうす首になることを感じていたティム・ロイドは、ネットワーク運用管理担当者である立場を利用して、分散型であった同社のネットワーク・システムを、1 台のサーバーがコントロールする中央管理型にプログラム変更を行った。次にバックアップ・ファイルを消去し、時限爆弾をネットワーク管理サーバーに仕掛けた。

オメガ・エンジニアリング社は、警告となる兆候を見逃し、さらに、セキュリティ・ポリシーも不在で、セキュリティに関する内部監査も実施していなかった。そして、ティム・ロイドに時限爆弾設をテストし、設置させる十分な時間を与えてしまった。

この事件を示す SD モデルは、以下の 3 つのモジュールから構成される。

・システムの稼動停止を表現したモジュール
・作業環境が悪くなり電算要員が犯罪を引き起こすようになることを表現したモジュール
・セキュリティ・レベルが低下していくことを表現したモジュール

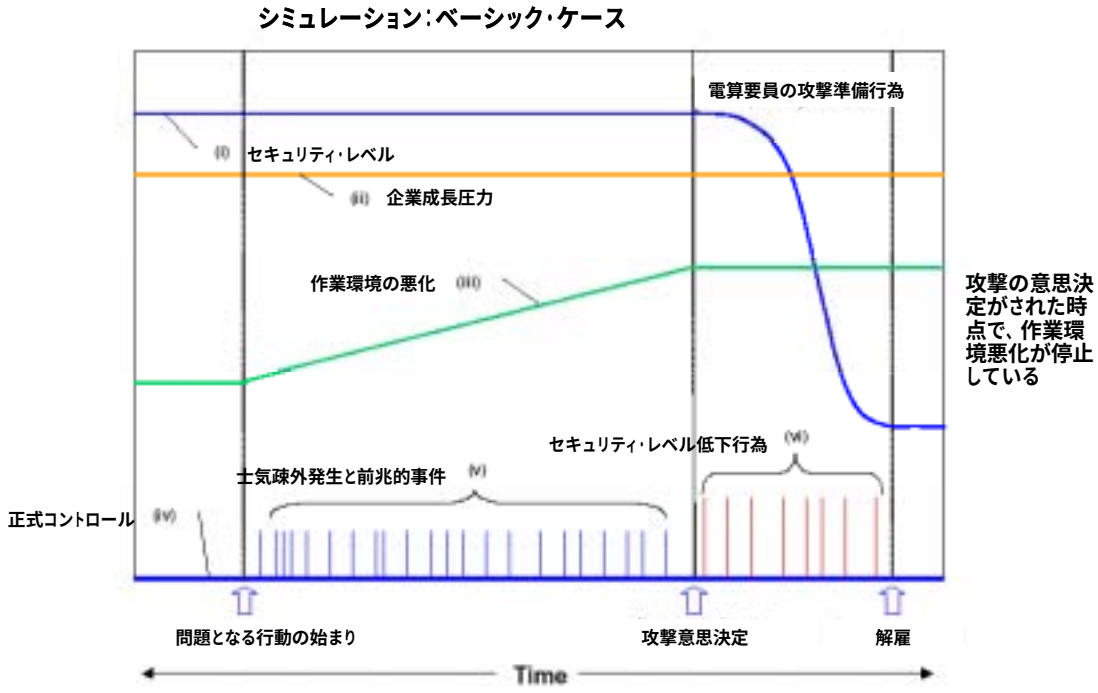
そして、システムの稼動停止は大きく 2 つの流れで発生する。

・前兆的な事件
・電算要員の問題となる挙動

また、この事件は、計画的というよりは、電算要員の不平不満が表面化したという要素が強いものと考え、さらに、技術的コントロールや制度的コントロールを否定するわけではなく、これらは有効であるが、十分ではないという前提でモデル化を行っている。

ベーシック・ケースとして、モデルを使ってシミュレーションしてみると、作業環境が悪化し、ティム・ロイドが時限爆弾設置を決意し、システムのセキュリティ・レベルを下げる様子がうまく表現できている。また、ティム・ロイドが時限爆弾設置を決意し

た後は、士気疎外の発生や前兆的事故がストップしている。また、悪化を続けていた作業環境も、この時点でフラットになっている。



管理者のシステム・セキュリティ・レベルの認知変化

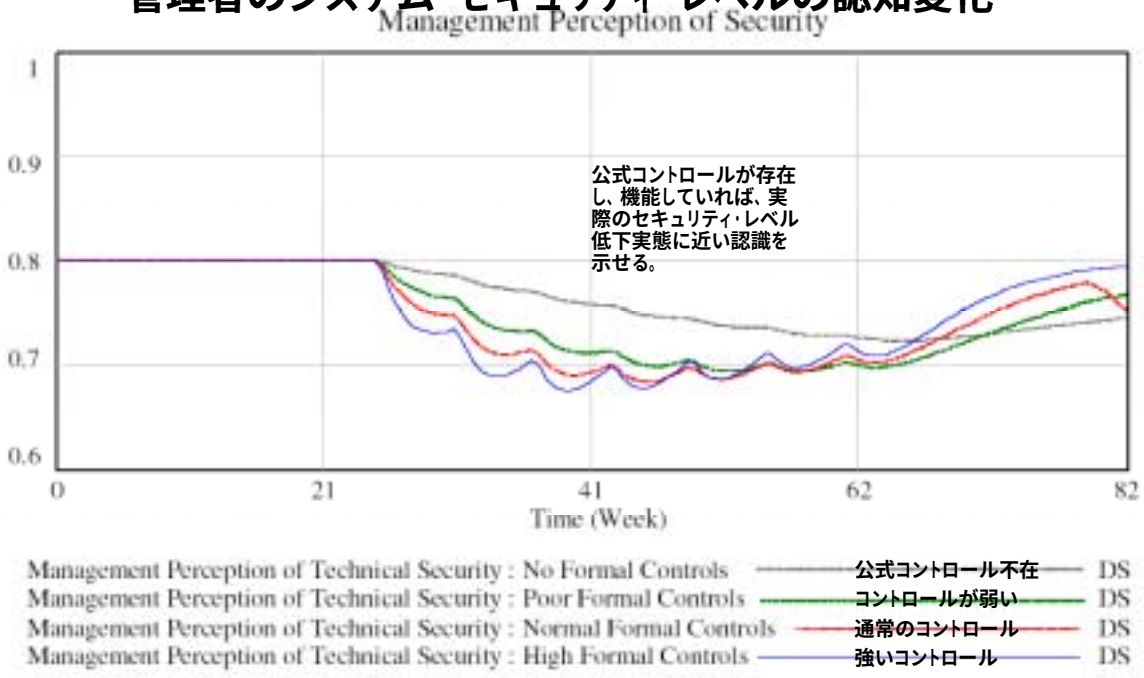


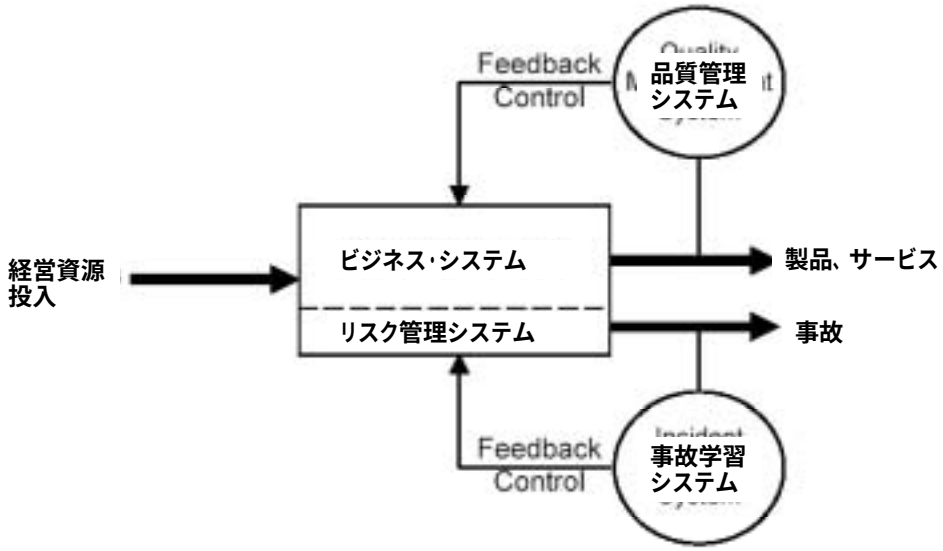
Fig. 9: Change in Management Perception of Security when Formal Controls increase.

このベーシック・ケースに対して、セキュリティ対策を設けることで、セキュリティ・レベルが低下したことを早期に発見でき、抑制効果があることがシミュレーションでも確かめられる。また、前兆的な事故を認識し、それを学習組織のループとして組み込むことも有効であることがシミュレーションで確かめられた。

3) Learning from Incident, by D. L. Cooke

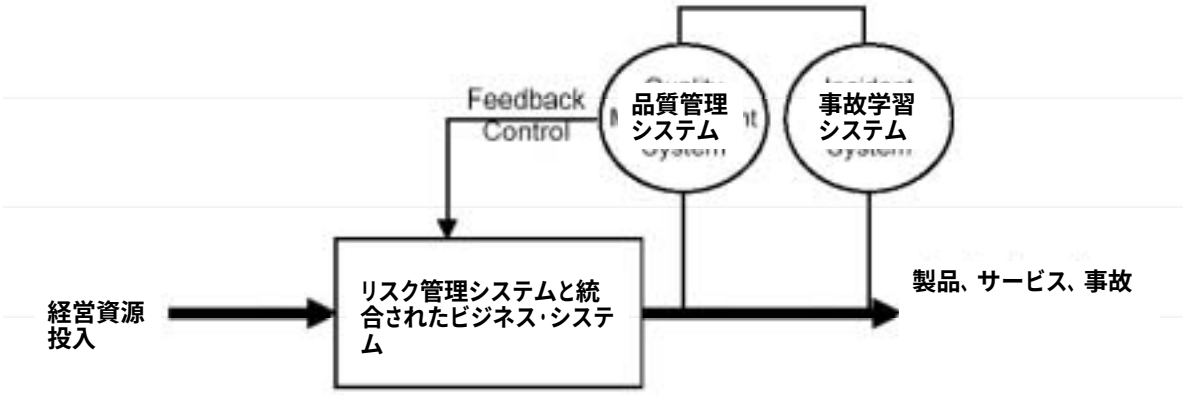
先の論文で、非公式的コントロールとしてのセキュリティ対策には、学習する組織の構造を組織に定着させることが有効であることが述べられている。この論文は、品質管理システムと統合した形で、事故から学ぶ、自己学習組織ならぬ事故学習組織のシステムをビジネス・システムに統合することの有効性を研究したものである。

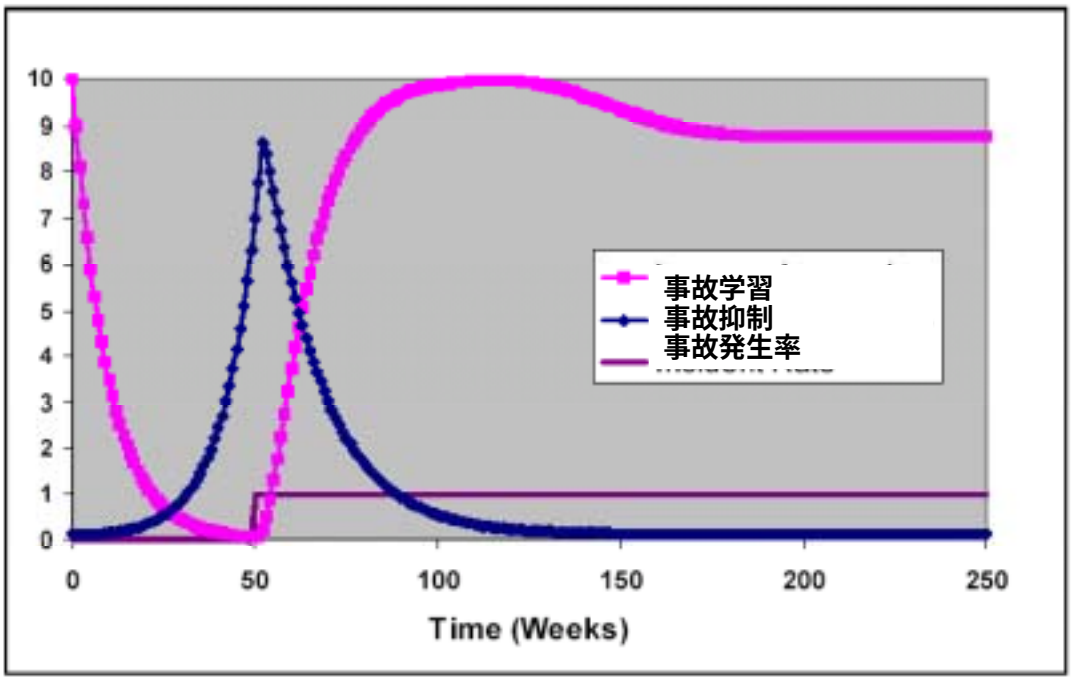
学習組織のシステム(Incident Leaning System)と品質管理システム(Quality Management System)を統合すればいいことは常識的なことではあるが、性格の違いがあり、従来的な品質管理システムだけではセキュリティは十分に確保できない。品質管理システムをどのように高度化させても、設計された範囲（さらには、予め分かっていた範囲）を超えられない。予め予想もできなかったことにより起きる事故もある。



そこで、事故学習システムをビジネス・システムに追加するような上記のシステムを採択する企業が多いが、これでは、品質管理に属する事故が事故学習システムにも情報として流れてきて適切ではない。そこで、以下のような統合システムが考えられる。

こうした、事故学習システムをビジネス・システムに統合し、このシステム機能を使い、前兆的な事故をしっかりと認識し、現場対策だけで終わらせないで、その発生構造を分析し、再発生させない対策をとると共に、事故を学習し知識や経験を蓄積し、これらの蓄積から、過去の事故に対する対応の擬似体験などで学習を組織に定着させることで事故発生を抑制できる。





4) まとめ

以上、いくつか、IT セキュリティに関する SD 研究を紹介してきたが、SD でこれまで研究されてきた学習する組織や、システム類型、そして、SD の特徴である動的な分析など、いわゆる SD 研究の成果を活用することで、セキュリティの研究は、従来の技術的コントロールや公式的コントロール一辺倒だけではなく、制度の形骸化の防止などもっと幅広く、別の視点からも光を当てることができることが期待できる。

(4) 質問及び討議から

IT セキュリティを SD でモデル化し、研究することに対して、このような SD モデルを経営者に示し、経営判断や経営意思決定を求めることは危険である、複雑すぎ、誤解を招くのではないかという意見があった。また、IT セキュリティを SD モデル化することに関しても、擬似体験学習という効果はあるにしても、経営に関するシステムとしてそのまま使うには無理があるし、動的にトレースする意味も薄いのではないかという意見があった。

例会では十分これらの回答に答えられなかったが、SD のセキュリティ研究の事例の紹介者としては、紹介したモデル（1.の論文）は、経営の意思決定や経営判断を主目的にしたものではない。この論文紹介の目的は、内部の悪意を持った従業員が犯罪に至る心理的な面をシミュレーションし、今まで不可能と考えられていた、心理的な面も考慮したモデル化が可能であるという例として紹介したものである。セキュリティ対策では、犯人の心理的な変化も含めて考慮しなければ、公式的及び非公式的なコントロールの効果が十分に分析できないと考える。そして、このことは、SD だからできることではないかと考える。

（文責：末武）