情報セキュリティマネジメントの構造分析に関する研究

代表研究者　　川　中　孝　章　　東京大学大学院工学系研究科　特任研究員
共同研究者　　六　川　修　一　　東京大学大学院工学系研究科　教授

1 はじめに

インターネットがもたらす影の側面としての情報セキュリティ問題は、それに対する防御の重要性が指摘され、対策が行われているにもかかわらず、一向に終息の気配はなく、むしろ多様化・拡大化の方向へと向かっている。情報通信を社会にとって役立つものにするためには、この問題に対する対応は避けて通れないものとなっている。本研究では、情報セキュリティ問題が企業経営に及ぼす影響に焦点をあて、インターネット社会で企業経営を行うにあたり、情報セキュリティの脅威からいかに企業を守り、いかにすれば安心して情報通信サービスを利用できるかについて、その対応策を提案する。

現在、企業では神経質なまでに情報セキュリティ対策が行われている。社員は本業が忙しい中で、情報セキュリティ対策にも注意を払わねばならず、本業の業務効率を下げることになるにもかかわらず、その対策の完璧な実施が求められる。一方、その割には、情報セキュリティ事故は減っておらず、国民を不安に落とし入れる事件が現在も発生し続けている。このような状況の中で、企業には、できるだけ効率の良い、効果的な対策の実施が求められることになる。

情報通信社会は環境の変化が激しく、IT 革命が進展している今日、企業は様々な状況変化に対応できるよう、情報セキュリティ対策を実施しなければならない。新しい脅威が出現するとそれに対応する対策の実施が求められ、企業においては、その対策が効果的なものになるかどうかがが最大の関心事となる。企業組織内で、対策を施したときにどのような効果が得られるのかについて、事前にシミュレーションが実施できれば、対策実施の意思決定のための有効な手段となる。本研究では、まず、情報セキュリティマネジメントについて企業組織面からモデル化を行い、対策の実施とその効果の測定方法を提案する。次に、最近特に注目されている生産現場における制御システムのセキュリティについて、セキュリティパッチの適用方法に着目してモデルを作成し、最適な対策を行う方法を提案する。最後に、企業の情報セキュリティ対策が適切に実施されているかを監視するための監査制度を取り上げ、情報セキュリティ監査制度が有効に働くための条件を、ゲーム理論によって導き出す。このように、情報セキュリティマネジメントに関して多面的にモデル化を行い、分析し、その結果からマネジメント全体の構造解明を行うことを本研究は目的としている。なお、紙面の制約上、全ての研究内容を掲載しきれていないため、研究の詳細については、各ジャーナルをご覧いただきたい。

2 本研究の構成

本研究では、情報セキュリティの問題に対して特に経営面からアプローチを行い、

① 企業における情報セキュリティのリスク分析（3 章）
② 生産制御システムへのサイバー攻撃におけるソフトウェア対策（4 章）
③ クラウドサービス市場における情報セキュリティ監査モデル（5 章）

といった、情報セキュリティ問題を多面的に検討するためのモデルを構築し、その分析結果を提示する。最後に 6 章で本研究の議論を整理するとともに、各章の提案モデルや考察から得られた研究成果を明らかにする。これにより、情報セキュリティマネジメント研究の新たな方向性を示唆するとともに、本研究の限界を踏まえた上での今後の研究課題についても整理する。

3 企業における情報セキュリティのリスク分析

3-1 概要

企業において情報セキュリティマネジメントを行う際、情報資産に関するリスク分析を実施する場合が多い[1]。これは、全情報資産の洗い出しを行い、それに関する脅威と脆弱性を分析するプロセスからなり、その結果を元に企業は対策を実施する。一方、方法としては、専門家の意見や標準規格を元に対策を実施する方法もある。前者は、労力がかかる反面、リスクの見落としが少なく、後者は、効率的ではあるが、現場の

状況を反映しにくいという面があり、両者は一長一短の側面を持つ。この章では、このようなリスク分析のプロセスにリスク評価を加えたリスクアセスメントに関して、新たなモデルを提案する。さらに、その評価に関しては、情報セキュリティ事象をマルチエージェントによりモデル化して、実験的に評価結果を導く手法を提案する。

3-2 情報セキュリティ事象のモデル化

3-2-1 情報資産に関する脅威・脆弱性・対策の関係

情報セキュリティ事象のモデル化を行うにあたり、その前提となる情報資産に関する脅威・脆弱性・対策の関係を**図 1** に示す[2]。ここでは、情報資産を攻撃する脅威とそれに対応する脆弱性は、それぞれ、同種のものどうしがカウンターパートとなって攻防を展開する。脆弱性は、企業の何らかの情報セキュリティ対策によって制御されるものとし、逆に脆弱性をなくそうと企業は情報セキュリティ対策に努めるものとする。

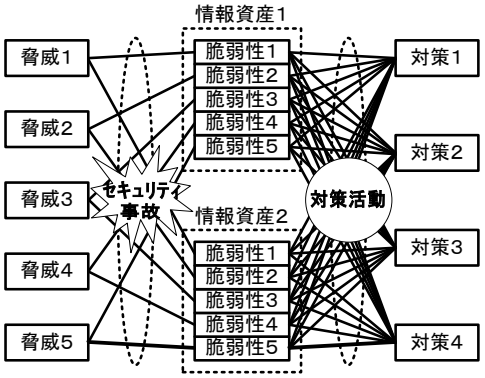


図 1　情報資産に関する脅威・脆弱性・対策の関係

3-2-2 情報セキュリティ事故のモデル化

情報セキュリティ事故（以下セキュリティ事故、又は単に事故ともいう）とは、何らかの脅威によって情報資産の機密性、完全性、可用性のいずれかが損なわれることであり、これによって情報資産の価値が損なわれる。本章では、事象をできるだけ単純化するためにセキュリティ事故が発生すると資産価値は完全に失われてしまうものとしてモデル化を行う。

方法としては、マルチエージェントを用いて情報セキュリティ事故をモデル化する[3]。この方法を用いたのは、情報資産エージェントと脅威エージェントの 2 種類のエージェントを設定することにより、本来、目に見えにくい情報セキュリティ事故という事象を視覚的に表現でき、また、エージェントの属性や行動ルールを変更することにより、事故の発生とそれに対するマネジメントの特徴を比較的たやすく記述できると考えたからである。

3-2-3 エージェントの配置と視野の概念

図 2 のような格子型に区切られた空間を設定し、そこに情報資産エージェントと脅威エージェントをランダムに配置する。この空間は情報資産と脅威が近い位置関係にあるのか、あるいは、遠い位置関係にあるのかを表すものであり、格子型空間の縦軸横軸は単に距離を表すものとする。脅威エージェントの種類は、コンピュータウイルス、システムトラブルなど 5 種類を設定する。

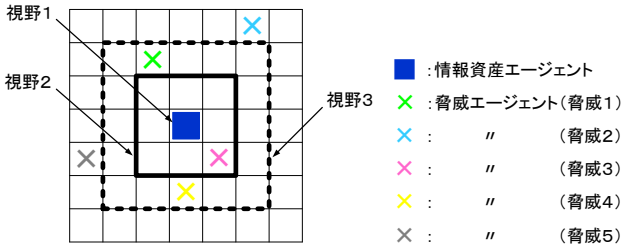


図 2　エージェントの配置と視野の概念

設定した空間のサイズとエージェント数は、次の通りである。なお、脅威の種類毎に、強さの度合いによって脅威エージェント数を案分している。

・空間サイズ
　50×50 の格子型 2 次元空間（企業空間）
・エージェント数
　情報資産エージェント → 100
　脅威エージェント　　→ 100（5 種類の合計）

さらに、このモデルの特徴として、情報資産エージェントに視野の概念を導入している。**図 2** の情報資産から見て自分自身の位置を視野 1、太い実線で囲まれた範囲を視野 2、点線で囲まれた範囲を視野 3 とする。視野が 4 以上の場合も同様の考え方で、数字が大きくなるに従い 1 セル分ずつ外側へ視野の範囲が拡大していくものとする。一方、視野が全くない状態を視野 0 とする。

情報資産エージェントにおける視野の概念を、企業の情報セキュリティマネジメントに置き換えてみると、視野が大きいとは、組織内においてリスク分析のための情報資産の洗い出しが正確になされ、脅威や脆弱性に関する情報収集が詳細に行われている状態をさす。逆に、視野が小さいとは、組織内で情報資産に関する調査を怠り、脅威や脆弱性に関する情報が少ない状態をさす。

3-2-4 エージェントの属性

情報資産エージェントと脅威エージェントには、それぞれ脆弱性と脅威という強弱を表す属性を持たせる。一般に、脆弱性は弱さを表す属性であり脅威は強さを表す属性であるが、ここでは属性毎に強弱の方向性を統一するため、脆弱性とは逆の「非脆弱性」という強さを表わす属性を使用する。このモデルでは、属性に基準値を与え、情報セキュリティ事故は、脅威と非脆弱性の基準値、双方の大小関係と事故率によって、確率的に引き起こされると設定している。

図 3 にエージェントによるシミュレーションの実行画面を示す。シミュレータは、構造計画研究所の artisoc を用いている。

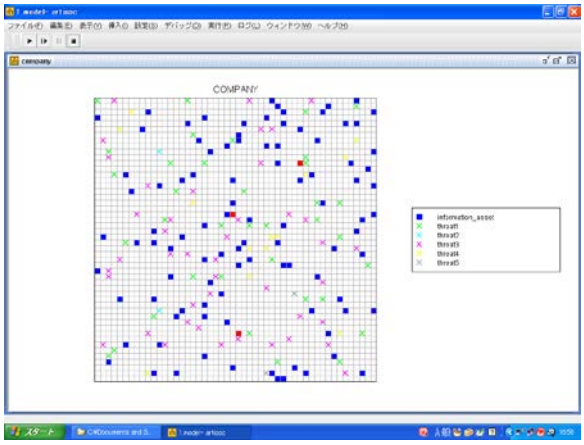


図 3 シミュレーションの実行画面

3-3 情報セキュリティにおけるリスクアセスメント

図 4 に情報セキュリティにおけるリスクアセスメントの流れを示す。

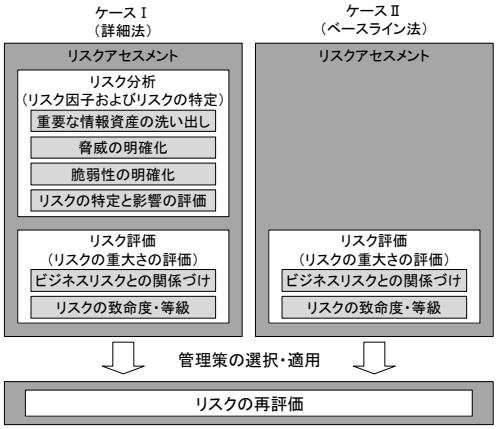


図 4　リスクアセスメントの流れ[1]

ケースⅠは、詳細法とも呼ばれており、情報資産を総当たり法で調べていく方法である。企業の膨大な資産を一つずつ洗い出していくこの方法は、プロセス的には全ての資産を調査するわけであるから、守るべき情報資産を明確化できるというメリットがある反面、全社でこれを行うには、時間とコストがかかるというデメリットがある。一方、専門家の意見や標準規格などを参考にしてベースラインを設定するケースⅡの方法は、ベースライン法とも呼ばれており、ケースⅠに比べて時間やコストがかからないというメリットがある反面、企業固有の問題点を見落としやすく、ベースラインの設定が分析者のセンスに依存するというデメリットがある。

ケースⅠとⅡは、互いにメリット・デメリットがあり、本研究では両者を組み合わせた方法を提案し、マルチエージェント・シミュレーションにより、その効果を分析することを試みる。

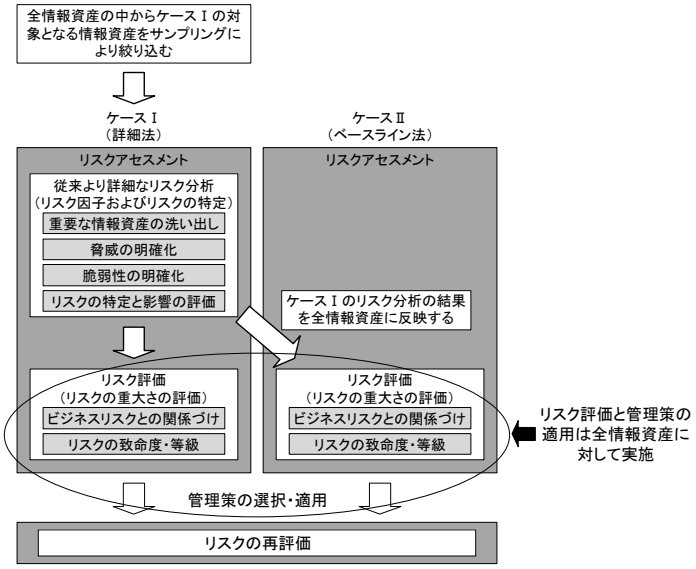


図 5　本章の提案（図 4[1]に筆者が加筆）

手順として、まず、企業内の情報資産について、ケースⅠの方法でリスクアセスメントを行う資産と、ケースⅡの方法で行う資産とに区別する。ここで、ケースⅠの方法で行う資産はサンプリングにより抽出する。その方法としては、課単位でも部単位でもよいが、なるべく、同種の業務を行う部署のみに偏らないように、全社から万遍なく対象部署を抽出する。次に、ケースⅠの情報資産を対象にリスク分析を行った上で、さらにリスク評価を行うわけであるが、このリスク評価の段階ではケースⅡの対象資産を含めた全情報資産に対して、ケースⅠのリスク分析結果を反映したリスク評価を行う。このようにして全社の情報資産に対してリスクアセスメントを実施し、それに対して管理策を実施した後に、リスクの再評価を行い対策の効果を確認する。

3-4 研究フロー図

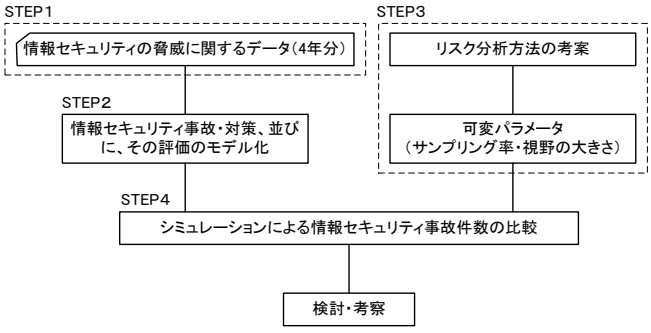


図 6　研究フロー図

3-5 データ収集

使用データ：経済産業省「平成 18～21 年 情報処理実態調査」の公開データ（4 年分）[4]
使用項目：「情報セキュリティトラブルの発生状況」「情報セキュリティトラブルの重要性に対する認識」
対象企業：民間事業者 9,500 社
集計企業：4 年間延べ　17,577 社
調査対象期間：平成 17 年 4 月 1 日～同 21 年 3 月 31 日

3-6 モデル化

情報セキュリティ事故、対策、並びに、その評価方法をモデル化する。

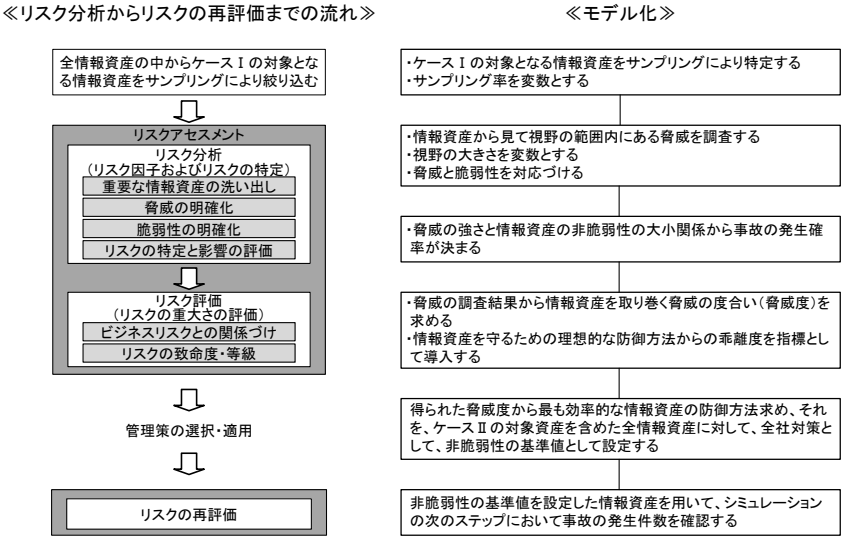


図 7　モデル化との対応関係

3-7 リスク分析の方法と可変パラメータ

本章で提案するリスク分析方法を次の 2 つのパラメータを用いて記述する。

① サンプリング率（調査する情報資産の割合）
　情報資産を全数調査する方式からサンプリング調査に変更した場合の影響を段階的に測定するためのパラメータ。

② 視野の大きさ（調査精度）
　情報資産を取り巻く脅威の調査精度を可変にした場合の影響を、段階的に測定するためのパラメータ。

3-8 シミュレーションによる情報セキュリティ事故件数の比較

過去の年度の調査結果を元に対策を行うと仮定した場合に、平成 20 年度の事故件数がどのように変化するかをシミュレートする。ここでは過去 1～3 年分の調査結果を用いて、合計 3 パターンを実施する。各パターンのシミュレーションにおいては、サンプリング率と視野の大きさを変えながら事故件数への影響を測定する。

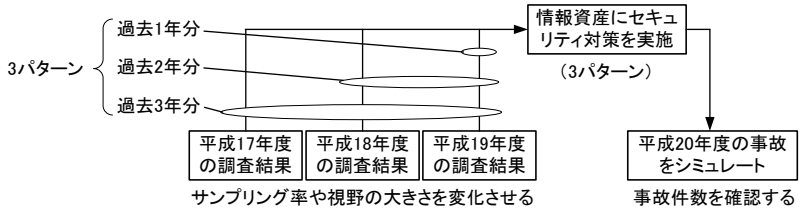


図 8　情報資産の調査結果と事故のシミュレーション

3-9 シミュレーション結果

シミュレーション結果をグラフ化したものを**図 9～11** に示す。

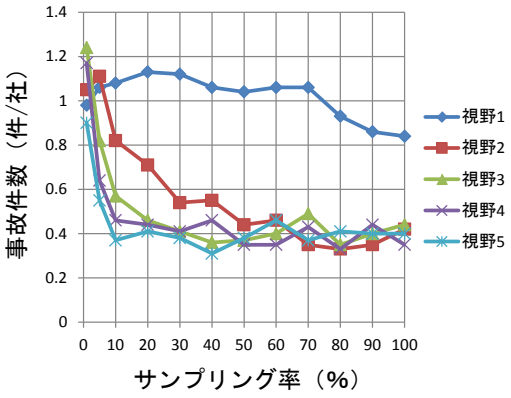


図 9　サンプリング率、視野、事故件数の関係
（過去 1 年分の調査結果を用いたパターン）

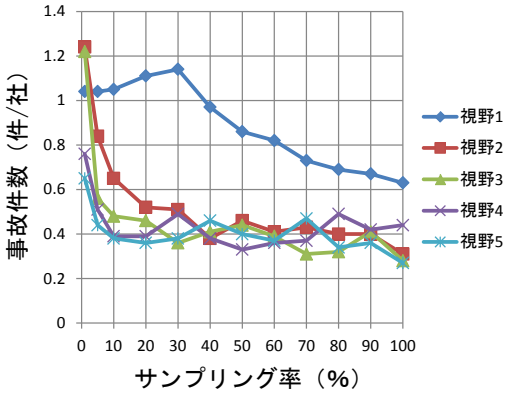


図 10　サンプリング率、視野、事故件数の関係
（過去 2 年分の調査結果を用いたパターン）

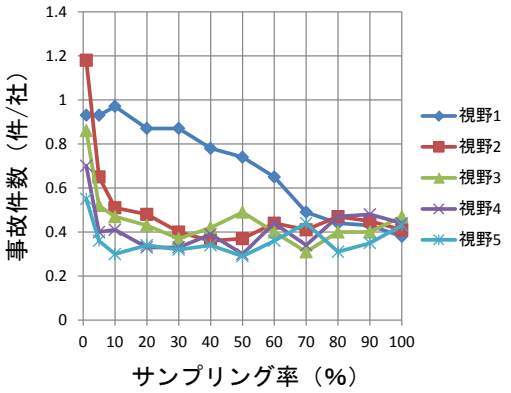


図 11　サンプリング率、視野、事故件数の関係
（過去 3 年分の調査結果を用いたパターン）

3-10 本章の考察

3 つのグラフを比較することにより、過去の複数年度の情報を元にして、対策を立案・実施することが、事故件数を減らすことに効果があることがわかる。いずれの視野においても、過去 1 年分→2 年分→3 年分と情報が多くなるに従い、特にサンプリング率 10%前後での事故件数の減少が著しくなっている。これは、変化が激しいと考えられている情報セキュリティの分野ではあるが、たとえ数年前の情報であってもそれを加味して対策を行う方が、事故件数の低減に役立つことを示唆している。

視野に着目すると、各グラフとも視野が大きくなるに従い、事故件数が小さくなっている。これはリスク分析の最初に情報資産の洗い出しを行う際に、より詳しく資産の情報を収集し対策を実施する方が、事故件数が小さくなることを意味している。

次に、サンプリング率に着目する。ここでは、企業が従来の調査精度のまま、全数調査（サンプリング率 100%）を行ったときの事故件数を基準値として用いる。経済産業省の公開データによる平成 20 年度の事故件数は 0.49 件/社である。事故件数がこの数字を下回ると、従来の調査精度で全数調査を行った場合と同等の効果があると判断し、それを収束と呼ぶことにする。グラフ上で収束しているときのサンプリング率でリスク分析を行えば、数字上は、従来の調査精度で全数調査を行ったときと、事故件数的には同じ効果が得られることになる。視野別に見ていくと、視野 3 以上の場合は、いずれのグラフにおいても、サンプリング率が 10%以内でほぼ収束している。視野 2 の場合は、過去 1 年分の調査結果を用いたときはサンプリング率 50%で、2 年分のときは 40%で、3 年分のときは 20%で収束に至っている。ところが、視野 1 の場合は、過去 1 年分と 2 年分の調査結果を用いたときは、サンプリング率 100%でも収束せず、過去 3 年分の結果を用いてようやく収束に至っている。従来の対策が過去何年分の調査結果を用いていたのかについては、正確にはわからないが、仮に 2 年以内の調査結果を元に行われていたと仮定した場合、従来の全数調査（サンプリング率 100%）で収束に至るには、少なくとも視野が 1 より大きくなければならない。これは現実の世界の調査精度が、このモデルでいうところの視野 1 より大きいことを表しており、現実の世界では、最低でも視野 1 と 2

の間の調査精度で情報資産の洗い出しを行っていることになる。調査員のスキルを上げ、調査精度を視野 2 のレベルにまで引き上げたとすれば、本章の視野 2 のシミュレーション結果を活用できることになる。

情報セキュリティマネジメントの施策について、企業の現場で予めその効果を測定することは非常に困難である。このような実験的方法は、それを解決するための糸口になると考えている。

4 生産制御システムへのサイバー攻撃におけるソフトウェア対策

4-1 概要

自動車、電機などの製造業や、電気、ガス、水道などのインフラ関連産業の生産制御システムは、これまで一般に普及している情報システムとは、ハード、OS、アプリケーションなどの面で、一線を介するものであった[5]。しかし、近年では、Windows などの汎用 OS が、生産制御システムにも使用されるようになっており[6]、情報システムを対象としていたサイバー攻撃の脅威が、生産制御システムにも及ぶ可能性が高くなってきた。

Microsoft などの OS メーカーでは、サイバー攻撃の脅威に対処するために、セキュリティパッチを発行している。しかし、生産現場では、それを適用したときの副作用の可能性や、副作用がないことを確認するための試験費用の発生を恐れて、見かけ上の不具合さえなければ、放置したまま運用されることがむしろ普通のようになっている。さらに、連続運転が要求される生産制御システムでは、パッチの適用などシステムを手直しできるタイミングが、長い時間待たないと巡ってこないこともしばしばである。

本章では、このような生産制御システムの現状を鑑み、サイバー攻撃からシステムを守るためのソフトウェア対策に関するセキュリティ・パッチの適用に焦点を当て、パッチを適用せずに放置しておく損失とパッチを適用したときに副作用がないことを確認するための試験費用の総和を最小化する方法により、最適なパッチ適用タイミングと、かけられる試験費用を求める方法を提案する。

4-2 本章のモデルの特徴

モデルの特徴は次の点である。

① 生産制御システムを使用する組織や企業の立場に立ち、サイバー攻撃に備えたソフトウェア対策を提案する点。

② ソフトウェアの脆弱性に焦点を当て、サイバー攻撃を受けるリスクとパッチ適用に関わる費用を考慮したモデルを提案する点。

③ パッチの適用周期と事前テスト期間の最適値を導く点。

4-3 研究フロー図

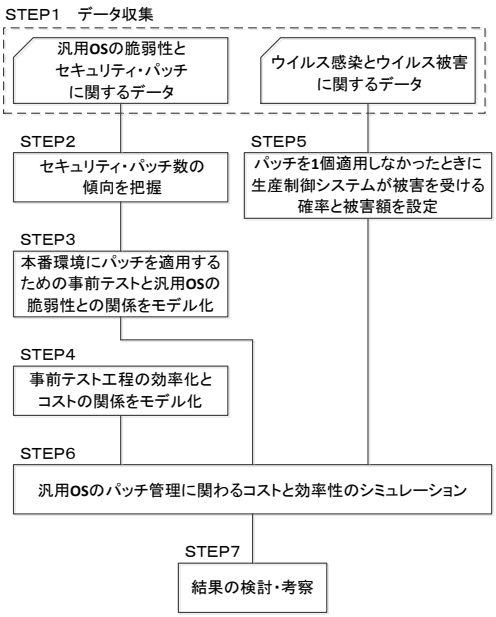


図 12　研究フロー図

4-4 データ収集

＜収集データ①＞

・対象 OS ：WindowsXP

・出典　　：Microsoft Security Bulletins[7]

・使用項目：「セキュリティ・パッチ（セキュリティ更新プログラム）」

・対象期間：2001 年 11 月～2013 年 12 月（145 ヶ月）

＜収集データ②＞

・出典　　：2011 年度情報セキュリティ事象被害状況調査－報告書－[8]

・調査機関：独立行政法人 情報処理推進機構

・使用項目：「セキュリティ・パッチの適用」「コンピュータウイルスによる被害状況」
「ウイルスの直接的な被害」

・対象期間：2011 年 4 月～2012 年 3 月

・回答企業：1767 社

4-5 セキュリティ・パッチ数の傾向を把握

WindowsXP が発売された 2001 年 11 月からの経過月数を横軸にとり、それ以降の累積セキュリティ・パッチ数を縦軸にとったグラフを**図 13** に示す。

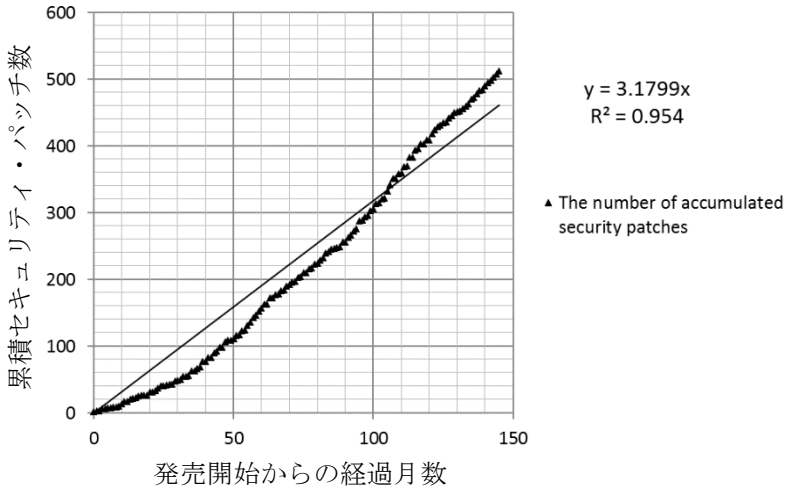


図 13　WindowsXP のセキュリティ・パッチ数

4-6 本番環境にパッチを適用するための事前テストと汎用 OS の脆弱性との関係をモデル化

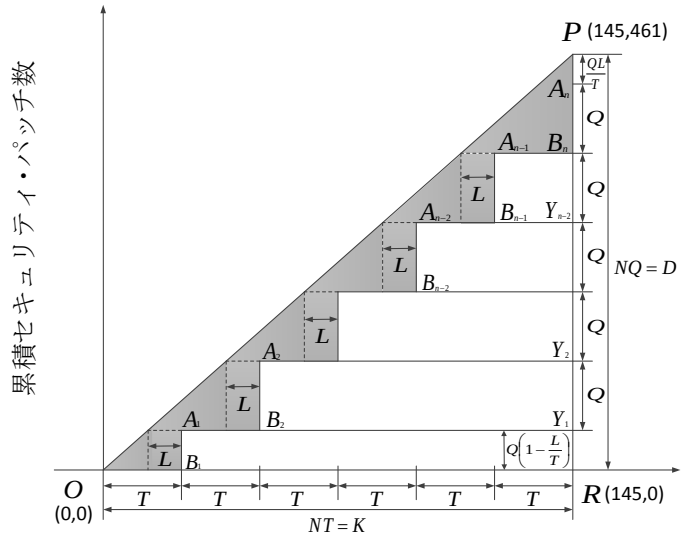


図 14　セキュリティ・パッチのロットサイズ（Q）、適用周期（T）、テスト期間（L）の関係

＜使用記号＞

D：全セキュリティ・パッチ数（＝461 個）（図 13 の近似直線の推定値より）

Q：1 回に適用するセキュリティ・パッチ数（個）

N：セキュリティ・パッチの適用回数（回）（（例）2001 年 11 月～2013 年 12 月の間での合計回数）

n：セキュリティ・パッチの適用回数を表す整数（$n = 1,2,\cdots,N$）

T：セキュリティ・パッチの適用周期（ヶ月）

K：OS が発売されたときから直近までの経過月数（＝145 ヶ月）

L：テスト期間(ヶ月)（期間短縮を考慮しないテスト期間表記（通常期間））

S：テスト費用（千円/回）（通常期間で実施する場合）

TC：パッチ管理に関わる総費用（Total Cost）（千円）

i ：テスト期間の短縮パターン（$i = 0,1,2,3,4$）

$$i = \begin{cases} 0\cdots\cdots\text{全工程を通常期間} \\ 1\cdots\cdots\text{第 1 工程を最小期間、他は通常期間} \\ 2\cdots\cdots\text{第 1～2 工程を最小期間、他は通常期間} \\ 3\cdots\cdots\text{第 1～3 工程を最小期間、他は通常期間} \\ 4\cdots\cdots\text{全 4 工程を最小期間} \end{cases}$$

L_i：期間短縮を考慮したときのテスト期間表記（ヶ月）

$C(L_i)$：テスト期間短縮費用（千円）

j ：第 j 工程（$j = 1,2,3,4$）

$$j = \begin{cases} 1\cdot\cdot\text{単体テスト} \\ 2\cdot\cdot\text{結合テスト} \\ 3\cdot\cdot\text{システムテスト} \\ 4\cdot\cdot\text{オペレーションテスト} \end{cases}$$

a_j：テストの第 j 工程の最小期間（ヶ月）

b_j：テストの第 j 工程の通常期間（ヶ月）

c_j：テストの第 j 工程を 1 ヶ月短縮するために必要な費用（千円/月）

u ：パッチを 1 個適用しなかったときに生産制御システムが被害を受ける確率

v ：生産制御システムが 1 回被害を受けたときの予想損失額（千円）

h ：パッチを 1 個適用しなかったときの予想損失額（千円）

今、**図 14** の網掛けの面積を求めることにする。**図 14** の直線 OP は、**図 13** の累積セキュリティ・パッチ数の近似直線に相当する。**図 14** に基づき、大きな三角形 OPR の面積から$OB_1A_1\cdots B_{n-1}A_{n-1}B_nP$ の階段状の面積を引くと、図の網掛けの面積が求まる。この面積は、例えば WindowsXP の場合であれば、2001 年 11 月～2013 年 12 月の間で既に公知になっていたにもかかわらずパッチを適用していなかった脆弱性数とその時間に比例する。なお、ここでのテスト期間の表記は、期間短縮を考慮しないテスト期間表記 L を用いる。

・網掛けの面積

$$= \frac{D}{2N}\left(N \times \frac{K}{N} + 2NL - 2L\right)$$

$$= \frac{KD}{2N} + DL - \frac{DL}{N} \qquad \cdots (1)$$

図 14 の大きな三角形 OPR の面積は、OS が発売されてからこれまでの間に公開された累積セキュリティ・パッチ数に経過月数をかけたものであり、言い換えれば、生産制御システムが汎用 OS を介してサイバー攻撃を受けるリスクの時間的総和である。一方、$OB_1A_1\cdots B_{n-1}A_{n-1}B_nP$の階段状の面積は分解すると、細長い短冊状の面積を積み重ねたものになり（$B_1A_1Y_1R + B_2A_2Y_2Y_1 + \cdots + B_{n-1}A_{n-1}B_nY_{n-2}$）、システムを手直しできるタイミングなどで定期的にパッチを適用していくことにより、短冊状の面積分のリスクが解消されていく。また、網掛けの面積は、公開後すぐに自動更新機能によるパッチ適用ができないような生産制御システムの端末などに一時的に残ってしまうリスクの大きさを表している。この面積はテスト期間の長短により増

減する。すなわち、テスト期間が長いとテストを開始する時点で決定した適用パッチが、テストを終えて実際の本番環境に適用するときには最新ではなくなり、最新パッチの適用が次回に先送りされることにより、網掛けの面積、つまりリスクが増大するのである。

4-7 事前テスト工程の効率化と費用の関係をモデル化

図 15　ソフトウェアテストのプロセス

今、テスト工程の中の第 j 工程が通常期間b_jで行われるとしたとき、これを最小期間a_jで行うための単位期間あたりのテスト期間短縮費用をc_jとする。一般に、製造現場や建設現場では、工期と費用はトレードオフの関係にあり[9]、この関係をモデル式で表すと次の（2）～（5）式のようになる。

テスト期間L_iは、

$$L_i = \sum_{j=1}^{4} b_j - \sum_{j=1}^{i} (b_j - a_j) \qquad \cdots (2)$$

ただし、

$$L_0 = \sum_{j=1}^{4} b_j \qquad \cdots (3)$$

i と j は、それぞれテスト期間の短縮パターン並びに各工程を表す（使用記号を参照）。ここでは 5 つのパターンを取り上げた。テスト期間短縮費用$C(L_i)$は、

$i = 0$のとき

$$C(L_0) = 0 \qquad \cdots (4)$$

i=1～4 のとき

$$C(L_i) = \sum_{j=1}^{i} c_j (b_j - a_j) \qquad \cdots (5)$$

で表すことができる。

4-8 パッチを 1 件適用しなかったときに生産制御システムが被害を受ける確率と被害額の設定

パッチを 1 件適用しなかったときに生産制御システムが被害を受ける確率uは次のようになる。

$$u = 5.98426 \times 10^{-4} \times (0.425 + 0.171 + 0.107)$$
$$= 4.20693 \times 10^{-4} \qquad \cdots (6)$$

生産制御システムが 1 回被害を受けたときの組織としての予想損失額vは、組織毎に様々な状況が予想されるため、一般的な損失額を設定することが難しい。むしろ、vを可変パラメータとして扱い、各組織の状況に合わせて損失額を設定する方が広い用途に対応できると思われる。uとvが決まれば、パッチを 1 個適用しなかったときの予想損失額hが求まる。

$$h = uv \qquad \cdots (7)$$

4-9 汎用 OS のパッチ管理に関わる費用と効率性のシミュレーション

汎用 OS としての WindowsXP に関して、発売されてからこれまでにパッチ管理にかかった総費用TCを数式で表す。そして TC が最小になるときの解を求める。

総費用 $TC = h \times$（図 14 の網掛けの面積）
$+$（テスト工程にかかる費用）
$+$（テスト期間の短縮費用）　$\cdots (8)$

$$TC = h\left(\frac{KD}{2N} + DL - \frac{DL}{N}\right) + NS + NC(L_i) \qquad \cdots (9)$$

今、$C(L_0)=0$の場合（テスト期間の短縮を考慮しない場合）を考えると、

$$TC = h\left(\frac{KD}{2N} + DL - \frac{DL}{N}\right) + NS \quad \cdots (10)$$

となり、これを N について 1 階偏微分すると、

$$\frac{\partial TC}{\partial N} = \frac{hD}{2N^2}(2L - K) + S \quad \cdots (11)$$

さらに、N についての 2 階偏微分は、

$$\frac{\partial^2 TC}{\partial N^2} = \frac{hD}{N^3}(K - 2L) \quad \cdots (12)$$

となり、

$L < \frac{K}{2}$のとき、$\frac{\partial^2 TC}{\partial N^2} > 0$ $\cdots (13)$

$L > \frac{K}{2}$のとき、$\frac{\partial^2 TC}{\partial N^2} < 0$ $\cdots (14)$

となって、この関数の形状を議論できる。ここで、K=145（ヶ月）であり、テスト期間 L が 72.5 ヶ月を超えることは現実的ではないため、ここでは（13）式の成立を前提に議論を進めていくことにする。このとき、TC は下に凸の関数となるため、

$\frac{\partial TC}{\partial N} = 0$ のとき、TC は最小となり、

$\frac{\partial TC}{\partial N} = \frac{hD}{2N^2}(2L - K) + S = 0$ から N を求めると、

$$N = \sqrt{\frac{hD(K - 2L)}{2S}} \quad \cdots (15)$$

となる。

今、D と K は既知で、それぞれ 461 個と 145 ヶ月である。また、h を（7）式から求め、テスト期間Lと 1 回あたりの通常期間テストにかかる費用 S を、それぞれの組織内の生産制御システムに応じて設定すれば、N は解析的に求めることができる。もっとも、N はパッチ適用回数のため正の整数であることが必要とされ、（15）式で求めた値に最も近い整数、かつ TC を最小にする整数 N がこのときの解となる。さらに、T=K／N であることから、ここから T も求まる。

さて、ここまではテスト期間の短縮を考慮せず、テスト期間Lを一定と置いたときの、N と T を解析的に求める方法を提示した。次に、テスト期間の短縮を考慮したときの最適なテスト期間の導出方法について、数値例を用いながらシミュレーションにより導く方法を提示する。ここでのテスト期間の表記は、テスト期間の短縮を考慮したときのテスト期間表記L_iを用いる。**図 14** の網掛けの部分の面積が、組織に損失を与える可能性の大きさを表すものとしてそれを費用として捉えて金額化する。そして、その費用がテスト期間短縮費用とトレードオフの関係にあることから TC が最小となるようなL_iをシミュレーションによって求める。テスト期間L_i、並びに、テスト期間短縮費用$C(L_i)$の算出には、（2）～（5）の関係式を用いる。

4-10 本章の結果

4-10-1 予想損失の設定

シミュレーションを行うにあたり、生産制御システムが 1 回被害を受けたときの組織としての予想損失額 v を設定する。損失額は組織や個々のシステムにより異なり、一律に定まるものではないため、ここでは v=100,000（千円）とおいて、シミュレーションを行う。このとき、パッチを 1 個適用しなかったときの予想損失額 h は、（7）式より、

$$h = 4.20693 \times 10^{-4} \times 100{,}000 \approx 42.1(\text{千円}) \quad \cdots (16)$$

となる。

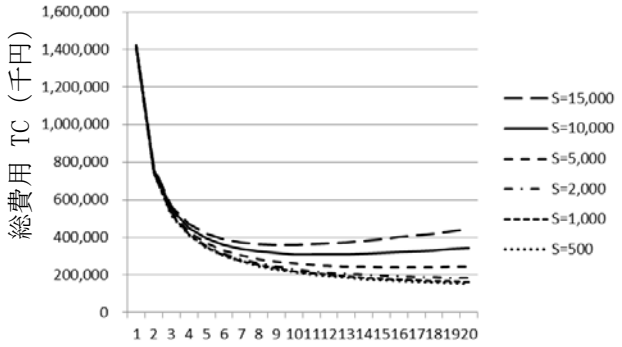
4-10-2 表、グラフ

テスト期間の短縮を考慮しない場合のシミュレーション結果を**図 16**、**図 17**、表 1 に示す。条件として、テスト期間Lを 4（ヶ月）に固定、テスト期間短縮費用$C(L_i)$を$i=0$の場合として 0（千円）に固定し、セキュ

リティ・パッチの適用回数Nやセキュリティ・パッチの適用周期Tを変化させながら、総費用TCが最小になるときのNとTを求める。このとき、テスト費用Sの大小によって総費用TCが変化するため、Sを 6 段階に変化させたときのNとTの値を表に示す。

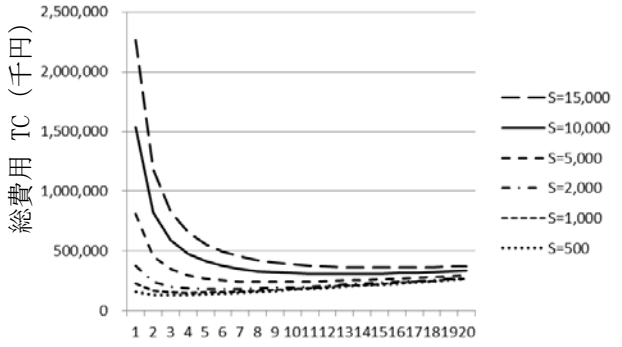
次に、テスト期間の短縮を考慮したシミュレーションを行うために、その元になる数値例を**表 2** に示す。この表の工程 j 毎の通常期間b_j、最小期間a_j、単位期間あたりの期間短縮費用c_jの値と、(2) ～ (5) の関係式から、**表 3** に示すテスト期間L_iとテスト期間短縮費用$C(L_i)$を求める。

さらに、**表 4** では、**表 3** で求めた数値を用いて、N=12（回）、T=12.1（ヶ月）、S=10,000（千円）の条件下での、テスト期間L_i毎の総費用TCを算出している。**図 18** はそのグラフである。



セキュリティ・パッチの適用回数N（回）

図 16　セキュリティ・パッチの適用回数Nと総費用TCの関係（$L=4, C(L_0)=0$の場合）（期間：2001 年 11 月～2013 年 12 月）



セキュリティ・パッチの適用周期T（ヶ月）

図 17　セキュリティ・パッチの適用周期Tと総費用TCの関係（$L=4, C(L_0)=0$の場合）（期間：2001 年 11 月～2013 年 12 月）

表 1　テスト費用Sとパッチの最適回数、最適周期（$L=4, C(L_0)=0$の場合）

テスト費用 S（千円）	15,000	10,000	5,000	2,000	1,000	500
セキュリティ・パッチの最適回数 N（回）	9	12	16	27	36	52
セキュリティ・パッチの最適周期 T（ヶ月）	16.1	12.1	9.1	5.4	4.0	2.8

表 2　テスト期間における工程別データ（数値例）

工程 j	通常期間bj（ヶ月）	最小期間aj（ヶ月）	短縮期間bj−aj（ヶ月）	期間短縮費用cj（千円/月）
1	0.8	0.3	0.5	800
2	0.8	0.3	0.5	900
3	1.2	0.6	0.6	2,000
4	1.2	0.6	0.6	3,000
合計	4.0	1.8	2.2	

表 3　テスト期間L_iと短縮費用$C(L_i)$

テスト期間の短縮パターン i	テスト期間 Li（ヶ月）	テスト期間短縮費用 C(Li)（千円）
0	4.0	0
1	3.5	400
2	3.0	850
3	2.4	2,050
4	1.8	3,850

表 4　テスト期間L_iと総費用TC（N=12（T=12.1）、S=10,000 の場合）

テスト期間 Li（ヶ月）	4.0	3.5	3.0	2.4	1.8
セキュリティ・パッチ適用回数 N（回）	12	12	12	12	12
セキュリティ・パッチ適用周期 T（ヶ月）	12.1	12.1	12.1	12.1	12.1
パッチ未適用期間のリスク（千円）①	188,420	179,524	170,629	159,955	149,280
テスト費用N回分 N*S（千円）②	120,000	120,000	120,000	120,000	120,000
期間短縮費用N回分 N*C(Li)（千円）③	0	4,800	10,200	24,600	46,200
総費用 TC（千円）（①＋②＋③）	308,420	304,324	300,829	304,555	315,480

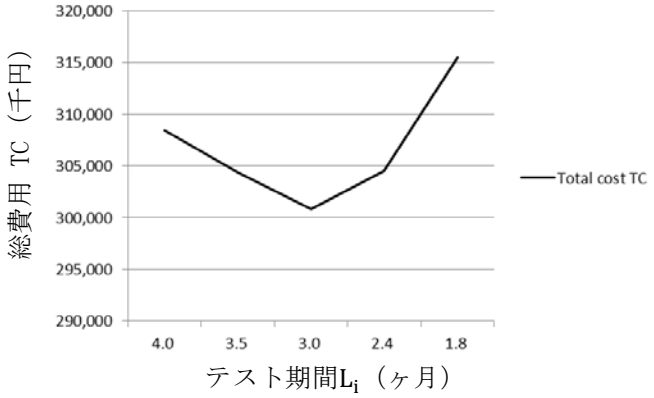


図 18　短縮費用$C(L_i)$を考慮したテスト期間L_iと総費用 TC の関係
（$N = 12, T = 12.1, S = 10{,}000$の場合）

4-11 本章の考察

最初に、テスト期間の短縮を考慮しない場合を考える。生産制御システムが 1 回被害を受けたときの予想損失額がわかっているとき、総費用TCは、テスト費用Sと、パッチの適用回数Nまたは適用周期Tによって決まる。**図 16** と**図 17** から、S が大きいほど TC が大きくなることがわかる。特に、N が大きくなるほど S の大小による TC の差異が顕著になることを**図 16** は示している。一方、T と TC の関係は，$T = K/N = 145/N$の関係式からわかるように、N とは逆の関係が成り立ち、T が大きくなるほど S の大小による TC の差異が小さくなることを**図 17** は示している。さらに、TC が最小になるときの N と T を求めると**表 1** のようになる。S が決まっているとき、パッチの適用周期をこの表に従って設定すれば、リスクを含めたパッチ管理に関する費用を最小化することができる。

次に、テスト期間の短縮を考慮する場合を考える。**表 2** の数値条件は、テストを 4 工程に分けた場合の各工程の特性値である。この表の工程 3 と 4 の単位期間あたりの期間短縮費用 c_jを大きくしているのは、それぞれシステムテストとオペレーションテストに該当し、この 2 工程が人が多く関わる工程と考え、人の投入に伴う期間短縮費用の増大を想定したためである。この数値条件に基づき、ここでは、N=12, S=10,000 の場合を対象に、テスト期間L_iと TC の関係を**図 18** のようにグラフ化した。グラフからテスト期間が 3.0 ヶ月のときに TC が最小値をとることがわかる。サイバー攻撃を受けるリスクの減少と期間短縮費用の増大が、このポイントでその総和が最小になる。この結果は数値条件に基づく一例であるが、本章の提案モデルから、セキュリティ・パッチ管理はテスト期間の短縮がポイントになり、それに予算を付けて短期間で精度の高いテストを実施することにより、サイバー攻撃から効率よく生産制御システムを守れることが確認できた。

5 クラウドサービス市場における情報セキュリティ監査モデル

5-1 概要

ネットワーク社会における IT の新しい利用形態として、クラウドコンピューティング（以下単にクラウドともいう）がある。IT 設備を自社で所有せず情報処理を外部に委託するこの形態は、可用性、拡張性、経済性の面で優位性があるといわれている反面、情報セキュリティ面が不安視されている。クラウドサービスの利用者が、情報処理をクラウド事業者に委託することにより、情報セキュリティガバナンスの主体が、互いに独立したクラウド利用者とクラウド事業者に分断されてしまう点にこの問題の本質がある。ガバナンスの主体が分かれると、クラウド事業者の情報セキュリティマネジメントがクラウド利用者側から見えにくくなり、両者の間に情報セキュリティに関する情報の非対称性が生まれる。この問題の解決策の一つとして、情報セキュリティ監査がある。

本章ではクラウド事業者とクラウド利用者の間の情報の非対称性に着目し、両者の関係をゲーム理論により考察を行い、クラウドサービス市場が健全に発展していくための情報セキュリティ監査が果たすべき役割について論述する。特にここでは保証型情報セキュリティ監査の 3 つの方式の中でも、クラウド利用者にとって比較的利用価値が高いと思われる利用者合意方式を取り上げ、監査制度が市場において信頼され、制度として有効に働くための条件を導き出す。利用者合意方式を対象としたのは、企業などのクラウド利用者がクラウド事業者に情報処理を委託する場合、委託先に期待する情報セキュリティ水準が明確である場合が多く、方式の目的を鑑みると、この方式がクラウド利用者のニーズに最も合致しやすいと考えたからである。

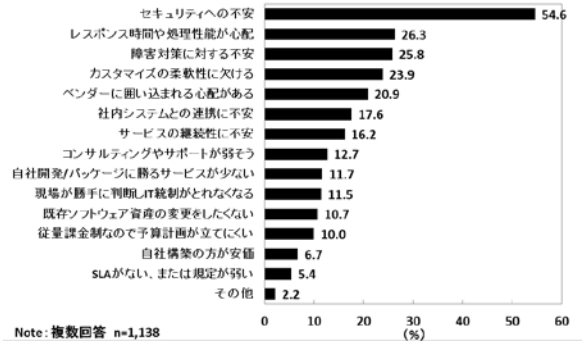
研究の流れとしては、監査制度として長い歴史を持つ、会計監査との比較において、情報セキュリティ監査がどうあるべきかを論じ、監査報酬、監査品質、情報セキュリティ対策の不確実性などについて、制度設計の観点から提案を行う。なお、本章では、クラウドサービスとしてはパブリッククラウドを想定し、クラウド利用者としては企業のような大口ユーザーを想定して議論を進めていく。

5-2 情報セキュリティ監査に関わる先行研究

情報セキュリティ監査の研究は、制度開始の初期段階ということもあり、監査の普及促進に向けた啓蒙的意味合いを持つ論文が多い。大木らは、日本セキュリティ監査協会のプロジェクトの中で、保証型情報セキュリティ監査の活用に向けた概念フレームワークを提示している[10]。伝統的な会計監査の分野では、Bolton and Dewatripont[11]が、プリンシパルを株主、エージェントを経営者として、経営者のモラルハザードや監査人との癒着の問題をモデル化している。さらに、King and Schwartz[12]は、監査の品質を考慮したモデルを提案し、加藤[13]は、そのモデルを拡張して、経営者と投資家が取引する際の会計監査の信頼性について、実証実験に基づいた研究を行っている。また、石井[14]は、情報セキュリティ監査人の法的責任について、公認会計士との比較により論じている。

5-3 クラウドコンピューティングの情報セキュリティ

クラウドコンピューティングでは、情報セキュリティに対する懸念がある。**図 19** に日本国内におけるパブリッククラウドサービスの利用阻害要因を、**図 20** にアメリカにおけるクラウド利用企業の課題を示す。



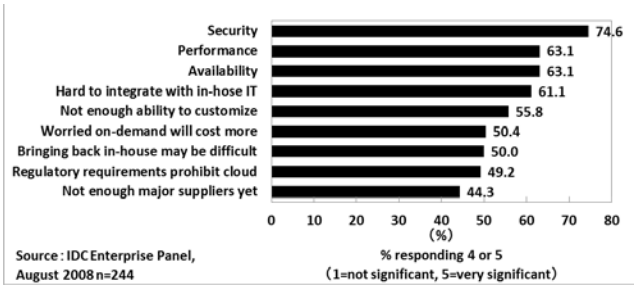


図 19　国内パブリッククラウドサービスの阻害要因
出典：IDC Japan (Jun. 2010) [15]

図 20　アメリカのクラウド利用企業の課題
調査：IDC Enterprise (Aug. 2008)
出典：Lee Badger, Tim Grance: Standards Acceleration to Jumpstart Adoption of Cloud Computing, NIST (May. 20, 2010) [16]

5-4 クラウドコンピューティングの情報セキュリティガバナンス

クラウドサービスを利用することは、情報システムの一部または全部を、自社所有から外部依存へとシフトさせることであり、ガバナンスの変化を伴う。**図 21** にそのフレームワークを示す。

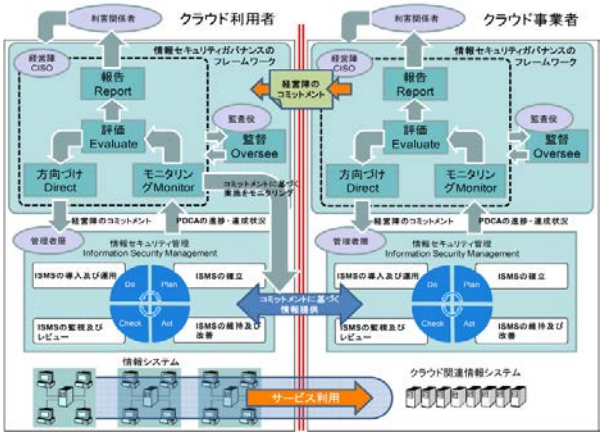


図 21　コミットメントに基づく情報セキュリティガバナンスのフレームワーク
出典：「クラウドサービス利用のための情報セキュリティマネジメントガイドライン」経済産業省[17]

5-5 情報セキュリティ監査

5-5-1 情報セキュリティ監査の三者関係

情報セキュリティ監査は、内部監査と外部監査に分けられる。本章では、特にクラウド事業者と利用者の関係について論じるため、外部監査を対象とする。**図 22** に後で述べる利用者合意方式の場合の、クラウドサービス市場における情報セキュリティ監査の三者関係を示す。

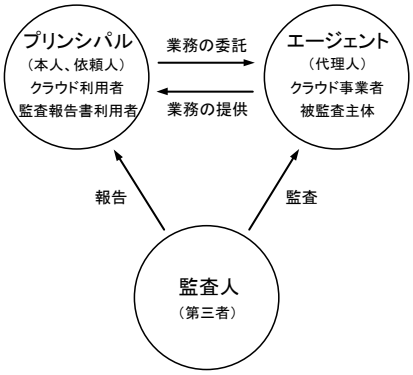


図 22　クラウドサービス市場における情報セキュリティ監査の三者関係

5-5-2 情報セキュリティ監査の基本的な視点

日本の情報セキュリティ監査は、2003 年の経済産業省の情報セキュリティ監査研究会報告書にその原点がある。基本的な視点として、情報資産に対するマネジメントを監査対象とすることがあげられている。ポイントは次の 2 点である[18]。

① 情報資産のセキュリティ確保

情報技術に関連するいわゆる情報システムのセキュリティだけではなく、より広く「情報資産」全体のセキュリティの確保を目的とする。

② 情報資産に対するリスクマネジメント

情報資産のセキュリティを確保するために、組織体としてリスクマネジメントが効果的に行われているかどうかを監査対象とする。従って、その時点における情報セキュリティの強度を対象とするのではない。情報セキュリティの確保を脅かすリスクは多様化かつ複雑化し、さらには日々変化していくものだからである。

さらに報告書では、多様なニーズに合わせて、保証型と助言型の 2 つの形態が定義されている[18]。

ⓐ保証型監査

監査の対象となる組織体の情報セキュリティに関するマネジメントや、マネジメントにおけるコントロールが監査手続を実施した限りにおいて適切である旨（又は不適切である旨）を伝達する監査の形態を、「保証型監査」と呼ぶ。 なお、この場合、「保証」といっても、結果としてインシデントが発生しないという絶対的な保証ではなく、一定の判断の尺度に従って監査手続を行った範囲における合理的な保証となることに留意が必要である。保証型監査は「監査報告書の利用者と約束した管理策を、被監査主体が約束通り実装し、運用しているか」について監査人が意見を表明するものである。

ⓑ助言型監査

監査の対象となる組織体の情報セキュリティに関するマネジメントや、マネジメントにおけるコントロールの改善を目的として、監査対象の情報セキュリティ上の問題点を検出し、必要に応じて当該検出事項に対応した改善提言を行う監査の形態を、「助言型監査」と呼ぶ。

報告書では、その他、情報セキュリティ管理基準や監査基準についても言及されている[18]。

5-5-3 保証型監査の概念フレームワーク

監査制度創設後、情報セキュリティ意識の高まりとともに監査の実施件数は増加している。もっとも、現段階では助言型監査がほとんどであり、保証型監査の実施件数はまだ少ない。しかし、クラウドコンピューティングが普及すると、クラウド事業者に情報処理を委託する企業にとって、委託先が期待通りの情報セキュリティ水準を確保しているかどうかが大きな関心事となる。ここで注意すべきことは、情報セキュリティ監査、特に保証型監査の場合、利用者の立場によってその目的や結果がもたらす効果が異なるということで

ある。一方、会計監査の場合、監査報告書の利用者はみな同じ立場であり区分する必要がない。そこで、保証型監査の概念フレームワークとして、日本セキュリティ監査協会では、社会的合意方式、利用者合意方式、被監査主体合意方式という利用者の立場によって、監査を 3 つに区分している[10]。

① 社会的合意方式
監査結果を広く社会全体の利害関係者に公表したい場合

② 利用者合意方式
報告書利用者である委託者が委託先に期待する水準が明確な場合で、委託先がその期待に応えていることについて保証を得たい場合

③ 被監査主体合意方式
受託者として求められる事項の遵守について保証を得たい場合

※上記の委託先、受託者、被監査主体は、クラウド事業者に該当する。一方、報告書利用者、委託者は、クラウド利用者に該当する。

この中で、クラウド利用者にとって最も利用価値が高いと思われる方式は、利用者合意方式であろう。クラウド利用者が、監査人と監査手続きを合意した上で、期待する水準の情報セキュリティマネジメントをクラウド事業者が行っているか否かについて、その保証を得たい場合に適用できるからである。本章ではこの後、保証型監査の利用者合意方式を対象に議論を進める。前述の情報セキュリティ監査の三者関係（**図 22**）は、利用者合意方式を前提とした関係図である。

5-6 情報セキュリティ監査の対象

情報セキュリティ監査は、**図 1** のフレームワークにおいて、どのように位置づけられるのであろうか。情報セキュリティ監査は、情報資産のセキュリティ確保を目的としている。その意味で情報資産が議論の中心に位置する。組織の情報セキュリティマネジメントを表すのは、**図 1** の右側の対策活動の部分であり、これが効果的に実施されているかどうかが情報資産のセキュリティを左右する。筆者らは、組織の対策活動によって決定論的に制御できるであろうこの部分が情報セキュリティ監査の対象であると認識している。一方、**図 1** の左側のセキュリティ事故の発生部分であるが、情報資産を脅かす脅威は、多様化かつ複雑化しており日々変化するものである。脆弱性が改善すると脅威に対する抵抗力が大きくなり、仮に脅威が一定であれば事故発生確率は小さくなる。しかし、日々変化する脅威に晒されている中で、事故発生確率を確実に小さくできるわけではなく、ましてや、ゼロにできるわけではない。筆者らは、確率論的事象であるこの部分は、情報セキュリティ監査の直接的な対象には含まれないと考えている。ただし、事故発生の情報が情報としてマネジメントに影響を与え、間接的に監査対象範囲に影響を及ぼすことは想定される。

保証型監査において保証とは、セキュリティ事故が発生しないという絶対的な保証ではなく、**5-5-2** で紹介したように、一定の判断の尺度に従って監査手続を行った範囲における合理的な保証である[18]。本章では、その保証の対象範囲は、**図 1** の確率論的事象の部分ではなく、対策と結果が、ある程度の因果関係を持って関係付けられる決定論的事象の部分であることを新たに提案する。

5-7 売り手と買い手の品質ゲーム

表 5 に売り手と買い手の品質ゲームの利得行列を示す。

表 5　売り手と買い手の品質ゲーム

			買い手	
			購買する	購買しない
			信頼	裏切り
売り手	高品質	信頼	5, 5	−5, 0
	低品質	裏切り	10,−5	0, 0

売り手と買い手の関係では、自分が生産した商品の品質についてよく知っている売り手は、高品質と偽って低品質の商品を買い手に売りつけ、**表 5** の左下のように利得 10 を獲得し大儲けができる。逆に高品質を信じて高い金を出してそれを買った買い手側は、騙されて不良品を手に入れることになるので、利得は同じ左下の−5 となる。買い手はこのような状況に陥ることを知ると、商品の購入には非常に消極的になる。たとえ売り手の中に高品質の商品を売る者があっても、買い手は**表 5** の右上で利得 0 とあるように購入しないで

あろう。すると、売り手にとって高品質な商品を作るために投入したコスト 5 は無駄になり売り手の利得は**表 5** の右上の－5 となる。**表 5** は非対称な利得行列である。これは、一方的囚人のジレンマ・ゲームと呼ばれている。

5-8 クラウドサービス市場における情報セキュリティ監査モデル

本章では、**表 5** の品質ゲームを拡張して、情報セキュリティ監査のモデル化を行う。なお、**表 5** の品質ゲームをより一般化してモデル化を行うために、利得行列の数字を変数に置き換え、**表 6** のような一般形にする。

表 6　クラウドセキュリティに関する事業者と利用者の品質ゲーム（一般形）

			クラウド利用者	
			利用する	利用しない
			信頼	裏切り
クラウド事業者	高セキュリティレベル	信頼	b−a, b−a	−a, 0
	低セキュリティレベル	裏切り	b, −a	0, 0

＜クラウド事業者＞
・努力する　：　コストa
　　→結果として高セキュリティレベルになる
・努力しない　：　コスト 0
　　→結果として低セキュリティレベルになる
＜クラウド利用者＞
・クラウドサービスを利用する　：　購入代金b
・クラウドサービスを利用しない　：　購入代金 0
＜クラウドサービスの価値＞
・高セキュリティレベル　：　価値$2b-a$
・低セキュリティレベル　：　価値$b-a$

≪使用記号≫
a　：クラウド事業者の努力のコスト（a＞0）
b　：クラウド事業者の報酬（b＞0、b＞a）
α　：クラウド事業者の意図通りのことがセキュリティレベルに反映される確率 $(1/2 \leqq \alpha \leqq 1)$
β　：監査人がクラウド事業者のサービスのセキュリティ品質を正しく報告する確率 $(1/2 \leqq \beta \leqq 1)$
γ　：監査報酬をクラウド事業者が負担する割合$(0 \leqq \gamma \leqq 1)$
C　：監査報酬 $(0 \leqq C \leqq (b-a)/2)$
Π_i：クラウド事業者の期待利得

$$i = \begin{cases} 1\cdots\text{クラウド事業者が努力する場合} \\ 2\cdots\text{クラウド事業者が努力しない場合} \end{cases}$$

※「クラウド事業者が努力する」とは、事業者自身が提供するクラウドサービスに関して、その情報セキュリティレベルを引き上げるための対策活動を行うことを指す。
※「クラウド事業者の意図通りのことがセキュリティレベルに反映される」とは、事業者が努力すれば、自身のサービスが高セキュリティレベルになり、事業者が努力しなければ低セキュリティレベルになることを指す。一方、αで表されるようなノイズの影響があると、事業者の意図通りのことが、セキュリティレベル

に反映されないこともある。すなわち、この場合は、事業者が努力したにもかかわらず、サービスが低セキュリティレベルになったり、事業者が努力しなかったにもかかわらず、偶然にも高セキュリティレベルになることもある。このようなケースを本研究では考慮に入れている。

5-9 会計監査の報酬制度に準じたモデル

ここでは、加藤[13]の会計監査のモデルを基礎としてモデル化を行う。まず、会計監査に準じた場合の監査報酬の流れを**図 23** に示す。仮に、プリンシパルを株主、エージェントを経営者とした場合、この三者関係は会計監査に相当し、被監査主体が監査人に対して監査報酬の全額を支払う形になる。

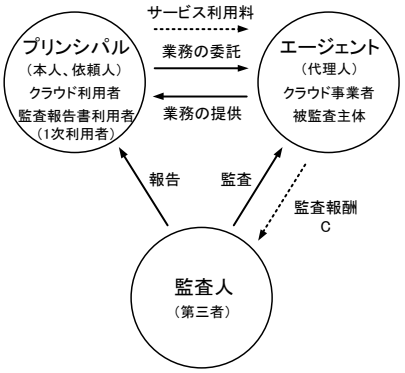


図 23　会計監査に準じた監査報酬の流れ

5-10 期待利得

図 23 の監査報酬の流れを前提にして、**図 24** のような展開形ゲームを考える。クラウド事業者と利用者の全ての戦略と利得はこの図に示されている。

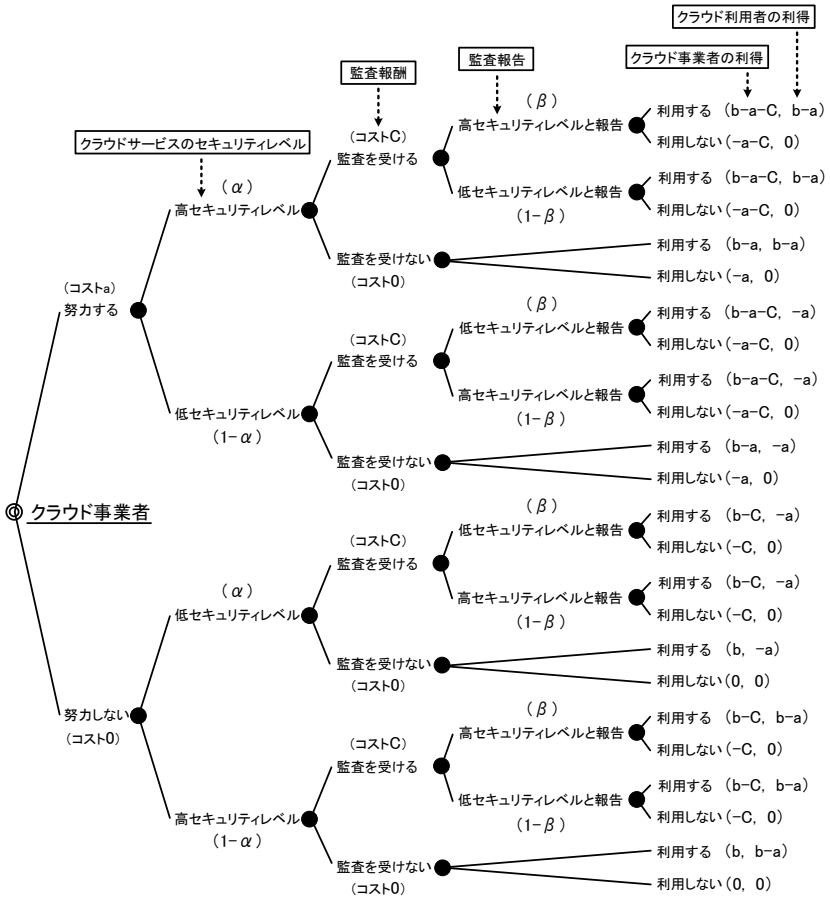


図 24　セキュリティ品質と監査精度を考慮したクラウド事業者と利用者の選択可能な戦略

＜ゲーム理論による数式展開は省略する。＞

5-11 監査報酬の流れに関する新たな可能性

前項では、会計監査の報酬の流れに沿った、被監査主体から監査人に対して報酬が支払われるモデルについて検討してきた。しかし、監査人の独立性の問題を考慮すると、会計監査に準じた報酬の流れとは一線を画した報酬制度が必要であると筆者らは考えている。ここでは、そのための新たな制度提案を行う。具体的には、**図 25** に示すように、監査人が報酬をクラウド事業者と利用者の両方から受け取る可能性を設定し、これに基づいて、まず市場において監査が信頼を得るための条件を検討する。

図 25 の監査人が受け取る報酬の総額は、これまでと同じCとし、クラウド事業者が負担する割合を$\gamma(0 \leqq \gamma \leqq 1)$、クラウド利用者が負担する割合を$1-\gamma$とする。

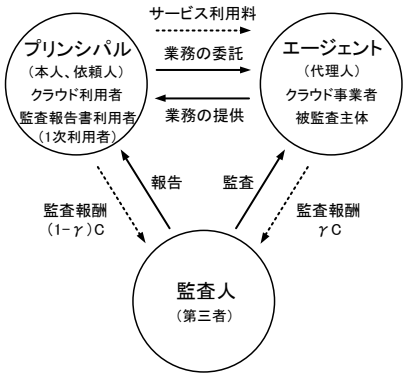


図 25　監査報酬の流れに関する新たな可能性

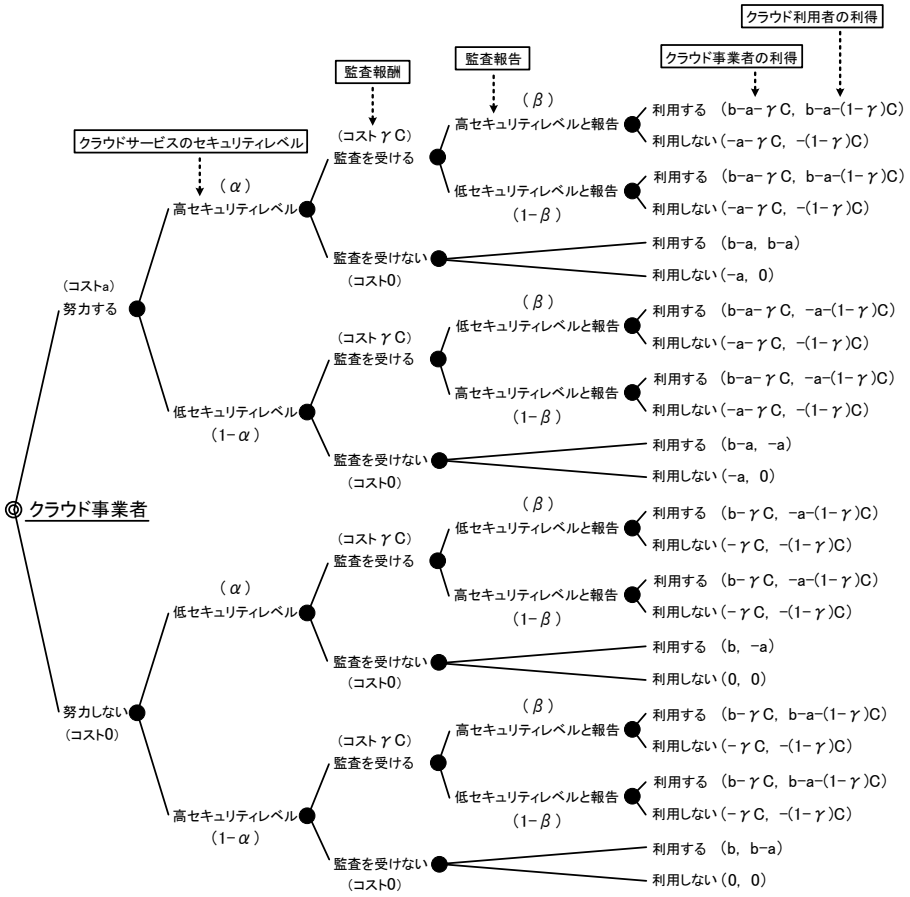


図 26　監査報酬の流れを変更した場合のクラウド事業者と利用者の選択可能な戦略

＜ゲーム理論による数式展開は省略する。＞

5-12 監査人の独立性とγの値

監査人の経済的利害関係は、監査人の独立性に影響を及ぼす。会計監査においては、制度上、誰が監査人を雇い又は解雇するかが、監査人の独立性に大きな影響を及ぼし、その意味で、被監査主体が監査人の顧客となる現在の監査制度には問題があることが指摘されている。さらに、投資ファンドにおいて投資家による監査人の選任が、監査人の独立性違反を著しく減少させるとも述べている。これらを情報セキュリティ監査に置き換えてみると、クラウド利用者による監査人の選任が、監査人の独立性確保に寄与することを意味している。

5-11 では、情報セキュリティ監査がクラウドサービス市場で信頼されるための条件を探索するため、監査人が報酬をクラウド事業者と利用者の両方から受け取る可能性について検討し、γの値を$0 \leqq \gamma \leqq 1$の連続量として扱ってきた。しかし、監査人の独立性の議論では、監査人が誰に雇われ誰に解雇されるかが焦点となる。このときのγの値は、監査人がクラウド事業者に雇われるか($\gamma = 1$)、クラウド利用者に雇われるか($\gamma = 0$)のどちらかである。以下では、$\gamma = 1$と0の 2 パターンについて議論する。

5-13 γ = 1と0 の比較

図 25 の形態では、$\gamma = 1$のとき、監査人はクラウド事業者に雇われ、$\gamma = 0$のとき、監査人はクラウド利用者に雇われる。

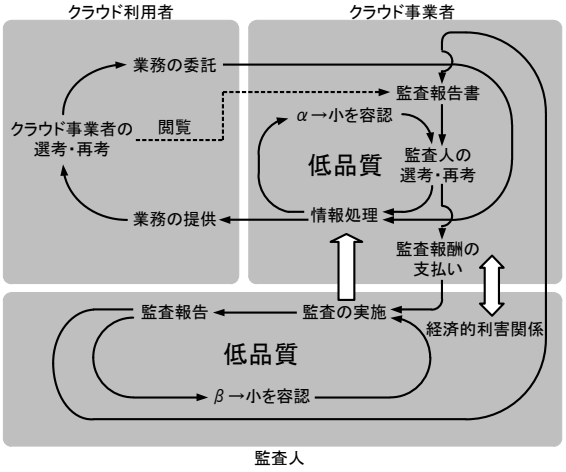


図 27　γ = 1のときの業務の流れ

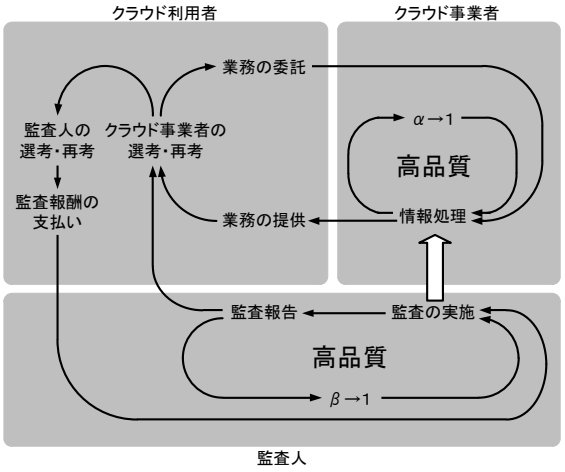


図 28　γ = 0のときの業務の流れ

図 27 のγ = 1の状態は、監査人が被監査主体（クラウド事業者）から監査報酬の全額を受け取るという、会計監査と同じ状態である。この状態は、監査人とクラウド事業者にとって、α、βが小さい、すなわち、低品質な状態であっても監査の信頼は確保できるという居心地のよい状態である。一方、クラウド利用者にとって、これは、監査人と被監査主体の癒着という面で不安を抱いてしまう状態である。従って、この状態が成立するのは、クラウド利用者がそれを容認できる場合に限られ、寛大なクラウド利用者の理解の下で、ぬるま湯の三者関係が構築され、品質の改善が停滞することが懸念される。保証型情報セキュリティ監査の利用者合意方式の報酬の流れとして、$\gamma = 1$の状態は、特定の 1 次利用者、並びにクラウドサービス市場にとって、必ずしも良い監査形態ではないと推測する。

図 28 のγ = 0の状態は、監査人がクラウド利用者から監査報酬の全額を受け取るという状態である。この場合、監査がシグナルとして信頼を得るには、監査人とクラウド事業者に、$\alpha = 1$、$\beta = 1$という完璧な条件が突き付けられる。クラウド利用者も監査報酬の全額を負担するわけで、監査人には高品質な監査を要求するであろう。監査人とクラウド事業者の関係も、もはや、ぬるま湯につかっている状態ではなくなり、互いに質の高さを競い合う厳しい関係になると予想できる。保証型情報セキュリティ監査の利用者合意方式の報酬の流れとして、$\gamma = 0$の状態は、質の高い監査市場、並びに質の高いクラウドサービス市場を創出する監査形態となる。

$\gamma = 1$と0はともに、努力するクラウド事業者を見分けるシグナルという点では有効に働くが、クラウドサービス市場に及ぼす影響という点では両者は異なるものとなる。$\gamma = 0$の方が、監査品質、サービス品質の面で、よりレベルの高い良い状態へと市場全体を向かわせるのである。

5-14 ISMS 適合性評価制度との関係

情報セキュリティ監査制度と ISMS 適合性評価制度の役割分担があいまいであるとの指摘がある。$\gamma = 1$の状態で考えると、クラウド事業者が監査人に対して監査を依頼し、その報酬を監査人に全額支払う形態は、ISMS 認証を取得したいクラウド事業者が審査機関に対して審査を依頼し、その費用を審査機関に全額支払う形態と、金銭の流れとしては類似している。この場合、情報セキュリティ監査制度と ISMS 適合性評価制度の、クラウド事業者を取り巻く利害関係の構図は同じである。

一方、$\gamma = 0$の状態では、両者の利害関係の構図は異なったものになる。この場合の情報セキュリティ監査制度の状態は、監査人がクラウド利用者から依頼を受け、クラウド事業者に対して厳しくかつ精度良く監査をし、その結果をクラウド利用者に報告する形となる。監査人は利用者側の立場に立ち、事業者側の立場に立つ ISMS の審査機関とは、その構図上、一線を画することになる。この場合、監査人はクラウド利用者のために仕事をし、審査機関はクラウド事業者のために仕事をする。$\gamma = 0$では、情報セキュリティ監査制度と ISMS 適合性評価制度は、明確に異なる役割を担うことになるのである。

6 おわりに

本研究では、情報セキュリティの経営分野に軸足を置き、組織として情報資産のセキュリティをいかに確保するかについて、企業社会で発生する情報セキュリティ事象をモデル化することにより、マネジメント上の知見を導いた。中でも、社会科学的事象を扱う際に問題となってきた実験的環境の構築方法、生産制御システムのセキュリティ、クラウドセキュリティにおける監査の役割などについて、その解決策を提示してきた。そして、構築したモデルから次の成果を得た。

① 企業における情報セキュリティのリスク分析について、マルチエージェント・シミュレーションを用いた実験的方法により、情報セキュリティ対策とその効果の関係を導いた。
② 生産制御システムのサイバー攻撃に関して、システムを攻撃から守るためのソフトウェア対策について、最適なセキュリティ・パッチの適用方法を提案した。
③ クラウドサービス市場におけるサービスのセキュリティ品質について、事業者と利用者の間の情報の非対称性に着目し、ゲーム理論によりモデル化を行い、それを解消するための情報セキュリティ監査が制度として有効に働く条件を導いた。

本研究では、情報セキュリティマネジメントの手法を抽象化かつ単純化し、様々な要因が絡む社会科学的事象に対して、あくまでも限定した条件下ではあるが、できる限り事象の本質を捉えるべく、そのモデル化を試みた。これにより、先行研究では実現されてこなかった、企業で発生している情報セキュリティ問題への対応策を導くための実験的アプローチを提案することができた。さらに、生産制御システムへのサーバー攻撃に対する防御策に関しては、IoT（Internet of Things）の時代にも生かされる対策であると考えている。情報セキュリティ監査制度については、本研究の提案を国の制度に取り入れることができれば、企業社会における信頼関係の構築に貢献できるものと考える。

今後の課題としては、次のことがあげられる。

A) 本研究では、情報セキュリティマネジメントを比較的単純なマルチエージェントモデルにより記述して事故の防御策等を提示したが、実際の組織では、その実施を妨げる方向に働くノイズの存在があり、これが単純な構造で記述される問題をより難しいものにしている。より現実に近いモデルにするために、セクショナリズム、コミュニケーションロス、セキュリティ対策の煩わしさなどの、ノイズを考慮したモデル構築を行う。
B) クラウドコンピューティングの普及とともに情報資産の管理が自社の手を離れつつあることから、その対策の必要性に迫られている。本研究のマルチエージェントによるシミュレーションモデルを拡張し、クラウド上に存在する情報資産のセキュリティ確保について、その対策と効果を記述するモデル構築を行う。

C) 本研究では、ゲーム理論によるアプローチにより、監査制度が有効に働くための条件を導いているが、実際にその制度を利用するのは人間であることから、理論による制度設計だけでなく、人間の感覚を制度の改善に取り入れることも重要である。そのための方法として、現在の理論研究に被験者実験を取り入れて、実験経済学へと研究を発展させることが有効であると考えられる。

本研究の成果が今後の情報セキュリティマネジメント研究の発展に寄与するものになれば幸いである。

【参考文献】

[1] 畠中伸敏編著:「情報セキュリティのためのリスク分析・評価 第 2 版」,日科技連(2008)
[2] 川中孝章, 六川修一,“情報セキュリティにおける脅威-脆弱性-対策に関する構造分析―決定論的事象と確率論的事象の二重構造―”,日本経営システム学会誌,Vol.28,No.2, pp.149-157(2011)
[3] 川中孝章, 六川修一,“マルチエージェントによる情報セキュリティの脅威-脆弱性モデル”,日本経営システム学会誌,Vol.28,No.1,pp.15-25(2011)
[4] 経済産業省:「情報処理実態調査」,http://www. meti.go.jp/statistics/zyo/zyouhou/(Jan.2011)
[5] 宮地利雄,“組織・企業の制御システムを守る”,電気学会誌,Vol.132,No.6,pp.354-358(2012)
[6] JPCERT コーディネーションセンター:国内制御システムにおける汎用通信プロトコルの利用状況およびセキュリティへの取組み状況に関する調査,(2008)
[7] Microsoft Security Bulletins:http://technet.microsoft. com/en-us/security/bulletin (2013.8.9)
[8] 情報処理推進機構:2011 年度情報セキュリティ事象被害状況調査－報告書－,pp.51-80(2012),http://www. ipa.go.jp/files/000014171.pdf
[9] Project Management for Construction, Advanced Scheduling Techniques : http://pmbook.ce.cmu.edu/(2013.10.8)
[10] 大木栄二郎,“保証型情報セキュリティ監査による個人情報保護の信頼醸成”,監査研究,Vol.33,No.3,pp.1-8(2007)
[11]P. Bolton, M. Dewatripont,「Contract Theory」,MIT Press,pp.338-342(2005)
[12]King, R.R., R. Schwartz,“Planning Assurance Services”,Auditing: A Journal of Practice & Theory, Vol.17, Supplement,pp.9-36(1998)
[13]加藤達彦,「監査制度デザイン論」,森山書店,pp.29-48(2005)
[14]石井夏生利,“情報セキュリティ監査人の責任”,九州国際大学法学論集,Vol.14,No.3,pp.264-235(2008)
[15]「国内クラウドサービス市場ユーザー動向調査結果を発表」,IDC Japan, 2010 年 6 月 3 日, http://www.idcjapan.co.jp/Press/Current/2010603Apr.html,(2010.6.8)
[16]Lee Badger, Tim Grance, ”NIST Standards Acceleration to Jumpstart Adoption of Cloud Computing (SAJACC) ”,May.20,2010,http:// www.nist.gov/itl/cloud/upload/nist_cloud_computing_forum-badger_grance.pdf,(2011.6.23)
[17]経済産業省,「クラウドサービス利用のための情報セキュリティマネジメントガイドライン」,2011 年 4 月 1 日, http://www.meti.go.jp/press/2011/04/20110401001/20110401001.html,(2011.6.25)
[18]経済産業省,「情報セキュリティ監査研究会報告書」,2003 年 3 月 26 日,http://www.meti.go.jp/policy/netsecurity/downloadfiles/IS_Audit_Report.pdf,(2011.8.4)

〈発　表　資　料〉

題　　名	掲載誌・学会名等	発表年月
企業組織における情報セキュリティマネジメントに関する研究	第48回日本経営システム学会講演論文集,pp.146-149	2012年6月3日
クラウドサービス市場における情報セキュリティ監査のゲーム理論的考察（平成24年度日本セキュリティ・マネジメント学会論文賞受賞）	日本セキュリティ・マネジメント学会誌,Vol.26,No.2,pp.3-23	2012年9月25日
記憶媒体の切り替えを考慮した情報の長期保存に関する研究	第50回日本経営システム学会講演論文集,pp.216- 219	2013年6月2日
企業における情報セキュリティのリスク分析に関する一考察	日本経営システム学会誌, Vol.30,No.1,pp.15-26	2013年7月15日
Information Sharing and Cost Reduction in Supply Chain Network	The Proceedings of the 9th Korea-Japan Workshop & the 3rd IWASM, pp.56-64	2013年8月24日
生産制御システムへのサイバー攻撃におけるソフトウェア対策に関する研究	第5回横幹連合コンファレンス論文集,pp.301-308	2013年12月21日
Software measure in cyber-attacks on production control system	Computers & Industrial Engineering,Vol.76,pp.378-386	2014年8月24日
Long-term Digital Storage by Switching Storage Medium	International Journal of the Japan Association for Management Systems,Vol.6,pp.15-24	2014年12月19日