2006－CSEC－33（2）
2006／5／12

分類された情報セキュリティ対策に依存する脅威発生率を導入したリスクアセスメントモデル

山口高康† 青野 博† 本郷節之† 松浦幹太††

† NTT ドコモ ネットワークマネジメント開発部 〒239-8536 神奈川県横須賀市光の丘 3-5

†† 東京大学 生産技術研究所 〒153-8505 目黒区駒場 4-6-1

E-mail: †{yamaguchita, aonoh, hongos}@nttdocomo.co.jp, ††kanta@iis.u-tokyo.ac.jp

あらまし リスクアセスメントに用いられる脅威発生率は、投資によって変化し、最適投資に影響を与える。しかし、従来のシステムセキュリティ設計手法では、ヒューリスティックに設定した脅威発生率を用いて事故率を求め、その事故率を用いて、複数の設計案の候補の中から見込み残存資産が最も多くなる設計案を選び出すという方法がとられていた。そこで、本研究では、投資後の脅威発生率を反映して、セキュリティに対する最適投資を調節する手法を提案する。本稿では、提案手法の有効性を調べるために、設計事例と事故率の統計データに基づいて、事故率レベルの低い設計案を選択するシミュレーションを行った。その結果、ある条件の下に限られるが、提案手法によって見込み残存資産がより多くなる設計案を選択することができる傾向があることを示した。

キーワード リスクアセスメント、見込み残存資産、事故率、脅威発生率

Risk Assessment Model using Threat Probability depending on Classified Information Security Measures

Takayasu YAMAGUCHI†, Hiroshi AONO†, Sadayuki HONGO†, Kanta MATSUURA††

† NTT DoCoMo, Inc., Network Management Development Department, 3-5 Hikarino-oka, Yokosuka-shi, Kanagawa, 239-8536, JAPAN

†† The University of Tokyo, Institute of Industrial Science, 4-6-1 Komaba, Meguro-ku, Tokyo, 153-8505, JAPAN

E-mail: †{yamaguchita, aonoh, hongos}@nttdocomo.co.jp, ††kanta@iis.u-tokyo.ac.jp

Abstract Threat probability used for risk assessment changes with investment and affects the optimal investment. However, in the conventional technique for system-security design, the incident probability is calculated using an investment-independent heuristic value of the threat probability. Based on the incident probability, the best design that maximizes the expected net benefit is selected out of a certain but limited number of candidates. In fear of the limitation of this heuristics, we propose a technique for a more sophisticated optimization of the investment by considering an investment-dependent threat probability. The technique we propose is evaluated by computer simulation whose setup is based on an actual survey of Japanese industry. In the simulation, we choose the design with the lowest level of the incident probability, and see if the choice is consistent with the best one regarding the expected net benefit. The simulation results show that our technique gives better consistency in comparison with the conventional approach of using the investment-independent value of the threat probability.

Keyword Risk assessment, Expected net benefit, Incident probability, Threat Probability

1. はじめに

近年、情報サービスに対するニーズは年々高まっている。一方で、情報サービスの提供にかかる企業の負担は、年々増加している。その負担増の主な原因として考えられるものに、「情報システムの安全性保証の困難」と「情報を取り扱う企業の責任の増加」が挙げられる。提供する情報サービスの量や質を高めようとすれば、情報システムは複雑な構成になる。しかし、複数の情報機器で構成した情報システムは、たとえ多額の投資を行ったとしても、その安全性を保証することが困難である。個人情報保護法が施行され、情報を取り扱う企業の責任は増加の一途を辿っている。情報を取り扱う企業が今後も存続していくためには、情報システムの安全性保証と、情報を取り扱う企業の責任を適切にマネジメントすることが必要不可欠である。

しかし、セキュリティのマネジメントは、経験に頼る部分が大きく、選択されたセキュリティ対策の妥当性などを、客観的に示すことは困難である。「情報システム設計におけるセキュリティ対策」の選択は、セキュリティポリシ策定、リスクアセスメント、セキュリティ対策基準の策定、セキュリティ対策の選択という手順で行われるのが一般的である。セキュリティ対策基準の策定に用いる、リスクアセスメントについては、ISO/IEC TR13335 などでガイドラインが示されている。しかし、リスクアセスメントについては、数学的算出手法で定式化する研究が行われ始めた段階である。

2. リスクアセスメント

2.1. 目的

情報を取り扱う企業のセキュリティマネジメントにおいて、リスクアセスメントを行い、企業経営における予算の範囲内で最適な選択肢を選び取っていくことは、重要な課題である。この課題を解決するためには、何を持って最適な選択肢とするかということと、企業が選ぶことができる選択肢とは何かということから、明らかにしていかなければならない。

選択肢を判断する基準としては、情報システムの堅牢さや運用のしやすさなども考えられる。しかし、経済的な面から選択肢の優劣を比較較しやすいことから、選択肢を判断する基準としては金額が適している。企

業の選択範囲としては、現実的には、情報システムはいかなる設計でも可能という場合は少ない。実際のプロジェクトでは、「さまざまな準備作業を経て、候補として出されてきた有限個数の設計案から１つを選択する」という形態が自然である。

そこで、本稿では、図 1 に示すように、企業が選ぶことができるシステムのセキュリティ設計案の選択肢の中から、見込み残存資産を最大にする選択肢を選び出すことができる、システムセキュリティ設計技術の実現を目的とする。

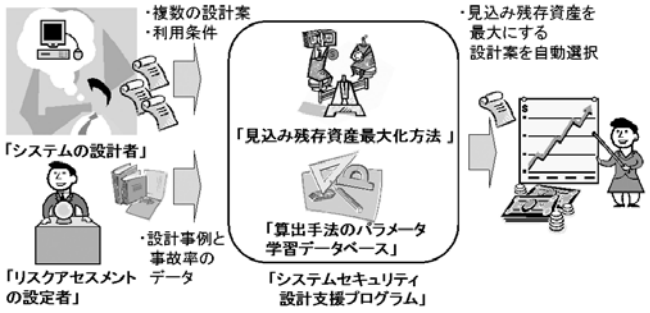

図 1 システムセキュリティ設計技術の利用イメージ

システムの設計者は、これからシステムを設計しようとする者である。リスクアセスメントの設定者は、当該システムの設計を補助する者である。両者の役割は同じ人物が行っても構わない。システムセキュリティ設計支援プログラムは、見込み残存資産最大化方法によって、システムの設計者が入力する複数の設計案と利用条件を元に、見込み残存資産を最大にする設計案を選び出す。システムセキュリティ設計支援プログラムは、算出手法のパラメータ学習データベースによって、リスクアセスメントの設定者が入力する設計事例と事故率のデータから統計量を算出して、見込み残存資産最大化方法が必要とするパラメータを事前に設定する。

2.2. 関連研究

文献[1]のゴードンの研究では、セキュリティに対する投資効果の定量化が試みられており、最適投資のモデルが提案されている。文献[2]の松浦の研究では、ゴードンのモデルに保険を取り入れたモデルが提案されている。文献[3]と文献[4]は、情報セキュリティと経済学の関係を、実際の統計データを用いて明らかにしようとする取り組みが行われている。保険を含めたセキュリティマネジメントの全体の概念は、文献[5]で述べられている。文献[6]の中村の研究では、ゴードンのモデルを踏まえて、見込み残存資産を最大にする設計案を選択する手法が提案されている。

ゴードンの研究では、セキュリティ投資に関する効果を定量的に示すモデル（1 式）が提案されている。

ここで、ENBIS（Expected Net Benefits of Investment in information Security）はセキュリティ投資に対して期待できる効果から投資（金額）を除いた値、v は脆弱性、S は投資後の脆弱性、z は投資、t は脅威発生率、λは事故が生じた場合の被害額を表す。脆弱性とは、対策を講じる前のシステムに対して悪者が攻撃を試みた場合に、その攻撃が成功する条件付確率である。投資後の脆弱性とは、対策を講じたシステムに対して悪者が攻撃を試みた場合に、その攻撃が成功する条件付確率である。

$$ENBIS\ (z) = \left\{v - S_{(v,z)}\right\} t\,\lambda - z \quad \cdots\ (1)$$

このモデルを参考にして、見込み残存資産を算出しようとすると、計算過程において事故率に相当する値を算出する必要がある。そのため、見込み残存資産を正しく算出できるかどうかは、いかにこの事故率を正しく求められるかに拠っている。

ゴードンの研究では、事故率は、2 式に示すように投資後の脆弱性と脅威発生率の積により計算される。ここで、事故率を A で表す。

$$A = S_{(v,z)}^{I\ or\ II}\, t \quad \cdots\ (2)$$

投資後の脆弱性は脆弱性と投資により計算する。投資後の脆弱性を表す関数は、3 式および 4 式に示す二種類のクラスが提案されている。そこで、S に I または II を添え字とすることで、両者を区別する。αおよびγは、ゴードンの研究における投資後の脆弱性を表す関数の調整パラメータである。

$$S_{(v,z)}^{I} = \frac{v}{(\alpha z + 1)^{\gamma}} \quad \cdots\ (3),\quad S_{(v,z)}^{II} = v^{(\alpha z + 1)} \quad \cdots\ (4)$$

しかし、脆弱性の定量化の方法は不明であるので、脆弱性を正確に設定することは困難である。また、記録として残らない未遂の脅威を把握する方法は不明であるので、脅威発生率を正確に設定することも困難である。

中村の研究でも、事故率に相当する値は、5 式に示すように投資後の脆弱性と脅威発生率の積により計算される。ここで、脅威の種類を表すインデックスを j で表す。S には III を添え字とすることで、先述の投資後の脆弱性と区別する。

$$A_j = S_{j(R,M)}^{III}\, t_j \quad \cdots\ (5)$$

投資後の脆弱性に該当する項は、6 式に示すように、実施した対策項目と「脅威と対策の関係」により計算する。ここで、対策の種類の総数を K、対策の種類を表すインデックスを k、対策の実施項目を M、脅威と対策の関係を R で表す。R は J 行 K 列のマトリクスで

ある。R の個々の値は Rjk で表し、それぞれ 0～1 の値を取る。Rjk の値は k 番目の対策が、j 番目の脅威による攻撃の成功率をどれだけ減少させるかという確率の減少率を表す。

$$S^{III}_{j(R,M)} = \prod_{k=1}^{K}\left(1 - R_{jk} M_k\right) \quad \cdots (6)$$

しかし、脅威と対策の関係の設定については、設計者が、ヒューリスティックに設定するという方法が用いられている。投資後の脆弱性の値は、この脅威と対策の関係の値に左右される。

ゴードンと中村の研究の内容を踏まえると、事故率を正確に計算することが困難であることは、脅威発生率と投資後の脆弱性を、正確に設定することが困難であることに起因していると考えられる。

2.3. 従来の問題点の分析

文献[7]でも述べられているように、実際に行われているリスクのコントロールでは、対策に投資して、脆弱性や脅威発生率などを抑制している。最適投資を正しく算出する為には、まず、これらの「投資の効果を踏まえた脆弱性」と「投資の効果を踏まえた脅威発生率」を正しく算出しなければならない。しかし、中村らが適用したゴードンのモデルでは、投資による脅威発生率の抑制が表現されていない。

中村の手法では、モデルのパラメータである脅威発生率をヒューリスティックに設定したうえで、講じるべきセキュリティ対策を選択している。しかし、脅威発生率の設定次第で、最適投資は変化する。例えば、1 式のゴードンのモデルにおいて、投資後の脆弱性をクラスⅡの関数で表せば、ENBIS を最大にする投資 z*（最適投資）は、7 式となる。この 7 式はグラフにプロットすると、図 4 のようになる。

$$z^* = \frac{\ln\left[1/\left\{-\alpha v t \lambda \ln(v)\right\}\right]}{\alpha \ln(v)} \quad \cdots (7)$$

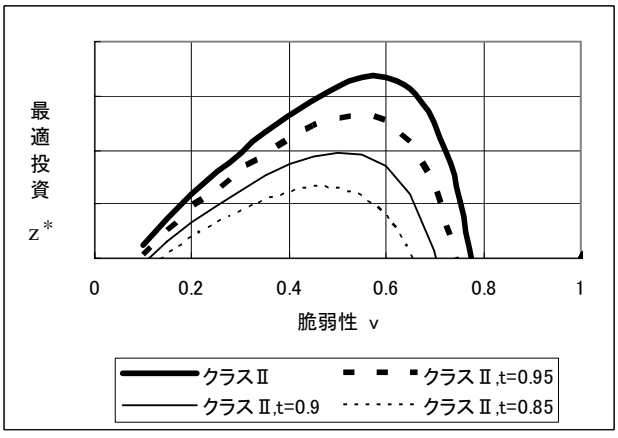

図 4 脆弱性と脅威発生率に応じた最適投資

図 4 のグラフでは、脅威発生率を小さくするにつれてグラフの頂上が左下へ移動している。このことは、脅威発生率の設定次第でシステムの脆弱性に応じた最適投資が変化すること、すなわち最適投資を行う上で選択すべき設計案が異なる可能性を示唆している。したがって、適切な設計案を選択するためには、脅威発生率を正しく設定することが必要になる。しかし、従来この脅威発生率の設定はヒューリスティックに行われていた。そして、この脅威発生率の正しい設定は、一般に困難な作業であった。

つまり、「投資による脅威発生率の抑制がモデルに反映されていないこと」と「脆弱性と脅威発生率のパラメータを、誰もが簡単に設定できないこと」が、従来手法における問題と言える。

3. 事故率の算出手法の提案

3.1. 前提条件

2.1 節で述べたシステムセキュリティ設計技術の利用イメージを踏まえて、前提条件を以下に示す。

「前提条件」

- **システムの設計者は、システムセキュリティ設計支援プログラムに、複数の設計案と利用条件とを入力する**
- **リスクアセスメントの設定者は、システムセキュリティ設計支援プログラムに、設計事例と事故率のデータを入力する**
- **設計案は、脅威が成功しないように講じる対策（対策費用を含む）と、脅威が成功してしまった場合に資産の減少を食い止めるように講じる保険（保険費用と補償額を含む）である**
- **利用条件は、資産と「資産と脅威の関係」に関する情報を含む**
- **投資後の脆弱性は、ゴードンの研究における脆弱性と投資により定められる関数である**

3.2. 要求条件とクリアすべき問題

2.1 節で述べたシステムセキュリティ設計技術の利用イメージを踏まえて、要求条件を以下に示す。

「要求条件」

- **システムのセキュリティ設計の複数の案の中から、見込み残存資産が最も多くなる設計案を選択する**

2.2 節の関連研究と、2.3 節の従来の問題点の分析を踏まえて、クリアすべき問題を以下に示す。

「クリアすべき問題」

- **投資による脅威発生率の抑制を、モデルに反映する**
- **脅威発生率と脆弱性のパラメータ設定を、より簡単にする**

3.3. 投資後の脅威発生率のモデル

我々は、投資後の脅威発生率を算出する際にセキュリティに対する投資を考慮し、事故率を算出する算出手法にそれを取り入れる一つの取り組みを行う。投資後の脅威発生率とは、対策を講じたシステムに対して

悪者が攻撃を試みる確率である。ここで、脅威発生率を抑制する投資を $z^{(t)}$、投資後の脅威の発生率を U、U を $z^{(t)}$で一階微分したものを Uz、U を $z^{(t)}$で二階微分したものを Uzz とする。投資後の脅威発生率の関数が満たすべき性質を以下に示す。

「投資後の脅威発生率の関数が満たすべき性質」

- **投資後の脅威発生率を表す関数は、少なくとも投資の増加に対して、減少する関数となる**（$Uz(t,z^{(t)})<0$）
- **システムが利用される状況において脅威が発生しなければ、投資の量に関わらず、投資後も脅威は発生しない**（$U(0,z^{(t)})=0$ for all z）
- **投資を行わなければ、脅威発生率は変わらない**（$U(t,0)=t$ for all t）
- **脅威発生率は 0 =< t =< 1 の値を取る**
- **最適投資を求めるために用いる関数であるので、投資後の脅威発生率は、下に凸の関数とする**（$Uzz(t,z^{(t)})>0$）

これらの条件を満足する関数の具体的な例としては、ゴードンの研究での投資後の脆弱性を算出する関数が該当する。そこで、本稿では先述したクラスⅡを真似て、8 式を投資後の脅威発生率の関数として用いる。

$$U_{(t,z^{(t)})} = t^{(\beta z^{(t)}+1)} \quad \cdots (8)$$

3.4. パラメータ設定

2.1 節で述べたシステムセキュリティ設計技術の利用イメージを踏まえて、モデルのパラメータ設定を行う。モデルのパラメータをΘとし、設計事例と事故率のデータを D で表す。事後確率 p(Θ| D)については、ベイズの定理から 9 式のような比例関係が得られる。ここで、左辺の確率を表すモデルは、これまでに述べた 4 式、8 式が該当する。また、モデルのパラメータΘは 4 式における v、8 式における t が該当する。

$$p(\Theta \mid D) = \frac{p(D \mid \Theta)p(\Theta)}{p(D)} \propto p(D \mid \Theta)p(\Theta) \cdots (9)$$

パラメータΘは、10 式に示すように、設計事例と事故率のデータを用いて 9 式の右辺を最大にする値とする。

$$\Theta_{MAP} = \arg\max_{\Theta} \{p(D \mid \Theta)p(\Theta)\} \quad \cdots (10)$$

3.5. 事故率の算出手法

3.3 節で述べた、投資後の脅威発生率を算出する関数を踏まえて、事故率（明らかに投資後の事故率であるが、用語の統一の為、以後も事故率と表す）を算出する手法について述べる。

設計案から、設計案の実施にかかる投資は、明らかである。設計者は、投資が「脅威発生の抑制に対する投資」と「防護に対する投資」のどちらであるかを分類して入力する。投資後の脆弱性は、設計者が入力した防護に対する投資より算出する。投資後の脅威発生率は、設計者が入力した脅威発生の抑制に対する投資より算出する。11 式に示すように、これら投資後の脅威発生率と投資後の脆弱性の積により、事故率を算出する。ここで、防護に対する投資を $z^{(v)}$で表す。

$$A = S_{(v,z^{(v)})} U_{(t,z^{(t)})} \quad \cdots (11)$$

我々が提案する事故率の算出手法を用いると、設計者は投資を分類して入力する手間がかかる。しかし、脅威発生率や脆弱性など、設定することが難しいパラメータの値を、設計者が設定する必要は無くなる。

4. 事故率レベルの算出手法の評価実験

4.1. 評価実験の目的

前章では、投資後の脅威発生率のモデルとモデルのパラメータ設定を踏まえて、事故率の算出手法を提案した。本章では、実データを用いた評価実験を行って、従来手法（2 式,クラスⅡ）と比較して提案手法（11 式）の有効性を示す。ここで示す有効性とは、提案手法が従来手法よりも「事故率レベルの低い設計案を選択する試行の回数が多いこと」である。

4.2. 評価実験に用いる実データ

提案手法の有効性を確認するため、我々は、セキュリティの投資に関するデータと、それぞれの投資を実施した場合に発生した事故率との対応が記載されている、「平成 15 年 情報処理実態調査の公開データ」を入手した。このデータは、経済産業省が行った民間事業者 9,500 社（有効データは 4,491 社）に対する、情報処理実態調査の結果である。

公開データにおいて、脅威となるセキュリティトラブルの原因は、9 種類が挙げられている。そこで、評価実験で想定する脅威は、これらと同じものとする。

公開データにおいて、対策となるセキュリティ対策は、12 種類が挙げられている。今回の評価実験では、「投資の額は、対策の策定率と強い相関がある」と考えられることから、対策の策定率を投資としてみなす。従来手法では、防護に対する投資の情報が必要である。提案手法では、脅威発生の抑制に対する投資と、防護に対する投資の情報が必要である。そこで、防護装置に分類されている「入退出管理、アクセス管理、ファイアウォールのセキュリティ対策策定率」を、防護に対する投資とみなす。監査体制に分類されている「監視ソフト、常時セキュリティ監視、外部定期的なセキュリティ監査、内部定期的なセキュリティ監査のセキュリティ対策策定率」を、脅威発生の抑制に対する投資とみなす。提案手法の評価では、合計 7 種類の対策のデータを用いる。

セキュリティ対策策定率と、それに対応するセキュリティトラブル発生確率のデータは、業種別に 27 種類が挙げられている。つまり、評価実験で用いるデータは、これまで述べた脅威、対策、業種の各マスタから、7 種類の対策の項目を持つ設計案のデータが 27 件と、9 種類の脅威に関する事故率のデータが 27 件となる。

なお、公開データでは、事故にあった企業の割合しか示されていないので、本評価実験で用いる事故率とは、企業が一度でも事故にあう割合とする。

4.3. 事故率のレベル分け

公開データでは、数千社のデータを 27 業種に纏めており、何パーセントの確率で、どれくらいの信頼度で事故が起こりそうかという議論を行うにはデータ数が少ない。

9 種類の脅威に関する事故率の平均値と分散値を求めると、それぞれの脅威ごとに、値が大きく異なる。各脅威で事故率の平均値や分散値が異なるということは、「事故が起こりやすい」とか「世の中の平均と同じくらい」とか「事故が起こりづらい」という事故率の値や範囲は、脅威ごとに異なるためだと考えられる。そこで、本稿での事故率の算出手法の評価実験では、事故率そのものを算出しない。世の中で起こっている事故率の平均値を基準にして、事故が起こりやすい、世の中の平均と同じくらい、事故が起こりづらいという事故率のレベルを算出する。データがより多い場合にはより詳細にレベル分けを検討する必要が出てくるが、今回は設計案が 27 件なので、事故率レベルを偏差値 45 未満（レベル 1 と呼ぶことにする）、偏差値 45 以上 55 未満（レベル 2）、偏差値 55 以上（レベル 3）の 3 段階に分けて考えることにする。

4.4. 提案手法を用いた事故率レベルの算出

提案手法である 11 式を元に、事故率レベルを推定する方法について述べる。

今回の評価に用いるデータには、複数の種類の脅威がある。それぞれの脅威ごとに、異なる事故率レベルを設定するので、11 式の各変数に、脅威の種類を表す添え字 j と、事故率レベルを表す添え字 c を付けて 12 式を得る。

$$A^{(c,j)} = S^{(c,j)}_{\left(v,z^{(v)}\right)} U^{(c,j)}_{\left(t,z^{(t)}\right)} \quad \cdots (12)$$

評価実験で用いるデータには、12 種類の対策の種類があるが、どの対策が、どの脆弱性やどの脅威発生率の抑制に対して、効果を持つのかを表すデータが無い。そこで、各対策は、各脆弱性と各脅威発生率の抑制に、均等に効果を持つと仮定する。事故率レベルが未知の設計案（$z^{(v)}$と $z^{(t)}$）の場合における、事故率レベルの推定値（$\hat{c}$）は、13 式で算出する。13 式で最大化する値は、12 式に 4 式と 8 式を代入して得られる。

$$\hat{c}^{(j)} = \arg\max_{c^{(j)}} \left[\prod_{k=1}^{K} \left\{ v_k^{(c,j)} \right\}^{\left(\alpha z_k^{(j,v)}+1\right)} \times \prod_{k=1}^{K} \left\{ t_k^{(c,j)} \right\}^{\left(\beta z_k^{(j,t)}+1\right)} \right] \cdots (13)$$

13 式における脅威発生率および脆弱性は、設計事例と事故率のデータを用いて 14 式で求める。14 式は、解を求めるために $\sum_{k=1}^{K} \theta_k = 1$ という条件をおき、10 式から導出する。評価実験で用いるデータには、27 種類の設計案があるので、設計案を示す番号を n、設計案の総数を N、調整パラメータを ϕ とする。脆弱性を算出する際には $\theta \rightarrow$v および $\phi \rightarrow \alpha$ という置換を行い、脅威の発生率を算出する際には $\theta \rightarrow$t および $\phi \rightarrow \beta$ という置換を行う。

$$\theta_k^{(c,j)} = \frac{\sum_{n=1}^{N^{(c,j,\theta)}} \left(\phi z_{k,n}^{(c,j,\theta)} + 1 \right) + 1}{\sum_{k=1}^{K} \sum_{n=1}^{N^{(c,j,\theta)}} \left(\phi z_{k,n}^{(c,j,\theta)} + 1 \right) + I} \quad \cdots (14)$$

なお、従来手法では、投資によって脅威発生率が変化しないので、13 式の大括弧内の下段の項を定数として、事故率レベルの算出を行う。本評価実験では、調整パラメータである α と β は、簡易のため 1 とする。

4.5. 提案手法の評価方法

4.4 節において、評価実験における事故率レベルの推定方法について具体的に述べた。本節では、提案手法が従来手法よりも事故率レベルの低い設計案を選択する試行の回数が多いことを示す評価方法について述べる。

本来ならば従来手法に比べて提案手法を用いることで、システムのセキュリティ設計の複数の案の中から、見込み残存資産が最も多くなる設計案を選択することができるようになることを示すべきである。しかし、これについては、さまざまな条件が想定されるため、適用すべき一般的な評価方法について、即座に見当をつけられない。そこで、評価実験を行う上で以下のような前提条件をおく。下記の評価実験の前提条件の下であれば、事故率レベルの低い設計案を選択することが、見込み残存資産が多くなる設計案を選択することになる。

「評価実験の前提条件」

- **各対策は、各脆弱性と各脅威発生率の抑制に、均等に効果を持つ**
- **各脅威によって被害にあう資産の額が等しい**
- **保険には加入しない**

計算機シミュレーションにより、従来手法と提案手法でシステムのセキュリティ設計の複数の案の中から、事故率レベルがより低くなる設計案を選び出すという試行を何度も繰り返す。提案手法が従来手法よりも事故率レベルの低い設計案を選択する試行の回数が多いことを示せれば、評価実験の前提条件の下で見込み残存資産が多くなる設計案を選択することができる傾向があることを示せる。

「評価実験の試行内容」

- **27 種類の設計案から、脅威レベルの異なる 2 種類の設計案をテストデータとして抜き出し、残りの 25 種類の設計案を学習データとする**
- **学習データで未知パラメータを推定する**
- **2 種類のテストデータの設計案について事故率レベルを推定する。「より事故率レベルが低いと推定した設計案」と「実データで、より事故率レベルが低かった設計案」が、一致する場合は試行が成功した（2 種類の設計案の中から、より事故率レベルが低くなる設計案を選択できた）とみなし、一致しない場合は試行が失敗したとみなす**

上記の試行では、公開データから取り出せるテストデータの全パターンを行う。試行が成功した回数を総試行回数で除した値を正解選択率とする。提案手法と従来手法で上記の試行を繰り返して、より正解選択率が高い手法が有効であると評価する。

4.6. 提案手法の評価結果

本節では、計算機シミュレーションにより、提案手法と従来手法で求めた正解選択率を比較する。評価実験の結果として、提案手法を用いたことによる、従来手法に対する正解選択率の変化を表 1 に示す。

表 1 提案手法による正解選択率の変化

番号	脅威	正解選択率の変化
1	システム内部の障害	+29%
2	整備的な障害	+12%
3	人為的な障害	－2%
4	外部事業者による障害	+23%
5	自然災害	－3%
6	物理的な不正アクセス	+20%
7	ﾈｯﾄﾜｰｸを通じた不正ｱｸｾｽ	+12%
8	ウィルスによる障害	+37%
9	その他	－28%

9 種類の脅威のうち 6 種類の脅威について、提案手法を用いる事によって正解選択率が向上した。この結果から、評価実験の前提条件の下であれば、提案手法が従来手法よりもシステムのセキュリティ設計の二つの案の中から、見込み残存資産がより多くなる設計案を選択することができる傾向があることを示した。

5. おわりに

本稿では、システムのセキュリティ設計の複数の案の中から、見込み残存資産が最も多くなる設計案を選択する方法について検討を行った。本検討において、投資後の脅威発生率のモデルとパラメータ設定を用いた事故率の算出手法を、新たに提案した。提案手法を用いれば、設計者が投資を分類して入力するだけで、パラメータを設定する困難から解放される。提案手法の有効性を確認するため、設計事例と事故率の統計データに基づいて、事故率レベルの低い設計案を選択する試行を行った。その結果、評価実験の前提条件の下に限られるが、提案手法はシステムのセキュリティ設計の二つの案の中から、見込み残存資産がより多くなる設計案を選択することができる傾向があることを示した。

6. 今後の課題

本研究について、今後の課題を以下に示す。

- 過去の統計データに基づいて、最適な設定案を選択するという手法の妥当性と適用範囲の検証
- 評価実験における前提条件の妥当性の検証
- 評価実験で用いた分析手法の体系化

文　献

[1]Lawrence A. Gordon, Martin P. Loeb, "The economics of information security investment", ACM Transactions on Information and System Security (TISSEC) archive, Vol. 5, No. 4, pp.438 - 457, Nov. 2002.

[2]松浦幹太, “情報セキュリティと経済学”, 2003 年暗号と情報セキュリティ・シンポジウム(SCIS2003), Vol.I, pp.475-480, Jan. 2003.

[3]Hideyuki Tanaka, Kanta Matsuura, "An Incentive Mechanism of Information Security Investment:An Empirical Study of e-Local Government in Japan", The 2004 Workshop on Information Security Research Supported by MEXT Grant-in-Aid Scientific Research on Priority Area "Informatics“, October 3rd, 2004.

[4]Wei Liu, Hideyuki Tanaka, Kanta Matsuuta, “Information Security Incidents and Countermeasures: An Empirical Analysis Based on an Enterprise Survey in Japan”, SCIS 2006, Jan. 2006

[5]Gordon, L. A., M. P. Loeb and T. Sohail, "A Framework for Using Insurance for Cyber Risk Management", Communications of the ACM, pp. 81-85, March 2003.

[6]中村逸一, 兵藤敏之, 曽我正和, 水野忠則, 西垣正勝, "セキュリティ対策選定の実用的な一手法の提案とその評価", 情報処理学会論文誌, vol.45, no.8, 2004 年 8 月.

[7]“リスクアセスメント調査報告書”, JASA, http://www.jasa.jp/about/seika2003.html