Information Processing Society of Japan

社団法人　情報処理学会　研究報告
IPSJ SIG Technical Report

2003－ＣＳＥＣ－22　(35)
2003／7／18

セキュリティ対策案選択問題のモデル化

兵藤 敏之[*1]　中村 逸一[*3]　西垣 正勝[*2]　曽我 正和[*4]

*1: 静岡大学大学院 情報学研究科　*2: 静岡大学 情報学部 〒432-8011 静岡県浜松市城北 3-5-1
*3: ㈱NTT データ セキュリティビジネスユニット　*4: 岩手県立大学 ソフトウェア情報学部

E-mail: *1,2: {cs8075,nisigaki}@cs.inf.shizuoka.ac.jp,
E-mail: *3: nakamuraitk@nttdata.co.jp, *4: soga@soft.iwate-pu.ac.jp

あらまし　近年，情報セキュリティポリシーを策定，運用する組織等が増えつつある．しかし，守るべき資産に対して最も効果的かつ効率的なセキュリティ対策を選択するための方法論は確立されていない．このため，現在の情報システム開発におけるセキュリティ対策案の選択は設計者や開発者の勘と経験に頼って行われていることがほとんどであり，また，選択されたセキュリティ対策案の妥当性を客観的に証明することもできないというのが現状である．本稿では，資産・脅威・対策案の関係をモデル化し，セキュリティ対策案選択問題を定式化することにより，対策案の最適な組み合わせを理論的に求める手法を導出する．本手法によれば，セキュリティ対策案選択問題は離散最適化問題として定式化される．

キーワード　情報セキュリティマネジメント，情報セキュリティポリシー，セキュリティ対策案選択問題，離散最適化問題

A modeling of security measure selection problem

Toshiyuki HYODO[*1]　Itsukazu NAKAMURA[*3]
Masakatsu NISHIGAKI[*2]　Masakazu SOGA[*4]

*1: Graduate school of Information, Shizuoka University
*2: Faculty of Information, Shizuoka University　3-5-1 Johoku, Hamamatsu, Shizuoka, 432-8011 Japan
*3: Security Business Division, NTT Data Corp.　*4: Faculty of Software and Information, Iwate Prefectural University

E-mail: *1,2: {cs8075,nisigaki}@cs.inf.shizuoka.ac.jp,
E-mail: *3: nakamuraitk@nttdata.co.jp, *4: soga@soft.iwate-pu.ac.jp

Abstract　Recently, information security management in many organizations is carried out based on a Information Security Policy. However, no effective method of selecting the optimum security measures has established yet. Hence, a security measures selection is now greatly dependent on the knowledge/experience of a system designer, and the objective evaluation of appropriateness of the selected security measures is impossible. To cope with the inconvenience, this paper shows a formulation of problem for selecting security measures.

Keyword　Information Security Management, Information Security Policy, Selection of Security Measures, Discrete Optimization Problem

NII-Electronic Library Service

Information Processing Society of Japan

1. はじめに

情報化社会も本格化し，ネットワーク環境および情報サービスが充実してくるにつれ，セキュリティインシデントは多発化，深刻化の一途をたどっている．この問題に対処するために，国内外で情報セキュリティ関連の法整備が進められるとともに，国際的なセキュリティ標準（ISO/IEC 17799[1]，ISO/IEC TR 13335[2]，ISO/IEC 15408[3]など）が策定されてきている．

コンピュータおよびネットワークは組織にとって必要不可欠なインフラとなっており，その上を各種の膨大な情報が駆け巡っている．今や，情報セキュリティマネジメントは各組織にとっての最重要課題の一つと認識されてきている[4]．また，ユーザから見た場合，自分の情報を預けている企業が情報に対する十分な管理体制を用意しているか否かは，その企業のサービスを安心して受ける上で重要である．

国内では ISMS(情報セキュリティマネジメントシステム)[5]の認証制度があり，これを取得する組織が次第に増えつつある状況である[6]．また，ISMS 認証の取得にまでは至っていないものの，情報セキュリティポリシーを策定して，ポリシーに沿ってネットワークやシステムを構築し，運用管理を行なう組織が多くなってきている．

しかし，情報セキュリティポリシーを策定し，それを現実のシステムやネットワークの構成および運用管理体制に展開するためには，システム全体を網羅する視点で検討し，守るべき資産に対して最も効果的かつ効率的な対策を施す必要がある．これには多大な労力と時間がかかり，かつ，その方法論は確立されていない．このため，現在の情報システム開発におけるセキュリティ対策は，設計者や開発者の勘と経験に頼って行われていることがほとんどであるというのが現状である．

実際に，官庁や企業内では情報セキュリティポリシーの重要性が認識され，企業の 45%が情報セキュリティポリシーを策定しているとの報告がある[7]が，自組織のセキュリティ対策が本当にポリシーに沿った最適なものとなっているかの検証をする手段が無く，情報セキュリティマネジメントの定着と運用について問題意識をもっている企業も少なくない．

本研究はシステムや組織内の情報セキュリティマネジメントの確立をその最終目的とし，特に本稿では，現在までにほとんど研究されていないセキュリティ対策決定手法について論じる．

2. セキュリティ確保の手順と課題

2.1. セキュリティポリシーの策定と運用

システムおよび組織におけるセキュリティ確保の最も重要な観点は，そのシステムや組織における資産の決定であろう．なぜなら守りたい資産が明確でなければ，誰から何をどのように守るのか，どの程度コストをかけてよいのかが明確にならないからである．このようなことからシステムおよび組織におけるセキュリティ確保の第一歩はセキュリティポリシー（方針）の策定にあると考えられる．

セキュリティポリシー（方針）が策定され，実際に守るべき資産が確定したならば，続いて，その資産を脅かす脅威を挙げ，その脅威からどのように資産を守るかを定式化していく．セキュリティ確保の手順は次のようになる．なお，情報セキュリティポリシーとは広義には，以下の(1)～(5)で策定される方針から標準，手順までを意味する．

(1) セキュリティポリシー（方針）の策定

そのシステムや組織の方針，理念を抽象的に表現し，守るべき資産の総体を示す．

(2) リスク分析の実施

そのシステムや組織において守るべき資産を明確にするとともに，その資産の資産価値とリスク頻度から対策を行うべき項目（対策項目）を抽出する．

(3) セキュリティ対策標準の策定

リスク分析から導いた対策項目を基に，そのシステムや組織で行うべき対策の普遍的な規定（ルール）を定める．

(4) セキュリティ対策の決定

各対策項目に対策標準のルールを適用し，個々の対策すべき項目に対する具体的な対策（実際のシステムの動作や組織を規定する具体的なルール)を決定する．

(5) セキュリティ実施手順の策定

システムおよび組織が行なう各サービスに対し，セキュリティ対策に即した形でその手順や設定を明確に規定する．

(6) セキュリティマネージメントの運用

セキュリティ実施手順に沿った運用により，実際にシステムや組織の情報セキュリティマネージメントを実施する．定期的に運用チェックを行い，PDCA サイクルを実現する．

2.2. 課題

2.1 で示した手順の中で，その手順実施の手助けとなる雛型が作成されているものがある．(1)，(3)については日本ネットワークセキュリティ協会(JNSA)ポリシーWG 報告書[8]があり，(2)については ISO/IEC TR 13335 (GMITS)の Part3[2]等があるが，(4)に関する合理的な対策の選択基準は今のところ決定的なものが存在していない．そのため，多くの情報システム開発や組織運用では，リスク分析後に，設計者や開発者の勘と

NII-Electronic Library Service

Information Processing Society of Japan

経験に頼って数多く考えられる対策案から実際にどの対策を採用するかを決定しており，必ずしも効果的かつ効率的な選択はなされていないという問題がある．

また，ポリシー，標準，手順のそれぞれの関連付けが明確でない点が別の問題として挙げられている．手順Aはどの標準を実現するための施策なのか，標準Bはポリシーのどの部分に関連付けられているのかといったことが明確でなく，ポリシーどおりのシステムや組織になっているのか確認することができない．

更に，セキュリティレベルの危殆化に関する理論が体系化されていない．一般に開発された情報システムは，その運用において時間とともにセキュリティレベルが低下するが，セキュリティレベルの危殆化のモデル[9]や動的にセキュリティレベルを保つ方式[10]に関する研究はまだ緒についたばかりである．

2.3. 定式化と自動化

2.2 で示した課題の全てもしくは幾つかを解決するために，(広義の)情報セキュリティポリシー策定に関する各種問題を数学的モデルで定式化し，これを自動化する研究が進められている．

リスク分析の分野では，古くからALE（Annual Loss Expectancy）により資産価値を定式化する方法が採られている．ALEは

$$ALE = SLE \times ARO$$

$$SLE = A \times E$$

として定式化される[11]．ここで，SLE（Single Loss Expectancy ）は一回の予想損失額で，資産価値（A）と起こりうる損害の可能性（E）により算出される．また，ARO（Annual Rate of Occurrence）は損害の年間予想発生回数である．ただし，情報資産にはコンピュータに保存されているデータ（顧客データ，プログラムのソースコードなど）や企業の信用などの無形物も含まれるため，その資産価値を正確な金額に換算することは一般に難しい．また，ニュース速報のような情報においてはその価値が時間とともに減少していくが，資産価値の時間的／動的な変動も定式化を困難にしている要因となっている．

情報セキュリティに対する最適な投資額を求めようとする研究に関しては，経済学的なアプローチにより行なわれているものが多い[12]．特に文献[13]では，投資額をz，投資により達成される平均損失額の減少（投資により得られる収益）をEBISとし，投資による純利益(収益から原価を引いたもの)の期待値ENBIS＝EBIS－zを最大化するzが最適投資額であるという理にかなった定式化が示されている．また文献[14]では，目的が不正コピー防止に限定されているものの，情報マネジメントに関する対策案選定問題をFTA（Fault Tree Analysis）により定式化するアプローチが提案されている．

本稿では，2.2で指摘した課題のうち，2.1(4)に関する合理的な対策の選択基準の不足を受け，セキュリティ対策案選定問題に対する定式化および自動化の一手法を検討する．対策案の選択が定式化できれば，

- ノウハウのある者に対して：自分が選択した対策案が必要最低限（守るべき資産は守られており，かつ，そのコストが最小）であることを理論的，客観的に示すことが可能となる
- ノウハウのない者に対して：定式化された手順に従い（または自動化された対策案選定システムを用いて），対策案の選択を行なうことが可能となる

などのメリットが得られる．

本稿はセキュリティ対策案選定問題の定式化を目的としているので，文献[13]のように投資対象を総体として扱うようなモデルでは不十分である．そこで，資産，脅威，対策のそれぞれを具体的な構成要素単位で取り扱うモデルを用いることとし，選択された対策案の組合せごとに，対策コストCと平均残存資産RAを算出し，RA－Cの期待値を最大化するというアプローチを採る．

なお，無形物の資産価値の算出は難しいことを前述したが，本項ではセキュリティ対策案選定問題に焦点を絞り，リスク分析については確実に行えるものとして扱う．

3. 資産・脅威・対策案のモデル

資産，脅威，対策案をモデル化するにあたり，本稿に登場する記号について説明しておく．

- A_k：Asset：組織内の各資産
- V_k：Value：資産A_kの価値
- T_j：Threat：各脅威
- P_j：Probability：一定期間内に脅威T_jが発生する確率
- E_{jk}：Effect Flag：脅威T_jが資産A_kに影響するか否かのフラグ
- CM_i：Countermeasure：各対策案
- C_i：Cost：CM_iの実施に必要なコスト
- R_{ji}：Risk Reducing Rate：脅威T_jに関する攻撃が発生した場合において，対策案CM_iによってその攻撃の成功率が減少する割合（何の対策案も施されていない場合，脅威T_jに関する攻撃が発生すると確率1でその攻撃は成功する．対策案CM_iの実施によって，脅威T_jに関する攻撃の成功率は$1-R_{ji}$に減少する．）

本稿では，資産・脅威・対策案を「資産と脅威の関

NII-Electronic Library Service

係」と「脅威と対策案の関係」に分けてモデル化を行なっていく．

3.1. 資産と脅威の関係

資産と脅威の関係は，それぞれの脅威 T_j が各資産 A_k に影響するか否かという点に着目して表として表す．

まず，図 1 のように各資産 A_k ($1 \leqq k \leqq K$)，各脅威 T_j ($1 \leqq j \leqq J$) をリストアップする．資産リストは各資産 A_k とその価値 V_k とをセットにしてリストアップしたものである．脅威リストは脅威 T_j とその発生確率 P_j とをセットにしてリストアップしたものである．

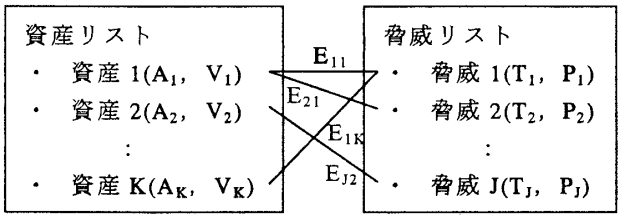

図 1: 脅威と資産の関係

図 1 において資産と脅威とをつないでいる線は，接続されている脅威が資産に影響することを表している．ここで「影響する」とは，脅威 T_j が発生した場合，T_j と線で結ばれている資産が失われるということを意味する．資産 A_k と脅威 T_j とをつないでいる線が存在するならば $E_{jk}=1$，線がなければ $E_{jk}=0$ である．

次に，図 1 の資産リストと脅威リストおよびその関係を表 1 のような表に変換する．

表 1: 脅威と資産の表

	資産 1 (A_1, V_1)	資産 2 (A_2, V_2)	…	資産 K (A_K, V_K)
脅威 1 (T_1, P_1)	E_{11}	E_{12}	…	E_{1K}
脅威 2 (T_2, P_2)	E_{21}	E_{22}	…	E_{2K}
:	:	:	:	:
脅威 J (T_J, P_J)	E_{J1}	E_{J2}	…	E_{JK}

3.2. 脅威と対策案の関係

脅威と対策案の関係は，それぞれの脅威 T_j に対し各対策案 CM_i がどの程度の効果を発揮するのかという点に着目して表として表す．

まず，図 2 のように各対策案 CM_i ($1 \leqq i \leqq I$)，各脅威 T_j ($1 \leqq j \leqq J$) をリストアップする．対策案リストは各対策案 CM_i とその実施に必要なコスト C_i とをセットにしてリストアップする．脅威リストは図 1 の脅威リストと同じである．

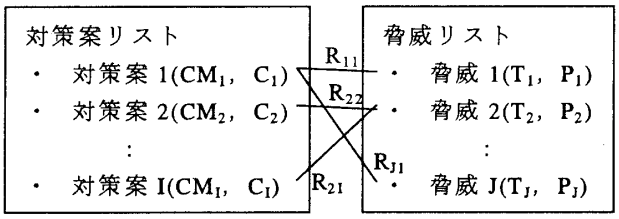

図 2: 脅威と対策案の関係

図 2 において対策案と脅威とをつないでいる線は，接続されている脅威に対して対策案が効力を発揮することを表している．ここで「効力を発揮する」とは，対策案 CM_i の実施によって，攻撃などの脅威 T_j が発生した場合にその攻撃が成功する確率が減少する（何の対策案も施されていない場合には攻撃は確率 1 で成功する）ことを意味する．対策案 CM_i と脅威 T_j とをつないでいる線が存在するならば，その対策案がその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（0～1）を R_{ji} として記す．

次に，図 2 の対策案リストと脅威リストおよびその関係を表 2 のような表に変換する．

表 2: 脅威と対策案の表

	対策案 1 (CM_1, C_1)	対策案 2 (CM_2, C_2)	…	対策案 I (CM_I, C_I)
脅威 1 (T_1, P_1)	R_{11}	R_{12}	…	R_{1I}
脅威 1 (T_2, P_2)	R_{21}	R_{22}	…	R_{2I}
:	:	:	:	:
脅威 J (T_J, P_J)	R_{J1}	R_{J2}	…	R_{JI}

3.3. 注意

本節のモデルでは，各資産，各脅威，各対策案はそれぞれ独立した事象としてモデル化されている．しかし実際には，

- それぞれの脅威を単体で見ている場合には問題に至らないが，複数の攻撃が組み合わさることで発生するような脅威が存在する
- ある対策案を単独で実施する場合にはそれなりの効果が発揮されるのであるが，すでに他の同様の対策案が実施されているところにその対策案を追加したとしても，更なる効果は期待できないことも多い
- 逆に，2 つの対策案を併用することで効果が倍増

NII-Electronic Library Service

Information Processing Society of Japan

することもある

など，各事象の間には相関関係があることが往々にしてある．

だが，相関関係等も考慮したモデルを作成しようとすると，モデル自体が複雑になってしまうばかりか，それを基に対策案の選択を行う方法も非常に難しいものになってしまうだろう．より現実に即したモデルは必要ではあるが，それを有効に用いることができなくなってしまったのでは意味がない．

そこで本稿では，まずはモデルを簡素にして，問題の定式化を簡明に行なうこととした．今後，本定式化によるセキュリティ対策案選択システムを構築し，本システムにより得られる対策案選定結果と，専門家がノウハウを駆使して実際に選択した対策案を比較検討することにより，本定式化の妥当性を検証し，必要に応じてモデルの改良を行なっていく予定である．

4. セキュリティ対策案選択問題の定式化

本稿はセキュリティ対策案選定問題の定式化を目的としているので，資産，脅威，対策のそれぞれを具体的な構成要素単位で取り扱うモデルを用いることとし，選択された対策案の組み合わせごとに，対策コストCと平均残存資産RAを算出し，RA－Cの期待値を最大化するというアプローチを採る．前章にて資産，脅威，対策のそれぞれを具体的な構成要素単位で取り扱うためのモデル化が完了したので，続いて本章で平均残存資産のモデル化を行い，対策案選定問題の定式化を行なっていく．

4.1. 残存資産

一定期間が経過した後に脅威によって失われなかった資産の総和を残存資産RAと定義する．

まず，資産（価値）の総和は単純に

$$\sum_k V_k \qquad (1)$$

で表される．

次に，何の対策も施されていない場合の残存資産を算出する．表1より，各資産A_kにはE_{jk}=1である脅威T_jが影響し，脅威T_jの発生により資産A_kは失われることが分かっている．何の対策も施されていない場合，脅威T_jの発生により資産A_kが失われる確率は1であるため，一定期間のうちに資産A_kが失われる確率はその期間内に脅威T_jが発生する確率P_jに等しい．逆に言えば，脅威T_jに対して資産A_kが失われずに残る確率は$1-P_j$である．そして，一定期間のうちに資産A_kを脅かす全ての脅威（資産A_kに対してE_{jk}=1である全ての脅威T_j）が発生しなければ，資産A_kは残存することになる．資産A_kに対してE_{jk}=1である全ての脅威T_jが一定期間のうちに発生しない確率は

$$\prod_j \left[1 - E_{jk}P_j\right]$$

であるため，一定期間後に残存している資産A_kの価値V_kの期待値は

$$V_k \prod_j \left[1 - E_{jk}P_j\right]$$

であり，残存する全ての資産の総和である残存資産の期待値は

$$\sum_k \left\{ V_k \prod_j \left[1 - E_{jk}P_j\right] \right\} \qquad (2)$$

で表される．

4.2. 対策後の残存資産

続いて，表2より，対策を行った際の残存資産を算出する．対策案CM_iの実施によって，脅威T_jに関する攻撃の成功率は$1-R_{ji}$に減少する．よって，脅威T_jが影響する（E_{jk}=1である）資産A_kが一定期間のうちに失われる確率は，その期間内に脅威T_jが発生する確率P_jと攻撃成功率$1-R_{ji}$の積となる．すなわち，対策案CM_iを選択するか否かのフラグS_iを用意し，S_i＝1により対策案CM_iの選択，S_i＝0により対策案CM_iの非選択を表すとすると，脅威T_jにより一定期間のうちに資産A_kが失われる確率は$P_j(1 - R_{ji}S_i)$となる．

脅威T_jに関する攻撃成功率を低下させることができる対策案はCM_iだけではなく，全ての対策案CM_i（$1 \leqq i \leqq I$）それぞれがR_{ji}の割合で脅威T_jに関する攻撃の成功率を減少させる．3.3で述べたように，対策案の相関関係は考慮の対象から外すことにし，各対策案による効果が単純に相乗されると仮定するならば，全ての対策案の選択／非選択により，脅威T_jに関する攻撃の成功率は

$$\prod_i \left(1 - R_{ji}S_i\right)$$

に減少する．よって，このとき，脅威T_jが影響する（E_{jk}=1である）資産A_kが一定期間のうちに失われる確率は

$$P_j \prod_i \left(1 - R_{ji}S_i\right) \qquad (3)$$

となる．

これは，対策案により式(2)のP_jが式(3)に変化する

NII-Electronic Library Service

Information Processing Society of Japan

ことを意味するので，式(2)の P_j を式(3)に変更してやることにより，$S_i=1$ となっているセキュリティ対策案 CM_i が選択された状況における残存資産の期待値を求めることができる．すなわち，次式が残存資産 RA である．

$$\sum_k \left\{ V_k \prod_j \left[1 - E_{jk} P_j \prod_i \left(1 - R_{ji} S_i \right) \right] \right\} \quad (4)$$

4.3. 対策の効果と最適化

資産を脅威から守るということは，対策を施すことによりなるべく多くの資産を残しておけるように努力することに他ならない．よって，対策案選定問題は式(4)の残存資産 RA を最大化する問題となる．ただし，各対策を施すにはそれなりのコストがかかる．すなわち，式(4)の残存資産 RA から対策にかかったコストの分を減じたものが，講じられた対策に対する「純粋な」効果となる．

以上より，セキュリティ対策案選定問題は

$$\sum_k \left\{ V_k \prod_j \left[1 - E_{jk} P_j \prod_i \left(1 - R_{ji} S_i \right) \right] \right\} - \sum_i C_i S_i \quad (5)$$

の値が最大となるような S_i の組み合わせを見つけるという問題に帰着する．これは，

$$S_i \in \{0,1\} \quad (1 \leqq i \leqq I) \quad (6)$$

なる制約条件の下で式(5)の目的関数を最大化するという離散最適化問題を解くことと等価となる．

表 3: 脅威と資産の表

	A_1 1,000,000	A_2 1,000,000	A_3 1,000,000
T_1, 0.2	1	0	1
T_2, 0.1	0	1	0
T_3, 0.05	0	1	1
T_4, 0.5	0	1	0
T_5, 0.7	1	1	1

5. 簡単な適用例

本稿で定式化した解法により簡単なセキュリティ対策案選択問題を解いた例を示す．本章の 2 つの適用例は，資産のうちの一つが異なるのみで，その他の部分は全く同一のものとなっている．

なお，離散最適化問題を効率良く解くアルゴリズムは今のところ見つかっていないので，今回は式(5)を最大化する S_i を総当たり法により発見する解析プログラムを作成した．

5.1. 適用例 A

リスク分析の結果，資産リスト，脅威リスト，対策案リストは以下のようになったとする．

資産リスト

- A_1：ウェブコンテンツ，M_1：1,000,000
- A_2：顧客情報，M_2：1,000,000
- A_3：労働力，M_3：1,000,000

脅威リスト

- T_1：ウェブコンテンツ改竄，P_1：0.2
- T_2：顧客情報の不正な読み取り，P_2：0.1
- T_3：顧客情報の改竄，P_3：0.05
- T_4：通信の盗聴，P_4：0.5
- T_5：ウィルス感染，P_5：0.7

対策案リスト

- CM_1：ID&Password，C_1：1,000
- CM_2：IC カード，C_2：100,000
- CM_3：VPN，C_3：250,000
- CM_4：ファイアウォール，C_4：200,000
- CM_5：IDS，C_5：200,000
- CM_6：アンチウィルスソフト，C_6：300,000
- CM_7：定期的なセキュリティパッチの適用，C_7：50,000

そして，脅威と資産の関係（E_{jk}），および，脅威と対策案の関係（R_{ji}）を洗い出した結果，表 3，表 4 のようになったとする．

表 4: 脅威と対策案の表

	CM_1 1,000	CM_2 100,000	CM_3 250,000	CM_4 200,000	CM_5 200,000	CM_6 300,000	CM_7 50,000
T_1, 0.2	0.5	0.6	0	0.4	0.2	0	0.5
T_2, 0.1	0.5	0.6	0	0.7	0.2	0	0.3
T_3, 0.05	0.5	0.6	0	0.7	0.2	0	0.4
T_4, 0.5	0	0	0.7	0.3	0	0	0
T_5, 0.7	0	0	0	0.5	0	0.9	0.4

NII-Electronic Library Service

Information Processing Society of Japan

ここで，各 E_{jk}，R_{ji} の値についてその値に設定した理由を簡単に述べておく．

(1)E_{jk}について：

資産 A_1「ウェブコンテンツ」はコンテンツが改竄されることによりその価値が失われるとする．コンテンツの改竄に関係する脅威は，T_1「ウェブコンテンツの改竄」と T_5「ウィルス感染」と考えられる．ウェブコンテンツは閲覧自由なので，T_4「通信の盗聴」については影響なしとした．

資産 A_2「顧客情報」は改竄に加え，情報の漏洩によってもその価値は失われるとしている．T_1「ウェブコンテンツの改竄」以外の脅威が全て顧客情報に影響する．

資産 A_3「労働力」とは従業員などのヒューマンリソースである．「何らかの脅威によって労働力を復旧業務などに投下しなければならず，普段の業務が遂行できずに得られるはずだった利益が得られない」と言う状況は，労働力という資産が脅威によって侵害されたと考える．そのため，データの復旧が必要となる T_1「ウェブコンテンツの改竄」，T_3「顧客情報の改竄」，T_5「ウィルス感染」の脅威が労働力に影響するとした．

(2) R_{ji}について：

対策案 CM_1「ID&Password」と対策案 CM_2「IC カード」はシステムへのアクセス制御の基本とも言えるユーザ認証を行うためのものなので，サーバ等へのアクセスに関わる脅威にある程度高い効果があるとした．また，ID&Password よりも IC カードを用いたほうが一般的により強固であることを踏まえ，R_{ji} の値を設定した．

対策案 CM_3「VPN」は基本的には通信路を暗号化するものなので盗聴の脅威に対してのみ高い効果を持つとした．対策案 CM_6「アンチウィルスソフト」はウィルスの脅威に対してのみ高い効果を持つとした．

対策案 CM_4「ファイアウォール」は各種攻撃に満遍なく効果を発揮するものとした．ただし，VPN やアンチウィルスソフトなどのような個別の対策に特化したものよりは各効果は低いとした．

対策案 CM_5「IDS」については，（侵入が検知された時点でデータは改竄されてしまっているであろうということで）直接，脅威から資産を保護するものではないが，存在そのものが抑止力として働く面があるため，ある程度脅威を減らす効果があるとした．ただし，盗聴は IDS で発見しづらいため，また，ウィルスはその動作の主体がプログラムの（意思のない）自動的な動作であるため，どちらに対しても IDS は抑止力とならない．

対策案 CM_7「定期的なセキュリティパッチの適用」については，システムのセキュリティホールを塞ぐものなので盗聴以外には効果があるとした．

以上をふまえ，これらの値を式(5)に代入し，これを解析プログラムで解いたところ，

$$(S_1,S_2,S_3,S_4,S_5,S_6,S_7) = (1,0,1,0,0,1,1)$$

つまり

- CM_1：ID&Password，C_1：1,000
- CM_3：VPN，C_3：250,000
- CM_6：アンチウィルスソフト，C_6：300,000
- CM_7：定期的なセキュリティパッチの適用，C_7：50,000

の 4 つを対策案として選択することにより最も残存資産の期待値が高くなるという解が得られた．残存資産の期待値は 2,017,272 であった．

IC カードによるユーザ認証やファイアウォールなどは守る資産の価値の総和に対する導入コストが高く，コストパフォーマンスを考えると ID&Password やセキュリティパッチのメンテナンスのみを採用したほうが得である，という判断が下されたことが分かる．

5.2. 適用例 B

次に，適用例 A における 2 番目の資産 A_2 である顧客情報の価値 V_2 のみを 1,500,000 から 3,000,000 に変更してみた．よって，資産リスト，脅威リスト，対策案リスト，脅威と資産の関係（E_{jk}），および，脅威と対策案の関係（R_{ji}）は V_2 が 3,000,000 に変わっている以外は適用例 A のものと同一となる．

これらの値を式(5)に代入し，これを解析プログラムで解いたところ，

$$(S_1,S_2,S_3,S_4,S_5,S_6,S_7) = (1,0,1,1,0,1,1)$$

つまり

- CM_1：ID&Password，C_1：1,000
- CM_3：VPN，C_3：250,000
- CM_4：ファイアウォール，C_4：200,000
- CM_6：アンチウィルスソフト，C_6：300,000
- CM_7：定期的なセキュリティパッチの適用，C_7：50,000

の 5 つを対策案として選択することにより最も残存資産の期待値が高くなるという解が得られた．残存資産の期待値は 3,715,360 であった．

顧客情報の価値が上がったため，顧客情報が存在するデータベースサーバに関係する脅威を減じることができるファイアウォールに関しては，導入におけるコストパフォーマンスが適正である，という判断が下されたことが分かる．

6. 今後の課題

6.1. 脅威および対策案の相関関係

3.3 で述べたように，複数の脅威が合わさって初め

NII-Electronic Library Service

Information Processing Society of Japan

て発生するリスクや，類似の対策案が選択された際の対策効果の実効性，相補的な対策案が選択された際の相乗効果などの，脅威や対策案の各項目間の相関関係については，本稿のモデルではこれを対象から外している．本方式の評価を行うことにより，項目の相関関係までをモデル化する必要があるか否かについて検討していく必要がある．

6.2. 資産や対策案の適正な評価

3.3 で述べたように，情報資産には電子データや企業の信用などの無形物も含まれるため，その資産価値を正確な金額に換算することは一般に難しい．また，その価値が時間的に変化する資産の定式化も困難である．ある脅威によりシステムが停止してしまった場合に，復旧まで時間がかかればかかるほど損害は大きくなるので，脅威によって失われる資産の価値が時間とともに変化するということも考えなければならない．

対策案の効果も時間的に変化する．例えば暗号は，方式が公開された瞬間から暗号解読の脅威にさらされることになるので，その安全性は時間とともに低下するのではないだろうか．また，対策案として「セキュリティ教育」を挙げたとすると，それを行った直後は比較的高い効果を発揮していたが，時間が経つにつれてユーザがだんだんと慣れてきて，緊張が緩んで効果が薄れていくということが予想できよう．これらをどうモデル化すればよいか検討の余地がある．

6.3. 離散最適化問題の解法

本稿の定式化によりセキュリティ対策案選択問題は離散最適化問題に帰着することが示されたわけだが，5 章の冒頭で述べたように，今のところ，離散最適化問題を効率的に解くアルゴリズム（多項式時間内で解を得る決定的アルゴリズム）は見つかっていない．5 章の適用例では対策案の数が少なかったので総当りにより最適解を得ることが可能であったが，現実の組織や情報システムを実際に設計する段階ではセキュリティ対策案の数も飛躍的に増加するため，総当り法は現実的ではないだろう．今後，ヒューリスティックや遺伝的アルゴリズムなどを用いる必要があると予想される．

7. まとめ

本稿では，資産・脅威・対策案の関係をモデル化し，セキュリティ対策案選択問題を定式化することにより，対策案の最適な組み合わせを理論的に求める手法を導出した．本手法によれば，セキュリティ対策案選択問題は離散最適化問題として定式化される．また，非常に単純な例ではあるが，具体的なセキュリティ対策案選択問題に対して本手法を適用し，およそ妥当な結果が得られたことを報告した．

今後は，現実の情報セキュリティポリシーの策定事例を本手法に適用し，専門家が実際に選択したセキュリティ対策案と本手法によって選ばれるセキュリティ対策案を比較することによって，本手法の実用性・有効性を評価していきたい．

謝辞

本研究を行うにあたり貴重な御助言をいただいた創価大学勅使河原可海先生，高橋雄志氏に感謝致します．

文　献

[1] ISO, “ISO/IEC 17799”, http://www.iso.ch/.

[2] ISO, “ISO/IEC TR 13335 1-5”, http://www.iso.ch/.

[3] ISO, “ISO/IEC 15408 1-3”, http://www.iso.ch/.

[4] IPA セキュリティセンター，“情報セキュリティの現状 2001 年版”, http://www.ipa.go.jp/security/fy13/sec2001/sec2001.pdf, May 2002（2003.6 確認）.

[5] JIPDEC, “情報セキュリティマネジメントシステム(ISMS)適合性評価制度”, http://www.isms.jipdec.or.jp/,（2003.6 確認）.

[6] JIPDEC, “ISMS 認証取得事業者一覧”, http://www.isms.jipdec.or.jp/lst/ind/,（2003.6 確認）.

[7] 菅谷光啓, “セキュリティポリシーの“実態””, NRI セキュアテクノロジーズ, SECURITY GUIDANCE, #04, http://www.nri-secure.co.jp/guidance.htm, Jun. 2002.

[8] 日本ネットワークセキュリティ協会，“情報セキュリティポリシー・サンプル解説書”, http://www.jnsa.org/policy/guidance/, (2003.6 確認).

[9] 佐々木良一，州崎誠一，“デジタル署名付文書の長期的安全性に関する考察”，情報処理学会研究報告，Vol.2003, No.45, pp13-18, May 2003.

[10] 兵藤敏之，西垣正勝，中村逸一，曽我正和，“セキュリティ状態のランク付け”，コンピュータセキュリティシンポジウム 2002(CSS2002)論文集，pp71-76, Oct. 2002.

[11] Keith W. McCammon, “Calculating Loss Expectancy”, http://mccammon.org/articles/loss_expectancy.php,（2003.6 確認）.

[12] 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)予稿集，Vol.I, pp.475-480, Jan. 2003.

[13] Lawrence A. Gordon and Martin P. Loeb, “The Economics of Information Security Investment”, ACM Transactions on Information and System Security, Vol. 5, No. 4, pp438-457, Nov. 2002.

[14] 佐々木良一，吉浦裕，伊藤信治，“不正コピーの最適組合わせに関する考察”，情報処理学会論文誌，Vol.43, No.8, pp2435-2446, Aug. 2002.

NII-Electronic Library Service