# 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

中村逸一[†1] 兵藤敏之[†2] 曽我正和[†3]
水野忠則[†4] 西垣正勝[†4]

近年，情報セキュリティポリシーを策定，運用する組織などが増えつつある．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具体的な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．本論文では，資産・脅威・対策の関係をモデル化し，セキュリティ対策選択問題を定式化することにより，対策の最適な組合せを論理的に求める手法を導出した結果，セキュリティ対策選択問題が離散最適化問題として定式化されることを示す．さらに，実システムにおいて設計者や開発者が勘や経験により実際に選択した対策と本手法が導いた結果を比較，検討し，本手法が十分実用的であることを示す．

# A Practical Approach for Security Measure Selection Problem and Its Availability

Itsukazu Nakamura,[†1] Toshiyuki Hyodo,[†2] Masakazu Soga,[†3]
Tadanori Mizuno[†4] and Masakatsu Nishigaki[†4]

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 any objective evaluation of appropriateness of the selected security measures is impossible. To cope with the inconvenience, this paper proposes an approach to formulate the problem for selecting security measures. Then, the availability of our method is evaluated by comparing the security measures that our method has selected with the ones that a system designer has chosen.

## 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，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1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うえで重要である．

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

†1 株式会社 NTT データビジネス開発事業本部
IT Business Development Sector, NTT Data Corporation
†2 中部テレコミュニケーション株式会社
Chubu Telecommunications Co., Inc.
†3 岩手県立大学ソフトウェア情報学部
Faculty of Software and Information, Iwate Prefectural University
†4 静岡大学情報学部
Faculty of Information, Shizuoka University

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，その具体的な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，企業の約 40.3%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なく，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持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，特に本論文では，現在までにほとんど研究されていない実用的なセキュリティ対策決定手法について論じる．以下，まず 2 章で，セキュリティマネジメントに関する現状と課題についてまとめる．続いて，3 章で資産・脅威・対策の関係をモデル化し，4 章でセキュリティ対策選択問題を定式化する．そして 5 章では，本手法により実システムのセキュリティ対策の選定を実際に行う．6 章で本手法によって選ばれた対策と設計者が選んだ対策とを比較，検討し，本手法が十分実用的であることを示す．最後に，7 章で今後の検討課題をあげ，8 章で本論文をまとめる．

## 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，そのために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．すなわち，システムおよび組織におけるセキュリティ確保の第 1 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あげ，その脅威からどのように資産を守るかを検討していく．セキュリティ確保の手順はおおむね次のようになる．なお，情報セキュリティポリシーとは広義には，以下の (1)〜(3) で策定される方針から基準までを意味する．

(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．たとえば，「当社は顧客情報を機密情報として位置づけ，顧客からの信頼感を得る」といった組織としての考えを示すものである．

(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) **セキュリティ対策基準の策定**
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（普遍的なルール）を定める．たとえば，機密情報の開示範囲や管理方法をルール化し「情報セキュリティ規定」といった規定類を作成することである．

(4) **セキュリティ対策の決定**
セキュリティ対策基準のルールを遵守するため，個々の対策すべき項目に対し具体的な対策（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．たとえば，セキュリティ対策基準で「事務室内に第 3 者の立ち入りは認めない」とあった場合に，事務室前に警備員を配置する案や IC カードゲート装置を設ける案などさまざまな対策案が考えられ，その対策案から適切な対策を決定する．

(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．たとえば，機密情報を開示する場合の手順，記録方法といった，情報を扱う者が具体的に何を行うべきかを示したドキュメント類を整備する．

(6) **セキュリティマネジメントの運用**
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ジメントを実施する．定期的に運用チェックを行い，マネジメントサイクルである PDCA（Plan，Do，Check，Act）を実現する．

### 2.2 セキュリティ確保における課題と本論文の目的

2.1 節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] などがあるが，(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，一部の専門家でないと対策を決定できない，また効果的かつ効率的な選択がなされているかの確認ができないという課題がある（課題 a)☆.

また，ポリシー，基準，手順のそれぞれの関連付けが明確でないという課題があげられている．手順 A はどの基準を実現するための施策なのか，基準 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．この問題を解決するための研究[9] も進められているが，研究の途上である（課題 b).

さらに，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．一般的に，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[10] や動的にセキュリティレベルを保つ方式[11] に関する研究はまだ緒についたばかりである（課題 c).

上記の 3 つの課題の中で，本論文が問題として特に重要視しているのが，セキュリティ対策選定に関する課題 a である．本論文は，課題 a を解決するための実用的手法を検討するものである．次節では，課題 a に焦点をあて，従来の関連研究と本論文の提案手法を説明していく.

### 2.3 セキュリティ対策選定における従来の研究と提案手法

情報資産のモデル化に対しては，リスク分析の分野で，古くから $ALE$（Annual Loss Expectancy）により年間予想損失額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[12]．ここで，$SLE$（Single Loss Expectancy）は 1 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.

しかし，セキュリティ対策選定問題を解くためには，情報資産だけでなく脅威や対策などをも含めて，(広義の）情報セキュリティポリシー策定に関する各種の事象を数学的モデルで定式化し，それらすべてを総合して解析する必要がある．このため，セキュリティ対策選定に関する既存の研究においては，具体的な対策各々を個別に扱うのではなく，情報セキュリティに対する最適な投資総額を求める経済学的なアプローチによる研究が多い[13]．特に文献 14) 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．これらの方法は，対策に要する投資が最適であったかを評価するためには利用できるが，数ある対策案から合理的に対策を決定するものではない.

これに対し，対策案の中から対策を選定する問題に取り組んだ研究が文献 15)，16) である．文献 15) では，情報システムにおけるセキュリティ対策選定問題を Fault Tree のミニマルパス解析により定式化するアプローチが提案されている．これは，脆弱性と資産価値に着目して，リスクに対抗する「必要最低限の対策」を選定するものであり，どの対策を選定すればよいのかについて一定の解を得ることができる．さらに文献 16) では，目的が不正コピー防止に限定されているものの，文献 15) の方法を拡張し，ある対策を実施した際の脅威発生確率の低減をも考慮することにより，リスクに対抗する「適用効率が一番高い対策」を選定する方法が示されている．文献 16) の方法はセキュリティ対策選定問題をモデル化するにあたっての非常に的確なアプローチであると考えられ，実際に，脆弱性に関する Fault Tree の作成が比較的容易な製品や単一のサービスを提供するシステムの設計においては一定の効果が得られるものと思われる．しかし，組織のセキュリティマネジメントおよび複数のサービスを提供する統合システムにおける一般的な設計手順の中で Fault Tree を作ることは通常行っておらず（または，複雑になりすぎて Fault Tree を作成することができない)，実用性に問題があるといえる.

そこで本論文では，セキュリティ対策の選定にあたって実際の企業や組織が一般に行っているセキュリティ確保の手順やその際の分析結果（リスク分析表など）が利用できるような，セキュリティ対策選定問題の定

☆ 対策の決定は，システムの設計者が費用対効果と導入のしやすさ（経験，環境，組織風土）を総合的に考慮し，多くの対策案から対策を選定しているのが現状である．これを本論文では,「設計者や開発者の勘と経験」と表現している．ただし，対策選択における基本的な考え方は存在する．たとえば，一般的に
- 抑止的対策は，組織的な活動により実現すれば費用対効果が高い（例：ルール化，マニュアル整備，啓蒙など)，
- 防止的対策は，物理的・技術的な対策で実現されるが比較的コストが高くなる（例：システムへのアクセス制御，データの機密性確保など)，
- 検知的対策，回復的対策は，組織的な活動と物理的・技術的な対策の併用で実現する，

ということなどがいわれている.

式化に対する実用的な一手法を提案する．対策の選定が定式化できれば，

**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）であることを他人に論理的，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選定システムを用いて），最適な対策の選択を行うことが可能となる．

などのメリットが得られる．

本論文では，専門家がシステムのセキュリティ対策を決定する際に行う手順を模範にし，資産・脅威・対策を「資産と脅威の関係」と「脅威と対策の関係」に分けてモデル化を行っていく（3 章に詳しく示す）．そして，情報資産の実質的な「残存資産」という概念を導入して，選択された対策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により対策選定問題を定式化する（4 章に詳しく示す）．

なお，無形物の資産価値の算出は実際には難しい問題を含むが，本論文ではセキュリティ対策選択問題に焦点を絞り，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・対策のモデル

2.1 節の手順 (4)「セキュリティ対策の決定」の実施にあたり，専門家がセキュリティ対策選定を行う際には，一般的に次のステップを踏む．

(i) 情報資産をすべてリストアップし，それぞれの資産価値（金額であったり他の資産との相対比較であったりする）を推定する．

(ii) それぞれの資産に対してどのような脅威が考えられるかをリストアップし，それぞれの脅威にその発生頻度（確率であったり他の脅威との相対比較であったりする）を推定する．

(iii) リスク（特に容認することができないリスク）に関与する脅威を低減させる具体的な対策案をリストアップし，種々の考え（勘と経験）のもとに最終的に対策を決定する．

すなわち専門家は，資産のリスト，脅威のリスト，対策のリストを用意し，資産に対する脅威をリスク分析により算出したうえで，脅威を低減させる対策案の中から実際に実施する対策を決定する（ただし上記のステップ (i)〜(iii) は，2.1 節の手順 (4) だけに関与するのではなく，手順 (2)「リスク分析の実施」，手順 (3)「セキュリティ対策基準の策定」の内容を考慮しながら進めることとなる）．

本論文はセキュリティ対策選定問題の定式化に対する実用的な一手法を確立することを目的としており，セキュリティ対策の選定にあたって専門家が実際に行う手順やその際の分析結果を利用できるようなモデル化を行う．よって，資産・脅威・対策を「資産と脅威の関係」と「脅威と対策の関係」に分けてモデル化を行っていく．

まずは資産，脅威，対策をモデル化するにあたり，本論文で使用する記号について説明しておく．

- $A_k(Asset)$：組織内の各資産（複数の資産を下付きの $k$ で区別する．なお，資産の総数を $K$ とする）
- $V_k(Value)$：資産 $A_k$ の価値
- $T_j(Threat)$：各脅威（複数の脅威を下付きの $j$ で区別する．なお，脅威の総数を $J$ とする）
- $P_j(Probability)$：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（複数の対策を下付きの $i$ で区別する．なお，対策の総数を $I$ とする）
- $C_i(Cost)$：$CM_i$ 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 $CM_i$ 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 $CM_i$ 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）

### 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 $A_k$（$1 \leq k \leq K$），各脅威 $T_j$（$1 \leq j \leq J$）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 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

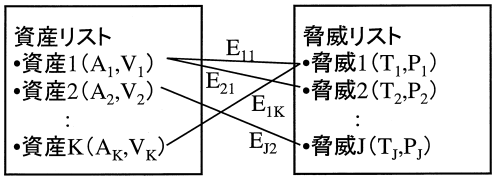



**図 1** 脅威と資産の関係
Fig. 1 Relation between threats and assets.

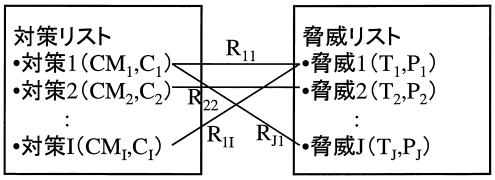



**図 2** 脅威と対策の関係
Fig. 2 Relation between threats and countermeasures.

**表 1** 脅威と資産の表
Table 1 Table for threats and assets.

| | 資産 1 $A_1, V_1$ | 資産 2 $A_2, V_2$ | $\cdots$ | 資産 K $A_K, V_K$ |
|---|---|---|---|---|
| 脅威 1 $T_1, P_1$ | $E_{11}$ | $E_{12}$ | $\cdots$ | $E_{1K}$ |
| 脅威 2 $T_2, P_2$ | $E_{21}$ | $E_{22}$ | $\cdots$ | $E_{2K}$ |
| $\vdots$ | $\vdots$ | $\vdots$ | $\ddots$ | $\vdots$ |
| 脅威 J $T_J, P_J$ | $E_{J1}$ | $E_{J2}$ | $\cdots$ | $E_{JK}$ |

**表 2** 脅威と対策の表
Table 2 Table for threats and countermeasures.

| | 対策 1 $CM_1, C_1$ | 対策 2 $CM_2, C_2$ | $\cdots$ | 対策 I $CM_I, C_I$ |
|---|---|---|---|---|
| 脅威 1 $T_1, P_1$ | $R_{11}$ | $R_{12}$ | $\cdots$ | $R_{1I}$ |
| 脅威 2 $T_2, P_2$ | $R_{21}$ | $R_{22}$ | $\cdots$ | $R_{2I}$ |
| $\vdots$ | $\vdots$ | $\vdots$ | $\ddots$ | $\vdots$ |
| 脅威 J $T_J, P_J$ | $R_{J1}$ | $R_{J2}$ | $\cdots$ | $R_{JI}$ |

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．

そして，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．

### 3.2 脅威と対策の関係

脅威と対策の関係は，それぞれの脅威 $T_j$ に対し各対策 $CM_i$ 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 $CM_i$（$1 \leq i \leq I$），各脅威 $T_j$（$1 \leq j \leq J$）をリストアップする．対策リストは各対策 $CM_i$ 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（ここでは，考えられうる対策を列挙することになるため，その意味では $CM_i$ は「対策案」と呼ぶべきかもしれない）．脅威リストは図 1 の脅威リストと同じである．

図 2 において対策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 $CM_i$ 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 $CM_i$ 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．

そして，図 2 の対策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．

### 3.3 注　　意

本節のモデルでは，各資産，各脅威，各対策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が，すでに他の同様の対策が実施されているところにその対策を追加したとしても，さらなる効果は期待できないことも多い，
- 逆に，2 つの対策を併用することで効果が倍増することもある，

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，相関関係など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

☆ 本モデルでは，資産 $A_k$ に影響する脅威 $T_j$ が発生すると $A_k$ の価値は完全に失われてしまうが，脅威によっては資産の一部のみが失われることも想定される．しかしそのような場合には，資産の分類を十分小さな単位で行い，「資産の一部」を個々の資産としてモデル化すればよいので，本モデルの一般性は失われない（たとえば，「製品情報」という大きなくくりで資産をモデル化するのではなく，その中に含まれている「ソースコード」「設計書」「社内規格」などをそれぞれ個別の資産と考える）．なお，正確な資産価値の推定のために，資産の見積りをなるべく小さい単位で行うことが実際に推奨されている．

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．

そこで本論文では，まずはこのような相関関係などについては考慮から除外することによりモデルを簡素にして，問題の定式化を簡明に行うこととした．このような簡素なモデルが妥当であるか否かについては，後続の章で，本モデルに基づいて定式化されたセキュリティ対策選択問題を解くことにより得られる対策選定結果と，専門家がノウハウを駆使して実際に選択した対策とを比較検討することにより検証することができると考える．

## 4. セキュリティ対策選択問題の定式化

3 章で示した資産，脅威，対策のモデルを用い，セキュリティ対策選択問題の定式化を行っていく．文献 14) で述べられているように，セキュリティ対策は単純に発生確率の高い脅威に対して行うだけでは不十分で，対策によって期待損失がどれくらい減少するかを尺度として決定しなければならない．そこで，選択された対策の組合せごとに，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．

### 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

$$\sum_k V_k \tag{1}$$

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．逆にいえば，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 $A_k$ を脅かすすべての脅威（資産 $A_k$ に対して $E_{jk} = 1$ であるすべての脅威 $T_j$）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 $E_{jk} = 1$ であるすべての脅威 $T_j$ が一定期間のうちに発生しない確率は

$$\prod_j (1 - E_{jk}P_j)$$

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

$$V_k \prod_j (1 - E_{jk}P_j)$$

となる．よって，残存するすべての資産の総和である残存資産の期待値は

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

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 $CM_i$ 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 $CM_i$ 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 $CM_i$ の選択，$S_i = 0$ により対策 $CM_i$ 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は $CM_i$ だけではなく，すべての対策 $CM_i$ $(1 \leq i \leq I)$ 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 節で述べたように，対策の相関関係は考慮の対象から外すことにし，各対策による効果が単純に相乗されると仮定するならば，すべての対策の選択/非選択により，脅威 $T_j$ に関する攻撃の成功率は

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

だけ減少する．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

---

☆ たとえば，2 つの資産 $V_1$，$V_2$ に対し，$V_1$ にのみ影響する脅威 $P_1$（すなわち $E_{11} = 1$，$E_{12} = 0$）と，$V_1$，$V_2$ の両方に影響する脅威 $P_2$（すなわち $E_{21} = 1$，$E_{22} = 1$）があった場合，すべての残存資産の「期待値」とは「($P_1$ と $P_2$ がともに発生しない場合の残存資産 ) $\times (1 - P_1)(1 - P_2)$+ ($P_1$ のみが発生した場合の残存資産 ) $\times P_1(1 - P_2)$+ ($P_2$ のみが発生した場合の残存資産 ) $\times (1 - P_1)P_2$+ ($P_1$ と $P_2$ がともに発生した場合の残存資産 ) $\times P_1P_2$」と定義される．$P_1$ が発生すると $V_1$ が失われ，$P_2$ が発生すると $V_1$ と $V_2$ の両方が失われるので，この式はすなわち，

$$(V_1 + V_2)(1 - P_1)(1 - P_2) + (0 + V_2)P_1(1 - P_2) + (0 + 0)(1 - P_1)P_2 + (0 + 0)P_1P_2$$

である．これを式変形すると

$$V_1(1 - P_1)(1 - P_2) + V_2(1 - P_2)$$

となり，式 (2) に一致することが確かめられる．

われる確率は

$$P_j \prod_i (1 - R_{ji} S_i) \quad (3)$$

となる．

これは，対策により式 (2) の中の “$P_j$”（より正確には “$P_j \times 1$” であり,「対策が施されていない場合は，脅威が発生したら，その攻撃は確率 1 で成功する」ということを示している）が式 (3) に変化する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 $CM_i$ 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．

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

### 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ほかならない．よって，対策選択問題は式 (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

$$\sum_i C_i S_i \quad (5)$$

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，セキュリティ対策選択問題は

$$\sum_k \left\{ V_k \prod_j \left[ 1 - E_{jk} P_j \prod_i (1 - R_{ji} S_i) \right] \right\} - \sum_i C_i S_i \quad (6)$$

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

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

なる制約条件の下で式 (6) 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．

## 5. 本手法の実システムへの適用

4 章に示した本対策選択手法に対し，実際の組織やシステム（以下，実システムと示す）を例にとり，実用性の検討を行う．ここでは,「ランク値付きマトリクス表利用リスク分析方法[17]」を応用したリスク分析を行い，専門家が勘と経験により対策を決定した実システムを使用する．まず本章で，この実システムのセキュリティ対策を本手法により選定する流れを説明する．そして次章で，本手法により選択された対策と専門家が実際に選択した対策を比較，検討し，本手法の実用性を評価する．

**表 3** リスク分析結果
Table 3 Risk analysis.

| 資産 | 場所 | 脅威 | 脆弱性 | 資産価値 | 脅威のレベル | リスク値 |
|---|---|---|---|---|---|---|
| ソフトウェア | コンピュータ/可搬型媒体 | 内部者の悪意または過失によるコピーなど | 教育の不足 | 5 | 高 | 7 |
| | | | 新入社員におけるセキュリティモラルの不足 | | 高 | 7 |
| | | | ⋮ | | ⋮ | ⋮ |
| ソフトウェア | コンピュータ/可搬型媒体 | ウイルスの感染 | ウイルス対策ソフトウェア及び管理策の不備 | | 高 | 7 |
| ソフトウェア | 可搬型媒体 | 内部者の悪意または過失による持ち出し | 媒体の持ち出し管理策の不備 | | 高 | 7 |
| ソフトウェア | 可搬型媒体 | 媒体の盗難 | 媒体の保管管理策の不備 | | 中 | 6 |
| | | | 第三者アクセスに関するセキュリティ管理の不備 | | 低 | 5 |
| ソフトウェア | 可搬型媒体 | 媒体の拾得 | 媒体の廃棄管理策の不備 | | 中 | 6 |
| ⋮ | ⋮ | ⋮ | ⋮ | | ⋮ | ⋮ |

### 5.1 実システムに対する対策選定

まず，この実システムに対するリスク分析の結果を**表 3** に示す．ただし，実際の組織やシステムにおいて，リスク分析や対策結果を公表することはありえない（当該組織・システムの弱点を公表することに等しいため）．本研究では，この組織より，リスク分析自体を公表しないこと，公表する評価結果からその組織が推定できないことなどを条件にリスク分析表の提供を受けた．このため表 3 は実際の分析表のごく一部のみを示すことしかできないが了承されたい．

次に，これを表 1 および表 2 の形に変換する．そ

**表 4** 実システムにおける資産と脅威の表
Table 4 Table for threats and assets in a real system.

| 脅威 $T_j$ | | 脅威の発生確率 $P_j$ | 資産（電子情報）$A_k$ | | | |
|---|---|---|---|---|---|---|
| | | | 1 | 2 | 3 | ··· |
| | | | PC 上の電子情報 | 可搬型媒体の電子情報 | 通信ケーブル上の電子情報 | ··· |
| 資産の価値 $V_k$（万円） | | | 15,000 | 500 | 50 | ··· |
| 1 | 内部者の悪意または過失による漏洩・改ざん・破壊，持ち出し，切断 | 0.5 | 1 | 1 | 1 | ··· |
| 2 | ウイルス対策ソフトウェア及び管理策の不備 | 0.5 | 1 | 1 | 0 | ··· |
| 3 | PC の無許可使用による不正アクセス | 0.3 | 1 | 1 | 0 | ··· |
| 4 | 内部ネットワークからの PC への侵入による不正アクセス | 0.3 | 1 | 0 | 0 | ··· |
| 5 | PC の盗難 | 0.3 | 1 | 0 | 0 | ··· |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ··· |

の際，ランク値付きマトリクス表においては，本手法で必要となる種々のパラメータが定量化されていないため以下の工夫を行った．

(1) **情報資産額（$V_k$）**
この組織では，おおよその資産額を 5 段階で評価（1〜100 万円，101〜1,000 万円，1,001〜5,000 万円，5,001 万〜1 億円，1 億円以上）していたので，それぞれの段階の中間値を資産額とした．なお，最上位の額は下限の 1.5 倍（1.5 億円）とした．

(2) **脅威の発生確率（$P_j$）**
この組織では，3 段階評価（高，中，低）を行っていたため，それぞれの発生確率を 0.5，0.3，0.1 とした．

(3) **対策（$CM_i$）**
ECOM の「情報セキュリティ対策マネジメント標準（JIS5080:ISO/IEC 17799）の解説」[18] をもとに現状で考えうる対策を列挙した．ただし，簡単化のために，組織的な活動により実現できる対策は優先的に実施されているものとして削除した．結果として，38 個の対策案があげられた．

(4) **対策コスト（$C_i$）**
この組織では，対策コストの見積りは行っていなかった．そのため，この組織が実際に対策を行っている施策についてはその実コスト，行っていない施策については一般的なコスト（製品，ランニングコストの合計）を調査し，各対策のコストとした．

(5) **リスク減少率（$R_{ij}$）**
この組織の対策選定を実施した設計者からのヒアリングを通して，38 個すべての対策の各脅威に対するリスク減少率を 5 段階（効果の度合い：大，中，小，関連あり，関連なし）で評価し，それぞれ 0.7，0.5，0.3，0.1，0 とした．

以上の定量化により得られた「資産と脅威の表」（表 1 に対応）を**表 4** に，「脅威と対策の表」（表 2 に対応）を**表 5** に示す．

### 5.2 本手法による対策の選定

表 4 および表 5 から 4.3 節の式 (6) における具体的な値がすべて求まるので，これを解けば対策が選定されることになる．

なお，式 (6) は，離散最適化問題であるので，対策数が増えてくると組合せが爆発的に増加し，総当たりで最適解を導出することはできない．そこで本論文では，ヒューリスティックな解法（Trade-off value の考え方に基づく手法[19]）によって準最適解を計算している．また，実際の組織やシステムにおいては各々に固有な制約が付加されることも多いが，それら個々の「お家の事情」は定式化が困難であるため，本手法は単純に費用対効果を最大にするように設計されている．以上より本手法によって選択される対策は完全には最適解ではないかもしれない．しかし本論文は，対策選定に関する厳密な手法を導く前に，まずはある程度の実用に耐えうる簡易な手法を開発することを第 1 の目的としている．よって，本手法により選択された対策と専門家の「勘と経験」により選択された対策との比較から，本手法の実用性を測ることにより，本手法を評価することとする．

## 6. 本手法の実用性に関する評価

### 6.1 対策の選択結果

5 章の実システムにおいて，専門家が勘と経験により実際に決定した対策と，5.2 節で本手法により選定された対策を比較することにより，本手法の実用性を検証する．

今回の例では 5.1 節に示したように，ECOM の「情

**表 5** 実システムにおける脅威と対策の表
Table 5 Table for threats and countermeasures in a real system.

| 脅威 $T_j$ | | 脅威の発生確率 $P_j$ | 対策案 $CM_i$ 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | … |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | セキュリティ情報の共有 | 緊急対応 | 社員教育・啓蒙 | | 入退出管理対策 | | | | |
| | | | 情報提供サービスの利用 | インシデントレスポンスチーム設置 | 外部による研修の実施 | WBTや関係書籍の配付と自己研修 | 監視カメラの設置 | 監視員の派遣 | IC カードによる入退出管理装置導入 | 生体情報による入退出管理装置導入 | … |
| JIS5080 の要求事項との関連項目 | | JIS5080 の章，節 | 4.1 | 4.1 | 6.2 | 6.2 | 7.1 | 7.1 | 7.1 | 7.1 | … |
| | | 項目名 | 情報セキュリティ基盤 | 情報セキュリティ基盤 | 利用者の訓練 | 利用者の訓練 | セキュリティの保たれた領域 | セキュリティの保たれた領域 | セキュリティの保たれた領域 | セキュリティの保たれた領域 | … |
| 対策コスト $C_i$（円） | | | 36 | 2,400 | 100 | 50 | 220 | 1,200 | 200 | 500 | … |
| ソフトウェア資産 | 内部者の悪意または過失によるコピー | 0.5 | 0 | 0.1 | 0.5 | 0.3 | 0 | 0 | 0 | 0 | … |
| | ウイルスの感染 | 0.5 | 0.5 | 0.3 | 0.3 | 0.1 | 0 | 0 | 0 | 0 | … |
| | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |

**表 6** 対策の選択結果
Table 6 Comparison of measure selection results.

| | 従来の方法 | 本手法 |
|---|---|---|
| 総資産価値（万円） | 54,150 | |
| 無対策時被害額（万円） | 41,124 | |
| 全対策案数（個） | 38 | |
| 採用対策数（個） | 21 | 21 |
| 合致対策数（個） | 18 | |
| 非合致対策数（個） | 6 | |
| 総対策コスト（$C$）（万円） | 3,766 | 4,666 |
| 残存資産価値（$RA$）（万円） | 38,991 | 40,950 |
| 対策効果（$RA - C$）（万円） | 35,225 | 36,284 |

報セキュリティ対策マネジメント標準の解説」に基づいて，主に物理的，技術的な対策案が 38 項目あげられている．その中からどの対策が実際に選択されたかについて，従来の方法（勘と経験による選択）と本手法を比べ，結果をまとめたものが**表 6** である．ここで,「採用対策数」とは,「全対策案数」38 項目中，従来の方法と本手法によりそれぞれ選択された対策の総数である.「合致対策数」は，選択された対策のうち，従来の方法でも本手法でも選択された対策の総数である.「非合致対策数」は，選択された対策のうち，従来の方法または本手法のいずれかでしか選択されていない対策の総数である．また,「総資産価値」は式 (1),「残存資産価値」は式 (4),「総対策コスト」は式 (5),「対策効果」は式 (6) のそれぞれの値である.「無対策時被害額」は何の対策も講じない場合の予想被害額，すなわち，何の対策も講じない場合の残存資産価値を総資産価値から引いたものである．

本手法の評価尺度を便宜的に下記のとおり設定する．

$$\text{適度率} = \frac{\text{合致対策数}}{\text{合致対策数} + \text{非合致対策数}}$$

本評価結果では，$18/24 = 75\%$ となった．

非合致対策項目を個別に調べたところ，以下が判明した．

(1) 本手法では選択しなかったが従来の方法では採用されている対策（3 項目）
- **ファシリティセキュリティ（2 重ドア，居室分離など）**：この組織はある理由から費用対効果を度外視して本施策を導入し，セキュリティ強化を行っていた（実際,「対策効果（$RA - C$）」の値は本手法の選択結果の場合のほうが大きい）．
- **IDS の導入**：同上．
- **配線の埋め込み**：ファシリティ上，対策の

実施がきわめて容易であるため，この組織では採用された．

(2) 本手法では選択したが従来の方法では採用されなかった項目（3 項目）

- **サーバ上のデータの暗号化**：導入の検討はされたが使い勝手の低下が発生すると考えられたため，この組織では採用を見送った．
- **生体情報による入退出管理**：同様な効果がある他の対策（IC カードゲート装置の導入）を選択したため，この組織では不要であると判断された．
- **監視員による入退出管理**：同上．

本手法と従来の方法（勘と経験による方法）との適合性が 75%であり，また選択が合致しなかった項目については，乖離の理由がおおむね説明できるものであるため，本手法の実用性は決して低くないと考えられる．

また，本手法を用いれば，従来の方法により選ばれた対策に対してもその対策コストおよび残存資産価値を定量的に把握することが可能であり，この意味でも本手法の実用が見込まれる．

なお，文献 14) でセキュリティ対策のコスト（投資）は「何の対策も講じない場合の予想被害額」の $1/e$（約 37%）以上になることはないということが述べられているが，本手法によるセキュリティ対策の選択結果はこれを満足している（表 6 の「総対策コスト」の値が「無対策時被害額」の値の $1/e$ 以下となっている）．

### 6.2 パラメータの特性

ランク値付きマトリクス表から表 4，表 5 を起こす際には，5.1 節で示したとおり，情報資産額（$V_k$），脅威の発生確率（$P_j$），対策（$CM_i$），対策コスト（$C_i$），リスク減少率（$R_{ji}$）を定量的化する必要がある．

このうち $V_k$，$P_j$ は組織・システムのリスク分析の際にある程度の目安が示されるので，その値に応じて機械的に定量化することは可能である．また，$CM_i$，$C_i$ は，ECOM の「情報セキュリティ対策マネジメント標準」などを利用して，すべての対策案を列挙し，各対策のコストを一度だけ調査すればよい（さらには，ある対策のコストをいったん，調査したなら，それはおおむね他の組織・システムの対策選定の際にも再利用可能であろう）．

$R_{ji}$ については，数値的な裏付けが最も困難であり，多くの評価を実施し，経験的な数値を導く必要がある．ただし，いったんある対策の $R_{ji}$ が定まったなら，この値は，他の組織・システムの対策を選定する際にも再利用することができると思われる．

**表 7** もう 1 つの実システムにおける対策の選択結果
Table 7 Comparison of measure selection results 2.

| | 従来の方法 | 本手法 |
|---|---|---|
| 総資産価値（万円） | 60,000 | |
| 無対策時被害額（万円） | 56,700 | |
| 全対策案数（個） | 38 | |
| 採用対策数（個） | 16 | 22 |
| 合致対策数（個） | 16 | |
| 非合致対策数（個） | 6 | |
| 総対策コスト（$C$）（万円） | 2,791 | 4,561 |
| 残存資産価値（$RA$）（万円） | 22,787 | 29,489 |
| 対策効果（$RA - C$）（万円） | 19,996 | 24,928 |

### 6.3 もう 1 つの実システムでの選択結果

先の結果が従来の方法と本手法の適度率が偶然一致した特殊ケースではないことを確かめるために，先の組織とは業界の異なる，もう 1 つの実際の組織のセキュリティ対策についても同様の評価を行った．

資産や組織規模，ファシリティが異なるため，資産額（$V_k$），対策コスト（$C_i$）は先の実システム評価と異なっているが，脅威の発生確率（$P_j$），対策（$CM_i$），リスク減少率（$R_{ji}$）のパラメータの定量化については 5.1 節と同一の方法を用いて評価した．

ここでは，結果のみ**表 7** に示す．

6.1 節で導入した適度率は，本評価結果については $16/(16+6) = 73\%$ となり，先の実システムとほぼ同様に本手法の実用性が確認できる結果を導くことができた．

## 7. 今後の課題

### 7.1 脅威および対策案の相関関係

3.3 節で述べたように，複数の脅威が合わさって初めて発生するリスクや，類似の対策が選択された際の対策効果の実効性，相補的な対策が選択された際の相乗効果などの，脅威や対策の各項目間の相関関係については，本論文のモデルでは対象から外している．実システムにおける本手法と従来の方法（勘と経験による方法）との比較・評価を行った結果，本モデルにより定式化された本手法の実用性は決して低くないことを確認することはできた．しかし，6.1 節で本手法と従来の方法の乖離要因を解析した結果，脅威や対策の各項目の相関関係（たとえば，6.1 節 (2) で考察したように，IC カード/生体情報/監視員による入退出管理は同様の効果があり，いずれかを採用すれば，他を併用する必要性は低い，など）の考慮を加えることにより，さらに本手法を実効的なものに改善することができると期待される．

### 7.2 資産や対策の適正な評価

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，対策の効果なども数値で示すのは難しいと考えられる．だが 6.2 節で述べたように，一度ある対策の効果が数値的に評価できれば，その値は再利用可能であると考えられる．

### 7.3 資産や対策の時間的変化

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．さらに，ある脅威によりシステムが停止してしまった場合，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．

また，対策の効果も時間的に変化する．たとえば暗号は，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，対策として「セキュリティ教育」をあげたとすると，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．

### 7.4 コスト以外の選択基準項目の存在

実システムでは様々な理由で費用対効果を度外視した対策も存在するのだが，これらをどのように扱うかという問題がある．しかし，これらについては本手法を適用する前に対策の決定をしておけばよい（そのような対策は前もって採用を確定させておき，本手法を適用する）ので大きな問題とはならないと思われる．

### 7.5 ユーザの利便性や製品の成熟度の考慮

実施すべきセキュリティ対策を決定しても，ユーザがこれを遵守しなければ，机上の空論となる．各セキュリティ対策がユーザの利便性を大きく低下させてしまう場合などには，ユーザはその対策を実際に実施しようとしないだろう．同様に，セキュリティ対策用製品の成熟度もこれに起因すると思われる．これらに対処するためには，各対策の効果を数値化する際に，ユーザの利便性や製品の成熟度に関しても考慮する必要があるのではないかと考える．

## 8. ま と め

本論文では，資産・脅威・対策の関係をモデル化し，セキュリティ対策選択問題を定式化することにより，対策の最適な組合せを論理的に求める手法を導出した．本手法によれば，セキュリティ対策選択問題は離散最適化問題として定式化される．そしてさらに，実システムにおいて開発者が実際に選択したキュリティ対策と本手法による対策の選定結果を比較・検討し，いくつかの課題は残るものの，本手法が基本的には実用上問題ない性能を有することを確認した．本手法を利用することにより，これまで定性的にしか示されなかったセキュリティ対策の費用対効果を，「対策効果（$RA - C$）」という実際の数値として示すことが可能となった．

## 参 考 文 献

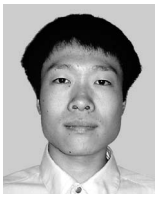

1) ISO: ISO/IEC 17799. http://www.iso.ch/
2) ISO: ISO/IEC TR 13335 1-5. http://www.iso.ch/
3) ISO: ISO/IEC 15408 1-3. http://www.iso.ch/
4) IPA セキュリティセンター：情報セキュリティの現状 2001 年版 (1995). http://www.ipa.go.jp/security/fy13/sec2001/sec2001.pdf
5) JIPDEC: 情報セキュリティマネジメントシステム（ISMS）合性評価制度. http://www.isms.jipdec.or.jp/
6) JIPDEC: ISMS 認証取得事業者一覧. http://www.isms.jipdec.or.jp/lst/ind/
7) 日経 BP コンサルティング，コンピュータ・アソシエイツ社：企業の情報セキュリティに関するアンケート—報告 (2003). http://www.caj.co.jp/etrust/research/
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 (2002). http://www.jnsa.org/policy/guidance/
9) 小熊慶一郎，中村逸一，西尾秀一，土屋茂樹，坂田祐司，菅野政孝，曽根岡昭直：組織間情報流通へのPOLICYCOMPUTING アーキテクチャ適用の検討，電子情報通信学会技術研究報告（ISEC2000-50），Vol.100, No.213, pp.195–202 (2000).
10) 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, pp.13–18 (2003).
11) 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，Vol.2002, No.16, pp.71–76 (2002).
12) McCammon, K.W.: Calculating Loss Expectancy. http://mccammon.org/articles/loss_expectancy.php
13) 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.1, pp.475–480 (2003).
14) Gordon, L.A. and Loeb, M.P.: The Eco-

nomics of Information Security Investment, *ACM Trans. Information and System Security*, Vol.5, No.4, pp.438–457 (2002).
15) 永井康彦，藤山達也，佐々木良一：セキュリティ対策目標の最適決定技法の提案，情報処理学会論文誌，Vol.41, No.8, pp.2264–2271 (2000).
16) 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, pp.2435–2446 (2002).
17) 佐々木良一，内田勝也，岡本栄司，菊池浩明，寺田真敏，村山優子（編）：情報セキュリティ事典，pp.618–632, 共立出版 (2003).
18) 電子商取引推進協議会（ECOM）：情報セキュリティ対策マネジメント標準（JIS5080:ISO/IEC 17799）の解説 (2002). http://www2.ecom.jp/report/pdf/H13/h13_security2.pdf
19) Schwartz, M.: *Computer-Communication Network Design and Analysis*, pp.171–192, Prentice-Hall (1997).

(平成 15 年 12 月 4 日受付)
(平成 16 年 6 月 8 日採録)

**中村 逸一**（正会員）

昭和 60 年茨城大学工学部卒業．昭和 62 年同大学大学院修了．同年日本電信電話株式会社入社．LAN システムの研究に従事．平成 8 年より（株）NTT データにてセキュリティ技術の研究・開発に従事．現在，同社ビジネス開発事業本部企画部部長．



**兵藤 敏之**

平成 14 年静岡大学情報学部情報科学科卒業．平成 16 年同大学大学院修士課程修了．同年中部テレコミュニケーション株式会社入社．現在，同社岡崎事業所に勤務．在学中，情報セキュリティに関する研究に従事．

**曽我 正和**（正会員）

昭和 33 年京都大学工学部電子工学科卒業．昭和 35 年同大学大学院修士課程修了．昭和 35 年〜平成 8 年三菱電機，計算機製作所副所長，情報電子研究所所長を経て平成 8 年静岡大学情報学部教授，平成 11 年岩手県立大学ソフトウェア情報学部教授，現在に至る．博士（工学）（東京大学）．汎用計算機，制御用計算機，制御用システムの開発．フォールトトレラントシステム，セキュリティシステムに関する研究に従事．IEEE，電子情報通信学会会員．

**水野 忠則**（正会員）

昭和 20 年生．昭和 43 年名古屋工業大学経営工学科卒業．同年三菱電機（株）入社．平成 5 年静岡大学工学部情報知識工学科教授，現在，情報学部情報科学科教授．工学博士．情報ネットワーク，モバイルコンピューティング，放送コンピューティングに関する研究に従事．著書としては『プロトコル言語』（カットシステム），『コンピュータネットワーク概論』（ピアソン・エデュケーション）等がある．電子情報通信学会，IEEE，ACM 各会員．当会フェロー．

**西垣 正勝**（正会員）

平成 2 年静岡大学工学部光電機械工学科卒業．平成 4 年同大学大学院修士課程修了．平成 7 年同大学院博士課程修了．日本学術振興会特別研究員（PD）を経て，平成 8 年静岡大学情報学部助手．平成 11 年同講師，平成 13 年同助教授．博士（工学）．情報セキュリティ，ニューラルネットワーク，回路シュミレーション等に関する研究に従事．