機能的適合性を考慮した情報システムのセキュリティ基本設計法の提案

永井康彦[†] 藤山達也[†]
荒井正人[†] 柚原直弘[††]

情報システムが社会基盤として活用されてきている現在，基本設計の段階から適切なセキュリティ対策を施しておくことが，情報システムに対する必須の前提条件となってきている．その対策は，情報システムが置かれる環境に想定される脅威に対して，コスト対効果の高いものであることが要求される．そこで，第1著者らは，脅威対抗策としての必要十分性と必要コストの観点から，セキュリティ対策目標を定量的に決定するためのセキュリティ対策目標最適決定技法をすでに提案した．しかしながら，対策目標の実現方式には，多数の候補が存在する場合がある，目標と実現方式とは概念が異なる，ことから，それらは必ずしも1対1対応ではなく，対応関係にあいまいさがある．そのため，対策目標に対する実現方式の適合性や現存の実現方式の機能的満足度などの指標も考慮して，対策目標を合理的に決定することが必要となる．本論文では，対策目標を現存の実現方式の機能的適合性も考慮して決定するセキュリティ基本設計法を提案する．本法は，脅威に関する複数の Fault Tree の相対正規化重要度計算とファジイ関係を用いた適合度計算に基づいて，対策目標に対して機能的に適合する実現方式を決定できるように，すでに提案した技法を拡張したものである．これにより，コスト対効果の高い対策目標とその実現方式を決定することができ，知識や経験が十分でない設計者にも，一連のセキュリティ基本設計過程の支援が可能となる．

A Proposal of Basic Security Design Method Based on Functional Suitability for Information Systems

Yasuhiko Nagai,[†] Tatsuya Fujiyama,[†] Masato Arai[†]
and Naohiro Yuhara[††]

For establishment of systematic information security countermeasures, the production of security objectives and security specification has become more important in basic security design. However, it is difficult to define the security objectives and security functions effectively and efficiently on complex mapping relationships between threats and objectives, and between objectives and functions. In this paper we propose a basic security design method. The method provides the ability to determine the security objectives and the security functions quantitatively from the viewpoint of effectiveness and efficiency. The method consists of two schemes. One is derivation scheme of security objective candidate sets for protection from possible threats by applying minimal path set on the fault trees (FT) with respect to the threats. The other is decision scheme of optimal security objectives and functions by calculating the functinal suitability using fuzzy relation and resolving the combinational optimization problem. Furthermore, we will show the validity of the method in a case study.

1. はじめに

情報システムの社会基盤としての活用が拡大されるにともない，プライバシー情報や企業機密情報の漏洩や改ざん，取引否認などの情報セキュリティに関する脅威が，社会的に大きな影響を及ぼすものになっている．このため，情報システムの基本設計の段階から，適切なセキュリティ対策を施しておくことが必須の前提条件となってきている．このことは，1999年6月に情報システムに関する国際セキュリティ評価基準 ISO/IEC 15408[1)]が標準化され，2000年7月には日本工業規格 JIS X 5070 として規格化されたことにも現れている．本基準は，情報関連製品やシステムの調達基準，システム相互接続基準，法制度上の要件等として活用される見込みであり，今後の情報関連製品・システム開発において，本基準でのセキュリティ設計・

† 株式会社日立製作所
Hitachi, Ltd.
†† 日本大学理工学部
Nihon University

開発と評価・認証取得がビジネス上や運用上の前提条件となる．

ところで，ISO15408 の認証取得のためには，評価対象製品やシステムのセキュリティ基本設計書（ST；セキュリティターゲット）[2]を作成することが必須の要件となる．ST とは，国際標準で形式や使用用語が統一された，セキュリティに特化した情報システムの基本設計書である．評価対象の概要，評価対象が利用される環境（前提，脅威，組織のセキュリティポリシ）の定義，環境からの脅威等への対抗としてのセキュリティ対策目標やセキュリティ要件の定義，セキュリティ要件の実現方式を記述したドキュメントである．開発者は，ST をまず作成し，これを基に以降のセキュリティを含む機能設計や詳細設計などを順次行うこととなる．このため，ST 作成は，情報製品やシステムのセキュリティ設計の基盤となる重要なものである．特に，ST を作成する際，その中のセキュリティ対策目標の設定は，情報システムが置かれる環境に想定される脅威に応じた，コスト対効果の高いものとすることが肝要である．

しかしながら，これまで，体系的なセキュリティ基本設計法は確立されていないため，セキュリティ対策目標の設定は，設計者である人間の経験やノウハウに依存しているのが現状である．また，その存在が想定される脅威とそれらの脅威に対抗する対策目標との複雑な対応関係のもとで，対策すべき脅威をすべて網羅でき，コスト対効果を考慮した対策目標を設計者が決定することも困難な作業となる．さらには，現状では，豊富な知識や経験を有するセキュリティ設計者が少ないため，情報システムのセキュリティ設計は，ウィルス対策やファイアウオールの設置などの個別的対策の実施にとどまりがちである．そのため，入退出管理やシステム監査機能などの体系的に必要となるセキュリティ機能が不足したり，逆に，必要もないにもかかわらず，必須アクセス制御機能などの強固なセキュリティ機能を設けて，かえって機能過剰による運用のしにくさやコスト増を招いたりしている場合がある．

セキュリティ基本設計を支援する方法としては，ETA（Event Tree Analysis）/ FTA（Fault Tree Analysis）手法を情報システム向けに改良したリスク分析手法[3]やセキュリティ対策目標を立案するための計画手法[4]が提案されているが，それらは，セキュリティ対策目標の策定方法については言及していないものであったり，必要コストの観点での評価がなかったりするなど，コスト対効果を十分考慮してセキュリティ対策目標を策定するものになっていないという問題があった．

このことから，第 1 著者らは，これまでに，コスト対効果の高いセキュリティ対策を実現するためのセキュリティ対策目標の最適決定技法[5]を提案している．その概略は次のようである．まず，各脅威に関する FT（Fault Tree）を作成し，脅威を抑止する必要最小限の基本事象の組合せ（ミニマルパスセット[6]）を特定する．次に，各パスセット内の基本事象を抑止するセキュリティ対策目標候補を定義することで，脅威対抗に必要最小となる対策目標候補集合群を導出する．そして，この候補集合群の中から，対象脅威のすべてに対抗でき，かつ対策目標の必要コスト総和を最小化する最適対策目標を組合せ最適化問題を解くことにより決定する．

しかしながら，対策目標の実現方式（セキュリティ機能や運用管理策）は，多数存在する場合がある，目標と実現方式とは概念が異なる，ことから，それらは必ずしも 1 対 1 対応ではなく，対応関係にあいまいさがある．そのため，対策目標に対する実現方式の適合性や現存の実現方式の機能的満足度などの指標を考慮して対策目標を合理的に決定することが必要とされる．しかし，既提案の技法は，対策目標候補に対する特定の実現方式を想定し，その必要コストのみの観点で最適対策目標を決定するものであり，上記要件には応えうるものではなく，また実現方式が対策目標をどの程度達成できるかも含めて，よりコスト対効果の高い対策目標を決定できるものではなかった．

本論文では，対策目標を現存の実現方式の機能的適合性も考慮して決定するセキュリティ基本設計法を提案する．本法は，各脅威に対するそれぞれの FT のリスク値の相対値を重みとした個別 FT における各基本事象の相対重要度計算と複数 FT の各基本事象の相対重要度を 5 段階の数値表現とする相対正規化重要度計算，対策目標対実現方式のファジイ関係を用いた機能適合度計算[7]により，対策目標に対して機能的に適合する実現方式を決定できるように，すでに提案した技法[5]を拡張したものである．これにより，コスト対効果の高いセキュリティ対策目標とその実現方式を決定することができ，知識や経験の十分でない設計者に対しても，一連のセキュリティ基本設計過程の支援が可能となる．以下，2 章ではセキュリティ基本設計法を示し，3 章では具体例で既提案の方法と本法との比較検討を行い，それによって本法の有効性を示す．

2. セキュリティ基本設計法

2.1 概　　要

本法は，**図 1** に示すように，セキュリティ対策目

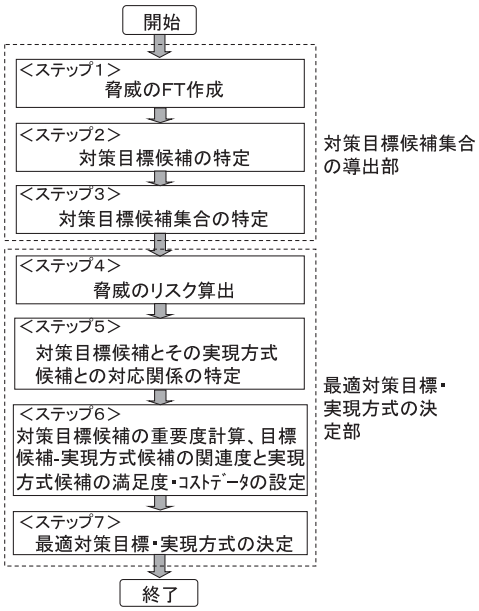

図 1 最適対策目標・実現方式決定手順
Fig. 1 Procedure of optimal security objectives and specification decision method.

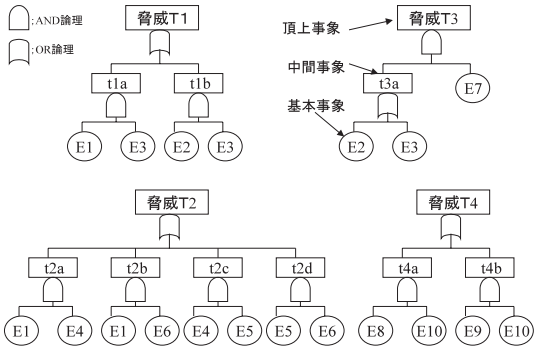

図 2 フォルト・ツリー（FT）例
Fig. 2 Examples of fault tree.

表 1 基本事象と対策目標候補の対応関係例
Table 1 An example of relationship between basic events and security objective candidates.

脅威	基本事象	対策目標候補
T1	E1	o1
	E2	o2
	E3	o3
T2	E1	o1
	E4	o4
	E5	o5
	E6	o6
T3	E2	o2
	E3	o3
	E7	o7
T4	E8	o8
	E9	o9
	E10	o10

標候補集合の導出部，最適セキュリティ対策目標・実現方式の決定部から構成される．本法は，既提案のセキュリティ対策目標の最適決定技法[5]にステップ 5〜6 を追加し，ステップ 7 を最適実現方式を決定できるよう拡張したものである．本法への入力データとしては，従来手法により抽出される，情報システムが適用される環境に対して想定される脅威一覧を用いる．

2.2 セキュリティ対策目標候補集合の導出方法

セキュリティ対策目標候補集合の導出は，以下のステップを順に実施することで行われる．

＜ステップ 1＞脅威の FT 作成

入力データとなる脅威一覧における各脅威を頂上事象とし，その頂上事象が生起する因果関係を演繹的にツリー表現した脅威の FT 図を，各々の脅威ごとに作成する．たとえば，脅威一覧として $T1$〜$T4$ の 4 つの脅威が想定される場合，**図 2** に示すような 4 つの FT が作成されることとなる．

＜ステップ 2＞対策目標候補の特定

作成された FT 図の基本事象を抑止することが脅威への対抗であることから，各基本事象の生起を抑止する対策をセキュリティ対策目標候補として定義し，それらを特定する．先の FT 例の場合，たとえば**表 1** のような形で，各 FT ごとの基本事象に対する対策目標候補が特定されているとする．ここで，説明の簡略化のために，各基本事象に対して対策目標候補を 1 つずつ対応づけているが，複数対応づけられる場合もある．また対策には，技術的対策，運用的対策，両者の組合せによる対策が考えられる．

＜ステップ 3＞対策目標候補集合の特定

ミニマルパスセット探索アルゴリズム[6]を用いて，ステップ 2 で作成した各々の FT のミニマルパスセットを求める．ミニマルパスセットとは，FT の頂上事象（脅威）の生起を抑止するのに必要十分となる基本事象の組合せである．したがって，求められたミニマルパスセットの各組合せに含まれる基本事象を，対応する対策目標候補に置き換えることで，脅威を抑止するのに必要十分な対策目標候補集合が得られることになる．

たとえば，脅威 $T1$ の場合では，$\{E1, E2\}$，$\{E3\}$ の 2 つがミニマルパスセットとなり，それを構成する各基本事象を，対応する対策目標候補に置き換えた {o1,o2}，{o3} が脅威 $T1$ のセキュリティ対策目標候補集合として特定される．

2.3 最適セキュリティ対策目標・実現方式の決定方法

最適セキュリティ対策目標および実現方式の決定は，以下のステップを順に実施することで行われる．

＜ステップ 4＞脅威のリスク算出

各脅威に対する FT に含まれる基本事象それぞれの発生確率データ（回/年）を与え，FT の論理構造に基づく頂上事象発生確率計算式により各脅威の発生確率を計算する．FT の中の 2 カ所以上に同一基本事象が含まれる場合には，確率の計算はブール代数による整理を行った後に実行する．ここで，基本事象の発生確率データは，統計値があればそれを，ない場合には類似事象の統計値などからの推定あるいは対象システムや脅威の攻撃方法を知る専門家の推定による主観値を用いる．これは，主観値でも各脅威のオーダー的なリスク評価が可能であるからである．次に，得られた脅威発生確率にその脅威が発生した場合の予想損失額を影響度（円/回）として掛け算したリスク値を各脅威ごとに算出する．

先の例の脅威 $T1$ の場合，基本事象の発生確率を各々 $P(E1) = 1.0$，$P(E2) = 0.5$，$P(E3) = 0.1$ とすると，脅威発生確率 $P(T1)$ は，以下の計算式により算出されることになる．

$$\begin{aligned} P(T1) &= 1 - (1 - P(E1) \cdot P(E3)) \\ &\quad (1 - P(E2) \cdot P(E3)) \\ &= P(E2) \cdot P(E3) + P(E1) \cdot P(E3) \\ &\quad - P(E1) \cdot P(E2) \cdot P(E3) \\ &= 0.05 + 0.1 - 0.05 = 0.1 \text{ (回/年)} \end{aligned}$$

また，脅威 $T1$ の影響度 $E(T1)$ を 1 億円とすると，リスク値 $R(T1)$ は，以下のように算出される．

$$\begin{aligned} R(T1) &= P(T1) \times E(T1) \\ &= 0.1 \times 100,000,000 \\ &= 10,000,000 \text{ (円/年)} \end{aligned}$$

$P(E4) = 0.1$，$P(E5) = 1.0$，$P(E6) = 0.001$，$P(E7) = 0.36$，$P(E8) = 1.0$，$P(E9) = 0.1$，$P(E10) = 0.1$ とし，同様にして算出した脅威 $T1$〜$T4$ の各リスク値を**表 2** に示す．

＜ステップ 5＞対策目標候補とその実現方式候補との対応関係の特定

各対策目標候補に対して，それを実現できる可能性のある方式案を実現方式候補と定義し，さらにそれらの間の関係を対応関係と定義する．実現方式候補は，対策目標候補の実現手段となる項目レベルのセキュリティ機能や運用管理施策で，具体的項目は過去のセキュリティ設計事例や公開されている事例[8]などを参考にして，項目間に包含関係がないように独立に求める．

表 2 導出データ例
Table 2 An example of data derived.

脅威	発生確率 (回/年)	影響度 (円/回)	リスク値 (円/年)	対策目標候補集合
T1	0.1	1億	1000万	{o1,o2} {o3}
T2	0.1	5000万	500万	{o1,o5} {o4,o6}
T3	0.2	500万	100万	{o2,o3} {o7}
T4	0.01	1000万	10万	{o8,o9} {o10}

この際，各対策目標候補に代替案となる複数の実現方式候補が存在する場合がありうる．また，対策目標と実現方式の関係は，目標–手段，抽象–具体といったように概念や記述レベルが相違していることや，個々の実現方式は設計や構築上の技術的視点から区分された項目単位とされることが多いことから，対策目標と実現方式とは必ずしも 1 対 1 対応とはならず，その対応関係にはあいまいさが存在する．そのため，既提案方法のように対策目標候補に対する特定の実現方式候補のもとで最適な対策目標を決定するのではなく，対策目標候補に対して可能性のあるすべての実現方式候補を明確化し，それらの中から対策目標に対して機能的に最も適合する実現方式が存在する最適な対策目標を，決定することが必要である．そこで，まず本ステップでは，代替案が存在する場合や，1 つの対策目標候補に単独または複数の組合せの実現方式候補が対応する場合，複数の対策目標候補に単独の実現方式候補が対応する場合，複数の対策目標候補に共通となる実現方式候補が対応する場合などの対応関係があることを考慮して，可能性のある実現方式候補をすべて定義するようにしている．対応関係の強さの度合い（関連度，**図 3**）は，次のステップ 6 で他のデータと合わせて設定する．先の例の対策目標候補とそれらの実現方式候補との対応関係を**表 3** に示す．

＜ステップ 6＞対策目標候補の重要度計算，目標候補–実現方式候補の関連度と実現方式候補の満足度・コストデータの設定

［相対正規化重要度の計算］

FT を用いた定量的解析の指標として重要度[6]が定義されている．この重要度とは，FT の各基本事象に対して計算され，FT の頂上事象の生起に関して各基本事象がどの程度寄与しているかを数値化したものである．重要度には，FT の構造のみから計算される構造重要度，基本事象の生起確率の増減が頂上事象の生起確率の増減に寄与する程度も考慮して計算される確

実現方式候補(f)

対策目標候補(o)	f1	f2	f3	f4	f5	f6	f7	f8	f9	f10	f11	f12	f13	f14	f15	f16	f17	f18
o1	1	0.75	0.5	0.5	0	0	0	0	0	0	0	0	0	0	0	0	0	0
o2	0.75	0	0	0	0.5	0.75	0.75	0.75	0	0	0	0	0	0	0	0	0	0
o3	1	0	0	0	0	0	0	0	0.5	1	0.75	0	0	0	0	0	0	0
o4	0	0	0	0	0	0	0	0	0	0	0.75	1	0	0	0	0	0	0
o5	0	1	0	0	0	0	0	0	0	0	0	0	0.25	1	0	0	0	0
o6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.75	0	0	0
o7	0	0	0	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0
o8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
o9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
o10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1

図 3 関連度データ
Fig. 3 An example of degree of relation.

表 3 対策目標候補とその実現方式候補との対応関係例
Table 3 An example of relationship between security objective candidates and specification candidates.

対策目標候補o	実現方式候補fとの対応関係
o1	o1–f1, o1–{f2, f3}, o1–f4
o2	o2–f5, o2–{f1, f6}, o2–{f7, f8}
o3	o3–f9, o3–{f1, f10}, {o3, o4}–f11
o4	o4–f12, {o4, o3}–f11
o5	o5–f13, o5–{f2, f14}
o6	o6–f15
o7	o7–{f5, f9}
o8	o8–f18
o9	o9–f19
o10	o10–f20

[ ]：複数目標対応

率重要度，基本事象の生起確率のパーセント変化が頂上事象の生起確率のパーセント変化に寄与する程度も考慮して計算されるクリティカリティ重要度があり，解析の詳細や目的に応じて選択して使用される．本法でも，脅威の FT の各基本事象の重要度を計算することで，各基本事象に対応する対策目標候補の脅威抑止に対する重要度とする．ただし，一般に重要度は 1 つの脅威の FT に関して計算されるものであるが，本法で扱う情報システムのセキュリティ設計で対象とする脅威は通常複数であり，それにともない脅威の FT も複数となり，それらには共通の基本事象が含まれることもありうる．また，本法で扱う重要度は，以降に述べる対策目標候補と実現方式候補との関連度や実現方式候補の満足度とともに，ステップ 7 における対策目標候補に対する実現方式候補の機能過不足度の計算に用いられる．なお，関連度や満足度を求める際には，それらに関する客観データの入手は困難であり計算も複雑になることから，5 段階の数値で表現された設計者の主観データを基にして機能過不足度をファジイ理論によって計算する方法を用いている．また，機能過不足度計算におけるデータ間の表現の整合をとるため，重要度も 5 段階の数値表現とすることが必要である．そこで，本法では，まず，ステップ 4 で求めた各 FT のリスク値の相対値をとり，それを重みとして個別 FT における各基本事象の相対重要度とする．これによって，複数の FT 全体に関する各基本事象の相対重要度が計算できる．ついで，相対重要度を 5 段階の数値表現とするよう新たに定義した相対正規化重要度を求める．この相対正規化重要度は，以下のような手順で算出される．

① 脅威 k に対する FT の基本事象 i（FT の共通基本事象は同じ i とする）の重要度 $Ik(i)$ を計算 たとえば，構造重要度[6]の場合は次式となる．

$$Ik(i) = n_\phi(i)/2^{in-1}$$

ここで，
in：脅威 k に対する FT の基本事象の総数
$n_\phi(i)$：基本事象 i に対するクリティカルカットベクトル（基本事象 i が生起するとき頂上事象が発生する状態）の総数

② n 個の FT に共通する基本事象がある場合も考慮して，複数 FT に対する基本事象の相対重要度 $TI(i)$ を，脅威 k のリスク値 $R(k)$ の相対値 $w(k)$ を重みとして次式により計算

$$TI(i) = \sum_{k=1}^{n} w(k) \cdot Ik(i)$$

ここで，

$$\sum_{k=1}^{n} w(k) = 1, \quad w(k) = R(k) / \sum_{k=1}^{n} R(k)$$

③ 算出された相対重要度の最大値で各基本事象の相対重要度を割り，切り上げして各基本事象の相対重要度を 0〜1 の 5 段階評価値（0.0，0.25，0.5，0.75，1.0）に正規化する．これを各基本事象の相対正規化重要度 $NI(i)$ とする

先の例の場合，重要度として構造重要度[6]を用いると，手順①による各脅威に対するそれぞれの基本事象の重要度は，

脅威 $T1$；$IT1(E1) = 0.5$，$IT1(E2) = 0.25$，$IT1(E3) = 0.5$

脅威 $T2$；$IT2(E1) = 0.375$，$IT2(E4) = 0.375$，$IT2(E5) = 0.375$，$IT2(E6) = 0.375$

脅威 $T3$；$IT3(E2) = 0.25$，$IT3(E3) = 0.25$，$IT3(E7) = 0.75$

脅威 $T4$；$IT4(E8) = 0.25$，$IT4(E9) = 0.25$，$IT4(E10) = 0.75$

手順②による相対重要度は，$w(T1) = 0.62$，$w(T2) = 0.31$，$w(T3) = 0.06$，$w(T4) = 0.01$ により，$TI(E1) = 0.426$，$TI(E2) = 0.17$，$TI(E3) = 0.325$，$TI(E4) = 0.116$，$TI(E5) = 0.116$，$TI(E6) = 0.116$，$TI(E7) = 0.045$，$TI(E8) = 0.003$，$TI(E9) = 0.003$，$TI(E10) = 0.008$

手順③による相対正規化重要度は，$NI(E1) = 1.0$，$NI(E2) = 0.5$，$NI(E3) = 1.0$，$NI(E4) = 0.5$，$NI(E5) = 0.5$，$NI(E6) = 0.5$，$NI(E7) = 0.25$，$NI(E8) = 0.25$，$NI(E9) = 0.25$，$NI(E10) = 0.25$ となる．

［関連度，満足度，コストデータの設定］

ステップ 5 で決定された対策目標候補と実現方式候補との対応関係（表 3）の強さの度合い（関連度）を，設計者の主観的評価による 5 段階の数値表現（直接対応する：1.0，関連が強い：0.75，関連がある：0.5，少しは関連がある：0.25，関連なし：0.0）で設定する．同様に，各実現方式候補の機能的満足の度合いを 5 段階の数値表現（十分使える：1.0，けっこう使える：0.75，まあまあ使える：0.5，あまり使えない：0.25，まったく使えない：0.0）で評価し，これを満足度として設定する．さらに，各実現方式候補に関して，採用する場合に必要となるコストデータを設定する．

先の例の場合，たとえば，図 3 に示すような関連度データ，**表 4** に示すような満足度およびコストデータが設定される．

＜ステップ 7＞最適対策目標・実現方式の決定

表 4 満足度/コストデータ
Table 4 An example of degree of satisfaction and cost.

実現方式候補	満足度	コスト
f1	1.0	100万円
f2	1.0	50万円
f3	0.75	30万円
f4	0.75	60万円
f5	1.0	10万円
f6	0.25	20万円
f7	0.5	30万円
f8	0.75	70万円
f9	0.5	20万円
f10	1.0	40万円
f11	0.75	50万円
f12	0.5	30万円
f13	1.0	20万円
f14	0.25	60万円
f15	0.5	15万円
f16	1.0	60万円
f17	1.0	100万円
f18	1.0	80万円

対策コストが最小となる最適対策目標と対策目標に最も機能的に適合する（機能過不足度が最小）最適実現方式を，最適対策目標に関する組合せ最適化問題の中に，最適実現方式に関する組合せ最適化問題を含んだ，2 重の組合せ最適化問題を解くことにより決定する．

［最適対策目標決定問題としての定式化］

2.2 節で述べた方法により得られた各セキュリティ対策目標候補を q，目標候補 q の対策コストを $C(q)$，各目標候補の採否を $obj(q)$：1 · · · 採用，0 · · · 不採用とすると，最適対策目標の決定問題は，対抗すべき脅威 k をすべて網羅でき，かつ対策コストの合計が最小となるように q の組合せを選択する組合せ最適化問題となり次のように定式化される．

目標関数：minimize

$$z = \sum_{q=1}^{m} C(q) \cdot obj(q) \tag{1}$$

制約条件：subject to

$$\sum_{k=1}^{n} \left[1 - \prod_{j=1}^{p_k} \prod_{q \in P_{k,j}} obj(q) \right] = 0 \tag{2}$$

$$obj(q) \in \{1, 0\}, \quad (q = 1, 2, \ldots, m) \tag{3}$$

$$R(k) > Ra, \quad (k = 1, 2, \ldots, n) \tag{4}$$

ここで，上記の記号の意味は以下のとおりである．

$C(q)$：対策目標候補 q の対策コスト（円）

m：対策目標候補数

$obj(q)$：目標候補 q を採用するか否かの指示変数 $obj(q) \in \{1, 0\}$, (1 · · · 採用, 0 · · · 不採用)

n：対象脅威数
p_k：脅威 k に対する対策目標候補集合の個数
$P_{k,j}$：脅威 k に対する j 番目の対策目標候補集合
$R(k)$：脅威 k のリスク値（円/年）
Ra：リスク許容値

式 (1) は，総コストが最小となるように対策目標候補の中から適切な対策目標を選択する操作を表す．式 (2) は，選択対策目標が構成する対策目標候補集合により対象脅威のすべてに対する対策が施されるという制約を表している．また，式 (4) は，指定したリスク許容値 Ra 以下のリスクとなる脅威は対策の対象としないことを表す．

［最適実現方式決定問題としての定式化］

前記最適対策目標の決定問題を解く過程での各実行可能解，すなわち採用可能な対策目標候補集合を S_s，S_s に関連する採用可能な実現方式候補集合を F_u，F_u により実現される各目標候補 s の機能的達成度を $mI'(s)$ とすると，最適実現方式の決定問題は，各対策目標の実現を必要条件として各対策目標の重要度（必要度）と実現方式による目標達成度の差分の合計（機能過不足度）が最小となるように実現方式の組合せ F_u を決定する組合せ最適化問題となり次のように定式化される．

目標関数：minimize

$$x = \left(\sum_{s=1}^{t} |mI'(s) - mI(s)| \right) / t \tag{5}$$

制約条件：subject to

$$Q_u \supseteq S_s \tag{6}$$

$$g : 2^{F_u} \to 2^{Q_u}$$

$$Q_u = g(F_u), \quad Q \in 2^Q, \quad F_u \in 2^F \tag{7}$$

$$mI'(s) = \bigvee_{f \in F_u} (mR(s,f) \wedge mF(f)), \quad s \in S_s \tag{8}$$

ここで，上記の記号の意味は以下のとおりである．
F_u：採用可能な実現方式候補集合群 F の u 番目の候補集合
Q_u：F_u により達成できる対策目標候補集合
S_s：実行可能解，すなわち採用可能な対策目標候補集合
s：S_s の対策目標候補
t：S_s の対策目標候補数
f：F_u の実現方式候補
$mR(s,f)$：対策目標候補と実現方式候補間の関連度からなるファジイ関係
$mF(f)$：実現方式候補の満足度からなるファジイ集合

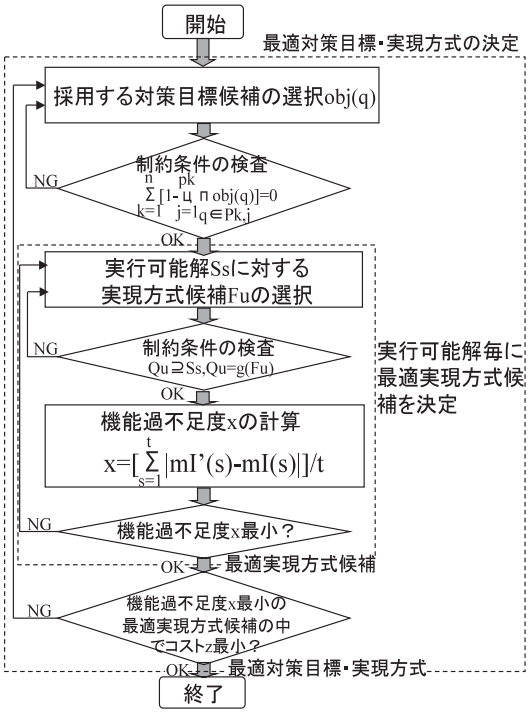

図 4 最適対策目標・実現方式決定処理フロー
Fig. 4 Solving process flow of optimal security objectives and specification decision problem.

$mI(s)$：対策目標候補の重要度からなるファジイ集合
$mI'(s)$：$mF(f)$ を $mR(s,f)$ を用いたファジイ合成演算で写像した，実現方式候補により達成できる対策目標候補の重要度（達成度）

式 (5) は，機能過不足度が最小となるように実現方式候補群の中から適切な実現方式候補を選択する操作を表す．式 (6) は，実行可能解の対策目標候補を，選択実現方式候補によりすべて達成できるという制約を表している．

［最適対策目標・実現方式決定問題の解法］

前述した最適対策目標・実現方式の決定問題は，整数計画問題の厳密解法により求解できる．ここでは変数の値が 0–1 に限定されている問題を扱う代表的な解法である間接列挙法[9]を採用している．

図 4 に本決定問題の求解の処理フローを示す．最適対策目標・実現方式は，最適対策目標を決定する過程で特定される実行可能解ごとに，実行可能解の対策目標に対する機能過不足度を最小とする最適実現方式を特定し，実現方式のコストが最小となる対策目標とその実現方式を特定するという 2 重の最適化問題を解くことで決定される．

なお，一般に整数計画問題の求解の計算量は，整数変数の個数の指数関数的なオーダとなる．本決定問題

の求解の計算量も，2 重の最適組合せ問題となることから，対策目標候補数 $n1$，実現方式候補数 $n2$ とすると，$2^{(n1+n2)}$ の規模となる．このため，対策目標候補数や実現方式候補数が多くなる事例に本法を適用する場合には，高速近似解法を採用することも実用上有効である．

先の例に対して，リスク許容値 $Ra = 100,000$（円/年）を設定した場合，まず制約条件式 (4) により脅威 $T4$ への対策は除外される．次に間接列挙法で求解すると，たとえば，1 つの実行可能解として対策目標候補 {o3,o4,o6,o7} が，その実現方式候補として {f5,f9,f11,f15}，{f5,f9,f12,f15}，{f1,f5,f9,f10,f12,f15} が特定され，その中で機能過不足度が 0.1875 と最小となる {f1,f5,f9,f10,f12,f15} が対策目標候補 {o3,o4,o6,o7} の最適実現方式として決定される．同様に，各実行可能解の対策目標候補に対する最適実現方式を決定する．ついで，それら最適実現方式の中から最終的に対策コストが最小となるものを探査する．その結果，脅威 $T1$〜$T3$ に対する最適対策目標として {o1,o2,o3,o4,o6} が，最適実現方式として {f1,f5,f9,f12,f15} が最適解として決定され，そのときの機能過不足度は 0.05，対策コスト最小値は 175 万円と求められる．

3. 適 用 例

3.1 適用対象

前章で述べたセキュリティ基本設計法の検証と既提案の方法[5]に対して拡張した部分の有効性を示すために，本法を既提案の方法で用いたものと同じ情報システムの例に適用した結果について述べる．適用対象は，IC カードシステムであり，運用時の利用手続き処理をするオペレータを脅威エージェントとした場合の IC カード内データに関する以下のような 3 つの脅威への対策目標や実現方式の決定を範囲とした例である．

(1) $T1$：「端末利用によるユーザデータへの不正アクセス」
(2) $T2$：「端末利用による暗号鍵データへの不正アクセス」
(3) $T3$：「ユーザデータの改ざん否認」

3.2 適用結果

本技法のステップ 1〜ステップ 4 までを実施した結果を**表 5** に示す．たとえば脅威 $T1$ に対しては，ステップ 1 で**図 5** に示すような $E1$〜$E8$ の 8 つの基本事象を持つ FT が作成され，ステップ 2 ではその FT の各基本事象を抑止する対策目標候補として表 5 の脅威 $T1$ の行に示すような候補が特定された．また続くステップ 3 でミニマルパスセットを導出すると，$\{E1, E2, E3, E6\}$，$\{E1, E2, E3, E7\}$，$\{E1, E2, E3, E8\}$，$\{E1, E2, E4, E6\}$，$\{E1, E2, E4, E7\}$，$\{E1, E2, E4, E8\}$，$\{E1, E2, E5, E6\}$，$\{E1, E2, E5, E7\}$，$\{E1, E2, E5, E8\}$ の 9 つのミニマルパスセットが求められ，これらミニマルパスセットの要素の基本事象に対応する対策目標候補への置き換えと重複目標候補や重複目標集合を整理することにより，表 5 に示すような脅威 $T1$ に関する 4 つの対策目標候補集合が特定された．たとえば，対策目標候補 $\{E1, E2, E3, E7\}$ の場合の対策目標候補集合は {o1〜o12} となる．次にステップ 4 で，図 5 の FT の論理構造と基本事象の発生確率データに基づき，以下の計算式により脅威 $T1$ の発生確率 $P(T1)$ が算出された．なお，本例では各基本事象の発生確率データの統計値がない場合であったため，対象システムや攻撃方法を知る専門家の推定による主観値を使用している．

$$\begin{aligned} P(T1) &= 1 - (1 - P(E1))(1 - P(E2)) \\ &\quad (1 - P(E3) \cdot P(E4) \cdot P(E5)) \\ &\quad (1 - P(E6) \cdot P(E7) \cdot P(E8)) \\ &= 1.1E - 2 \text{ (回/年)} \end{aligned} \tag{9}$$

また，脅威 $T1$ のリスク値 $R(T1)$ は，脅威の発生確率と影響度 100 億（円/回）から 1.1 億（円/年）となる．

脅威 $T2$，$T3$ に対しても上述のステップによる計算を行う．以上によって，本例の場合，合計 17 項目のセキュリティ対策目標候補と表 5 に示した 16 個の対策目標候補集合が導出された．

次に，ステップ 5 で，各対策目標候補を実現する実現方式候補として，**表 6** にその一部を示すような 90 個の実現方式候補が特定された．さらに，ステップ 6 で，対策目標候補の重要度計算，対策目標候補―実現方式候補間の関連度定義，実現方式候補の機能満足度および対策コスト定義により，**図 6** に示すデータが設定された．なお，ここで重要度は，FT の論理構造だけでなく，基本事象の発生確率が頂上事象（脅威）の発生確率に寄与する程度や基本事象の発生確率の改善の容易性をも考慮したクリティカリティ重要度[6]を用いている．

最後に，リスク許容値 $Ra = 200$ 万（円/年）としてステップ 7 を実施した結果，コスト $z = 21809$ 万円，機能過不足度 $x = 0.4$ でコスト最小となる最適対策目標と最適実現方式が以下のように決定された．

最適対策目標：o1〜o10
最適実現方式：f1〜f6，f8，f10，f12，f14〜f25，f28〜f35，f37，f38，f40〜f42，f49〜f51，f55〜f60

表 5 脅威のリスク値と対策目標候補集合
Table 5 Risk value for threats and security objective candidate sets.

脅威(頂上事象)					基本事象	対策目標候補		対策目標候補集合
記号	内容	発生確率 (回/年)	影響度 (円/回)	リスク値 (円/年)	(記号)	記号	内容	
T1	端末利用によるユーザデータへの不正アクセス	1.1E−2	100億	1.1億	本人認証ロジックを変更して認証機能を無効化してデータアクセス (E1)	o1	開発・製造従事者の適正調査及び教育	{o1〜o10}
						o2	開発・製造設備等の入退出管理	{o1〜o12}
						o3	ドキュメントやシステム内の機密情報へのアクセス管理	{o1〜o10,o13}
						o4	フォトマスクの積層構造化による耐タンパー構造化	{o1〜o13}
						o5	直接的調査からのICカード構成情報の機密性確保	
					本人認証データを不正入手してデータアクセス (E2)	o6	ユーザガイドライン(認証データ守秘義務)の制定	
						o7	ICカード内本人認証データの機密性確保	
						o8	ICカードとリーダライタ間通信データの機密性確保	
						o9	外部IT機器内機密データの機密性確保	
						o10	ユーザの識別及び認証の実施	
					ファイル属性変更ツールを用意する (E3)	o1	開発・製造従事者の適正調査及び教育	
						o2	開発・製造設備等の入退出管理	
						o3	ドキュメントやシステム内の機密情報へのアクセス管理	
						o5	直接的調査からのICカード構成情報の機密性確保	
					ロジック変更ツールを既存の端末にインストールする (E7)	o11	端末の管理	
						o12	端末と周辺機器とのIFの制限	
					⋮	⋮	⋮	
T2	端末利用による暗号鍵データへの不正アクセス	7.5E−5	100億	750万	ファイル属性変更ツールを用意する (E3)	o1	開発・製造従事者の適正調査及び教育	{o1,o2,o3,o5}
						o2	開発・製造設備等の入退出管理	{o1,o2,o3,o5,o11,o12}
						o3	ドキュメントやシステム内の機密情報へのアクセス管理	{o1,o2,o3,o4,o5}
						o5	直接的調査からのICカード構成情報の機密性確保	{o11,o12}
					ファイル属性変更ツールを既存の端末にインストールする (E4)	o11	端末の管理	{o4,o11,o12}
						o12	端末と周辺機器とのIFの制限	{o1,o2,o3,o5,o13}
					⋮	⋮	⋮	{o11,o12,o13}
								{o4,o13}
T3	ユーザデータの改ざん否認	3.0E−3	50億	150万	ICカードシステムに気付かれない (E9)	o14	操作履歴の保存及び監査	{o14}
					ICカードに強い電磁波を近づけて利用記録を破壊する (E10)	o15	利用記録のバックアップ	{o1,o2,o3,o5,o15,o16}
								{o15,o16,o17}
					⋮	⋮	⋮	{o11,o12,o15,o16}

本適用例では，FT の $T1$ の $E2$ “本人認証データを不正入手してデータアクセス” への対策が，相対正規化重要度 $NI(E2) = 1.0$ で他の基本事象に比べて重要度最大となった．このため，たとえば，その対策目標の 1 つとして選択された o9 の “外部 IT 機器（リーダライタ）内機密データの機密性確保” に対しては，対策の重要性から，複数の実現方式候補の中で，f37 の “リーダライタ内での機密データ暗号処理機能” だけでなく，f49 の “筐体不正開放検出時のリーダライタ内機密データ消去機能” などの物理的な不正アクセスへの対策も備えた実現方式が選定されている．このことから，対策目標に対して機能的に適合する実現方式が選定されていることが分かる．また，機能過不足度 $x = 0.4$ は，図 6 に示す対策目標 o1〜o10 の各重要度 (0.25,0.25,0.25,0.25,0.25,1.0,1.0,1.0,1.0,1.0) と，図 6 の対策目標候補と実現方式候補との関連度および実現方式候補の満足度を用いて式 (8) より求められる最適実現方式による対策目標 o1〜o10 の各達成度

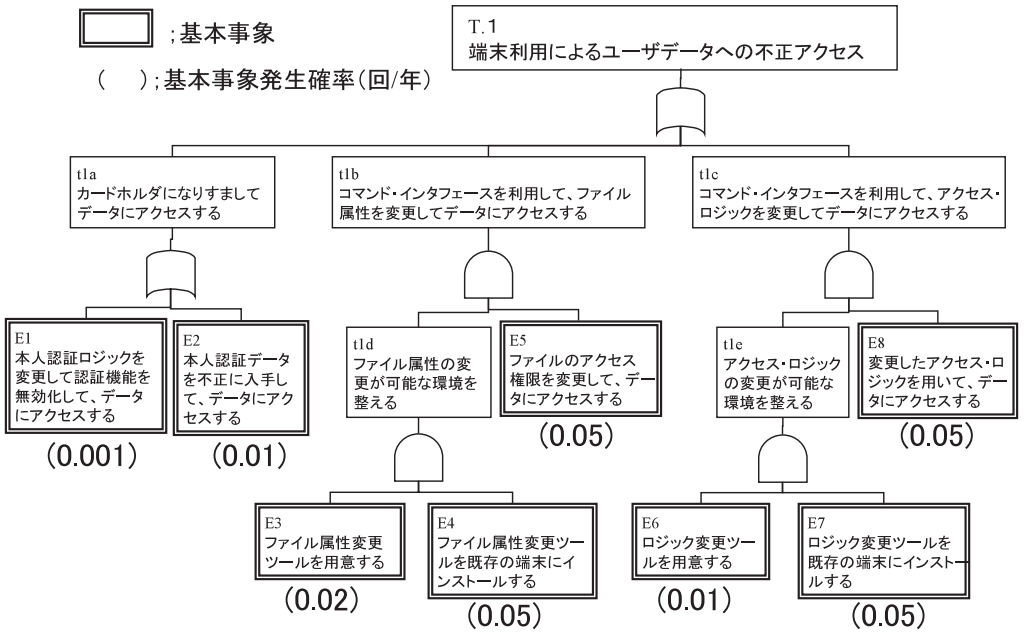

図 5 脅威 $T1$ の FT
Fig. 5 Fault tree for threat $T1$.

表 6 実現方式候補一覧
Table 6 Security specification candidates.

記号	対象	実現方式候補
f1	開発・製造者	採用時に開発・製造従事者の能力や勤務態度などの適正調査を実施
f2	開発・製造者	開発・製造従事者に対して定期的にセキュリティ教育を実施
f3	開発・製造者	採用時に開発・製造従事者と機密保持契約を締結
⋮	⋮	⋮
f30	カード利用者	カード利用者と認証データ守秘義務契約を締結
f31	ICカード	特定回数以上の認証ﾃﾞｰﾀｱｸｾｽ時のICチップを非活性化機能
f32	ICカード	暗号処理専用コプロセッサによるデータ暗号化/復号化機能
f33	ICカード	マスクROM化した暗号処理ﾓｼﾞｭｰﾙによるデータ暗号化/復号化機能
⋮	⋮	⋮
f37	リーダライタ	マスクROM化した暗号処理ﾓｼﾞｭｰﾙによるデータ暗号化/復号化機能
⋮	⋮	⋮
f47	リーダライタ	筐体の不正開放時の警告音発生機能
f48	リーダライタ	特殊ねじを使用して筐体を閉じる
f49	リーダライタ	不正開放検出時リーダライタ内機密データ消去機能
⋮	⋮	⋮
f58	端末	ID＆パスワードによる端末ログイン機能
f59	端末	ID＆パスワードによるアプリケーションログイン機能
f60	端末	特定回数以上の認証ﾃﾞｰﾀｱｸｾｽ時の端末ロック機能
⋮	⋮	⋮
f74	端末	ICカードに対するｵﾍﾟﾚｰﾀの操作履歴保存機能
f75	端末	端末に対するｵﾍﾟﾚｰﾀの操作履歴保存機能
f76	端末	ICカードの取引情報保存機能
⋮	⋮	⋮

(0.75,1.0,1.0.1.0,1.0,0.5,1.0,1.0,1.0,1.0) との差分の合計として算出されている．したがって，機能過不足度の内訳から，決定された最適実現方式 f1〜f6，f8，f10，f12，f14〜f25，f28〜f29 による対策目標 o1〜o5 の達成度は 0.75 または 1.0 で，重要度 0.25 に対して過剰，実現方式 f30 による対策目標 o6 の達成度は 0.5 で，重要度 1.0 に対して不足，また実現方式 f31〜f35，f37，f38，f40〜f42，f49〜f51，f55〜f60 による対策目標 o7〜o10 の達成度は 1.0 で，重要度 1.0 に対して適度であるというように，機能が過不足である対策目標が分かる．さらに，対策目標と実現方式の対応関係から，達成過不足となる対策目標に関連する機能過不足な実現方式も特定することができる．これにより，特に機能不足となる f30 の実現方式（運用管理施策）“カード利用者と認証データ守秘義務契約を締結” については，利用者教育や定期的監査を加えて施策を強化するなど，最適実現方式をさらに効果的，効率的な実現方式に洗練するための指針も得ることができる．

実現方式候補(f)

対策目標候補(o)

	重要度	f1	f2	f3	f4	f5	f6	f7	f8	f9	f10	f11	f12	f13	f14	f15	f16	f17	f18	f19	f20	f21	f22	f23	f24	f25	f26	f27	f28	f29	f30
コスト(万円)		100	100	1	1	1	100	100	10	100	500	500	10	10	70	100	1	100	10	10	1000	1000	100	1000	1000	1000	1000	1000	50	10000	1
満足度		0.5	0.5	1	1	0.5	1	1	1	0.5	0.75	1	1	0.25	1	1	1	0.5	0.5	0.5	1	1	1	1	1	1	1	1	1	1	0.5
o1	0.25	1	1	0.5	0.75	0.5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
o2	0.25	0	0	0	0	0	1	0.5	0.75	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
o3	0.25	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0.5	1	0	0	0	0	0	0	0	0	0	0	0
o4	0.25	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0
o5	0.25	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0.5	1	1	1	0	0	0.5	0.25	0
o6	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
o7	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
o8	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
o9	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
o10	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
o11	0.25	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
o12	0.25	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
o13	0.25	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
o14	0.25	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
o15	0.25	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
o16	0.25	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	0	0	0
o17	0.25	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

	f31	f32	f33	f34	f35	f36	f37	f38	f39	f40	f41	f42	f43	f44	f45	f46	f47	f48	f49	f50	f51	f52	f53	f54	f55	f56	f57	f58	f59	f60	f89	f90
コスト(万円)	100	1000	1000	100	100	1000	1000	100	100	100	100	100	200	10	200	1	50	20	100	100	100	1	50	20	50	50	500	1	1	10	100	50
満足度	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0.5	1	0.75	1	1	1	0.5	1	0.75	1	1	1	1	1	1	1	0.75
o1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
o2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
o3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
o4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
o5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
o6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
o7	0.5	1	1	0.5	0.5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
o8	0	1	1	0.5	0.5	1	1	0.5	0.5	1	1	0.5	0.5	0.5	0.75	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
o9	0	0	0	0	0	1	1	0.5	0.5	0	0	0	0	0	0	0.5	0.75	0.5	1	1	0.5	0.5	0.75	0.5	0	0	0	0	0	0	0	0
o10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.25	1	0.25	1	1	1	0	0
o11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
o12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
o13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
o14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
o15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
o16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
o17	0.5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.5	0.5

図 6　重要度・関連度・コストデータ

Fig. 6　An example of importance, degree of relation and cost.

3.3　既提案の方法と本提案の方法との比較検討

本提案の方法は，想定脅威のすべてに対抗でき，かつ対策コストの総和が最小となるコスト対効果の高いセキュリティ対策目標を定量的に決定する既提案の方法[5)]を，対策目標の実現に最も機能的に適合する実現方式をも決定できるよう拡張したものである．この拡張により，本提案の方法では，既提案の方法のように対策目標候補に対する特定の実現方式のもとで最適対策目標を決定するのではなく，対策目標候補に対して可能性のある複数の多様な実現方式候補の明確化が図られ，対策目標に対して機能的に最も適合する実現方式が存在する対策目標を最適対策目標として決定することができる．その結果として，決定された最適対策目標（実現方式）は機能的には既提案の方法によるものより優れるもののコスト的には高いものとなる場合もありうる．以下に，このことを本論文で使用した具体例で述べる．

＜対策コストが下がる場合＞

適用例において，本提案の方法による対策コストは，3.2 節で示したように 21809 万円となるのに対し，リスク許容値 $Ra = 200$ 万での対策対象となった脅威 $T1$ と $T2$ のセキュリティ対策目標候補 o1〜o13 に対する実現方式を，f1〜f6，f8，f10，f12，f14〜f25，f28〜f42，f46〜f49，f52〜f73 であると特定して既提案方法を用いると，最適対策目標は，o1〜o10 と本提案の方法のそれと同じになるが，対策コストは 23098 万円となる．すなわち，本提案の方法による解の方が低コストとなる．これは，本提案の方法では複数の実現方式候補から対策目標に機能適合する実現方式を決定できることから，より経済的な既提案の方法とは別の実現方式が決定されたことによるものである．なお，適用例は，最適解が機能過不足度最小でかつ対策コストも最小となるものであったため，既提案の方法でどの実現方式を想定したとしても，本提案方法の方が対策コストは下がるものとなる．

＜対策コストが上がる場合＞

2 章の方法説明で用いた例では，本提案の方法による対策コストは，175 万円となるが，リスク許容値 $Ra = 100,000$ 円での対策対象となった脅威 $T1$〜$T3$ のセキュリティ対策目標候補 o1〜o7 に対して実現方式を f1，f5，f9，f12，f13，f15 であると特定して既提案方法を用いると，最適対策目標は，o1，o2，o3，o5 または o1，o3，o5，o7，対策コストは両目標ともに 150 万円となる．すなわち，本提案の方法による解の

方が高コストとなる．しかしながら，既提案の方法による2つの最適対策目標に対応する実現方式（f1，f5，f9，f13）の機能過不足度を求めると，0.125と0.25となり，本提案の方法による最適実現方式の機能過不足度は，0.05であることから，本提案の方法の方が機能適合性は向上している．

この例のように対象によっては，既提案の方法による対策目標よりも，対策コストの高い対策目標とその実現方式が最適解となる場合もある．しかし，対策目標は単にコストの観点からだけでなく真に対策として有効なものであることが重要であり，そのため，対策目標候補に対する複数の実現方式候補の中からまず機能的に適合し，かつその中でコスト最小のものを最適解として決定できる本提案の方法は有用なものであると考える．

4. おわりに

本論文では，国際セキュリティ評価基準ISO15408に準拠したセキュリティ設計仕様書の作成などの情報システムのセキュリティ基本設計を支援するセキュリティ基本設計法を提案した．本方法は，想定脅威のすべてに対抗でき，かつ対策コストの総和が最小となるコスト対効果の高いセキュリティ対策目標を定量的に決定する既提案の方法に，対策目標の実現に最も機能的に適合する実現方式を決定する方法を追加することで既提案の方法を拡張したもので，これによって，実現方式が対策目標をどの程度達成できるかを考慮してよりコスト対効果の高い対策目標を決定できる．また，本方法を具体的な事例に適用して，提案の方法が基本的に妥当なものであることを確認した．今後多くの事例に適用して，本方法をより実用的なものへと洗練させていく必要はあるが，本方法は，セキュリティ基本設計の支援に有効活用できるものと考える．

参考文献

1) ISO/IEC 15408-1: Evaluation criteria for IT security Part1: Introduction and general model (1999).
2) ISO/IEC PDTR 15446: Guide on the production of Protection Profiles and Security Targets (2000).
3) 宝木ほか：情報システムにおけるリスク分析の一方法，電気学会論文誌 C，Vol.108-C，No.4，pp.260–267 (1988).
4) 織茂ほか：セキュリティシステム構築のための計画手順の提案，情報処理学会コンピュータセキュリティシンポジウム'98 論文集，Vol.98，No.12，pp.75–80 (1998).
5) 永井ほか：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).
6) 総合安全工学研究所：FTA 安全工学，pp.107–118，日刊工業新聞社 (1979).
7) 永井ほか：企業情報システム構築支援のための機能的適合性評価の一手法，電気学会論文誌 C，Vol.119-C，No.3，pp.344–349 (1999).
8) Centralised Certified Product List. http://www.commoncriteria.org/epl/index.html
9) 今野ほか：整数計画法と組合せ最適化，pp.27–47，日科技連 (1982).

(平成15年4月10日受付)
(平成16年2月 2 日採録)

永井 康彦（正会員）

昭和58年日本大学理工学部航空宇宙工学科卒業．昭和60年同大学大学院理工学研究科修士課程修了．同年（株）日立製作所入社．システム開発研究所勤務．情報セキュリティ，ネットワーク管理システム，グループウェア等の研究開発に従事．現在同研究所セキュリティシステム研究部主任研究員．電子情報通信学会，電気学会各会員．

藤山 達也（正会員）

平成5年東京大学工学部機械工学科卒業．平成7年同大学大学院工学系研究科修士課程修了．同年（株）日立製作所入社．システム開発研究所勤務．情報セキュリティ，ネットワークセキュリティ等の研究開発に従事．現在同研究所セキュリティシステム研究部研究員．

荒井 正人（正会員）

平成2年日本大学理工学部電子工学科卒業．平成4年同大学大学院理工学研究科修士課程修了．同年（株）日立製作所入社．マイクロエレクトロニクス機器開発研究所を経て，システム開発研究所に勤務．現在，同研究所セキュリティシステム研究部主任研究員として情報システムのアクセス制御技術，セキュリティ設計技術の研究開発に従事．

柚原 直弘

昭和 44 年日本大学大学院理工学研究科博士課程単位取得．同年日本大学理工学部機械工学科助手．昭和 47 年同専任講師．昭和 51 年同航空宇宙工学科助教授．昭和 56 年から同教授．飛行力学，飛行制御，人間–機械系，車両制御，システム計画，システム最適化，運転エージェント等の研究に従事．工学博士．昭和 63 年自動車技術会論文賞，平成 2 年精密工学会論文賞，平成 12 年 Advanced Vehicle Control・2000 Best Paper Award 等を受賞．AIAA，IEEE，日本航空宇宙学会，システム制御情報学会，計測自動制御学会，自動車技術会，人間工学会，System Safety Society，日本機械学会，ヒューマンインタフェース学会等の会員．