セキュリティ対策目標の最適決定技法の提案

永井康彦† 藤山達也† 佐々木良一†

組織や情報システムトータルとしての体系的な情報セキュリティ対策のため，また，国際セキュリティ評価基準ISO15408による認証取得に必要となるセキュリティ設計仕様書の作成のためにセキュリティポリシーやセキュリティ対策目標を策定することが重要となってきている．しかしながら，脅威と対抗する対策目標との複雑な対応関係の下で，効果的，効率的な対策目標を策定することは困難な作業となる．本論文では，セキュリティ対策目標を脅威対抗としての必要十分性の観点と必要コストの観点から効率的に，定量的に決定できるセキュリティ対策目標最適決定技法を提案する．本技法は，2つの方法から構成される．1つは，各脅威の因果関係を表現したFault Tree（FT）を作成し，ミニマルパスセット探索アルゴリズムを適用することで脅威を抑止する必要最小限の基本事象の組合せを特定，さら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対応づけて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方法である．もう一方は，導出対策目標候補集合群の中から，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求解することにより決定する方法である．これにより，コスト対効果の良い対策目標の策定が実現できる．また，具体的事例に本技法を適用し，有効性を確認している．

An Optimal Decision Method for Establishment of Security Objectives

Yasuhiko Nagai,† Tatsuya Fujiyama† and Ryoichi Sasaki†

For establishment of systematic information security countermeasures, the production of security policies or security objectives in a security design specification based on the international security evaluation standard ISO15408 has become more important. However, it is difficult to define the security objectives effectively and efficiently on complex mapping relationships between threats and objectives. In this paper we propose an optimal security objectives decision method. The method provides the ability to determine the security objectives 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 search algorithm on the fault trees (FT) with respect to the threats. The other is decision scheme of optimal security objectives for minimizing required cost by resolving a combinational optimization problem. Furthermore, we will show the usefulness of the method in a case study.

1. はじめに

EC（Electronic Commerce）に代表されるように情報システムは，社会環境や企業活動の基盤を形成するようになってきている．しかし一方で，プライバシー情報や企業機密情報の漏洩や改ざん，取引否認等の情報セキュリティに関する脅威も社会的に大きな影響を及ぼすものになっており，十分な対策を施すことが重要になってきている．特に最近の動向としては，従来のウィルス対策やファイアウォールの設置等の個別対策ではなく，組織やシステムトータルとしての体系的な情報セキュリティ対策のためにセキュリティポリシーの策定が進められていることがあげられる[1]．また，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ISO15408が標準化された[2)~4)]．本基準は，情報関連製品・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，本基準での評価・認証取得がビジネス上や運用上の必須条件となる．

ところで，このISO15408の認証取得のために必須となる評価対象製品・システムのセキュリティ要求仕様書（プロテクションプロファイル）[5)]やセキュリティ基本仕様書（セキュリティターゲット）[5)]の作成や組織の情報セキュリティポリシーの作成において，適用

† 株式会社日立製作所
Hitachi, Ltd.

環境に想定される脅威を洗い出し，各脅威のリスク分析・評価を行い，脅威に対抗するコスト対効果の良いポリシーやセキュリティ対策目標（以下では両者を合わせてセキュリティ対策目標と呼ぶ）を定義することが必要である．これまで，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[6]や体系的なセキュリティ対策目標を立案するための計画手法[7]が提案されている．前者は脅威の抽出とそのリスク評価に主眼を置いたものであり，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る．これに対し，後者はセキュリティ対策目標の策定を体系的に支援する手法であり，抽出脅威に対する FTA を用いたリスク分析・評価を行い，各脅威のリスク値の大きいものから順に優先順位づけしてから，各脅威の因果関係を表す FT（Fault Tree）の各基本事象を抑止する対策をセキュリティ対策目標として決定するものである．しかしながら，全体として漏れや抜けなく論理的に対策目標を導出できるが，各脅威に対するすべての基本事象に対抗する対策目標であるために対策目標として過剰なものになること，単にリスク値の大きさから対策順位や範囲を決める方法であり，各対策目標の必要コストの観点での評価がなく，セキュリティ対策目標としてコスト対効果を十分配慮したものにならないという問題がある．さらに，脅威やその基本事象と対抗する対策目標との対応関係は，通常 1 対 1 ではなく 1 対多であり，そのうえ複数の脅威に共通となる対策目標も存在する．これら複雑な対応関係の下で，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定義者が決定することも困難な作業となる．

そこで，本論文では，セキュリティ対策目標を脅威対抗としての必要十分性の観点と必要コストの観点から効率的に，定量的に決定できるセキュリティ対策目標最適決定技法を提案する．この技法は，(1) 各脅威に関する FT にミニマルパスセット探索アルゴリズム[8]を適用することで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）を特定，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対応づけて脅威対抗に必要最小となる対策目標候補集合群を導出し，(2) 導出対策目標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求解することにより決定するものである．以下，2 章ではセキュリティ対策目標の最適決定技法を示し，3 章では本技法を具体的な事例に適用し，有用性を検討する．

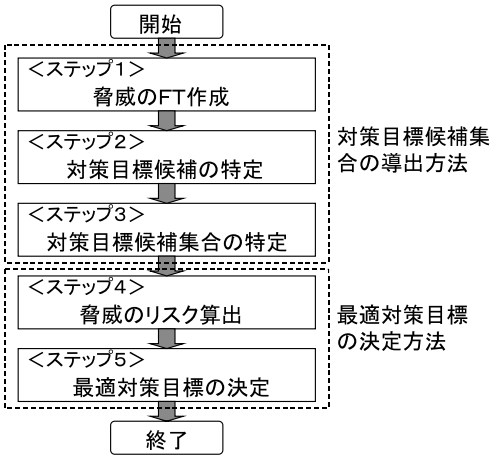

図 1 最適対策目標決定手順
Fig. 1 Procedure of optimal security objectives decision method.

2. セキュリティ対策目標の最適決定技法

2.1 概　　要

本技法は，**図 1** に示すように，大別してセキュリティ対策目標候補集合の導出，最適セキュリティ対策目標の決定の 2 段階から構成される．技法への入力データとしては，従来手法により適用環境に関して抽出された環境に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の各脅威を頂上事象とし，その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となるため，各基本事象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，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対応づけられる．ここで，説明の簡略化のため対策目標候補が基本事象に対し 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

作成 FT 各々に対してミニマルパスセット探索アルゴリズム[8]を実行し，各 FT のミニマルパスセットを

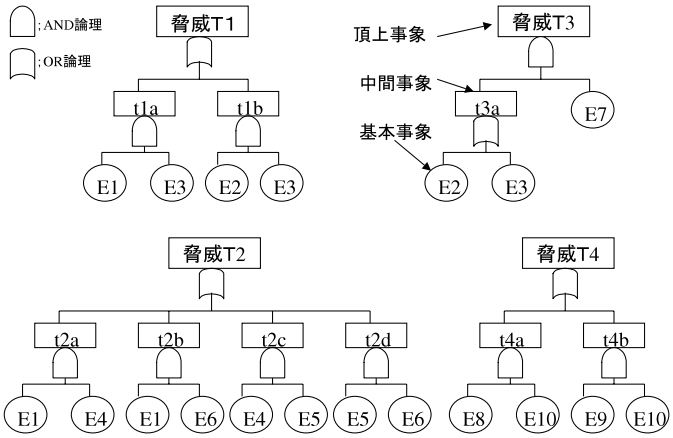

図 2 フォルト・ツリー（FT）例
Fig. 2 Examples of fault tree (FT).

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

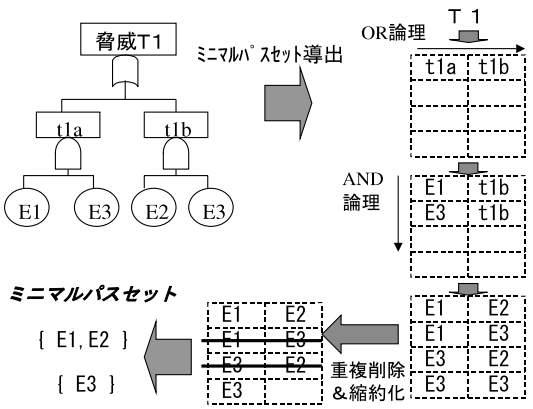

図 3 ミニマルパスセット導出例
Fig. 3 A derivation example of minimal path sets.

求める．ミニマルパスセットとは，FT の頂上事象（脅威）の発生を抑止するために必要十分となる対策すべき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，脅威を抑止するために必要十分な対策目標候補集合が得られる．ミニマルパスセット探索アルゴリズムとしては Fussell のアルゴリズム[8]等がある．図 2 の脅威 $T1$ の FT 例に Fussell のアルゴリズムを適用した場合の探索例を**図 3** に示す．

マトリックス空間を用意し，まずその上左端に FT の頂上事象 $T1$ を配置する．次に配置した $T1$ を直下の中間事象である $t1a$，$t1b$ に置き換えることで展開する．その際，頂上事象との因果関係が OR ゲートの場合は，マトリックス空間上の右横方向に展開し，AND ゲートの場合は下縦方向に展開する．この展開を基本事象に辿りつくまで繰り返し行う．展開完了後，得られたマトリックス空間の各行のべき等律を用いた簡略化（同じ基本事象の重複削除），各行間比較で包含関係がある場合には最小となる行以外の行を削除する縮約化を行う．以上の処理の結果得られる各行の基本事象の組合せ，脅威 $T1$ の場合は $\{E1, E2\}$，$\{E3\}$ の 2 つがミニマルパスセットとなる．また，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の決定方法

最適セキュリティ対策目標の決定は，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

各脅威の FT の基本事象に対してその発生確率データ (回/年) を付与し，各 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．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用い，ない場合は類似事象の統計値等か

らの推定や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付与する．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 $E1 = 1.0$，$E2 = 0.5$，$E3 = 0.1$ 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．

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

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．

$$\begin{aligned} R(T1) &= P(T1) \times E(T1) \\ &= 0.1 \times 100000000 = 10000000 \text{ (円/年)} \end{aligned}$$

〈ステップ 5〉最適対策目標の決定

［組合せ最適化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 $\text{obj}(q) : 1 \cdots$ 採用，$0 \cdots$ 否採用とすると，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 0-1 整数計画問題となり，次のように定式化される．

$$\text{目標関数：minimize} \quad z = \sum_{q=1}^{m} C(q) \cdot \text{obj}(q) \tag{1}$$

$$\text{制約条件：subject to} \quad \sum_{k=1}^{n} \left[1 - \prod_{j=1}^{pk} \prod_{q \in Pk,j} \text{obj}(q) \right] = 0 \tag{2}$$

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

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

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)
対策の具体的実現手段により変化するが平均的，一般的代表値を与える．

m： 対策目標候補数

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

n： 対象脅威数

pk： 脅威 k の対策目標候補集合の個数

Pk, j： 脅威 k の j 番目の対策目標集合

$R(k)$： 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をすべて対策されるという制約を表している．また，式 (4) は指定値 Ra 以下のリスクの脅威は許容できるものとして対策から除外するリスク許容値を表す．

［最適対策目標決定問題の解法］

前述した最適対策目標の決定問題は，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．間接列挙法は，解ベクトル $X = (\text{obj}(1), \text{obj}(2), \cdots \text{obj}(m))$ のある部分解 $Sr = (\text{obj}(1), \text{obj}(2), \cdots \text{obj}(r))$ とし，この部分解の実行可能な完成解の中で，(a) 目標関数を最小とするものを発見，あるいは (b) 実行可能解が存在しないか，しても暫定解 z より小さくないことが判明したとき，その部分解は探査済みとなり列挙の対象から除くという処理を行う求解方法である．

先の例に対して**表 2** に示すようなデータが前述までの方法で導出および特定され，リスク許容値 $Ra =$ 100000 (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，次に間接列挙法で求解すると最適解として採用目標 $O2$, $O3$, $O4$, $O6$ のとき，対策コスト最小値 750000 円が求められる．したがって，脅威 $T1$ に対する対策目標として $O3$，脅威 $T2$ に対する対策目標として $O4$ と $O6$ の組合せ，脅威 $T3$ に対する対策目標として $O2$ と $O3$ の組合せが最適セキュリティ対策目標として決定される．

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

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	備考 (対策コスト)
T1	0.1	1億	1000万	{O1,O2} {O3}	O1：100万円 O2：10万円 O3：20万円 O4：30万円 O5：20万円 O6：15万円 O7：40万円 O8：60万円 O9：100万円 O10：80万円
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}	

表 3 脅威のリスク値と対策目標候補集合
Table 3 Risk value of 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	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	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	
						O5	直接的調査からのICカード構成情報の機密性確保	{O1～O13}
					本人認証データを不正入手してデータアクセス	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	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	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	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	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	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	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}
					⋮	⋮	⋮	

3. 適 用 例

3.1 適用対象

前章で述べたセキュリティ対策目標の最適決定技法を具体的な情報システム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 3**，**表 4** に示す．たとえば脅威 $T1$ に対しては，ステップ 1 で**図 4** 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 3 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，各基本事象に対応する対策目標候補への置き換えと重複候補や重複集合を削除して整理することにより，表 3 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 $\{O1 \sim O12\}$ となる．次にステップ 4 で図 4 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付与している．

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

また，脅威 $T1$ のリスク値 $R(T1)$ は，脅威の発生確率に影響度 100 億 (円/回) を掛け算することで 1.1 億 (円/年) と算出された．

以上のようなステップを脅威 $T2$，$T3$ に対しても同様に実施することで，本例の場合，合計 17 項目のセキュリティ対策目標候補と 16 個の対策目標候補集

表 4 対策目標候補一覧
Table 4 Security objective candidates.

対策目標候補		
記号	内容	対策コスト
O1	開発・製造従事者の適正調査及び教育	100万円
O2	開発・製造設備等の入退出管理	1000万円
O3	ﾄﾞｷｭﾒﾝﾄやｼｽﾃﾑ内の機密情報へのｱｸｾｽ管理	100万円
O4	ﾌｫﾄﾏｽｸの積層構造化による耐ﾀﾝﾊﾟｰ構造化	1000万円
O5	直接的調査からのICカード構成情報の機密性確保	100万円
O6	ﾕｰｻﾞｶﾞｲﾄﾞﾗｲﾝ(認証ﾃﾞｰﾀ守秘義務)の制定	100万円
O7	ICカード内本人認証ﾃﾞｰﾀの機密性確保	100万円
O8	ICカードとﾘｰﾀﾞﾗｲﾀ間通信ﾃﾞｰﾀの機密性確保	100万円
O9	外部IT機器内機密ﾃﾞｰﾀの機密性確保	100万円
O10	ﾕｰｻﾞの識別及び認証の実施	100万円
O11	端末の管理	10万円
O12	端末と周辺機器とのIFの制限	10万円
O13	ﾌｧｲﾙへのｱｸｾｽ権限の管理	100万円
O14	操作履歴の保存及び監査	100万円
O15	利用記録のバックアップ	100万円
O16	規定外乱時の処理停止及び復帰	1000万円
O17	ﾕｰｻﾞ端末に対する実行権限の確認	10万円

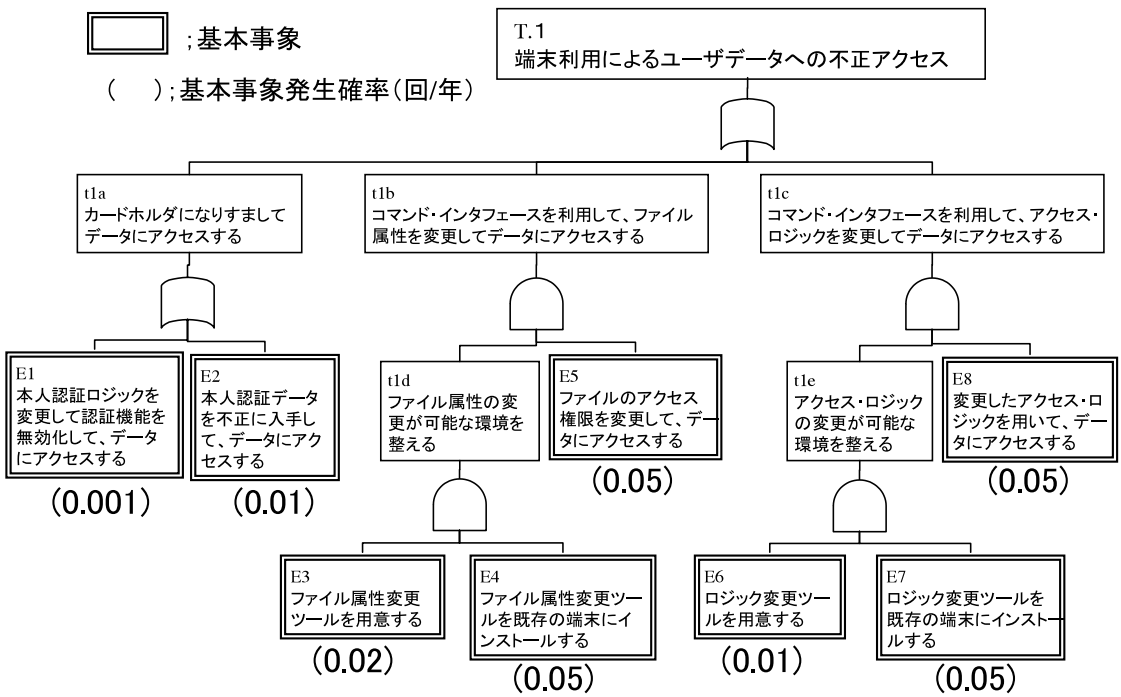

図 4 脅威 T1 の FT
Fig. 4 Fault tree of threat T1.

合が導出された．

また，表 4 の各対策目標候補の対策コストデータを用い，リスク許容値 $Ra = 100$ 万 (円/年) としてステップ 5 を実施した結果，コスト最小となる最適セキュリティ対策目標として以下の 11 の対策目標が決定された．

(1) $O1$：「開発・製造従事者の適正調査および教育」
(2) $O2$：「開発・製造設備等への入退出管理」
(3) $O3$：「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」
(4) $O4$：フォトマスクの積層構造化による耐タンパー構造化
(5) $O5$：直接的調査からの IC カード構成情報の機密性確保
(6) $O6$：ユーザガイドライン（認証データ守秘義務）の制定
(7) $O7$：IC カード内本人認証データの機密性確保
(8) $O8$：IC カードとリーダライタ間通信データの機密性確保
(9) $O9$：外部 IT 機器内機密データの機密性確保
(10) $O10$：ユーザの識別および認証の実施
(11) $O14$：操作履歴の保存および監査

3.3 結果の検討

本適用例で決定された最適セキュリティ対策目標の対策コストの総和は，2900 万円となる．これに対し，従来方法ではすべての対策目標候補を実施することとなるため対策コストの総和は，4130 万円となる．また，決定対策目標数も 11 項目に対して従来方法の場合は 17 項目すべてとなる．したがって，適用例の場合，本技法により，従来に比べ対策コスト面および対策項目数で約 65%に洗練したコスト対効果の良いセキュリティ対策目標が決定できたことが分かる．

4. おわりに

本論文では，セキュリティポリシーの作成や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において，セキュリティ対策目標の策定を支援するセキュリティ対策目標の最適決定技法を提案した．本技法は，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良いセキュリティ対策目標を定量的に決定することができる．また，本技法を具体的な事例に適用し，基本的に有効なものであることを確認した．

今後の課題としては，コストだけでなく対策目標の実現容易性や信頼性も考慮できる，より実用的な技法へ拡張することがあげられる．

参考文献

1) Wood, C.C.: INFORMATION SECURITY POLICIES MADE EASY Version 6, Baseline Software, Inc. (1997).
2) ISO/IEC FDIS 15408-1, Evaluation criteria for IT security Part1: Introduction and general model (1998).
3) ISO/IEC FDIS 15408-2, Evaluation criteria for IT security Part2: Functional security requirements (1998).
4) ISO/IEC FDIS 15408-3, Evaluation criteria for IT security Part3: Assurance security requirements (1998).
5) ISO/IEC WD 15446, Guide on the production of Protection Profiles and Security Targets (1999).
6) 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).
7) 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).
8) 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).
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 11 年 12 月 8 日受付)
(平成 12 年 6 月 1 日採録)

永井 康彦（正会員）

1983 年日本大学理工学部航空宇宙工学科卒業．1985 年同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横浜ラボラトリ勤務．情報セキュリテイ，ネットワーク管理システム，グループウエ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センタ主任研究員．電気学会，電子情報通信学会，日本航空宇宙学会各会員．

藤山 達也（正会員）

1993 年東京大学工学部機械工学科卒業．1995 年同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横浜ラボラトリ勤務．情報セキュリテイ，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センタ企画員．

佐々木良一（正会員）

1971 年東京大学医学部保健学科卒業．同年（株）日立製作所入所．システム開発研究所にてシステム高信頼化技術，セキュリティ技術，ネットワーク管理システム等の研究開発に従事．現在同研究所主管研究長兼セキュリティシステム研究センタ長．工学博士（東京大学）．1983 年電気学会論文賞受賞．1998 年電気学会著作賞受賞．著書に「インターネットセキュリティ—基礎と対策技術」（共著，オーム社，1996 年），「インターネットセキュリティ入門」（岩波新書，1999 年）等．IEEE，電子情報通信学会，電気学会各会員．