情報システムにおけるセキュリティ対策立案のための計画手法

織茂昌之[†] 津原進[††]
山本倫子[†††] 佐々木良一[††]

情報システムが社会において果たす役割が増大するとともに，情報システムのセキュリティに対する脅威が増大している．これに対応するためには，対象となるシステムの特徴，利用形態に応じた適切なセキュリティ対策を講じることが必要である．本論文では，フォールトツリー分析手法をベースとし，セキュリティ対策を体系的に立案するための計画手法を提案する．本手法は，対象とする情報システムを襲うと想定される脅威を体系的・論理的に抽出し，これに対して過不足のないセキュリティ対策を効率的に導出すること目的とし，(1) 評価対象のモデル化，(2) 脅威の抽出，(3) 対策方針の導出，(4) セキュリティ目標の確立，(5) セキュリティ対策の策定，の 5 つのプロセスを実施するものである．また，提案手法を具体的な情報システムのセキュリティ対策立案に適用することにより，体系的な脅威の抽出とそれに対する対策の立案を効率的に行えることを確認した．

Security System Planning Method for Information Systems

Masayuki Orimo,[†] Susumu Tsuhara,[††] Michiko Yamamoto[†††] and Ryoichi Sasaki[††]

Threats to the information system security have been increasing more and more. It has been seriously required to design sufficient countermeasures for protecting the system security form possible threats. This paper proposes a method for security system planning. The proposed method makes it possible to systematically design countermeasures for possible threats to the target system. The proposed method also enables to check the rationale of designed countermeasures easily. This method has been developed based on a fault tree analysis technique. This method consists of five processes, that is, (i) description of target of evaluation, (ii) description of possible threats, (iii) derivation of principles for countermeasures, (iv) definition of security objectives, (v) design of countermeasures for attaining the security objectives. The effectiveness of proposed method has been identified through the application to actual systems.

1. はじめに

インターネット/イントラネット/イクストラネット，電子マネー/電子商取引，電子乗車券など，ネットワーク情報社会の形成にともなって，なりすまし，偽造，改ざん，盗難，盗聴，取引否認，ウィルスなどの，情報セキュリティに対する脅威が増大している．これに対応するためには，上記のような多様なシステムに対し，それぞれのセキュリティ上の要求を満足させるためのセキュリティ対策を施すことが必須となる．このためには，システムを襲うと想定される脅威を体系的・論理的に抽出し，これに対して過不足のないセキュリティ対策を設計することが必要である．これまで，対象システムに想定されるリスクを抽出し，その発生頻度，損失額から影響度合いを評価するリスク分析手法が提案されている[1),2),6)]．宝木らは，従来，故障分析に用いられていたフォールトツリー分析手法[3)]を用いて不正行為に起因するセキュリティ事故のリスク分析を行う手法を提案した[2)]．この中では，フォールトツリーを作成することにより想定される脅威の定性分析を行い，作成したフォールトツリーに発生確率を付与することにより脅威原因に対する定量分析を行う．これらの手法は，リスクの抽出と，その影響度評価に主眼を置いたものであり，抽出，評価したリスクの発生を防ぐためのセキュリティ対策の策定については明確な議論がなされていなかった．セキュリティ対策の策

† 株式会社日立製作所情報・通信グループ新事業推進センタ
Business Development Division, Hitachi, Ltd.
†† 株式会社日立製作所システム開発研究所
Systems Development Laboratory, Hitachi, Ltd.
††† 株式会社日立製作所システム開発本部
Business & Information Systems Development Division, Hitachi, Ltd.

定については，IC カード型電子マネーシステムを対象として手順の検討がなされている[4]．しかし，電子マネーシステムを対象とした枠組みが規定された段階であり，その汎用化，また，具体的な進め方については，今後さらに検討が進められるものと考えられる．

一方，情報システムのセキュリティ機能とその保証に関して，国際的に統一された評価基準とすることを目的として，Common Criteria（CC）Ver.2.0 のドラフトが 1997 年 12 月に発行されている[5]．CC では，製品やシステムが具備すべきセキュリティ機能に関する汎用的な要件（機能要件）のセット，これらの機能要件の実現の確かさを保証するための汎用的な要件（保証要件）のセットを規定している．対象とするシステムで必要となる機能要件，保証要件を，CC で規定される要件のセットの中から選択することにより，対象システムに対応するサブセットを作成することが要求されているが，この具体的な作成方法については明確な規定がなされていない．

本論文では，宝木らが提案したフォールトツリー分析に基づくリスク分析手法の考え方を展開し，ターゲットとなるシステムに対応したセキュリティ対策を体系的に策定するためのセキュリティシステム計画手法を提案する．以下，2 章にてセキュリティ対策立案のプロセスとその課題について，また，3 章にて提案手法における課題解決のための方針を示す．4 章にて提案手法の詳細について示し，最後に 5 章にて本提案手法を具体的な事例に適用した結果の評価を示す．

2. セキュリティ対策立案プロセスとその課題

2.1 セキュリティ対策立案におけるプロセス

情報システムに対するセキュリティ上のリスク分析を行い，対象とするシステムにおいて具備すべきセキュリティ対策を立案するための手順として，以下の手順が示されている[1]．

(1) 分析対象の理解と計画
分析対象とする情報システムの構成や利用環境などについて十分な知識を得るための予備調査を実施する．

(2) 脅威（リスク）の発見と識別
情報システムの構成要素に対して，いかなるセキュリティ上の脅威（リスク）が発生しうるかを抽出する．

(3) 関連分析と予想損失額
脅威（リスク）の発生がどのようなセキュリティ上の阻害を引き起こし，それがどのようにして損失の発生となるかを分析する．

(4) 損失の分類とインパクトの評価
損失の性格を，直接的損失，間接的損失，対応費用の観点から分類し，その財務的インパクトを評価する．

(5) 対策の検討および評価
脅威（リスク）に対する対策を検討し，その有効性，妥当性，コストを評価する．

また，情報システムのセキュリティ機能とその保証に関して，国際的に統一された評価基準とすることを目的として，Common Criteria（CC）Ver.2.0 のドラフトが 1997 年 12 月に発行されている[5]．これは今後 ISO で標準化される予定である．CC では，計画している製品やシステム（TOE: Target of Evaluation）ごとに，Protection Profile（PP）を作成するよう規定している．PP は，対象とするシステムが具備すべきセキュリティ上の要件を規定するものである．PP で記述することが要求されている項目（PP 目次）を示したものが**表 1** である．表 1 に示されるように，CC においては，上記 (3)，(4) の予想損失額，インパクトの分析については明確に要求されていないが，セキュリティ対策を上記 (1)，(2)，(5) のプロセスにより策定することが規定されている．

上記 (3)，(4) で示される，脅威に対する予想損失額，インパクトの評価については，リスク分析手法としてすでにいくつかの手法が開発，適用されている[2),6)]．しかし，上記 (2) および (5) のプロセスについては，筆者らの知る限り，これらを実施するための明確な手法についての十分な議論がなされていない．本論文では，セキュリティ対策立案プロセスのなかで重要な位置を占める，これら (2)，(5) のプロセスを体系的，効率的に実施するための手法を提案する．なお，以下では，特に (2)，(5) のプロセスをセキュリティ対策立案プロセスと呼ぶ．

2.2 セキュリティ対策立案プロセスにおける課題

前節で示したセキュリティ対策立案プロセスは一般的手順として示されているものであり，実際に実施する場合は，実行する人/グループの裁量に任されているのが実態である．このプロセスを実施するうえでは，以下の課題が存在する．

(1) 脅威の体系的な抽出方法の欠如

セキュリティ対策を立案するためには，まず，対象とする情報システムにどのような脅威が発生しうるかを抽出することが前提となる．この脅威の抽出が不十分であると，その結果として立案されるセキュリティ対策も不十分なものとなってしまう．脅威抽出の抜け，漏れを最小限にするための体系的な手法が必要となる

表 1 CC（Common Criteria）における PP（Protection Profile）の目次
Table 1 Contents of PP (Protection Profile) in CC (Common Criteria).

1. PP (Protection Profile) introduction
1.1 PP identification
1.2 PP overview
2. TOE (Target of Evaluation) description
3. TOE security environment
3.1 Assumptions
3.2 Threats
3.3 Organizational security policies
4. Security objectives
4.1 Security objectives for the TOE
4.2 Security objectives for the environment
5. IT security requirements
5.1 TOE security requirements
5.1.1 TOE security functional requirements
5.1.2 TOE security assurance requirements
5.2 security requirements for the IT environment
6. PP application notes
7. Rationale
7.1 Security objectives rationale
7.2 security requirements rationale

が，従来，このための手法については明確に規定されたものがなく，実施担当者のノウハウに任されていたという問題が存在する．

（2）抽出した脅威を防ぐための対策の体系的な導出方法の欠如

上記で抽出した脅威を防御するために対象システムが具備すべき要件，すなわち，セキュリティ対策を導出しなければならない．情報システムに対する一般的なセキュリティ要件としては，機密性，保全性，可用性，否認防止の保証が示されており，これらを実現するための要素としての情報セキュリティ技術は十分に研究開発されている[7]．しかし，脅威として抽出された事象を防ぐためには，これら要素技術をどのように組み合わせればよいか，また，その要素技術のみで十分な対策となりうるかなどの，対象システムに発生しうる脅威に応じた対策を導出するための手法については，(1) と同様，明確に規定されたものがなく，実施担当者のノウハウに任されていたという問題が存在する．

3. 課題解決のための方針

前章で示した課題を解決するため，本論文で提案する計画手法では，評価対象システムから構成要素を抽出し，それぞれの構成要素に対して想定される脅威を抽出してゆく方針をとる．具体的には以下の 2 つの方針に基づき，計画手法を提案する．

3.1 脅威を体系的に抽出するための方針

（1）評価対象の明確化

評価対象システムの構成要素を決定するために，オブジェクト指向における包含ツリーの考え方を適用する．包含ツリーは，対象となるオブジェクトを頂上要素として，その構成要素を包含関係に基づきツリー状に，より詳細に展開してゆくものである[8]．この手法を適用することにより，対象とするシステムの構成要素を体系的に抽出することが可能となる．**図 1** は，包含ツリー分析作業例である．頂上に評価対象となるシステムをおき全体と部分の関係に着目して分析する．図示の例では，評価対象が，E11，E121，E122，E21，E22 の 5 つの基本要素から構成されることを示している．さらに，これら基本要素間の通信路も抽出し評価対象に加える．以上の処理により抽出した基本要素および通信路から，評価すべき要素（評価要素）を決定する．

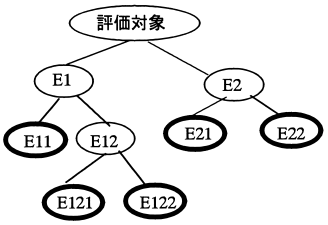

図 1 包含ツリー分析例
Fig. 1 Example of containment tree analysis.

（2）評価対象に対する脅威の導出

脅威の抽出は，抽出作業者が不正行為実行者（アタッカー）の観点に立ち，どのような不正を行えるかを考える，という作業が基本となる．これは，人間の行動について分析する作業であり，「どこで（Where），誰が

（Who），いつ（When），なぜ（Why），何を（What），行うか」という 5W 型誘導の考え方で分析することが，作業者の思考過程に合致すると考えられる．本提案手法では，この 5W 型誘導に基づき想定される脅威を体系的に抽出する方針をとる．具体的には，Where に相当する上記（1）で決定した評価要素のそれぞれに対し，誰が（Who），いつ（When），どのような動機で（Why），の順で展開し，どのような不正行為が行われうるか（What）を抽出し，これを脅威とする．

なお，一般的に不正行為は，その行為にかかる労力・費用に見合った見かえりがある場合に，発生する危険性が高くなる．本提案手法で用いる 5W 型誘導における「Why」は，不正行為実行の動機を示すものであり，この動機の高低は，不正行為の発生する危険性を示す 1 つの目安として利用することが可能である．

3.2 セキュリティ対策を体系的に導出するための方針

（1）フォールトツリー分析による脅威の詳細化

フォールトツリー分析手法（FTA: Fault Tree Analysis）[3]は，故障の発生原因をトップダウンに分析し，その結果を用いて信頼性解析を行うための手法であり，長年の実績があり確立された手法である．FTA は，①故障原因の分析（FT の作成），②分析結果（①で作成した FT）に確率を付与することによる信頼性解析，の 2 つのフェーズからなる．脅威の発生要因の分析においても，FTA における①の故障原因分析と同様のアプローチをとることにより，体系的に実施することが可能である．以上のことより，本提案手法では，FTA における①の手法を適用することにより，前節で抽出した脅威を防御するための対策を体系的に導出する方針をとる．具体的には抽出した脅威を頂上において（これを頂上事象と呼ぶ），それを引き起こす原因となる事象に論理的に展開し，それ以上は展開できない事象（これを基本事象と呼ぶ）に至るまで続ける．原因となる事象への展開には，AND ゲートや OR ゲートなどの論理ゲートが使用される（**図 2**）．OR ゲートは下位事象のどれかが生起したときに上位事象が生起するときに，AND ゲートは下位事象のうちのすべてが生起したときに上位事象が生起するときに，それぞれ用いられる．このような展開を実施することにより，基本事象から中間の事象を経て頂上事象に至るまでの，事象間の因果関係を論理的に明らかにすることができるので，頂上事象の発生を抑止するためにはどのような基本事象を抑止すべきかなどの検討が可能となる．

（2）FTA 展開結果から取るべき対策の体系的な導出

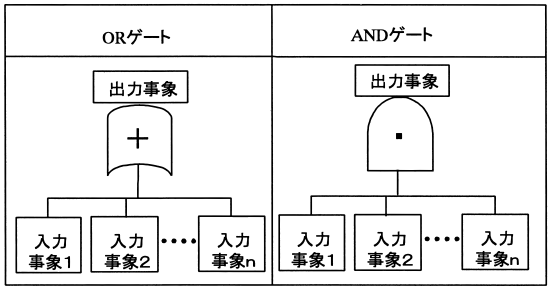

図 2 FTA における AND ゲート，OR ゲート
Fig. 2 AND gate/OR gate in FTA.

上記で展開した FTA 展開結果の基本事象それぞれに対する対策を検討することにより，頂上事象である脅威の発生を防御するための対策を体系的に立てることが可能である．この対策検討においては，次の原則が基本となる．

- 上位事象と下位事象が AND ゲートで結合されている場合は，下位事象のどれか 1 つの事象の発生を防御することにより上位事象の発生を防御できる．すなわち，複数の下位事象の発生を防御することは，上位事象の発生に対する多重防御を実施することを意味する．セキュリティ対策においては，多重防御は望ましい対策の打ち方である．
- 上位事象と下位事象が OR ゲートで結合されている場合は，下位事象のすべての事象の発生を防御することにより上位事象の発生を防御できる．

以上示したように，AND ゲート，OR ゲートにより，対象とする脅威に対する対策の位置付けを明確化することが可能である．

以下では，本章で示した方針に基づくセキュリティ対策立案手法を示す．

4. セキュリティ対策立案のための計画手法

4.1 全体概要

評価対象のモデル化（フェーズ I），脅威の抽出（フェーズ II），対策方針の導出（フェーズ III），セキュリティ目標の確立（フェーズ IV），セキュリティ対策の策定（フェーズ V）の 5 つのフェーズからなる計画手法を提案する．各フェーズで実施する作業の概要は次のとおりである．

（1）評価対象のモデル化（フェーズ I）

①包含ツリー分析，②通信路設定，③評価要素の決定，を実施する．①で評価対象の基本要素を明らかにし，②で基本要素間の通信路を設定し，③で評価すべき基本要素（以下，評価要素と呼ぶ）を決定する．

表 2 各フェーズで用いるワークシート
Table 2 Work-sheets used in each phase.

フェーズ	ステップ	作成するワークシート
(Ⅰ)評価対象のモデル化	(a)包含ツリー分析	包含ツリー図
	(b)通信路設定	通信路マトリックス
	(c)評価要素の決定	評価要素リスト
(Ⅱ)脅威の抽出	(a)５W 展開	５W 展開図
	(b)重複脅威の解消	脅威リスト
(Ⅲ)対策方針の導出	(a)フォールトツリー解析	フォールトツリー図
	(b)対策方針の導出	対策方針リスト
	(c)重複対策の解消	
(Ⅳ)セキュリティ目標の確立		脅威／セキュリティ目標マトリックス
(Ⅴ)セキュリティ対策の策定		セキュリティ対策リスト

（2）脅威の抽出（フェーズ II）

①5W（Where, Who, When, Why, What）展開, ②重複脅威の解消, を各評価要素ごとに繰り返す．これにより，各評価要素を襲うと想定される脅威（What）を抽出する．なお，②の重複脅威の解消は，脅威が 5W 展開の各事象ごとに個別に抽出されるため，これら脅威間で同一内容のものが存在しているかをチェックする作業である．

（3）対策方針の導出（フェーズ III）

①フォールトツリー解析，②対策方針の導出，を脅威，評価要素ごとに繰り返し，引き続き，③重複対策の解消，を評価要素ごとに繰り返す．これにより，各評価要素で実施すべき対策方針を導出する．なお，③の重複対策の解消は，対策方針が各脅威ごとに個別に導出されるため，これら対策方針間で同一のものが存在しているかをチェックする作業である．

（4）セキュリティ目標の確立（フェーズ IV）

上記（3）で抽出した脅威と，上記（4）で導出した対策方針との関連を，評価要素ごとに明確化する．これより，達成すべき対策方針をセキュリティ目標として確立する．

（5）セキュリティ対策の策定（フェーズ V）

上記（4）で確立したセキュリティ目標を実現するための対策機能の概要を決定する．

なお，実際の作業では，**表 2** に示す各種ワークシートを作成しながら進めることにより，これらのプロセスを効率的に実行することを実現する．以下，これらの各フェーズごとに，そこでの作業内容を詳細に示す．

4.2 評価対象のモデル化（フェーズ I）

4.2.1 ステップ 1：包含ツリー分析

包含ツリー分析作業は，評価対象となるシステムの基本要素を明確化する作業である．頂上要素を，それに包含される下位の構成要素にツリー状に展開し，それ以上は展開不要である要素（以下，基本要素と呼ぶ）にいたるまで展開を続ける．この分析作業には，表 2 で示したワークシート「包含ツリー図」を用いる．ここでは，3.1 節で示した図 1 の例を用いて包含ツリー図の作成について説明する．図 1 の個々の要素は楕円（これをノードと呼ぶ）と略称で表示され，要素間の関係は線分で表示される．略称は，要素の特徴を端的にとらえて作業者が考案し，ノード内に文字列として入力する情報であり，通常は名詞を使用する．包含ツリー図の作成は，頂上要素に評価対象システムを設定し，下位の要素への展開は作業者の洞察にまかされる．このとき，要素間の通信路は次ステップで設定するので，ここでは除外して洞察する．図 1 の例では，基本要素として E11，E121，E122，E21，E22 が展開されている．

4.2.2 ステップ 2：通信路設定

通信路策定作業は，ステップ 1 で展開した基本要素に対し，必要に応じて各要素間の通信路を設定する作業である．この設定作業には，表 2 で示したワークシート「通信路マトリックス」を用いる．通信路マトリックスは，ステップ 1 で展開した基本要素を縦軸と横軸に設定したものである．図 1 の包含ツリー分析例に対する通信路マトリックスの例を**表 3** に示す．基本要素間で通信路が存在する場合に，マトリックスの該当する欄に「C」を記入する．表 3 の例では，E11-E122，E121-E21，E121-E22，E122-E21 の間に双方向の通信路が存在することが示されている．本ステップ作業により，評価対象システムの通信路をもれなく抽出することができる．

4.2.3 ステップ 3：評価要素の決定

包含ツリー分析および通信路設定作業により抽出した基本要素および通信路から，セキュリティシステム計画を行う目的に応じて評価すべき対象の要素（評価要素）を決定する．ここで決定した評価要素は，表 2 に示すワークシート「評価要素リスト」の形式でまとめる．評価要素リストは，抽出した基本要素および通信路を列挙し，そのうちどれを評価要素とするかを示

表 3 通信路マトリックス例
Table 3 Example of communication path matrix.

	E11	E121	E122	E21	E22
E11			C1		
E121				C2	C3
E122	C1			C4	
E21		C2	C4		
E22		C3			

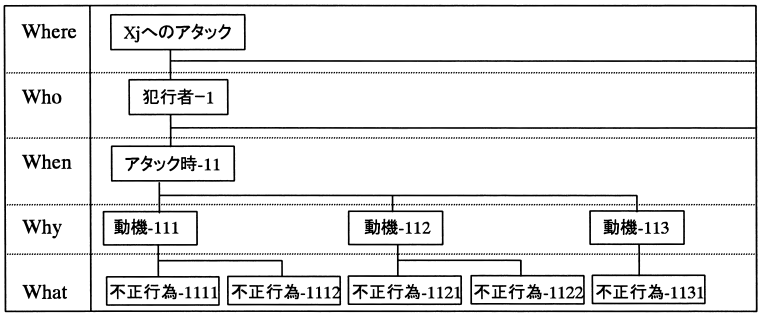

図 3 5W 展開図例
Fig. 3 Example of 5W derivation.

すものである．また，評価要素に対しては，その概要と選択した理由もあわせて記載しておく．

4.3 脅威の抽出（フェーズ II）

4.3.1 ステップ 1：5W 展開

5W 展開作業は，前節で抽出した評価要素ごとに，それを襲うと想定される脅威を 5W（Where，Who，When，Why，What）の視点から誘導することにより，もれなく抽出する作業である．この展開作業には，表 2 で示したワークシート「5W 展開図」を用いる．5W 展開図の例を**図 3** に示す．個々の展開項目は長方形とその特徴を端的にとらえる名称で表示する．図 3 の例では，評価要素 Xj についての 5W 展開図が以下の構成で展開されている．図 3 の最後の What の段に展開された事象が，Where で対象としている評価要素に対する不正行為，すなわち，脅威となる．

(1) Where：評価要素 Xj に対するアタック
(2) Who：評価要素 Xj へのアタックは，犯行者-1，または，犯行者-2，… によってなされる．
(3) When：犯行者-1 によるアタックは，アタック時-11，または，アタック時-12，… に実行される．
(4) Why：アタック時-11 のアタックの動機は，動機-111，または，動機-112，または，動機-113 である．
(5) What：動機-111 による不正行為は，不正行為-1111，または，不正行為-1112 である．

4.3.2 ステップ 2：重複脅威の解消

評価要素 Xj に対する 5W 展開により抽出された不正行為（What），すなわち，脅威間での重複を解消するための作業である．上記ステップ 1 により展開された各不正行為内容を比較し同一内容のものがある場合は，5W 展開図でのそれら各不正行為に対し同一名称を設定する．

以上の 5W 展開，重複脅威解消の 2 ステップの作業を，すべての評価要素について繰り返す．この結果を表 2 に示したワークシート「脅威リスト」としてまとめる．脅威リストは，各評価要素ごとに，抽出された不正行為とその概要を示したリストである．

4.4 対策方針の導出（フェーズ III）

4.4.1 ステップ 1：フォールトツリー解析

フォールトツリー解析作業は，対象とする評価要素に対して，フェーズ II にて抽出した各脅威の生起に関する論理的な因果関係を明確化する作業である．この作業は 5W に対して How に相当する解析作業である．この解析作業には，表 2 に示したワークシート「フォールトツリー図」を用いる．**図 4** に，評価要素 Xj に対する脅威（不正行為-1111）についてのフォールトツリー図の例を示す．評価要素 Xj に対する脅威（不正行為-1111）を頂上事象として下位事象に展開しており，個々の事象は長方形とその内容を示す短文とで構成する．図 4 で示される内容は，次のとおりである．

(1) 頂上事象である不正行為-1111（What）の生起

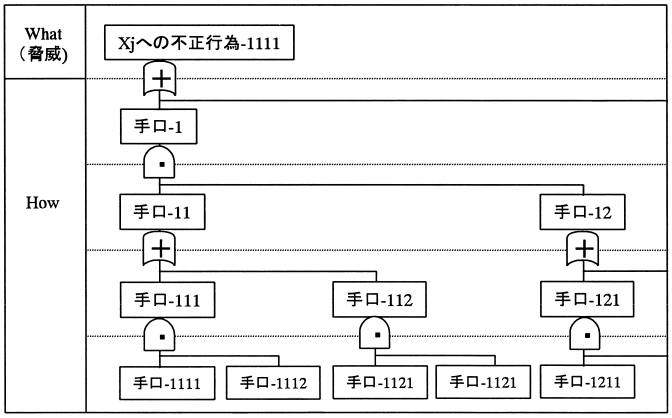

図 4 フォールトツリー図例
Fig. 4 Example of FTA.

表 4 対策方針リスト例
Table 4 Example of countermeasure guideline list.

脅威	対象評価要素	評価要素 Xk での対策方針	対策方針概要
不正行為-1111	Xj	対策方針 Xk-1	XXXXXXXXXXX
不正行為-1111	Xj	対策方針 Xk-2	XXXXXXXXXXX
不正行為-1112	Xj	対策方針 Xk-3	XXXXXXXXXXX

の原因は，手口-1 の生起，または，…，である．

(2) 手口-1 の生起の原因は，手口-11 の生起，かつ，手口-12 の生起である．

(3) 手口-11 の生起の原因は，手口-111 の生起，または，手口-112 の生起である．

(4) 手口-111 の生起の原因は，手口-1111 の生起，かつ，手口-1112 の生起である．

なお，フォールトツリー解析において，これ以上展開できない，または，展開する必要がないと考えられる最下位の事象を基本事象と呼ぶ．

4.4.2 ステップ 2：対策方針の導出

対策方針の導出作業は，上記ステップ 1 で作成したフォールトツリー図に基づいて，頂上事象の脅威の生起を抑止するための対策方針を導出する作業である．ここで基本となる考え方は，「基本事象の生起を抑止することが，頂上事象の脅威の生起を抑止することにつながる」ということである．すなわち，基本事象の生起を抑止することを対策と位置付け，AND ゲート，OR ゲートによる分岐の構造を考慮しながら，頂上事象を抑止するための対策を策定するための方針を導出する．なお，ここで，対策とはシステムとしての対策であることから，「現在注目している評価要素 Xj ではなく，他の評価要素 Xk での対策により，評価要素 Xj に対する基本事象の生起を抑止する」という場合もありうる．たとえば，クライアント端末に対する不正行為を，サーバマシンで検出しその不正行為の成立を抑止するというような場合である．したがって，本ステップで導出した対策方針のそれぞれに対し，どの評価要素に対する対策方針であるかを明確化することが必要である．本ステップ作業の結果は，表 2 に示したワークシート「対策方針リスト」にまとめる．対策方針リスト例を**表 4** に示す．対策方針リストは，脅威の対象となる評価要素（Xj）ではなく，対策がなされる評価要素（Xk）ごとに作成する．

上記のステップ 1，2 を，対象とする評価要素（Xj）に対するすべての脅威について繰り返し実行する．さらに，この作業をすべての評価要素に対して実行することにより，表 4 の対策方針リストを完成する．

4.4.3 ステップ 3：重複対策の解消

上記作業により導出した対策方針間での重複を解消するための作業である．上記作業の結果作成された対策方針リストの各対策方針内容を比較し同一内容のものがある場合は，それらをまとめて 1 つの対策方針として再定義する．対策方針リストは，対策がなされる評価要素ごとに作成されており，本ステップの作業も対策がなされる評価要素ごとに繰り返す．本ステップ作業完了後の対策方針リストに記載されている対策方針を，評価要素 Xk（対策がなされる評価要素）に対するセキュリティ目標と呼ぶ．

4.5 セキュリティ目標の確立（フェーズ IV）

このフェーズでは，フェーズ II で抽出したすべての脅威と，フェーズ III で導出したすべてのセキュリティ

表 5 脅威/セキュリティ目標マトリックス例
Table 5 Example of threats/security-objectives matrix.

セキュリティ目標 / 脅威		評価要素 X1			評価要素 X2			...
		目標 X1-1	目標 X1-2	...	目標 X2-1	目標 X2-2	...	...
評価要素 X1	脅威 X1-1		●		●			...
	脅威 X1-2	●						...
	...							...
評価要素 X2	脅威 X2-1					●		...
	脅威 X2-2					●		...
	...							...
...	...							...

表 6 セキュリティ対策リストフォーマット
Table 6 Format of security countermeasures list.

脅威	セキュリティ目標	対策	
		情報処理技術による対策	運用による対策
脅威 X1-1	目標 X1-2	XXXXXXXXXXXXXXX	XXXXXXXXXXXXXXX
	目標 X2-1	XXXXXXXXXXXXXXX	XXXXXXXXXXXXXXX
...	...	...	...

目標との関連を明確化することによりセキュリティ目標の妥当性をチェックし，最終的にセキュリティ目標を確立する．この作業には，表 2 に示されるワークシート「脅威/セキュリティ目標マトリックス」を用いる．**表 5** にこのマトリックスの例を示す．マトリックスの縦軸にはすべての脅威を，横軸にはすべてのセキュリティ目標を配置し，脅威と目標が関連する欄には●を記入する．表 5 で，縦軸の $X1, X2, \ldots$ は脅威の対象となる評価要素を示し，横軸の $X1, X2, \ldots$ は対策がなされる評価要素を示す．このマトリックスにより，ある脅威は，どの要素に対するどのセキュリティ目標により対策がなされるかを一覧することが可能となる．

4.6 セキュリティ対策の策定（フェーズ V）

このフェーズでは，上記フェーズ IV で確立したセキュリティ目標を実現するための対策機能の概略を決定する．セキュリティ対策には，情報処理技術による対策と運用による対策が存在するが，達成しようとする目標に応じてどちらの対策とするか，また，それらを組み合わせるか，を適切に設計することが重要である．情報処理技術対策の場合はその機能概略を，運用対策の場合は運用内容概略を決定し，対象としているセキュリティ目標と対応付けてセキュリティ対策リストとして，**表 6** の形式にまとめる．

以上の 4.2 節〜4.6 節で示した手法に基づくことにより，対象とするシステムに応じて，そのシステムを襲うと想定される脅威を体系的・論理的に抽出し，抽出した脅威に対して過不足のないセキュリティ対策を効率的に導出することが可能となる．

5. 事例による評価

前章までで提案した手法を，ケーススタディとして，IC カードを利用したチケット販売・入場ゲート管理システムのセキュリティ対策立案に適用することにより，以下の結果を得た．

5.1 適 用 結 果

（1）本手法による解析結果

「評価対象システムのモデル化」（フェーズ I）作業により，評価要素として通信路を含む 13 個の要素を抽出した．これら各要素の中で有人発券端末部分に対して「脅威の抽出作業」（フェーズ II）を実施することにより，脅威として 40 個の不正行為を抽出した．そのうち影響度の大きい上位 3 個の脅威に対して 42 個のセキュリティ目標を，「対策方針の導出」（フェーズ III），「セキュリティ目標の確立」（フェーズ IV）作業により導出した．以上のプロセスを経て，最後の「セキュリティ対策の策定」（フェーズ V）作業により，情報処理技術によるセキュリティ対策 31 個，運用によるセキュリティ対策 50 個を導出することができた．

（2）マンパワー

上記作業を実施するにあたり，4 人・月のマンパワーを要した．このうち，評価対象のモデル化に 0.3 人・月，脅威の抽出/対策方針の導出/セキュリティ目標の確立に 2.5 人・月，セキュリティ対策の策定に 1.2 人・月を費やした．なお，本適用を効率的に進めるために，パーソナルコンピュータ上に，フォールトツリー作成支援ツールのプロトタイプを開発した．

5.2 適用結果の評価，考察

本章での事例適用を通じて得た評価，考察を以下に

示す.

（1）本提案手法の各フェーズでの実施内容は以下のとおりである.

①評価対象のモデル化（フェーズ I）

評価対象の構成要素を，ホストシステム/店舗システム/…，さらに，店舗システムの構成要素を有人発券端末/無人発券端末/IC カード/…，というように，体系的に詳細化してゆくことが可能であった.

②脅威の抽出（フェーズ II）

Where として有人発券端末を選択し，有人発券端末に対する Who として関係者/利用者/…，を抽出，関係者に対する When としてカード発行時/…，を抽出，カード発行時の Why として不正利益取得/…，を抽出，というように展開し，不正利益取得という観点からの脅威として何が発生しうるか（What）を抽出した．これより，体系的に脅威（What）を抽出することが可能であった.

③対策方針の導出（フェーズ III）

フェーズ II で抽出した各脅威に対して，その脅威が発生するための条件を，フォールトツリー解析の手法を用いてトップダウンに解析を実施した．本作業実施者の意見を，意見が出されるごとにフォールトツリーの形でまとめてゆくことは，議論を体系立てて効率的に進めるうえで有効であった.

④セキュリティ目標の確立（フェーズ IV）

フェーズ I〜III までの作業結果を，表 5 で示したマトリックスの形式にまとめることにより，各評価要素および，各脅威とそれに対するセキュリティ目標の関係を一覧することが可能となる．表 5 は，本作業を通じた議論での漏れ，抜けがないかの確認に有効であった.

⑤セキュリティ対策の策定（フェーズ V）

表 6 で示した形式で，脅威とそれに対するセキュリティ目標が明確になっているため，セキュリティ目標を達成するためにどのような対策を講ずるべきかの検討を効率的に進めることが可能であった.

上記フェーズ I〜IV の作業は，複数メンバによるブレーンストーミング形式で実施した．本手法の手順をとることにより，作業実施者間の考えの方向性を一致させることができ，議論の発散を避け，効率的に作業を進めることが可能であった.

以上のことにより，試行錯誤的ではなく，本提案手法による体系だった作業を行うことにより，抽出すべき脅威の漏れ，抜けを極力少なくすることが可能であると評価できる．また，抽出した各脅威と策定した各セキュリティ対策との対応が，本提案手法の実行を通じて明確になっているため，抽出した脅威それぞれに対して，セキュリティ対策が施されていることの検証を行ううえでも有効であることが確認できた.

（2）セキュリティ対策の策定には，セキュリティ設計者と，対象とするシステムを担当する専門家との共同作業が必須である．本提案手法の特に，フェーズ I〜III の作業を進める過程で，専門家が持つ見識を具体的に引き出すことができた．さらに，これら作業を通じて，対象システムの担当者に対し，発生しうる脅威，セキュリティ対策の理解，納得，意識付けが同時になされ，この面でも有効であった.

（3）上記（1),（2）の評価より，本提案手法は，従来，情報システム化されていなかった分野を含むシステムに対するセキュリティ対策立案時，また，既存システムに新規システムを追加する場合の新規部分に対するセキュリティ対策立案時に，特に，有効であると考えられる.

（4）本計画手法の適用により作成した，包含ツリー図，5W 展開図，フォールトツリー図は，それぞれ，対象とするシステムの構造，対象システムに対する脅威とその原因を体系的に示したものである．このため，他の同様なシステムで再利用することができ，この場合は，既作成図をベースにフェーズ I〜III の作業を進めることが可能である．これにより，特にマンパワーを要するフェーズ II，III の作業を効率的に進められることが確認できた.

（5）今回の適用では，作業の効率化を目的としてパーソナルコンピュータ上で動作する支援ツールプロトタイプを開発し，それを利用した．本提案手法では，各フェーズで作成するワークシートが明確に規定されているため，ツールとして支援すべき内容が明確であり，支援ツールの設計が容易であった．また，フェーズ II，III の作業において，5W 展開図，フォールトツリー図作成をツールにより自動化することは，作業メンバの議論を効率的に進めるうえで，特に有効であった.

（6）今後，本提案手法をさまざまな対象に適用するにあたっては以下の考慮が必要である.

①大規模なシステムの場合，いくつかの構成要素ごとに複数のグループに分かれて，並列して本提案手法のプロセスを進めることが考えられる．この場合，各グループで導出した脅威，セキュリティ目標を統合することが必要であり，各グループ間で事前に用語を統一しておくことが望ましい.

②本提案手法により導出した対策に対し，実際のシステム開発においてそれらのうちのどこまでの対策を

施すかは，脅威発生による影響度，対策実現に要するコストなどを考慮して決定することが必要である．

③本提案手法は，システムを構成する各要素ごとにそれらに対する脅威を体系的に抽出し，セキュリティを守るうえで必要となる対策項目を導出するものである．これら対策項目を実現するセキュリティシステムを設計するにあたっては，対策項目間でのシステム全体としての整合性を考慮して設計することが必要である．

④セキュリティ対策立案作業実施者の想定できない脅威，新たなアタック方式の発見による脅威が存在する可能性があるため，本提案手法によっても，対象とするシステムに発生しうるすべての脅威を抽出することは保証できない．このため，システム運用後においても，セキュリティ監視，侵入テストなどによる，セキュリティ対策の定期的な見直しを行うことが必要である．本提案手法により作成した各種ワークシートは，立案したセキュリティ対策の根拠を示すものであり，この見直しの際においても，有効に活用できると考えられる．

なお，それぞれの評価対象で作成した，5W 展開図，フォールトツリー図，セキュリティ対策リストをデータベース化することにより，大幅な効率化が可能となる．今後，さまざまな対象に適用した結果をパターン化，蓄積してゆくことが有効であると考える．

6. おわりに

情報システムが社会において果たす役割が増大するとともに，情報セキュリティに対する脅威が増大している．これに対応するためには，対象となるシステムの特徴，利用形態に応じたセキュリティ対策を講じることが必要である．本論文では，フォールトツリー分析をベースとし，セキュリティ対策を体系的，効率的に立案するための計画手法を提案した．本手法は，対象とするシステムを襲うと想定される脅威を体系的・論理的に抽出し，これに対して過不足のないセキュリティ対策を効率的に導出すること目的とし，(1) 評価対象のモデル化，(2) 脅威の抽出，(3) 対策方針の導出，(4) セキュリティ目標の確立，(5) セキュリティ対策の策定，の 5 つのプロセスを実施するものである．また，提案手法を具体的なシステムのセキュリティ対策立案に適用することにより，体系的な脅威の抽出とそれに対する対策の立案を効率的に行えることを確認した．

謝辞 本研究を進めるにあたり，ご指導，ご鞭撻いただいた，(株) 日立製作所システム開発研究所片岡雅憲所長，宝木和夫セキュリティシステム研究センタ副センタ長，および，本研究にご協力くださった，(株) 日立製作所情報システム事業部武村泰夫技師，Pennsylvania State University 太田和泉氏をはじめとする関係者の方々に深く感謝する．

参考文献

1) 日本セキュリティ・マネジメント学会：セキュリティハンドブック I，日科技連 (1998).
2) 宝木ほか：情報システムにおけるリスク分析の一手法，電学論 C，Vol.108, No.4, p.260 (1988).
3) 総合安全工学研究所：FTA 安全工学，日刊工業新聞社 (1979).
4) 電子商取引実証推進協議会共通セキュリティ関連技術 WG：共通セキュリティ関連技術 WG 中間報告書 (1997.5).
5) http://csrc.gov/cc/ccv20/ccv2list.htm
6) 日本情報処理開発協会 (編)：リスク分析調査報告書 (1984.12–1989.3).
7) 佐々木ほか：インターネットセキュリティ—基礎と対策技術，オーム社 (1996).
8) 大鐘：SNMP と CMIP—TCP/IP と OSI ネットワーク管理，ソフト・リサーチ・センタ (1993).

(平成 11 年 5 月 19 日受付)
(平成 11 年 11 月 4 日採録)

織茂 昌之（正会員）

1979 年京都大学工学部機械工学科卒業．1981 年同大学大学院修士課程修了（精密工学）．同年（株）日立製作所入社．同社システム開発研究所にて，自律分散システム技術，セキュリティシステム技術等の研究開発に従事．1998 年より同社情報・通信グループ新事業推進センタ勤務．情報メディア関連事業の推進に従事．IEEE，計測自動制御学会各会員．

津原　進（正会員）

1970 年九州工業大学電気工学科卒業．同年（株）日立製作所入社．同社中央研究所等を経て，現在，システム開発研究所セキュリティシステム研究センタ勤務．生産計画と管理，文書画像処理，小形計算機の応用ソフトおよび基本ソフト，計算機ネットワークの設計・構築とその運用・管理，ヘルプデスクの設計・構築に関する研究の後，現在，セキュリテイ・システムの計画に関する研究に従事．電子情報通信学会，計測自動制御学会，日本ファジィ学会，電気学会各会員．立教大学非常勤講師．工学博士．

山本　倫子

1997 年東京理科大学基礎工学部電子応用工学科卒業．同年（株）日立製作所ビジネスシステム開発センタ入社．1998 年より同社システム開発本部勤務．現在，セキュリティシステムの構築・評価技術の開発に従事．

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）．著書に，「情報科学入門—教養としてのコンピュータ」（日本理工出版会，1995 年），「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，電気学会等会員．昭和 58 年電気学会論文賞受賞．平成 10 年電気学会著作賞受賞．立教大学，香川大学等の非常勤講師を経験．