SCIS 2013 The 30th Symposium on Cryptography and Information Security
Kyoto, Japan, Jan. 22- 25, 2013
The Institute of Electronics, Information and Communication Engineers

セキュリティ保証ケースを用いた対策立案方法の提案

Proposal on Countermeasure Decision Method using Security Assurance Case

金子朋子* 山本修一郎† 田中英彦*
Kaneko Tomoko Yamamoto Shuichiro Tanaka Hidehiko

あらまし ソフトウェアのシステム開発において，お客様の要求を適切に把握し，実現させることは非常に大切なことである．しかし，上流工程における要求分析が不十分であるためにシステム開発に重大な影響を及ぼすことは多い．特にセキュリティ要求分析においては，的確に脅威を洗い出したとしても，それに対する対策が不十分では，お客様が望む品質を確保したとはいえない．システムや製品が望ましい性質をもち，危険な状況に陥らないことを保証することは，特にお客様から望まれている．そこで本論文では，脅威やリスクに対して，保証できる範囲を明確にし，顧客と議論の上で合意を得る手順を示す．問題の解決に必要な手法として，保証（アシュアランス）ケース（ISO/IEC15026）を用いて，セキュリティ独自の観点で必要なモデルをセキュリティ保証ケースとして提唱する．また，セキュリティ保証ケースを使用した対策の具体的立案手順と事例を示す．さらに GSN に代表される図形式の保証ケースと等価性をもつ表形式の保証ケースを提案し、この具体的事例を示す．

キーワード セキュリティ要求分析，保証ケース，セキュリティ対策の立案，GSN，ISO/IEC15026

1 はじめに

まず 2 章関連研究で信頼性とセキュリティ特性の比較，リスク分析，ソフトウェア開発ライフサイクル保証ケース，2.5 Security Assurance Case について述べる．3 章で保証ケースの意義と課題，4 章でセキュリティ特性から考察したセキュリティ保証ケースの意義と課題，5 章で対策立案の作成手順，6 章でセキュリティ保証ケースによる対策の具体的手順と適用事例を示す．7 章で提案事例を評価し，8 章で今後の課題をまとめる．

2 関連研究

2.1 信頼性とセキュリティ特性

セキュリティとディペンダビリティの定義[1]によるとセキュリティとディペンダビリティに共通する属性は可用性と一貫性でセキュリティに独自な属性は秘匿性である．セキュリティ対策立案の手法を検討するにあたり、セキュリティとディペンダビリティの違いを明確にし、セキュリティ特性を反映できることが望まれる．

2.2 リスク分析

ISO27001(JISQ27001) [2]によると、リスクアセスメントとはリスク分析からリスク評価までの全てのプロセスである．リスク分析はリスク因子を特定し、リスク算定することで実施され，その結果でリスク評価をする．リスクアセスメント手法には各種定性的評価手法、定量的評価手法があるが，GMITS の詳細リスク分析は代表的な手法の１つである．

2.3 ソフトウェア開発ライフサイクル

ISO/IEC12207 [3] はソフトウェアライフサイクル国

* 情報セキュリティ大学院大学，〒221-0835 神奈川県横浜市神奈川区鶴屋町 2-14-1,Institute of Information Security, Tsuruya-cho, Kanagawa-ku, Yokohama-city, Kanagawa, JAPAN
† 名古屋大学，〒464-8601 名古屋市千種区不老町, Nagoya University, Furo-cho, Chikusa-ku, Nagoya, JAPAN

際標準規格である．共通フレーム 2007 [4]（SLCP-JCF2007）は，上記規格から日本のソフトウェア産業界で必要とされるプロセスや作業項目等を鑑みて追加，変更して作成されたフレームワークであり、ソフトウェアのライフサイクルプロセスにわたる共通の物差しを提供する．各プロセスごとに発注者側も含めて役割を明確化した手順を示し、取引の更なる可視化の実現を目指している．

信頼できるコンピューティングのセキュリティ開発ライフサイクル[5]では，マイクロソフトでの開発プロセスのセキュリティに重点を置いた活動を記載している．

2.4 保証ケースについて

ISO/IEC15026 part2 に定義されるアシュアランスケース assurance case（以後，保証ケースと呼称）とは，システムが重要安全性を満足することを示す手法である．ISO/IEC15026[6] や OMG の ARM （ Argument Metamodel） [7] と SAEM （Software Assurance Evidence Metamodel）[8]などで標準化がすすめられている．

ISO/IEC15026 では，対象範囲，適合性，利用法，保証ケースの構造と内容，適用成果物などについて規定している．代表的な表記法は、欧州で約 10 年前から使用されている GSN（Goal Structuring Notation）[9] [10]である．イギリスの University of York で開発され，要求を抽出した後の確認に用い，システムの安全性や正当性を確認するための手法である．

OMG では，構造化保証ケースメタモデル Structured Assurance Case Metamodel (SACM)の標準化を進めている．SACM には議論メタモデル Argumentation Metamodel (ARM) と，ソフトウェア保証証跡メタモデル Software Assurance Evidence Metamodel (SAEM) の２つの仕様がある．ARM では構造的な方法によって開発対象システムやサービスが保証要求に合っていることを確認することができる．ARM では，異なる表記法に対するメタモデル ARM(ARgumentation Metamodel) を定義しているので，GSN や CAE(Claims-Arguments-Evidence)などの類似しているが異なる保証ケースを記述する手法の差を吸収して，構造化された議論ができる．これに対して SAEM では，コンプライアンスやリスク分析で必要となる証跡要素の詳細なモデルを定義できるメタモデルを提供する．SAEM 構造によってソフトウェア保証の過程でシステムの証跡を格納，相互参照，評価，報告するためのツールを容易に構築できるように論理設計の基礎を提供している．

他に法律ドメインで Assurance Case の理論的背景となる Toulmin Structures[11],イギリス Adelard 社、City University London の開発した要求，議論，証跡のみのシンプルな ASCAD[12]もある．日本国内では GSN を拡張した D-CASE[13] [14]が JST CREST DEOS プロジェクトで推進されている．保証ケースを用いたサービス提供判断方法の提案[15]もなされている．

2.5 Security Assurance Case

日本国内ではセキュリティ独自の観点にわたって，具体的手順、事例を示している研究はほとんどない．海外では metrics，論議，証跡について以下のような研究がなされている．

GSN を提唱した YORK 大学の Tim Kelly ら[16]が Security Assurance Cases の作成に関する既存の手法とガイダンス，安全性とセキュリティの定理的および実践的な違い，現在のセキュリティ実践の潜在的効果，セキュリティケースに移行する実践的側面などを述べている．しかし, 具体的事例は示しておらず, Security Assurance Cases に関する詳細なガイダンスは数年のうちに発表するとしている．

Software Engineering Institute の Goodenough J[17]らはバッファオーバーフローのコーディング欠陥の事例を通じて，セキュリティに対する Assurance Cases 文書作成のアプローチを説明している．Software Engineering Institute の Lipson H[18]らは信頼できるセキュリティケースには保証の証跡こそが重要であると主張している．

T. Scott Ankrum[19]らは ASCAD を使用し、高難易度の航空システムにＣＣも利用したセキュリティ保証ケースを適用した事例を示している．

IEEE インターナショナルワーキンググループでは，2005 年のワークショップのレポート[20]や IEEE の SECURITY & PRIVACY2006 の記事[21]や 2007 年にはメトリックスの重要性を論議などでセキュリティに関する Assurance Cases に関する検討状況[22]を公開している．

Vivas [23]らは，システム開発に伴う保証ケースを統合した保証メソドロジを提唱している．セキュリティのシステム開発のライフサイクルを通じてセキュリティケースを構築、維持するためのメソドロジを開発することを目指している．PICOS（コミュニティサービスに対するプライバシーとアイデンティティ管理）プロジェクトでは PICOS 保証ケースを提唱している．

3 保証ケースの意義と課題

3.1 保証ケースの意義

保証ケースとは何でありその意義と課題は何かを最初に説明したい．

ISO/IEC15026 の定義によると，保証ケースの構造と内容に対する最低限の要求は，システムや製品の性質に対する主張(claim)，主張に対する系統的な議論（argumentation），この議論を裏付ける証跡(evidence),

明示的な前提（explicit　assumption）が含まれること，議論の途中で補助的な主張を用いることにより、最上位の主張に対して、証跡や前提を階層的に結び付けることができることである．この定義を満たすものは保証ケースとみなすことができる．

保証ケースの意義として，大きく 2 点に分けて論じる．１つめは，構造化による保証要求の確認のしやすさである．保証ケースでは，システム保証に関する議論を構造化して開発対象システムやサービスが保証要求に合っていることを確認することができる．フリーテキストの場合より構造化されている保証ケースの方が要求を記載する場合，ゴールが何であり，前提条件に何があり，どのような戦略で何を実施すべきかを視覚的に捉えやすい．そこで重要システムの実行中に優先順位の高い要求を満足することを確認することなどに，保証ケースが利用できる．

2 つめは，ゴールを達成できる証跡を残すことで根拠が明確になることである．後から問題が生じた場合の証跡に戻ってどのような判断のもとに何を決定したのかを確認することができる．また顧客との合意をとった証跡であれば，法的な問題が生じた際にも根拠とできる．ソフトウェア開発という形のないものを作成する場合，顧客との合意形成は重要であり、合意形成のツールとして，保証ケースは役立つものにできる．

3.2　保証ケースの課題

3.1 項の定義をみたすものは保証ケースであるが，逆にいえば，これ以外に具体的な手順，証跡の残し方に対する詳細な規定はない．そして保証ケースには以下の課題があると考える．

① システムに対する信頼性の高い保証をするためには，具体的な作成手順，証跡の残し方の基準設定が必要である．この基準設定のあいまいさが保証ケースの課題である．
② 作成段階で保証ケースを作り，レビューし証跡を残すのは従来の作業からの追加となり，時間も稼働コストも余計に必要になることが課題である．
③ 更に保証ケースをライフサイクルにわたって使用する場合，①作成，②レビュー，③維持管理，④再利用の各段階にわたるサポートやツール等がないことが課題である．
④ 保証ケースは GSN がディペンダビリティに適用されてきた経緯があり，セキュリティに適用されている事例は少ない．また，セキュリティ独自の観点にわたって，具体的手順、事例を示している研究は数少ない．セキュリティ特性に対応した保証ケースがないことが課題である．
⑤ 現状では保証ケースのほとんどが図形式の記法だが，図形式は記述要素が多くなると複雑でわかりにくくなる課題がある．

4　セキュリティ特性からみたセキュリティ保証ケースの提案と意義

4.1　セキュリティの特性とリスク

セキュリティ特性に対応した保証ケースがないことが課題の１つであると 3.2 項に示した．ではセキュリティ特性とはどのようなものであろうか？

国際標準を取り込んだ JIS Q 27001（=ISO/IEC 27001）においては情報セキュリティ（information security）は情報の機密性、完全性および可用性を維持すること．さらに真正性，責任追跡性，否認防止および信頼性のような特性を含むことができるとされている．

機密性（confidentiality）とは許可されていない個人、エンティティ又はプロセスに対して、情報を使用不可又は非公開にする特性である．完全性（integrity は資産の正確さおよび完全さを保護する特性である．可用性（availability）とは許可されたエンティティが要求した時に、アクセスおよび使用が可能である特性としている．ほかに真正性（情報およびそのユーザーが本物と確認できること），責任追跡性（問題が発生した時のその動作が開始された元まで追跡できること），否認防止（あとから否定（ごまかし）ができないこと），信頼性（情報システムを構成する機器が意図した通りに動作していること）もセキュリティの属性とされる．

脅威と脆弱性との関係からリスクを考察してみる．

脅威とは、それに悪意が伴うかに関係なく、結果的に組織が保有する情報資産に対して害を及ぼす、または発生する可能性のある事象であり，盗難や不正アクセス、紛失、操作ミス、故障などの他に、地震や火災、洪水といったものも脅威である．

脆弱性とは、組織の情報セキュリティ体制上、これらの脅威に対する攻撃に弱い状態のことである．第三者が脅威となる行為(システムの乗っ取りや機密情報の漏洩など)を行うことができる欠陥や仕様上の問題点といったシステム上の問題点や、機密情報の管理体制が整っていないなどといった人間の振る舞いに関する問題点も脆弱性となり得る．

リスクとは、組織の情報セキュリティの脆弱な部分を付いて脅威が侵入し、情報資産の漏えいなどといった被害を及ぼす可能性のことである．情報セキュリティが100%完全なものであるならば、リスクは0と言えるが、そのようなことはほとんどない．GMITS ではリスク値=「情報資産の価値」×「脅威」×「脆弱性」　としている．

4.2　「セキュリティ保証ケース」の提案と持つべき特性

保証ケースのセキュリティへの適用を筆者らは「セキュリティ保証ケース」と名付け，その提唱をしたいと考

えている.「セキュリティ保証ケース」はセキュリティ特性を重視した手法であるべきである.信頼性確保のために利用されてきた従来の保証ケース以外に「セキュリティ保証ケース」を提唱する理由はセキュリティ特性を考慮した保証ケースが必要であると考えるからである．セキュリティ特性を考慮すると「セキュリティ保証ケース」は「①リスク値を考慮でき,②残存リスクを明確化でき,③頻繁な修正の必要性に対応できる」ことが望ましい．上記３点をあげた理由について以下に具体的な説明をする．

情報セキュリティは，常にリスクを考慮し、低減するために構築される．リスクはセキュリティ特性ごとに存在する，脆弱性を考慮して上で，脅威と情報資産の価値を掛け合わせて把握ができる．このリスク値を考慮した上でのセキュリティ対策の評価・選択が重要になると考える．そこで，リスク値を考慮できる「セキュリティ保証ケース」が必要になる．

リスク対策は起こるかどうかわからない脅威に対する対策であるので，予算や時間等の関係で実施する対策と実施しないものに分かれる．実施されない対策に関してはリスクが残存する．そこで，残存リスクを明確化できる「セキュリティ保証ケース」が必要になる．

セキュリティ対策上，最も厄介なのは悪意の伴う脅威,すなわち，見えない敵の存在である。見えない敵の存在により、予想もしない攻撃を受ける．予想もしない攻撃に対しては，想定外のスコープでの新たな対策が必要になる．想定外の攻撃は頻繁に発生しており、対処には頻繁な修正が必要となる．この頻繁な修正の必要性がセキュリティ最大の特性であり，この対処にはライフサイクルにわたる証跡の維持が必須であると考える．

そこで，ライフサイクルにわたる証跡の維持のために,頻繁な修正の必要性に対応できる「セキュリティ保証ケース」が必要になる．

5　対策立案の作成手順

5.1　対策立案の３ステップ

システム開発からサービス提供にわたるライフサイクルには、要求分析，設計，開発，テスト，運用ライフサイクルにわたる保証があるが、本稿ではそのうちの要求分析における対策立案への適用を対象とする．保証ケースの１つの特長であるゴールを達成できる証跡を残すことであるが，これはどのような対策を実施するのかを決める段階で残しておくことに価値があるからである．

対策立案段階で保証ケースを利用する目的は脅威を的確に対策化するためである．

また，筆者らが提案した脅威分析手法 SARM[23] [24] [25]で洗い出した脅威を用いて，脅威に対する対策の立案を保証ケースで作成し，両手法を統合したセキュリティ要求分析フレームワークに発展させることを予定しているからである．

対策立案を保証するには「①対策評価基準が妥当である，②対策に対する評価が妥当である．③対策の選択が妥当である.」の３段階が必要だと考える．

対策の立案は実施する対策のみの提示では，保証としては不十分である.対策が妥当であると評価するためには評価基準が妥当性をもって定められており，評価基準に対して顧客の承認を得ていることが必要となる．対策は様々な観点からまずは列挙され，その上で実施するものを選択することになるが，選択には妥当性のある評価基準に基づき，妥当性のある評価を実施することとその評価結果に対して顧客の承認を得ていることが必要である．そしてその評価結果に基づき妥当性のある選択を実施し，選択結果に対して顧客の承認得ていることでその選択の経緯が明らかになり，選択結果に対して顧客との合意がなされているといえる．この対策立案の３ステップを踏むことによって，顧客にとっては保証される，ベンダーにとっては保証すべき要件が確定される．

5.2　対策立案のセキュリティ保証ケース

一般的な対策でなく、セキュリティ対策の場合、見えない敵が存在し，想定外の新たな脅威が発生すること，それに対して更なる対策を繰り返す必要が生じる．それゆえ，セキュリティ対策は①当初の想定とは全く違う要件に対応しやすいこと，②繰り返される変更に対処しやすいことが求められる．

セキュリティ対策立案にさいし，「セキュリティ保証ケース」には，セキュリティ独自の観点で実施が望まれる事項や必要とされる以下の事項を含むことが望ましい．

① セキュリティ対策の評価基準に妥当性をもたせるために，コスト・効果などの一般的な基準以外にリスク対応の観点の基準を入れる．
② セキュリティ対策の選択に妥当性をもたせるためには，実施する対策の承認を得るだけでなく、実施しない対策から発生する残存リスクを明確化し、顧客の承認を得る．

このポイントに基づき作成した「セキュリティ保証ケース」を図１に示す．

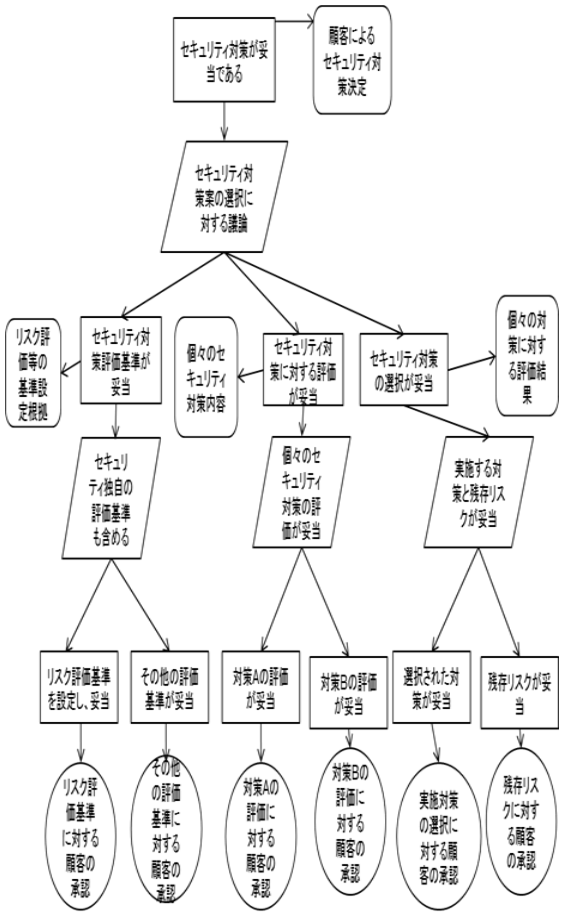

図 1. 対策立案のセキュリティ保証ケース（図形式）

5.3 セキュリティ保証ケース（表形式）の提案

保証ケースを使用した代表的な手法である GSN は図を用いて表現する手法であるが，表を用いて表現する方法も提案されている[13]. ISO/IEC 15026 では，保証ケースが持つべき構造と内容を規定対象としており，保証ケースの品質については規定していない．また，保証ケースについてこれまでに提案されている用語や図式を制限しないように，保証ケースの基本概念だけを標準化している．したがって，表形式による保証ケースの可能性が ISO15026 で否定されているわけではない. 実際のサービス開発作業では，Excel など表形式で階層を表すことができる方が導入が容易であると判断する．この理由は，本稿での提案手法は，表形式で作成するアクタ関係表を用いたセキュリティ要求分析における脅威分析手法により得られた対策と連動する手法を想定しているからである. そこで親和性の高い同じ表形式での作成をする．更に GSN 構文を学習する必要がないことや GSN エディタがまだ普及していない現状では表形式のほうがより作成しやすいという点でもメリットがある.

表形式の保証ケースを提案に際し，GSN と同じ構成要素を備え，同等の表現ができるように意図して作成した．GSN を選んだ理由は最も代表的な保証ケースの手法であり，日本国内で現在普及が推進されている D-CASE も GSN をベースにしているからである.

表形式の保証ケースの作成手順を説明する.

① GSN は上から下へ縦方向のネスト構造になっているが，表形式は左から右へ横方向のネスト構造をとる.

② 表のヘッダ部に前提（context），ゴール（goal），戦略（strategy），サブゴール（subgoal），証跡（evidence）を配置する．任意だが GSN で利用する図形のマークもわかりやすいように設定可能である.

③ GSN で使用する矢印（→）は表形式では左列から右列に矢印がひかれているものとみなし使用しない.

④ 表の要素が 1 対 1 対応の場合は隣列どうしが同じ幅のセルになっている．1 対 n 対応の場合は 1 つの列の隣の列が複数のセルをもつ形式になる.

⑤ ゴール・サブゴールに対する前提条件は該当ゴール・サブゴールの左側に配置され，戦略は右側に配置される.

⑥ 証跡は対応するゴール・サブゴールの右側に配置される.

表 1. 対策立案のセキュリティ保証ケース（表形式）

前提	ゴール	戦略	前提	サブゴール	戦略	サブゴール	証跡
context	goal	strategy	context	goal	strategy	goal	evidence
▭	□	▱	▭	□	▱	□	○
顧客による セキュリティ対策決定	セキュリティ対策が妥当である	セキュリティ対策案の選択に対する議論	リスク評価等の基準設定根拠	セキュリティ対策評価基準が妥当	セキュリティ独自の評価基準も含める	リスク評価基準を設定し、妥当	リスク評価基準に対する顧客の承認
						その他の評価基準が妥当	その他の評価基準に対する顧客の承認
			個々の対策の内容	対策に対する評価が妥当	個々の対策の評価が妥当	対策Aの評価が妥当である	対策Aの評価に対する顧客の承認
						対策Bの評価が妥当である	対策Bの評価に対する顧客の承認
			個々の対策に対する評価結果	セキュリティ対策の選択が妥当	実施する対策と残存リスクが妥当	選択された対策が妥当	実施対策の選択に対する顧客の承認
						残存リスクが妥当	残存リスクに対する顧客の承認

6 セキュリティ保証ケース作成の具体的適用事例

6.1 図形式によるもの

図 2 に「データの改ざんの対策が妥当である」というゴールに対するセキュリティ保証ケースの事例における

作成手順を示す.

① 前提条件として,「顧客によるセキュリティ対策決定」を示す.

② ゴールとして「データの改ざんの対策が妥当である」を示す.

③ 「データの改ざんの対策の選択に対する議論」として,「データの改ざんの対策評価基準が妥当」と「データの改ざん対策に対する評価が妥当」と「データの改ざん対策の選択が妥当」の３つのサブゴールを設定する.

④ 「データの改ざんの対策評価基準が妥当」に対しては,「セキュリティ独自の評価基準も含める」という戦略のもとに「リスク値をＣＩＡごとに求める」と「コスト・効果の一般的評価基準も使用する」というサブゴールが設定され，リスク値を考慮できる保証ケースとなっている.

⑤ 「データの改ざん対策に対する評価が妥当」に対しては,「リスク値とコスト、効果により個々の対策を評価する」という戦略のもとに個々の対策とその根拠が示される.

⑥ 「データの改ざん対策の選択が妥当」に対しては「実施する対策と残存リスクが妥当」という戦略のもとに残存リスクを明確化し，顧客との合意の証跡を残すことができる.

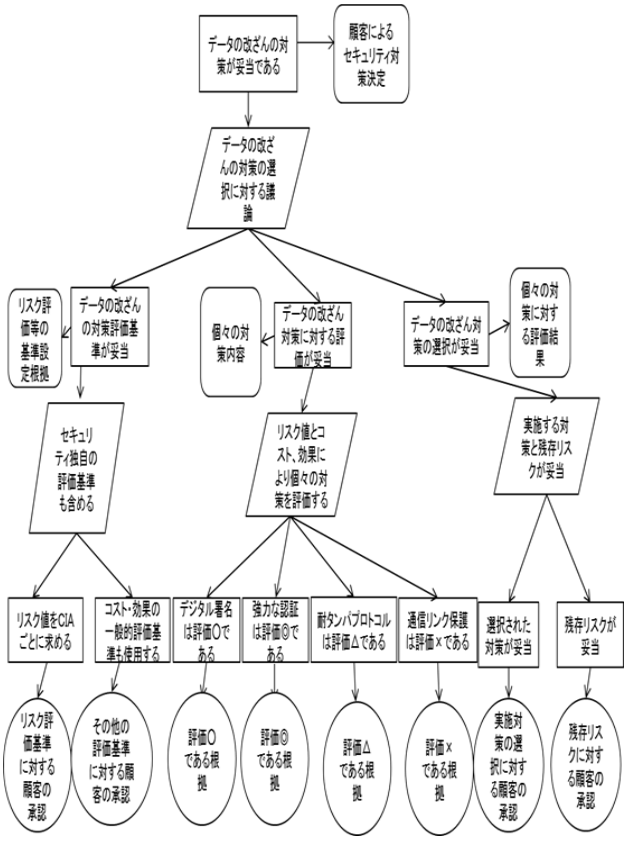

図 2. セキュリティ対策立案の事例（図形式）

6.2 表形式によるもの

表形式のセキュリティ対策立案も図形式と内容は全く同じに記載することができる.

このように図形式と表形式が同じ形式で記載可能な場合,「アクタ関係表に基づくセキュリティ要求分析手法（SARM）を用いたスパイラルレビュー」[23]と同様に両方の手法の長所を利用して，スパイラルレビューを実施することができる．例えば，多人数で思いついてことをホワイトボードなどに書いていく場合，視覚的にわかりやすい図形式を使用し,記載する量が多くなった場合,表形式で一覧化する，また，表形式で網羅性を確認するなどの利用方法が考えられる.

更に表形式の場合，基準の評価に関して各項目ごとに判断した根拠をマトリックス化して評価しやすいという特長をもつ．表 2 に上記評価を追記した例を示す．こうした表記の拡張がしやすいことも表形式の利点である.

表 2. セキュリティ対策立案の事例（表形式）

前提	ゴール	戦略	前提	サブゴール	戦略	サブゴール	証跡	評価値	リスク値＝脅威×脆弱性×資産の価値					その他の評価	
context	goal	strategy	context	goal	strategy	goal	evidence		脅威	脆弱性			資産の価値	コスト	効果
										機密性（C）	完全性（I）	可用性（A）			
□	□	▱	□	□	▱	□	○								
顧客によるセキュリティ対策決定	データの改ざんの対策が妥当である	データの改ざんの対策の選択に対する議論	リスク評価等の基準設定根拠	データの改ざんの対策評価基準が妥当	セキュリティ独自の評価基準も含める	リスク値をCIAごとに求める	リスク評価基準に対する顧客の承認		大:3 中:2 小:1	大:3 中:2 小:1	大:3 中:2 小:1	大:3 中:2 小:1	大:3 中:2 小:1		
						コスト・効果の一般的評価基準も使用する	その他の評価基準に対する顧客の承認							大:1 中:2 小:3	大:3 中:2 小:1
			個々の対策内容	データの改ざん対策に対する評価が妥当	リスク値とコスト、効果により個々の対策を評価する	デジタル署名は評価○である	評価○である根拠	144	2	3	2	2	1	2	3
						強力な認証は評価◎である	評価◎である根拠	216	2	3	2	2	1	3	3
						耐タンパプロトコルは評価△である	評価△である根拠	32	2	2	2	2	1	1	2
						通信リンク保護は評価×である	評価×である根拠	16	2	1	2	2	1	2	1
			個々の対策に対する評価結果	データの改ざん対策の選択が妥当	実施する対策と残存リスクが妥当	選択された対策が妥当	実施対策の選択に対する顧客の承認								
						残存リスクが妥当	残存リスクに対する顧客の承認								

7　提案手法の評価

7.1　セキュリティ保証への評価

本稿でセキュリティ特性を考慮して，セキュリティ保証ケースに組み込んだ手順は以下の３つである．それぞれの効果は①リスク値を考慮できる保証ケースは，予防効果の高い対策を選択できるという効果をもつ．

②残存リスクを明確化できる保証ケースは，選択した対策でできることできないことを顧客と合意したうえで想定外の脅威が発生したときに，対策をうちやすくする効果をもつ．③頻繁な修正の必要性に対応できる保証ケースは，変更容易性が高いという点で効果がある．セキュリティ保証ケース作成時には証跡を残す手間がかかるが，変更時には証跡がある方が早く的確に修正ができる．変更作業が多いセキュリティ要件に関しては，変更容易性はより効果を発揮する。

ただし，上記はいずれも定性的な評価であり，今後は定量的な評価を実施していきたい．特に保証ケース適用の効果はシステム開発からサービス提供のライフサイクルにわたって利用することで効果を発揮するものであり，ライフサイクルにわたるセキュリティ保証ケースの作成手順と定量的な効果測定をどのように実施するのかは今後の研究課題としたい．

7.2　表形式への評価

表形式のセキュリティ対策立案の第１の利点は，図形式と等価性をもって記載することができるように工夫して提案していることである． これにより，図形式と表形式のスパイラルレビューが可能となり，より網羅性のある対策案の発出が可能となる．第２の利点は，同じ表形式で一覧化して，評価の過程を証跡として残せる点である．また，基準の評価に関して各項目ごとに判断した根拠を追記しやすい．通常のシステム開発では要件マトリックスを作成することが多いため，開発現場になじみやすい手法にできる効果がある．

8　今後の課題

本論文で示したセキュリティ保証ケースの課題として，以下が考えられる．

(1)ライフサイクルにわたる証跡の維持のために，頻繁な修正の必要性に対応できる「セキュリティ保証ケース」が必要になることを 4.2 項に述べたが，この特性は保証ケースの図の中に示される性質のものではない．ライフサイクルにわたって証跡が維持されたときに初めて効果がわかるものである．この効果に対する評価の方法は検討が必要である．

(2) 対策立案の３ステップをセキュリティ対策に限ってみる場合、「②対策に対する評価が妥当である．」と「③対策の選択が妥当である．」は分離して考えるより，一対で考える方が望ましいケースが多いかもしれない．セキュリティ対策立案のステップをどのように規定すべきかそれに基づいたセキュリティ保証ケースはどのように作成されるべきかについては検討が必要である．

(3)対策の立案に，セキュリティ保証ケースを利用する方法を示したが，リスク値とその他の評価にあげた判断基準の妥当性の検証が将来的に必要である．

(4)対策の選定は、脅威に対する対策の列挙→評価→実行対策選定、というステップを踏んでいるが，「選定に残らなかった」対策に対応するリスクが残存リスクである．残存リスクの選定作業を詳細化することが保証の具体的な意味合いになるため，重要である．また、定義された残存リスク以外のリスクが顕在化した場合の措置も処置を詳細化することが今後の課題として重要である．残存リスクを定義することと，それが顕在化した事象に対する対処手順を定義する必要がある．さらに，定義された残存リスク以外のリスクが顕在化した場合への対処も確化する必要がある．

(5)セキュリティ対策に対する評価に妥当性をもたせるためには，対策を実施・未実施だけでなく、どの程度まで実施するのか，つまり対策のＳＬＡを明確化し、顧客の承認を得ることが望ましい．

(6)CC を用いたセキュリティ要求分析については，ゴール指向やユースケースを用いた手法が提唱されており[26]，それらとの比較を通じて，セキュリティ保証ケースの拡張として，今後の検討が望まれる．

尚、今回の考察は予備的な段階にある．よりしっかりした評価は今後の課題である．

参考文献

[1] 木下佳樹，松野裕，高村博紀，武山誠，”対訳　ディペンダブル・セキュアコンピューティングの基本概念と用語”，独立行政法人　産業技術総合研究所　システム検証研究センター，2009

[2]ISO27001, Information Security Management System , 2005

[3]ISO/IEC12207, Software Life Cycle Processes,1997

[4] 独立行政法人　情報処理推進機構　ソストウェア・エンジニアリング・センター，”共通フレーム 2007”，オーム社，2007

[5] Steve Lipner,Michael Howard,”信頼できるコンピューティングのセキュリティ開発ライフサイクル ”,http://msdn.microsoft.com/ja-jp/library/ms995349.aspx，2005

[6]ISO/IEC15026-2-2011, Systems and Software engineering-Part2:Assurance case

[7]OMG,ARM,http://www.omg.org/spec/ARM/1.0/Beta1/

[8]OMG,SAEM,http://www.omg.org/spec/SAEM/1.0/Beta1/

[9] T P Kelly & J A McDermid, “Safety Case Construction and Reuse using Patterns”, in Proceedings of 16th International Conference on Computer Safety, Reliability and Security (SAFECOMP'97), Springer-Verlag, September 1997.
[10] Tim Kelly and Rob Weaver, “The Goal Structuring Notation – A Safety Argument Notation, ” Proceedings of the Dependable Systems and Networks 2004 Workshop on Assurance Cases, July 2004
[11]Stephen Edelston Toulmin, “The Uses of Argument,” Cambridge University Press,1958
[12]The Adelard Safety Case Development (ASCAD), Safety Case Structuring: Claims, Arguments and Evidence,http://www.adelard.com/services/SafetyCaseStructuring/index.html
[13] DEOS プロジェクト, http://www.crest-os.jst.go.jp
[14]松野裕，高井利憲，山本修一郎，D-Case 入門，～ディペンダビリティ・ケースを書いてみよう！～, ダイテックホールディング, 2012 ， ISBN 978-4-86293-079-8
[15]小林茂憲　山本修一郎,”保証ケースを用いたサービス提供判断方法の提案，” 電子情報通信学会，信学技報, vol. 111, no. 489, KBSE2011-70, pp. 7-12, 2012 年 3 月
[16] Rob Alexander, Richard Hawkins, Tim Kelly, “Security Assurance Cases: Motivation and the State of the Art, ”, High Integrity Systems Engineering Department of Computer Science University of York Deramore Lane York YO10 5GH, 2011
[17] Goodenough J, Lipson H, Weinstock C. “Arguing Security - Creating Security Assurance Cases,”2007. https://buildsecurityin.us-cert.gov/bsi/articles/knowledge/assurance/643-BSI.html
[18] Lipson H, Weinstock C. “Evidence of Assurance: Laying the Foundation for a Credible Security Case, “, 2008. https://buildsecurityin.us-cert.gov/bsi/articles/knowledge/assurance/973-BSI.html
[19] T. Scott Ankrum, Alfred H. Kromholz, ”Structured Assurance Cases: Three Common Standards, “Proceedings of the Ninth IEEE International Symposium on High-Assurance Systems Engineering (HASE’05), “ 2005
[20]Robin E Bloomfield, Sofia Guerra, Marcelo Masera, Anne Miller, O. Sami Saydjari, “Assurance case workshop 2005, “ 2005
[21]Robin Bloomfield, SOFIA GUERRA, Marcelo Masera, Ann Miller, CHARLES B.WEINSTOCK, “International Working Group on Assurance Cases (for Security),”IEEE SECURITY & PRIVACY ,2006
[22]Robin Bloomfield, Marcelo Masera, Ann Miller, O. Sami Saydjari, Charles B. Weinstock, “Assurance Cases for Security: The Metrics Challenge”, 37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN'07) , 2007
[23]Jose Luis Vivas, Isaac Agudo, Javier Lopez,”A Methodology for Security Assurance Driven Development,” Requirements Engineering Volume 16, Issue 1 , pp 55-73,2011
[23]金子朋子，山本修一郎，田中英彦,”アクタ関係表に基づくセキュリティ要求分析手法（SARM）を用いたスパイラルレビューの提案”,情報処理学会論文誌 52 巻 9 号
[24]Tomoko Kaneko, Shuichiro Yamamoto, Hidehiko Tanaka “A Spiral Review Method for Security Requirements based on 'Actor Relationship Matrix',”ProMAC2010, P1227-1238
[25] Tomoko Kaneko, Shuichiro Yamamoto, Hidehiko Tanaka,”Specification of Whole Steps for the Security Requirements Analysis Method (SARM)- From Requirement Analysis to Countermeasure Decision - ,”ProMAC2011, D04
[26] 吉岡信和，田口研治他，“コモンクライテリアのためのモデリング手法の提案，” 情報処理学会研究報告, 2009