より安全なシステム構築のために～CC-Case_i によるセキュリティ要件の見える化

株式会社 NTT データ　金子　朋子

1　はじめに

近年政府機関や企業へのサイバー攻撃や遠隔操作ウイルス事件など様々なセキュリティ事故が頻発し，メディアを騒がせている．また金銭搾取を目的としてフィッシング詐欺，スマートデバイスを狙った犯行の横行など，個人ユーザに対しても各種の脅威が取り巻いている．こうした脅威はシステム，ソフトウェアの脆弱性を突いて攻撃を仕掛けてくる．

より巧妙化する脅威に対して，より安全なシステム・ソフトウェアを開発するにはどうしたらよいだろうか？解決方法として，開発者に対する教育と訓練，経験の伝達，プロジェクト管理の徹底，運用管理の向上，セキュリティ方針の厳密化などとともに，開発方法論からの対応が必要である（図 1）．システム・ソフトウェアの作りの仕組みの中に脅威への対抗手段を含めることがより根本的な対策になりうるからである．

システム開発の観点からの取り組みには要求，設計，実装，テスト，保守の各段階からの対応があり，全開発工程に対して安全性を考慮した方法論が望まれる．設計段階ではセキュリティプロトコルの検証，実装段階ではセキュリティメカニズム，セキュリティを意識したコーディング規約，テスト段階では侵入テスト，脆弱性テスト，運用段階ではセキュリティアップデートによる取り組みが可能である．しかし要求段階においては「2.1 セキュリティ要求分析手法」に後述するように，セキュリティ要求に関して様々な研究がなされているが，セキュリティ要求を抽出・分析・仕様化，妥当性確認，要求管理する全段階をサポートしている要求分析手法もセキュリティ要求分析の標準的な手法もまだできていない．また運用時のインシデント後のシステム改修等本格対応する際にはセキュリティ要求が必要となるが、これらをトータルに考慮した手法もまだできていない．つまり現在のシステム開発方法論は，要求分析，要件定義プロセスにおいてセキュリティの獲得，分析，定義を行っていないなどセキュリティ要求の取り扱いが不十分な状況にある．

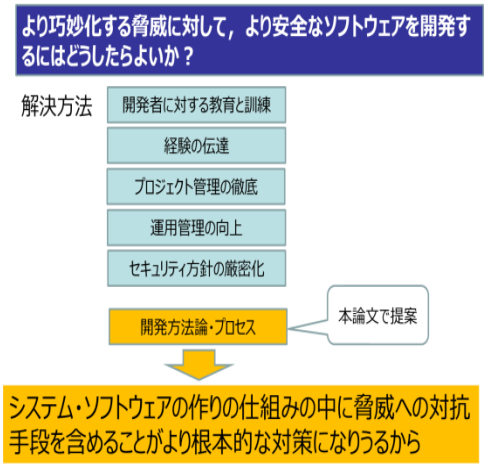


図 1　開発方法論・プロセスからの対応

この現状の課題を解決するために，筆者らは，コモンクライテリア（CC：Common Criteria. ISO/IEC15408 と同義）[1][2][3] とアシュアランスケース（ISO/IEC15026）[4]を用い，セキュリティ仕様を顧客と合意の上で決定する手法 CC-Case[5] [6]を提案している．しかしながら、従来の CC-Case は CC 認証を伴うセキュリティ要件定義中心の対応で、CC 認証を伴わない開発・運用に対応していない．そこで CC 認証を伴わない開発・運用の中でも、現在の情報セキュリティ対策の主流であるインシデントとその後の開発に着目した．CC-Case を拡張し、運用時のインシデント対応やインシデント後のシステム改修等本格対処する際のセキュリティ要件仕様にも利用できるフレームワークを新たに提案する．

2　関連研究

2.1　セキュリティ要求分析手法

セキュリティ要求分析では，顧客は要求に基づく機能要件の分析に加えて攻撃者の存在を考慮した非機能

要件の分析を必要とする．そこでセキュリティ要求はアセットに対する脅威とその対策の記述が必須となる．セキュリティ要求分析の手法にミスユースケース[7], Secure Tropos[8]，i*-Liu 法[9][10]，Abuse Frames[11]やアクタ関係表に基づくセキュリティ要求分析手法（SARM）[12] [13]などがある．いずれの手法もセキュリティを考慮した脅威分析やそれに対する対策立案の手法だが，明示されない非機能要求に関してあらゆる要件をつくすことは難しいのが実情である．

また SQUARE[14] [15]はセキュリティのシステム品質を高めるために定められた特定の手法によらないプロセスモデルである．SQUARE は生産物の定義に基づいてリスク分析し，セキュリティ要求を抽出・優先順位付け・レビューする手順である．

マイクロソフトのセキュリティ開発ライフサイクル[16] はデータフロー図を詳細化し脅威の観点 STRIDE で脅威分析を実施する．設計による安全性確保を重視し設計段階でセキュリティ要求を抽出している．しかしながら，セキュリティ要求を抽出・分析・仕様化，妥当性確認，要求管理する要求の全段階をサポートしているセキュリティ要求分析の標準的な手法や**運用時のインシデント後のシステム改修等本格対処する際のセキュリティ要件仕様までトータルに考慮した手法は**まだできていないのが現状である．

2.2 コモンクライテリアについて

IT セキュリティ評価の国際標準である CC[2]は,開発者が主張するセキュリティ保証の信頼性に関する評価の枠組みを規定したものである[4]．CC のパート 1 には評価対象のセキュリティ目標（ST: Security Target）やプロテクションプロファイル (PP : Protection Profile) に記載すべき内容が規定されている(図 2)．CC のパート 2 に TOE のセキュリティ機能要件（SFR : Security Functional Requirement）が規定されている．準形式化するために, CC パート 2 には機能要件がカタログ的に列挙されており，選択等の操作にパラメタやリストを特定することにより，準形式的な記載ができる．図 3 で説明すると, 機能要件 FIA_AFL1.1 で TSF は、[割付：認証事象のリスト]となっているので, 図 4 の事例のように「最後に成功した認証以降の各クライアント操作員の認証」，「最後に成功した認証以降の各サーバ管理者の認証」のパタメータの割り付けする． CC のパート 3 にはセキュリティ保証要件（SAR : Security Assurance Requirement）が規定されている． CC はセキュリティ機能自体の形式化を図ることにより、IT セキュリティを評価する基準であり、特にパート 1 に規定されたセキュリティ目標を作成するプロセスは、CC 認証を伴わないセキュリティ要求仕様においても汎用的に利用可能である．

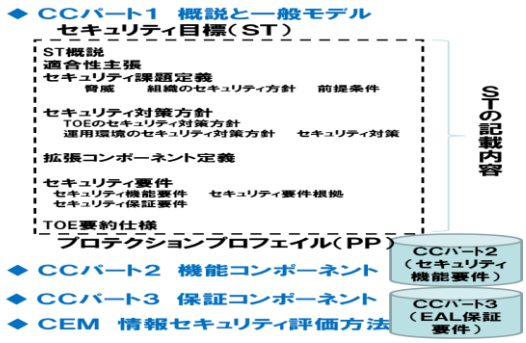


図 2　CC 構成と ST の記載内容

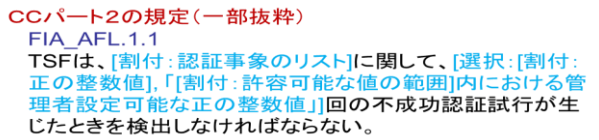


図 3　CC パート 2 の規定

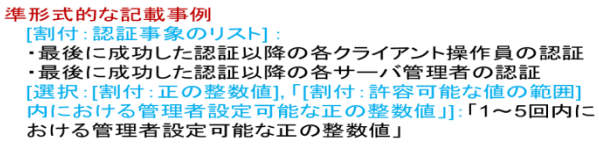


図 4　準形式的な記載事例

2.3 アシュアランスケースについて

アシュアランスケース（assurance case）とは，テスト結果や検証結果をエビデンスとしてそれらを根拠にシステムの安全性，信頼性を議論し，システム認証者や利用者などに保証する，あるいは確信させるためのドキュメントである[17]．アシュアランスケースは欧米で普及しているセーフティケース[18]から始まっており，近年，安全性だけでなく，ディペンダビリティ

やセキュリティにも使われ始めている．アシュアランスケースはISO/IEC15026やOMGのARM [19]とSAEM [20]などで標準化がすすめられている．

アシュアランス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．代表的な表記方法は，欧州で約 10 年前から使用されているGSN [21]であり，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ことができる．他に法律分野でアシュアランスケースの理論的背景となる Toulmin Structures[22]や要求，議論，証跡のみのシンプルなアシュアランスケースである ASCAD[23]もある．日本国内では GSN を拡張した D-CASE [24] [25]が JST CREST DEOS プロジェクトで開発されている．

2.4 セキュリティケースについて

GSN を提唱した Kelly ら[26]が Security Assurance Cases の作成に関する既存の手法とガイダンス，セーフティケースとセキュリティケースの違いなどを述べているが，具体的に作成したセキュリティケースの事例は示していない．Goodenough [27]らはセキュリティに対するアシュアランスケース作成の意味を説明している．Lipson H[28]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．Ankrum[29]らは CC，や ISO154971，RTCA/DO-178B という 3 つの製品を保証するための規格を ASCAD でマップ化し，ASCE などのアシュアランスケースツールが有効であり，保証規格を含むアシュアランスケースは似た構造をもつことを検証している．セキュリティケースはセキュリティ設計品質の見える化やセキュリティ要件の妥当性確認の容易化につながる手法であり，CC-Case の重要な技術要素である．

2.5 CC の動向

政府における IT 製品・システムの調達に関して、ISO/IEC 15408(CC) に基づく評価・認証がされている製品の利用が推進されており，注目すべき最新の CC の動向として，情報セキュリティ政策会議で決定された「政府機関の情報セキュリティ対策のための統一基準（平成 26 年度版）」[30]が挙げられる．

本統一基準の「5.2.1 情報システムの企画・要件 定義」において、機器調達時には「IT 製品の調達におけるセキュリティ要件リスト」を参照し、適切なセキュリティ要件を策定することが求められている ．経済産業省より公開されている「IT 製品の調達におけるセキュリティ要件リスト」[31]では、指定したセキュリティ要件が満たされていることの確認手段として、CC 認証のような国際基準に基づく第三者認証を活用することを推奨している．

CC における認証制度や cPP 活用で想定される今後の動向については,筆者らの論文[32]を参考にしてほしい. CC は認証制度のコスト負担の問題などで利用しづらい基準とみなされることもあるが，国内外の CC 活用動向を元に考えると，大変重要な基準である．

3 CC-Case の CC 認証を伴わない幅広いセキュリティ要求分析への適用方法

3.1 セキュリティインシデントとそのプロセス

一般にセキュリティインシデントとは、事業運営に影響を与えたり、情報セキュリティを脅かしたりする事件や事故のことをいう[33] [34].

セキュリティインシデント対応には「1. 平時におけるインシデント対応の準備」として，インシデントに対応する際の目的と目標事項，通知体制の確立が必要である．これらはセキュリティポリシーに記載すべき事項である．次に「2. 情報セキュリティ侵害を検出」として，インシデントであることと，その重要性に対するインシデントの識別が必要になる．更に「3. 情報セキュリティインシデント対応」としては暫定的対応

と本格的対処を行う．このインシデントの本格的対処はシステムの改修や運用方法の変更を伴うことも多い．

3.2　CC-Case インシデント対応版提案の背景

CC はその複雑さからデジタル複合機などの特定のセキュリティ機能のハードウェア製品や政府調達対象案件には利用されているものの，それ以外のセキュリティ要求分析にはあまり利用されていないという課題を抱えている．それゆえ CC-Case 自体の用途も限られ，提案手法の利用はなされていないのが現状である．そこで，CC-Case は認証を取るための開発以外においても，一般のセキュリティ要求分析に利用できることを示したい．特にセキュリティインシデント後の本格対処において CC-Case を利用可能としたいと筆者は考えている．何故ならばセキュリティは非機能要件であり，当初のシステム設計時には機能要件として挙がらないが，その後のインシデント発生により，システム改修が必要となる事例が多いからである．

3.3　CC-Case_i の定義と目的

インシデント発生に伴い，一時対処が終了した後の本格対処時に利用できるように CC-Case 活用の幅を広げ，CC-Case インシデント対応版を CC-Case_i と命名し提案する．　CC-Case_i は CC 認証を伴わないセキュリティインシデントの本格対処に適した「セキュリティ要求分析と保証」をサポートするプロセスと記法の統合手法である．

CC-Case_i の目的は，より巧妙化する脅威に対して，より安全なシステム・ソフトウェアを開発するために，現在のインシデントの本格対応も含め，CC 認証を伴わない一般的な開発におけるセキュリティ上の課題を解決できるセキュアなシステム開発への対応を実施することである．

3.4　CC-Case_i の構造

CC-Case_i も CC-Case と同様に論理モデルと具体モデルの 2 層構造をもつ(図 5)．論理モデルはセキュリティインシデントを解決するプロセスを提示し，具体モデルは実際の事例を記述する．具体モデルとは，論理モデルの最下層ゴールの下に作成される実際のケースに応じたアシュアランスケースである．具体モデルは証跡を最下層に提示するまで適宜論理分解されて記述される．具体モデルは実際のケースにおける証跡と合意によるステークホルダの承認結果を証跡として残す．各種証跡は次々と貯まりその結果，論証に使えるものになる．要望は確定的ではなく，変化することがありうるが，変化に応じた証跡を残すことが必要である．そのため CC-Case_i では，全ての証跡を要求管理 DB に格納し，変更要求に随時応じられるようにする．具体モデルの各証跡は ST の認証のための記述事項以外の必要な項目として 3.5 項に示すプロセスを全て含むように作成され，保証のできる証跡を残していき，要求管理として実施される．

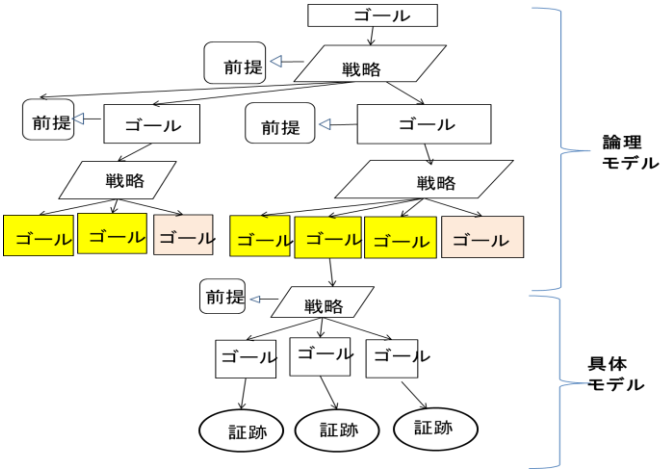


図 5　論理モデルと具体モデル

3.5　CC-Case_i のプロセス

CC-Case_i は普遍的に記載する以下の論理モデルをもつ(図 6)．「G_1　XX システムのセキュリティインシデント解決方法は妥当である」をトップゴールとし，「C_1 インシデントの発生」の前提条件，「S_1 インシデント対応が適切であることを論証する」戦略に則り，「G_2 インシデント認識は妥当である」，「G_3 現状調査と原因分析は妥当である」，「G_4 対策立案と選択は妥当である」,「G_5 対策実施は妥当である」，「G_6 結果の評価は妥当である」の 5 つの段階を規定している．これらのプロセスは一般的な問題解決手順に沿っており，主張と証拠を記述することで，ステー

クホルダ間の議論をしやすくすることを意図している．また要件定義段階の CC-Case にはない「G_5 対策実施は妥当である」，「G_6 結果の評価は妥当である」の段階を追加している．これによって，そのインシデント解決自体が的確に要求を満たせるように行われたのかを客観的に評価し，保証することを可能としている．つまり要求段階における期待としての保証ではなく，実際の結果を伴う保証が可能である．また理想的なインシデント解決は検討段階において，ステークホルダ間で議論し，対策実施の確認と評価の手段として証拠をもつべきであり CC-Case_i はそれを可能としている．

表 1 CC-Case_i のプロセス

段階	ゴール	目的	入力	手続き	出力	出力に対する確認方法
G_1	XXｼｽﾃﾑのセキュリティインシデント解決方法は妥当である	セキュリティインシデントの解決方法の妥当性を確認する	・インシデントの発生	G-2からG-6までのゴールがすべて満たされていることを確認する	・インシデント解決の評価	妥当性確認
G_2	インシデント認識は妥当である	インシデントを認識し，一時対処が妥当であることを確認する	・セキュリティ方針	基準に基づき，結果を評価する	・一時対処の実施結果	妥当性確認
G_3	現状調査と原因分析は妥当である	本格対処に必要な現状調査・分析を行う	・設計書 ・保護資産	・システム構成装置や機能等に分けて脅威分析する	・ｼｽﾃﾑとｼｽﾃﾑ間の脅威分析結果	妥当性確認
G_4	対策立案と選択は妥当である	最適な対策を選択する	・前提条件	・技術と運用の対策に分けて、洗い出した脅威に対策をたてる ・基準に基づき、対策を選択する ・残存リスクを影響分析する	・対策選択根拠 ・選択対策への承認結果 ・残存リスク	妥当性確認
G_5	対策実施は妥当である	対策を着実に実行する	・選択した対策	実施状況を管理し，対策を実施する	・実施結果	妥当性確認
G_6	結果の評価は妥当である	実施結果を評価し，次の改善につなげる	・実施結果	基準に基づき、結果を評価する	・実施状況の評価結果	妥当性確認

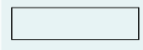
図 6 に CC-Case_i の論理モデルと具体モデルを図示する．G_1 から G_6 までのゴールは論理モデルとして固定であるが，それ以外は具体モデルである． G_1 から G_6 までのゴールは表 1 の CC-Case_i のプロセスに示すゴールごとの入力，手続き，出力を基本的に必要とする．その理由は 3.8 項に後述するように CC-Case_i は CC-Case 同様，CC 基準に則って作成するからである．

そこで図 6 に示した論理モデルの直下にある前提条件や戦略は具体モデルとして，そのセキュリティインシデントにあわせた具体的な内容を記述するが，表 1 の CC-Case_i のプロセスに示すゴールごとの入力，手続き，出力を具体的内容として記述することが求められる．そのため論理モデルの直下にある前提条件や戦略は図 6 の GSN の形式で記述することが基本になると筆者は考えている．ただし，必ずしも全ての項目を記述しなければならないわけでなく，実際のケースに応じて，表 1 の CC-Case_i のプロセスのテーラリングは可能である．例えば「システム改修を伴わない運用のみによる対策実施の場合は技術の対策は記述しない」などのテーラリングができる．また図 7 は「XX システムが標的型攻撃を受けた場合の対処」の CC-Case_i の事例である．

3.6 CC-Case_i とアシュアランスケースの役割

CC-Case_i も CC-Case 同様にアシュアランスケースの代表的な記法である GSN[21]を使用する．GSN の構成要素を表 2 に示す．

表 2 GSN の構成要素

名称	図式要素	説明
ゴール（主張）		システムが達成すべき性質を示す。下位の主張や説明に分かれる
戦略（説明）		主張の達成を導くために必要となる説明を示す。下位の主張や説明に分解される
コンテキスト（前提）		主張や説明が必要となる理由としての外部情報を示す
未定義要素		まだ具体化できていない主張や説明であることを示す
証跡		主張や説明が達成できることを示す証拠

3.7 CC-Case_i の対象範囲・適用対象

CC-Case_i の対象範囲はインシデント発生による本格対処時から解決までのライフサイクルである．

また CC-Case_i の適用対象はセキュリティインシデント後の本格対処時のシステムまたは製品である．CC-Case_i も顧客と開発者との合意を形成する手法として利用できるが，セキュリティインシデント対応で仕様を決める際に承認を取る特定の顧客がいない場合は，要件を決めるうえでの関係者と読み替える．

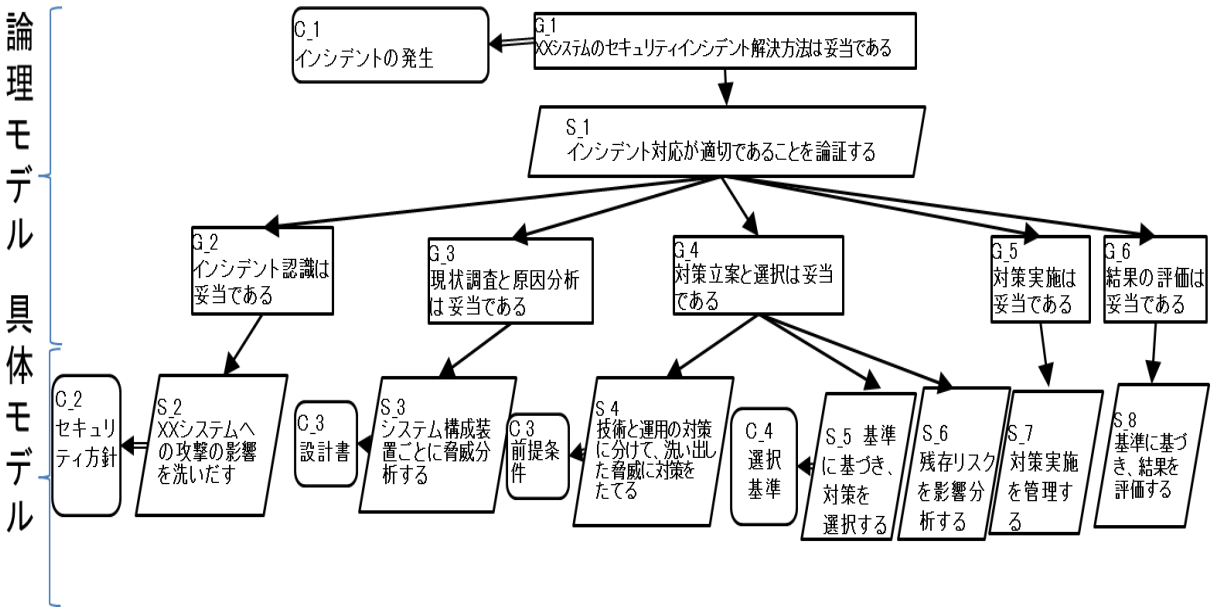


図 6.CC-Case_i のプロセス

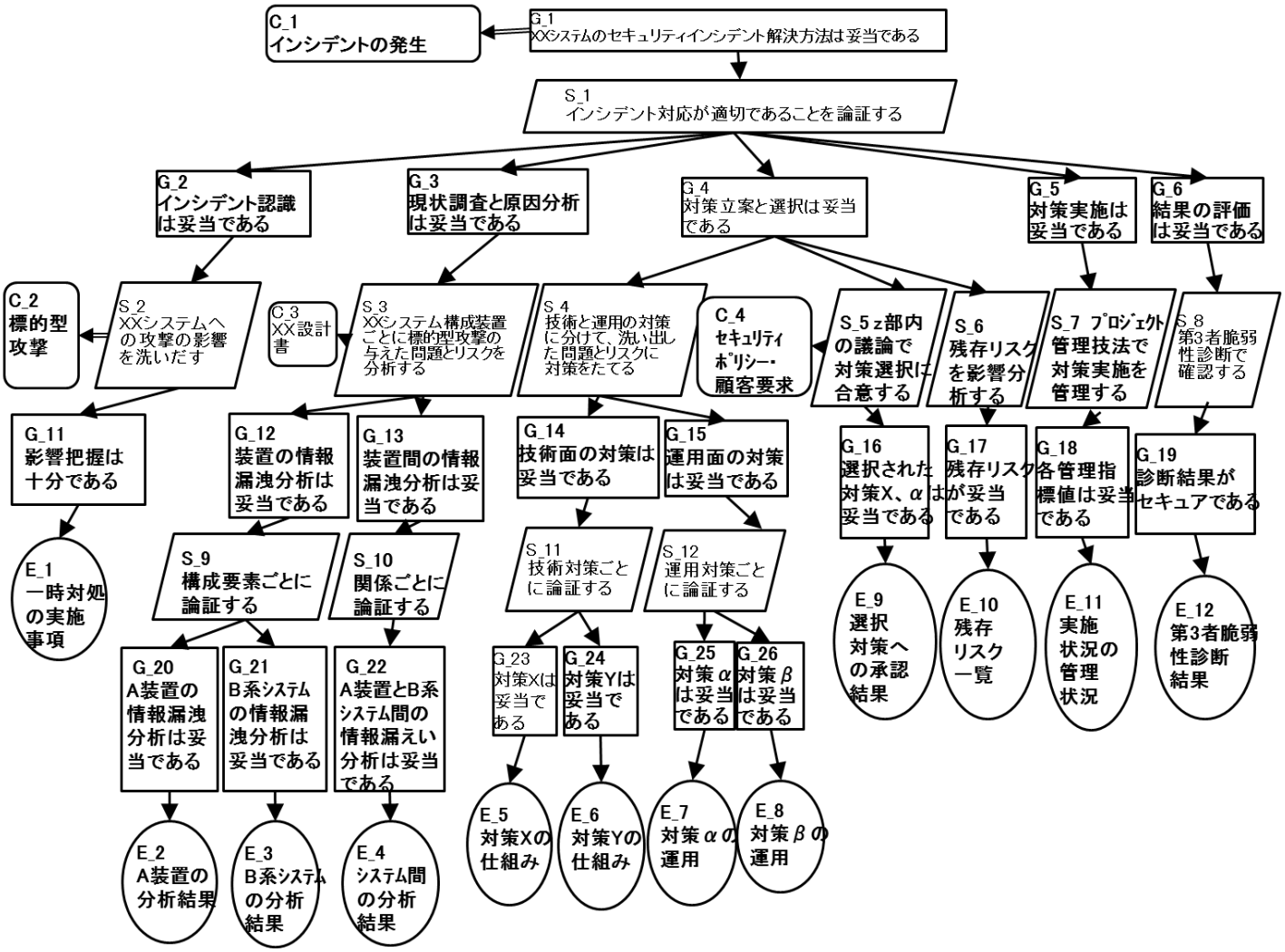


図 7.CC-Case_i の事例

3.8　従来の CC-Case との関係

従来の CC-Case が CC の ST とどのような関係をもち，その CC-Case と CC-Case_i がどのような関係になるのかを順に説明する．

(1)ST の構成とセキュリティ要求分析

CC-Case はセキュリティ要求分析として ST に必要な成果物を作成している．その理由は ST における作業プロセスとセキュリティ要件の解析方法は非常に類似しているからである．ST における作業プロセスは概ね以下の手順で実施される．資産ベースのセキュリティ要件の分析獲得の実施，攻撃者がいかに資産に対して脅威を与えるかについて脅威分析の実施，如何に資産を防御するかについてセキュリティ方針を規定，セキュリティ要件の獲得・分析し，セキュリティ機能として整理する．図 8 に示すように，セキュリティ要求分析として「2.適合性主張」と「6.2 セキュリティ保証要件」以外は従来の手法で作成可能である．従来の手法においても，攻撃タスクはミスユースケースに，システムのセキュリティゴールはセキュリティユースケースに，セキュリティ課題定義との関係とセキュリティ対策方針との関係はゴールモデルに対応しているからである．但し従来の手法は ST 全体に整合性を保ち網羅的に要求分析しながら，CC のセキュリティ基準に則った保証を可能とする手法ではない．

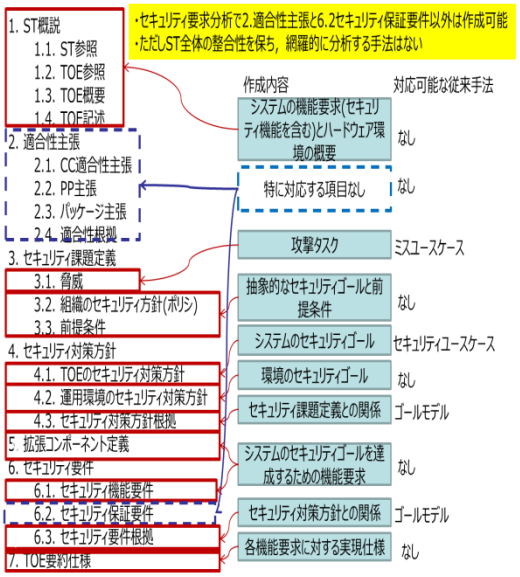


図 8　ST の構成と対応可能な従来手法

(2)ST の構成と CC-Case

図 9 に示すように要求段階の CC-Case のセキュリティ対策立案段階は，セキュリティ課題定義として，攻撃タスクと抽象的なセキュリティゴールと前提条件を洗い出す「3. セキュリティ課題定義」とこれをもとにシステムのセキュリティゴール，環境のセキュリティゴール，セキュリティ課題定義との関係を示す「4. セキュリティ対策方針」のプロセスを含んでいる．これらは CC 認証を伴わない一般的なセキュリティ要求分析の中でも重要な要素である．そこでセキュリティ対策立案段階で認証のための ST 記載事項を除いたプロセスを含み，セキュリティインシデント対処に適したプロセスに組み替えたものを CC-Case_i として定義する．CC-Case_i はステークホルダ間で妥当性確認をする際に用い，CC-Case のセキュリティ対策立案段階の最終ゴール「セキュリティ対策方針は妥当である」での妥当性確認に相当する(図 10).

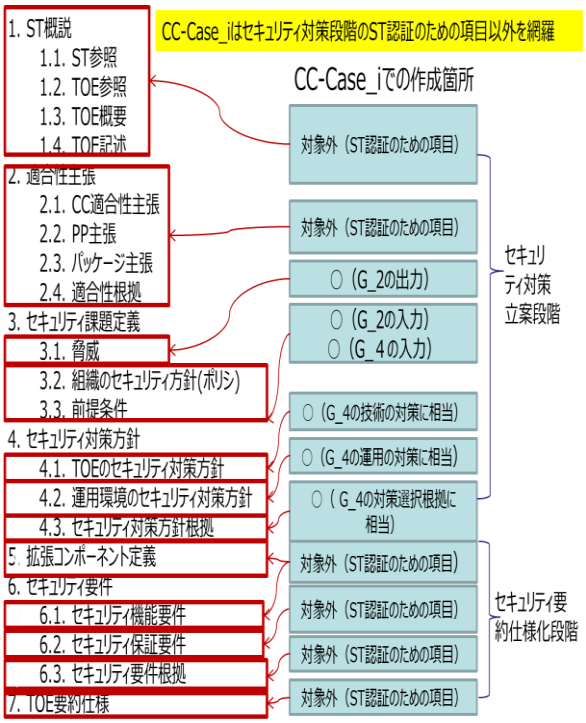
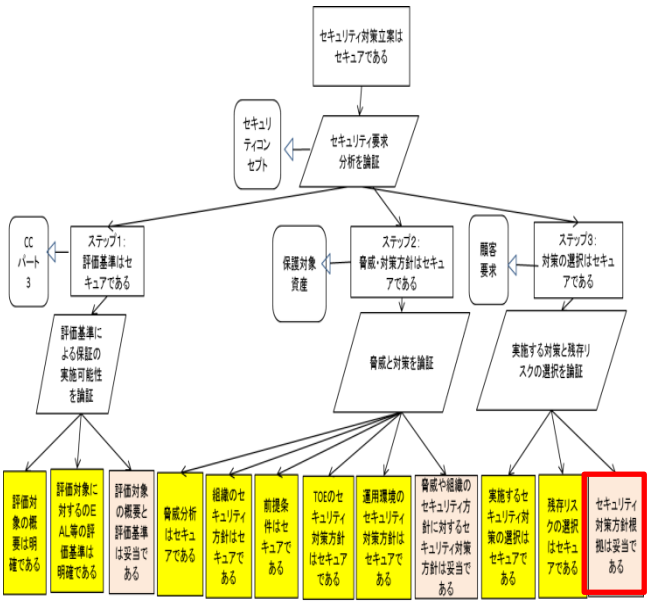


図 9　ST の構成と CC-Case_i



*黄色ゴールは検証, 赤色ゴールは妥当性確認を示す.

図 10　セキュリティ対策立案段階

4　CC-Case_i の特長

4.1　セキュリティインシデントの本質的原因

セキュリティインシデントには本格対処が必要な大きな事故もあれば，対外的には問題にならないトラブルもある．システム運用時には「アプリケーションバグや設計ミスでセキュリティ機能が動作しない．処理能力を超えた極限稼動でセキュリティ機能の動作不備が露呈する．本来見えないはずのデータにアクセス可能な方法が存在していた．明らかな使用ルール違反（内部犯罪など）だが痕跡の残らないシステム利用が行われた．」などのセキュリティ関連トラブルが日常的に発生する．

このようなセキュリティインシデントを起こす本質的な原因とは，脅威分析・システムリスク評価が不十分，各フェーズ間のセキュリティに関する分析の一貫性欠如，セキュリティ対策の検証方法のあいまいさ，設計・実装時のレビューが不十分でシステムバグ（ITまたは運用環境）を見つけ切れていないとことが考えられる．

解決方法にしても，運用でカバーする部分もあれば，同様なインシデントを防ぐ仕組みの確立やシステム自体の大規模な技術的改修も必要になることもある．インシデントが起きた装置・システムだけでなく他の装置への影響を考える必要性も生じる．単なる問題解決だけでなく今後のリスク対処も必要である．対処の確定には多様な関係者による検討が必要になる場合もある．またセキュリティの問題は，日々変化する脅威や技術を常に追いかける必要があるため，セキュリティ専門家の知見，ノウハウ，能力を活用することも有効である．

こうしたセキュリティインシデントの特性を考慮すると，インシデントから本格対処が必要な問題を抽出して，本質的な原因を分析し，対策をたて，実現していくプロセスを議論による「レビューの強化」を伴って実現することが必要になると考える．そのため筆者は CC-Case_i に見える化と使い方の観点で後述の長所をもたせた．

4.2　見える化の特長

CC-Case_i は３つの見える化の特長をもつ．「1.主張と証跡の見える化」，「2.論理の見える化」，「3.保証ストーリーの見える化」である．

(1)「1.主張と証跡の見える化」はゴールとしての主張とその主張の正しさを裏付ける証跡が存在することである．GSN はトップゴールの主張を満たすことを可視化できる手法だからである．

(2)「2.論理の見える化」は前提条件，戦略，ゴールの関係性の明示により，トップの主張から証跡までの論理が明確化されることである．GSN は図の最下層に主張が正しいことを示す証跡を記述するからである．多様な GSN の論理モデルが提供されており, 利用可能である[35].　更にインシデントの本格対応に適したモデルとして，筆者は本稿で CC-Case_i を提案している．

(3)「3.保証ストーリーの見える化」はプロセスと実施事項の明確化によりインシデント全体の解決ストーリーの可視化である．

CC-Case_i は管理プロセスと各インシデントへの対処がつながる統合方法論である．プロセスアプローチに

よるインシデント抽出，分析，管理は定性的にも定量的にも適用可能であり，インシデント解決の適切性を保証できる．

4.3　使い方の特長

使い方の観点で CC-Case_i は「議論のツール」，「セキュリティ保証のツール」，「脅威と対策の資産化ツール」としての長所をもつ．

(1)CC-Case_i は論理的根拠を明示することにより，「議論のツール」として利用できる．通常，適切な対策を選択していることは確認するのは難しい．CC-Case_i は，証跡ベースで事象の論理関係を明確化するため，この種の確認に適している．CC-Case_i を用いることによりステークホルダ間の認識の食い違いを防ぐ．評価基準を示し，証跡に対する適切な妥当性確認を実施できる．

セキュリティ対策の場合，セキュリティの専門家とされる人たちと一般のシステム開発者に理解の壁が生じることがある．また，インシデント解決には会社の経営層などの意志確認が不可欠である．それらの異なるバックグラウンドをもつステークホルダ間で理解の壁をなくし，互いのもつ見識を活かしたインシデント解決を図るために役立ててほしいのがこの CC-Case_i である．

このため，CC-Case_i は実用性にこだわっており，以下の利用方法を推奨したい．

まず，できる限り 1 枚の図で論理の全体像を表記し，インシデント解決ストーリーをステークホルダで共通認識ができるようにする．また証跡や前提条件など各項目の詳細内容にはリンクを張って参照できるようにする．さらに進捗段階に応じて，妥当性確認を完了した決定事項と計画段階の未決定段階を区別し，内容を書き換えていく．図 7 の G_5 と G_6 の事例のように未決定段階のプロセスには網掛けをすることで決定事項と未決定段階を区別し，ステータス管理が可能である．

(2)CC-Case_i は「セキュリティ保証のツール」であり，インシデント解決の妥当性確認の一連のプロセスと結果が要件を満たすことを確認するツールである．また単に要件に対する検証を実施するだけでなく，ステークホルダ間の議論による妥当性確認が可能である．

(3)CC-Case_i は「脅威と対策の資産化ツール」である．CC-Case は一連のプロセスを形式化しているため，証跡単位で DB 化して脅威と対策のノウハウを資産化できる．利用者が自社等のシステムにおいて資産化を進めることにより，将来的に自社システムにおけるプロアクティブな対処につなげられる可能性がある．

5　まとめ

本稿では，として CC-Case_i を提案し，その目的，定義，プロセス，特長と事例等を示した． CC-Case_i は本稿で新たに提案したものであり，まだ利用実績はない．今後，多くの実績を積み重ね，実際の利用者の意見をいただき，より利便性の高いものに適宜改善していきたい．本研究が現在の開発のセキュリティ上の課題解決に役立つよう，世の中で広く利用されていくことを念願するものである．

謝辞

数々の有益なご指摘を賜った査読者の方々をはじめ，この研究をするにあたりサポートして頂いた日本ネットワークセキュリティ協会の皆様，情報セキュリティ大学院大学の先生方，㈱NTT データの皆様，励ましを頂いた恩師，友人，家族に謹んで感謝の意を表する．

参考文献

[1] Common Criteria for Information Technology Security Evaluation, http://www.commoncriteriaportal.org/cc/
[2]セキュリティ評価基準（CC/CEM) http://www.ipa.go.jp/security/jisec/cc/index.html
[3]田淵治樹：国際規格による情報セキュリティの保証手法,日科技連，2007 年 7 月
[4]ISO/IEC15026-2-2011,Systems and Software engineering-Part2:Assurance case
[5]金子朋子，山本修一郎，田中英彦： CC-Case～コモンクライテリア準拠のアシュアランスケースによるセキュリティ要求分析・保証の統合手法，情報処理学会論文誌 55 巻 9 号(2014)
[6] Kaneko,T.,Yamamoto, S. and Tanaka, H.: CC-Case as

an Integrated Method of Security Analysis and Assurance over Life-cycle Process, IJCSDF 3(1): 49-62 Society of Digital Information and Wireless Communications, 2014 (ISSN:2305-0012)
[7]Sindre, G. and Opdahl. L. A. : Eliciting security requirements with misuse cases, Requirements Engineering, Vol.10, No.1, pp. 34-44 (2005).
[8]Mouratidis, H. : Secure Tropos homepage, (online), available from <http://www.securetropos.org/>.
[9]Liu, L., Yu, E. and Mylopolos, J. : Security and Privacy Requirements Analysis within a Social Setting, *Proc. IEEE International Conference on Requirements Engineering* (*RE 2003*), pp.151-161(2003).
[10]Li, T. Liu, L. Elahi, G. et al. : Service Security Analysis Based on i*: An Approach from the Attacker Viewpoint, *Proc. 34th Annual IEEE Computer Software and Applications Conference Workshops* , pp. 127-133 (2010).
[11]Lin, L. Nuseibeh, B. Ince, D. et al. : Introducing Abuse Frames for Analysing Security Requirements, *Proc. IEEE International Conference on Requirements Engineering* (*RE 2003*), pp.371-372 (2003).
[12]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(2011)
[13]Kaneko,T.,Yamamoto, S. and Tanaka, H.: Specification of Whole Steps for the Security Requirements Analysis Method (SARM)- From Requirement Analysis to Countermeasure Decision -,Promac2011
[14]Mead, N. R., Hough, E. and Stehney, T. :Sequrity Qualty Reqirements Engineering(SQUARE) Methodology(CMU/SEI-2005-TR-009), www.sei.cmu.edu/publications/documents/05.reports/05tr009.html
[15]Mead, N. R, 吉岡信和: SQUARE ではじめるセキュリティ要求工学,「情報処理」Vol.50 No.3（社団法人情報処理学会，2009 年 3 月発行）
[16]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
[17]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
[18]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.
[19]OMG, ARM, http://www.omg.org/spec/ARM/1.0/Beta1/
[20]J.R.Inge.The safty case,its development and use un the United Kingfom.In Proc.ISSC25,2007.OMG, SAEM, http://www.omg.org/spec/ SAEM/1.0/Beta1/
[21]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
[22]Stephen Edelston Toulmin, “The Uses of Argument,” Cambridge University Press,1958
[23]The Adelard Safety Case Development (ASCAD), Safety Case Structuring: Claims, Arguments and Evdence,http://www.adelard.com/services/SafetyCaseStructuring/index.html
[24]DEOS プロジェクト, http://www.crest-os.jst.go.jp
[25]松野　裕　山本修一郎: 実践　D-Case～ディペンダビリティケースを活用しよう！～,株式会社アセットマネジメント，2014 年 3 月
[26]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
[27]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
[28]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
[29]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
[30] 政府機関の情報セキュリティ対策のための統一基準（平成 26 年度版），http://www.nisc.go.jp/active/general/kijun26.html
[31]IT 製品の調達におけるセキュリティ要件リスト,http://www.meti.go.jp/press/2014/05/20140519003/20140519003.html [32] 金子朋子，村田松寿：セキュリティ基準コモンクライテリアが変わる-ユーザもベンダも乗り遅れるな！，情報処理学会デジタルプラクティス. Vol6　No.1(Jan.2015)
[33]情報処理推進機構 セキュリティセンタ,「インシデントマネジメント V1.0」 http://www.ipa.go.jp/security/awareness/administrator/incident.pdf
[34]コンピュータセキュリティインシデント対応ガイド, NIST Special Publication 800-61Revision 1, （2008 年 3 月）
[35] Robin Bloomfield & Peter Bishop: “Safety and Assurance Cases: Past, Present and Possible Future – an Adelard Perspective”,2010 scsc.org.uk/pubs/2010%20Bloomfield.pdf