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

金子 朋子† 山本 修一郎†† 田中 英彦†††

†, †††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
iisec@iwasaki.ac.jp

‡名古屋大学
464-8601 愛知県名古屋市千種区不老町
yamamotosui@icts.nagoya-u.ac.jp

あらまし ソフトウェアの開発において，顧客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．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保証を顧客から望まれている．そこで CC-Case と名付けたアシュアランスケース（ISO/IEC15026）とコモンクライテリア(CC)によるセキュリティ要求分析・保証の統合手法を提案する．本手法は脅威に対して保証できる範囲を明確にし，CC に基づくセキュリティ仕様を顧客と合意の上で決定できる．更に CC-Case の保証の意義と利点の活用を考察する．

CC-Case As a Integrated Method of Security Analysis and Assurance using Common Criteria-based Assurance Case

Kaneko Tomoko† Yamamoto Shuichiro†† Tanaka Hidehiko†††

†, ††† Institute of Information Security
2-14-1 Tsuruya-cho, Kanagawa-ku, Yokohama, Kanagawa 221-0835, JAPAN
iisec@iwasaki.ac.jp

‡Nagoya University
464-8601Furo-cho,chikusa-ku,Nagoya,Aichi,JAPAN
yamamotosui@icts.nagoya-u.ac.jp

Abstract It is important to grasp and realize needs of customers in the system development. However, lack of requirements analysis in upper process often gives a crucial influence to the system development. Customers expect that systems and products satisfy the necessary conditions and guarantees not to fall into any dangerous situations. We show the description of countermeasures and procedures which clarify scope of assurance for the menace, and which obtain an agreement on the assurance level with the customer using Assurance Case and Common Criteria though CC-Case. We consider significance of assurance and show how to use its merits.

1　はじめに

ソフトウェアのシステム開発において，顧客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．ところが，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．要求分析がうまくいかない理由は，顧客の要望を開発者が仕様化する際にギャップが生じるからである．すなわち，顧客（利用者）の早く，安く，良いものを使いやすくといった要望に対して，開発者は利害関係者の合意を図り，IT 技術・方式を決め，要員のスキルやソフトウェアの再利用方法などを定め，要求仕様を作成しなければならない．この顧客要望の要求仕様への変換時にギャップが生じる．

セキュリティ要求分析は，ソフトウェアの一般的機能の要求分析に比べて，顧客と開発者のギャップは更に大きくなる．セキュリティ要求分析は，分析すべき情報が多様であり，お互いが複雑に関連していることやシステムを取り巻く状況の変化が目まぐるしい中で，新たな攻撃に早く対処する必要があること，セキュリティの実現には，利便性などの他の特性と相反する要求が生じ，バランスを取る必要があるなどの難しい課題を抱えているからである．例えば，顧客はセキュリティ機能自体に興味がないことが多く，問題が起きないこと，費用がかからないことを漠然と求める．これに対して，開発者は脅威・リスクの洗い出しに漏れはないかが不明確，各工程で何をどこまでやればいいのかも不明確，新たな脅威への対処は一般にはわからないので困難といった課題を抱えながら，顧客と何らかの合意をとってセキュリティ仕様を定めていかなければならない．

またセキュリティ要求には，まず脅威の洗い出しが必要だが，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，顧客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対策を立案し，その対策を実施されることによる保証を顧客から望まれているのである．

この現状の課題を解決するために，本論文では，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 を提案する．2.1 項に後述するようにセキュリティ要求分析には様々な手法がある．しかし，あるシーンにおいての脅威分析やそれに対する対策立案の手法がほとんどである．本論文は多様な要求に対して網羅的な要求分析が可能であり，対策の保証も実施する手法を提案している．

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[5]，Secure Tropos[6]，i*-Liu 法[7][8]，Abuse Frames[9]やアクタ関係表に基づくセキュリティ要求分析手法（SARM）[10] [11]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[12] [13]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[14] 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1). 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 2 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3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.

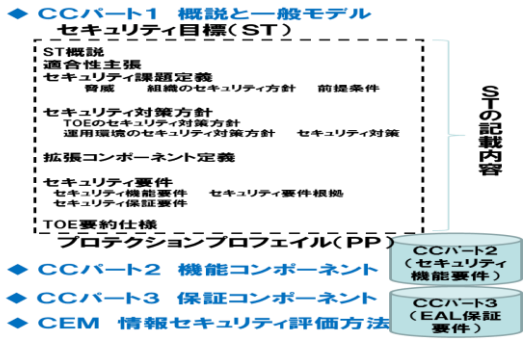

図 1　CC 構成と ST の記載内容

CCパート2の規定(一部抜粋)
FIA_AFL.1.1
TSFは、[割付:認証事象のリスト]に関して、[選択:[割付:正の整数値],「[割付:許容可能な値の範囲]内における管理者設定可能な正の整数値」]回の不成功認証試行が生じたときを検出しなければならない。

図 2　CC パート 2 の規定

準形式的な記載事例
[割付:認証事象のリスト]:
・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
[選択:[割付:正の整数値],「[割付:許容可能な値の範囲]内における管理者設定可能な正の整数値」]:「1～5回内における管理者設定可能な正の整数値」

図 3　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[15]. 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[16]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 [17]と SAEM [18]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 [19]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[20]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[21]もある. 日本国内では GSN を拡張した D-CASE [22] [23]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[24]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 [25]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[26]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[27]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. CC に対しては, PART3 セキュリティ保証要件についてのみの検討を行っている.

3 CC-Case の提案

3.1 CC-Case の目的

セキュリティ要求を獲得する際の技術的な難しさに対応することと同時に CC 準拠の保証をすることが CC-Case の目的である. セキュリティ要求を獲得する際の技術的な難しさには①扱う情報に対する複雑性, ②状況の変化, ③トレードオフの 3 つの観点があると言われている[28]. 現状のセキュリティ要求分析手法は, あるシーンにおいての脅威分析やそれに対する対策立案の手法がほとんどであり, 上記3つの観点に適切な対応が可能なセキュリティ要求分析手法はまだできていない.

CC-Case のセキュリティ要求分析はこれらの難しさに対応できることを目指す. ①扱う情報に対する複雑性に対しては, CC-Case はセキュリティ要求分析で扱う脅威, リスク, 対策, 資産等の複雑な情報を系統的に分析し, 検証する. ②状況の変化とは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であり, それに対して更なる対策を繰り返す必要が生じる. CC-Case は, アシュアランスケースに要求管理 DB を設定しており, 全ての証跡と論理的根拠を残している. これにより当初の想定とは全く違う要件でもどの機能にどのような影響があるのか, どのように変更すべきかの判断がしやすく, 繰り返される変更に対処しやすい. 次に③セキュリティ要求を考えるときに, 競合する要求との間にコストや機能の使いやすさ等, 他の要件とのトレードオフが生じる. CC-Case はセキュリティ対策を競合する要件を考慮し, 顧客と合意の上でどこまでの対策を実施するのかを選択するプロセスを含んでおり, 顧客との合意という根拠をもってトレードオフに対処する.

さらに, CC-Case は CC 準拠の保証も利用できることを目的にしている. セキュリティ保証を体系的に実施するためには, 評価の枠組みが必要である. これを規定している IT セキュリティ評価の代表的な国際標準は CC である. しかし CC は ST を作成するための元となる要求分析や脅威分析の手法を定めていない[29]. この具体的な手順を与えることにより CC-Case は ST を作成するための元となる要求分析や脅威分析を実施し, CC に基づく保証を可能とする.

3.2 CC-Case の定義

CC-Case は CC とアシュアランスケースの長所を統合したセキュリティ要求分析手法かつ保証手法である.
本手法ではセキュアな仕様を作成するために, セキュリティコンセプトの定義, 対策立案, 要約仕様の手順を定め ST に必要な成果物を作成する. この手順をアシュアランスケースとして定義し, 証跡を残す. こうして作成したセキュリティ仕様アシュアランスケースは, CC 準拠 と顧客と合意による保証の根拠となる.

図 4 に CC-Case のセキュリティ仕様作成の手順と用いる入力並びに生成される証跡の関係を示す. セキュリティ仕様のアシュアランスケースは, システム構築時の入力(前提), 手順, 証跡を含んだ文書である. すなわち, 作業は図の前提条件を入力とし, 手順に従って進められるが, それとともに生成される証跡によってアシュアランスケースが必要とする情報が出来上がっていく.

図 4 は CC-Case 要求分析の手順やライフサイクルでの位置づけ, 保証の意義を示した全体像である. 図 5 のセキュリティ仕様のアシュアランスケースは検証されるゴールと証跡を記載した CC-Case の文書である.

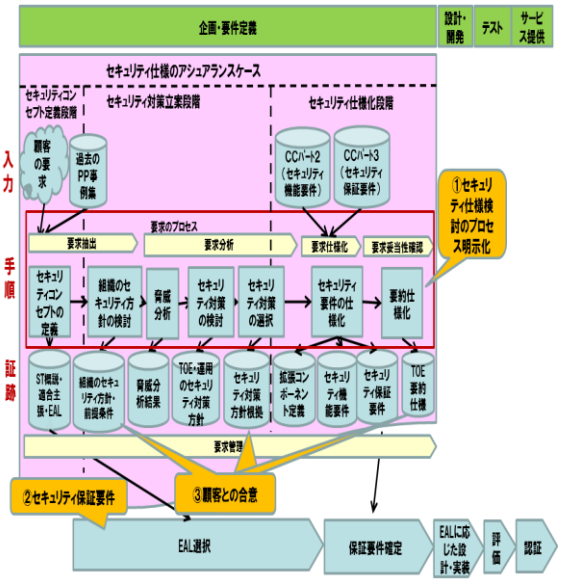

図 4　CC-Case の全体像

尚，本論文における CC-Case の対象範囲は要求段階の全てのプロセスを含むが，設計段階からサービス提供段階は含まない．また CC-Case の適用対象はシステムまたは製品である．CC-Case は顧客と開発者との合意を形成する手法であるが，製品開発など，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てほしい．

3.3　CC-Case におけるアシュアランスケースの役割

(1)CC-Case と GSN

CC-Case はアシュアランスケースの代表的な記法である GSN を使用する．GSN の構成要素を表 1 に示す．

表 1　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

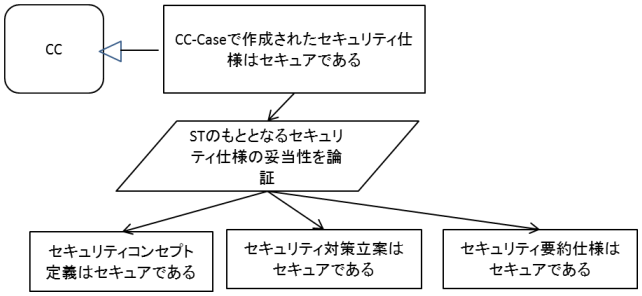

図 5　CC-Case のアシュアランスケース

GSN の構成要素がアシュアランスケースの中でどのように用いられているかを具体的に説明する．CC-Case の最上位のゴールは「CC-Case で作成されたセキュリティ仕様はセキュアである」である．これを最上位のゴールとするアシュアランスケースは「CC」を前提とし，「ST の元とのなるセキュリティ仕様の妥当性を論証」する戦略によって，「セキュリティコンセプト定義はセキュアである」と「セキュリティ対策立案はセキュアである」と「セキュリティ要約仕様はセキュアである」の 3 段階のゴールに分かれる．すなわち，これら 3 段階のゴールが満たされれば，「ST の元となるセキュリティ仕様の妥当性」が論証されることになる．「セキュリティコンセプト定義はセキュアである」のゴールをトップゴールとすればそれは図 6 に示すように細分化された命題を満たすことが求められる．また，図 6 の最下位に示された「セキュリティ要求抽出結果」等の証跡の 1 つ 1 つは上位ゴールが達成できることを示す証拠となる．

(2)セキュリティ仕様のアシュアランスケース

CC-Case ではセキュリティ仕様のアシュアランスケース(図 5)を作成する．図 4 中のアシュアランスケースに示すように，それは 3 段階に分かれる．すなわち，①セキュリティコンセプト定義段階(図 6)で要求抽出し，②セキュリティ対策立案段階(図 7)で要求分析，③セキュリティ要約仕様化段階(図 8)で仕様化，妥当性確認を行う．各段階の証跡は後の利用の為に，セキュアであること，すなわち技術的に安全性が保証されたことを検証するためのデータであって，データベース（要求管理 DB）内で管理される．

①セキュリティコンセプト定義段階

セキュリティコンセプト定義段階では，セキュ

リティ要求を抽出し，仕様の要件，コスト，顧客ニーズに応えるための仕様等を決める．セキュリティコンセプトは顧客と開発者で何度も繰り返し検討して決めていくものである．本段階では，利用者視点で製品に求められるセキュリティ要求を収集整理する．PP は公開されており，評価対象の種別に対して適用すべきセキュリティ仕様として適切な PP があれば，それを利用することができる．十分な要求を抽出した後，次にコスト等顧客の重要戦略を踏まえたセキュリティ要求検討を実施する．セキュリティコンセプトの顧客の承認結果を合意して証跡として残すことが重要である．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．

セキュリティコンセプト定義段階では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 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．

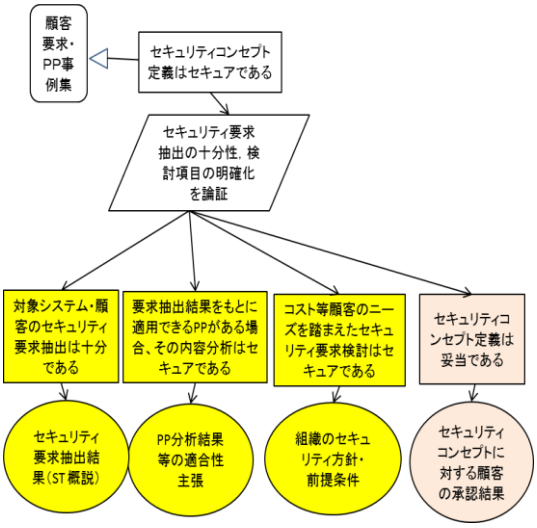

図 6　セキュリティコンセプトの定義段階

②セキュリティ対策立案段階

セキュリティ対策立案段階は，セキュリティコンセプトをもとに評価基準を定め，脅威分析を行い，並びに，対策の立案と評価，対策の選択と機能要件を定める．それぞれがセキュアであることを検証する．以上のような作業のステップごとにセキュリティ要求間の対応関係や論理関係の分析と根拠を顧客に提示し合意を得て決定していくがそれを整理して，以下の 3 ステップとした．

ステップ 1:最初に評価対象の範囲を定め，次にどこまでのレベルで保証するのかを EAL として定め，評価基準が妥当であるかを確認し，顧客の承認を得る．

ステップ 2:保護対象とする資産に関する脅威モデルを定義し，それに基づいて脅威を分析し，想定する特定の運用環境における対策を抽出する．脅威と対策の関係の評価が妥当であることを論証し，セキュリティ対策方針根拠に対する顧客の承認を得る．

ステップ 3:ステップ 2 で上がった対策案の中から実施する対策を選択し，対策を実施しないリスクは残存リスクとして管理していく．次にこれらの選択が妥当であることを論証し，セキュリティ対策の選択結果に対する顧客の承認を得る．

この対策立案の 3 ステップは「①評価基準が妥当である，②対策評価が妥当である．③対策の選択が妥当である．」のシステマテックな手順をきちんと踏んでセキュリティ対策を顧客と合意し，証跡を残すことを規定していることになる．

③セキュリティ要約仕様化段階

この段階（図 8）では，拡張コンポーネント定義，セキュリティ機能要件，セキュリティ保証要件，要約仕様がセキュアであることを検証し，顧客との合意を取る．まず，CC パート 2・3 だけでは機能要件や検証要件を明確にできない場合に，拡張コンポーネント定義をする．セキュリティ機能要件は，セキュリティ対策立案段階で選択した TOE のセキュリティ対策方針を，技術的な対策として実現するために，パート 2 からの機能要件の選択を行い，それにより作成される．セキュリティ保証要件は，CC パート 3 からの保証要件の参照等により，作成する．要約仕様はセキュリティ機能要件を実システム上で実装する方法を示す．このセキュリティ要約仕様に対して顧客の承認を得て妥当性確認をする．

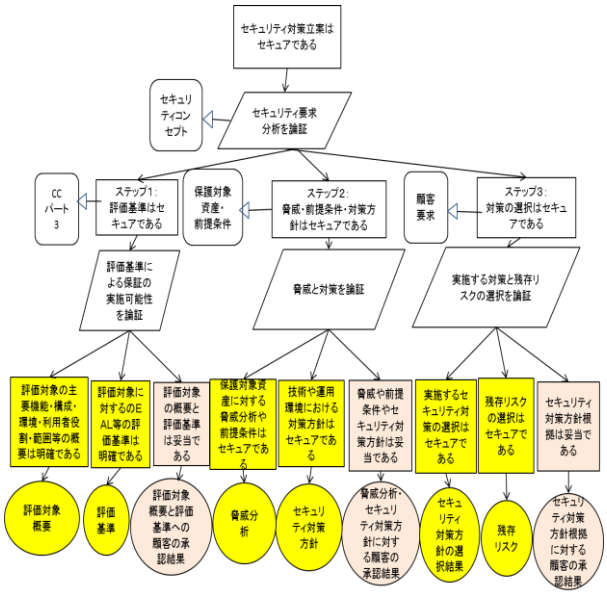

図 7　セキュリティ対策立案段階

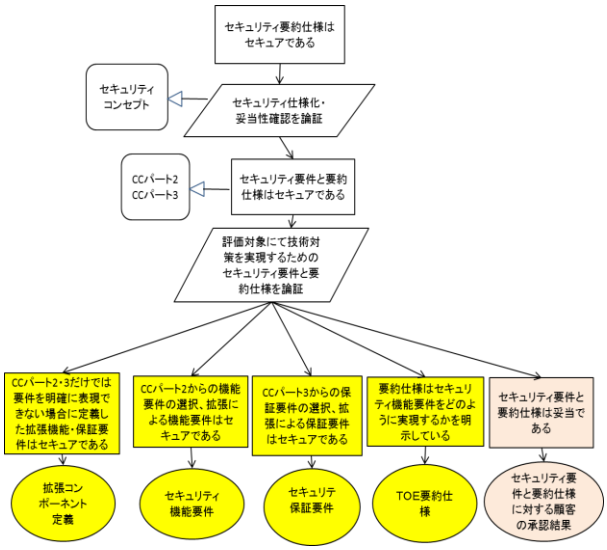

図 8　セキュリティ要約仕様化段階

3.4　CC-Case の利点

(1)要求分析と保証の手法

CC-Case は，CC に則り要求分析の段階で顧客と合意した範囲におけるセキュリティ保証要件を定め，保証をするために必要なセキュリティ機能要件を，網羅的に抽出・分析・妥当性検証・仕様化・管理を行う要求分析手法である．更に CC-Case は，①セキュリティ仕様検討プロセスの明示化，②セキュリティ保証要件，③顧客との合意のプロセスの明示化による保証手法である．

CC-Case のプロセスは，セキュリティ要求分析実施プロセスに検証（verification）と妥当性確認（Validation）のプロセスを含んでおり，成果物はアシュアランスケースの証跡に ST の成果物を必要十分に含んでいる．

CC-Case のセキュリティ要求分析実施プロセスは「セキュリティ仕様のアシュアランスケース」としてセキュリティ目標 ST を作成する際に必要なプロセスが明示化されている．そこで CC に準拠したシステム・製品の仕様要求，セキュリティ要求の対応関係や論理構造を漏れなく分析できる．また，セキュリティ要求分析実施プロセスは仕様が正しいことの検証を行う（図 6,7,8 の黄色のゴールに相当）．顧客との合意プロセスは顧客の要求に対して応えているという妥当性確認を行う（図 6,7,8 のオレンジ色のゴールに相当）．

また，成果物の利点として「セキュリティ仕様のアシュアランスケース」の各証跡は ST として必要な項目を全て含んでいる．セキュリティ要求分析実施プロセスにより，必要十分性の検証と妥当性確認した結果を逐次 DB 化し，保証のできる証跡を残していく．

(2)関係者の観点でみた利点

開発者・保守運用者にとっては，①ST を作成する際に必要なプロセスが明示化され，製品やシステムの ST が妥当であることを検証できる．②準形式的なセキュリティ機能要件を利用できるので齟齬が生じず，設計しやすい．③証跡を要求管理DBで管理するので，新たな脅威の発生などに伴う仕様変更の対応が楽にできる④CC パート 2 に規定されたセキュリティ機能要件は形式化・カタログ化されているので要件を再利用しやすい．

顧客（要件決定の関係者）にとっては①要件が明確化され，判断の根拠が与えられる．②コスト・難易度などセキュリティ以外の他のニーズでもどこまでの保証レベルとするかの主張ができる③EAL 保証要件を用いることで，実装責任が明確になるので，必要なセキュリティレベルに応じて必要な機能を具備し，運用や管理まで考慮した製品やシステムを，適正なコストで導

入しやすくなる.

4　今後の課題

4 章の評価・考察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．以下の点を今後の課題とする．

(1)アシュアランス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アシュアランスケースの作成手順と定量的な効果測定が必要である．

(2)具体的な例示に関しては，IPA の ST 事例[30]に対し，CC-Case をもとに記述した．その結果表記方法の工夫により，事例全体をアシュアランスケースで書けることを確認している．この詳細な中味は別途提示する予定である．

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]Sindre, G. and Opdahl. L. A. : Eliciting security requirements with misuse cases, Requirements Engineering, Vol.10, No.1, pp. 34-44 (2005).

[6]Mouratidis, H.：Secure Tropos homepage, (online), available from <http://www.securetropos.org/>.

[7]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).

[8]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).

[9]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).

[10]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

[11]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

[12]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

[13]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）

[14]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

[15]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

[16]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.

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

[18]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/

[19]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

[20]Stephen Edelston Toulmin, “The Uses of Argument,” Cambridge University Press,1958

[21]The Adelard Safety Case Development (ASCAD), Safety Case Structuring: Claims, Arguments and Evdence,http://www.adelard.com/services/SafetyCaseStructuring/index.html

[22]DEOS プロジェクト, http://www.crest-os.jst.go.jp

[23]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

[24]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

[25]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

[26]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

[27]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

[28]セキュリティ要求工学の概要と展望 吉岡信和 Bashar Nuseibeh 情報処理 Vol.50 No.3 Mar.2009

[29]金子浩之，コモンクライテリアにおけるセキュリティ要求の規定の現状と課題，「情報処理」Vol.50 No.3（社団法人情報処理学会，2009 年 3 月発行）

[30]A 社個人情報処理システムアプリケーションセキュリティターゲット，https://www.ipa.go.jp/security/jisec/index.html