# CC-Case のライフサイクルサポートと CC の動向に対する可能性

金子 朋子† 山本 修一郎†† 田中 英彦†††

† 株式会社 NTT データ
135-8671 東京都江東区豊洲 3-3-9
kanekotm@nttdata.co.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

†††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

**あらまし**ソフトウェアの開発において，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．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: ISO/IEC15408)によるセキュリティ要求分析・保証の統合手法はセキュリティ要求分析を実施するとともに CC 準拠の保証もでき，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手法である．本論文では CC-Case のライフサイクルサポートの概要と意義を考察する．更に製品分野ごとの PP 拡充の国際的動向と CC-Case の有効性について考察する．

The Concept of Life-Cycle Support of CC-Case and its Capability with the Trend of CC

Kaneko Tomoko† Yamamoto Shuichiro†† Tanaka Hidehiko†††
† NTTDATA
135-8671 3-3-9 Toyosu koutou-ku Tokyo-to
kanekotm@nttdata.co.jp

‡Nagoya University
464-8601Furo-cho,chikusa-ku,Nagoya,Aichi,JAPAN
yamamotosui@icts.nagoya-u.ac.jp
††† Institute of Information Security
2-14-1 Tsuruya-cho, Kanagawa-ku, Yokohama, Kanagawa 221-0835, JAPAN
iisec@iwasaki.ac.jp

**Abstract** Customers expect that systems and products satisfy the necessary conditions and guarantees not to fall into any dangerous situations in the system development. We show the description of countermeasures and procedures which clarify scope of assurance for the threat, and which obtain an agreement on the assurance level with the customer using Assurance Case and

Common Criteria though our original method named CC-Case. CC-Case can provide not only security requirement analysis method but also assurance according to the standard of Common Criteria. We show its concept of life-cycle support and consider the capability of CC-Case with the trend of CC.

# 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．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．

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 を提案している．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．

本論文では，要求定義段階のみの手法として提示していた CC-Case をライフサイクルサポートに拡張し，その概要と意義を考察する．更に製品分野ごとの PP 拡充の国際的動向と CC-Case の有効性について考察する．

# 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[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.

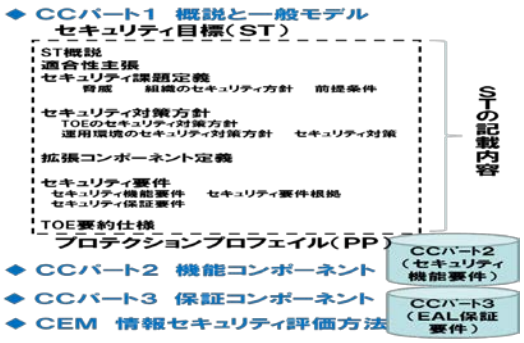


図 1 CC 構成と ST の記載内容

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.

### 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）」[28]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」[29]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．

製品分野ごとにセキュリティ要件は異なるためデジタル複合機（MFP），ファイアウォール
不正侵入検知/防止システム（IDS/IPS），
OS（サーバ OS に限る），データベース管理システム（DBMS），スマートカード（IC カード）の 6 つの分野から情報セキュリティリスト作成は開始されている． 直近の対象追加予定分野は USB メモリである．

# 3 CC-Case の提案

## 3.1 CC-Case の定義・目的

CC-Case を「セキュリティ要求分析と保証の開発方法論」と定義する．ここで「セキュリティ要求分析」には脅威への対抗手段を含め，統合開発方法論の「統合」はセキュリティ要求分析を実施するとともに CC 準拠の保証を実施することを意味している．一般にシステム開発手法とはシステムの作り方を指す，広義であいまいな概念であるに対し，システム開発方法論とは体系化されたシステムの作り方のことであり，何らかの原理・意図・観点に基づいて，各種の方法・手順・手段を統合した知的体系として定義される．

CC-Case 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．

尚，CC-Case はライフサイクルの全段階に対して安全性を考慮しているが，システム開発方法論は，セキュリティ要求の取り扱いが不十分であることが多いため，特に要求段階のプロセスに重点を当てている [30] ．

## 3.2 CC-Case の対象範囲・適用対象とアシュアランスケースの役割

CC-Case の対象範囲は要求，設計，実装，テスト，保守段階までのライフサイクルの全段階を含む．このライフサイクルの全段階のプロセス定義をライフサイクルプロセスとする．
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る．

CC-Case はアシュアランスケースの代表的な記法である GSN[19]を使用する．GSN の構成要素を表 3-2 に示す．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図 3-3-2 に具体的に説明する．

表 3-2 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 |

## 3.3 CC-Case のライフサイクルプロセス

より適切なセキュリティリスク対応のためにはラ

イフサイクルプロセスを規定した手法が望まれるため，CC-Case はライフサイクルプロセスを具備している．

### 3.3.1 ライフサイクルプロセスの構造

CC-Case は論理モデルと具体モデルの 2 層構造をもつ．図 3-3-1 に論理モデルと具体モデルの関係を示す．具体的な分け方として，論理モデルは図の上位層にあるライフサイクルプロセスと中位層にある各段階のプロセスをもつ．論理モデルはライフサイクルプロセスの最下位のゴールをトップゴールとして各段階のプロセスを提示する．また下位層は具体モデルである．具体モデルは各段階のプロセスの最下位のゴールをトップゴールとして実際の事例を記述する．

論理モデルは手順を定めたプロセスのアシュアランスケースである．具体モデル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成果物のアシュアランスケースである．論理モデルは検証の対象を具体モデルに明記できるレベルまで手順を定めている．論理モデルがそれ以上展開できない理由は，要求段階における ST の各項目のレベルにそろえた定義をしており，CC に則ったシステム・製品の対応ができるようにそろえているからである．

要求段階の場合，論理モデルはセキュリティ仕様検討のプロセス（ST に含むべき項目）の明示と顧客合意リスクに対処するための妥当性確認項目の明示とする．また具体モデルは対象となるシステム・製品の ST を満たすセキュリティ要求仕様と顧客との合意結果である．
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顧客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 では，全ての証跡を DB に格納し，変更要求に随時応じられるようにする．

論理モデルと具体モデルに分ける理由は，論理モデルは下位に続く具体モデルの検証を行う役割があることや以下のメリットを生むことである．

論理モデルでプロセスが規定され，具体モデルのみを更新すれば良いため，修正箇所の特定が早く，変更要求に伴う対応漏れを低減させることが期待できる．

CC-Case は要求管理 DB に CC 認証製品のアーキテクチャを具体モデルとしてモジュール化して管理することにより，部分再利用時のアーキテクチャ上の整合確保がしやすくなり，再利用を容易化でき，分析漏れによる脅威や脆弱性の低減が期待できる．

CC に基づいた手順は論理モデルとして共通化しており作成不要である．また収集すべき証跡も規定されているため，これらの規定のないアシュアランスケース構築に比べて，生産性向上が期待される．

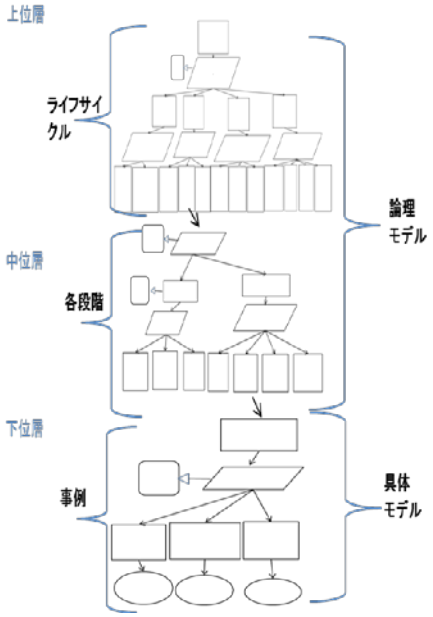


図 3-3-1 論理モデルと具体モデルの関係

### 3.3.2 CC-Case のライフサイクルプロセスの詳細

CC-Case の要求，設計，実装，テスト，保守段階までのライフサイクルの全段階を含んだライフサイクルプロセスを図 3-3-2 に示す

CC-Case の最上位のゴールは「CC-Case で作成されたシステム・製品はセキュアである」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」をコンテキスト（前提）とし，「ライフサイクルにわたる開発作業の妥当性を確認」する戦略（説明）によって「CC-Case による要件定義はセキュアである」と「CC-Case による設計はセキュアである」と「CC-Case による実装はセキュアである」と「CC-Case による総合テストと出荷はセキュアである」の 4 段階のサブゴールに分かれる.

前提とサブゴールに分かれる戦略の明示により論理関係を明確にしたうえで，各サブゴールが成り立つことで，最上位のゴールが成り立つことが保証される.

「CC-Case による要件定義はセキュアである」のという第 2 階層のゴールは「セキュリティ機能の開発に関わる要件の妥当性を確認」する戦略（説明）を介して「CC-Case で作成されたセキュリティ仕様はセキュアである」と「CC-Case での開発環境定義はセキュアである」の 2 つの第 3 階層のゴールに分かれる. このうち「CC-Case で作成されたセキュリティ仕様はセキュアである」が要求段階の CC-Case で示すセキュリティ仕様のアシュアランスケースのトップゴールに相当する. つまりこのセキュリティ仕様のアシュアランスケースのトップゴールのもとに論理モデルと具体モデルのアシュアランスケースが展開されるのである.

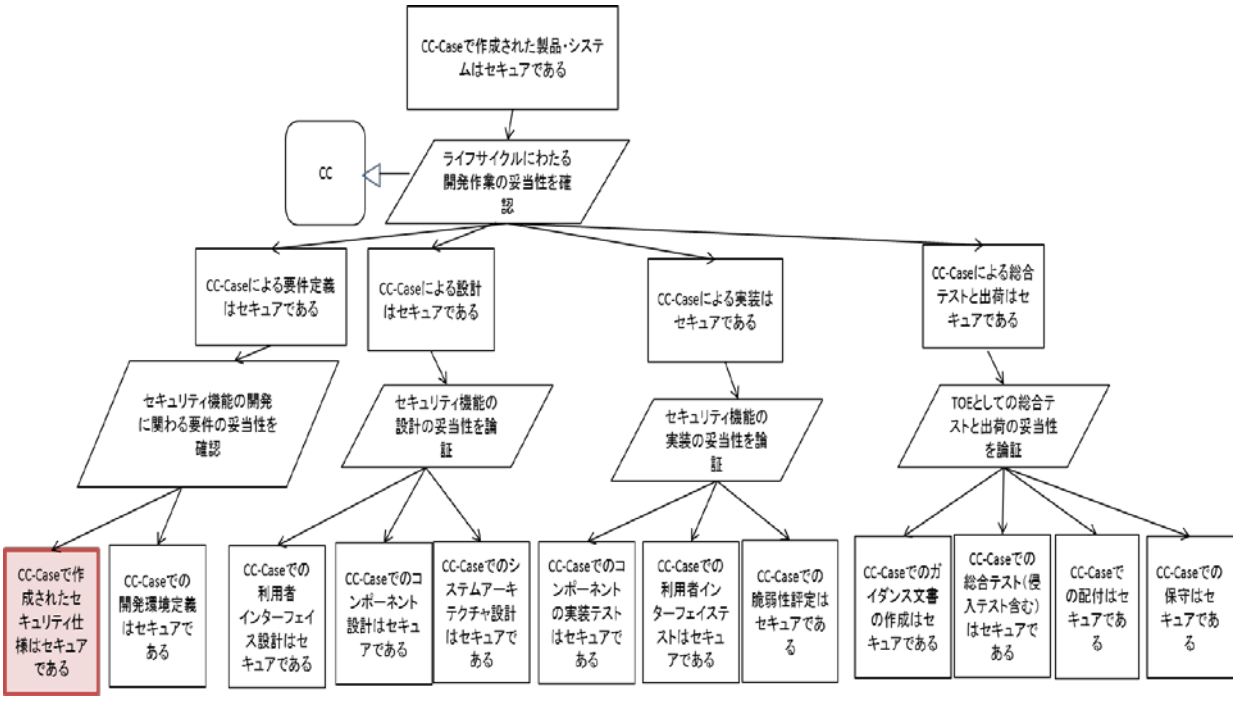


図 3-3-2　CC-Case のライフサイクルプロセス

## 4　考察

### 4.1　PP 利用における CC-Case の特長

CC-Case ではセキュリティ規格に適合した CC に基づく PP のセキュリティ要件を利用して対象とするシステムのセキュリティ保証を確保する. 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. 適切な PP が存在した場合はそのセキュリティ要件を利用する.

新しいシステムなどで適切な PP を特定することが難しい場合は, まずは類型化した PP を作成し, 同様の PP を知識資産化していくことが重要になる. その知識資産化にはプロセス定義を詳細化した上でのアシュアランスケースの利用が適している. 詳細なプロセス定義で同種のプロセスをカテゴリ化し, アシュアランスケースの証跡として残していくことで再利用がしやすいからである. CC-Case はこのプロセスの詳細化と具体モデルとしての証跡の残し方を明確に定義している.

日本では 2001 年より ISO/IEC 15408 に基づく「情報セキュリティ評価認証体制」[40]を運用しているが, PP の普及は不十分であった. しかし「政府機関の情報セキュリティ対策のための統一管理基準（平成 26 年度版）」において, 適切な情報セキュリティ対策の確保のため, 「機器等を調達する場合には, 「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, 利用環境における脅威を分析した上で, 当該機器等に存在する情報セキュリティ上の脅威に対抗するためのセキュリティ要件を策定すること」が求められている. また経済産業省による「IT 製品の調達におけるセキュリティ要件リスト」[29]を策定された. 本リスト CC に基づいたセキュリティ仕様を製品分野ごとに PP で定義されている. 「IT セキュリティ評価及び認証制度」を運営している独立行政法人情報処理推進機構（IPA）では, 今後製品分野ごとの PP を拡充していくことを目指している[31].今後は情報系システムの大規模な SI 現場において利用可能な PP も含め, PP の利用促進が活発化していくことが期待される. また世界では多くの製品・システムに PP が存在する[32]. また CC の業界での最近の動向では、これまで PP の開発は主としてセキュリティ製品の認証を望んでいる企業が行ってきたが, 現在, 企業が連携して共同 PP (cPP:Collaborative PP)を実現しようとしており[33], バンキングシステムの PP を共同開発事例などが報告されている[34]. このように最近の CC 状況を考慮すると, 今後本研究の有効性が高まると考える.

## 5　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より詳細な作成手順と定量的な効果測定が必要である.

(2) PP ごとにより詳細なセキュリティ機能と保証を規定し利用を推進しようとする最近の CC の動向を踏まえ, この PP の類型化への具体的な対処を検討する必要がある. また新しいシステムなどでは適切な PP を特定することが難しい場合や PP が存在しない場合の対処も今後の検討事項である.

## 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] 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
[29]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
[30] 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,
[31] IPA (独立行政法人情報処理推進機構):「IT セキュリティ評価及び認証制度に関する説明会」資料,http://www.ipa.go.jp/security/jisec/seminar/cc_semi_20140610.html
[32] Protection Profiles of Common Criteria, http://www.commoncriteriaportal.org/pps/
[33] The 2013 International Common Criteria Conference (ICCC) website, http://www.commoncriteriaportal.org/iccc/ICCC_arc/
[34] Jareno, A. D. et al.: Producing Protection Profile for Internet Banking Application, http://www.fbcinc.com/e/ICCC/presentations/T3_D2_3pm_Jarno_Collab_Efforts_in_Malaysia_to_Product_PP.pdf