Vol.2016-DPS-166 No.14
Vol.2016-CSEC-72 No.14
2016/3/3

CC-Case を用いた IoT セキュリティ認証方法の提案

金子朋子[†1]　髙橋雄志,[†2]　勅使河原可海,[†2]　田中英彦,[†1]

概要：モノのインターネットといわれる IoT システムは今後急激な普及・拡大が見込まれる．しかし，つながる世界は様々なリスクも抱えており，セキュリティ設計技術，認証技術，標準化はつながる世界では更に重要になる．筆者らは，IoT セキュリティ認証方法として，コモンクライテリア（CC）とアシュアランスケースを用いてセキュリティ要求分析と保証を実現する手法である CC-Case の利用を提案する．IT セキュリティ評価基準である CC による認証技術と品質説明力の強化を図れるアシュアランスケースの統合が，IoT の複雑なセキュリティ要件を可視化する認証技術となりうると考えるからである．

キーワード：IoT，認証技術，アシュアランスケース，セキュリティケース，コモンクライテリア，CC-Case

Proposal of an IoT Security Certification Method Using CC-Case

KANEKO　TOMOKO[†1]　TAKAYHASHI　YUJI[†2]
TESHIGAWARA YOSHIMI[†2]　TANAKA HIDEHIKO[†1]

Abstract: Abstract: IoT, Internet of Things, systems are expected to be in widespread use rapidly all over the world. However, the connected world using the Internet has various risks. The security design technology, the certification technology, and the standardization become more important in such the connected world. We propose an IoT certification method by applying the CC-Case which realizes security requirement analysis and assurance by using the Common Criteria (CC) and the assurance case. The CC is an IT security evaluation standard and the assurance case can strengthen quality description. Therefore, we are convinced that the integration of the CC and the assurance case can become an effective certification technology to describe precisely and complicated security requirements of IoT.

Keywords: IoT, authentication techniques, Assurance Case, Security Case, Common Criteria, CC-Case

1. はじめに

現代のシステムはネットワークを介して様々な機器やクラウドと連携しながら動作している．このように異なる分野の製品や産業機械などがつながって新しいサービスを想像するモノのインターネット（Internet of Things）は新産業革命とまで言われ，大きな期待を集めている．IoT は家電，自動車，各種インフラ業者など新規プレーヤーの登場を産み，その取り込みは加速化している．しかし．相互につながる際に最も懸念されるのは，IoT システムへのセキュリティ上の脅威である．IoT システムにおいても攻撃者はシステム，ソフトウェアの脆弱性を突いて攻撃を仕掛けてくる．

IoT システムへの脅威に対して，より安全な機器，システム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）．なかんずく製品・システムの中で動くソフトウェア自体の開発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と考える．

つながる世界である IoT にとって，現在最も求められているのはセキュリティ脅威に対して安全・安心を確保するための開発指針であり，開発技術である．そして開発指針と開発技術を伴うセキュリティ認証方法であると筆者らは考える．

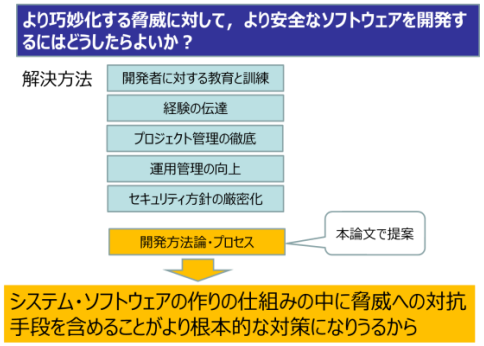


図 1　開発方法論・プロセスからの対応

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．これ

†1 情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY
†2 東京電機大学
TOKYO　DENKI　UNIVERSITY

Vol.2016-DPS-166 No.14
Vol.2016-CSEC-72 No.14
2016/3/3

までの CC-Case では，CC 認証を伴うセキュリティ要件定義中心に公開してきたが，本来要求，設計，実装，テスト，保守の各段階からの対応ができ，全開発工程に対して安全性を考慮した方法論である．またコモンクライテリア（CC）とアシュアランスケースを用いてセキュリティ要求分析と保証を実現する手法である．本論文では CC 認証制度が個々の製品のセキュリティ要求（ST）中心の評価から、プロテクションプロファイル（PP）のひな型を利用する効率的な評価へ移行される現状に応じて，CC-Case 自体を用いた認証方法も効率的化できることを述べる．さらに多様な機器の組合せによって生じる IoT の複雑性への対処の方向性についてもふれ，CC-Case が IoT の複雑なセキュリティ要件を可視化し，品質を保証する認証技術となりうることを示す．

2. 関連研究

2.1 IoT セキュリティの現状

IoT システムへの脅威事例[7][8][9]]は日増しに増加している．2004 年の HDD レコーダーの踏む台化は情報家電に対する初期の攻撃事例である．この事例では HDD レコーダーが外部サーバアクセス機能を有していたため踏み台として利用された．2013 年の心臓ペースメーカの不正操作は無線通信で遠隔から埋め込み型医療機器を不正に操作できる脅威を示したものである．また 2013 年には Jeep を車載のインフォメーションシステムを経由してインターネットから操作できる研究も発表され，自動車メーカーを驚かせた．2014 年にはスマホで ATM から現金を引き出すウイルスで 14 歳少年が ATM 管理モードに入り表示画面を書き換える事件も起きている．また世界中からハッカーの集まる Black Hat ではカテゴリの中に HW／組込み，IoT，スマートグリッド／インダストリといった IoT 関連テーマが登場し，注目されている．今後 IoT ハッキング技術を身につけ，実践をはじめるハッカーが増えることは想像にかたくない．

2.2 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[10]，Secure Tropos[11]，i*-Liu 法[12][13]，Abuse Frames[14]やアクタ関係表に基づくセキュリティ要求分析手法（SARM）[15] [16]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[17] [18]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[19]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 IoT セキュリティ要求に最適化した手法はまだ定められてはいない．

2.3 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．

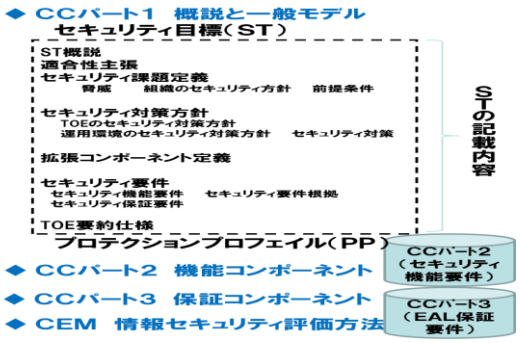


図 2 CC 構成と ST の記載内容

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 3 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 4 準形式的な記載事例

2.4 アシュアランスケース

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[20]．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[21]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 [22]と SAEM [23]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 [24]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[25]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[26]もある．日本国内では GSN を拡張した D-CASE [27] [28]が JST CREST DEOS プロジェクトで開発されている． また宇宙航空研究開発機構（JAXA）ではアシュアランスケースを用いた検証活動への効果的な活用がなされている[29].

2.5 セキュリティケース

GSN を提唱した Kelly ら[30]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 [31]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[32]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[33]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-Case[5] は IT セキュリティ評価基準(CC)に基づくセキュリティケースであり, セキュリティに関する事例として有用である[7]．CC の要求や保証・ライフサイクルをサポートしたセキュリティケースは CC-Case のみである．

2.6 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）」[34]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」[35]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[36]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，CC のもつセキュリティ基準としての汎用性，国内外の CC 活用動向を元に考えると，やはり CC は大変重要な基準である．

3. CC-Case の IoT セキュリティ認証への適用方法

3.1 IoT セキュリティの課題

1.1 節に述べたように IoT セキュリティリスクへの不安が高まっている．IoT システムには多様な業界の多様な製品，システムがつながってくる．これらは業界，製品・システムごと要件が異なるため，セキュリティの対応レベルが異なり，標準化の動向も異なっている．いわばセキュリティホールだらけの IoT である．しかも対象が情報だけでなく，実体を伴うモノになるため．与える被害も致命的であり，攻撃の被害は甚大にならざるを得ない．従って IoT のセキュリティを確保するのは大変に重大なことである．

しかしながら IoT のセキュリティを確保するための技術や手法，標準，基準はまだ確立されていない．このこと自体が IoT セキュリティにおける大きな課題である．

IoT セキュリティの対象となる機器やシステムに対する脅威には盗聴や不正アクセスによる情報漏えいプライバシー侵害、データやソフトウェア改善による誤動作や予期せぬ停止など，様々なものが想定される．これらの脅威により，事故の発生や顧客の信頼失墜，機器交換・システム改修コストなど多大な損害も懸念される．そのため確実なセキュリティ対応が求められる．セキュリティ対応のプロセスとしては，まず守るべき対象や目標を設定する．次にこれらに対する脅威を特定し，その発生しやすさと被害の深刻度からリスクを評価する．この結果得られたリスクの規模に応じてセキュリティ設計を進める．[7]

この脅威の特定からセキュリティ設計までのプロセスにおいて，多様な機器・システムが複雑に関連する IoT セキュリティに対する，脅威となる対象の洗い出しや目標を設定するセキュリティ要求分析手法，リスク評価の手法，

要件を可視化する技術はまだ特定されていない．これらは要求段階から洗い出し，セキュア設計へつなげ，セキュリティ機能のセキュリティを保証したうえで，製品化またはシステム化されることが求められる．さらに運用段階におけて，随時発生し続ける脅威に対し続けることが必要なのである．そのためには製品・システムを作る段階からセキュリティを考慮する手法や技術，さらに脅威にライフサイクルで対応し続ける仕組みと，それを定める基準または標準が必要とされる．

3.2 IoT の特長にあった可視化手法

2.2 節で述べたように各種セキュリティ要求分析手法は存在するが， IoT セキュリティ用の手法はまだ存在しない．多様な機器・システムがより複雑に関連するという IoT の特徴にあった技術，手法は何だろうか？

筆者らはアシュアランスケースであると考える．その理由の 1 つは欧州を中心に IoT の対象となる機器類の安全性規格やガイドラインで要求され，広く利用されているアシュアランスケースを利用する手法だからである．アシュアランスケースは航空，鉄道，軍事，自動車，医療機器の分野の複数の安全性規格やガイドラインで要求されている[28].

アシュアランスケースは対象となる機器やシステムについて，なぜその設計で目標が達成されるかを事実に基づき，論理的かつ第三者でも容易に理解できる表記で説明する手法である．可視化の手法でもあるため，近年設計の現場でも複雑な設計情報を共有する手段として活用され始めている．

IoT とは個々の製品がつながることであるため，製品自体のセキュリティ機能と製品やシステムをつなぐ間の関係性においても安全性を確保しなければならず，セキュリティ要件は複雑になる. その複雑化 I o T セキュリティ機能もやはり複雑化する．このように複雑なセキュリティ要件をもつことになる IoT にはアシュアランスケースが向いている．

3.3 IoT の特徴にあった基準

では多様な機器・システムがより複雑に関連するという IoT の特徴にあった基準，標準は何だろうか？ここではセキュリティ規格の比較の観点から IoT の特徴にあった基準を考えてみたい．

IoT は多様な機器・システムがつながるため，個別の機器，個別の業界の基準のみではサポートできない部分が発生する．そこでより汎用的で広く認知されたセキュリティ基準として国際規格である CC と ISMS[37]を比較してみる. CC は製品・システムセキュリティ機能のライフサイクルサポート規格だが、ISMS の確立及び実施については、それをどのように実現するかという方法ではなく、組織が何を行うべきかを主として記述している. 一方 ISMS（ISO/IEC 27001）は，マネジメント規格であり，IoT セキュリティ機能を評価する規格ではない．

IoT セキュリティ基準は相互につながる機器・システム上のセキュリティリスクに対して．個々のセキュリティ機能がどのように実現されたのかを示して，その安全性を示す必要がある．何故ならば相互に依存する機器・システムはその 1 つ 1 つが安全であり，相互依存関係においても安全でなければ，セキュリティ上の保証ができないからである．

そこで CC は製品・システムのセキュリティ機能の安全性を第 3 者に示し，保証することができる基準であり，より IoT の特徴にあった基準は CC であると筆者は考える．

3.4 IoT の特徴と CC-Case

IoT の特徴にあった要件の可視化手法はアシュアランスケースであり，IoT の特徴にあったセキュリティ基準をもつ方法論は CC であることを示した．筆者らが提案してきた CC-Case は，このアシュアランスケースを利用して CC に基づくセキュリティ要求分析と保証を行う手法である．それゆえ CC-Case は IoT の特徴にあった手法だということができる．具体的な IoT への利用方法は CC-Case の目的・定義等の概要と共に次節以降に説明する．

3.5 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[38]．現状のセキュリティ要求分析手法は，特定の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 つの観点に網羅的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確立されていない．

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．さらに，CC-Case はセキュリティ要求分析を実施するとともに CC 準拠の保証も利用できることを目的にしている．

3.6 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． 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 は論理モデルと具体モデルの 2 層構造をもつ．論理モデルは CC 基準に基づくプロセス定義のアシュアランスケースであり, 具体モデルは実際の事例を記述であり, 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．

なお，当初の CC-Case の対象範囲は要求段階の中心に説明していたが，本論文の CC-Case は設計段階からサービス

提供段階のライフサイクルを含む[6]．IoT セキュリティの場合も要件定義で論理的にセキュリティ仕様アシュアランスケースを作成するプロセスを提示する段階の論理モデルは変わらない．具体的な内容は個々の製品・システムの特徴を反映したものになる．セキュリティ仕様を作成する移行の設計段階における論理モデルは今後の課題であるが，3 章に後述するメリットをもつ設計，実装，テストになるであろう．図 5 に論理モデルと具体モデルを図示する．図 6 にライフサイクルにおける CC-Case 論理モデルを示す．

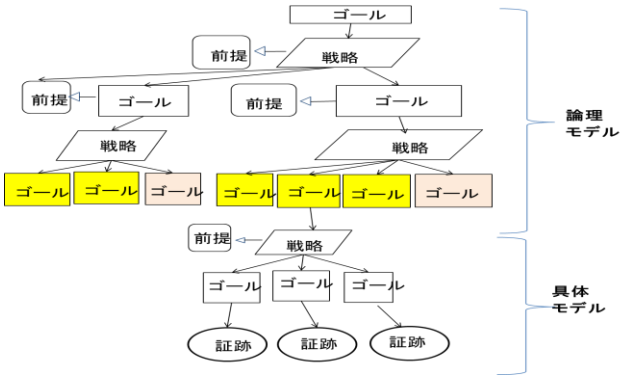


図 5　論理モデルと具体モデル

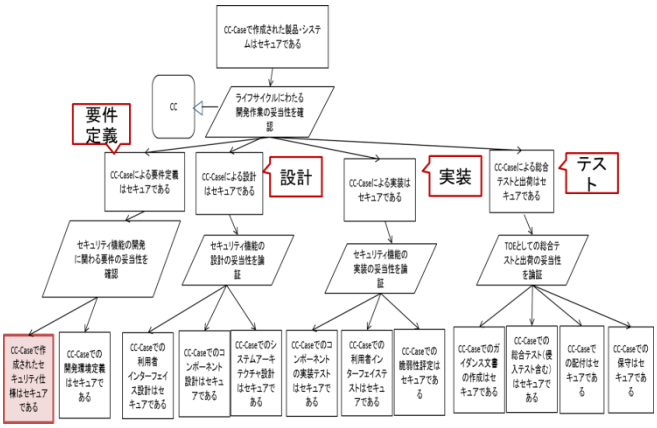


図 6 ライフサイクルにおける CC-Case 論理モデル

3.7 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

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 6 で具体的に説明する．ライフサイクルにおける CC-Case の最上位のゴールは「CC-Case で作成された製品・システムはセキュアである」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か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」，「CC-Case による設計はセキュアである」，「CC-Case による実装はセキュアである」と「CC-Case による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．

4. IoT セキュリティ認証への CC-Case の有効性

3 章までは， IoT に適用する場合の CC-Case の目的・定義等を中心に説明した．本章では，本論文のテーマである「認証とは何か？」そして「IoT 認証には何が必要か？」について考察したうえで，IoT 認証方法としてどのように CC 及び CC-Case が有効かを示す．

4.1 IoT セキュリティの認証と必要な要素

大辞泉によると認証とは以下の 2 つの意味を持つ.「1 一定の行為または文書の成立・記載が正当な手続きでなされたことを公の機関が証明すること．2 コンピューターやネットワークシステムを利用する際に必要な本人確認のこと．通常，ユーザー名やパスワードによってなされる.」本論文でいう認証とは「IoT 製品・システムのセキュリティ機能が正当な手続きでなされたことを証明すること」である．これは 2 を含んだ 1 であるが，認証制度ではなく，認証方式であるため，公の機関による証明までは求めていない．

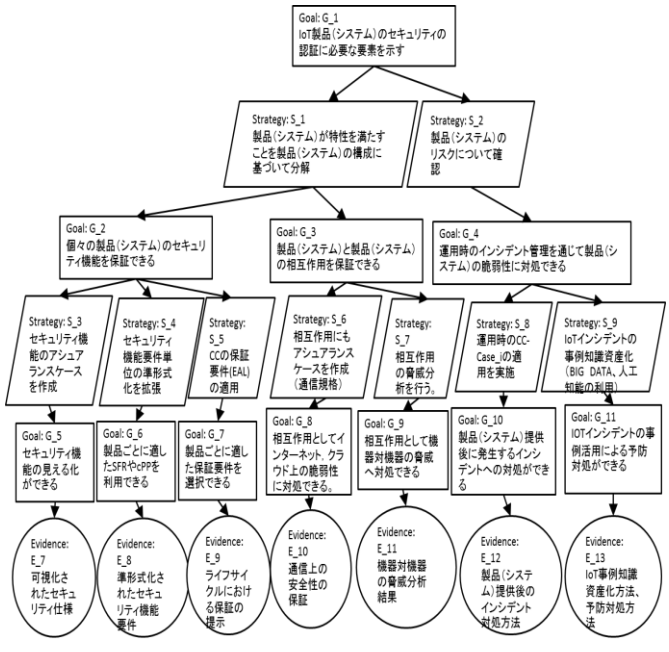


図 7 IoT セキュリティ認証で明確化すべき要素

IoT 製品・システムのセキュリティ認証に必要な要素，すなわち網羅性を保証ケースで示すと図 7 のようになる．まずは個々の製品（システム）の機能がセキュアであることが重要であり，本論文ではこの点を中心に述べる．そのうえで個々の製品（システム）の相互関係がセキュアであること，さらに運用時のインシデント管理を通じて製品（システム）の脆弱性に対処できることで網羅性をもった品質確保が可能となるのであり，今後順次検討をしていく．

4.2 IoT セキュリティ認証に対する CC の有効性

CC-Case の主要な技術要素である CC は基準としてさらには認証制度として，IoT セキュリティ認証に対して，どのような有効性をもちうるかに対して考察する．

CC に対し「CC に基づく認証はコスト高であり、認証を求めると IoT 製品のコストに跳ね返るため、適用は難しい」という懸念が現状多くなされている．この懸念に対する筆者らの見解を述べたい．

筆者らはまず第 1 に運用方法と認証の方式や参照とする基準は分けるべきだと考える．CC への批判の大部分は今の制度の運用方法からくるコスト増である．このコスト増は認証機関が時間をかけて審査しているため、発生しているものである．しかしながら、認証制度の課題と CC 自体のセキュリティ基準としての価値は別に考えるべきである．CC は IT セキュリティ評価の汎用的な国際的規格として，現状最も浸透しており、すぐれた基準である．従って，この審査上の非効率を改めることは大事であるけれども，CC 基準で認証方式を考えることはやはり必要である．

第 2 に PP 利用によるセキュリティ仕様明確化のしやすさである．CC では個々の製品・システムのセキュリティ要件を記述したセキュリティターゲット（ST）を作成するが，ST を作成しやすくできるプロテクション・プロファイル（PP）という ST の雛型も存在している（図 8）．PP とはある評価対象のタイプ（OS，ファイアウォール，スマートカード等）に対するセキュリティの設計仕様書であり． PP は，具体的な実装方法には依存しないため，多数の ST で再利用することができる．

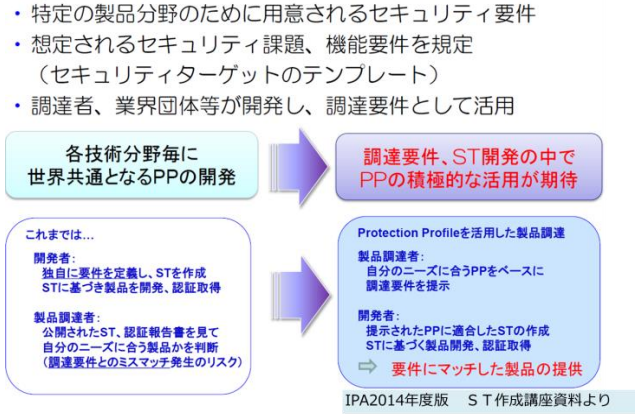


図 8 PP とは何か？

PP の目的は、利用者側のセキュリティに関する要求を明確にすることである．この PP は日本にはほとんど存在しなかったが，最近，表 2 にみられるように各種の PP が作成されてきている．この PP を利用することにより，CC のセキュリティ仕様（ST）は非常に簡単に作成可能となる．図 9 に示すようにこのひな形があれば PP 利用で ST の第 2 章から第 6 章というほとんどの部分をコピーして使用できるようになる．それにより製品開発側はその製品の具体的仕様をセキュリティ機能要件（SFR）のパラメータで示し，個別仕様に関して追記してセキュリティ仕様を書くことだけでセキュリティ仕様（ST）を記述可能なのである．

表 2 公開されている PP の例

分野	PP名称	発行日
ネットワーク基盤	PP_ND_V1.1	2012/6/8
ファイアウォール	PP_ND_TFFW_EP_V1.0	2011/12/19
VPNゲートウェイ	PP_ND_VPN_GW_EP_V1.1	2013/4/15
IPsec VPNクライアント	PP_VPN_IPSEC_CLIENT_V1.4	2013/10/23
SIPサーバー	PP_ND_SIP_EP_V1.0	2013/2/6
無線LANアクセスポイント	PP_WLAN_AS_V1.0	2011/12/1
無線LANクライアント	PP_WLAN_CLI_V1.0	2011/12/19
汎用OS	PP_GPOS_V3.9	2013/1/15
モバイルデバイス基盤	PP_MD_V1.1	2014/2/18
モバイルデバイス管理	PP_MDM_V1.1	2014/3/7
USBフラッシュドライブ	PP_USB_FD_V1.0	2011/12/1
ソフトウェアフルディスク暗号化	PP_SWFDE_V1.1	2014/3/31
認証局	PP_CA_V1.0	2014/5/16

分野	PP名称	発行日
VOIPアプリ	PP_VOIP_V1.2	2013/10/23
Emailクライアント	PP_EMAILCLIENT_V1.0	2014/4/1
Webブラウザ	PP_WEBBROWSER_V1.0	2014/3/31
BIOSアップデート	PP_BIOS_V1.0	2013/2/13
企業セキュリティ管理ポリシー管理	PP_ESM_PM_V2.1	2013/11/21
企業セキュリティ管理アクセス制御	PP_ESM_AC_V2.1	2013/11/12
企業セキュリティ管理ID・クレデンシャル管理	PP_ESM_ICM_V2.1	2013/11/21
データベース管理システム	PP_DBMS_V1.3	2010/12/24
デジタル複合機	PP_HCD_EAL2_V1.0	2010/2/26
デジタル複合機	PP_HCD_BR_V1.0	2009/6/12
IDS(侵入検知システム)	pp_ids_sys_br_v1.7	2007/7/25

IPA2014年度版　ＳＴ作成講座資料より

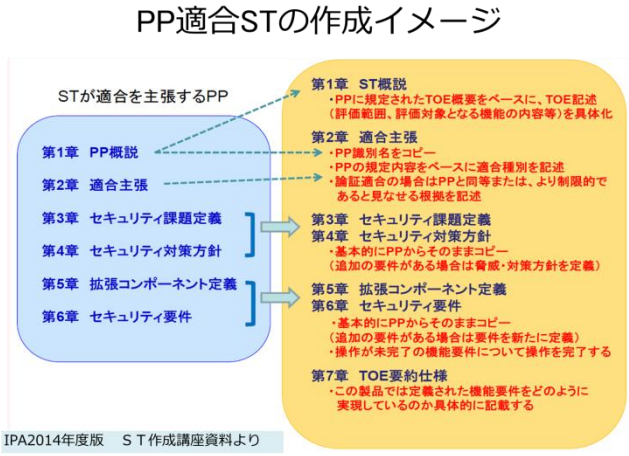


図 9 適合 ST の作成イメージ

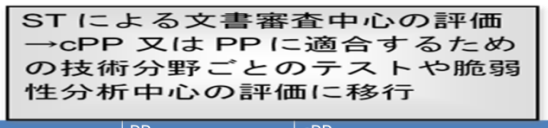
この PP は汎用的に各種製品のセキュリティ機能に対して作成可能であり，CC は IoT セキュリティ認証に対して，実用的な有効性をもちうる．

なお，PP は国ごとに個別に作成されてきたため、同じ製品分野の異なる PP が CC 承認アレンジメント（CCRA）内に複数存在することとなり，PP による機能の要件の不一致等の問題が表面化してきた．そこで CCRA では各国制度の承認のもとに PP を各技術分野ごとに世界共通化したひな型である cPP を作成することになった（表 3）．この cPP は CCRA の 2 年後には必須となることが決定されている．従来の PP では評価期間に 18 か月以上かかっていたのが cPP を用いた場合，米国では 90 日以下で認証可能になっている．

IoT 認証に対しては，CC 認証制度と同じ枠組みで行うこ

とは必ずしも必要ではない．ただし現在の CC では作成されていない個々の IoT 製品の各技術分野に対する世界共通のひな型である cPP の方式も参考にし，認証対象の形式化とよりコストのかからない運用制度を考える事は必要であろう．さらに認証機関によるものでなくても，アシュアランスケースで準形式的に示し，自己検証ができることも認証と認めるなどの緩和処置を施すことで認証コストを抑えることができるはずである．

表 3 従来の PP と cPP の違い



	PP	cPP
対象範囲	製品分野	技術分野
作成者	調達者（政府機関・認証機関）	国際的テクニカルコミュニティ（製品ベンダ，調達者，評価者，認証者）
評価保証レベル	EAL3～4	原則EAL1～EAL2
評価期間	18か月～	6か月以下（米国は90日以下を目標に推進中）
評価品質	評価者の能力に強く依存（評価機関・国によるバラツキ）	具体的なテスト，評価手法をサポート文書として規定することで，必要な品質を確保
暗号評価	CC/CEMに詳細な規定なし	サポート文書に詳細なテスト方法を記載．将来的にCC/CEMに盛り込む計画

4.3 IoT セキュリティ認証に対する CC-Case の特長

CC-Case は各製品・システム自体のセキュリティ機能における実際の認証実現について，CC に基づくセキュリティ要求プロセス，セキュリティ保証要件の提示等様々な期待できるメリットを提示している．この CC-Case の各種メリットの中で CC-Case の設計段階で cPP 作成にアシュアランスケースを利用し，見える化を図ることと「セキュリティ保証のツール」とし用いることが IoT 認証への適用時の最も特長的な内容である．

CC-Case この見える化は「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」の 3 種類である．

(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．

IoT 対応に際しては当該製品がセキュアであるという主張を当該製品の技術分野に適した PP を利用して当該製品のセキュリティ機能の論理を見える化し，証跡としてセキュリティ仕様を提示することになる．

アシュアランスケースを利用すれば要件の見える化，検証，妥当性確認がしやすい．さらにセキュリティ機能要件（SFR）単位の準形式化を個々の製品に適合した SFR へ拡張することで準形式化によるセキュリティ機能の見える化ができる．準形式的・カタログ化により齟齬が生じず，設計，相互理解，要件の再利用のしやすさが期待できる．

(3)「3.保証ストーリーの見える化」はアシュアランスケースの論理モデルによるプロセスと実施事項の明確化による可視化である．IoT 対応に際しては CC に規定されたセキュリティ保証要件に対応し，セキュリティ機能に対してどのレベルまでの対応が達成できているのかを提示し，保証することが可能となる．さらにこの保証と実現事項の対応をアシュアランスケースで見える化して提示可能である．さらに 製品･システム提供後のインシデント対応に関しては CC-Case のインシデント対応版である CC-Case_i[39]を用いて，インシデント対応を図り，新たに発生する脅威に対しても脆弱性対応を図っていくことができる．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．

使い方の観点ではその製品・システムが的確なセキュリティ機能を有していることを示す「セキュリティ保証書」の役割を担えるのが CC-Case である．セキュリティ機能とは個人情報や機密情報を暴露されたり,システムの稼働を妨害されたりすることがないように管理する機能である CC ではセキュリティ監査，通信，識別と認証,プライバシー等の 11 のクラスに分けてこれら機能の枠組みを規定している．セキュリティ機能には①正確に動作する②有効に機能することが要求される[3].一般の IT 機能であれば，利用者はその機能について，実際に利用してみることで保証されていることを確認できる．しかしセキュリティ機能は利用者が不測の事態を発生させてセキュリティ機能が正確かつ有効に動くことを確認することは大変困難である．そこで開発者自身がセキュリティ保証を検証しなければならない．IoT 認証に適しているかを妥当性確認するのは，第 3 者機関であり，製品・システムの利用者であり，開発者は彼らに理解してもらいやすい保証書を提示する必要がある．

アシュアランスケースで図示するため，この種の検証・妥当性確認に適しており[29]，CC-Case は検証・妥当性確認を CC ベースでセキュリティ要件の論理関係を明確化して実施するものであり，開発者と第 3 者機関や製品・システムの利用者というステークホルダ間の認識の食い違いを防ぎ，納得感のもてる検証・妥当性確認を可能とする．

5. おわりに

本論文では，CC-Case を、IoT セキュリティ認証に適用する方法を示し，①アシュアランスケース利用により、複雑な個々の IoT 製品の認証が簡便にできる可能性があることと②IoT 製品ごとの PP 及び cPP 作成の有効性等を示した．実際には IoT セキュリティ認証方法はまだ定まっておらず，

本論文で取り上げたこと以外に多くの検討が必要である．筆者らは今後，IoT 対応に適したモデルとして，CC-Case 設計段階の具体的詳細化を進めていく．また個々の IoT 製品に適した PP をセキュリティ機能要件（SFR）の利用と拡張により作成できることを示し，実際の IoT 製品で実証研究を行っていきたい．本研究が現在のセキュリティ認証の課題解決に役立ち，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　この研究をするにあたりサポートして頂いた皆様，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) 独立行政法人情報処理推進機構,つながる世界のセーフティ＆セキュリティ設計入門～IoT 時代のシステム開発『見える化』, 2015
8) 後藤厚宏， IoT 時代のセーフティ・セキュリティ確保に向けた課題と取組み,IPASEC セミナー（2015)
9) 伊藤公祐， IoT 時代のセキュリティの確保に向けて, IPASEC セミナー（2015)
10) Sindre, G. and Opdahl. L. A. : Eliciting security requirements with misuse cases, Requirements Engineering, Vol.10, No.1, pp. 34-44 (2005).
11) Mouratidis, H. : Secure Tropos homepage, (online), available from <http://www.securetropos.org/>.
12) 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).
13) 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).
14) 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).
15) 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)
16) 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
17) 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
18) 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）
19) 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
20) 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
21) 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
22) OMG, ARM, http://www.omg.org/spec/ARM/1.0/Beta1/
23) 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/
24) 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
25) Stephen Edelston Toulmin, “The Uses of Argument,” Cambridge University Press,1958
26) The Adelard Safety Case Development (ASCAD), Safety Case Structuring: Claims, Arguments and Evdence,http://www.adelard.com/services/SafetyCaseStructuring/index.html
27) DEOS プロジェクト, http://www.crest-os.jst.go.jp
28) 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
29) 梅田浩貴,第 3 者検証におけるアシュアランスケース入門～独立検証及び妥当性確認(IV&V)における事例紹介 , ETwest(2015)
30) 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
31) 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
32) 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
33) 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
34)　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
35) 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
36) 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)
37) 島田裕次, ISO27001 規格要求事項の解説とその実務―情報セキュリティマネジメントの国際認証制度への対応,日科技連,(2006)
38) 吉岡信和, Bashar Nuseibeh, セキュリティ要求工学の概要と展望　情報処理 Vol.50 No.3(2009).
39) 金子朋子，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,JNSA,2015