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]　TAKAHASHI　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 be an effective certification technology to describe precisely complicated security requirements of IoT.

Keywords: IoT, certification technique, 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創造するモノのインターネット（IoT: 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の脆弱性を突いて攻撃を仕掛けてくるためである．

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 に、開発方法論・プロセスからの対応を示す．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．なお，詳細は 4.1 節に示すが，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

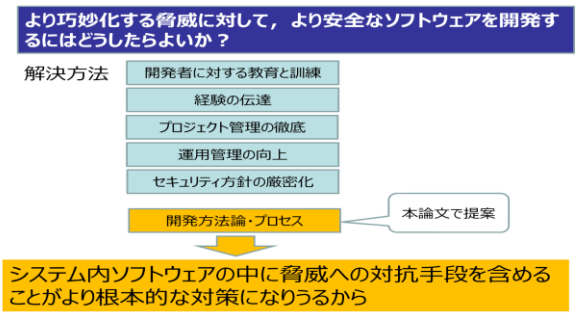


図 1　開発方法論・プロセスからの対応

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

†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

意の上で決定する手法 CC-Case[5] [6]を提案している. また CC-Case は 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．これまでの CC-Case では, CC 認証を伴うセキュリティ要件定義中心を主たる目的として提案してきたが，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[6]であり，本論文ではライフサイクルごとのモデルを提示する． CC-Case は製品・システム自体のセキュリティ機能を保証する基準としては CC をベースにするが，製品（システム）と製品（システム）の関係性や運用時の変更要求管理・インシデント管理を通じた製品（システム）の脆弱性対処においては，CC の応用とは異なるソリューションを想定している. また CC 認証制度が個々の製品のセキュリティ目標（ST: Security Target）中心の評価から、プロテクションプロファイル（PP: Protection Profile）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が効率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 の複雑性への対処可能性については，CC-Case が IoT の複雑なセキュリティ要件をアシュアランスケースの利用によって可視化し，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 レコーダーの踏み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 年にはジープを車載のインフォメーションシステム経由で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を用いて 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 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 コモンクライテリア(CC)

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）やプロテクションプロファイル(PP)に記載すべき内容が規定されている．図 2 に，CC 構成と ST の記載内容を示す． CC のパート 2 に評価対象（TOE:Target Of Evaluation）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ー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 に CC パート 2 の規定、図 4 に準形式的な記載事例を示す．図 3 に示すように，機能要件 FIA_AFL1.1 で TOE セキュリティ機能（TSF: TOE Security Functions）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をする． 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.

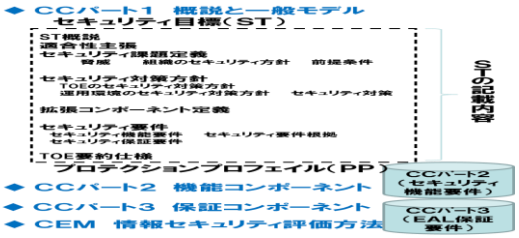


図 2 CC 構成と ST の記載内容

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

2.3 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].

2.4 セキュリティケース

GSN を提唱した Kelly ら[30]がセキュリティアシュアランスケース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 ISO14971，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].

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)」[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（Collaborative PP)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．cPP については、4.2 節で詳しく述べる．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 セキュリティ認証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 セキュリティ特徴にあった基準，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 セキュリティ認証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保証に関するライフサイクルサポート規格である．一方 ISMS（ISO/IEC 27001）は，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.製品（システム）が利用される段階になって，管理する際には ISMS は重要であるが，IoT のセキュリティ機能の認証においては CC の方が用途にあっている．

IoT セキュリティにはつながる対象となる個々の製品のセキュリティ機能保証が不可欠である．従って 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．

CC は製品・システムのセキュリティ機能の安全性を第三者に示し，保証することができる基準であり，これをベースに用いて，個々のセキュリティ機能を示すことと，それらの相互依存関係の保証を行うことにより，システム全体としての保証を示すのが適切であると考える．

4. IoT セキュリティ認証への CC-Case の有効性

本章では，本論文のテーマである「認証とは何か？」そして「IoT セキュリティ認証には何が必要か？」について考察したうえで，IoT セキュリティ認証方法としての CC の有効性及び今までハイレベルの枠組みしか定義されていなかった CC-Case のライフサイクルにおける方針を述べる．

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 に近い．理由は CC-Case のスコープが 2 の個人認証だけでなく，製品（システム）のセキュリティ機能，及び製品（システム）と製品（システム）の相互依存の関係性に相当する通信と相互作用，運用時の脆弱性対処の保証を包括的に含んでいるが，認証制度ではなく，認証方法であるため，公の機関による証明までは求めていないからである．

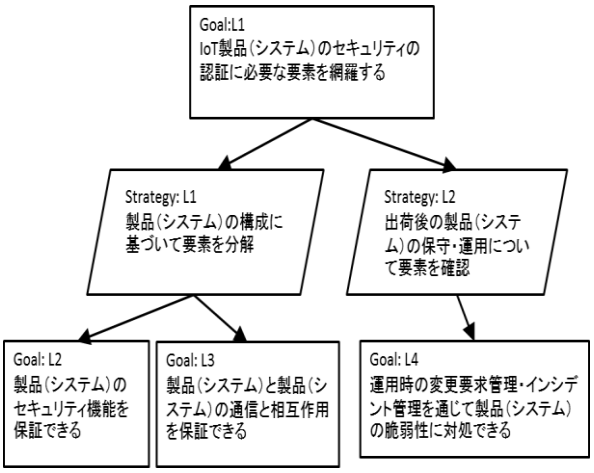


図 5 IoT セキュリティ認証で明確化すべき要素

IoT 製品・システムのセキュリティ認証において，考慮すべき点の 1 つは特に業界分野における取組状況の違いである．IoT 製品・システムは多種多様であり，自動車，家電，携帯電話，制御システム，ヘルスケア等つながるモノの自体の対策状況は業界分野においても異なっている[9]. 自動車業界は米国や欧州のメーカーやサプライヤによる委員会等で標準化と検討が幅広く進んでいるが, ヘルスケア, 家電の分野では標準検討段階中であるなど，業界分野ごとにセキュリティ対応レベルも異なり，標準の動向も異なっている．しかしながらインターネットを通じてつながる世界は業界分野ごとに限定された基準のみで保証できるわけではない．そこで業界分野による状況の違いを踏まえたうえで共通的に製品（システム）を保証する必要が生じている. その保証は単に製品単体だけでなく, 製品（システム）相互の関係性，製品出荷後の対応までに及ぶべきであると筆者らは考える.

そこで IoT 製品・システムのセキュリティ認証に必要な要素を網羅的にアシュアランスケースで示すと図 5 のようになる.「Goal:L1　IoT 製品（システム）のセキュリティの認証に必要な要素を洗い出す」は，製品（システム）の構成に基づいて考えると，製品（システム）自体の機能と製品（システム）と製品（システム）の関係性に分けることができる．さらに製品（システム）と製品（システム）の関係性は通信など製品（システム）と製品（システム）の間に存在する関係と機器対機器の相互作用の 2 つを示している．そこで Goal:L1 は「Goal:L2 製品（システム）のセキュリティ機能を保証できる」ことと「Goal:L3 製品（システム）と製品（システム）の通信と相互作用を保証できる」に分解することができる．さらに製品（システム）のリスクに基づいて考えると IoT 製品（システム）のセキュリティの認証に必要な要素は,「Goal: L4 運用時の変更要求管理・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」こととなる.

つまり個々の製品（システム）の機能がセキュアであること，個々の製品（システム）の通信と相互作用がセキュアであること，さらに運用時の変更要求管理・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セキュリティ確保が可能となるのである.

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 に認証制度の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認証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も含め利用範囲, 利用方法等に関する更なる検討は必要だが，IoT のための認証方法のベースとしてはセキュリティ機能要件と保証要件を規定している CC を利用したい.

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目標（ST）を作成するが，ST を作成しやすくできる PP という ST の雛型も存在している（図 6）．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.

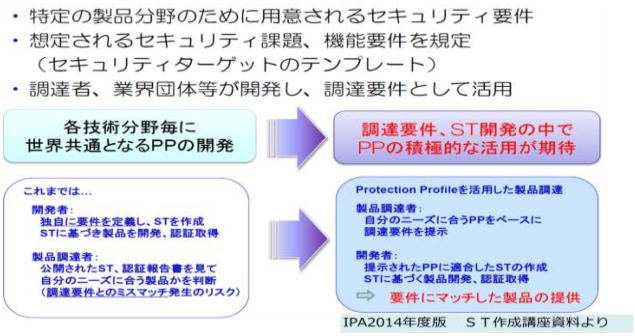


図 6 PP とは何か？

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 1 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 ST は非常に簡単に作成可能となる. 図 7 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 ST を記述可能なのである．

表 1 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

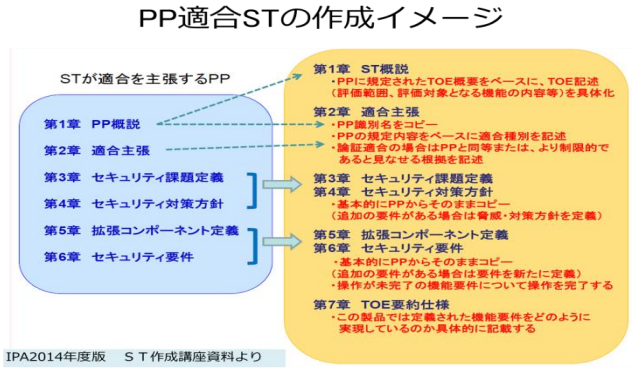


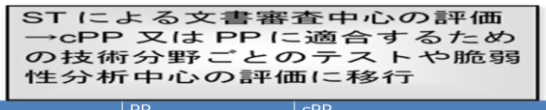
図 7 適合 ST の作成イメージ

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 :Common Criteria Recognition Arrangement）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 2 に従来の PP と cPP の違いを示すこの cPP は 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 セキュリティ認証に対しては，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 2 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必要な要素を満たすための CC-Case の方針

4.1 節で示したように IoT セキュリティ認証に必要な要素は，個々の製品のセキュリティ機能の認証，製品（システム）の通信と相互作用の認証と運用時の脆弱性対処に分けて考えることができる．

そこで CC-Case により，これらの要素を満たすために，どのようなことをするべきであるかを(1)セキュリティ機能の保証,(2)製品（システム）の関係性の保証，(3)運用時の脆弱性対処の 3 つの観点から述べる．

(1)セキュリティ機能の保証

前述のように業界分野ごとの取り組み状況の違いを踏まえたうえで，共通的に製品（システム）自体と製品（システム）の通信と相互作用，製品出荷後の対応を保証する必要が生じている．筆者らが提案する CC-Case による IoT セキュリティ認証とは特定の分野に閉じた認証ではない．インターネットを通じてつながる IoT に共通な認証基盤として，CC-Case とその拡張を推奨している．しかし現実に多様な製品（システム）がつながる以上，まずはその製品（システム）の(1)セキュリティ機能の保証が必要であると

考える．このため「Goal: L2 製品（システム）のセキュリティ機能を保証できる」がゴールとしてあげられる．

「Goal: L2 製品（システム）のセキュリティ機能を保証できる」を達成するために CC-Case を利用すると 3 つの戦略に基づくゴールが考えられる（図 8）．

1 つめは，セキュリティ機能のアシュアランスケースを作成することにより，「G_1 個々の製品（システム）のセキュリティ機能の見える化ができる」ことである．証跡は可視化されたセキュリティ仕様となる．各製品固有のセキュリティ機能全体に対してセキュリティ要件の見える化を図ることでその製品自体の保証が可能となる．見える化の手段として安全性分野で欧州を中心に広く用いられているアシュアランスケースを用いる．従来から安全性は自然に発生する故障や人為的なミスを対象としているが，セキュリティは悪意を持った攻撃を対象にすることが大きく異なる．セーフィティとセキュリティの設計は独立したプロセスで実現されることが多いと想定されるが，IoT でつながる世界においては双方を切り離すのではなく，共に関係性をもって推進されることが必要である．セキュリティ要求のアシュアランスケースである CC-Case は安全性分析の延長線上に悪意を持った攻撃への対応を可能とする手法となっている．そのため安全性手法との親和性が高く実用的である．

2 つめはセキュリティ機能要件単位の準形式化を現在，PP で対応している製品だけでなく，IoT 製品に拡張することにより，「G_2 分野・製品ごとに適した SFR や cPP を適用できる」状態にすることである．現在，製品（システム）のセキュリティ機能は業界分野ごとに製品（システム）の特性に応じたセキュリティ機能基準を定めていく方向性にある．この流れにあわせて業界分野ごとに準形式化されたセキュリティ機能要件を各 IoT 製品分野で作成していくことを推奨したい．準形式化されたセキュリティ機能要件という基準で各業界分野の製品（システム）が共通的に作成されるならば，相互理解が容易となり，業界分野の違う製品も共通的に保証することが可能となる．さらに 4.3 節であげたメリットを享受できよう．証跡は準形式化されたセキュリティ機能要件となる．

3 つめは CC の保証要件(EAL)の適用により，「G_3 製品ごとに適した保証要件を選択できる」ことである．証跡はライフサイクルにおける保証の提示となる．CC 保証要件の EAL レベル 7 では形式的検証済み設計，およびテストが必須となっている．よりセキュアな組込み機器のセキュリティ機能を形式手法によって開発することも今後の検討事項となろう．

上記のセキュリティ機能の保証の中で，製品ごとに適した SFR や cPP を作成していくこと以外は従来から CC-Case での実現方法を IoT 製品（システム）に拡張的に適用することで可能であるが，いずれのゴールに対しても今後具体的に適用を具体的に行い，その評価を行って，事例を増やしていくことが必要になる．

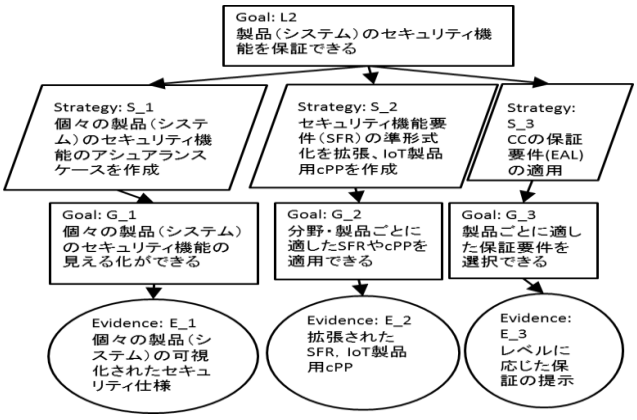


図 8 セキュリティ機能の保証

(2) 製品（システム）と製品（システム）の通信と相互作用の保証

「Goal: L3 製品（システム）と製品（システム）の通信と相互作用を保証できる」を達成するために以下の 2 つの戦略に基づくゴールの達成が必要と考えられる（図 9）．

1 つめは，製品（システム）・製品（システム）間の通信のセキュリティ確認にアシュアランスケースを作成することにより，「G_4 インターネット，クラウド，通信の脆弱性と暗号化などの対処を見える化できる」ことである．証跡は通信上の安全性の保証となる．今までの CC-Case はセキュリティ製品（システム）の機能の保証をテーマとしてきており，通信上の安全性の保証は検討範囲に入っていなかった．アシュアランスケースを利用してインターネット，クラウド等の通信上の安全性を見える化することは可能であろう．ただし各種通信プロトコル規格，暗号規格とその脆弱性（リスク）に照らして，現状起こりうる脅威，必要な対策，残すべき証跡を的確に洗い出し，論理モデルを構築することが必要になる．その上で，その製品（システム）の利用シーンに応じた具体モデルを構築することになろう．

またスマートグリッドなどの社会インフラ制御システムにおいてはサーバに複数の組込みシステムが接続される形態が大多数であり，組込みシステムはクラウド化がすすんでいる[41]．そのため，組込み機器向けの対策以外にサーバ向けの対策が必要になる．

2 つめは相互作用の脅威分析を行うことにより，「G_5 機器対機器の相互作用から生じる脅威へ対処できる」ことである．証跡は機器対機器の脅威分析結果である．相互作用の脅威分析に関しては，「アクタ関係表に基づくセキュリティ要求分析手法（SARM）」の拡張により対応可能と考えている．SARM は CC-Case におけるセキュリティ要求分析手法である，今後詳細を公開していく．SARM[15]は複数アクタ対複数アクタの関係で相互の意図を表形式の交差する欄に記入していく「アクタ関係表（ARM）」を利用し，そのアクタに攻撃者を記述することで攻撃者の意図を表記するセキュリティ要求分析手法である．このアクタに対して，

人物ではなく機器（システム）を設定することにより，複雑に絡む機器（システム）対機器（システム）の関係性を網羅的に表形式に整理して表現することが可能となる．セキュリティ要求分析手法である SARM は，要求分析手法であるアクタ関係表を拡張して，悪意を持った攻撃手法の分析も可能にした手法であり，セーフティとセキュリティの両方の分析ができる．

IoT 製品・システムのセキュリティ認証において，考慮すべき点としてセキュリティ上の対象（守るべき資産）の違いがある．情報セキュリティの対象は情報である．これは情報セキュリティの CIA はいずれも情報の特質に着目した特質であることからも明らかである．これに対して IoT セキュリティが対象としているのはモノである．ここでいうモノとは自動車，家電機器などの製品の場合，人の生命，健康，財産を含むが，情報は財産の一部であるに過ぎない．プラントなどの制御システムの場合，対象は情報ではなく、設備、製品などのモノと連続稼働を必要とするサービスになる．そこで IoT 製品のセキュリティ認証は情報以外の対象に対しても保証が必要性である．情報以外のモノ，サービス等対象に対しても脅威分析が可能となるように SARM を拡張する必要がある．

上記の製品（システム）の通信と相互作用の保証は，要件定義段階が中心である従来の CC-Case では明示されてこなかった範囲であるが，IoT セキュリティ認証に必要な要素であり，具体的な提示が今後の課題である．

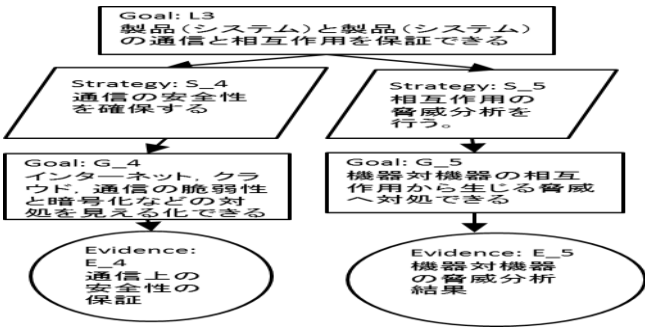


図 9 セキュリティ機能の保証

(3)運用時の脆弱性対処

セキュリティ機能の保証と製品（システム）の関係性の保証は製品（システム）の出荷・運用開始前の状態での保証を指している．しかし，運用時の脆弱性対処は製品（システム）の出荷・運用開始後の状態を指す．

運用時の製品（システム）のリスクに基づいて考えると「Goal: L4 運用時の変更要求管理・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」を達成するために以下の 2 つの戦略に基づくゴールの達成が必要と考えられる（図 10）．

1 つめは，インシデントの事例を知識資産化すれば，脅威に対してより効果的な予防処置をとることができよう．ただし IoT の場合，その知識資産化は IoT センサー機器からの情報収集を必要とし複雑で大容量となることは想像に難くない．そのためビッグデータ，人工知能の利用等の先端 IT 技術を用いた知識資産化により「G_6 IoT インシデントに対する的確な対応や予防対処ができる」ことが望まれる．さらに確実な知識資産化のためには，IoT の複雑な要件をマネジメントし，継続的に改善を実施していくための新たな品質マネジメントシステムも必要になろう．証跡としては，IoT 事例知識資産化方法，予防対処方法となる．上記の運用時の脆弱性対処には，CC-Case の運用時の手法である CC-Case_i や CC-Case では明示されてこなかった IoT インシデントの事例活用が必要であり，具体的な提示は今後の課題である．

2 つめは，運用時にアシュアランスケースの適用を実施することにより,プロセスアプローチに基づいた「G_7 製品（システム）提供後に発生する変更要求やインシデント対処の見える化ができる」ことである．長期に渡り利用することが前提となる生活機器，制御システム等の場合，新たな脆弱性の発見，攻撃者による新たな手法の開発，技術進歩に伴う搭載されたセキュリティ技術の陳腐化などによる脆弱性への対応が必要である[7]．脆弱性への対応するためにはセキュリティ更新作業等の変更要求への対処が必要である．運用時はインシデント対応を含めて，製品（システム）提供後に発生する変更要求に対処するプロセスを定義しているが，今後より具体的なアプローチを定めていくことにより有用性が期待できる．証跡として製品（システム）提供後のインシデント対処方法となる．

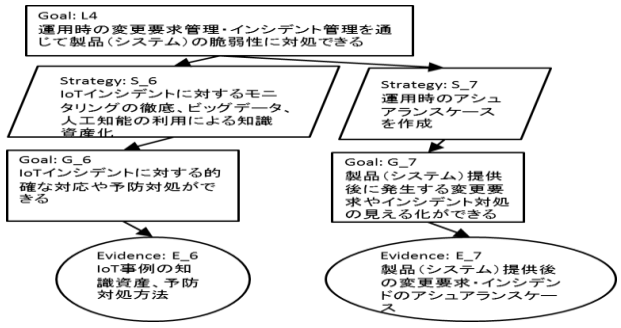


図 10　運用時の脆弱性対処

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，①CC-Case がアシュアランスケースを利用しているという特徴から利用により、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 作成を利用すること有効性等を示した．そして今後，より具体的なセキュリティ要求・設計・運用基盤として推進するための方向性を提示した．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ろう．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．

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
40) 梶本一夫,家電業界におけセーフィティ＆セキュリティ，第 40 回 ISS スクエア水平ワークショップ
41) 金井遵,組込みシステムにおけるセキュリティの課題～セキュアプラットフォーム研究開発の取組み～，第 40 回 ISS スクエア水平ワークショップ