Vol.2016-MBL-80 No.5
Vol.2016-CDS-17 No.5
2016/8/24

CC-Case を用いた IoT セキュリティ要件の可視化

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はつながる世界では重要である．つながる対象の広がりに応じて，IoT セキュリティ要件はより複雑化するため，その可視化は特に重要な課題である．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 によるセキュリティ要件の可視化を提案する．これは従来の脅威分析に比べ，シンプルで分かり易い図示手法である．本論文では IoT セキュリティの具体的事例をもとに CC-Case による脅威分析から対策立案までのプロセスとそのメリットを示す．

キーワード：IoT セキュリティ，可視化，GSN，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

Visualization of IoT Security Requirements using CC-Case

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

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 becomes more important in such the connected world. Depending on increasing a variety of connected targets, IoT security requirements becomes even more complicated. Therefore, the visualization of IoT security requirements become a important issue. We propose a visualization method of IoT security requirements by applying the CC-Case which realizes security requirement analysis and assurance by using the Common Criteria (CC) and the assurance case. This method has simpler, and plainer diagrammatic representation than conventional threat analyses. In this paper, We show the drafting process and merits of CC-Case from threat analysis to countermeasure are planning using a concrete example of IoT security.

Keywords: IoT security, Visualization, GSN, 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．

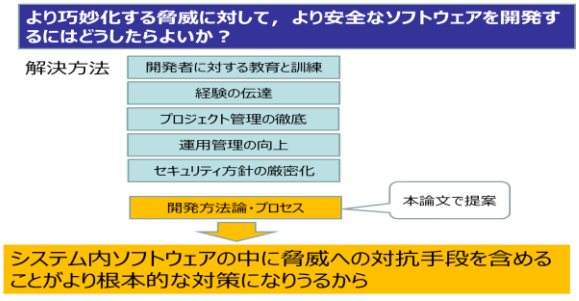

図 1　開発方法論・プロセスからの対応

†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-MBL-80 No.5
Vol.2016-CDS-17 No.5
2016/8/24

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．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．本論文では 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する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は日増しに増加している[7][8][9]. 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[9]．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[9]. 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[9]．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[9]．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[9]．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[9]．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(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．

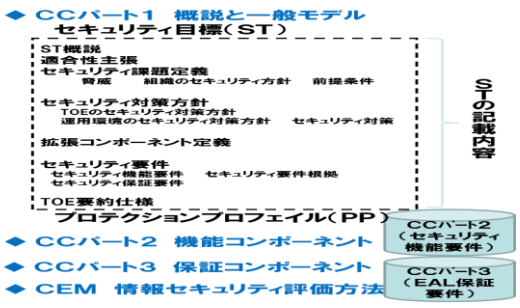

図 2 CC 構成と ST の記載内容

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

2.4 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 が JST CREST DEOS プロジェクトで開発されている[27] [28]． 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[30]．Goodenough 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[31]. Lipson H 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[32]．Ankrum 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[33]．CC-Case 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[5] [7].

3. CC-Case によるセキュリティ要件可視化

3.1 IoT セキュリティの課題

2.1 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・システムごとに要件が異なるため，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変更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いて，随時発生し続ける脅威に対処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[7] [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，製品やシステムをつなぐ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．その結果，IoT 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，機器類の安全性規格等で広く利用されていること，及び目標達成を事実に基づき，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ことからアシュアランスケースが向いていると考える．

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．具体的な IoT セキュリティ要求分析への利用方法は CC-Case の目的・定義等の概要と共に次節以降に説明する．

3.3 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[34]．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している．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．

3.4 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であり，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の記述であり，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を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．具体モデルは個々の製品・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設計段階における論理モデルは今後の課題であるが，4 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．

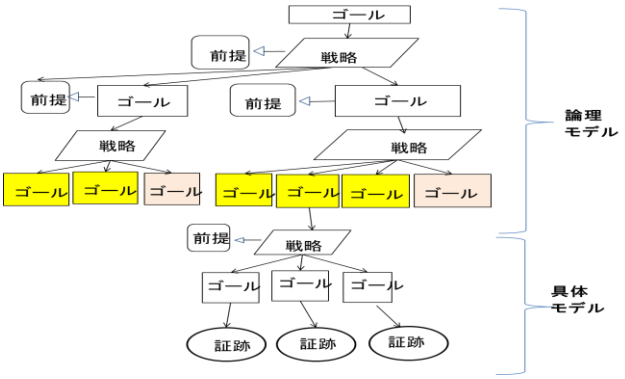

図 5　論理モデルと具体モデル

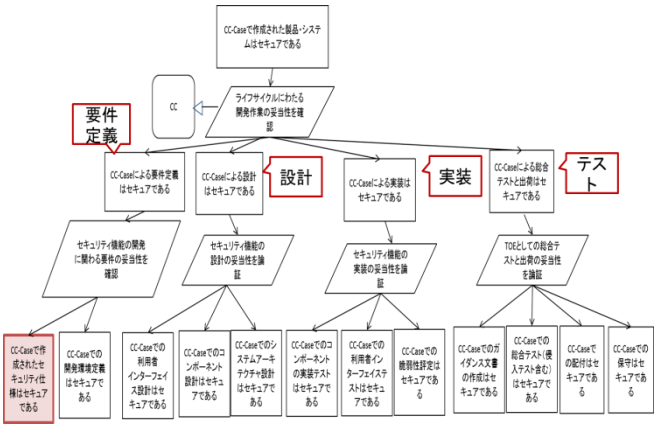

図 6 ライフサイクルにおける CC-Case 論理モデル

3.5 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ゴール構造表記法(GSN:Goal Structuring Notation)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，「ライフサイクルにおけ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 セキュリティ要求の可視化

4.1 CC-Case の可視化の特長

CC-Case は 3 つの可視化（=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[35].

(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．

(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るセキュリティ要求の解決ストーリーの可視化である． CC-Case はセキュリティ要求段階において，脅威を重複なく網羅的に洗い出しやすいプロセスと脅威への対処方法の可視化を行う．プロセスアプローチによる必要十分な脅威の抽出を行い，シンプルに可視化できる．さらに実施対策の合意と残存リスクの提示により，脅威分析の適切性を保証できる．尚、本論文でいう保証は，規定するプロセスに関係者の合意があること，残存リスクの可能性を明記することより生じている．

4.2 CC-Case の使い方の特長

使い方の観点で CC-Case 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 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 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 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セキュリティ要求分析のために役立ててほしいのがこの CC-Case である．このため，CC-Case 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．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 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 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ノウハウの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．

4.3 IoT セキュリティの脅威と対策のプロセスと具体的適用事例

本節では「IoT 開発におけるセキュリティ設計の手引き」に示された IoT の具体的事例をもとに CC-Case によるセキュリティ要件の可視化方法を示す[36]．図 7 はスマートハウスの脅威と対策の検討例を図示したものであり，「HEMS コントローラを中心に接続された HEMS 対応機器やそれ以外のネットワーク対応機器がホームルータを介してインターネットに接続されており，外出先からスマートフォンを用いてクラウドサービス経由で家庭内の機器にアクセスすることによって，家庭内の機器の様子を監視したり，遠隔操作したりすることが可能となる．このシステムでは，スマートハウス内に設置された機器の一部に保存されたデータの漏えい,通信路上のデータの盗聴･改ざん，クラウドサービスやインターネット上に接続された中継機器への不正アクセス,（不正ログイン，その後の不正コマンド発行による許可なき遠隔操作),クラウドサービスやインターネット上に接続された中継機器への DoS 攻撃，クラウドサービス上に保存されたデータの漏えいなどの脅威が想定される」との考察がなされている．[36].

図 7 の事例を CC-Case で記述したものが，図 8 である．図 8 は「G_1 スマートハウスのセキュリティ設計は安全である」というゴールを満たすために,「S_1 脅威分析の洗い出しと対策を示す」戦略を「G_2 スマートハウスの脅威分析は妥当である」と「G_3 スマートハウスの脅威に対する対策立案と選択は妥当である」の 2 つのゴールに分けて説明している．図 8 に示す G_2 以下はスマートハウスにつな

がっている機器ごとと機器間の通信ごとに脅威を洗い出すことを求めている．各機器と機器間の通信の双方の脅威の出所をおさえれば，網羅的な脅威の洗い出しが可能になるからである．これらは G_4 から G_11 のゴールとして設定され，各ゴールで洗い出した脅威に対する対策を E_1 から E_8 の証跡として提示する．図 7 の事例をもとにすると脅威の詳細が各証跡となる．

図 9 に示す G_3 以下は，洗い出した「S_4 対策ごとに論証する」,「S_5 対策選択に合意する」,「S_6 残存リスクを影響分析する」という 3 つの戦略をプロセス化している．E_1 から E_8 であがった対策の中には，発生箇所が異なっていても対策として同じものが含まれるため，対策ごとに実施方法を証跡として示す．これらは脅威の洗い出しに対する重複の排除となる．また，実施する対策は経営層・顧客等のステークホルダとの合意が必要である．さらにコスト等そのステークホルダ等を考慮して実施可能な対策でなければ実施できない．そこで実施の合意を得られた対策は合意を証跡として残し，コスト等の事情で実施にいたらなかった対策は影響分析をして残存リスクを証跡として示すことが必要である．これらは選択する対策と残存リスクを対処するプロセスとなる．尚，G_12 から G_19 のゴールが妥当である根拠として E_1 から E_8 の証跡を示しているが，これらが実際に「妥当である」というためには，また別の考察や判断基準が必要であろう．本論文のいう妥当性と実際の妥当性の提示にはかなりのギャップがあり，本論文ではある項目に対して何が妥当性なのかを提示する必要があるためその明示を求めている．

4.4 IoT セキュリティ要件可視化に対する CC-Case の特長

IoT セキュリティ要求可視化に対する CC-Case の特長は，「網羅性の高さ」,「必要十分性の確保」,「シンプルな記法」の 3 点に集約できる．これらは IoT セキュリティ自体の特徴と 4.1 節から 4.3 節で示した CC-Case の可視化と使い方や脅威と対策のプロセスの特長を考慮したうえで結論づけられる．

(1)「網羅性の高さ」は 4.3 節で示したように CC-Case がつながっている機器と機器間の通信という脅威の発生ポイントに網羅性をもたせた要求分析であるため可能である．IoT では情報のみでなくモノもつながるため，攻撃を受けた場合，損害は健康や生命にもおよび，より重大になる．そこでセキュリティ要件の洗い出しに漏れがないことが必要である．従来の脅威分析は特定のシーンの分析が主流であるが，特定の脅威シーンの中での思いついたことを洗い出すアドホックな手法では，網羅的に脅威をあげることが難しく，CC-Case はアドホックな手法に対してアドバンテージをもつと考える．

(2)「必要十分性の確保」は 4.3 節で示した CC-Case の脅威の洗い出しと対策選択のプロセス化とそれを最適化する 4.2 節で示した使い方によるものである．

CC-Case では脅威は発生箇所が異なっていても対策として同じものが含まれるため，対策ごとに脅威をまとめ，これらは脅威の洗い出しに対する重複の排除を行うプロセスケを規定している．さらに対策においては現実的にはコストが高いから実施不可能ということが起こるが,「議論のツール」である CC-Case はステークホルダの合意を得られる対策を追求する．その上で対策できたことと残したリスクを明確化する手順を規定している．IoT は異なる業界のより多くのステークホルダを含む合意が必要となると考えられ，要求段階においてこのような合意形成の重要性はより増すと想定される．近年 IoT を支えるセーフティ&セキュリティの関連技術の 1 つとして、プロセス技術が重要視されてきている[37]. 手順, 権限をはっきりさせ, リスク分析, 脅威分析から設計，実装，検証の各内容・結果の相互関係のトレーサビリティを保証する技術である．CC-Case はまさにこのように求められているプロセス技術自体を CC とアシュアランスケースをベースに体系化した開発方法論である．

(3)「シンプルな記法」に関して 4.1 節可視化の特長で示したように CC-Case は主張と証跡，論理をシンプルに図示する記述法である．IoT とは個々の製品がつながることであるため，IoT セキュリティ要件はより複雑になる．複雑化すればするほど要件はわかりにくくなるため，わかりやすさが求められる． IoT セキュリティ要件可視化において，テキストベースでの要件記述や 2.2 節に示した従来の手法と異なり，必要十分な要件をシンプルに図示し，可視化が簡便できる特長は有効であろう．

Vol.2016-MBL-80 No.5
Vol.2016-CDS-17 No.5
2016/8/24

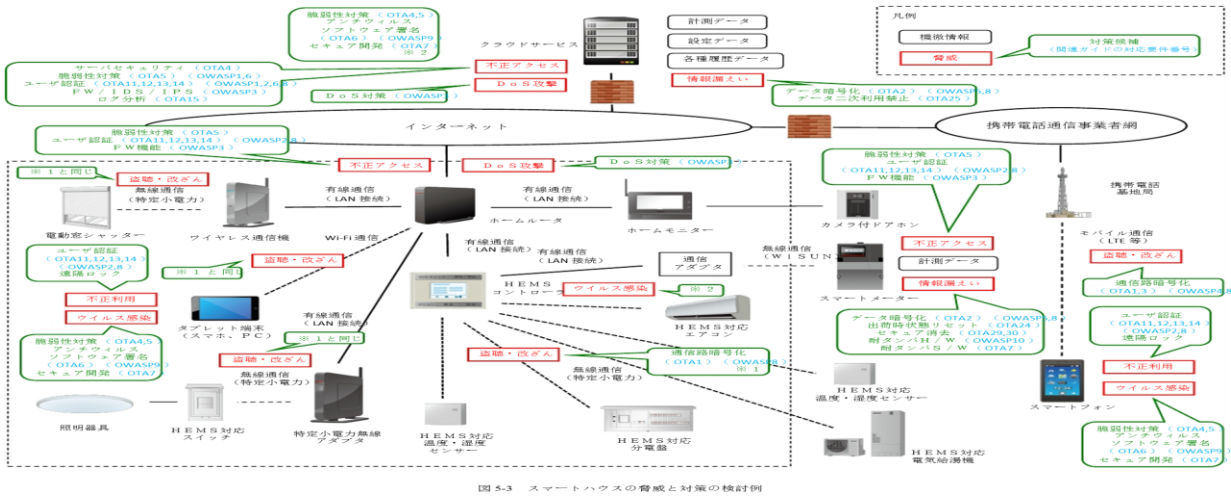

図 7　スマートハウスの脅威と対策の検討例

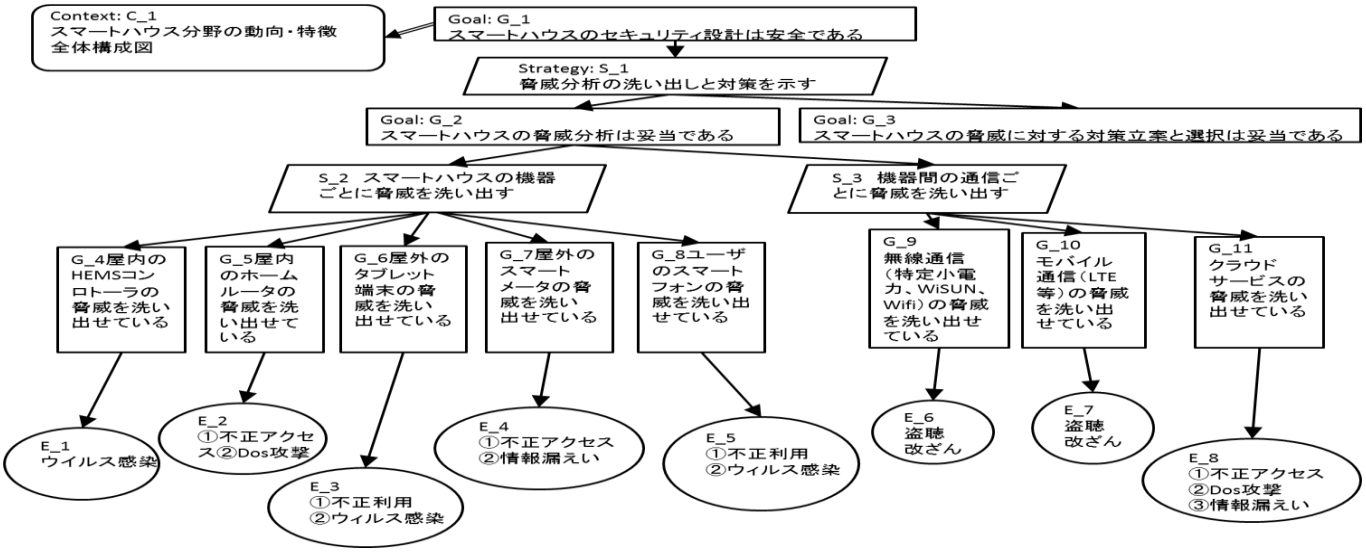

図 8.スマートハウス事例への CC-Case の適用例（脅威分析部分）

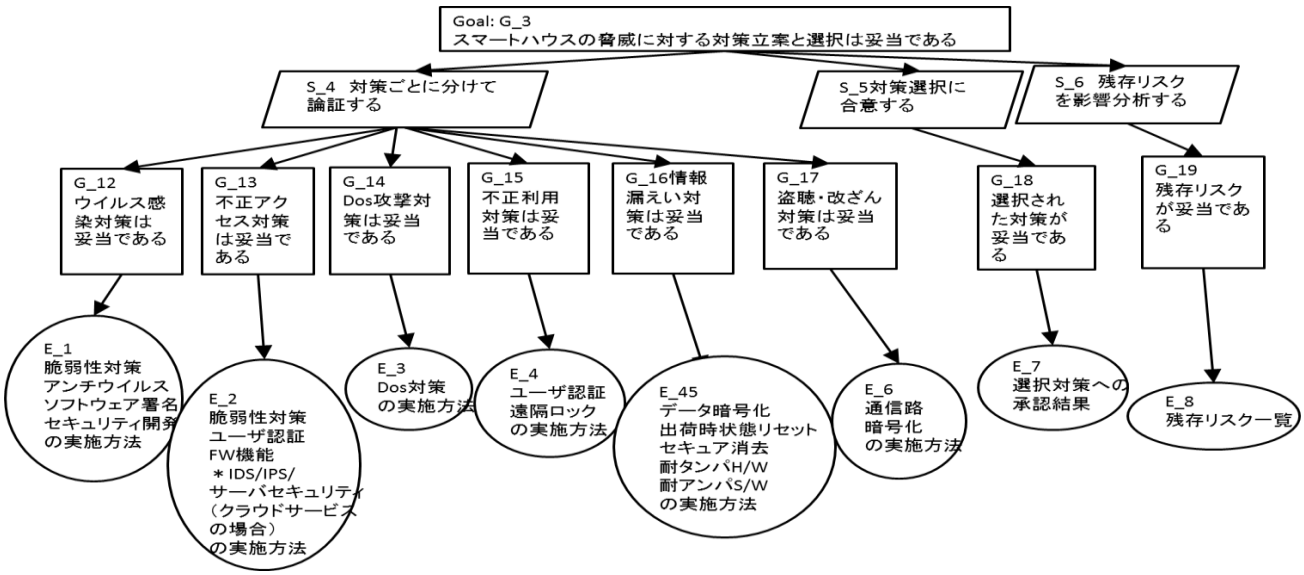

図 9.スマートハウス事例への CC-Case の適用例（対策立案と選択部分）

5. おわりに

本論文では，CC-Case を IoT セキュリティ要求分析に適用する方法を示し，CC-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 製品の要件可視化が簡便できる可能性があることとを示した．実際には IoT セキュリティ要件の可視化技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．本研究が現在のセキュリティ要件可視化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) 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).
35) 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
36) IPA，IoT 開発におけるセキュリティ設計の手引き,2016
37) 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