情報処理学会論文誌　コンシューマ・デバイス & システム　Vol.8　No.1　11–26 (Jan. 2018)

コンシューマ・サービス論文

セキュリティ要求分析・保証の統合手法CC-Caseの有効性評価実験

金子 朋子[1,a)]　髙橋 雄志[2]　勅使河原 可海[2]　吉岡 信和[3]　山本 修一郎[4]
大久保 隆夫[1]　田中 英彦[1]

受付日 2017年6月30日, 採録日 2017年10月31日

概要：筆者らが提案してきたCC-Caseは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自体が含んでいる要素の中でもライフサイクル全体を通じて用いられるアシュアランスケースは根幹をなすものである．CC-Caseのアシュアランスケースは単にGSNの表記方法ではなく，プロセスを論理モデルとして定義し，そのプロセスに則っていることを具体モデルによって提示する手法である．ただし，CC-Caseのアシュアランスケースがどの程度の有効性を持つのかははっきり示されていなかった．そこで，本論文では脅威分析のプロセスを論理モデル化したCC-Case，プロセス構造を持たないGSNと構造化されていない平文（自然言語表記）を比較する実験を実施した．実験の結果，CC-Caseの要件の可視化と妥当性確認における有効性を確認することができた．

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

Evaluation Practice for the Effectiveness of CC-Case as an Integrated Method of Security Requirement Analysis and Assurance

Tomoko Kaneko[1,a)]　Yuji Takahashi[2]　Yoshimi Teshigawara[2]　Nobukazu Yoshioka[3]
Shuichirou Yamamoto[4]　Takao Ookubo[1]　Hidehiko Tanaka[1]

Received: June 30, 2017, Accepted: October 31, 2017

Abstract: We have proposed CC-Case that is a security requirement analysis and assurance by using the Common Criteria (CC) and the assurance case. The assurance case is used by life-cycle in CC-Case. Therefore, it is main factor of CC-Case. The assurance case of CC-Case is not the description of GSN but the method which defines process as the logical model, and presents as the concrete model that conforms to the process. However, the effectiveness of CC-Case has not been shown. In this paper, we compared CC-Case which has logical model of threat analysis process, GSN, and non structured natural language representation by evaluating practice. We evaluated the effectiveness visualization and verification of requirements of CC-Case.

Keywords: common criteria, assurance case, security case, GSN, CC-Case

1. はじめに

情報セキュリティ上の攻撃は近年，より巧妙化している．現在の情報セキュリティ対策は発生したインシデントへの対応，運用管理の向上，セキュリティ方針の厳密化など運用など運用対処が中心であるが，「より巧妙化する脅威に対して，より効果的に対策をするにはどうしたらよいか？」という課題をかかえている．これに対し開発方法論からの対応がより根本的な対策になりうると筆者らは考えている．そこで筆者らは，コモンクライテリア [1], [2], [3] とアシュ

[1] 情報セキュリティ大学院大学
Institute of Information Security, Yokohama, Kanagawa 221–0835, Japan
[2] 東京電機大学
Tokyo Denki University, Adachi, Tokyo 120–8551, Japan
[3] 国立情報学研究所
National Institute of Informatics, Chiyoda, Tokyo 101–8430, Japan
[4] 名古屋大学
Nagoya University, Nagoya, Aichi 464–0814, Japan
[a)] dgs128101@iisec.ac.jp

アランスケース（ISO/IEC15026: Assurance Case）[4] を用い，セキュリティ仕様を顧客と合意のうえで決定する手法 CC-Case [5], [6] を提案している．コモンクライテリアとは，IT セキュリティ評価の国際標準 ISO/IEC15408 であり，CC と呼称される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．アシュアランスケースとは，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．なお，本論文でいう保証とは assurance を指す．つまり製品が品質基準に合致しているかを，設計・試作・製造・検査のすべての工程で確認する仕組みがあり，それを実行していることを保証する，請合う，自信を持っていうことである．

また CC-Case は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．セキュリティ要求分析とは，どのような脅威が想定されるかを洗い出し，各々の脅威に対して適切な対策方針を検討する要求分析プロセスであり，脅威を意図的に実現する手段である攻撃を考慮した分析である．なお，脅威分析はセキュリティ要求分析と同義だが，要求分析工程だけでなく設計工程で実施されるものも指すことが多い．

脅威分析手法，コモンクライテリアの機能要件の活用などの CC-Case 自体が含んでいる各種要素の中でもアシュアランスケース [4], [7] は根幹をなすものである．CC-Case のアシュアランスケースは単に一般的なゴール構造表記法で表記する表記方法ではなく，プロセスを論理モデルとして定義し，そのプロセスに則っていることを具体モデルによって提示する手法である．CC-Case のアシュアランスケースは工程ごとやライフサイクルにおいて繰り返し使用可能であり，変化し続ける要求への対応とその保証に役立てることができる．セキュリティ要求は新たな攻撃事象の発生にともない，その対応策が新たな要求事項となるため要求の変化が必須である．たとえば，新種の攻撃が発生し，分析対象とするシステムに新たなソフトウェアの脆弱性が見つかれば，それに対しての要求分析が必要になるのである．そして，その要求分析が確実に実施されていることをアシュアランスケースによって確認する仕組みを持つことで保証が可能となる．

ただし，CC-Case のアシュアランスケースがどの程度の有効性を持つのかははっきりしていなかった．そこで，脅威分析のプロセスを論理モデル化した CC-Case，アシュアランスケースの代表的な表記法である GSN [8] と自然言語表記（以下，平文）を比較する有効性評価実験を実施した．

本論文は 2 章で関連研究およびそれに関連した技術を紹介し，3 章は CC-Case とその特長を述べる．続く 4 章では CC-Case の有効性について実験を行い，5 章でその実験結果を示す．6 章では実験の設問ごとについて考察し，7 章で実験全体の結果をまとめ，8 章で今後の課題，9 章で今後の取り組みについて述べる．

2. 関連研究および技術

2.1 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．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，選択など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．本論文の提案手法である CC-Case はセキュリティ要求分析時にプロセスとして CC を利用する．

2.2 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証跡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．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 [7], [9] 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 [7]．アシュアランスケースは ISO/IEC15026 や OMG の ARM [10] と SAEM [11] 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 [8] 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 [12] 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 [13] もある．日本国内では GSN を拡張した D-CASE [14], [15] 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 [16]．本論文の提案手法である CC-Case はアシュアランスケースの代表的な表記方法である GSN を用いて表記するが，GSN にプロセス化の概念を付加し

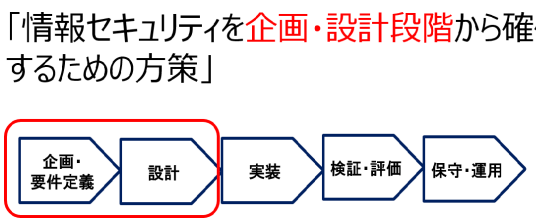


図 1　セキュリティ・バイ・デザインの定義
Fig. 1　Definition of security by design.

ている．

2.3　セキュリティケース

GSN を提唱した Kelly ら [17] 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 ら [18] 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 ら [19] 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 ら [20] 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持つことを検証している．セキュリティケースは特定の標準に基づいているわけではないが，本論文の提案手法である CC-Case [5] は IT セキュリティ評価基準（CC）に基づいてプロセス化されている [7]．

2.4　セキュリティ・バイ・デザイン

内閣府サイバーセキュリティセンター（NISC）によると「セキュリティ・バイ・デザイン」とは「情報セキュリティを企画・設計段階から確保するための方策」[21] であり，「安全な IoT システムのためのセキュリティに関する一般的枠組」[22] においては，目的としてまた基本原則として掲げられている重要な概念である [23]．IoT 時代を迎え，セキュリティ上の脅威が多大な被害を及ぼす可能性が出てきているため，企画・要件定義工程や設計工程というより早い段階から事前にセキュリティを作りこむことが求められているのである（**図 1**）．本論文の提案手法である CC-Case は事前にセキュリティ・バイ・デザインの概念に基づく手法の 1 つである．

3.　CC-Case とその特長

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 つの観点があるといわれている [24]．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．

表 1　GSN の構成要素
Table 1　Contents of GSN.

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

3.2　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であり，保証手法である [5], [6]．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と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 層構造を持つ．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．

3.3　CC-Case におけるアシュアランスケースの役割
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）を使用する．GSN の構成要素を**表 1** に示す．

CC-Case のアシュアランスケースは単に GSN で表記する表記方法ではなく，プロセスを論理モデルとして定義し，そのプロセスに則っていることを具体モデルによって提示する手法である．CC-Case のアシュアランスケースは各工程のプロセスを論理的に準形式化しうる．さらにソフトウェアの論理を可視化し，製品・システムの認証に必要な第 3 者による妥当性確認をしやすくする．

3.4　CC-Case の可視化の特長

平文や表記法としての GSN に比べ，プロセス定義をと

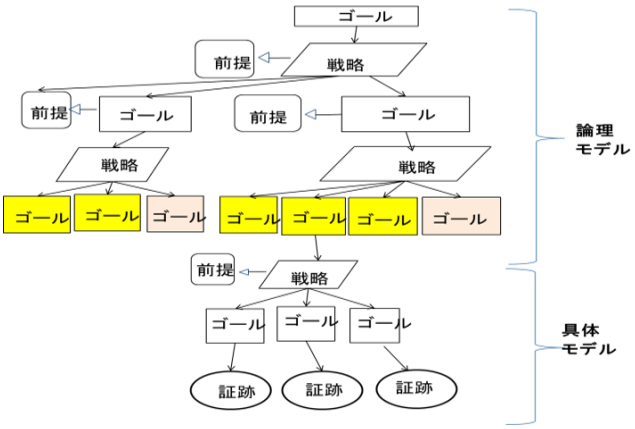


図 2　論理モデルと具体モデル
Fig. 2　Logical model and concrete model.

もなうアシュアランスケースである CC-Case は要件記述手法として有効性を持つ．3.4 節と 3.5 節ではその理論的特長について述べる．

CC-Case は 3 つの可視化（= 見える化）の特長を持つ．「1. 主張と証跡の見える化」,「2. 論理の見える化」,「3. 保証ストーリの見える化」である [25].

(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．**図 2** に示すように CC-Case 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．図 2 に示すように CC-Case 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り妥当性のある脅威の抽出を行い，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．なお，脅威の抽出と対策立案における保証は，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により生じている．

3.5　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」としての長所を持つ．

(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持つステークホルダ間で理解の壁をなくし，互いの持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．利用者が自社などのシステムにおいて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．

3.6　CC-Case の課題

CC-Case のアシュアランスケースは各工程のプロセスを論理的に準形式化しうる．さらにソフトウェアの論理を可視化し，製品・システムの認証に必要な第三者による妥当性確認をしやすくする．つまり CC-Case はプロセスの可視化，妥当性確認のしやすさを特徴として備えている．しかしながら，その特徴の有効性が評価されたことはなく，実用に際する効果が分からないため，普及展開にいたっていない．また，CC に特定の脅威分析の手法はないため，脅威などのセキュリティリスクの洗い出しには別な手法の組合せをしていくことも技術的な課題となっている．

4.　CC-Case の有効性評価実験

4.1　実験の概要

CC-Case の有効性主張のために観念的な論拠ではなく，実証と評価が必要である．そこで実験とアンケートを実施し，平文や表記法としての GSN に比べ，プロセス定義をと

もなうアシュアランスケースである CC-Case が要件記述手法として有効性を持つことを示すことにした．つまり，平文，GSN，CC-Case の 3 手法の比較とは，表記法を持たない平文，構造的な表記法であるが記述ルールは持たない GSN，記述ルールであるプロセスを GSN により構造的に表記する CC-Case の比較となる．

実験の目的はセキュリティ設計における CC-Case の可視化と妥当性確認の有効性評価であり，比較対象は脅威分析のプロセスを論理モデル化した CC-Case，表記法としての GSN とスマートハウスの図から起こした平文である．実験方法は CC-Case，GSN，平文による設計資料を用いた元の図の再構築であり，評価指標は平文資料と GSN 資料と CC-Case 資料を提示し，スマートハウスの図に対しどれを与えたほうが正解をだしたか（= 正解・正答率），誤りを発見し（= 誤り摘出率），変化するリスクに対応できたか（= リスク対応率）などである．

実験で利用したスマートハウスの図とは IoT セキュリティ設計の手引きで示されているスマートハウスの脅威と対策の検討例 [26] を実験用に一部修正ししたものである．Appendix にスマートハウスの図（**図 A·1**）とその正答および被験者に提示している資料（**図 A·2**，**図 A·3**）を掲載している．

セキュリティ要求は筆者らの業務経験からして単純に要求の羅列でありドキュメント化されないことが多い．そのため平文は章立てをしたり，箇条書きを使ったりするなどして，読みやすさを高めた工夫は特に実施しないものとした．資料（付録 A.2）は付録 A.1 のスマートハウスの図を単純に GSN や CC-Case の資料に書いてあることと同じ内容を構造化させずに文書化している．屋外，屋内の各機器別に脅威と対策を順番に記載している．

GSN は表記法であるため記述ルールがないと全体の構造化はできない．プロセスは記述ルールに相当し，CC-Case と GSN はプロセスベースであるかとどうかが異なる．そのため GSN は付録 A.3 に一部事例を示すように機器ごとの脅威や対策を独立した個々の GSN として作成している．個別の構造化はなされているが，全体での構造化はなされていない．

一方 CC-Case はプロセス構造を持っているため，全体の論理モデルとして構造化できる．脅威分析のプロセスを論理モデル化し CC-Case として記述した事例が，付録 A.4 である．脅威分析のプロセスは脅威の洗い出しと対策立案，選択した案と残存リスクへの対処の妥当性確認をするものである．付録 A.4 の CC-Case 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一連の脅威分析と対策立案の流れを第 1 階層のゴールと第 2 階層の戦略までで論理モデル化し，サブゴールの段階からスマートハウスの事例に特化した具体モデルを記載している．

図の再構成実験では，時間制限を設けた代わりに図の再構成に必要な要素数を明示しなかった．これは，所要時間による効率性を測るのではなく，解答の正しさを測ることを本実験の目的としたためである．

そして，被験者のシステム設計および GSN の理解度を考慮し実験前には事前講義も行った．また，図の再構成の実験に合わせて，資料に関するアンケート調査も行った．主要な技術である GSN の理解度の偏りがないように，事前講義の後に理解度のアンケートを行って担当する資料の割当てを行った．

被験者は，専門学校生から業務経験のある社会人博士課程の学生までの 45 名（全体を通しての未回答者 3 名を含む）である．実験のサンプリング数は 45 名と一般化に十分な数であったものの，そのうち 11 名の社会人博士課程の学生は実際の開発現場の技術者とギャップはないが，残りの大学生や専門学校生は，実際の開発現場の技術者とは経験値が異なることが想定される．本来「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と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」ことが定義されており [5]，開発現場の技術者とは経験値が異なる大学生や専門学校生が含まれていること自体は問題ではない．念のため「業務経験のある社会大学院生」と他の学生により実験結果に差があるかについて【設問 1】と【設問 2】の f 値について，両側，分散不一致として t 検定（5%）を行った結果，【設問 1】では有意差が見られたが，【設問 2】では有意差が見られなかった．この結果は作業慣れしている「業務経験のある社会大学院生」は【設問 1】からスムーズに回答できたが，作業慣れしていない他の学生は【設問 2】の段階になって理解が追い付いてくるケースが多かったからと推定される．同様な実験を繰り返せば，作業慣れしていない他の学生も「業務経験のある社会大学院生」と変わらないパフォーマンスを発揮するはずであり，被験者の選定は妥当であると考えられる．

4.2　実験手順

手順 (1)　事前講義およびグループ分け

事前講義では，背景となるセキュリティ・バイ・デザイン，CC-case の中心技術となる CC，GSN，アシュアランスケース，CC-Case そのものに関する内容を 30 分程度の時間で講義を行った．講義終了後，担当資料を決めるため以下の設問で理解度調査を行った．【事前設問 1】の GSN の理解度が分散するように担当する資料を決めている．

【事前設問 1】GSN の理解度
① 講義前に GSN を知っており，自分で GSN を書いたことがある．
② 講義前に GSN を知っていたが，自分で GSN を書いたことはない．

表 2　実験の区分・資料・観点
Table 2　Experiment classification/material/perspective.

【設問】	区分	資料	観点
1	実験	自分の与えられた担当資料（1 種類）	正解・正答率
2	実験		誤り摘出率
3	実験		リスク対応率
4	アンケート		可視化
5	アンケート		妥当性確認
6	アンケート	3 つの資料	可視化
7	アンケート		妥当性確認

③ 講義前には GSN を知らなかったが，講義を聞いてある程度 GSN を理解できた．
④ 講義前には GSN を知らず，講義を聞いてもほとんど GSN を理解できなかった．

【事前設問 2】ソフトウェア設計経験の確認
① ソフトウェア設計経験がある．
② ソフトウェア設計経験がない．

【事前設問 3】リスク分析経験の確認
① リスク分析を実施したことがある．
② リスク分析を実施したことがない．

手順 (2)　担当資料の読み込み

以降の作業に制限時間を設けたため，実作業に入る前に，資料の内容確認の時間を設けた．被験者は，担当資料のみを受け取り資料に書かれた内容の確認を 10 分程度の時間行ってもらった．

手順 (3)　スマートハウスの図の再現

配布資料を作成するために使用したスマートハウスの図 [21] を加工し，【1】リスクや対応策を削除したり，【2】記述内容を誤ったものに書き換えたりしたものを解答用紙として配布し，図を正す作業を行った．また，配布資料では【3】機器の追加も加えた資料もあり，追加の機器の設定も行ってもらった．上記の【1】，【2】，【3】に対応する 3 つの設問に分け，それぞれの制限時間を 8 分とし所要時間の申告もしてもらった．【設問 1】では 6 カ所，【設問 2】では 5 カ所のエラーが含まれている．ただし，先の設問に対する回答が完了している場合には，次の設問に進み回答を始めることを可とした．

本実験【設問 1】から【設問 3】と【設問 4】から【設問 7】は性質の異なる設問であるため，その違いを説明する．**表 2** に【設問 1】から【設問 3】は 3 つの異なる資料（平文資料と GSN 資料と CC-Case 資料）によるパフォーマンスを比較する実験である．つまり 3 つの異なる資料を提示し，スマートハウスの図に対し，【設問 1】はどれを与えたほうが正解をだしたか（= 正解・正答率），【設問 2】は誤りを発見したか（= 誤り摘出率），【設問 3】は変化するリスクに対応できたか（= リスク対応率）を比較する実験となっている．これに対して【設問 4】から【設問 7】はアンケートによる被験者の評価結果である．つまり【設問 4】，【設問 5】は自分が与えられていた資料に対する被験者の評価結果であり，【設問 6】，【設問 7】は 3 つの資料を見比べたうえでの有効性の高いものを選ぶ各人の評価結果である．また，【設問 4】，【設問 6】は可視化，【設問 5】，【設問 7】は妥当性確認の観点からの被験者の評価となっている．

スマートハウスの図に対し設問は以下のとおりである．

【設問 1】
スマートハウスの図では，記述が不足しています．与えられた資料に基づき追加すべき記述をスマートハウスの図に記入し，すべて指摘してください．

【設問 2】
スマートハウスの図に記載されている対策で，与えられた資料とは異なる内容が記載されている個所があります．すべて指摘してください．記入は直接，スマートハウスの図を訂正してください．

【設問 3】
スマートハウスの図のリスクが変化しました．どこに何が追加され，どんな脅威と対策がもつのかを，与えられた資料をもとに，スマートハウスの図に記入して指摘してください．（絵で記入しなくても言葉による記入で可とします．）

手順 (4)　配布資料に関するアンケート

手順 (3) で使用した資料に関して以下の設問でアンケート調査を行った．設問は以下のとおりである．

【設問 4】
与えられた資料は分析しやすいですか？
（⑤ 分析しやすい・④ やや分析しやすい・③ どちらともいえない・② やや分析しづらい・① 分析しづらい）

【設問 5】
与えられた資料は理解しやすいですか？
（⑤ 理解しやすい・④ やや理解しやすい・③ どちらともいえない・② やや理解しづらい・① 理解しづらい）

手順 (5)　資料の比較アンケート

手順 (3) で使わなかった資料を配布し，見比べてもらい有効性についてのアンケート調査を行った．それぞれの設問ではフリーアンサによるコメントも収集した．設問は以下のとおりである．

【設問 6】
以下の 3 種類の資料を見比べて可視化の観点より，一番有効であると思われるものに○をし，理由を記載してください．
（平文・GSN・CC-Case・わからない）

【設問 7】
以下の 3 種類の資料を見比べて第三者による妥当性確認の観点より，一番有効であると思われるものに○をし，

理由を記載してください．
（平文・GSN・CC-Case・わからない）

5.　実験結果

本実験では設問ごとに，未回答者および作業をともなう実験の回答時間に制限時間より大幅に長い時間を示すなど明らかに異常がみられる場合は該当設問に対して無効回答とし母数に加えなかった．

5.1　手順 (1)

担当資料分けのための【事前設問 1】では，約半数の被験者が ③（22 名）となり，一部 ①（2 名）②（1 名）の経験者がいて，残りは ④（16 名）で理解が追い付かないという結果となった．残り 4 名は未回答または解答用紙の回収ができなかったため確認ができなかった．ただし，担当資料分けの際は挙手で確認を行い，割り振りをしたので担当資料ごとの理解度には偏りがないものと考える．

5.2　手順 (3)

以下の【設問 1】および【設問 2】では両方とも未回答である被験者と，回答時間が制限時間を超えていたり，あまりに短かったりという異常が見られる被験者（11 名）を分析対象から除外した．

なお，正解となる指摘内容の数を a，被験者が回答した回答数を b，そのうち正解の数を c として，c/a で正答率を，c/b で正解率を求めた．また，正答率と正解率の調和平均として f 値を $(2 \times c)/(a+b)$ で求めた．

【設問 1】

【設問 1】における担当資料ごとの平均値と標準偏差は**表 3** の示すとおりである．表 3 は平文，GSN，CC-Case を比較し，正答率，正解率，f 値（正答率と正解率の平均）において赤字が最も高いことを示している．いずれも CC-Case である．また平均が最も高いところを赤字とし，標準偏差が最も低いところは青字とした．平均が高く，標準偏差が低いのは CC-Case である．ばらつきが少ないことは個人差に影響されずに正答，正解を出していることを示す．

また，各被験者の値を x 軸を正答率，y 軸を正解率，z 軸（バブルのサイズ）を f 値としたバブルチャートを**図 3** に示す．図 3 で上に行くほど正解率は高く，右に行くほど正答率は高くなる．平文は青，GSN はオレンジ色，CC-Case は銀色の球で示される．大きさは f 値を示し，大きいほど良好である．なお，図 3，図 4 はバブルチャートで記述したため，同一スコア，同一グループの人は重なりにより単一に見え，また 0 点の人は表記されていない．

表 3　【設問 1】担当資料ごとの平均値と標準偏差
Table 3　【Q1】The average and standard deviation.

	正答率(x軸) c/a			正解率(y軸) c/b			f値(z軸) 2×c/(a+b)		
	平文	GSN	CC-Case	平文	GSN	CC-Case	平文	GSN	CC-Case
平均	0.467	0.439	0.667	0.777	0.576	0.805	0.558	0.481	0.717
標準偏差	0.281	0.310	0.157	0.305	0.320	0.152	0.253	0.292	0.110

【設問 2】

【設問 2】における担当資料ごとの平均値と標準偏差は**表 4** に示すとおりである．設問 1 と同様に赤字が平均が最も高いもの，青字が標準偏差が最も小さいものを示す．

また各被験者の値を【設問 1】と同様にバブルチャートを**図 4** に示す．【設問 1】と同様に色と球の大きさで表現している．

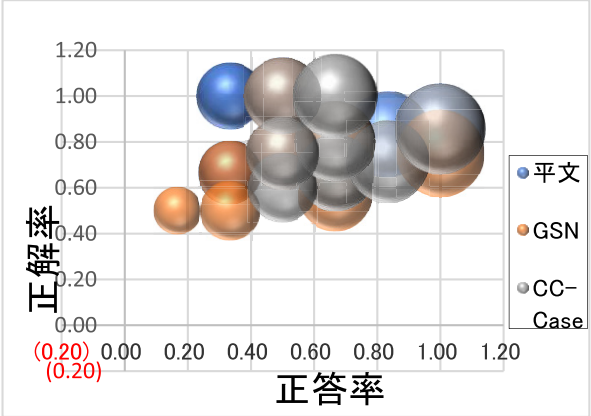


図 3　【設問 1】における各被験者の値
Fig. 3　【Q1】The value of each subject.

表 4　【設問 2】担当資料ごとの平均値と標準偏差
Table 4　【Q2】The average and standard deviation.

	正答率(x軸) c/a			正解率(y軸) c/b			f値(z軸) 2×c/(a+b)		
	平文	GSN	CC-Case	平文	GSN	CC-Case	平文	GSN	CC-Case
平均	0.460	0.418	0.717	0.745	0.703	0.643	0.544	0.513	0.537
標準偏差	0.272	0.204	0.326	0.317	0.358	0.374	0.273	0.170	0.328

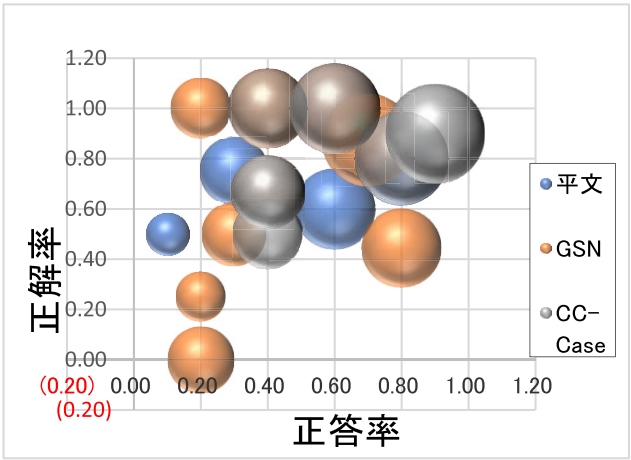


図 4　【設問 2】における各被験者の値
Fig. 4　【Q2】The value of each subject.

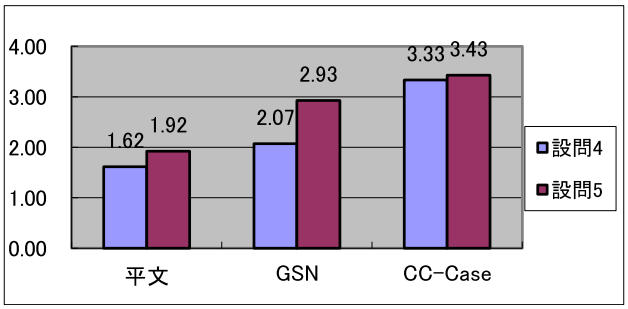


図 5　【設問 4，5】資料の分析しやすさと理解しやすさ
Fig. 5　【Q4, 5】Ease of document analysis and understandability.

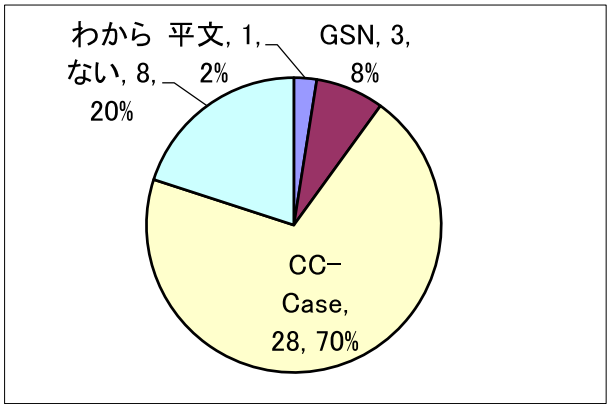


図 6　【設問 6】可視化の観点からの有効性
Fig. 6　【Q6】Effectiveness from the viewpoint of visualization.

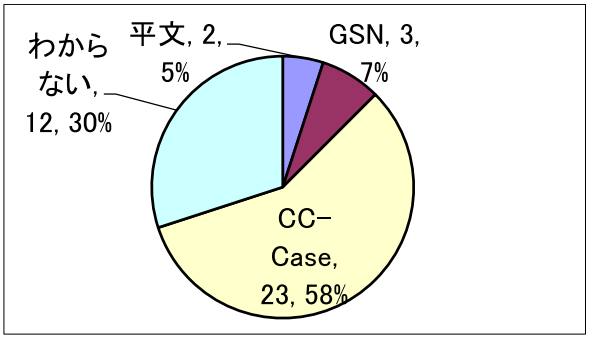


図 7　【設問 7】妥当性確認の観点からの有効性
Fig. 7　【Q7】Effectiveness from the viewpoint of validation.

【設問 3】
リスクの変化を追加できたかどうかで判断しようとしたが，有効な値を得られていない．バラツキは個人差によるものと考えられる

5.3　手順 (4)

担当資料ごとのアンケート結果を選択肢の番号をそのままスコアとしてその平均を図 **5** のグラフに示す．資料の分析しやすさと理解しやすさとも CC-Case が最も高く，GSN，平文の順となる．

5.4　手順 5

【設問 6，7】における回答の実数と割合を図 **6**，図 **7** に示す．可視化の観点からも妥当性確認の観点からも有効性は CC-Case が最も高く，GSN，平文の順となる．

CC-Case が【設問 6】【設問 7】は 3 つの資料を見比べたうえでの有効性の高いものを選ぶ各人の評価結果であるため，より客観的な評価になっていると考えられる（両設問に 5 名の無回答あり）．

フリーアンサの回答では，局所的な確認において GSN が有効であるという意見や，事例によっては平文で十分であるという意見もあったが，全体的に視覚的な効果で CC-Case が優れているという意見が多かった．

6.　実験の考察

今回の実験およびアンケートを行うことで，「GSN，平文と比較し CC-Case は，可視化と妥当性確認の観点から有効性を持つ」ことを確認できた．設問ごとの考察を以下に示す．

【設問 1】
CC-Case は，測定したすべての値で優位性が見て取ることができた．また，標準偏差も低いことから安定して回答することができていることを見て取ることができる．

GSN は，最も低い値を示すこととなった．個別の機器の設定が書かれていたため制限時間内では，解答用紙と資料を照らし合わせて該当箇所を見つけることができなかったものと推察される．そのため設計の経験や GSN の理解度などで結果が変わる可能性があると推察される．

平文は，比較的高い数値を示しているが標準偏差が高く，個人差が大きく出る結果となった．正解率が高いことからきちんと文章が読めれば正解を導けているので文章解読能力に依存する結果になると推察される．しかし，正答率が低いので読み違いにより誤った脅威や対策を選んでしまっていると推察される．

【設問 2】
全体的に標準偏差が高く，個人差が大きく出る結果となった．

CC-Case は，正答率で優位性を見て取ることができた．正答率が高いことから指摘個所を見つけることができれば，正確に訂正することができている．しかし，すべてを見つけるためには個々人の能力によると推察される．

GSN は，優位性がみられなかったが標準偏差が比較的低く，誤り訂正では安定した結果を得られている．これは個々の機器に対する記述に分かれているため確認箇所の選別が容易であったと推察される．

平文は，正解率，f 値で優位性を見て取ることができた．文章を追って順次確認していく作業から異なる個所の見落としが少なく多くの指摘個所が発見できたものと推察される．しかし，文章の読み違いなどにより，誤った訂正が行

われることがあり正答率が下がっている．正解率が特に高いためf値もCC-Caseを上回る結果となった．

ただし，所要時間の観点ではCC-Caseが手早く作業を終えているため，制限時間を決めずに作業時間を評価軸にした場合は結果が変わる可能性がある．

【設問3】

特徴的な点が見いだせず，十分な評価ができないため，今回は分析を見送ることになった．

【設問4】

分析の容易さとしては，CC-Caseが高いスコアを示している．次いでGSNのスコアが高い．図示されているが図が多くまとまっていない印象があったためと推察される．最も低いスコアの平文は，文章量が多く確認するだけでも困難であったり，全体像を文だけで把握することも困難であったりするために低いスコアとなったと推察される．

【設問5】

理解度としては，こちらもCC-Caseが最も高いスコアを示した．全体像を見せているために理解も容易であったと推察される．次いでGSNも高いスコアを示したが，こちらも図示されていることがポイントであったと推察される．しかし，図が理解できていても【設問1〜3】の結果より，必ずしも正しい理解につながっていなかったと思われる．最もスコアの低い平文は，理解できているか自信を持てなかったものと推察される．そのため，【設問1】からの作業にあたり細かく資料を再点検しながら取り組んでいると推察され，高い成果につながっていると推察される．

そのため，【設問4，5】の考察より，文章は時間をかければ理解が上がり，図解は見た目の印象で理解度が上がるものと推察される．

【設問6】

可視化の観点では，CC-Caseが最も高い評価を受けた．フリーアンサでも多くの回答で全体像に関する話が触れられているため，全体像を示すことが可視化の評価につながっていると推察される．また，他の資料を選択した被験者の中にはCC-Caseほど細かく示さなくてもGSNや平文で事足りるという意見もありCC-Caseを評価したうえでの判断であり，CC-Case自体は十分な評価を得たと推察される．他にCC-Caseを選ばなかった理由としてCC-CaseとGSNの違いが分からないというものや，新しいものを理解しないと分からないのは違うと思うというものもあった．手法の理解が進むことでさらに優位性が高まるものと推察される．

【設問7】

妥当性の観点では，CC-Caseが最も高い評価を受けた．フリーアンサも【設問6】とほぼ同じ傾向であったが，局所的な妥当性において，平文やGSNの方が優れているのではないかという意見もあった．CC-Caseでも注力するポイントを分かりやすくする工夫などをすればより高い評価を受けることができるものと推察される．

7. 実験のまとめ

実験の結果を全体として考察すると，CC-Caseはアンケート【設問4，7】ではすべての設問で3種類中第1位であった．演習実験【設問1，2】でも正答率では3種類中第1位となり，全般的に高い評価を受けたといえる．GSNと違いがでるのが不明であったが，プロセスベースで形式化を図ったCC-Caseの方が有用であるとの評価になった．アンケート結果では，CC-Caseが良いと記述した理由には「平文と比較して多量の文章を読まなくてよい．GSNと比較して多量のツリー図を見なくてよく全体を見通しやすい」，「脅威や対策が見やすい」，「問題と解決がまとめて横並びにされていて見やすい」など，全体感にたったときに，可視化がしやすいことに評価が高かった．また，「エビデンスとの対応が分かりやすく見やすいと思いました」，「コンパクトにまとまっているCC-Caseが見やすいし，図の形さえ分かれば，理解できるため有効そうだと思った」など妥当性の評価にも期待が寄せられた．

また，「分からない」を選択した以外の人を対象にすると，【設問6】か【設問7】のどちらかには全員がCC-Caseを選択していたことから，手法として理解ができ慣れれば，直観的に理解しやすいため，普及しやすい手法になると推察される．

演習実験に相当する【設問1〜3】で，平文とCC-Caseが競い合う形になったことより，理解度の低いユーザであればGSNよりもCC-Caseの方に優位性があることが推察される．時間をかければ理解度に関係なく分かる平文よりも優位となるような，さらなる工夫があればよいと考える．そのことはアンケート結果からも見て取れる．

ただしCC-Caseは普及・理解の度合いがまだまだ足りていないため，理解度が深まればより高い評価にたどり着くであろうという印象を受けた．導入に関する容易さ，理解度向上のための仕組みなどを工夫することにより改善ができるものと考える．

8. 今後の課題

8.1 本実験でのCC-Caseの限界と課題

3.6節に述べたように，CC-Caseのアシュアランスケースはプロセスの可視化，妥当性確認のしやすさを特徴として備えているが，その特徴の有効性が評価されたことはなく，実用に際する効果が分からないため，普及展開にいたっていない．しかしながら，本実験を実施したことによりプロセスの可視化と妥当性確認のしやすさについて，平文やGSNと比較し，有効性を持つといえる結果を得ることができた．

この実験でのCC-Caseの限界としては，【設問3】のリスクへの対応性に関して有効な値を得られていないことである．この課題の克服のため，今後は有効性評価を適切に実施することが必要であり，特徴性を把握できる観点からの分析を試行していきたい．

8.2　CC-Case の技術的課題

CC-Case のアシュアランスケースには，以下の技術的課題と運用展開の課題がある．技術的課題とは CC-Case のライフサイクルでの適用と他要素との統合的推進である．

(1) ライフサイクルでの適用

本実験では，セキュリティ要求分析のプロセスのみの可視化したが，今後は CC-Case のライフサイクルでの具体的プロセス化 [6] を進め，各工程のプロセスを論理的に準形式化していくことが必要である．

(2) 脅威分析手法との統合を具体的に提示

CC に特定の脅威分析の手法はないため，脅威などのセキュリティリスクの洗い出しには他の手法の組合せ [27], [28] をしていくことも技術的な課題となっている．

(3) 認証手法の統合を具体的に定義

さらにソフトウェアの論理を可視化し，製品・システムの認証に必要な第三者による妥当性確認をしやすくする特長を CC-Case は持っている．CC-Case は他の構成要素として CC の PP 活用 [5], [29] を含んでいる．この PP 活用とアシュアランスケースを組み合わせて妥当性確認ができることを提示しているが，具体的な実施手法として提示することが必要である．将来的には製品・システムの第三者確認ができる認証手法として完成させることを目指していきたい．

8.3　CC-Case の運用展開の課題

本実験で CC-Case はプロセスの可視化，妥当性確認のしやすさの有効性は評価できたが，実用に際する効果を明確化し，普及展開をしやすい工夫を施していく必要がある．

(1) 実用しやすい工夫

3.5 節に示したように CC-Case は使い方の観点で長所を持っているが，この具体的展開をしやすくするため表形式と図形式の連動などを含めたツール化の推進が望まれる．

(2) IoT への展開とセーフティとの統合

アシュアランスケースは本来セーフティ手法であるが，筆者らは CC-Case としてアシュアランスケースをセキュリティに適用してきた．「安全な IoT システムのためのセキュリティに関する一般的枠組」[22] において，「IoT（Internet of Things）システムについては，モノが接続されることから，IT と物理的システムが融合したシステムとしてとらえる必要があり，同システムが提供するサービスには，従来の情報セキュリティの確保に加え，新たに安全確保が重要となる」と規定されている．つまり IoT 時代には安全性も含めた情報セキュリティの対策が求められており，CC-Case をセーフティとセキュリティを統合する手法 [23] に拡張していくことも今後の課題である．

9.　おわりに

本論文では CC-Case のアシュアランスケースについて，その有効性を評価した．実験において CC-Case の利点として複雑で分かりにくい事象に対して，理解しやすさを理由にあげる人が多数みられた．この実験結果より CC-Case は複雑でより多くの脅威の洗い出しと確実な事前対処が望まれる事象に用いることに適していると想定される．そこで IoT セキュリティのような複雑な事象に適用するなど特性をいかして CC-Case のアシュアランスケースの本格的な適用をはかっていきたい．

CC-Case は 8 章で提示した今後の課題を解決したうえで，最終的には IoT 時代に求められる製品とシステムの安全・安心を実現できる統合開発方法論を目指している．その具体的内容は可視化 [30] と認証 [31]，セーフティとセキュリティの統合 [23] などである．

さらに今後の取り組みとしては，現状はコンセプトレベルに筆者らがとどめている統合開発方法論に対して，必要となる各技術・手法を 1 つずつ創生し，検証評価のうえ，確立していくことを考えている．そのうえで CC-Case 自体の理解を深める普及展開を実施し，実用化を目指していく所存である．

謝辞　CC-Case の有効性評価実験の実施にあたり多大なご協力をいただいた，東京電機大学未来科学部佐々木良一教授と学生の皆様，情報科学専門学校の武藤幸一教諭と学生の皆様，情報セキュリティ大学院生の皆様に，謹んで感謝の意を表する．

参考文献

[1] Common Criteria for Information Technology Security Evaluation, available from ⟨http://www.commoncriteriaportal.org/cc/⟩.
[2] セキュリティ評価基準（CC/CEM），入手先 ⟨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 (July 2007).
[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，Vol.55, No.9 (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*, Vol.3, No.1, pp.49–62, Society of Digital Information and Wireless Communications (ISSN:2305-0012) (2014).
[7] IPA：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] Kelly, T. and Weaver, R.: The Goal Structuring Notation — A Safety Argument Notation, *Proc. Dependable Systems and Networks 2004 Workshop on Assurance Cases* (July 2004).
[9] Kelly, T.P. and McDermid, J.A.: Safety Case Construction and Reuse using Patterns, *Proc. 16th International Conference on Computer Safety, Reliability and Security* (*SAFECOMP'97*), Springer-Verlag (Sep. 1997).
[10] OMG, ARM, available from ⟨http://www.omg.org/spec/ARM/1.0/Beta1/⟩.
[11] Inge, J.R.: The Safety Case, its Development and Use

in the United Kingdom, *Proc. ISSC25*, OMG, SAEM (2007). available from ⟨http://safety.inge.org.uk/20070625-Inge2007_The_Safety_Case-U.pdf⟩
[12] Toulmin, S.E.: *The Uses of Argument*, Cambridge University Press (1958).
[13] The Adelard Safety Case Development (ASCAD), Safety Case Structuring: Claims, Arguments and Evdence, available from ⟨http://www.adelard.com/services/SafetyCaseStructuring/index.html⟩.
[14] DEOS プロジェクト，入手先 ⟨http://www.crest-os.jst.go.jp⟩.
[15] 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 (March 2014).
[16] 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).
[17] Alexander, R., Hawkins, R. and Kelly, T.: 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).
[18] Goodenough, J., Lipson, H. and Weinstock, C.: Arguing Security - Creating Security Assurance Cases (2007). available from ⟨https://buildsecurityin.us-cert.gov/bsi/articles/knowledge/assurance/643-BSI.html⟩.
[19] Lipson, H. and Weinstock, C.: Evidence of Assurance: Laying the Foundation for a Credible Security Case (2008). available from ⟨https://buildsecurityin.us-cert.gov/bsi/articles/knowledge/assurance/973-BSI.html⟩.
[20] Ankrum, T.S. and Kromholz, A.H.: Structured Assurance Cases: Three Common Standards, *Proc. 9th IEEE International Symposium on High-Assurance Systems Engineering* (*HASE'05*) (2005).
[21] NISC：available from ⟨ww.nisc.go.jp/conference/seisaku/dai15/pdf/15siryou02.pdf⟩.
[22] NISC：安全な IoT システムのためのセキュリティに関する一般的枠組.
[23] 金子朋子：セキュリティ・バイ・デザインとアシュアランスケース，入手先 ⟨www.ipa.go.jp/files/000055734.pdf⟩ (2016).
[24] 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).
[25] 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).
[26] 独立行政法人情報処理推進機構：IoT 開発におけるセキュリティ設計の手引き (2016).
[27] 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，Vol.52, No.9 (2011).
[28] IPA：はじめての STAMP/STPA（実践編)—システム思考に基づく新しい安全性解析手法，IPA (2017).
[29] 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，Vol.6, No.1 (Jan. 2015).
[30] 金子朋子，髙橋雄志，勅使河原可海，田中英彦：CC-Case を用いた IoT セキュリティ要件の可視化，第 14 回 CDS 研究発表会 (2016).
[31] 金子朋子, 髙橋雄志, 勅使河原可海, 田中英彦：CC-Case を用いた IoT セキュリティ認証方法の提案，第 72 回 CSEC 研究発表会 (2016).

付　　録

A.1　提示資料

本来のスマートハウスの図（図 **A·1**）[26] とその正答および被験者に提示している【設問 1】～【設問 3】の提示資料を以下に掲載する.

A.1.1　スマートハウス

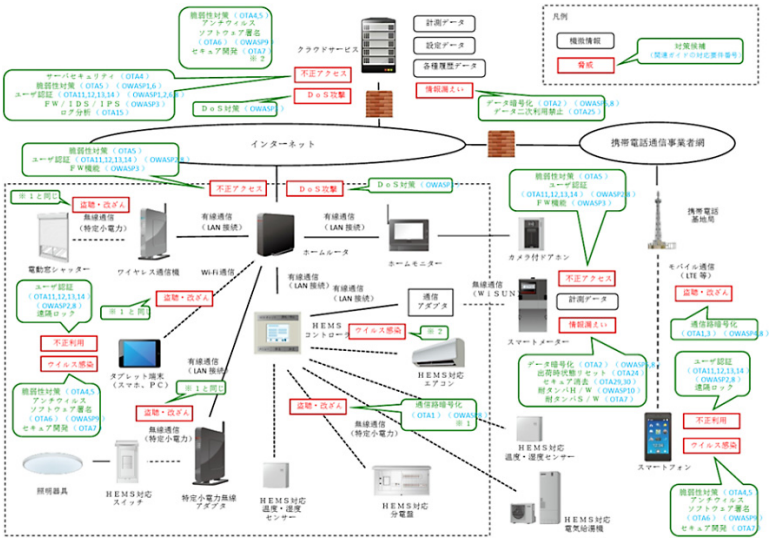


図 **A·1**　スマートハウスの脅威と対策の検討例 [21]

Fig. A·1　Example of Threats and countermeasures to the smart house.

A.1.2 ［設問 1］

【設問 1】以下の 5 項目が白消しになっている（オレンジで表記）

左上　ユーザ認証，遠隔ロック，左下　不正利用，中上　不正アクセス，中下　情報漏えい，右　　盗聴・改ざん

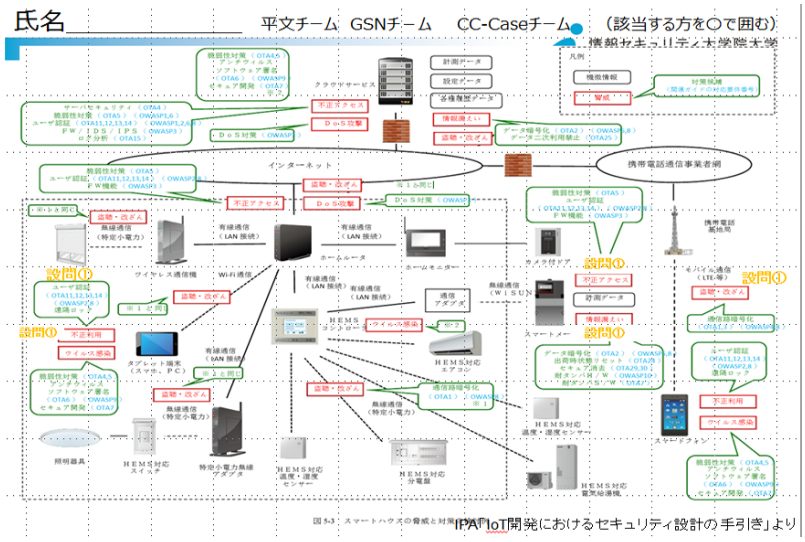


図 A·2　【設問 1】の正答

Fig. A·2　The answer of【Q1】.

A.1.3 ［設問 2］

【設問 2】以下の 5 項目が違う内容を上書きされている（青字と○囲み）左から順に示す

正　DOS 攻撃　誤　盗聴・改ざん　正　DOS 対策　誤　*1　　に同じ　正　何もない　誤　盗聴・改ざんが書かれている

正　遠隔ロック　誤　*1　　に同じ　　正　不正利用　誤　　盗聴・改ざん

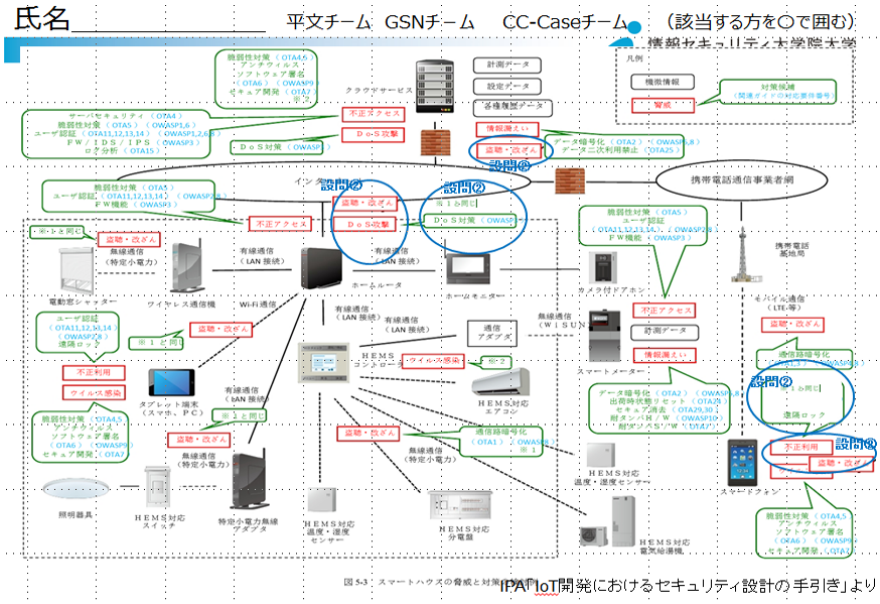


図 A·3　【設問 2】の正答

Fig. A·3　The answer of【Q2】.

A.1.4 ［設問 3］

【設問 3】以下が記入されていれば○

・監視カメラの追加　　個人情報の流出（画像）の脅威　　認証設定厳格化　の対策

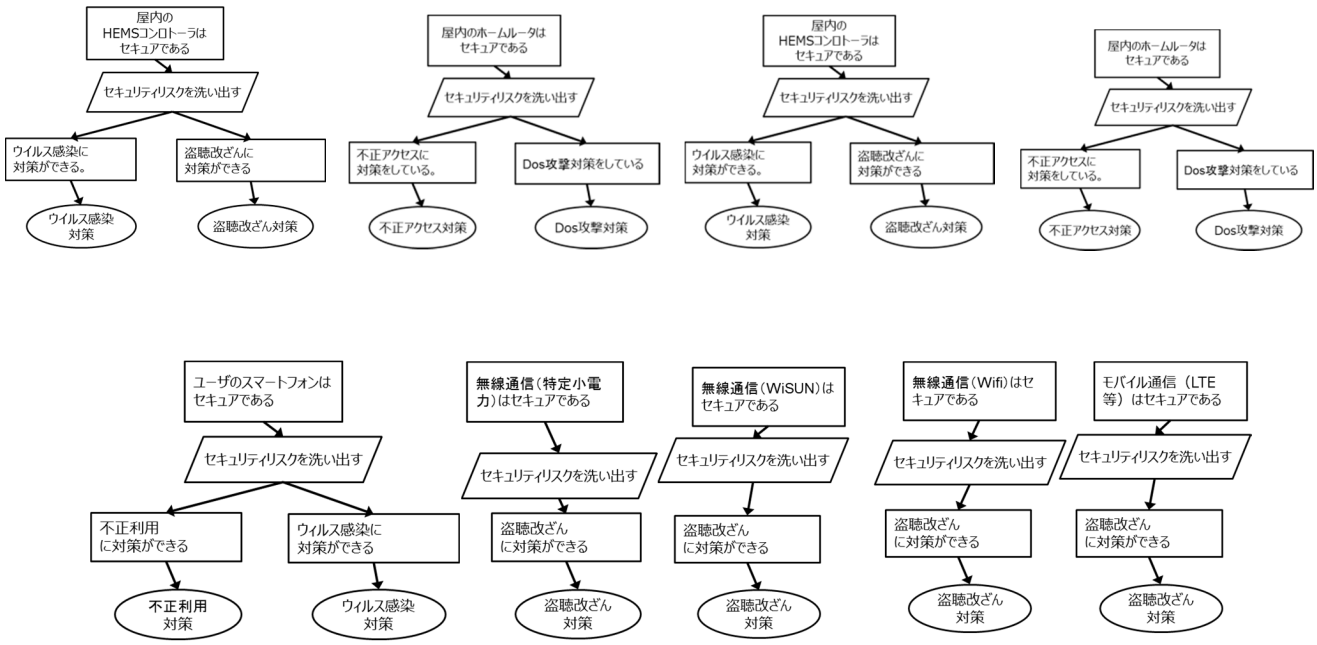
A.2　平文の事例

【平文 2】
スマートハウスの屋外にはスマートメーター、ＨＥＭＳ対応 電気給湯機、ＨＥＭＳ対応 温度・湿度 センサー、カメラ付ドアホンがある。屋外には監視カメラが追加され、ホームモニターから有線通信（LAN 接続）で設置された。
スマートメーターには不正アクセスや情報漏えいの脅威が想定される。
スマートメーターの不正アクセスの脅威に対して、脆弱性対策、ユーザ認証、ＦＷ機能が対策として挙げられる。
スマートメーターの情報漏えいの脅威に対して、データ暗号化、出荷時状態リセット、セキュア消去、耐タンパ H/W、耐タンパ S/W が対策として挙げられる。
スマートフォンにはウイルス感染、不正利用の脅威が想定される。
スマートフォンの不正利用にはユーザ認証、遠隔ロックが対策として考えられる。
スマートフォンのウイルス感染には脆弱性対策、アンチウィルス、ソフトウェア署名、セキュア開発が対策として挙げられる。
スマートハウスの屋外ではスマートフォン・ 基地局間の無線通信が可能である。
スマートフォン・ 基地局間のモバイル通信 （LTE 等）において、盗聴・改ざんなどの脅威が想定される。
基地局間のモバイル通信 （LTE 等）の盗聴・改ざんに関しては通信路暗号化が対策として挙げられる。
スマートハウスの屋内にはホームルータ、ＨＥＭＳ コントローラ、ＨＥＭＳ対応 温度・湿度 センサー、タブレット端末 （スマホ、ＰＣ）がある。
ＨＥＭＳ コントローラは通信 アダプタと有線通信 （LAN 接続）されている。
ＨＥＭＳ コントローラはウイルス感染の脅威が想定される。
ＨＥＭＳ コントローラはウイルス感染の脅威に対して、脆弱性対策、アンチウィルス ソフトウェア署名、セキュア開発が対策として挙げられる。
ホームルータには、不正アクセス、ＤｏＳ攻撃の脅威が想定される。
ホームルータの不正アクセスには脆弱性対策、ユーザ認証、ＦＷ機能の対策がある。
ホームルータのＤｏＳ攻撃にはＤｏＳ対策が対策として挙げられる。
スマートハウスの屋内には無線通信 （特定小電力）でホームルータと特定小電力無線アダプタが接続されている。
ホームルータと特定小電力無線アダプタ間の無線通信 （特定小電力）には盗聴・改ざんの脅威が想定される。
ホームルータと特定小電力無線アダプタ間の無線通信 （特定小電力）における盗聴・改ざんの脅威に対して、通信路暗号化が対策として挙げられる。
スマートハウスの屋内には無線通信 （Wi-Fi 通信）でホームルータとタブレット端末 （スマホ、ＰＣ）が接続されている。
ホームルータとタブレット端末 （スマホ、ＰＣ）間の無線通信 （Wi-Fi 通信）には盗聴・改ざんの脅威が想定される。
ホームルータとタブレット端末 （スマホ、ＰＣ）間の無線通信 （Wi-Fi 通信）における盗聴・改ざんの脅威に対して、通信路暗号化が対策として挙げられる。
無線通信 （ＷｉＳＵＮ）でスマートハウスの屋内の通信アダプタとスマートハウスの屋外のスマートメーターが接続されている。
スマートハウスの屋内の通信アダプタとスマートハウスの屋外のスマートメーターの間の無線通信 （ＷｉＳＵＮ）には盗聴・改ざんの脅威が想定される。
スマートハウスの屋内の通信アダプタとスマートハウスの屋外のスマートメーターの間の無線通信 （ＷｉＳＵＮ）における盗聴・改ざんの脅威に対して、通信路暗号化が対策として挙げられる。
スマートハウスの屋内のタブレット端末 （スマホ、ＰＣ）には不正利用、ウイルス感染の脅威が想定される。
スマートハウスの屋内のタブレット端末 （スマホ、ＰＣ）に対する不正利用の脅威に対して、ユーザ認証、遠隔ロックが対策として挙げられる。
スマートハウスの屋内のタブレット端末 （スマホ、ＰＣ）に対するウイルス感染の脅威に対して、脆弱性対策、アンチウィルス、ソフトウェア署名、セキュア開発が対策として挙げられる。
クラウドサービスには、不正アクセス、DoS 攻撃、情報漏えいの脅威が想定される。
クラウドサービスの不正アクセスの脅威に対して、脆弱性対策、ユーザ認証、FW／IDS／IP、ログ分析、サーバセキュリティが対策として挙げられる。
クラウドサービスの DoS 攻撃の脅威に対して、ＤｏＳ対策が対策として挙げられる。
クラウドサービスの情報漏えいの脅威に対して、データ暗号化、データ二次利用禁止が対策として挙げられる。
監視カメラには個人情報の流出（画像）の脅威が想定される。
監視カメラの個人情報の流出（画像）の脅威に対して、認証設定厳格化が対策として挙げられる。

＊【平文 2】は【平文 1】より監視カメラの追加に関する情報（2 行目と最後の 2 行のみ）が追加されている．

図 A·4　平文の事例
Fig. A·4　Example of Natural language representation.

A.3　GSN の事例



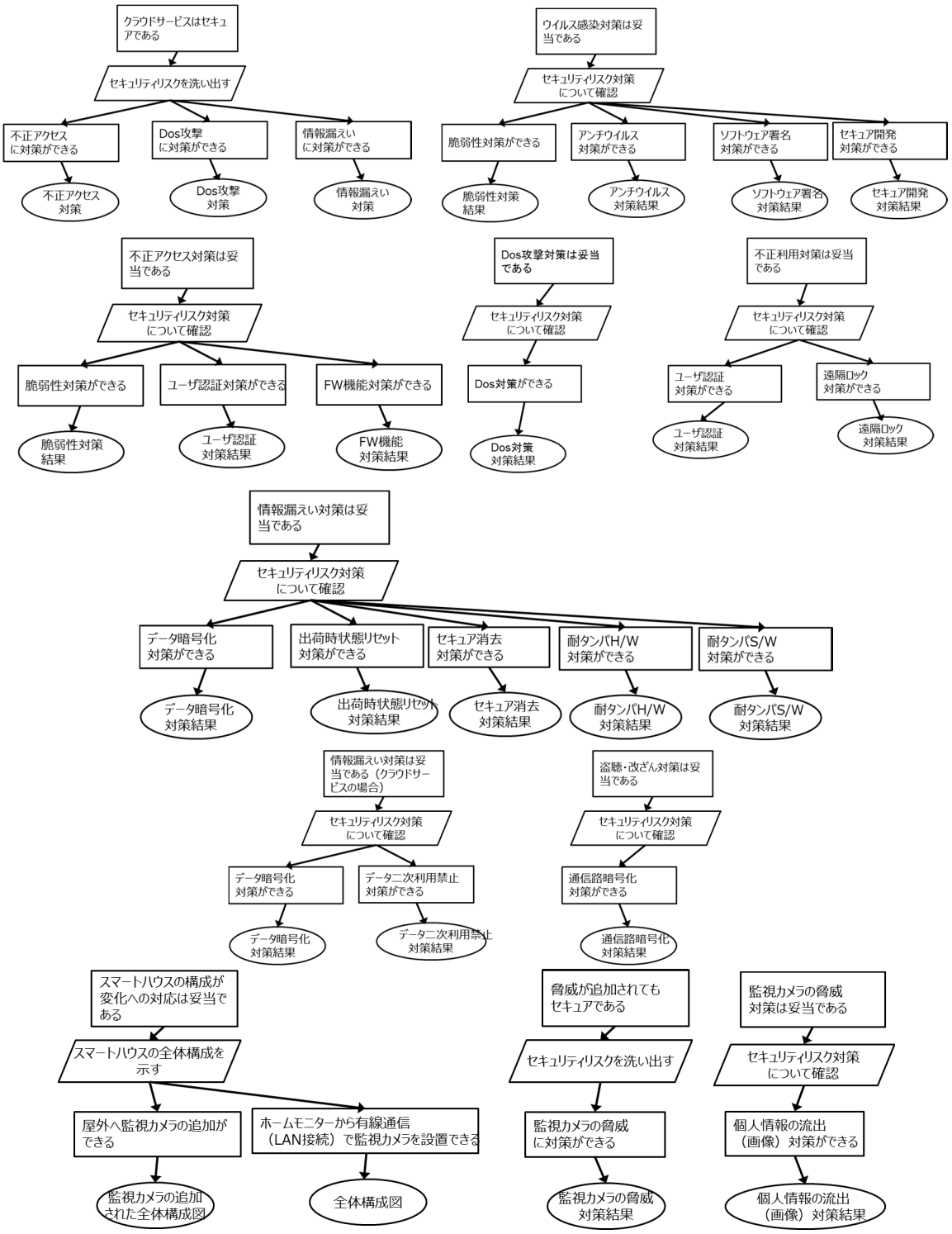
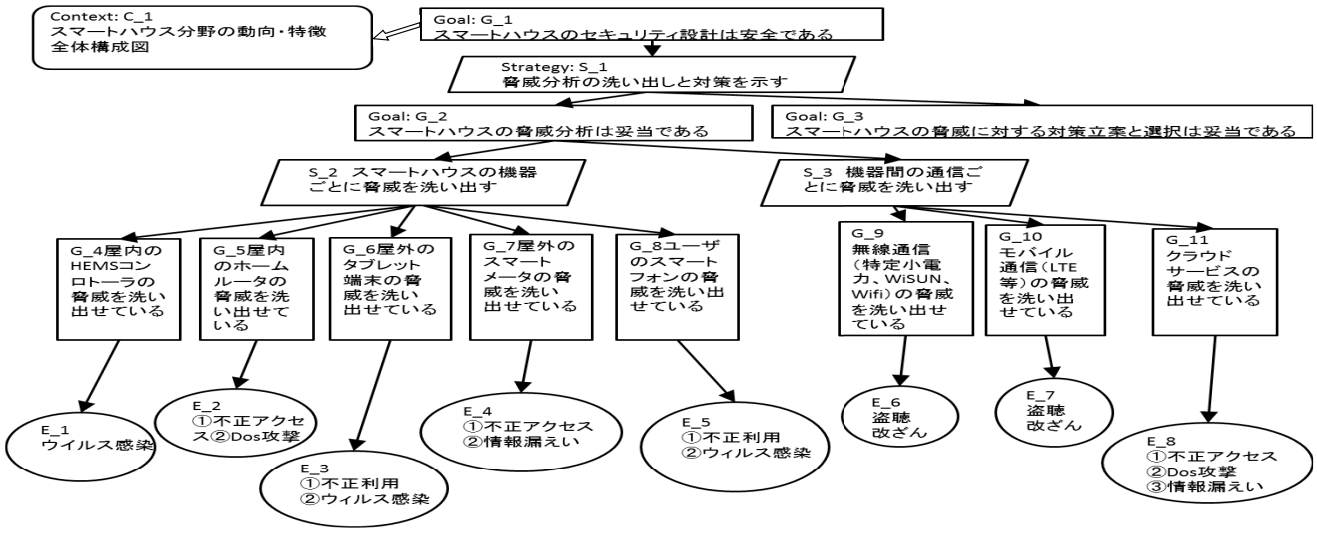


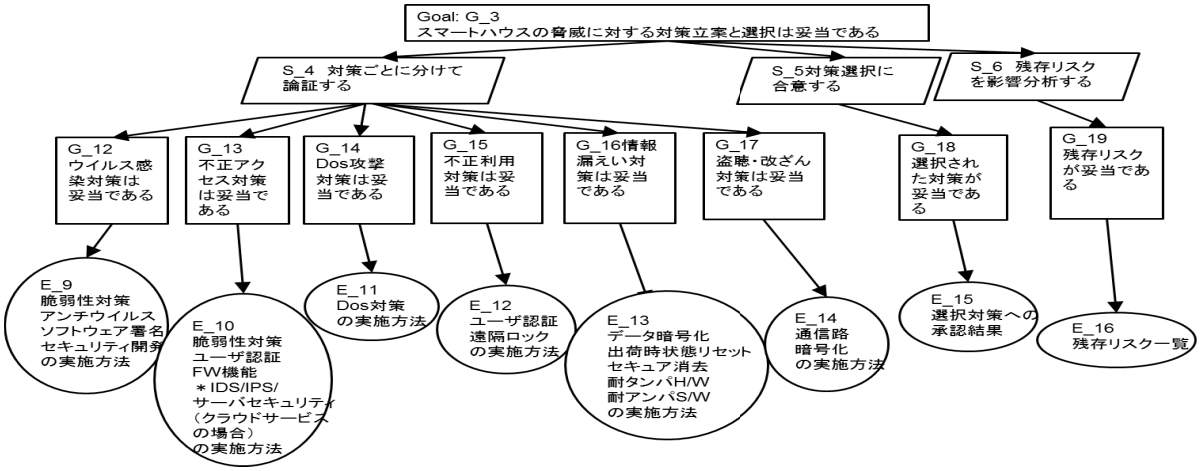
図 **A·5**　GSN の事例

Fig. A·5　Example of GSN.

A.4　スマートハウス事例への CC-Case の適用例



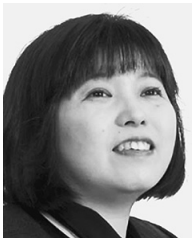
脅威の洗い出し部分(The part of threat analysis)



対策立案と選択部分(The part of countermeasures)

図 **A·6**　スマートハウス事例への CC-Case の適用例

Fig. A·6　Example of CC-Case applied to to the smart house.



金子 朋子　（正会員）

1988 年慶応義塾大学卒業．同年（株）NTT に入社後，（株）NTT データにてコンピュータシステム設計開発に従事．2010 年情報セキュリティ大学院大学博士前期課程修了．2014 年同後期課程修了．博士（情報学）．2016 年より（独）情報処理推進機構ソフトウェア高信頼化センター研究員．情報セキュリティ大学院大学客員研究員．公認情報セキュリティ監査人．（社）日本科学技術連盟ソフトウェア品質管理研究会セーフティ&セキュリティ開発分科会主査．2015 年日本ネットワークセキュリティ協会（JNSA）15 周年記念論文優秀賞受賞．

髙橋 雄志　（正会員）

1977 年生．2001 年創価大学工学部情報システム学科卒業．2003 年同大学大学院工学研究科情報システム工学専攻博士前期課程修了．2014 年同大学院博士後期課程修了，博士（工学）．現在，東京電機大学総合研究所複合領域サイバー・セキュリティプロジェクトサイバーセキュリティ研究所研究員．情報セキュリティマネジメントの研究に従事．日本セキュリティ・マネジメント学会会員．

勅使河原 可海　（正会員）

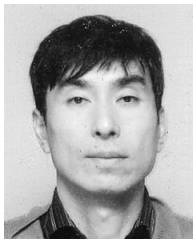
1942 年生．1970 年東京工業大学大学院理工学研究科博士課程修了，博士（工学）．同年日本電気入社．コンピュータネットワーク，ネットワークアーキテクチャ，衛星データネットワーク等の開発に従事．1974～1976 年ハワイ大学アロハシステム客員研究員．1995 年創価大学工学部教授，工学部長等を歴任．現在，東京電機大学総合研究所複合領域サイバー・セキュリティプロジェクトサイバーセキュリティ研究所研究員．ネットワークセキュリティ，e-learning，ユビキタスコンピューティング等の研究に従事．オペレーションズリサーチ学会フェロー，情報処理学会平成 23 年度功績賞．創価大学名誉教授．本会フェロー．

吉岡 信和　（正会員）

1998 年北陸先端科学技術大学院大学情報科学研究科博士後期課程修了．博士（情報科学）．同年（株）東芝入社．2002 年より国立情報学研究所に勤務，現在，同研究所准教授，2007 年より総合研究大学院大学准教授を兼務，セキュリティ・プライバシソフトウェア工学，ソフトウェア工学，学術クラウドの研究・開発に従事．2015 年より IEEE CS Japan Chapter 役員．2011 年から 2015 年まで日本ソフトウェア科学会理事を歴任．電子情報通信学会，日本ソフトウェア科学会，人工知能学会，IEEE Computer Society 各会員．

山本 修一郎　（正会員）

1979 年名古屋大学大学院修士課程修了．同年日本電信電話公社（現，NTT）入社．以後，研究所において，言語処理プログラム，ソフトウェア開発支援環境，DB トランザクションモニタ，Web データベース連携エンジン，IC カード運用管理システム等の研究・実用化に従事．2002 年（株）NTT データ技術開発本部副本部長．2007 年同社初代フェロー．システム科学研究所所長．2007 年東京工業大学統合研究院医療情報プロジェクト特任教授．2009 年名古屋大学情報連携統括本部情報戦略室教授．2016 年同大学情報科学研究科教授．AI 学会知識流通ネットワーク研究会主査，PM 学会中部支部長，IPA システム構築上流工程強化部会主査．ACM，IEEE，電子情報通信学会，人工知能学会，日本情報経営学会各会員．



大久保 隆夫　（正会員）

1991 年東京工業大学物理情報工学専攻修了．同年株式会社富士通研究所に入社．リバースエンジニアリング，分散開発環境，アプリケーションセキュリティの研究に従事．2006 年情報セキュリティ大学院大学入学，2009 年同修了．博士（情報学）．2013 年より情報セキュリティ大学院大学准教授．2014 年より同教授．情報処理学会コンピュータセキュリティ研究会専門委員．電子情報通信学会，日本ソフトウェア科学会，IEEE CS 各会員．Aviation Security 研究会幹事，脅威分析研究会幹事．専門はシステムセキュリティ，セキュリティ・バイ・デザイン．

田中 英彦　（名誉会員）

1970 年東京大学大学院修了，工学博士．東京大学工学部教授，同大学大学院情報理工学系研究科教授・研究科長を経て，2004 年情報セキュリティ大学院大学教授・研究科長．2012～2016 年同学長．計算機アーキテクチャ，知識処理，デペンダブル情報システム等に興味を持つ．著書に「非ノイマンコンピュータ」「Parallel Inference Engine」等．人工知能学会名誉会員，電子情報通信学会フェロー，IEEE ライフフェロー．