Vol.2017-UBI-54 No.16
Vol.2017-CDS-19 No.16
2017/5/26

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]　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]

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もつのかははっきり示していなかった．そこで，脅威分析のプロセスを論理モデル化した CC-Case, GSN と自然言語表記を比較する実験を実施し,要件の可視化と妥当性確認における有効性を評価した．

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

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

KANEKO　TOMOKO[†1]　TAKAHASHI　YUJI[†2]
TESHIGAWARA YOSHIMI[†2] YOSHIOKA　NOBUKAZU[†3]
YAMAMOTO　SHUICHIROU[†4]　OOKUBO　TAKAO[†1]
TANAKA HIDEHIKO[†1]

Abstract: We 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 show the conformation to the process as the concrete model. However, the effectiveness of CC-Case has not shown. In this paper, we compare CC-Case which has logical model of threat analysis process, GSN, and Natural language representation by evaluating practice. We evaluate the effectiveness visualization and verification of requirements.

Keywords: Assurance Case, CC-Case, GSN, Security Case, Common Criteria

1. はじめに

筆者らは，コモンクライテリア（CC：Common Criteria. ISO/IEC15408 と同義）[1][2][3]とアシュアランスケース（ISO/IEC15026）[4]を用い，セキュリティ仕様を顧客と合意の上で決定する手法 CC-Case[5] [6]を提案している．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．これまで CC-Case については，CC 認証を伴うセキュリティ要件定義中心に展開してきたが，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，ライフサイクルごとの開発工程に対するセキュリティ要求分析と保証の統合開発方法論[6]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(Goal Structure Notation)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ている．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している．さらに 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 IoT 時代の要求への対応とその保証に役立てることができる．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もつのかははっきりしていなかっ

†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
†3 国立情報学研究所　NATIONAL INSTITUTE OF INFORMATICS
†4 名古屋大学　NAGOYA　UNIVERSITY

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 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．

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．図 2 に，CC 構成と ST（Security Target）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．

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] [8]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 [9]と SAEM [10]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 [11]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].

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 [18]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[19]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[20]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．C-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である[7].

3. CC-Case の有効性評価実験

3.1 実験の概要

セキュリティ設計（以下，セキュリティ・バイ・デザイン）における CC-Case の有効性検証のために，スマートハウスの図から起こした平文，GSN，CC-Case による設計資料のそれぞれを用いて元の図を再構築する実験を行った．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）を比較する実験を行った．

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を図示したものである（図 1）[21].

平文（図 2）は図 13 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 は図 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．図 1 の事例を脅威分析のプロセスを論理モデル化した CC-Case で記述したものが，図 4 と図 5 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．図 4 と図 5 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一階層のゴールと第 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．

Vol.2017-UBI-54 No.16
Vol.2017-CDS-19 No.16
2017/5/26

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．

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（未回答者含む），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り当てを行った．

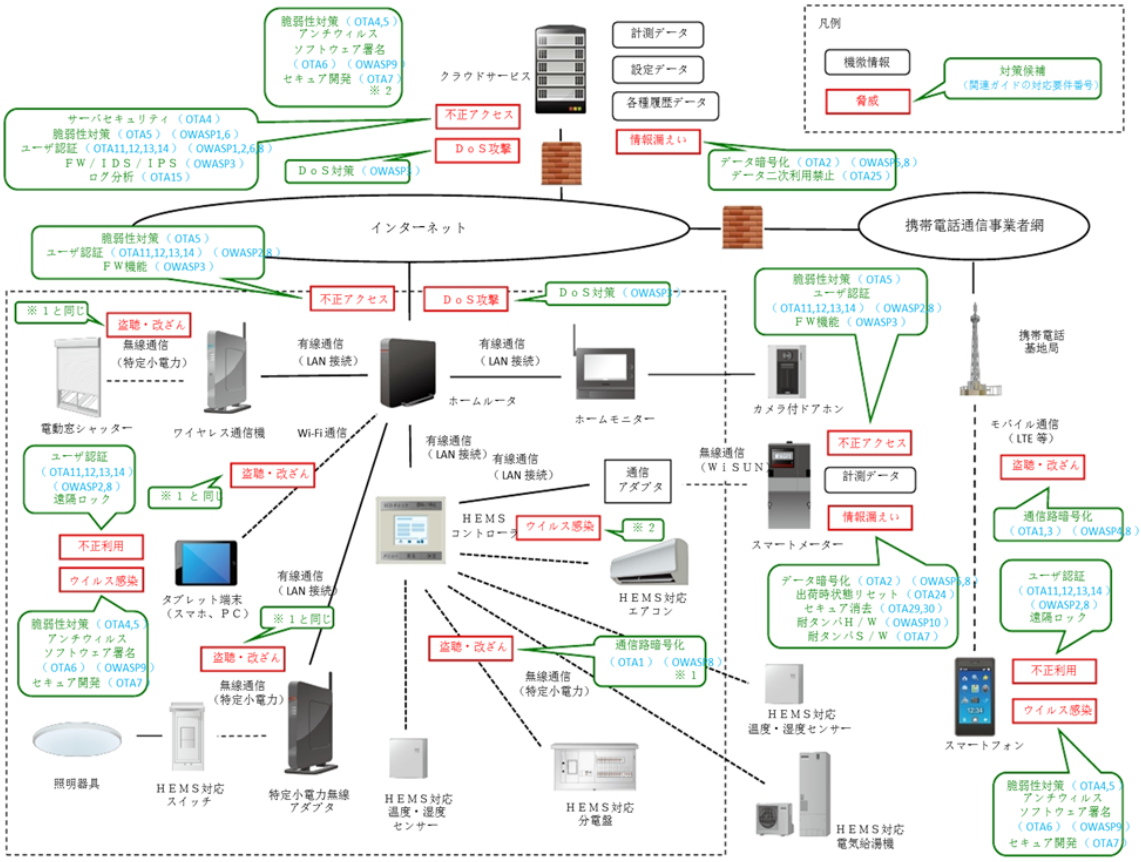

図 1　スマートハウスの脅威と対策の検討例[21]


【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．

図 2　平文の事例

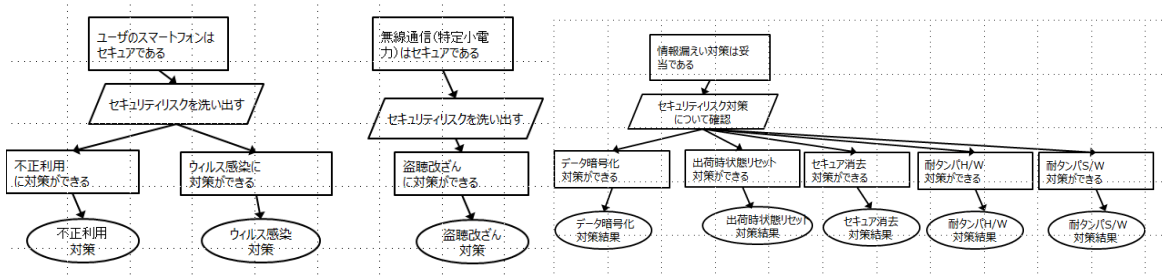

図 3　GSN の事例

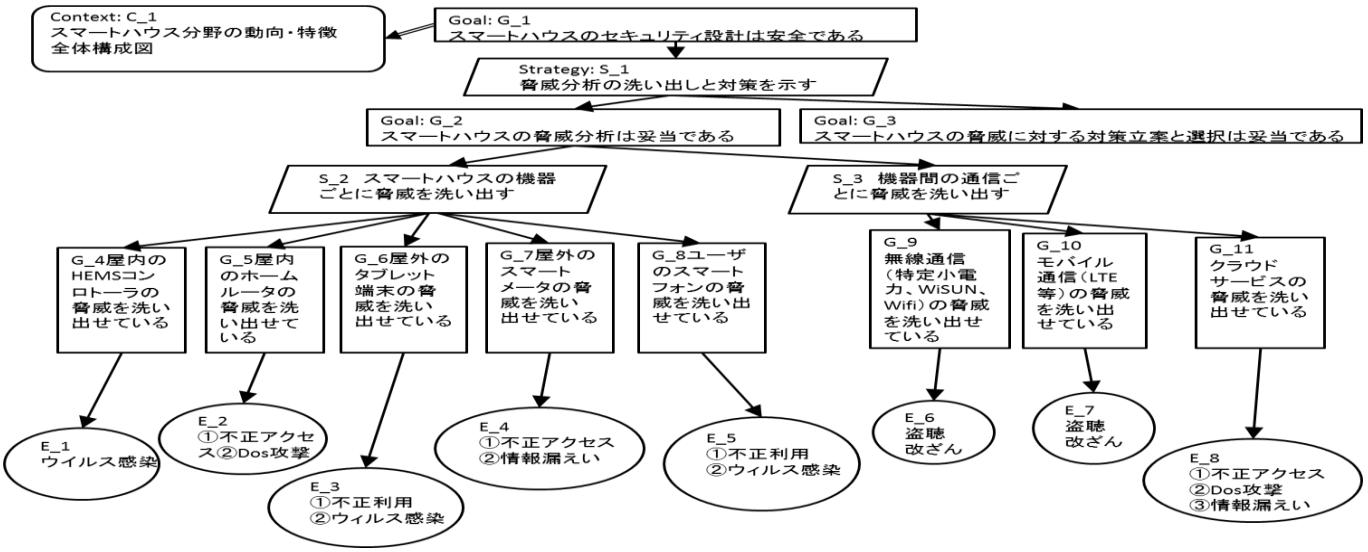

図 4.スマートハウス事例への CC-Case の適用例（脅威の洗い出し部分）

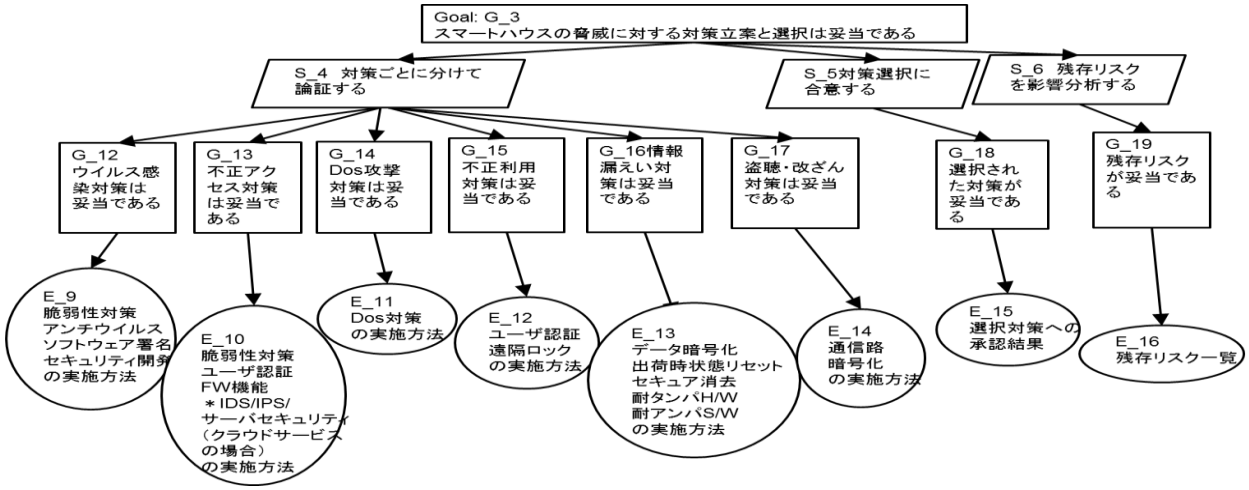

図 5.スマートハウス事例への CC-Case の適用例（対策立案と選択部分）

3.2　実験手順

(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．

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.

(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.

(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 箇所,【設問 2】では 5 箇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．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．設問は以下の通りである.
【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.）

(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．設問は以下の通りである.
【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）

(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ーによるコメントも収集した．設問は以下の通りである.
【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〇をし，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〇をし，理由を記載してください.
（平文・GSN・CC-Case・わからない）

3.3 実験結果

本実験では設問ごとに，未回答者および作業を伴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.
・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.

・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

Vol.2017-UBI-54 No.16
Vol.2017-CDS-19 No.16
2017/5/26

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×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 1 の示す通りである．表 1 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．また標準偏差で青字が最も小さいのは 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示す．

表 1. 【設問 1】における担当資料ごとの平均値と標準偏差

	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

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 6 に示す．図 6 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．

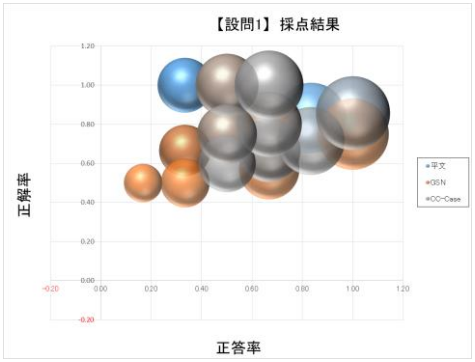

図 6. 設問 1 における各被験者の値

【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 2 に示す通りである．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．

表 2. 【設問 2】における担当資料ごとの平均値と標準偏差

	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

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 7 に示す．設問 1 と同様に色と球の大きさで表現している．

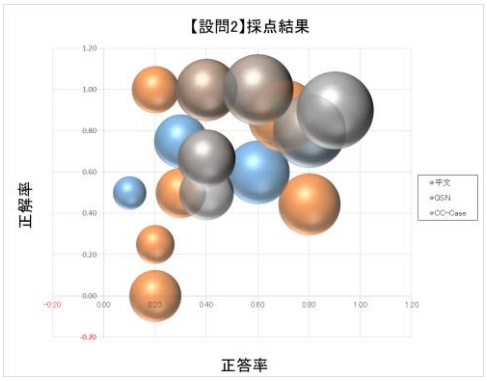

図 7. 【設問 2】における各被験者の値

【設問 3】

リスクが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

・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 8 のグラフに示す．

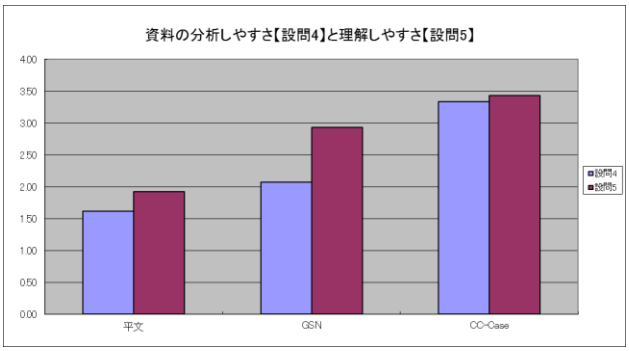

図 8. 【設問 4,5】資料の分析しやすさと理解しやすさ

・手順 5

設問 6，7 における回答の割合を図 9，図 10 に示す．

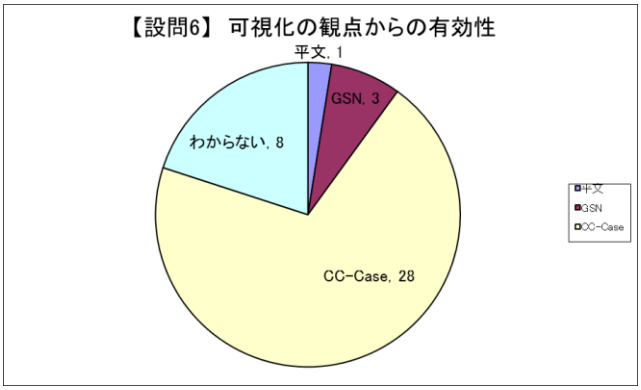

図 9. 【設問 6】可視化の観点からの有効性

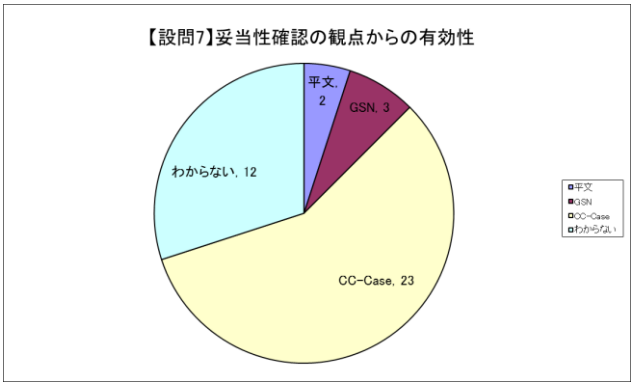

図 10.【設問 7】妥当性確認の観点からの有効性

フリーアンサーの回答では，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．

3.4 実験の考察

【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．フリーアンサー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わ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．フリーアンサーも設問 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．

4. まとめ

実験の結果を全体として考察すると， CC-Case は全般的に高い評価を受けた. 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み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わ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，図の形さえわかれば，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,「わからない」を選択した以外の人を対象にすると，問 6 か問 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 から 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わかる平文よりも優位となるような更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.

今後の課題としては，設問 3 のリスクへの対応性に関して，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.

今後の取り組みとしては，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きたい．さらに CC-Case の利点として複雑でわ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，スマートハウスの事例を実験に用いたように，今後 IoT セキュリティのような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 の特性を分析し，IoT システム自体への本格的な適用をはかっていきたい.

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) 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) 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
9) OMG, ARM, http://www.omg.org/spec/ARM/1.0/Beta1/
10) 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/
11) 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
12) Stephen Edelston Toulmin, “The Uses of Argument,” Cambridge University Press,1958
13) The Adelard Safety Case Development (ASCAD), Safety Case Structuring: Claims, Arguments and Evdence,http://www.adelard.com/services/SafetyCaseStructuring/index.html
14) DEOS プロジェクト, 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, 2014 年 3 月
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) 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
18) 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
19) 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
20) 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
21) 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