多様なステークホルダの満足度に着目したシステムの安全性・セキュリティ要件の抽出と検証

System Requirements Analysis for Safety and Security with Multiple Stakeholder Perspectives on STAMP/STPA

柳原 靖司
ブラザー工業株式会社
yasushi.yanagihara@brother.co.jp

吉田 邦雄
オムロン株式会社
kunio.yoshida@omron.com

石川 冬樹
国立情報学研究所
f-ishikawa@nii.ac.jp

栗田 太郎
ソニー株式会社
taro.kurita@sony.com

要旨

本論文では，ステークホルダの多様な視点を取り入れながら客観的かつ系統的にシステムの安全性・セキュリティ要件の抽出と検証を行う手段として，SSMS 法（Safety and Security requirements analysis method with Multiple stakeholder perspectives on STAMP/STPA）を提案する．近年，AI/IoT に代表されるようにソフトウェアが大規模・複雑化する中で，抜け漏れなくシステムの安全性・セキュリティ要件を抽出し，かつステークホルダの間で合意形成することが難しくなっている．SSMS 法を用いることで，対象ドメインの知識を十分に有してなくても複雑なシステムのハザードと脅威に対する対策群を実用的な量で獲得し，要件の満足度に関する評価指標で定量的に評価することができる．

This paper presents a safety and security requirements analysis method with multiple stakeholder perspectives on STAMP/STPA called SSMS Method. In recent years, as software has become larger and more complex, as represented by AI/IoT, it has become difficult to extract safety requirements comprehensively and to form consensus among stakeholders adequately. SSMS Method facilitates developers to acquire safety and security requirements without sufficient knowledge of the target domain and to evaluate them quantitatively based on their assent.

1. はじめに

システム開発の上流工程において抜け漏れなくシステムの要件を抽出し*1，ステークホルダ間で合意形成することは難しく，大規模・複雑化する先進システムの開発ではその傾向が顕著である．システム要件の中でも運用段階で生じるハザードや脅威に対応するための安全性やセキュリティといった要件の抽出は重要であり，次世代システム安全性解析手法のひとつである STAMP/STPA（Systems-Theoretic Accident Model and Processes/ System-Theoretic Process Analysis）による解決アプローチが注目されている．米国を中心に航空宇宙，プラントの分野で適用実績が積まれてきており，最近では AI/IoT といった領域にも応用範囲が広がっている．システムに関わる人，環境，機械といった要素をモデル化し，その相互作用に着目することで安全・安心を脅かす要因を系統的に解析していくが，解析者が持つ思考特性によって導出される結果に偏在性が生じる等，手法が持つ適用汎用性から生じる課題も分かってきている．そこで，我々はシステム構築の要求分析・要件定義の分野で用いられているステークホルダの合意形成プロセスの知見を STAMP/STPA に導入し，安全性とセキュリティの対策を網羅的に抽出できるようにした上で，要件の満足度の指標で定量的に評価するプロセスモデル SSMS 法（Safety and Security requirements analysis method with Multiple stakeholder perspectives on STAMP/STPA）を考案した．

*1 要件定義における「抜け」とは，ユーザ企業（発注元）からの要求に適合するように網羅的に要件化されていないこと．「漏れ」とは，考慮漏れのことで，ビジネス目標を達成する上で要件が要求を満足できていないこと（非機能要件の不完全性等）．

第三者による実験では，STAMP/STPA に多様なステークホルダの視点を導入することで抽出されるシステム要件の視点の豊かさが増し，かつドメインの有識者でなくても量と質（目的合理性）の点でドメインの有識者に近いシステム要件を客観的かつ系統的に抽出できることが分かり，SSMS 法の有効性が確認できた．以下，本論文の構成を述べる．

まず，2 章では現状分析と課題提起を行う．次に 3 章では関連技術について言及し，4 章，5 章で夫々，解決策の提案と評価結果を示す．6 章で評価結果に関する考察を行い，最後に 7 章で成果と将来への発展で結ぶ．

2. 解決すべき課題

2.1. 現状分析

AI/IoT に代表される複雑なソフトウェア集約型システムが登場しており，コンポーネント単位の信頼性を担保するような従来型の品質保証に加え，多数のコンポーネントが相互に連携するつながるシステムを俯瞰的に捉えながら，安全・安心を保障することが社会の課題として認識されている．この課題に対するアプローチとして，要求工学の分野ではステークホルダが連携しながらシステムのライフサイクル全体を分析するためのガイドラインが構築されている[1]．システムの安全設計・安全性論証の分野では STAMP/STPA[2]，アシュアランスケース等の活用研究が進められている．

2.2. 課題提起

現在，システミック・アプローチで複雑なシステムの安全性を解析する技術として STAMP/STPA が知られている．FTA（Fault Tree Analysis），FMEA（Failure Mode and Effect Analysis），HAZOP（Hazard and Operability Study）といった従来手法とは異なり，解析対象システムに影響を及ぼす人，環境，機械をモデル化し，構成要素の創発特性から生じるハザードを解析するアプローチを用いる．解析手法としての汎用性があるため，様々な産業のシステムに適用可能であるが，解析者が持つ思考特性により抽出されるハザードと脅威の対策群に偏りが生じる課題が本研究の予備実験から分かっている[3]．予備実験では文献[1]を参考にしながら，抽出された対策群を表 1 に示すような 3 つのステークホルダの視点で分類したが，例えばベンダの開発者であれば，システムの実装に関する対策群が解析の結果として抽出されやすい傾向があり，その他の視点は検討の優先順位が下がる．システム開発の要求分析や要件定義では，多様なステークホルダ間の合意形成を促進することが望ましいので，システムの安全設計・安全性論証の領域にも要求工学の知見を取り入れる必要がある．

3. 関連技術の説明

我々の研究の技術的拠り所として用いている STAMP/STPA 及び AGORA[4]（Attributed Goal-Oriented Requirements Analysis Method）について述べる．

3.1. STAMP/STPA

STAMP/STPA では，図 1 に示すようなコントロールストラクチャ（CS: Control Structure）を用いてシステムの構成全体をモデル化し，コントローラから被コントロールプロセスに対して発行されるコントロールアクションの乱れ（UCA: Unsafe Control Action）に着目しながら，安全制約を逸脱するようなハザード要因（HCF: Hazard Causal Factor）を解析していく．ハザード要因の解析には STPA の中で予め提供されているガイドワードを利用することで，様々な視点で HCF を強制発想できるように工夫されている．HCF が抽出された後は，各 HCF に対する対策群を立案することで解析が完了する．当初の STAMP/STPA

表 1 各ステークホルダが持つ視点

ステークホルダ	ステークホルダが持つ視点
ユーザ企業の管理者	システムを実現する上での制約よりも，システム稼働後のビジネス収益性や業務変革の視点から価値を最大化することを目的とする．災害時の事業継続やセキュリティリスクに高い関心を持つ．
ベンダの開発者	受託企業としてユーザ企業とのトラブルは避けたい．QCD のバランスに配慮して手堅く進めたい．無理な要件の実装は避けたい．
ユーザ企業の担当者	現場業務の改善（業務の効率化）の思考が強く，やや保守的な変化を好む傾向を示す．要件定義に当たっては既存業務との整合性を重視し，業務変革レベルの視点が弱い．

では機能安全に関する領域で研究が進められていたが，その後，システムのセキュリティに関する脅威を解析することができるようにプロセスモデルが拡張されている[5][6].

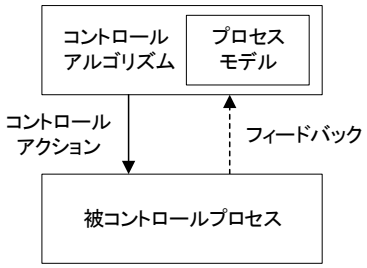

図 1 STAMP/STPA CS の例

3.2. AGORA（属性つきゴール指向要求分析法）

AGORA とはゴール指向要求分析手法のひとつで，AND-OR ツリーグラフ（図 2）に属性値を付与した上で，下流に向かって対案となるサブゴールを展開していきながら，ステークホルダ間の要求獲得に関する合意形成を促進させるための手法である．属性値のひとつとして満足度行列（図 3）があり，例えば，各ステークホルダが顧客・管理者・開発者の視点でサブゴールの評価値を 3 行 3 列の行列に登録すれば，ユーザに関する要素の総和からゴール適合度（式 1）を求めたり，列方向の要素の分散値から意見の対立度を求めたりすることができる．

なお，ゴール指向要求分析手法には AGORA 以外にも NFR（Non-Functional Requirements）フレームワーク[7]，GSN（Goal Structuring Notation）[8]等が知られているが，先行研究[9]の成果を踏まえ，AGORA の満足度行列が要件のゴール適合度を求めたり，ステークホルダ間の意見対立を可視化したりする上で分かり易く，かつ現場の実務に導入し易いと考えた為，AGORA を採用した．

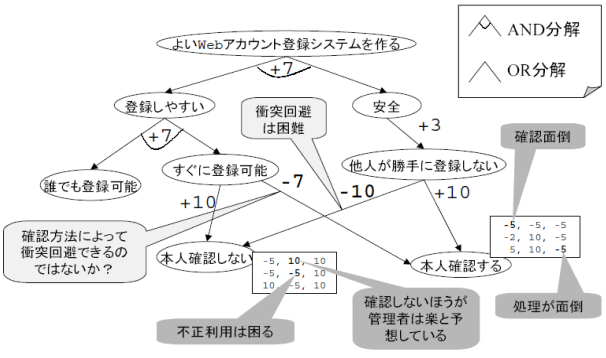

図 2 AND-OR ツリーグラフ[4]

評価の視点

評価者	顧客	管理者	開発者
顧客	8	8	(4)
管理者	5	5	2
開発者	4	8	-6

凡例：(4) 顧客が開発者の視点で要求を評価した結果

図 3 満足度行列[4]

$$Cup(g) \stackrel{\text{def}}{\equiv} \frac{\sum_{s \in Stakeholder, c \in Customer} m(g)_{s,c}}{|\,Stakeholder\,| \times |\,Customer\,|}. \quad (1)\,[10]$$

$Cup(g)$は，ゴールgに対する顧客の選好度，$Stakeholder$は全てのステークホルダ（顧客，管理者，開発者），$Customer$はユーザに関するステークホルダ（顧客，管理者）である．式(1)の分子はゴールgの満足度行列に含まれる$Customer$の要素の総和，分母は$Stakeholder$と$Customer$に関する集合の濃度の直積集合として計算すれば$Cup(g)$が求まる．

図 3 の満足度行列を例に計算方法を示す．

$Cup(g)$：6.3

分子：38

$Customer$に関する素点の合計値

{顧客の素点}＋{管理者の素点}

= {8 + 5 + 4} + {8 + 5 + 8}

分母：6

次の値の平方根

{ $Stakeholder$の濃度：9}×

{ $Customer$の濃度：4}

※集合の濃度とは，個数である．

4. 解決策の提案

4.1. 課題の解決方針

我々は 2.2 節で取り上げた課題を解決するため，SSMS 法を提案する．SSMS 法は多様なステークホルダの視点を STAMP/STPA に導入しながら，客観的かつ系統的にシステムのハザードとセキュリティ脅威の対策群を抽出した後，これらを安全性・セキュリティ要件として AGORA の満足度行列を用いて評価するプロセスモデルである．このモデルが狙っている効果は，システム安全性

の解析結果(STAMP/STPA の対策群)の多様性を創出することであるが，解析者が持つ思考特性がシステムの安全性解析結果に偏在性を生じさせる性質に対応するために，予めシステムの開発において利害関係が生じやすい複数のロールの立場で思考制約を設けてSTAMP/STPA による解析を実行する．SSMS 法では，図 4 に示すように管理者，担当者，開発者の視点を導入している．STAMP/STPA による解析結果で得られた対策群をシステムの安全性要件として実装に移していく過程では，どの要件を採用するべきか，ステークホルダ間で合意形成が必要である．SSMS 法では，抽出された対策群を要件の満足度の観点で評価した後，要件毎に満足度行列の形で整理し，さらに「ゴール適合度」と「意見対立の相関」の2つの指標で定量化する．要件の質(目的合理性)が定量化できるので，システムの安全性・セキュリティ要件の決定プロセスにおいて，ステークホルダ間の合意形成促進に貢献できる．

なお，SSMS 法のプロセスモデルでは，要件の抽出プロセスに AGORA のツリーグラフではなく，STAMP/STPA のシステミック・アプローチを導入している．これは AI/IoT に代表される先進システムの要素間の複雑なインタラクションからもたらされる創発特性を捉えやすくすることを期待している．特に人とシステムの相互作用に関わる解析では，ツリーグラフのように上流から下流に展開される構造モデルでは解析が困難だからである．また，STAMP/STPA を導入する別の利点として，熟練技術者が持つ業務知識や知見への依存度を抑える役割もある．STPA の手順化されたプロセスによって，技術の専門家ではないユーザ企業の管理者や担当者をシステム安全性解析フェーズに巻き込み易くなると考える．以上の点から SSMS 法では，多様なステークホルダの視点を活用できる点で従来手法に比べ優位性がある．

4.2. SSMS 法の解析手順

図 4 に示すプロセスに従い，システムの安全性・セキュリティ要件の抽出と検証を行う．

STEP1: システムのゴールを明確化し，システム構成図を作成する．

STEP2: STAMP/STPA の解析に必要なアクシデント，ハザード，安全性制約を列挙する．

STEP3: システム構成図から構成要素，コントロールアクション，フィードバックを特定し，コントロールストラクチャを定義する．(モデル化)

STEP4: システム開発に携わるユーザ企業の管理者，担当者及びベンダの開発者が，STAMP/STPA を用いて夫々，解析を行う．このとき，各解析者は自身の役割(ロール)を適切に意識し，ロール毎の思考制約の中で解析を行う．(UCA 抽出→HCF 特定→システムのハザードとセキュリティ脅威に対する対策群の立案)

STEP5: 対策群を集約し，システムの安全性・セキュリティ要件としての評価を行う．要件を定量化する手法として AGORA の満足度行列を用い，前記ステークホルダが自身と他のステークホルダの視点で-10から+10の範囲で要件としての満足度を評価し，素点を付ける．そして，満足度行列から「ゴール適合度」と「意見対立の相関」を計算することで定量化を行う．

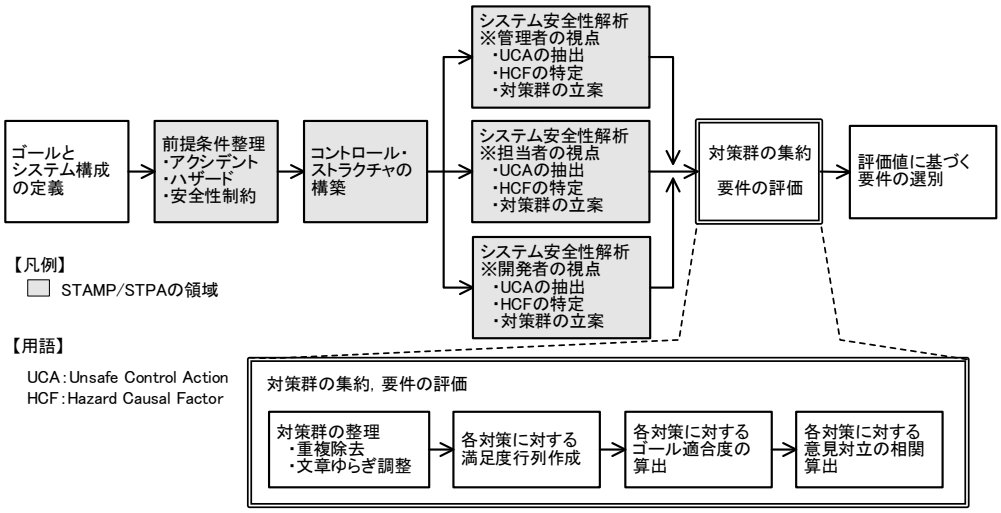

図 4 SSMS 法のプロセスモデル

STEP6: ステークホルダの間で要件の評価値を見ながら要件を選別する.

4.3. 仮説と研究設問

SSMS 法で解決しようとする仮説と研究設問を述べる.

[仮説]

多様なステークホルダの視点を STAMP/STPA に導入してシステムのハザードと脅威に対する対策群を抽出し, これらを要件としてゴール指向で分析すれば, 客観的かつ系統的に合意形成されやすい安全性・セキュリティ要件を獲得できる.

[研究設問]

RQ1:解析者にロールを与えてシステムのハザードとセキュリティ脅威を解析することで, 多様な視点(異なるステークホルダの視点)で安全性・セキュリティ要件を獲得できる.

RQ2:ドメイン知識を十分に有しなくても複数のロールを持たせて SSMS 法で解析することで, 当該ドメインの有識者と同等量の安全性・セキュリティ要件を獲得できる.

RQ3:ドメイン知識を十分に有しなくても複数のロールを持たせて SSMS 法で解析することで, 当該ドメインの有識者が抽出した要件に近い質(目的合理性)の安全性・セキュリティ要件を獲得できる.

5. 解決策の評価

5.1. 評価方法

仮説の検証は, 図 5 に示す仮想の QR コード決済システム(以降,「対象システム」と呼ぶ)に対して RQ1, RQ2, RQ3 の妥当性を確認することで実施した. 対象システムは Enterprise システムの一種であるが, システムのハザードと脅威の解析に当たっては, 端末とセンターサーバ間で発生するトランザクションの他, 人とシステムの協調という総合的なシステム運用に関する知識が要求される.

今回, 対象システムの解析を実施する上で, 第三者の被験者 I群, II群(IIa 群, IIb 群), III群を用意した(表 2). 各被験者は独立で, 夫々, 表 2 に示すような役割と前提

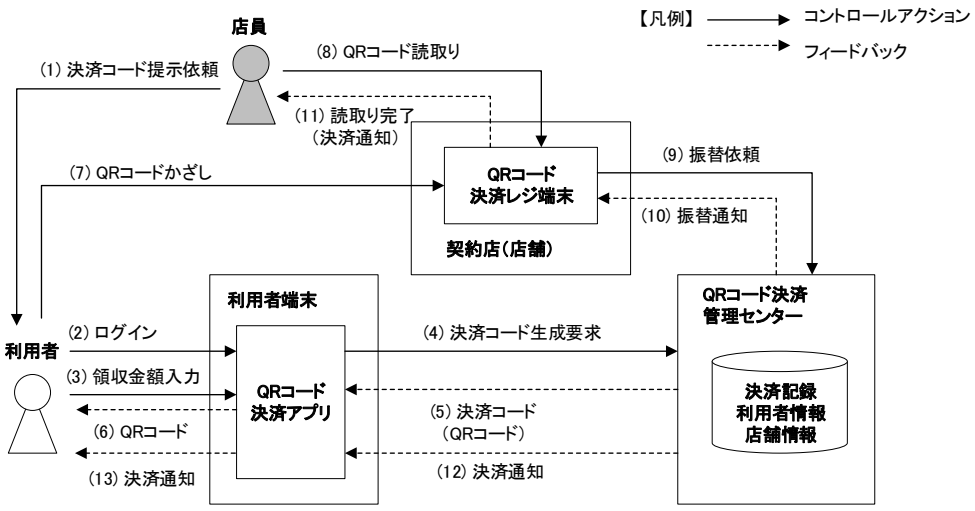

図 5 仮想 QR コード決済システム(STAMP/STPA のコントロールストラクチャ(CS))

表 2 被験者の役割と前提条件

被験者	役割	条件
I群	解析と対策群の抽出	3 名; Enterprise システム開発に非精通; 特定ロールを不付与
IIa 群	解析と対策群の抽出	3 名; Enterprise システム開発に精通; 特定ロールを付与
IIb 群	解析と対策群の抽出	3 名; Enterprise システム開発に非精通; 特定ロールを付与
III群	対策群の評価(定量化)	3 名; Enterprise システムの技術を解釈可; 特定ロールを付与

[補足] 特定ロール:ユーザ企業の管理者, ユーザ企業の担当者, ベンダの開発者

条件を持つ. 実験では, ロールなしの被験者(Ⅰ群)についてはロールを意識しないで対策を抽出してもらい, 他方, ロールありの被験者(Ⅱ群)については夫々対応するひとつのロールを意識してシステムを解析してもらった. その上で, 解析結果として得られたシステムのハザードと脅威に対する対策群に対し, 第三者(Ⅲ群)がロールを考慮しながら評価した. 解析時間の目安として, KKD(解析者の経験と勘から対策を見つける方法) は 120 分, STAMP/STPA は 240 分*2とし, 基準時間の目安から10%を超過した場合には実験を再試行することにしたが, 今回の実験では各被験者の抽出時間はすべて基準時間内に収まった.

ここで, 各被験者のドメイン知識とロールに関する特記事項を示す.

[ドメイン知識]

・Enterpriseシステム開発に精通(Ⅱa群):
Enterpriseシステムのベンダに所属し, 開発経験あり

・Enterpriseシステム開発に非精通(I群, IIb群):
車載システムもしくは産業システムのベンダに所属し, 開発経験あり

[ロールに関する実務経験]

・ユーザ企業の管理者:
所属する企業の役職が管理職であり, ユーザ企業の管理者の視点を理解できる.

・ユーザ企業の担当者:
ベンダの開発者としてユーザ企業の担当者のシステム開発における要求を理解できる.

・ベンダの開発者:
ベンダの開発者としてシステム開発に求められる基礎的な知識と業務経験がある.

5.2. 評価結果

[RQ1 に関する評価結果]

特定ロールを付与しない被験者I群と特定ロールを付与した被験者II群に対象システムのハザードとセキュリティ脅威を解析してもらい, 対策の抽出量を比較した.

図6は各被験者の対策抽出量であるが, 被験者にロールを付与すると, 保有するドメイン知識の量(Enterpriseシステム開発の精通度)に係わらず付与したロールに対応する対策の抽出量が最多となった. 逆に, 被験者にロールを付与しないとそのような傾向がみられなかった. 特記事項として, Ⅱa群のロールあり(管理者)とⅡb群のロールあり(開発者)に該当する被験者は, 他の被験者と比べ対策群を2倍以上抽出したが, これは個人差から生じていると推察される. 例えば, Ⅱa群の管理者ロールを担当した被験者は, 国内大手のSIerで20年以上に渡りシステム開発に従事し, 所属企業ではベテラン管理職としてプロジェクト横断で業務支援を行っていることから, Enterpriseシステム開発の精通度が高い特性があった.

次に, 図7では各被験者が抽出した対策群をⅠ群とⅡ群でロール属性ラベル毎に合計し, ロールの有無によって抽出量に与える影響を調べた*3. 同図から分かることは, ロールを付与しないと, 管理者のロール属性ラベルに該当する対策抽出量が少なくなる点である. Ⅰ群では

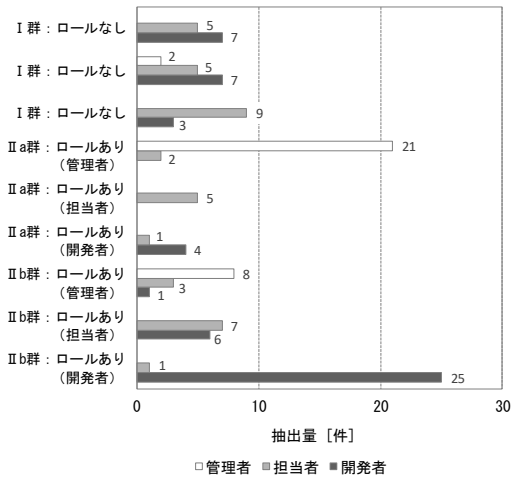

図 6 被験者毎の対策抽出量

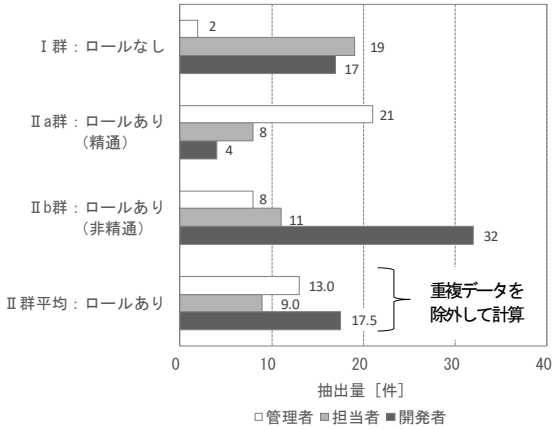

図 7 ロール有無毎の対策抽出量

*2 STAMP/STPA による抽出では専用ツールを用いて対話型の解析を行う為, KKD の2倍の時間を設定した.

*3 I群とII群の被験者数を揃えて比較する為, II群については重複データを除外してからIIa 群とIIb 群の抽出量を平均した.

合計抽出量 38 件の 5.3%(2 件)が管理者のロール属性であるのに対して，Ⅱ群では 32.9%(13 件)がそれに該当した．実際，Ⅰ群の被験者にインタビューしたところ，システムの安全性・セキュリティ要件の解析に当たって思考制約を与えないと，現場の視点での抽出が容易な担当者や開発者に関するロール属性ラベルの対策が優先的に検討され，管理者の視点での検討が後回しにされることが分かった．以上のことから，システムの解析時にロールという思考制約を与えることで，そのロールに適合する視点で解析された対策が抽出され易くなると言える．ここで，本実験より抽出された対策群の例を表 3 に示す．同表に示したものは各ステークホルダの視点で抽出された対策群の一部であるが，システムの安全性とセキュリティに関する対策が抽出されていることが分かる．

[RQ2 に関する評価結果]

ドメイン知識を有する被験者IIa 群とドメイン知識を有しない被験者IIb 群の夫々が KKD と STAMP/STPA を適用し，対象システムのハザードとセキュリティ脅威を解析した．図 8 はⅡa 群とⅡb 群の被験者が抽出した対策群を対策立案部位毎に纏めたものである．対策立案部位とは，図 5 におけるコントロールもしくはフィードバックに該当し，(1～13)と共通部を加えて計 14 箇所ある．

まず，各被験者群が抽出した対策立案部の網羅率に着目すると，Ⅱa 群は 10 箇所(1,2,3,4,5,8,9,10,12,共通)から抽出しているのに対し，Ⅱb 群は 7 箇所(1,2,3,4,7,8,9)から抽出している．網羅率を計算すると，前者が 71%で後者が 50%であり，ドメインの知識を有しない被験者Ⅱb 群の抽出能力が低くみえるが，これは，STAMP/STPA の解析プロセスがコントロールアクションに対して解析を行う仕組みであることが起因している．図 5 のコントロールアクション 7 箇所(1,2,3,4,7,8,9)に限定すると，Ⅱb 群の網羅率は 100%である．一方，KKD で解析したⅡa 群は，コントロールアクションに加えてフィードバックからも対策を抽出している点で幅広い部位から抽出できることが分かった．次に，全体の抽出量に着目すると，Ⅱa 群は 33 件であるのに対して，Ⅱb 群は 51 件であり，1.5 倍多く抽出できている．特に，「QR コード読み取り」や「振替依頼」からの抽出量が多いが，被験者の解析内容を調べると STAMP/STPA の UCA を精緻に掘り下げて分析しており，ドメインの知識が少ない解析者であっても STAMP/STPA の解析プロセスにあるヒントワードを使うことで抽出する対策のバリエーションを増やすことができていた．ここで，STAMP/STPA を使った具体的な解析事例を表 4 に示す．担当者の視点にある「QR コードかざし」に関する対策は KKD によるⅡa 群の被験者からは抽出されなかったが，STAMP/STPA によるⅡb 群からは 8 件抽出された．表 4 の解析プロセスをみると，対象システムの制約として提示された「決済に要する時間は現金決済よりも速い」に対して，「利用者が認知しづらい QR コード読取り完了の表現手段を採用した」為，「QR コードの読取り完了前に，かざし動作を止めてしまう」という因果のシナリオに基づいて対策を導出できていることが分かる．STAMP/STPA のモデルベースの解析プロセスが解析者の対策抽出を助長しているものと考えられる．

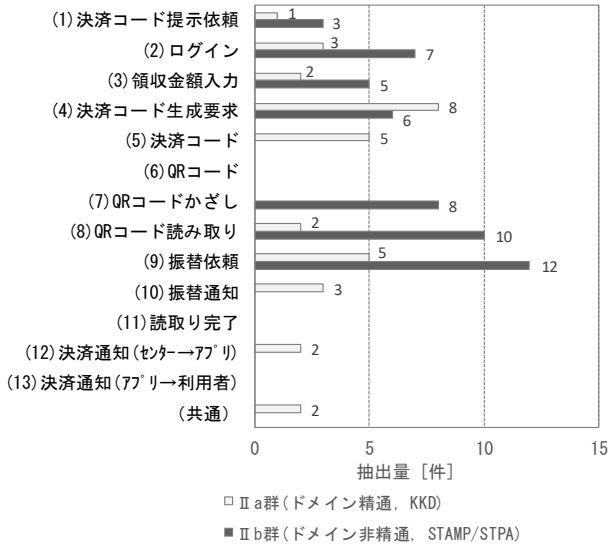

図 8 ドメイン精通度と解析手段に応じた対策抽出量

表 3 各ステークホルダの視点から抽出された対策の例

抽出された対策例	対策の種別	対策の視点
BCP（事業継続計画）の観点からディザスタリカバリ，業務継続拠点の確保を検討する．	安全性	管理者
QR コード決済レジ端末は搭載するセンサの自己診断を行い，店員に結果を提示する．	安全性	担当者
決済管理センターから時間内に振替通知を受信しなかったら，自己診断処理を起動する．	安全性	開発者
ユーザの個人情報の漏洩対策を強化する．	セキュリティ	管理者
ログインされたときは利用者に通知を送信する．	セキュリティ	担当者
決済が済んだデータはクリアする．	セキュリティ	開発者

表 4 STAMP/STPA による対策の抽出プロセス例

対策の視点	管理者	担当者	開発者
図 5 CS 該当矢印	(1) 決済コード提示依頼	(7) QR コードかざし	(8) QR コード読取り
UCA	QR コード決済の意図や行動のタイミングが伝わらず, 利用者が困惑する.	QR コードの読取り完了前に, かざし動作を止めてしまう.	当該店舗での取引と無関係の QR コードを読み取ってしまう.
違反する制約	決済に要する時間は現金決済よりも早い.	決済に要する時間は現金決済よりも速い.	決済金額を間違ってはならない.
HCF	店員から利用者に対する QR コード提示の働きかけ方が判りづらい.	利用者が認知しづらい QR コード読取り完了の表現手段を採用した.	過去に生成された QR コードがアプリ内部に保持されており, 誤使用される.
対策	接客応対に関するオペレーションの習熟をはかる. (教育活動の強化)	LED や効果音等の表現手段により, 利用者に読取り完了状態を伝える.	QR コード生成時刻等を QR コードに含め, 期限切れの場合に警告表示する.

[RQ3 に関する評価結果]

被験者 IIa 群と被験者 IIb 群の夫々が KKD と STAMP/STPA を適用し, 対象システムのハザードとセキュリティ脅威を解析した.

まず, 前処理として, 抽出された対策群の中から, 表 5 に示す 12 個の対策区分*4 に該当する KKD と STAMP/STPA の対策群に対して AGORA で用いられている満足度行列を作成した. そして, この満足度行列に基づいて「ゴール適合度」と「ステークホルダの意見対立の相関*5」を各対策について求めた. ここで, ゴール適合度とは, 満足度行列におけるユーザ企業の担当者と管理者の数値の合計値を正規化した値である. ステークホルダの意見対立の相関とは, 満足度行列における列方向の 2 系列の共分散である. 以下, 統計処理により KKD と STAMP/STPA のサンプルに有意な差が無いことを検証した結果を述べる. 検証のゴールは, 各サンプルの母集団が正規分布に従っていると仮定した上で, KKD と STAMP/STPA から得られた系列の母集団に差が無いという帰無仮説が正しいことを t 検定により確認することである. 少数サンプルの検定では系列群の等分散性と観測者の独立性が重要なので, F 検定の計算値により等分散性を判断し*6, 被験者が所属する産業分野以外の因子(会社, 役職, 業務, 年齢等)が異なることを確認することで独立性を判断してある.

STAMP [#1-#12]と KKD [#1-#6]*7について t 検定を実施した結果, ゴール適合度については検定統計量が 0.17(＞0.05), 意見対立の相関については検定統計量が 0.10(＞0.05)となり, いずれも KKD と STAMP/STPA の2つのサンプルに有意な差が無いことが確認された. 一方, 被験者Ⅱb 群のみが抽出した STAMP [#7-#12]と KKD [#1-#6]でt検定を行うと, 2つのサンプルに有意な差があることが確認された. このことから, Ⅱb 群が抽出した対策群の全体では, ドメイン知識を十分に有しなくても STAMP/STPA を用いることで, 有識者が経験と勘で解析した結果に近い質(目的合理性)の対策群(安全性・セキュリティ要件)を獲得できる場合もあるが, ドメインの知識量が少ない解析者が関わると成立しない可能性があると言える.

具体的に, Ⅱb 群の被験者が STAMP[#7-#12]で抽出した対策群のひとつを確認してみると, 「#7 店舗口座設定は, 郵送(簡易書留)で行う」(ゴール適合度: -4.67, 意見対立の相関: 58.33)というものがある. Enterprise システム開発に精通した技術者の視点で判断すると, #7 の対策にはシステム運用時のコストや煩雑さに課題があると推

*4 対策区分は, 対策立案部から抽出された対策の視点から分類したものである.

*5 満足度行列における列方向の「評価の視点」の2つの系列(対策立案者の系列と, それとは分散値が最も離れているもうひとつの系列)の共分散である. 計算値が大きい場合, 各ステークホルダで該当要件に対する満足度が対立している状態になる.

*6 F 検定(片側確率)の結果, ゴール適合度については 0.11(＞0.05)で等分散が確認されたが, 意見対立の相関については 0.04 (＜0.05) で等分散性が確認されなかった. 従って, 後者については Welch の t 検定を用いた.

*7 Ⅱa 群の被験者は, 対策区分#7-#12 に該当するものを抽出しなかった為, 表 5 に数値が入っていない.

表 5 各対策の評価値(左:ゴール適合度, 右:意見対立の相関)

ゴール適合度

#	対策区分	STAMP	KKD
1	認証機能	6.67	6.83
2	認証機能②	5.00	3.67
3	金額確認	6.17	6.33
4	店舗確認	3.17	3.50
5	QR ｺｰﾄﾞ改竄・破損ﾁｪｯｸ	3.50	3.67
6	性能向上	7.17	7.33
7	店舗登録	-4.67	-
8	店舗登録②	0.67	-
9	誤操作防止	2.83	-
10	誤操作防止②	2.67	-
11	障害対策	2.83	-
12	障害対策②	2.67	-
	平均	3.22	5.22
	分散	9.91	3.22

意見対立の相関

#	対策区分	STAMP	KKD
1	認証機能	8.00	6.33
2	認証機能②	6.00	6.50
3	金額確認	10.00	10.00
4	店舗確認	13.00	23.00
5	QR ｺｰﾄﾞ改竄・破損ﾁｪｯｸ	1.33	1.33
6	性能向上	1.00	1.00
7	店舗登録	58.33	-
8	店舗登録②	39.00	-
9	誤操作防止	35.17	-
10	誤操作防止②	11.00	-
11	障害対策	9.67	-
12	障害対策②	35.33	-
	平均	18.99	8.03
	分散	333.59	65.49

察されるが, Ⅲ群の(管理者ロールの)評価者についても各ステークホルダの視点で満足度行列に-10pt.の素点を 3 つ付与しており, システムの安全性・セキュリティ要件の質(目的合理性)を低下させ, 意見対立の相関を高めた.

6. 考察

6.1. 得られた知見

[研究設問に対する評価]

5.2 節に示す評価結果によれば, 解析者に異なるロールを与えて多様な視点でシステムのハザードとセキュリティ脅威を解析すれば, 獲得できる安全性・セキュリティ要件の多様性が増し(RQ1), さらにシステムの解析手段として SSMS 法を適用することで量と質(目的合理性)の点で有識者が抽出したものに近い安全性・セキュリティ要件が条件付きで得られることが分かった(RQ2, RQ3).

ここでの「条件」とは, システム解析者のドメイン知識の量や業務経験に関するもので, RQ3 に関する評価結果で述べたとおり, 対象システムの開発に精通していない解析者が SSMS 法を使用するとプロジェクトの QCD の点で有識者が暗黙知で除外するようなシステム要件を抽出する可能性があることから, SSMS 法を効果的に適用するのであれば, 解析者のドメイン知識を一定水準以上に揃えることが望ましい.

[提案手法の改良案]

今回, SSMS 法では, STAMP/STPA のようなモデルベースのシステム解析手法をベースに AGORA で利用されている満足度行列を用いて要件の質(目的合理性)と意見対立の相関を検証する手法を提案した. 5.2 節の実験では, STAMP/STPA は特定の対策立案部(領域)を深掘りして抜けのない対策抽出ができる一方で, KKD のように幅広い領域で万遍なく対策を抽出することが弱い課題が確認された. そこで SSMS 法の改良案として, 図 4 に示すプロセスモデルの「コントロールストラクチャの構築」の後に, 前段でロールありの KKD で対策を抽出してから, 後段でロールありの STAMP/STPA で対策を抽出するような仕組みを作れば, KKD と STAMP/STPA の両者の強みを併合できるのではないかと考えている.

6.2. 妥当性への脅威

[内的妥当性への脅威]

RQ3 に関する実験の検証で用いたサンプル数は計 18 個であるため, 統計処理を行う上で必ずしも十分とは言えない. ただし, 検定では母集団に有意な差が無いことを示す上で, 等分散性と観測値の独立性に配慮した.

[外的妥当性への脅威]

今回の実験はひとつのドメインに対して実施したものであるため, 手法の汎用性を示すためには異なるドメインでの実験が必要である.

7. まとめ

7.1. 成果

本研究ではステークホルダの視点を STAMP/STPA に導入し, SSMS 法としてモデルを構築することで, 解析者がドメインの知識を十分に有しなくてもハザードと脅威に対する対策群を実用的な量で獲得し, これらを要件の満足度に関する評価指標で定量化できることを示した. 本報告では Enterprise システムを例に挙げその有効性を評価したが, SSMS 法は STAMP/STPA が持つ汎用性を活かしながらプロセスモデルを拡張してあるので, 制御系が含まれる AI/IoT システムにも適用可能であると考える. 今後, 複雑化する先進システムの開発で STAMP/STPA が展開されていく際に, 多様なステークホルダの視点を用いたシステム安全性解析の考え方が取り込まれ, 解析の視点の抜け漏れ防止に繋がることを期待したい.

7.2. 将来への発展

・SSMS 法では, 前段で解析したハザードの深刻度(リスク)を抽出された対策群の評価にフィードバックしていない. ゴール指向要求分析で使われる指標に加え, リスクを考慮しながら総合的に対策群の良し悪しを判断する仕組みを考慮できるとよい.
・SSMS 法では, STAMP/STPA の解析時にステークホルダの視点を導入しているが, コントロールストラクチャを作成する段階から多様な視点を導入すると, 獲得される安全性・セキュリティ要件の多様性が更に増大する可能性がある.
・情報セキュリティの学術領域ではリスクコミュニケーションを考慮した定量分析が提案されている[11][12]. SSMS 法に本領域の知見を融合すると, モデルを精緻化できる可能性がある.

8. 謝辞

本研究は, 日本科学技術連盟 2019 年度 ソフトウェア品質管理研究会 研究コース 5(分科会:仕様と要求のエンジニアリング)の中で取り組んだ内容です. 所属分科会の荒木啓二郎アドバイザーには, 多方面にわたり御指導を賜りました. また, 研究コース 5 の研究員の皆様, オムロン株式会社の紺田隆一郎氏, 古賀純平氏には実験に御協力を頂きました. 関係者の皆様に厚く御礼申し上げます.

参考文献

[1] システム構築上流工程強化部会 システム化要求 WG, ユーザのための要件定義ガイド 第 2 版, 情報処理推進機構 社会基盤センター(2019)
[2] Nancy G. Leveson, “Engineering a Safer World – Systems Thinking Applied to Safety”, The MIT Press (2011)
[3] 柳原靖司, 吉田邦雄, 栗田太郎, 石川冬樹, 多様なステークホルダの視点を STAMP/STPA に導入する試み, AI/IoT システムのための安全性シンポジウム(2019)
[4] 海谷治彦, 佐伯元司, 海尻賢二, 属性つきゴール指向要求分析法, 電子情報通信学会技術研究報告. SS, ソフトウェアサイエンス 101(673)(2002)
[5] William Young, Reed Porada, System-Theoretic Process Analysis for Security (STPA-SEC):Cyber Security and STPA, STAMP 2017 Conference(2017)
[6] 金子朋子, 髙橋雄志, 大久保隆夫, 勅使河原可海, 佐々木良一, 安全解析手法 STAMP/STPA に対するセキュリティ視点からの脅威分析の拡張提案, コンピュータセキュリティシンポジウム(2017)
[7] John Mylopoulos, Lawrence Chung, Brian Nixon, Representing and Using Nonfunctional Requirements: A Process-Oriented Approach, IEEE Transactions on Software Engineering, Vol.18 No.6 pp.483-497(1992)
[8] SCSC Assurance Case Working Group, Goal Structuring Notation Community Standard Version 2, https://scsc.uk/publications (2020 年 4 月 30 日)
[9] 新原敦介, 河野仁一, 海谷治彦, 佐伯 元司, ゴール指向要求分析を用いたステークホルダの対立の検出, 情報処理学会研究会報告, Vol. 2004, No. 30, pp.99-106(2004)
[10] 佐藤慎一, 石川冬樹, 猪原健弘, 貢献度と顧客のニーズに関する妥当性の間のコンフリクト検出指標, ソフトウェアエンジニアリングシンポジウム(2011)
[11] 佐々木良一, 石井真之, 日高悠, 矢島敬士, 吉浦裕, 村山優子, 多重リスクコミュニケータの開発構想と試適用, 情報処理学会論文誌, Vol.46, No.8, pp.2120-2128(2005)
[12] 佐々木良一, 日高悠, 守谷 隆史, 谷山充洋, 矢島敬士, 八重樫清美, 川島泰正, 吉浦裕, 多重リスクコミュニケータの開発と適用, 情報処理学会論文誌, Vol.49, No.9, pp.3180-3190(2008)