研究コース５（チーム GOBIT）

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

研 究 員：柳原　靖司　（ブラザー工業株式会社）
吉田　邦雄　（オムロン株式会社）

研究概要

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，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．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，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[2]．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．システム開発の要求分析や要件定義において考慮されるべき，多様なステークホルダ間の合意形成を促進する上で,次世代システム安全性解析手法である STAMP/STPA に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[3] (Attributed Goal-Oriented Requirements Analysis Method) について述べる．

3.1 STAMP/STPA

STAMP/STPA では，システムの構成要素を図 1 に示すようなコントロールストラクチャ（CS: Control Structure）でモデル化し，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）を特定しながら安全制約を逸脱するハザード要因（HCF: Hazard Causal Factor）を解析する手順をとる．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.当初の STAMP/STPA 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，セキュリティの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た[4][5].

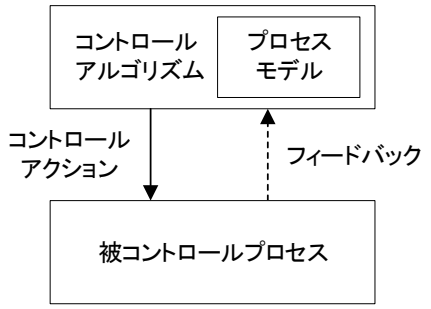

図 1　STAMP/STPA CS の例

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[6]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．

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 2 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,ステークホルダ間でどの要件を採用するべきか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二つの指標で定量化する．要件の質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．

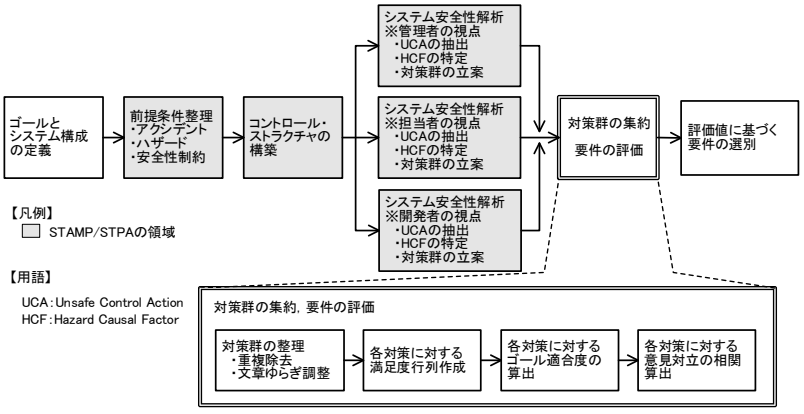

図 2　SSMS 法のプロセスモデル

4.2 SSMS 法の解析手順

図 2 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．
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 STAMP/STPA を適用することで，多様な視点で安全性・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 STAMP/STPA 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 STAMP/STPA 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 3 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．

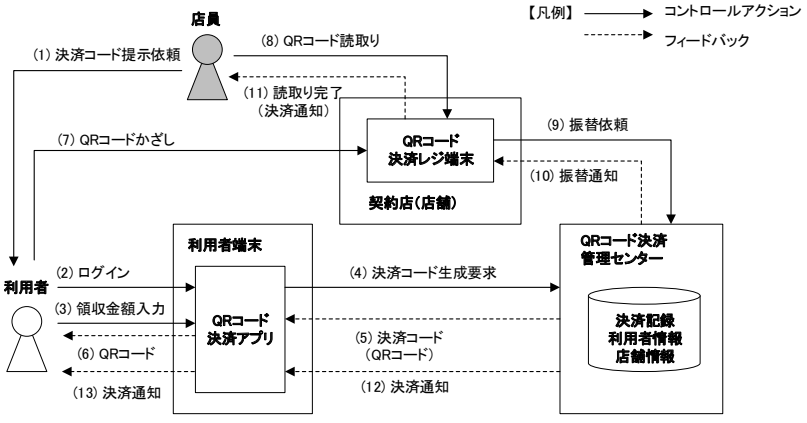

図 3　仮想 QR コード決済システム（STAMP/STPA の CS)

今回，対象システムの解析を実施するに当たり，第三者の被験者 Ⅰ群，Ⅱ群（Ⅱa 群，Ⅱb 群），Ⅲ群を用意した（表 1）．各被験者は独立で，夫々，以下のような役割と前提条件を持つ．なお，Ⅱb 群に属する被験者は車載システム開発に精通しているが，Enterprise システムには精通していない．

表 1　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

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群が対象システムのハザードとセキュリティ脅威の解析をした結果を，特定ロールを与えた被験者Ⅱ群の解析結果と比較した．図 4 に示すように，ロールを付与しないで解析した場合には，抽出された対策群（安全性・セキュリティ要件）の 95%がベンダの開発者若しくはユーザ企業の担当者の視点に分類された．他方，特定ロールを付与して解析した場合には，63%がそれに該当した．この結果より，明示的にロールを与えないでシステムを解析すると，抽出される対策群の視点に偏りが生じることが分かった．なお，被験者に対するインタビューの結果，実際の役職が管理職であっても，システム解析に当たって思考制約を与えないと，立案難度が高い管理者の視点に分類される対策の検討が後回しにされることも分かった．具体例として，本実験において各ロールを意識しながら STAMP/STPA で抽出した対策内容を表 2 に示す．解析過程を検証すると，人とシステムの相互作用に関わる解析が行われている．

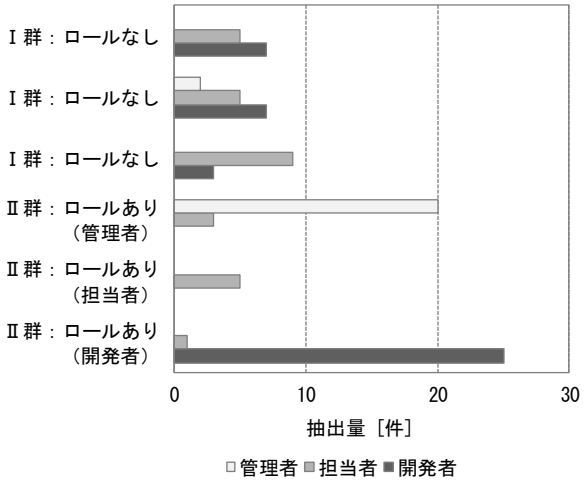

図 4　抽出された対策群のロール分類結果

表 2　多様な視点から抽出された対策の例（解析手段：STAMP/STPA）

対策の視点	管理者	担当者	開発者
図 3 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早い．	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．

[RQ2 に関する評価結果]

被験者Ⅱa 群と被験者Ⅱb 群の夫々が KKD（解析者の経験と勘から対策を見つける手段）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．解析結果である対策群を対策立案部毎に集計したものを図 5 に示す．図 5 からは２つのことが確認された．第一に KKD を用いた被験者Ⅱa 群の方が STAMP/STPA を用いた被験者Ⅱb 群に比べ対策立案部の網羅率が 1.6 倍高いが，対策群の抽出範囲が特定ロール(管理者)に偏っている．第二に，STAMP/STPA を用いた被験者Ⅱb 群の対策抽出量（51 個）は KKD を用いたⅡa 群の抽出量（33 個）に対して 1.5 倍多く，抽出量が特定ロールに偏っていない．これらの結果より，ドメイン知識を十分に有しなくても STAMP/STPA を用いれば,各ロールの抽出量のばらつきを抑えながら KKD 同等量以上の対策群（安全性・セキュリティ要件）を獲得できることが分かった．

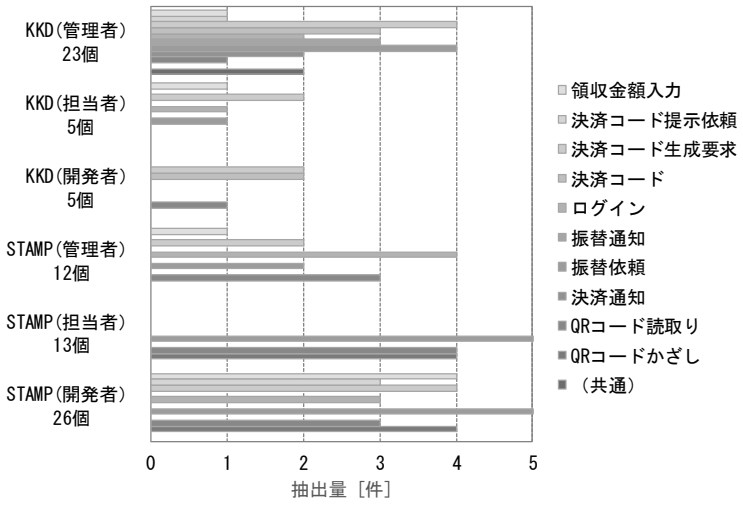

図 5　対策立案部位毎の抽出量（被験者毎）

[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 3 に示す 12 個の対策区分[a]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，この満足度行列からゴール適合度とステークホルダの意見対立の相関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（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．以下，STAMP と KKD のサンプルを統計処理により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[b]，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．

t 検定の結果，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 STAMP と KKD の２つのサンプルに有意な差が無いことが確認された．このことからドメイン知識を十分に有しなくても STAMP/STPA を用いれば，有識者が経験と勘で解析した結果に近い質の対策群（安全性・セキュリティ要件）を獲得できることが分かった．

---

a) 対策区分は，対策立案部をグループ化したもの．今回のサンプル解析では，ひとつの対策区分に複数の対策が含まれているものを対象とした．

b) F 検定（片側確率）の結果，ゴール適合度については 0.08（＞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．

表 3　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

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 STAMP/STPA を適用することで対象システムのドメイン知識を十分に有しなくても量と質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得られることが分かった（RQ2，RQ3)．

[仮説に対する整合性]

我々が立てた仮説のうち，「多様なステークホルダの視点を STAMP/STPA に導入してハザードとセキュリティ脅威に対する対策群を抽出した後，ゴール指向で分析すれば，客観的かつ系統的に安全性･セキュリティ要件を獲得できる」という点は妥当性を確認できたが，「合意形成されやすい要件を獲得できる」という点は必ずしも示せていない．表 3「意見対立の相関」の KKD で得られた数値を確認すると，有識者が経験と勘で抽出した対策群の中にも意見の対立が大きいものが#4 に含まれており，ステークホルダ間で合意形成が難しい要件が抽出されることがある．従って，多様な視点を入れて STAMP/STPA で解析しても，抽出された要件が合意形成されやすいとは言えない．

[提案手法の改良案]

社会学や感性工学の点から合意形成を取り扱った研究によれば，人の判断や意見は十分な一貫性がなく，同じ選択肢でも表現や状況の違いにより意思決定が変化すると述べられている．最適化問題として扱うのではなく，コミュニケーションを通して選択肢を選ぶ過程の共有が重要であるとも述べられている[7]．本知見を考慮し，SSMS 法のプロセスモデルの後段にステークホルダが議論をしながら要件に対する評価を繰り返し，満足度行列のばらつきを収斂させる手続きを追加することで，合意形成を促進できると考えられる．

6.2 妥当性への脅威

今回の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，観測値の独立性に配慮した．また，本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[8]．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

荒木啓二郎アドバイザー，栗田太郎主査，石川冬樹副主査には，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．

9. 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] 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）
[3] 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）
[4] William Young，Reed Porada，System-Theoretic Process Analysis for Security (STPA-SEC):Cyber Security and STPA，STAMP 2017 Conference（2017）
[5] 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）
[6] 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）
[7] 浜田百合，庄司裕子，合意形成プロセスの成功パターンの特徴分析に関する研究，日本感性工学会論文誌，Vol.16 No.1 pp.43-50（2017）
[8] 佐々木良一他，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）