STAMP S&S～システム理論によるセーフティ・セキュリティ統合リスク分析

金子朋子[†1†4] 髙橋雄志[†2] 林浩史[†2] 吉岡信和[†4] 大久保隆夫[†3] 佐々木良一[†2]

概要： IoT 時代の複雑なシステムに対する新たな安全性解析手法として注目を集めている理論とその安全分析手法に STAMP（System Theoretic Accident Model and Processes）と STPA（System Theoretic Process Analysis） がある．本稿では STAMP/STPA によるセーフティとセキュリティ統合視点でのリスク分析とその有効性を提示する．具体的には従来手法と比較の上，STAMP をベースとしたセーフティとセキュリティのリスク分析の枠組みを検討する．さらに自動運転レベル 3 の事例において実験を行った結果と効果の考察を行う．

キーワード: STAMP/STPA，セーフティ・セキュリティ，システム理論，STPA-SafeSec

STAMP S&S～Safety and Security Integrated Risk Analysis based on System Theory

KANEKO TOMOKO[†1†4] TAKAHASHI YUJI[†2] HIROSHI HAYASHI[†2]
NOBUKAZU YOSHIOKA[†4] TAKAO OKUBO[†3] RYOICHI SASAKI [†2]

Abstract:
STAMP (System Theoretic Accident Model and Processes) and its safety analysis application, STPA (System Theoretic Process Analysis) have attracted much attention as a new safety analysis method for complex systems of IoT. This paper presents risk analysis from safety and security integration viewpoint by STAMP/STPA and its effectiveness. Specifically, the framework of risk analysis of safety and security based on STAMP is considered in comparison with the conventional method. In addition, we will discuss the results and effects of experiments conducted in the case of level 3 automatic operation.

Keywords: STAMP, STPA, Safety･Security, System Theory, STPA-SafeSec

1. †はじめに

IoT 時代には相互につながるシステムへの脅威に対して，安全な機器，システムを開発することが必要とされる．そのためには，従来の情報セキュリティ上の機密性と完全性と可用性に加え，安全性の視点が必要になる．そこで筆者らは安全の視点でリスク分析を行うために IoT 時代の複雑なシステムに対して相互作用に着目した事故モデルである STAMP（System Theoretic Accident Model and Processes）[1][2]とそのハザード分析手法である STPA （System Theoretic Process Analysis） [3][4]に着目し，セーフティとセキュリティを統合的な分析を示す．STAMP/STPA はセーフティを中心に展開されてきたが，セキュリティ上のリスク分析にも適用可能性が示されており[4]，STPA のセキュリティ対応手法である STPA-Sec も提案されている[5][6]．さらにセーフティとセキュリティの脆弱性に着目した STPA の拡張である STPA-SafeSec も提案されている[7][8].

ハザードに相当するセキュリティの状態は脅威であるが，従来の STAMP ベースのセキュリティ分析手法である STAMP-STPA-Sec はビジネスレベルの問題分析が中心であり，脅威分析が具体化されていない．またもう１つのセキュリティ分析手法である STPA-SafeSec は物理層に対する脆弱性分析が中心で，上流工程からのセキュリティ分析ができない.

しかし相互作用に着目した STAMP の特長をいかし脅威をセキュリティ属性別に網羅的に識別するためにはさらな

†1(株)NTT データ NTTDATA Corporation
†2 東京電機大学 TOKYO DENKI UNIVERSITY
†3 情報セキュリティ大学院大学 INSTITUTE of INFORMATION SECURITY
†4 国立情報学研究所 National Institute of Informatics

る工夫が要ると筆者らは考えている．そこで STAMP モデルを使って STPA の手順に従いつつ，セキュリティの脅威に着目した方法を提案し，セーフティとセキュリティを企画・要求段階から同時に分析できる手法を提示する．さらにそのフレームワークに対して適用評価を行った．そこで本稿では STAMP セーフティとセキュリティの枠組みを提示（リスク＝脆弱性×脅威に基づく）した上で，STAMP ベースのモデリングによる脅威分析の具体化を図る．さらにこのフレームワークにもとづく実験結果による効果を提示する．自動運転のブレーキシステムにセーフティとセキュリティ統合フレームワークを適用して実施した実験結果とその適用評価を提示する。

なお，筆者らはシステム理論に基づく安全性，リスク，事故分析などの様々な分析手法を STAMP S&S と呼称する．S&S とは，Safety, Security の他，System, Software, Service, Society 等の略称を指す．この略称を併記する理由は多様な機器やシステムだけでなく，人や組織など多様なコンポーネントの相互作用を分析できる STAMP の適用範囲の広さをベースにしているからである. STAMP S&S は STAMP の各種分析方法等をより広範囲に異なる観点で適用することで STAMP の可能性を引き出し，その領域や観点で適用した場合の課題を明確化しつつ効果をうむための調整を図り，その具体的な適用方法を確立することを目的としている．STAMP S&S は様々な適用範囲がありうるが，本稿ではセーフティとセキュリティ統合の方法を示し,その適用検証を実施する．

本稿は 2 章で STAMP と各種ハザード手法，セキュリティ要求分析に関連した技術と考え方を紹介する．続く 3 章は STPA のセキュリティ対応手法である STPA-Sec と STPA-SafeSec の説明とその課題を示し, 各手法の比較の観点を説明したうえで STPA への脅威モデリングの適用方法を述べ，セキュリティ・バイ・デザインを実現するセーフティとセキュリティ統合のフレームワークとしての STAMP S&S を提示する．4 章では自動運転に適用した実験概要を説明し，5 章では提案方式に関する考察とフレームワークの有効性評価を行う．6 章で今後の方針，7 章でまとめについて述べる．

2. 関連研究

2.1 STAMP と関連手法

STAMP とはシステム理論に基づく事故モデルであり，STPA は STAMP モデルにもとづく代表的な手法として，ハザード分析を行うものである．前提として，システム事故の多くは，構成要素の故障ではなく，システムの中で安全のための制御を行う要素（制御要素と被制御要素）の相互作用が働かない事によって起きるとし，「要素（コンポーネント）」と「相互作用（コントロールアクション）」に着目してメカニズムを説明し，「アクションが働かない原因」が「コントロールアクションの不適切な作用」に等しいという視点を持つことで原因を有限化している．

STAMP に基づく分析の道具立てプロセスとして，仕様記述，安全性ガイド設計，設計原理などのシステム工学，リスク管理の運用，管理の原則／組織設計の規制を利用する．ツール（手法）には STAMP モデルに基づき，事故／イベント分析（CAST: Causal Analysis based on STAMP），ハザード分析（STPA），早期概念分析（STECA: Systems-Theoretic Early Concept Analysis），組織的／文化的リスク分析，先行指標識別，セキュリティ分析（STPA-Sec）が提示されている．事故／イベント分析（CAST）は事故が起きてからイベントとして分析する手法，STPA-SEC はそのセキュリティ版である．セーフティとセキュリティを統合する手法としては STPA-SafeSec が提案されている[7][8]．また，脅威分析のコントロールストラクチャー(以下，CS)に STRIDE を適用した事例[9]やハザード分析としてのセーフティ・セキュリティ統合の手法[10]なども提案されている．

2.2 ハザード分析手法

FTA（Fault Tree Analysis），FMEA（Failure Mode and Effect Analysis）は，フォールトツリー図や影響分析表を用いてハザード要因を分析する伝統的なハザード分析手法である．システムの構成要素と故障モードが決まるアーキテクチャ設計の段階から適用できる．機器や組織の単一故障をハザード要因として識別する分岐条件を論理的に組むことで網羅的に分析できる特徴をもつが，深く分析できる反面，構成要素間の相互作用から発生するアクシデントといった全体的な視野を必要とする分析が難しい．

STPA は STAMP モデルに基づき，安全制約の実現に関係するコンポ―ネントとその相互作用を制御構造図にした CS とコントロールループ図を用いてハザード要因を分析する安全解析手法である．システムの大まかな構成要素が決まる概念設計の段階から適用できる．複数の機器や組織（人間）が，相互作用を行う複雑なシステムにおいて，相互作用に潜むハザード要因を識別する特徴をもち，過去のアクシデント事例データに基づくガイドワードにより分析する．またシステム全体の振る舞いを確認しながら分析できる．

2.3 セキュリティ分析の手法と種類

セキュリティ分析手法にはアタックツリー[11][12]，ミスユースケース[13]，マイクロソフトのセキュリティ開発ライフサイクル[14]，S(なりすまし)，T(改ざん)，R(否認)，I(情報の暴露)，D(サービス不能)，E(権限の昇格)による STRIDE 分析を含む脅威モデリング[15] [16] [17]などがある．セキュリティ開発ライフサイクル[14]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．また STRIDE を元にした Threat Tree 分類[15]も示されている．ただし，安全解析における FTA，FMEA 等の

ように歴史があり，標準化もなされたセキュリティ分析手法は存在せず，開発現場でも普及した設計手法は定まっていないのが現状である．

システムなどに脆弱性が内在し、それを突く脅威にさらされることでセキュリティ・リスクが顕在化するため，セキュリティ分析は脆弱性分析と脅威分析に大別される．脅威は攻撃者が起こすものであり，攻撃者は脆弱性を探し悪用され，脅かされる資産はさまざまである．

3. STPA のセーフティとセキュリティ対応

3.1 STPA-Sec とその課題

ハザード分析手法 STPA のセキュリティ拡張版である STPA-Sec は，セキュリティ上の脅威抽出に必要な分析の視点が追加される．要因の特定に関して「コントローラーなどに悪意ある，権限を持たない，部分的なインプット」が STPA のヒントワードに加わり，追加的に分析される．

なお，現在の STPA-Sec はミッション・ビジネス運用とシステム脆弱性に焦点を当てて，ハザード分析を行うものが公開されているだけで，システマチックな脅威分析を実施する手順や事例は公開されていない．MIT の事例[6]をみても非安全なコントロールアクションに対して，セキュリティ制約をどうやって，導き出すかの手法が提示されていない．また，STPA 分析手順の要因分析段階である Step2 では，要因のシナリオを導き出す際にセキュリティ要因の必要十分性を説明できないのが現状である．セキュリティ要因の洗い出しは，ハザード要因分析のヒントワードに部分的,悪い形状の情報オペレーションを追加しただけである．なぜ，セキュリティ要因の洗い出しのこれらの追加がなされたのかの説明がなされていない．筆者らは本来，セキュリティ誘発要因（SCF）には，悪意ある者の攻撃にもとづいた脅威分析が必要であると考えた．

3.2 STPA-SafeSec とその課題

STPA-SafeSec[7][8]は安全性と脆弱性を統合して分析できる STPA の拡張である．

STPA-SafeSec はセーフティとセキュリティ対策を統合できる枠組みを主張している．それは機能 CSD（Control Structure Diagram）と物理 CSD の二つの CSD を利用，Step2 で使用する HCF ヒントのセキュリティへの拡張という特徴とその派生効果による [8]．しかしながら 2 つの CSD のうち，下位レイヤでしかセキュリティの要因分析を行わない.また STPA-SafeSec では採用されているセキュリティに係る HCF ヒントとは，物理 CSD においてのセキュリティ上の既知の脆弱性を利用するものである．これは分析対象に存在する脆弱性を考慮するやり方である．

個別の機器，ソフトウェアに対するセキュリティ上の脆弱性は数も多く，絶えず変化するものである．また，どのような攻撃に対してその脆弱性が脅威になるのかを明確化しないと，設計への指針レベルでの対策が立てづらい．攻撃による脅威を明確化した上での網羅的な要因分析になりづらい. これでは､潜在的な脅威を洗いだしに限界がある．つまりこの形式での統合はセーフティ中心の統合であり、セキュリティの上流工程からの作りこみができていないと考える．

3.3 STAMP S&S（Safety & Security）方式

今後重要となる IoT システムは，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捉える必要がある．そのためセーフティとセキュリティを共に分析できることは必要であり，どの工程段階でもセーフティとセキュリティを考慮する網羅性が望まれている．特にコスト面での影響を抑えるためには初期段階である企画・要件定義工程から安全を作りこむことが求められている．

STAMP/STPA は物理システムのセーフティ分析手法として, 上記の必要性を満たすものである. STAMP/STPA-Sec はこのセキュリティ拡張版だが，前述のようにサイバーセキュリティ分析における悪意ある者の攻撃にもとづいた脅威分析が不十分である．そこで，筆者らは攻撃者の意図を踏まえた脅威洗い出しができる STPA-Sec とは異なる新たなヒントワードを定義し，脅威分析を STPA-Sec の手順に追加する方式を提案してきた[15] [16] [17]. 具体的には代表的な脅威分析モデルである Microsoft 社の STRIDE を非安全なコントロールアクションに対するセキュリティ制約，セキュリティ要因を洗い出す STPA-Sec（Step2）の段階に組み入れている．

以下の 3 つ条件を満たしていることを示し，適用評価とする．①企画・要件定義工程からセーフティとセキュリティの分析ができる．②セーフティの分析として人の生命・健康に関わるハザードとその要因が多く抽出できている．③セキュリティの分析として脅威が多く抽出できている．

4. 比較実験

4.1. 実験概要

実験の目的は，初期段階である企画・要件定義工程からセーフティとセキュリティの双方を作りこむことが可能であるかの検証である．

本稿での提案手法 STAMP S&S は STAMP のセキュリティとして STRIDE によって脅威分析を詳細化したうえでセーフティとセキュリティの統合分析を実施する．この効果を評価するため，STRIDE の適用を試行した実験 1[18]と特に何も手法を利用しない従来方式と STPA と STPA-Sec に STRIDE を追加した STAMP S&S の 2 つの方式を比較した実験 2[19]を実施してきた．なお，STPA-SafeSec は 3.2 節に示したようにセーフィティ中心の分析であり，上流工程からの作りこみができていないため，初期段階である企画・要件定義工程からセーフティとセキュリティの双方を作りこみという実験の目的に適していないため，検証の対象としない．

4.2. 実験 1 の概要と結果

実験 1[18]はセーフティとセキュリティ両面のリスクを分析し検証できる手法として，STAMP/STPA を STRIDE のヒントワードで拡張する方法を提案した。事例として自動車の自動運転に焦点を当て，脅威分析から検証の一連の流れを作成した．特に脅威分析に関しては STEP2 において，STAMP/STPA-Sec のヒントワードと STRIDE をヒントワードとする脅威分析の 2 種類の試行を実施した．その結果，STPA-Sec のヒントワードでは，1 件のセキュリティ要因の抽出にとどまったが，STRIDE をヒントワードとして拡張することで，33 件のセキュリティ要因が抽出できた．特に STRIDE 要素であるなりすましや権限の昇格から導出したセキュリティ要因は権限設計に活かすことができると考えるので有用である．また，CS にデータの流れやデータストアを記載することによって，STRIDE によるセキュリティ要因の抽出がより容易になった．

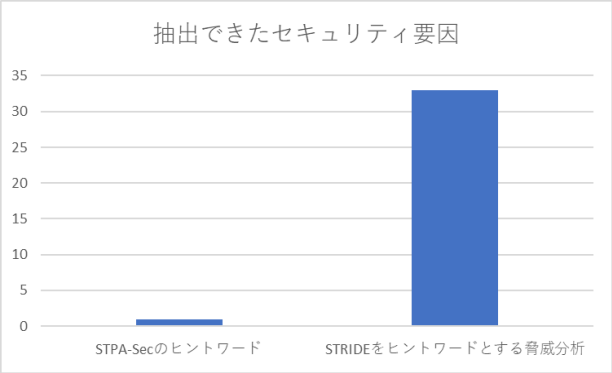

図 1 抽出できたセキュリティ要因数

4.3. 実験 2 の概要と結果

質問紙調査によって自動車の専門家ではない被験者を STAMP/STPA を知らない被験者グループ A と STAMP/STPA を知っている被験者グループ B に分けた．今回 STAMP/STPA を知っている被験者グループ B は数時間から数日程度学習はしたが，実務では実施していない STAMP/STPA の初心者である．

30 名の被験者に質問紙調査を行った．問 1 と問 2 の結果を

表 1 に示す．このうち問 1 並びに問 2 の回答が共に「はい」となった被験者グループ B は 6 名であり，この 6 名が STAMP を用いた分析を実施した．それ以外のうち問 1 問 2 の回答が共に「いいえ」となった被験者グループ A の 22 名が STAMP を用いない分析を実施した．

表 1 質問紙調査: 問 1 と問 2 への回答結果

		問 1	
		はい	いいえ
問 2	はい	6 名	1 名
	いいえ	1 名	22 名

問 3: 1 人当たりのリスク件数は STAMP を用いた分析では 70.7 件, STAMP を用いない分析では 6.1 件であった．
問 4: 1 人当たりのリスク対策の件数は STAMP を用いた分析では 33.0 件，STAMP を用いない分析では 4.1 件であった（表 2）．

表 2 被験者 1 人当たりのリスク件数

	STAMP を用いた分析	STAMP を用いない分析
平均（件数）	70.7	6.1

質問紙調査の回答で得られたリスクについてそのリスクがセーフティまたはセキュリティのどちらに基づくリスクであるか(図 2)，また，リスクに対する対策の有無（表 3）を示す．

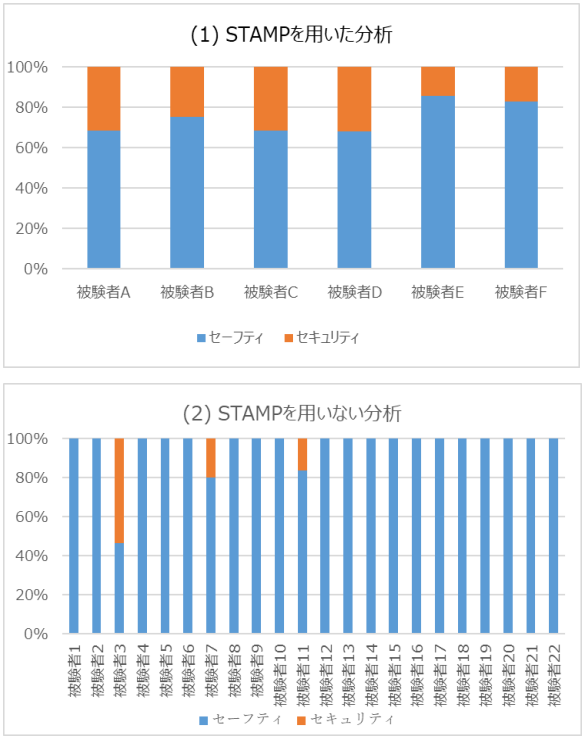

図 2 抽出したリスクのセーフティ/セキュリティの割合

表 3 抽出リスクの対策の有無

	STAMP を用いた分析		STAMP を用いない分析	
	対策あり	対策なし	対策あり	対策なし
平均（件数）	63.8	6.8	4.4	1.7
平均（%）	90.3%	9.7%	79.4%	20.6%

抽出したセキュリティ，セーフティのリスク図 3，**図** 4，図 5 に示すようにグループで分類を行った．

また，被験者グループ B の STAMP を用いた分析を行った際に作成された CS の 1 つを図 5 に示す．

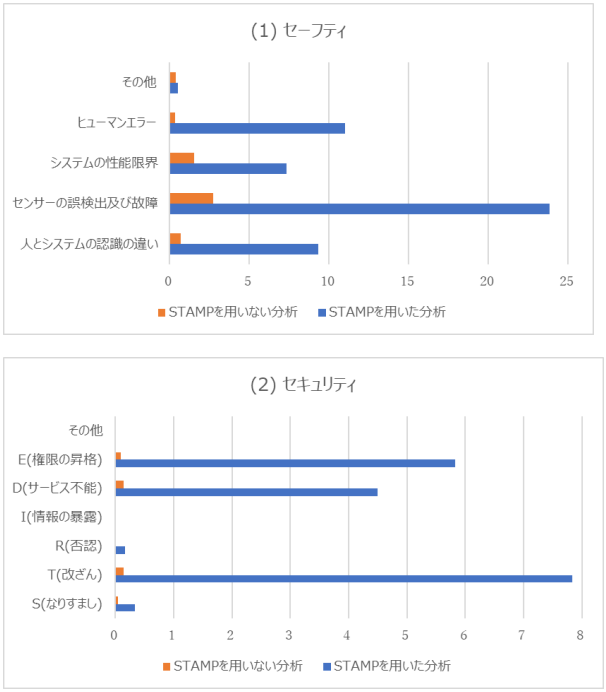

図 3 被験者 1 人当たりのリスク件数の内訳

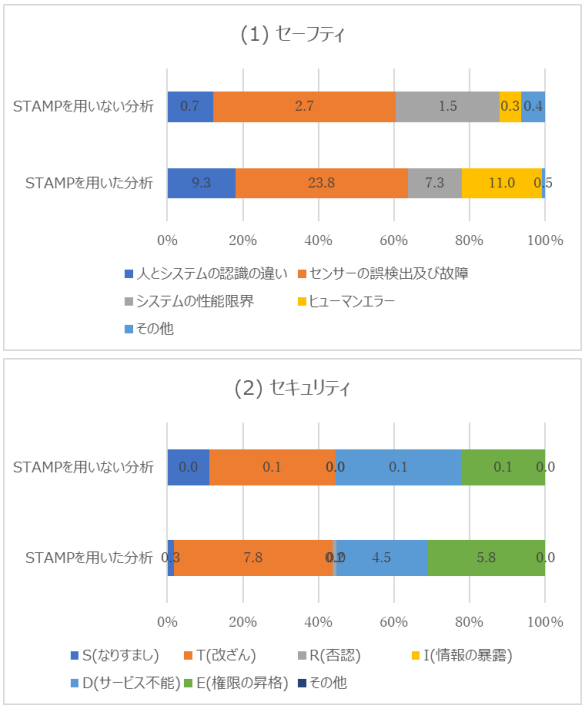

図 4 被験者一人当たりのリスクの割合

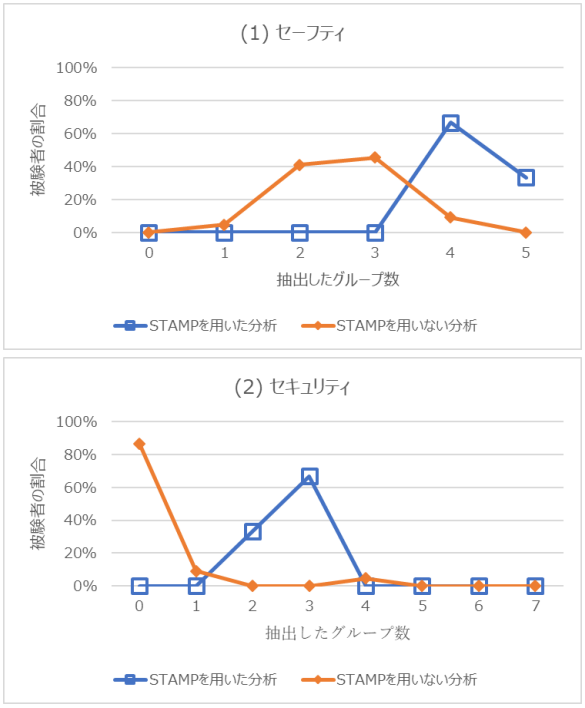

図 5 抽出したグループ数ごとの被験者の割合

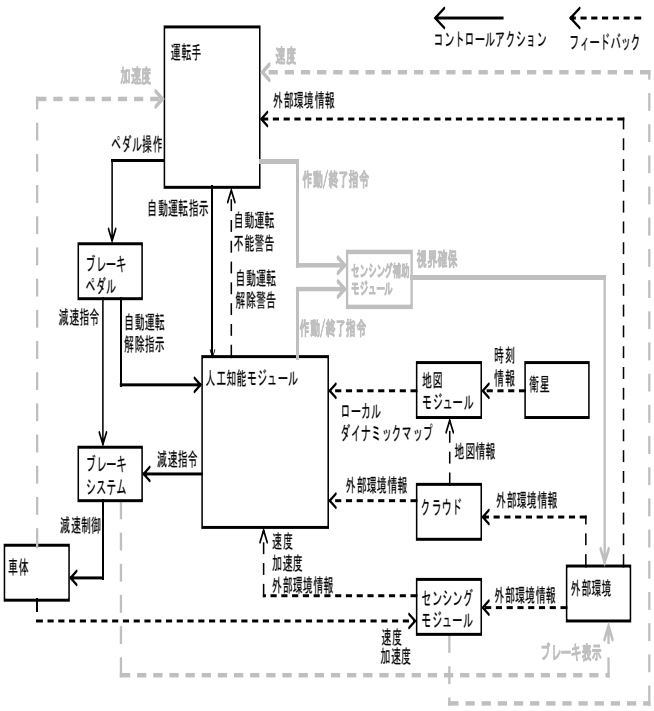

図 6 被験者グループ B が作成した CS

5. 考察とヒアリング結果

5.1. 考察

適用の結果，「①企画・要件定義工程からセーフティとセキュリティの分析ができる．」についてはベースとなる STAMP が企画要件定義からの分析手法であるため自明である．同様に「②セーフティの分析として人の生命・健康に関わるハザードとその要因が多く抽出できている．」についても，STAMP/STPA がセーフティ分野のハザード分析手法であるため，満たしている．「③セキュリティの分析とし

て脅威が多く抽出できている.」については，実験 1，実験 2 の結果から，多くの脅威が抽出できているので満たしている.

実験 1[18]では,セーフティの手法である STAMP/STPA（STPA-Sec）に STRIDE のヒントワードを拡張することで,セーフティとセキュリティ両方に関する脅威を洗い出すことができた. そして, STAMP の特徴である要素間の相互作用をモデリングすることによって，運転手と自動車の両方に関わる要因を考慮した分析結果を得た.

これらは STAMP のハザード分析手法とともに STRIDE のヒントワードを利用した脅威分析手法を実施することにより，セーフティとセキュリティの双方のリスク分析を 1 つの CS 上で実施できることを示したものである.

そして, 実験 2[19]では, STAMP を用いた分析と, STAMP を用いない分析の比較を行い, STAMP を用いた分析の方が良好な結果となった.

(1) 被験者 1 人当たりのリスク件数は STAMP を用いた分析の方が 11.6 倍多い（表 2）.
(2) STAMP を用いた分析は,セーフティにおいて多くのグループでリスクを検出している（図 5 において，グラフのピークが，右側，すなわちグループ数の大きな方にあることから示される）.
(3) STAMP を用いない分析では, 多くの被験者でセキュリティ・リスクが抽出できていないのに対して，STAMP を用いた分析では，全員抽出できている.（図 2）

(1) 及び(2)について, STAMP を用いた分析に以下の特徴があることが要因と考える.

- STAMP を用いた分析は, CS を利用して手順通りに分析を進めるため, すべてのコンポーネントを考慮できている.
- STAMP を用いた分析は，システムだけではなく，人間も分析対象としている．これは，図 3 及び
- **図** 4 でヒューマンエラーや人とシステムの認識の違いが STAMP を用いない分析より非常に多く挙げられていることから分かる.
- STAMP を用いた分析は，システム内部の要素のやり取りも分析対象としている．同じく，図 3 及び
- **図** 4 で人とシステムの認識の違いが非常に多く挙げられていることから分かる.
- STAMP を用いた分析は，ガイドワード及びヒントワードを利用している. 何もないところからリスクを導き出すことは難しいが, これらのワードがあることで導出しやすくなっていると考える.

(3)について，STRIDE をヒントワードとして拡張することが，有効に作用している.

5.2. 有識者へのヒアリング結果

抽出されたリスクに対して，セーフティならびにセキュリティ分野の有識者よりコメントをいただいた.

セキュリティの有識者からは「STAMP を用いた分析の方は，どこでどのようなことがあったのかが分かった．リアリティのあるよい題材となっている」,「同じリスクであっても，どこでリスクが発生しているのかによって対策は異なる. STAMP を用いた分析の方は, 発生個所が特定されているので，対策が具体化されているようだ」,「マルウェアや多段攻撃が考慮できていない」,「運用時の運転だけではなく，製造・保守・破棄のフェーズもあるので，考慮するとよい」との知見を得ることができた.

また，セーフティの有識者より本実験の分析について「手法の有用性として，リスクの捕捉率があるとよい．すべてのリスクを洗い出すのは困難だが，全員で抽出できたリスクを総和して，さらに議論して新たなリスクを考えれば全リスクと類似できるではないか」,「抽出されるリスクの有効性を論じることができるとよい．容易に気が付くかどうかをレベル付けして,集計するとわかるのではないか」というコメントをいただくことができた.

6. 今後の課題

前節のヒアリング結果に基づき,「マルウェアや多段攻撃が考慮できていない」について，階層化して詳細を考慮すると，抽出可能と考えるので，階層化して分析を行うことを実施したい. また,「運転時のみではなくその他のフェーズについても考慮に入れる」について，アクシデントの識別方法を検討する必要がある.

さらに，セーフティ&セキュリティのチェックリストなどを用いる場合と本実験の結果との比較を行うことで有効性を主張できると考える．一方で，セーフティまたはセキュリティのチェックリストを用いた場合との比較は可能であるので今後比較を行うことを課題とする. これらは今後, STAMP/STPA 分析の効果をより具体的に測る上での課題である.

7. まとめ

本稿では，自動車の自動運転システムを取り上げ, STAMP S&S のセーフティ・セキュリティ統合リスク分析の適用評価を行った．提案手法は 2 つの実験結果から 3.3 節で示した 3 つの条件を満たしていたためセーフティ・セキュリティの統合リスク分析ができることがわかった．今後, 6 章で述べた課題に取り組むと共に, 更なる事例作成, 普及展開を図る.

謝辞　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，日本科学技術連盟ソフトウェア品質管理研究会（SQiP）演習コースⅢの研究員の皆様に謹んで感謝の意を表する.

参考文献

1) Nancy G. Leveson, Engineering a Safer World, Systems Thinking Applied to Safety ,2012

2) ナンシー・G・レブソン，セーフウェア，安全・安心なシステムとソフトウェアを目指して

3) IPA，はじめての STAMP／STPA,2016

4) IPA，はじめての STAMP／STPA（実践編）, 2017

5) William Young, Nancy Leveson. Systems Thinking for Safety and Security, Proceedings of the 29th Annual Computer Security Applications Conference （ACSAC 2013）, pp.1-8 （2013）.

6) William Young, Reed Porada, System-Theoretic Process Analysis for Security（STPA-SEC）:Cyber Security and STPA, 2017 STAMP Conference

7) Ivo Friedberg, Kieran, Paul Smith, David Laverty and Sakir Sezer. STPA-SafeSec: Safety and security analysis for cyber-physical systems, Journal of Information Security and Applications, Volume 34, Part 2, pp.183-196 （2017）.

8) 岡本圭史，岡野浩三，STAMP　海外事例の紹介：STPA-SafeSec，SEC journal 52 号

9) NISC,www.nisc.go.jp/conference/seisaku/dai15/pdf/15siryou02.pdf

10) 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

11) Schneier, B, Attack Trees. Dr. Dobb's Journal of Software Tools 24（12） （1999） 21–29

12) Barbara Kordy, Sjouke Mauw, Saša Radomirović, Patrick Schweitzer, Foundations of Attack–Defense Trees

13) Sindre, G. and Opdahl. L. A : Eliciting security requirements with misuse cases, Requirements Engineering, Vol.10, No.1, pp. 34-44 （2005）.

14) 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, https://msdn.microsoft.com/ja-jp/library/ms995349.aspx

15) 金子朋子，高橋雄志，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停案，" CSS2017，Oct. 2017.

16) 金子朋子，高橋雄志，大久保隆夫，勅使河原可海,佐々木良一．" 安全性解析手法 STAMP／STPA への脅威分析（＝STRIDE）の適用, ",CSEC 研究会,Mar8.2018

17) Tomoko Kaneko, Yuji Takahashi, Takao Okubo and Ryoichii Sasaki,"Threat analysis using STRIDE with STAMP/STPA," The International Workshop on Evidence-based Security and Privacy in the Wild 2018

18) SQiP 研究会演習コースIII,"セーフティ＆セキュリティ開発のための技術統合提案～STAMP/STPA とアシュアランスケースの統合～", www.juse.jp/sqip/library/shousai/?id=378

19) SQiP 研究会演習コースIII, " セーフティ&セキュリティ開発における STAMP_STPA の有効性検証", http://www.juse.jp/sqip/library/shousai/?id=392