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

研究員
西澤　賢一（GEヘルスケア・ジャパン）
中嶋　良秀（ノーリツ）
大森　淳夫（パイオニア）
畑　久美子（インテック）
田中　基大（ナブテスコ）
渡邉　泰宙（コニカミノルタ）
仲田　謙太郎（東京精密）

主査
金子　朋子（情報セキュリティ大学院大学）
副主査
髙橋　雄志（アイダック）
アドバイザー
佐々木　良一（東京電機大学）

演習Ⅲ セーフティ&セキュリティ開発 実績

回	日時	講演テーマ	講演者	演習
1	5/11	前年度実績をもとに考えるセーフティ・セキュリティ開発のポイント	金子 朋子	なし
2	6/15	・IoT高信頼化機能とCCベースのセキュアシステム設計 ・セキュリティ・パターンと設計	金子 朋子 国立情報学研究所 吉岡 信和　准教授	PP機能要件 セキュリティ・パターン
3	7/12 7/13 （合宿）	・STAMP/STPAを活用したセーフティ＆セキュリティ開発 ・設計者にとって役に立つ手法と基準や仕組みづくり	金子 朋子 髙橋 雄志	STPA／STPA-Sec・GSN
4	9/13-14	ソフトウェア品質シンポジウム（臨時会　論文チーム検討）		
5	10/12	アシュアランスケースとその応用	JAXA 梅田浩貴氏	論文検討
6	11/16	デジタルフォレンジック	東京電機大学 佐々木 良一教授	論文検討・事例化
7	12/3-4	臨時会　第3回STAMPワークショップ		
8	12/14	プライバシー概論	明治大学 菊池 浩明教授	論文検討・事例化
9	1/11	セーフティ・セキュリティ開発方法論	金子 朋子	論文作成・事例化
10	2/1	臨時会　論文作成　成果発表会準備		

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

研究員
西澤　賢一（GEヘルスケア・ジャパン）
中嶋　良秀（ノーリツ）
大森　淳夫（パイオニア）
畑　久美子（インテック）
田中　基大（ナブテスコ）
渡邉　泰宙（コニカミノルタ）
仲田　謙太郎（東京精密）

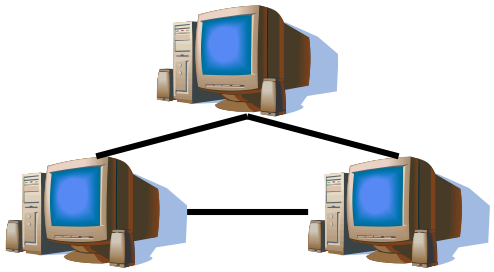
主査
金子　朋子（情報セキュリティ大学院大学）
副主査
髙橋　雄志（アイダック）
アドバイザー
佐々木　良一（東京電機大学）

目次

はじめに (1)

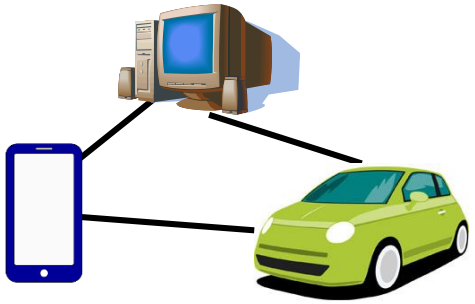
セーフティ
の
時代

機器は独立で
ネットワークの
ない時代



セキュリティ
の
時代

ネットワークが
繋がり他の機器に
影響がある時代



セーフティ &
セキュリティ
の
時代

IoT時代の到来によ
りあらゆる機器が影
響を及ぼしあう時代

セーフティとセキュリティの
バランスの取れた開発方法論が必要

はじめに (2) STAMP/STPA

STAMP (Systems-Theoretic Accident Model and Processes)

システム理論に基づく事故モデル

STPA (System–Theoretic Process Analysis)

STAMPアクシデントモデルを前提とするシステムの
ハザード要因を分析する新しい安全解析手法

従来の手法
FMEA, FTA, HAZOPなど

アクシデントは構成機器の故障や
オペレーションミスに起因すると仮定

STAMP/STPA

アクシデントは構成要素間の全体俯瞰
に基づく相互作用が働かないことに
起因すると仮定

STAMP/STPAを用いることで
複雑なシステムのリスク分析が可能

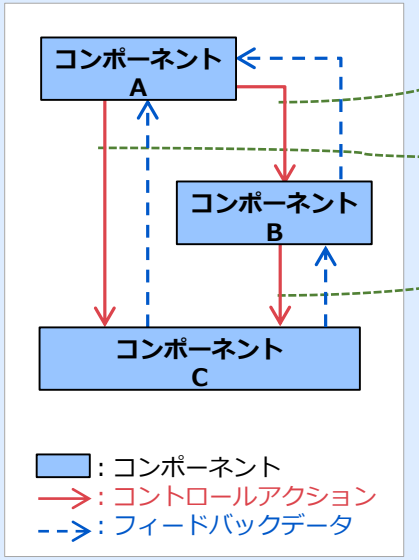
はじめに (3) STAMP/STPAの概観

【Step0-準備1】➡【Step0-準備2】➡【Step1】➡【Step2】

システムレベルのアクシデント、ハザード、安全制約の識別

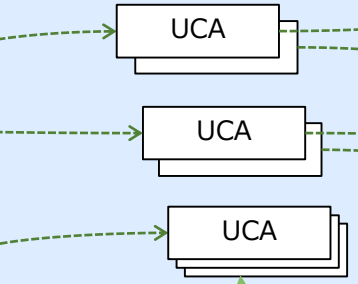
コンポーネント間の制御関係を表すモデルの構築

※コントロールストラクチャー

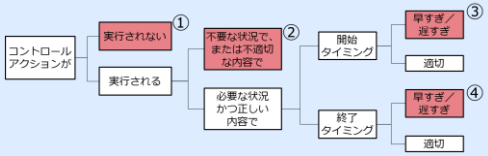


ハザードにつながるコントロールアクションの識別

※**UCA**
(Unsafe Control Action)

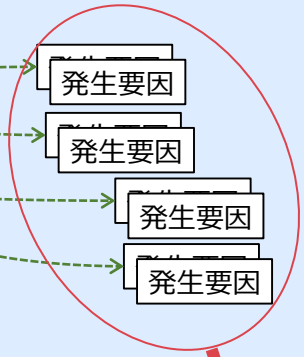


危険な制御のパターンを利用して分析



UCAの発生要因の分析

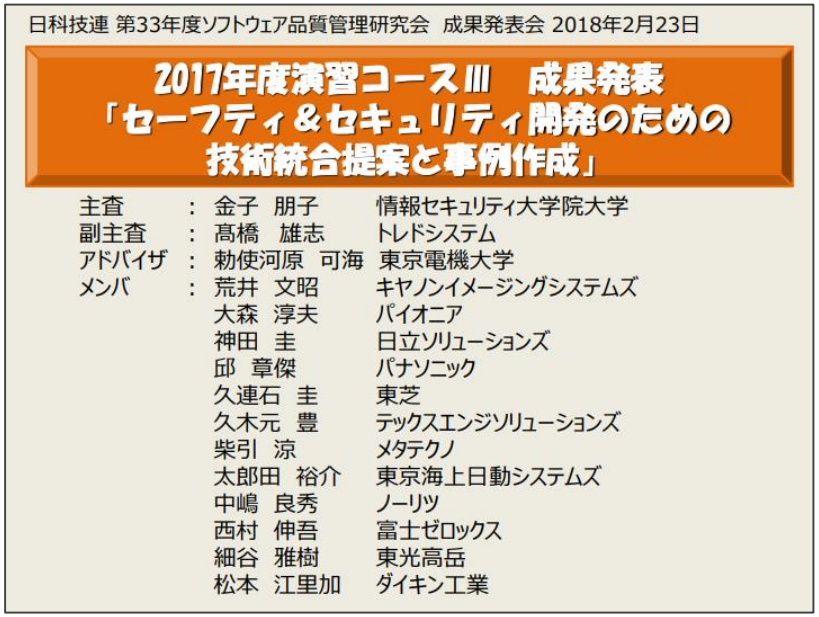
※**HCF**
(Hazard Causal Factor)



コンポーネントが満たすべき安全要件を導出

はじめに (4)

2017年度の演習コースⅢの成果発表


日科技連 第33年度ソフトウェア品質管理研究会 成果発表会 2018年2月23日

2017年度演習コースⅢ 成果発表
「セーフティ＆セキュリティ開発のための技術統合提案と事例作成」

主査	：	金子 朋子	情報セキュリティ大学院大学
副主査	：	髙橋 雄志	トレドシステム
アドバイザ	：	勅使河原 可海	東京電機大学
メンバ	：	荒井 文昭	キヤノンイメージングシステムズ
		大森 淳夫	パイオニア
		神田 圭	日立ソリューションズ
		邱 章傑	パナソニック
		久連石 圭	東芝
		久木元 豊	テックスエンジソリューションズ
		柴引 涼	メタテクノ
		太郎田 裕介	東京海上日動システムズ
		中嶋 良秀	ノーリツ
		西村 伸吾	富士ゼロックス
		細谷 雅樹	東光高岳
		松本 江里加	ダイキン工業

STAMP/STPA に STRIDE を組み合わせる

↓

対象分野の専門知識を持たない技術者でもセーフティ&セキュリティのリスクを同時に分析可

↓

STAMP/STPAを用いた場合と用いない場合のリスク分析に差があるのかの検証はできていなかった

STAMP/STPAを用いた場合と用いない場合のリスク分析に差があるのかを実験

はじめに (5) STRIDE

マイクロソフト社が定義する脅威モデル

脅威	訳	説明
Spoofing Identity	なりすまし	コンピュータに対し、他のユーザを装うこと
Tampering	改ざん	データを意図的に操作すること
Repudiation	否認	ユーザがあるアクションを行ったことを否認し、相手はこのアクションを証明する方法がないこと
Information Disclosure	情報の暴露	アクセス権限を持たない個人に情報が公開されていること
Denial of Service	サービス不能	攻撃により正規へのユーザへのサービスが中断される
Elevation of Privilege	権限の昇格	権限のないユーザがアクセス権限を得ること

目次

実験: 概要(1)

比較実験: リスク分析の結果に差があるのかを確認

- **リスク分析の対象** 自動車の自動運転

  自動車自動運転レベル3の夕暮れ時かつ雨天のシーンにおける**ブレーキ周り**

- **被験者** 自動車の**専門家でない**メンバー

STAMP/STPAを知らない被験者

STAMP/STPAを知っている被験者

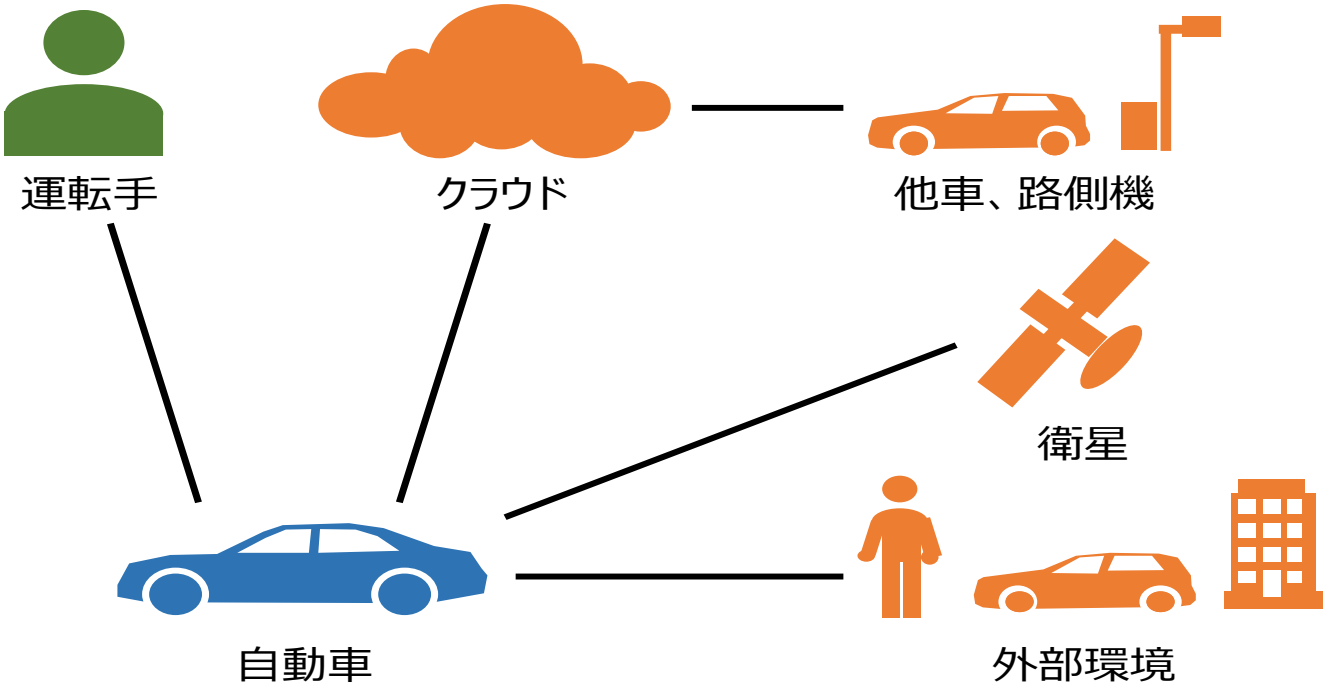
実験: 概要(2)

自動車の自動運転イメージ

ネットワークに接続された　レベル3の自動運転自動車

①通常，自動車は自動運転で走行する

②システムが扱いきれない場合，運転手が運転する



実験: 手順(1)

【手順1】 質問紙調査

#	問
1	STAMP/STPAを知っていますか？
2	STAMP/STPAを使った分析を過去にしたことがありますか？
3	自動車自動運転レベル3の、夕暮れ時かつ雨天のシーンにおけるブレーキ回りのセーフティ並びにセキュリティ上のリスクを5つ以上思いつく限り挙げてください (※レベル3とは自動運転と手動運転が混在するものである)
4	問3で上げたリスクに対する対策をお答えください.

【手順2】 質問紙の集計ならびにパラメータの設定

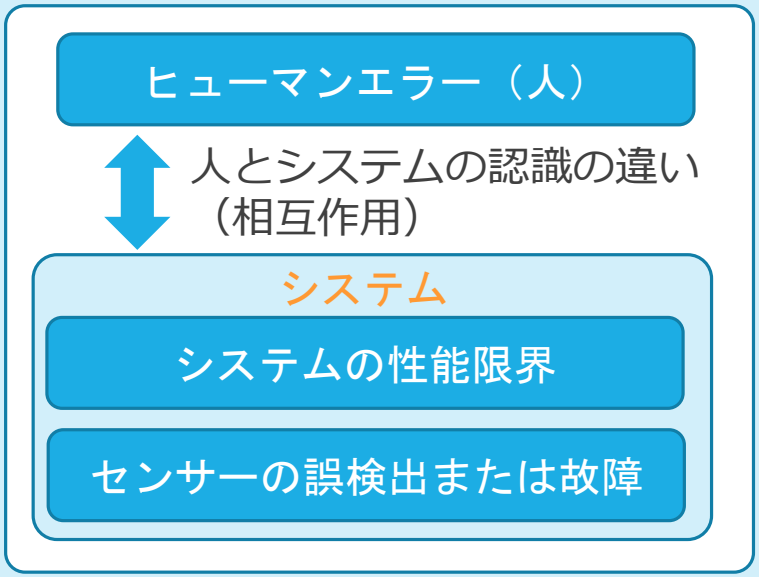
- リスクがセーフティまたはセキュリティどちらに基づくリスクであるのか
- リスクに対する対策の有無を判別する

実験: 手順(2)

【手順3】集計結果のグルーピング

セーフティ

- ヒューマンエラー
- 人とシステムの認識の違い
- システムの性能限界
- センサーの誤検出または故障
- その他



セキュリティ

- 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)
- その他

実験: 手順(3)

【手順4】データ集計

洗い出しができた件数を集計する

【手順5】傾向性の考察

STAMP/STPAを用いない分析とSTAMP/STPAを用いた分析の結果にどのような傾向性があるかを考察

目次

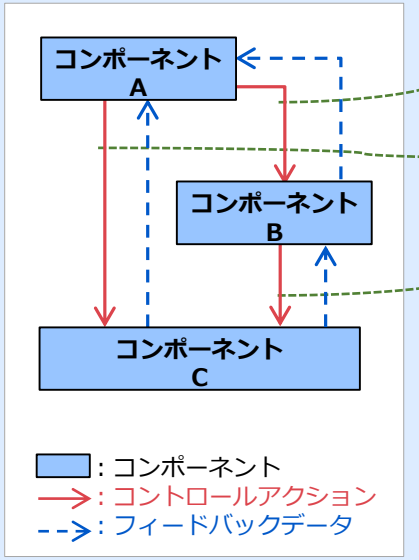
STAMP/STPAの実施手順: 概観

【Step0-準備1】➡【Step0-準備2】➡【Step1】➡【Step2】

システムレベルのアクシデント、ハザード、安全制約の識別

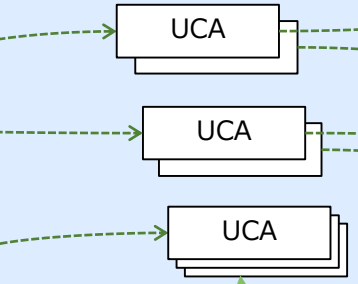
コンポーネント間の制御関係を表すモデルの構築

※コントロールストラクチャー

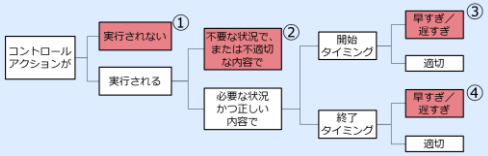


ハザードにつながるコントロールアクションの識別

※**UCA**
(Unsafe Control Action)

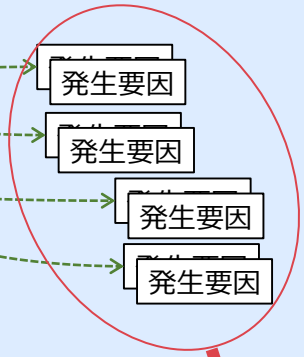


危険な制御のパターンを利用して分析



UCAの発生要因の分析

※**HCF**
(Hazard Causal Factor)



コンポーネントが満たすべき安全要件を導出

STAMP/STPAの実施手順(1)

【Step0-準備1】

システムレベルのアクシデント、ハザード、安全制約の識別

アクシデント	ハザード	安全制約
自動車が外部環境（歩行者/他の車/周辺物）と衝突/接触する	自動車が、ブレーキをかけても、外部環境の前で停止できない (H1)	自動車が、外部環境と衝突しないようにブレーキをかける（外部環境までの距離や相対速度を制御する） (SC1)
	ブレーキがかからない (H2)	運転手と自動車の両方がブレーキをかけられない状態にならない (SC2)
	急ブレーキにより後方車両から追突される (H3)	SC1に違反しない程度に緩やかに減速する (SC3)

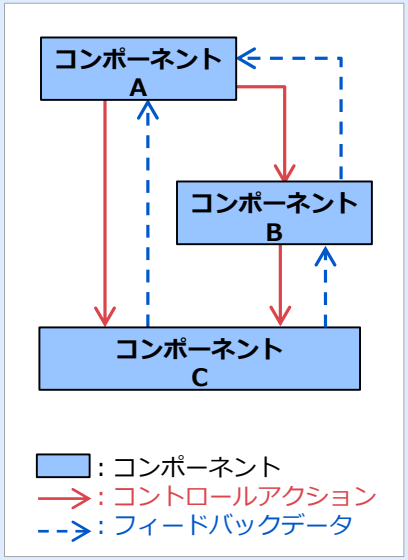
STAMP/STPAの実施手順(2)

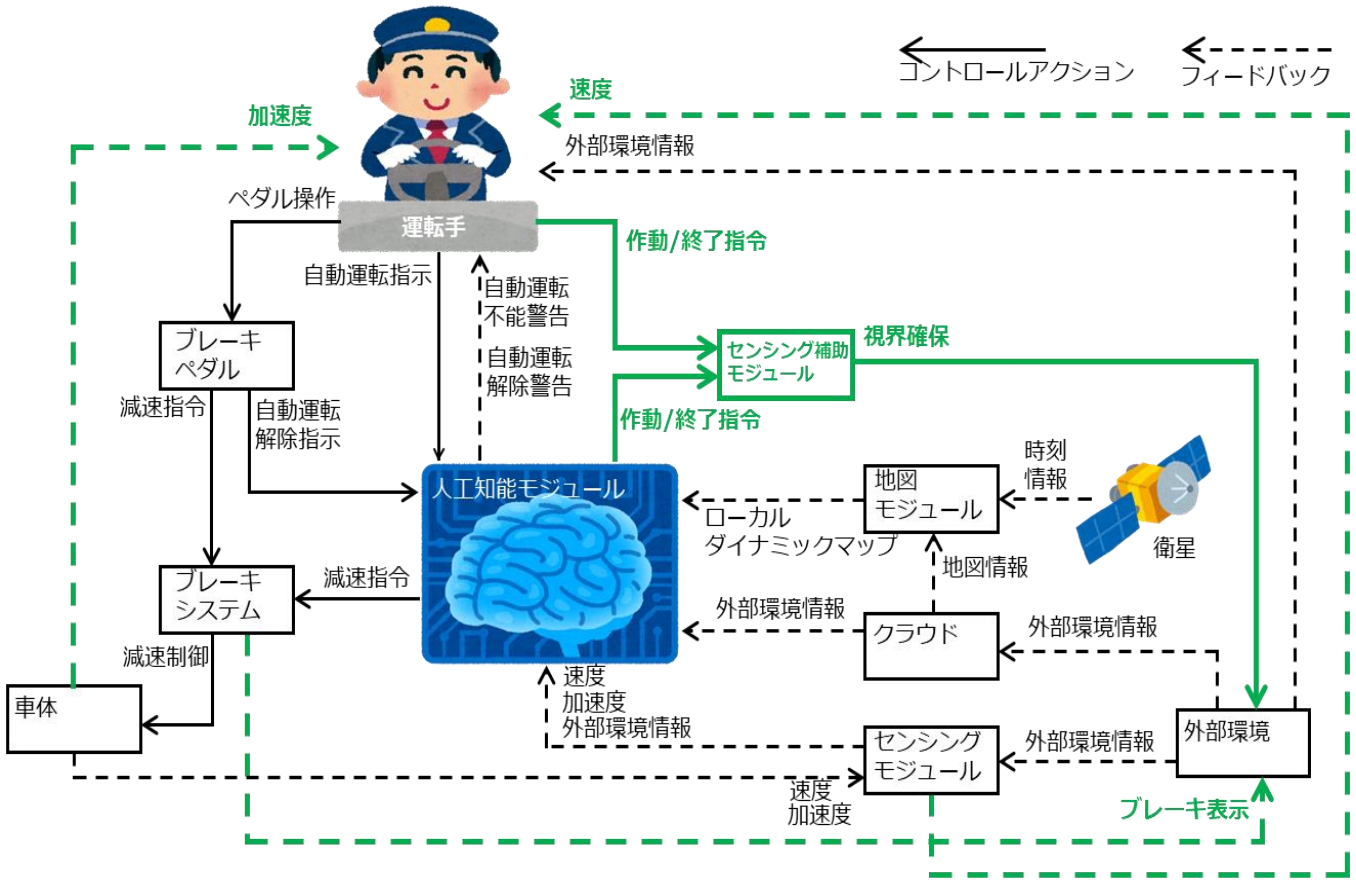
【Step0-準備2】

今回の実験でのコントロールストラクチャー

コンポーネント間の制御関係を表すモデルの構築

※コントロールストラクチャー





(*) 緑色: 昨年度のCSからの追加

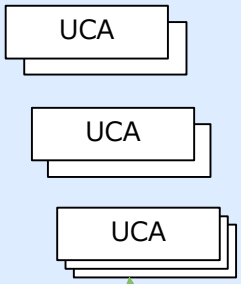
STAMP/STPAの実施手順(3)

【Step1】

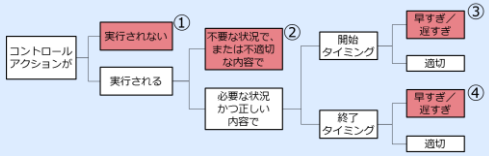
Unsafe Control Actionの一覧（一部抜粋）

ハザードにつながるコントロールアクションの識別

※UCA
(Unsafe Control Action)



危険な制御のパターンを利用して分析



No	CA	Not Providing	Providing causes hazard	Too early / Too late	Stop too soon / Applying too long
1	運転手によるブレーキペダル操作	(UCA1-N) 自動運転不能時に運転手がペダルを踏まないと減速指令が出ず外部環境と衝突する. [SC1][SC2]	(UCA1-P) 自動運転中に意図しないペダル操作が発生し，自動運転が解除されブレーキが作動しなくなり外部環境と衝突する [SC1][SC2]	(UCA1-T) 非自動運転時にペダル操作が遅すぎる場合，減速指令が遅れ，外部環境と衝突する [SC1]	(UCA1-D) 非自動運転時にペダルを踏む時間が不足すると，減速指令が不足して外部環境と衝突する [SC1] ブレーキを踏む時間が長すぎると必要以上に減速し，渋滞の原因となる
2	ブレーキペダル操作によるブレーキシステムへの減速指令	(UCA2-N) 減速指令がないと，そのまま外部環境と衝突する [SC1]	(UCA2-P) 不必要に強い減速指令が出され，後方車両から追突される [SC3]	(UCA2-T) 運転手のペダル操作に対して減速指令が遅すぎた場合，外部環境との適切な距離が保てず衝突する [SC1]	(UCA2-D) 十分な減速が行われる前に減速指令が終了し，外部環境との適切な距離が保てず衝突する [SC1] 必要な減速が完了した後も減速指令を出し続け，加速が困難になる
3	ブレーキシステムによる車体の減速制御	(UCA3-N) 減速制御が行われないと，そのまま走行方向の外部環境と衝突する [SC1][SC2]	減速指令を受けてないのに減速が発生し，交通渋滞となる (UCA3-P) 不必要に強い減速が生じ，後方車両から追突される [SC3]	(UCA3-T-1) 減速指令に対して減速が遅すぎる場合，外部環境との適切な距離が保てず衝突する [SC1] (UCA3-T-2) 外部へのブレーキ表示前に減速を始め，後方の車両から衝突される [SC3]	(UCA3-D) 減速指令が終了する前に減速が終了し，外部環境との適切な距離が保てず衝突する [SC1] 減速指令が終了した後も減速制御を行い，加速が困難になる
4	運転手による人工知能モジュールへの自動運転指示	自動運転指示が行われないと，自動運転が開始されない	意図しない自動運転が開始され，運転手が混乱する	-	-
5	人工知能モジュールによるブレーキシステムへの減速指令	(UCA5-N 自動運転時に人工知能が減速指令を出さないとそのまま外部環境と衝突する. [SC1]	(UCA5-P) 不必要に強い減速指令が出され，後方車両から追突される [SC3]	(UCA5-T) 減速指令が遅れた場合，前方の外部環境との適切な距離が保てず衝突する [SC1]	(UCA5-D) 十分な減速が行われる前に減速指令が終了し，外部環境との適切な距離が保てず衝突する [SC1] 必要な減速が完了した後も減速指令を出し続け，加速が困難になる
6	ブレーキペダル操作による人工知能モジュールへの自動運転解除指示	自動運転の解除指示が行われないと，運転手がブレーキ操作をすることができない	(UCA6-P) 意図せず自動運転が解除され，衝突回避のためのブレーキ指令をだすことができない [SC1][SC2]	-	-
7	人工知能モジュールによるセンシング補助モジュールの作動/終了指令	視界確保無しで人工知能モジュールが外部環境を認識できない場合，作動指令がなされないと人工知能による自動運転が不可能となる	不要な視界確保動作が行われ，部品の寿命が縮む	-	-
8	運転手によるセンシング補助モジュールの作動/終了指令	(UCA8-N) 非自動運転かつ運転手が視界の確保無しで運転ができない状況となった場合に作動指令が出せないと，運転手が外部環境を認識できず，ブレーキをかけずに外部環境と衝突する [SC1]	不要な視界確保動作が行われ，部品の寿命が縮む (UCA8-P) 非自動運転かつ運転手が視界の確保無しで運転ができない状況となった場合で，運転手の視界確保可能な状況となる前に終了指令が出されると，運転手が外部環境を認識できず，ブレーキをかけずに外部環境と衝突する [SC1][SC2]	-	-
9	センシング補助モジュールによる外部環境の視界確保	(UCA9-N) 視界の確保が行われないと，運転手/人工知能が外部環境を認識できず，ブレーキをかけずに衝突する [SC1][SC2]	(UCA9-P) 運転手/人工知能が外部環境を認識できないほど視界の確保機能が働き，ブレーキをかけずに衝突する [SC1][SC2]	(UCA9-T) 視界の確保作動のタイミングが遅すぎ，運転手/人工知能が外部環境を認識できない状態となり，ブレーキをかけずに衝突する [SC1][SC2]	-

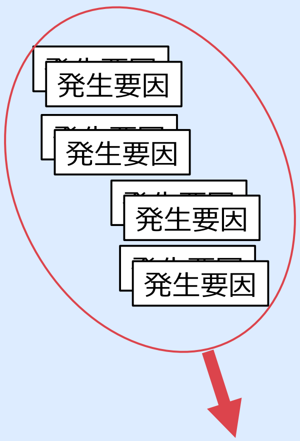
STAMP/STPAの実施手順(4)

【Step2】

Hazard Causal Factorの一覧（一部抜粋）

UCAの発生要因の分析

※HCF
(Hazard Causal Factor)



コンポーネントが満たすべき安全要件を導出

	HCF																				
UCAx	(1) コントロールの入力か外部情報が欠けているか間違っている	(2) コントロールアルゴリズムの生成の欠陥、プロセス変更、不正確な修正や適応	(3) プロセスモデルの矛盾、不完全、不正確	(4) コンポーネント故障、経時変化	(5) 不適切か欠けているフィードバック、フィードバックの遅れ	(6) 情報が与えられないか間違っている。測定が不正確。フィードバックの遅れ	(7) 遅れたアクション	(8) 不適切、有効でない欠けたコントロールアクション	(9) プロセスへの入力が欠けているか間違っている	(10) 識別されないか範囲外の妨害	(11) プロセスの出力がシステムハザードの一因に	(12) アクチュエーターの不適切なオペレーション	(13) センサーの不適切なオペレーション	(14) 他のコントローラーとの通信が欠けているか間違っている	(15) 矛盾するコントロールアクション	Spoofing（なりすまし）	Tampering（改ざん）	Repudiation（否認）	Information Disclosure（情報漏えい）	Denial of Service（サービス拒否）	Elevation of Privilege（特権の昇格）
(UCA1-D) 非自動運転時にペダルを踏む時間が不足すると，減速指令が不足して外部環境と衝突する [SC1]	-	運転手が雨による路面摩擦の低下を考慮せずにブレーキ操作をする	運転手が前方の車両の減速度が増加していることに気付かない	-	-	-	-	運転手がペダルを踏んではいるが，ブレーキのあそび部分しか踏んでいない	-	-	-	-	-	-	-	-	運転手の意識をそらし，ブレーキから足を離すようにしむける	-	-	-	-
(UCA1-N) 自動運転不能時に運転手がペダルを踏まないと減速指令が出ず外部環境と衝突する. [SC1][SC2]	悪天候など外部環境の情報が鮮明でなく，運転手が危険察知をしない	運転手が十分な操作知識を持っておらず，ペダルを踏む場所を誤って覚えている	運転手が危険を察知したが自動運転を過信して，ブレーキを踏まない	-	スピード表示が実際より低速となっており，危険な速度であることを察知しない	-	-	他のペダルと踏み間違える	-	-	-	-	-	人工知能モジュールが自動運転不能と判断したが，自動運転の解除警告が通知されない	-	外部環境の一部になりすまし，誤った外部環境情報をクラウドへ送信，自動運転不能な状態であっても人工知能に自動運転可能であると判断させ，自動運転不能警告をださせない	・クラウドからの情報を改ざんし，自動運転不能な状態であっても人工知能に自動運転可能であると判断させる ・外部環境からセンシングモジュールへの情報を改ざんし，自動運転不能な状態であっても人工知能に自動運転可能であると判断させ，自動運転不能警告を出させない ・外部環境からセンシングモジュールへの情報を改ざんし，自動運転不能な状態であっても人工知能に自動運転可能であると判断させ，自動運転不能警告を出させない ・自動運転不能警告を改ざんし(運転手の気をそらす・警告手段を破壊するなど），運転手への警告を遮断する	-	-	・人工知能モジュールに高負荷(物理的なものを含む)を与え，自動運転不能であることを報知できなくさせる ・運転手に対して大量or致命的な情報を与え，正常な判断をすることが不可能な状態にする	-
(UCA1-P) 自動運転中に意図しないペダル操作が発生し，自動運転が解除されブレーキが作動しなくなり外部環境と衝突する [SC1][SC2]	-	自動運転解除警告以外に気をとられ，自動運転が解除されたことを認識しない	運転手の足が意図せずペダルに触れてしまう	-	-	-	-	-	-	-	-	車の振動などの慣性力でペダルが動作する	-	自動運転解除警告が表示されない	-	-	・運転手以外の何かがペダルに触れる ・自動運転解除警告を表示させない	-	-	-	-
(UCA1-T) 非自動運転時にペダル操作が遅すぎる場合，減速指令が遅れ，外部環境と衝突する [SC1]	外部環境が見え辛く，運転手の判断が遅れる	体調などで運転手の判断能力が低下しており，ペダルを踏むのが遅れる	-	-	実際の速度より低速で速度表示がなされ，運転手が危険回避までの猶予があると勘違いする	-	ペダルのあそびが大きく，運転手の指示より減速指令が遅れる	-	-	-	-	経年劣化でペダルが硬くなり，ブレーキ指示を出すまでに時間がかかる	速度表示をせず，運転手が速度を認識できなくなる	自動運転不能の警告が遅れ，運転手が非自動運転であることの認識が遅れる	-	-	風などで信号と運転手の間に障害物が入るor信号の向きがかわることにより，運転手が危険を察知するのが遅れる	-	-	信号機が破壊し，運転手を迷わせる	-
(UCA2-D) 十分な減速が行われる前に減速指令が終了し，外部環境との適切な距離が保てず衝突する [SC1]	-	-	-	-	-	-	-	運転手が濡れた足で操作することによりペダルが滑り，減速指令が解除される	-	-	-	接点不良などの異常が生じ，減速指令が出力されない	-	-	-	-	-	-	-	-	-
(UCA2-N) 減速指令がないと，そのまま外部環境と衝突する [SC1]	-	-	-	-	-	-	-	-	-	-	-	接点故障などにより，ペダル操作がなされても，減速指令を出力がされない	-	-	-	-	ブレーキシステムへの減速指令出力を改造し，指令がブレーキシステムへ届かないようにされている	-	-	ブレーキペダルが破壊されている	-
(UCA2-P) 不必要に強い減速指令が出され，後方車両から追突される [SC3]	-	-	-	ブレーキシステムの故障により緩やかな減速が不能となる	-	-	-	・ブレーキペダルの遊びによる減速指令の遅れが生じることによる運転手の焦りにより，ペダルが強く踏み込まれる ・雨により制動距離が長くなったことにより生じた運転手の焦りにより，ペダルが強く踏み込まれる	-	-	-	ペダルの反力が弱く，必要以上に運転手がペダルを踏み込む	-	-	-	-	ブレーキシステムへの指令が改ざんされ，不要な減速指令が出力される	-	-	-	-
(UCA2-T) 運転手のペダル操作に対して減速指令が遅すぎた場合，外部環境との適切な距離が保てず衝突する [SC1]	-	-	-	-	-	-	・ペダルの遊びが大きく，減速指令が遅れる ・雨でペダルが滑り，減速指令が遅れる	-	-	-	-	-	-	-	-	-	-	-	-	-	-

目次

実験: 結果 (1)

【手順1】 質問紙調査

問1 & 問2

STAMPを用いた分析

問2: 実施経験		問1: 知っている？ はい	問1: 知っている？ いいえ
	はい	6 名	1 名
	いいえ	1 名	22 名

STAMPを用いない分析

実験: 結果 (1)

【手順1】 質問紙調査

問3: 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

11.7倍！

問4: 被験者1人当たりのリスク対策件数

	STAMPを用いた分析	STAMPを用いない分析
平均（件数）	63.8	4.4

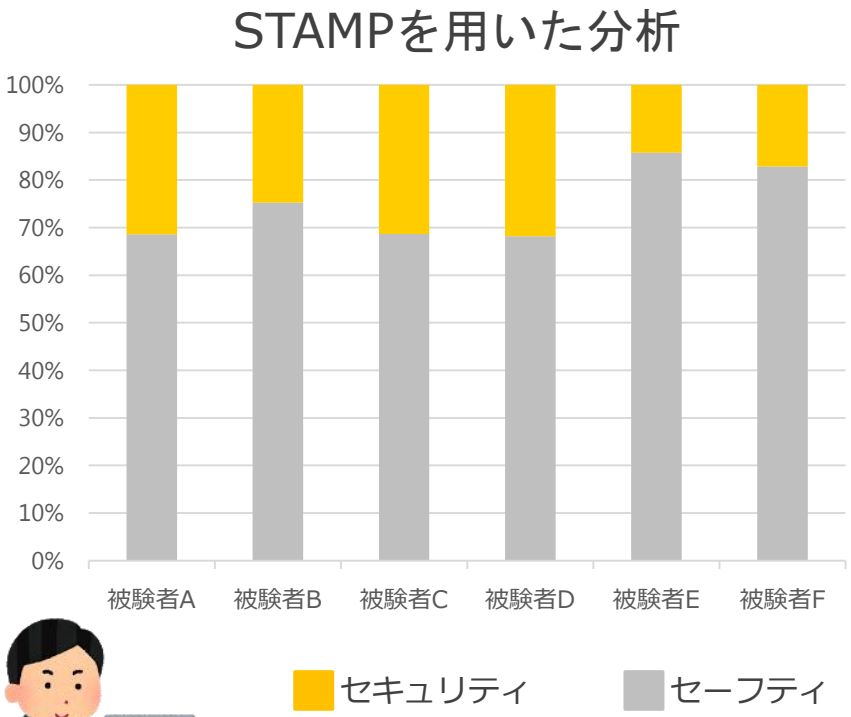
14.5倍！

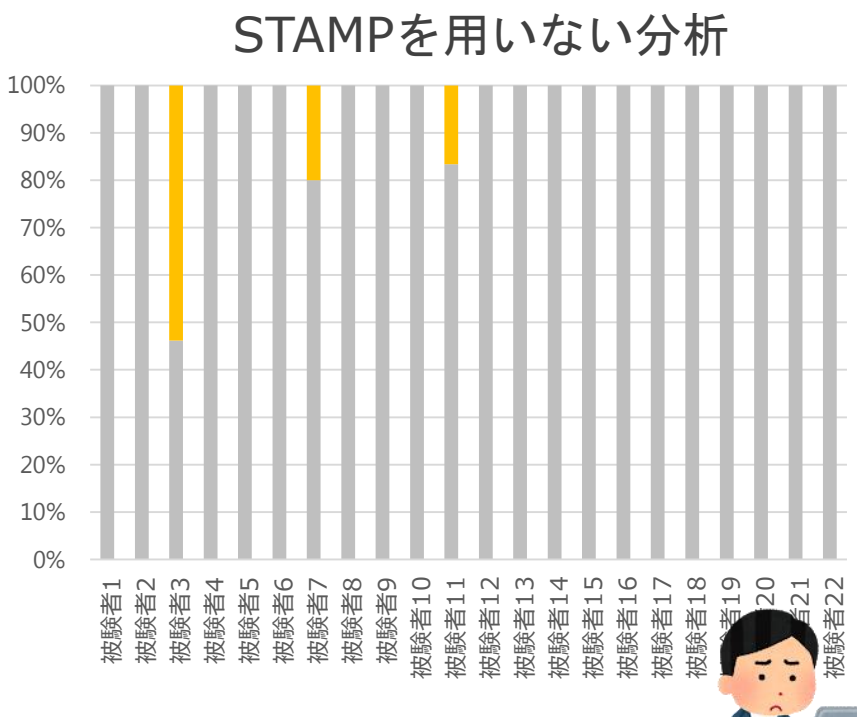
リスク件数・リスク対策件数ともに
STAMPを用いた分析の方が多い

実験: 結果 (2)

【手順2】質問紙の集計ならびにパラメータの設定

抽出したリスクのセーフティ/セキュリティの割合



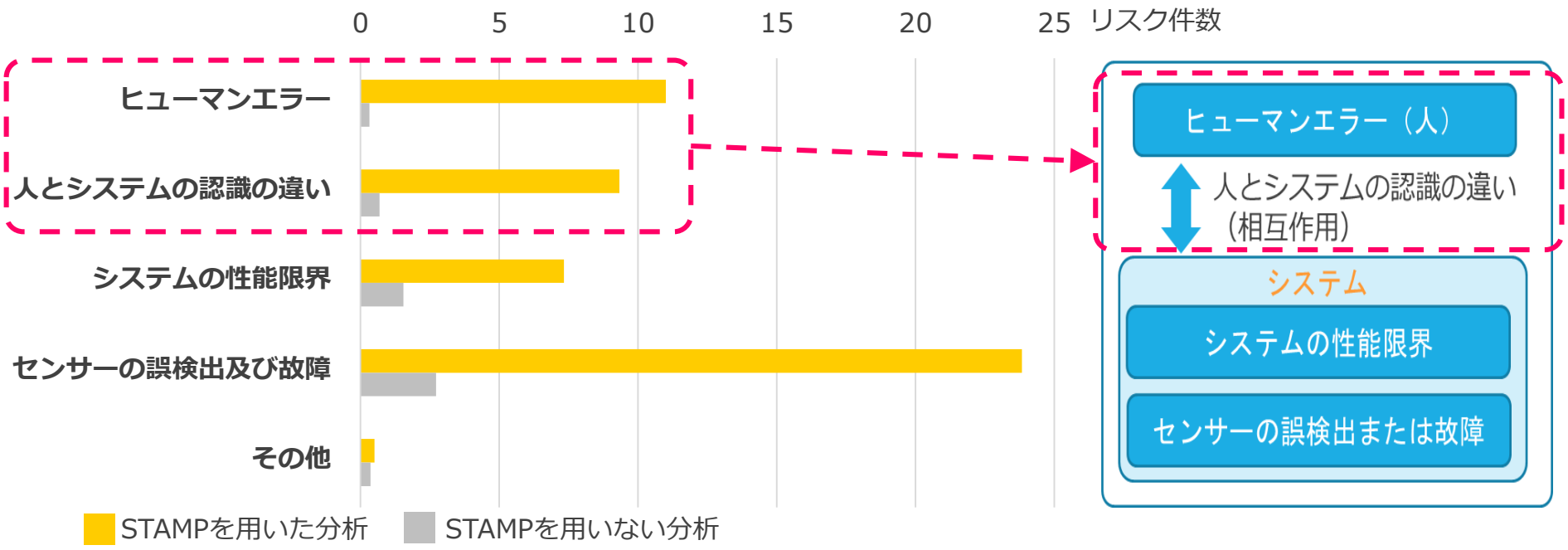


STAMPを用いた分析では
全員がセキュリティ・リスクを抽出

実験: 結果 (3)

【手順3】集計結果のグルーピング

被験者1人当たりのリスク件数の内訳(セーフティ)

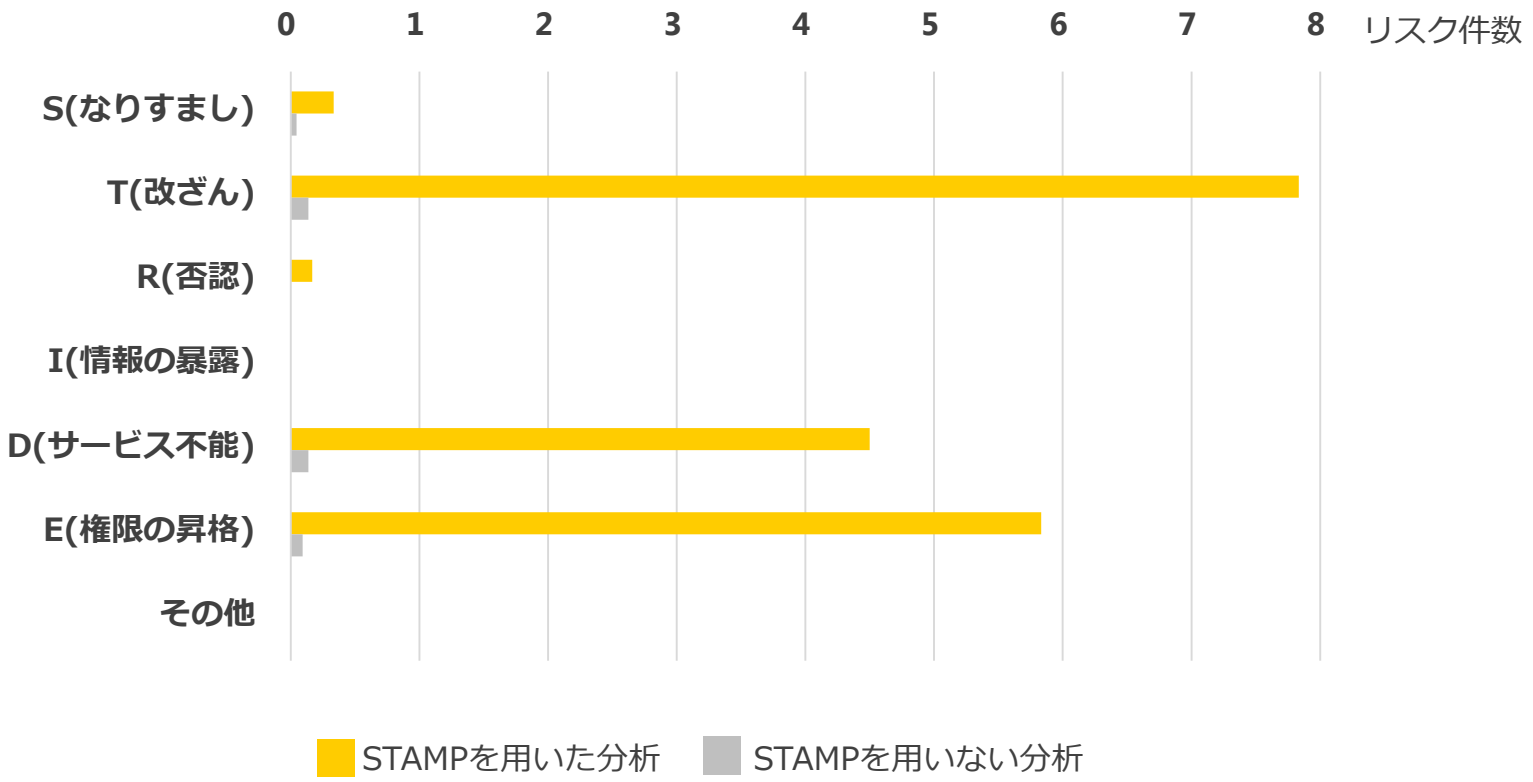


STAMPを用いた分析では
人が関連するリスクを多く検出

実験: 結果 (4)

【手順3】集計結果のグルーピング

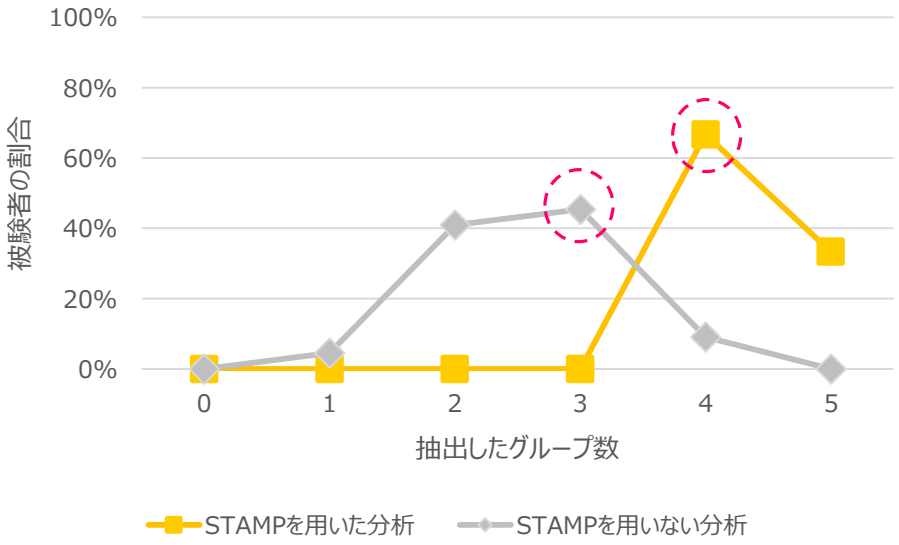
被験者1人当たりのリスク件数の内訳(セキュリティ)



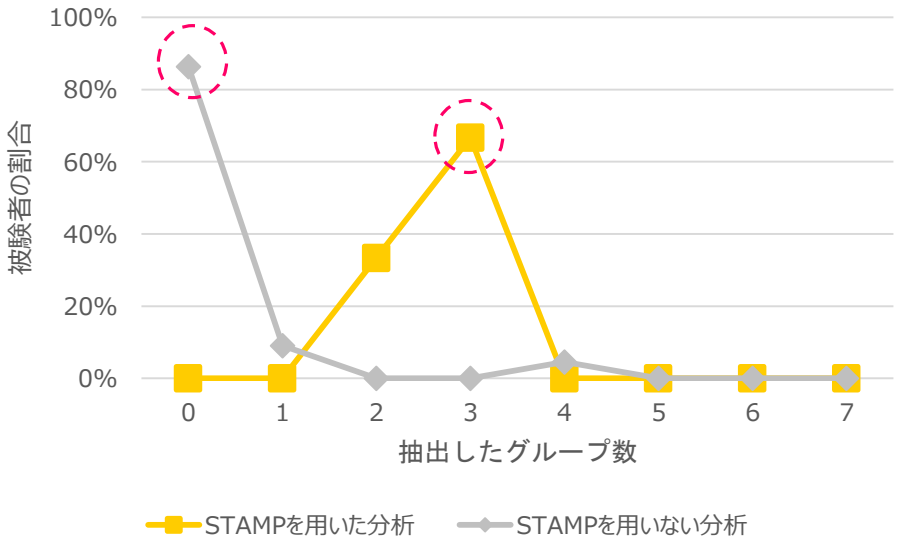
実験: 結果 (5)

【手順4】データ集計

グルーピングできたグループ数ごとの被験者の割合



セーフティ



セキュリティ

STAMPを用いた分析では
多くのグループでリスクを検出

実験: 結果 (6)

【手順5】傾向性の考察

STAMPを用いた分析で導出されたリスク (一部)

- 運転手が意図せずに、ブレーキペダルを踏み込み、自動運転が解除される. かつ運転手が自動運転解除警報に気が付かず、手動で運転していない

  ➡ **STAMPが人とシステムの相互作用を分析するからこそ導出**

- 人工知能モジュールに侵入されて、ブレーキの指示アルゴリズムを改ざんされ、減速指示をなしにさせられる

  ➡ **STAMPにSTRIDEを導入したからこそ導出**

有識者からの指摘

- マルウェアや多段攻撃が考慮できていない
- 運転だけでよいのか？製造・保守・破棄のフェーズもあるので、考慮するとよい

STAMPには弱点もある

目次

まとめ

研究の成果

- STAMP/STPAを用いたリスク分析をすれば、**セーフティとセキュリティを同時に考えることができる**ということを、データとして示し、その**有効性を確認**した

今後の課題

- マルウェアや多段攻撃が考慮できていない
  ➡ 階層化して分析
- 運転時のみでよいのか？
  ➡ アクシデントの識別方法を検討
- 手法の有用性分析: リスクの捕捉率の分析

ご清聴ありがとうございました