一般社団法人日本科学技術連盟
第37年度（2021年度）ソフトウェア品質管理研究会 成果発表会
研究コース6 「セーフティ＆セキュリティ」
2022年2月25日（金）

STAMP モデリングの スマートシティに対する安全性分析への適応

発表者：畠山　剛（三菱電機）

主査：　金子　朋子（国立情報学研究所）
副主査：　高橋　雄志（日本AIシステムサービス）
アドバイザー：　佐々木　良一（東京電機大学）

目次

- 研究員紹介
- はじめに
- 関連研究
- 安全性分析の実験
- 考察
- まとめ
- 今後の課題

研究員の紹介

氏名	所属	部署	開発対象	一言
鎌田 桂太郎	アイホン	品質保証部 品質保証課	インターホンシステム全般	参加2年目でSTAMPが少しずつ理解できました。製品に活かしたいです。
菅野 浩司	エプソンアヴァシス	事業推進4部	セイコーエプソン製品全般の評価業務	知見のないテーマをSTAMPで分析したことで、業務に活かせるスキルを得ることができました。
小長谷 義浩	TIS	エンハンスメント革新部	全社の保守開発品質管理	STAMPってハンコだと思ってました（嘘です！）。対面＋アフターをやりたかったです。
畠山 剛	三菱電機	ソフトウェア技術推進部	インフラ系 システム全般	オンラインでも意外となんとかなりますね！
浜田 淳	テックスエンジソリューションズ	金融SOL第1部 2グループ	金融系システム基盤導入支援、保守業務	オンラインも悪くないですが、対面飲み会もやりたかったですね。
福田 秀樹	TIS	プロジェクトリスク監理室	全社の不採算化PJの検知・エスカレーション	大きな分析の流れ・概念をある程度理解できましたが、セキュリティ分析とか、調査範囲の拡大などもう少しできたかも。対面でやれてればもう少し突っ込んだ議論できたかな。。。
和田 久	NTTコミュニケーションズ	プラットフォームサービス本部 マネージド＆セキュリティサービス部	セキュリティサービス	セーフティだけでなく、セキュリティも分析したかった。 一度くらいは対面でやりたかったです。

はじめに

スマートシティは、IoTやAI等、先端技術の活用によって、様々な社会課題の解決や新たな価値の創造を期待されている。

社会課題	少子高齢化	感染症	災害	インフラの老朽化	・・・等

政府機関

地方自治体

民間企業

https://www8.cao.go.jp/cstp/society5_0/smartcity/00_scguide_s.pdf

はじめに

政府機関（内閣府・総務省・経済産業省・国土交通省）によってスマートシティガイドブックが作成されている。この中で、セキュリティについては定義されているもののスマートシティ全体に対する安全性（セーフティ）については指針が示されていない。

内閣府
Cabinet Office

内閣府ホーム > 内閣府の政策 > 科学技術政策 > 新着情報一覧 > スマートシティ・ガイドブック（第１版）の公開

スマートシティ・ガイドブック（第１版）の公開
～Society 5.0の社会実装に向けた一体的推進～

令和３年４月１２日
科学技術・イノベーション推進事務局
プレスリリース

内閣府、総務省、経済産業省、国土交通省は、全国のスマートシティの構築・運営を支援するため、地方公共団体や地域協議会・エリアマネジメント団体等に活用いただける「スマートシティ・ガイドブック」を作成・公開しました。

政府では、令和３年３月に閣議決定された「第６期科学技術・イノベーション基本計画」等に基づき、「次世代に引き継ぐ基盤となる都市と地域づくり」を展開するため、スマートシティを推進しています。
この度、スマートシティに取り組む地方公共団体、協議会等の取組を支援するため、地方公共団体の職員等に対し、スマートシティの取組に係る知見、気付きを提供する導入書として、先行事例における成功・失敗体験等を踏まえつつ、スマートシティの意義・必要性、導入効果、及びその進め方等について ガイドブックとしてとりまとめました。
ガイドブックの策定に当たっては、令和３年１～３月に開催されたスマートシティ関連の有識者による「スマートシティ・ガイドブック検討会」及び、スマートシティ官民連携プラットフォーム*1の会員・オブザーバー約８０団体が参加した「スマートシティ・ガイドブック分科会」を通じて作成されました。分科会では(一社)コード・フォー・ジャパンの協力の下、オンラインツール「Decidim*2」を活用し意見収集を行いました。

今後も「スマートシティ官民連携プラットフォーム」を軸に、本ガイドブックを活用し、官民が一体となってスマートシティの取組を加速していきます。

スマートシティ・ガイドブックの概要とポイントについては別紙を参照ください。
また、ガイドブック本編・詳細は内閣府Webサイトに掲載しています。

＊１　内閣府、総務省、経済産業省、国土交通省によって令和元年８月に設立。企業、大学・研究機関、地方公共団体、関係府省等、合計７６４団体（令和３年３月時点）から構成
＊２　オンラインで多様な市民の意見を集め、議論を集約し、政策に結びつけていくための機能を有している参加型民主主義プロジェクトのためのツール。バルセロナやヘルシンキなど世界中の30を超える自治体で利用されており、日本国内では兵庫県加古川市で初めて導入された。

(別紙)スマートシティガイドブックの概要（PDF：624KB）

https://www8.cao.go.jp/cstp/stmain/20210412scity.html

スマートシティガイドブック　目次

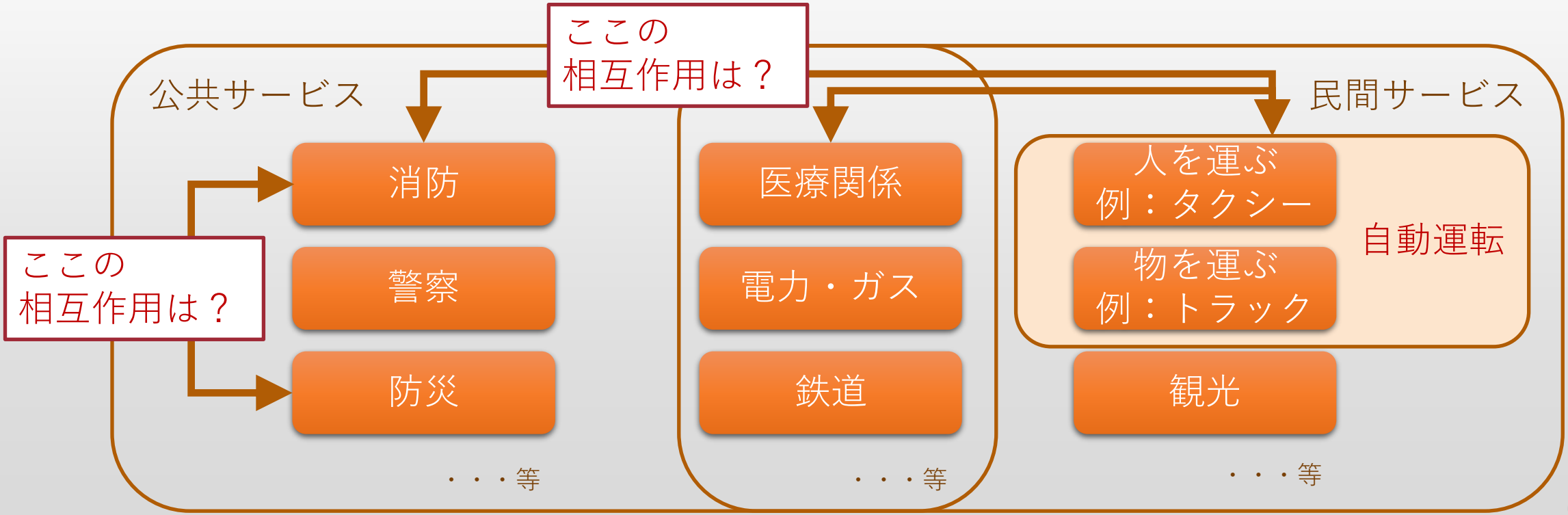
1

https://www8.cao.go.jp/cstp/society5_0/smartcity/01_scguide_1.pdf

はじめに

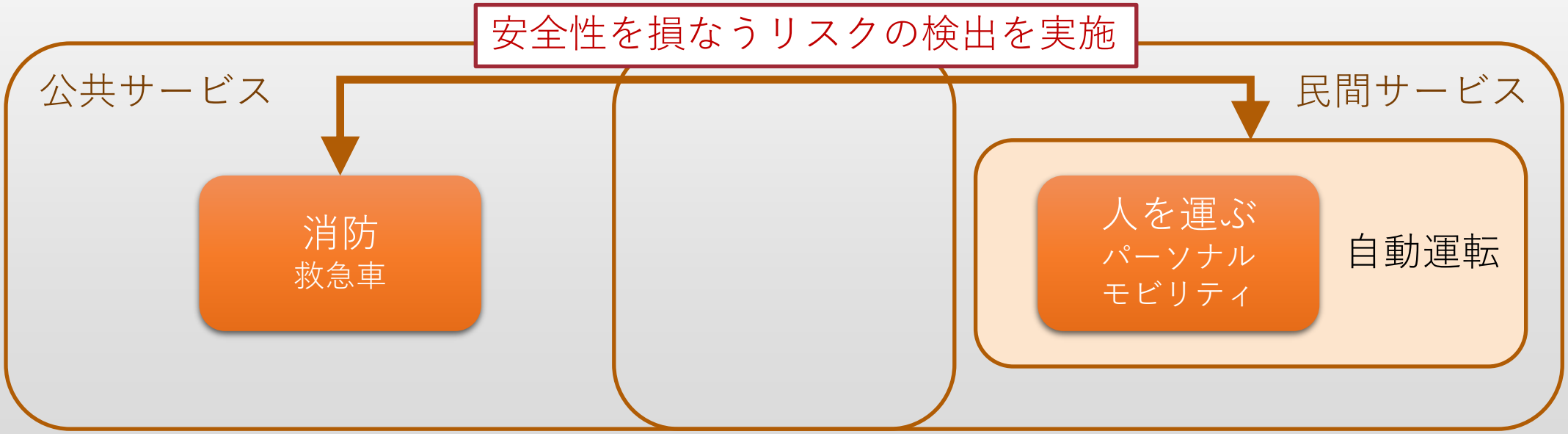
スマートシティでは・・・

- 交通や防災などにおいて多種多様なサービスが存在し、関連する公共・民間サービス提供者が、独自に要素毎の安全性分析を実施している。
- 自身の責任範囲に限定した分析に留まっており、公共・民間サービスやシステムが連携／関与する相互作用については十分考慮されていない。



はじめに

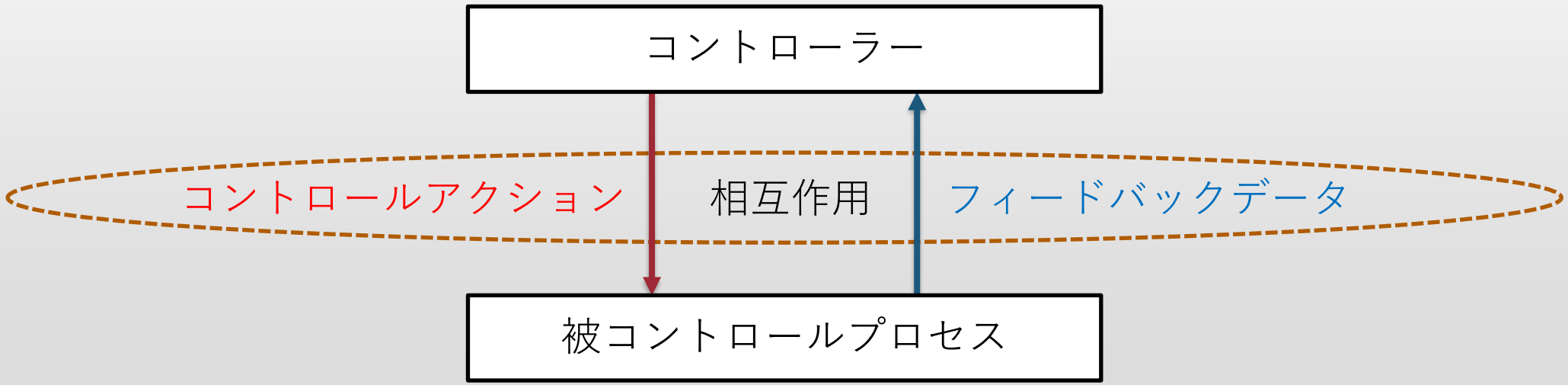
- 多種多様なサービスが連携／関与する特性を、STAMPの制御構造図と、STAMP S&Sの5階層モデルを用いてモデリング
- 自動運転車両を例に、**公共・民間サービスやシステムが連携／関与する相互作用に着目した安全性分析を実施**
- この一環で、公共・民間サービス間の連携によって
  自動運転車両へ間接的にもたらされる、安全性を損なうリスクの検出を実施



関連研究

STAMP（System-Theoretic Accident Model and Processes）

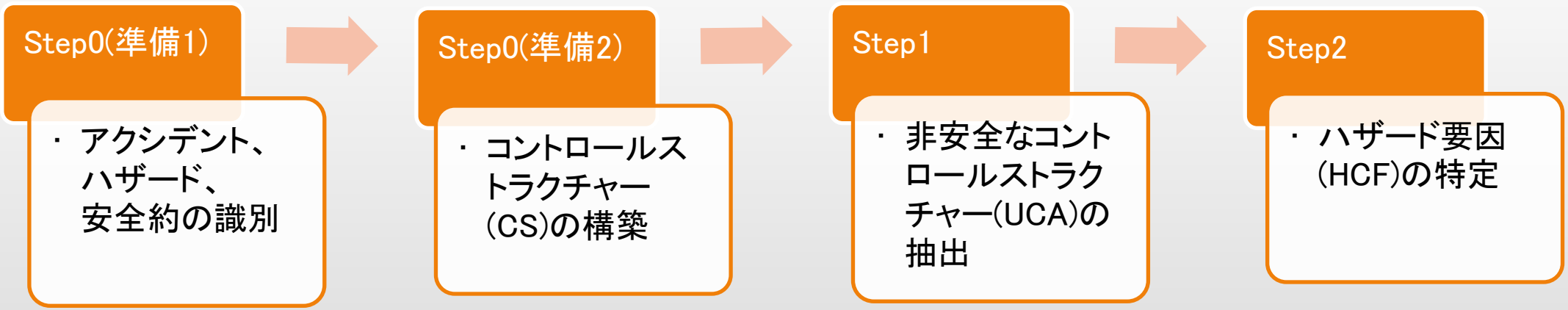
- システムの事故の多くは、構成要素の故障ではなく、システムの中で制御を行う制御要素と、被制御要素の相互作用が適切に働かないことによっておきているという前提をおく。
- 「制御要素（コントローラー）」と「被制御要素（被コントトールプロセス）」の「相互作用」に着目してメカニズムを説明する。
- 「アクションが働かない原因」＝「相互作用の不適切な作用」という視点を持つことで原因を具現化する。



関連研究

STPA（**S**ystem-**T**heoretic **P**rocess **A**nalysis）

STAMP アクシデントモデルを前提として、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である。



関連研究

STAMP S&S

（Safety and Security Integrated Risk Analysis Based on System Theory）
STAMPの適用範囲の広さをベースにして、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、その具体的な適用方法を確立している。本研究では、その中の5階層モデルを活用する。

階層	説明
Society	社会環境・社会生活（規則、基準、習慣）・自然環境（天候などの自然環境）
Stakeholder	ビジネスプロセス。企業や組織が責任を持つ単位
Service	人、サービス、および人と組織によって提供されるサービス
System	コンピュータシステム、ハードウェア、通信機器、半導体チップ
Software	プログラム（アプリケーションソフトウェア、OS、およびその他のソフトウェア）、サイバー情報、データ、AI

安全性分析の検証実験

実験手順

手順１：スマートシティをモデル化する

　スマートシティと自動運転車両の関係を構成する要素をSTAMP S&Sの5階層モデルの考え方（Society、 Stakeholder、 Service、 System、 Software）を用いて抽出する。

　この時点で要素の数や、その関係の複雑性が高過ぎると考えられる場合には、分析の前提条件を追加し、抽出した要素やその関係の中から除外できるものを検討する。

https://global.toyota/jp/newsroom/corporate/31170943.html

https://global.toyota/jp/newsroom/corporate/29933339.html

安全性分析の検証実験

手順２：モデル化したスマートシティのリスクを分析する

STEP0：準備１

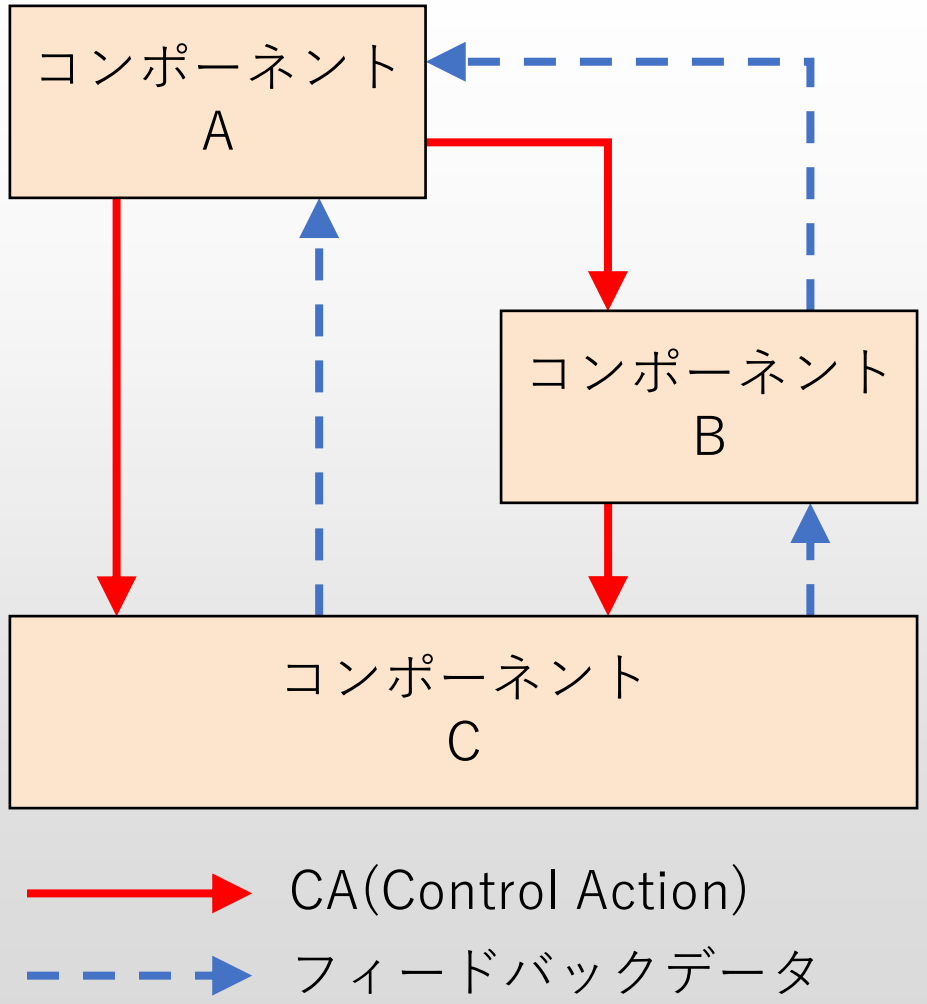
(1) 前提条件の整理
どの領域を重点的に分析するか、あるいは考慮しないかといった、前提を整理。

(2) アクシデント・ハザード・安全制約表の検討
アクシデントを引き起こすハザードを検討し、その発生を防ぐための安全制約を導き出す。

(3) 分析対象のコンポーネントの抽出
分析対象となるコンポーネントを抽出し、それらの責務、CA、フィードバックを導き出す。

STEP0：準備２

安全性分析をしたい具体的な対象について、想定するシチュエーションを検討する。そして、そのシチュエーションにおいて登場する要素を再抽出し、CS図を作成する。



安全性分析の検証実験

手順２

STEP１：Unsafe Control Actionの抽出

　それぞれのコンポーネント間のControl Action（以降、CAと表記）に対し、4つのガイドワードを用いてリスクを検討する。そして、ハザードにつながるCAとしてUnsafe Control Action（以降、UCAと表記）を抽出する。

ガイドワード	説明
Not Providing	適切なアクションが提供されない
Providing causes hazard	提供されたアクションが原因でハザードが起きる
Too early / Too late	アクションの実行が早すぎる／遅すぎる
Stop too soon / Applying too long	アクションの終了が早すぎる／実行が長すぎる

安全性分析の検証実験

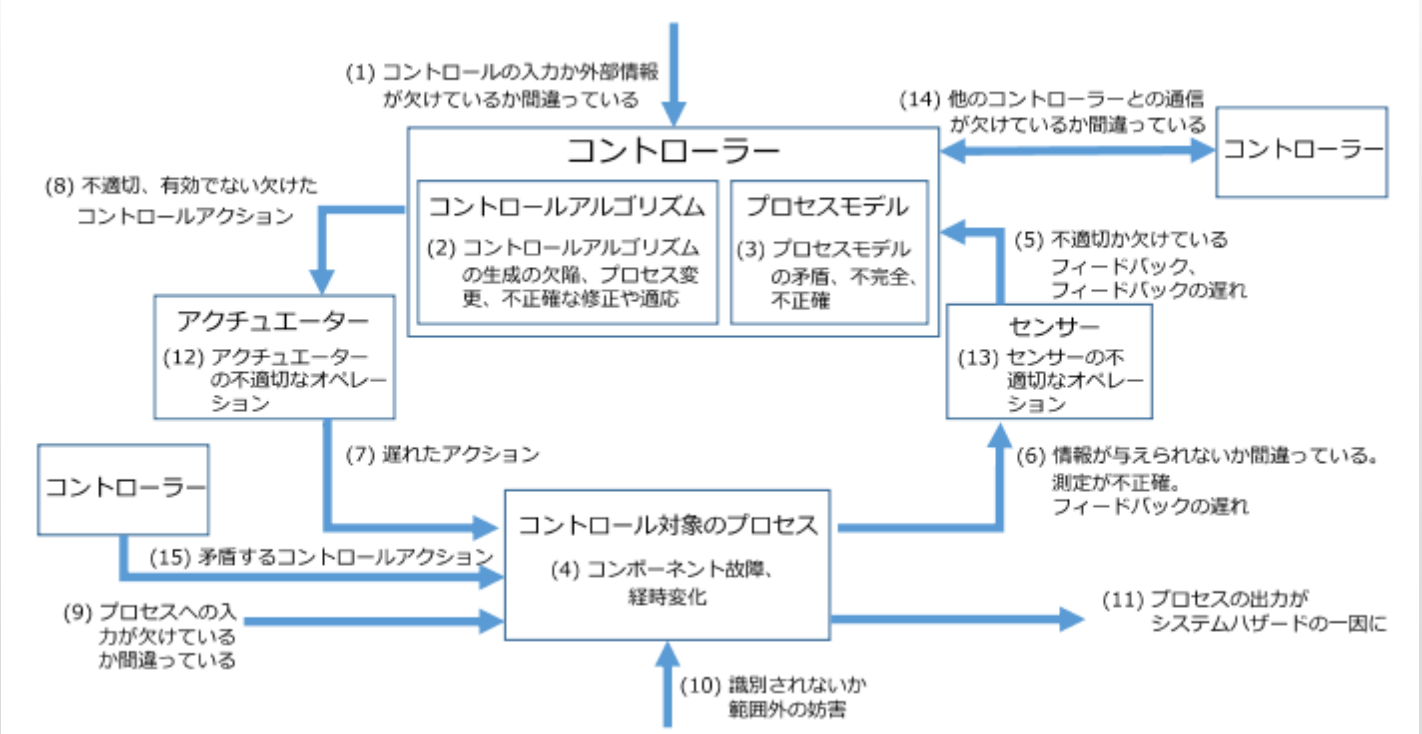
手順２

STEP２： UCAの発生要因 Hazard Causal Factor の特定

UCAを引き起こす Hazard Causal Factor（以降、HCFと表記）を、ヒントワードを用いて特定する。

HCFの特定後、どのようなシナリオでHCFが発生するかを文章にて表現する。

このシナリオが**安全性を損なうリスク**に該当する。



STAMP workbenchより

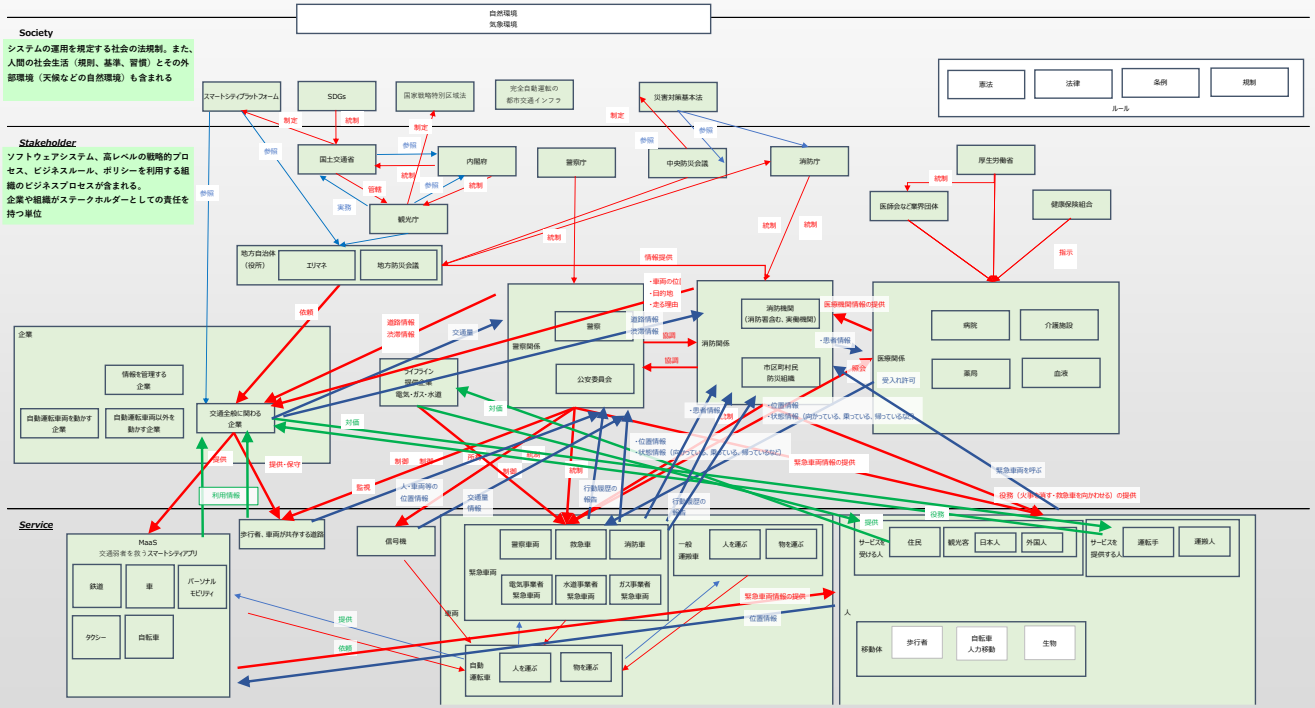
安全性分析の検証実験

実験結果

手順1

　スマートシティの中で、自動運転車両と救急車両の関係に限定した要素を抽出しただけでも、以下のように、多くの要素が現れ、複雑な関係を持つ様を確認できる。
（Societyで5件、Stakeholderで24件、Serviceで25件）

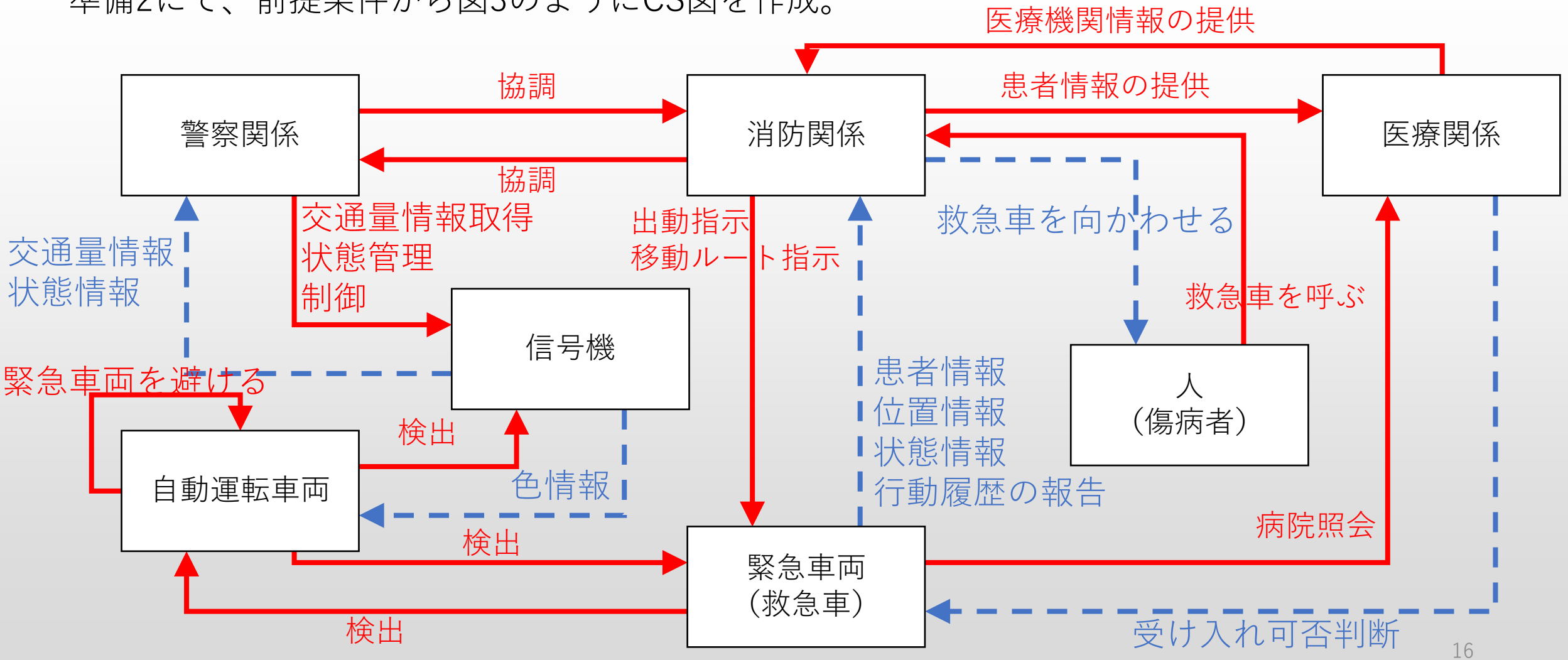
今回の実験では特に人命に係る関係として、
「**救急車が、消防署から出発して、傷病者のいる現場（自動車専用ではないところ）まで向かい、傷病者を収容して病院に搬送し、再び消防署に戻る**」
というシチュエーションとした。



安全性分析の検証実験

手順２

準備2にて、前提条件から図3のようにCS図を作成。



安全性分析の検証実験

手順２ STEP１：Unsafe Control Actionの抽出

CA毎に作業担当者を分け、**UCAを32件抽出**

今回の実験では、stop too soon/applying too longを使って抽出できたUCAは無かった。

UCA抽出結果（一部抜粋）

CA	From	To	Not Providing	Providing Causes hazard	Too eary/Too late	Stop too soon/Applying too long
移動ルート指示	消防関係	緊急車両	(UCA11-N-1)緊急車両に対して目的地が指示されない。 (UCA11-N-2)緊急車両に対して、移動ルートが指示されない。	(UCA11-P-1)誤った目的地が指示される。 (UCA11-P-2)渋滞した移動ルートが指示される。	(UCA11-T-1)道路の通行止め情報が遅れて伝達される。 (UCA11-T-3)解消されていない通行止めが解消されたと伝達される。	-

安全性分析の検証実験

手順２ STEP２：UCAの発生要因 Hazard Causal Factor の特定

HCFの特定は、UCA単位で担当者を割振って実施し、**HCFを56件、付随するシナリオを58件特定した。**

本実験で使用した分析支援ツール”STAMP Workbench”には、分析対象システムの特徴に応じて選択可能なヒントワードのセットが複数用意されていた。今回は情報・機械からなるシステムにおけるHCFの特定で使いやすいヒントワードを主に活用した。組織対組織といったシステムで使いやすいヒントワードを活用する場合もあった。

HCFの特定結果（一部抜粋）

HCF	ヒントワード	シナリオ
基準があいまいで、警察関係者へ緊急車両の出動情報が伝達されない	(1) Not Providing（指示がでない）	消防から警察への伝達方法、手段があいまいで、警察関係者へ緊急車両の出動情報が伝達されない。その結果、信号が緊急用に切り替わらない。
伝達手段が故障し、警察関係者に緊急車両の出動情報が伝達されない	(5) 指示（口頭・電話・メール・FAXなど光、音、旗）	消防から警察への伝達手段が故障し、警察関係者へ緊急車両の出動情報が伝達されない。その結果、信号が緊急用に切り替わらない。

考察

良かった点（1/2）

- 自動運転車両と救急車両との間の直接的な相互作用だけではなく、間接的な組織、装置等の相互作用の問題によって自動運転車両の衝突リスクがあることを検出できた。
  例：消防と警察の連携不良により、交通管制が適切に行えず緊急車両と
  　　自動運転車両の衝突に繋がる、など

- 公共・民間サービス提供者の関係性を5階層モデルで精緻化できた。
  但し、コンポーネントが増えるほど関係性が複雑になる。このため、どのような抽象度でモデル化するかは吟味が必要である。

考察

良かった点（2/2）

- STAMP Workbenchのガイドワード・ヒントワードを使えば、5階層モデルの上位層・下位層によらず分析は（初心者でも）可能なことを確認できた。
  ⇒　但し、分析対象のドメインや階層によって、ガイドワード・ヒントワードをより最適なものに変える余地はあると考える。

- HCFのヒントワードを使うことによって、CS図のCAを加えた方がよい、といった気づきも得られた。
  例：ヒントワードに記載の「矛盾したCA」から、矛盾・競合しうるCAが抜けていないか？という観点が生まれる。

考察

悪かった点（工夫すべき箇所）

- ガイドワード「Stop too soon / Applying too long」はStakeholder・Serviceの階層に適用しても、有用なUCAが検出できなかった。
  この階層に関しては新たなガイドワードを設ける余地がある。

- 対象が多くて複数人で分析を分担する際には、UCAやHCFの表現に揺らぎが生じるリスクがある。前提条件の置き方、分析観点の設定、分析対象の絞り込みについて事前の十分な認識合わせが必要。

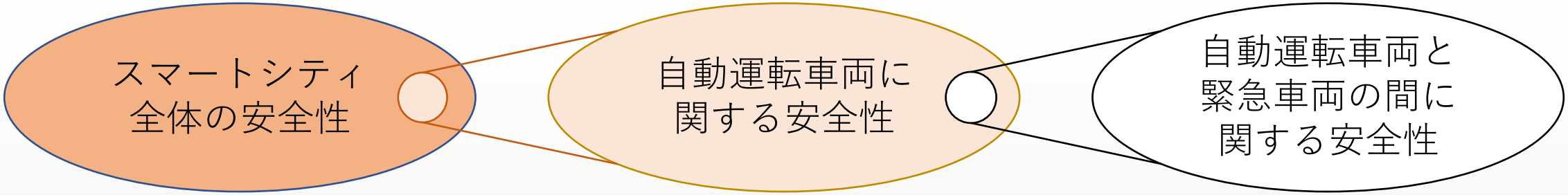
- スマートシティではコンポーネントが多様になるため、分析は膨大な作業量になる。
  前提条件や分析対象の絞り込みを行い、「もっとも防ぎたいハザード」から
  優先順位をつけて分析を施すことが必要。ハザードの発生確率と発生時の影響度を
  勘案するとよい。

まとめ

- スマートシティにおける公共・民間サービスやシステムが連携／関与する部分について、本研究では自動運転車両に着目した。そして、STAMPを活用して、安全性分析を行い、自動運転車両へ間接的にもたらされるリスクを検出することができた。
- STAMP S&Sの5階層モデルの適用によって、スマートシティの開発にあたって考慮すべき、組織間の連携を明らかにすることができた。
- STAMP/STPAのCS図を用いることで、複雑な構成要素間の関係を考慮して分析することができた。

今後の課題

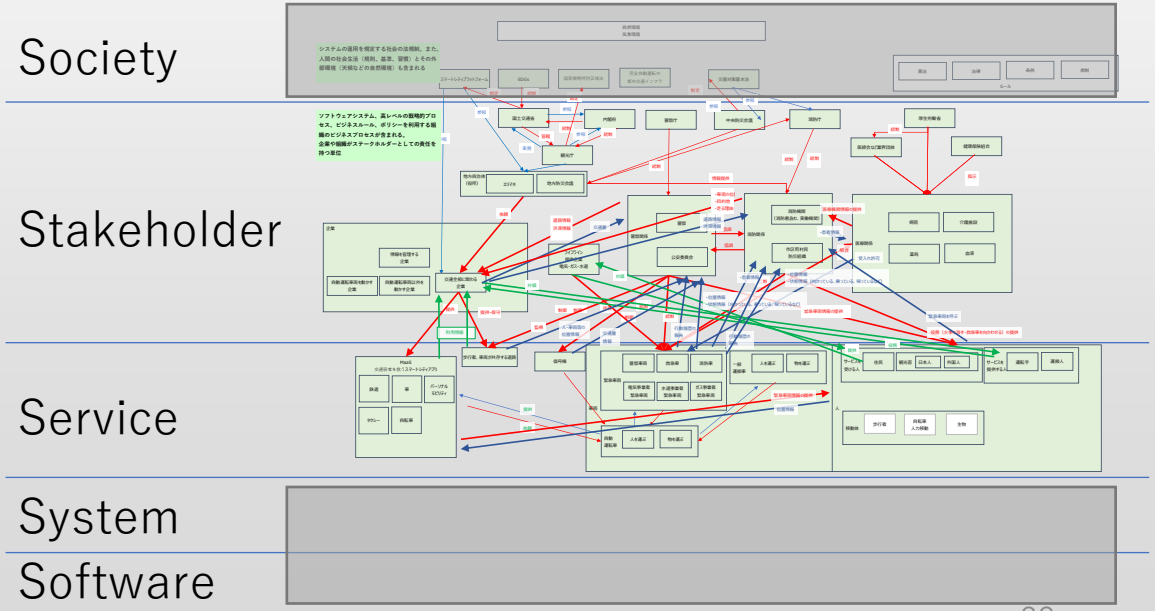
分析の対象範囲に関する課題



- 本研究における安全性分析の対象は、スマートシティ全体で考慮すべき安全性のごく一部。今後はこの分析対象をスマートシティ全体へと広げていく必要がある。

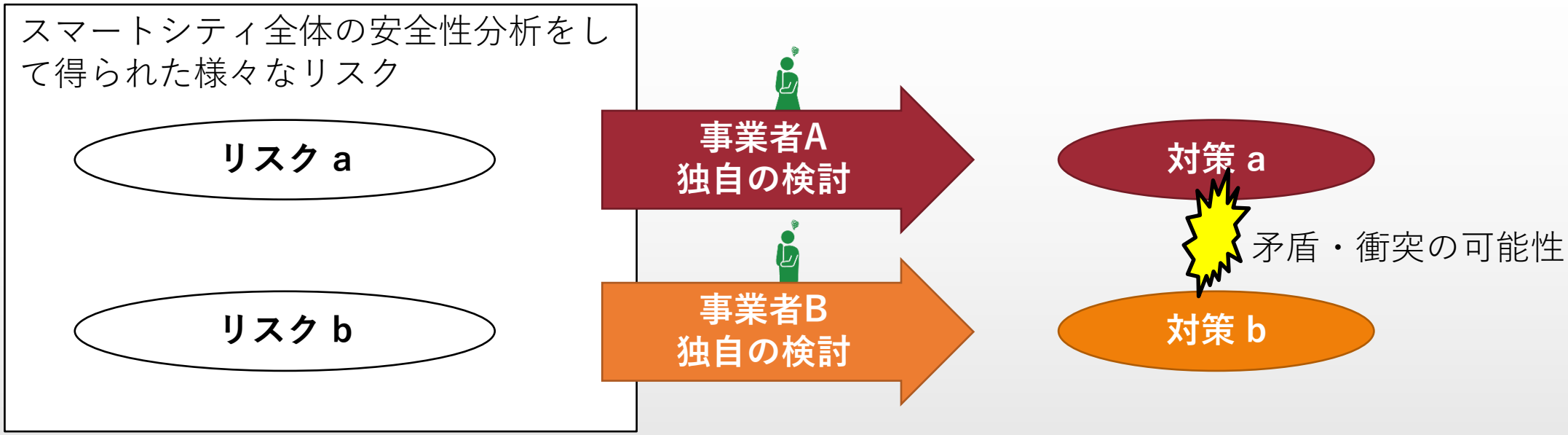
- 今回は、Societyの領域まで含めた分析はしなかった。今後、スマートシティに対する安全性の分析を進める場合、この領域も含める必要がある。

- 今回の分析ではセキュリティについては言及しなかった。今後の分析において、セーフティとセキュリティの分析を合わせて実施できる方法も検討したい。



今後の課題

STAMP/STPAを活用する場合の課題



STAMP/STPAは安全性分析手法であり、得られたリスクへの対策を検討する手法は含まれていない。
この対策において、妥当性と一貫性を確保する必要がある。Society、Stakeholder、Serviceの領域ではこうした課題を解決できる手法の研究例はなく、今後の検討が必要である。

参考資料

- 内閣府・総務省・経済産業省・国土交通省 スマートシティ官民連携プラットフォーム, スマートシティガイドブック, https://www8.cao.go.jp/cstp/society5_0/smartcity/00_scguide_s.pdf
- 総務省, スマートシティセキュリティガイドライン(第2.0版), https://www.soumu.go.jp/main_content/000757800.pdf
- ISO：ISO/IEC Guide 51:2014, https://www.iso.org/standard/53940.html
- Kaneko, Tomoko; Yoshioka, Nobukazu; Sasaki, Ryoichi. “STAMP S&S: Layered Modeling for the complexed system in the society of AI/IoT”, 2020 IEEE 20th International Conference on Software Quality, Reliability and Security Companion (QRS-C), 2020, 2020.12.11-14
- 独立行政法人 情報処理推進機構(IPA),はじめてのSTAMP/STPA ～システム思考に基づく新しい安全性解析手法～ Ver.1.0, https://www.ipa.go.jp/sec/reports/20160428.html
- 独立行政法人 情報処理推進機構(IPA),STAMP Workbench Ver.2.0.0, https://www.ipa.go.jp/sec/tools/stamp_workbench.html
- スマートシティおよび自動運転車両の参考画像 https://toyotatimes.jp/toyota_news/construction_wovencity/122.html https://global.toyota/jp/newsroom/corporate/29933339.html

参考スライド