一般社団法人日本科学技術連盟
第38年度（2022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」
2023年2月24日（金）

STAMP/STPAを用いた 高齢者見守りシステムのIoT化に対する安全性分析

発表者：鎌田　桂太郎（アイホン）

主査：　金子　朋子（エヌ・ティ・ティ・データ）
副主査：　髙橋　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 品質保証第一課	インターホンシステム全般	参加3年目でSTAMPが少しずつ理解できました。 今年度は当社製品に関連した分析に取り組みました。

https://www.aiphone.co.jp/

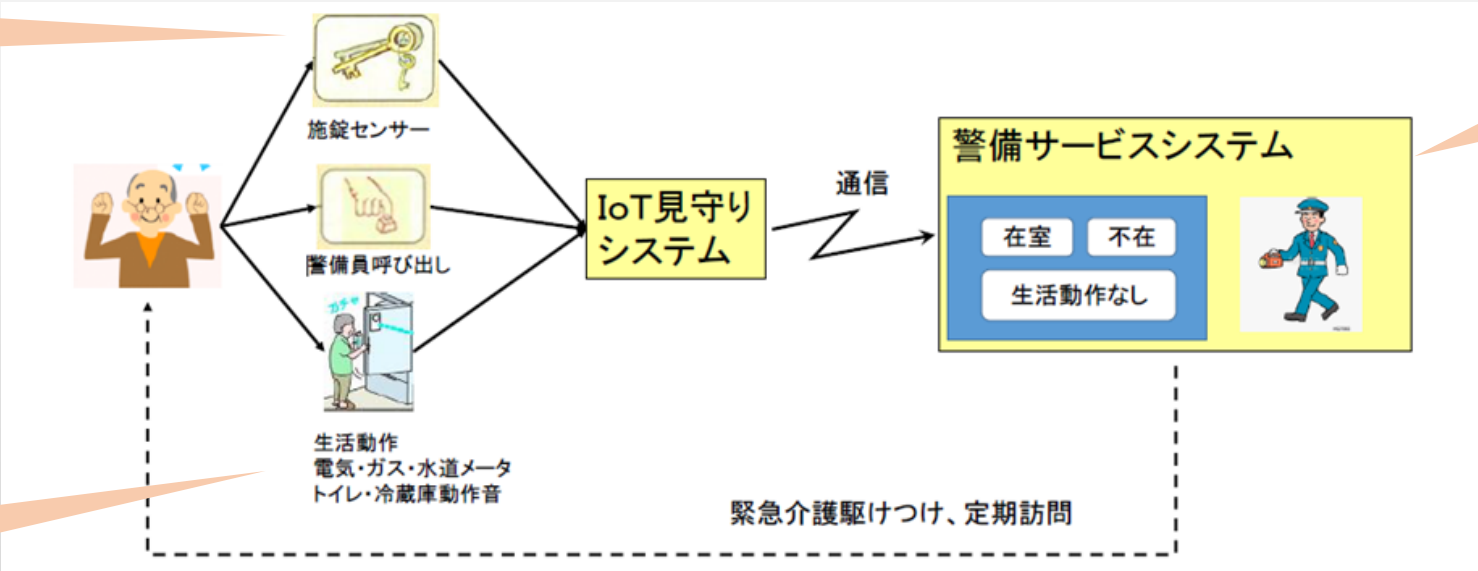
アイホン株式会社は、住宅向けインターホン・ドアホン、オフィス・工場向け各種通話機器、医療・福祉施設向けナースコールなどの製造販売メーカーです。

はじめに

高齢者見守りサービスは少子高齢化・介護労働力不足・孤独死などの社会課題を解決するとともに，新たな価値を創造する取り組みとして期待されている

社会課題 | 少子高齢化 | 介護労働力不足 | 孤独死 | 感染症 | ・・・等

センサー類



民間企業

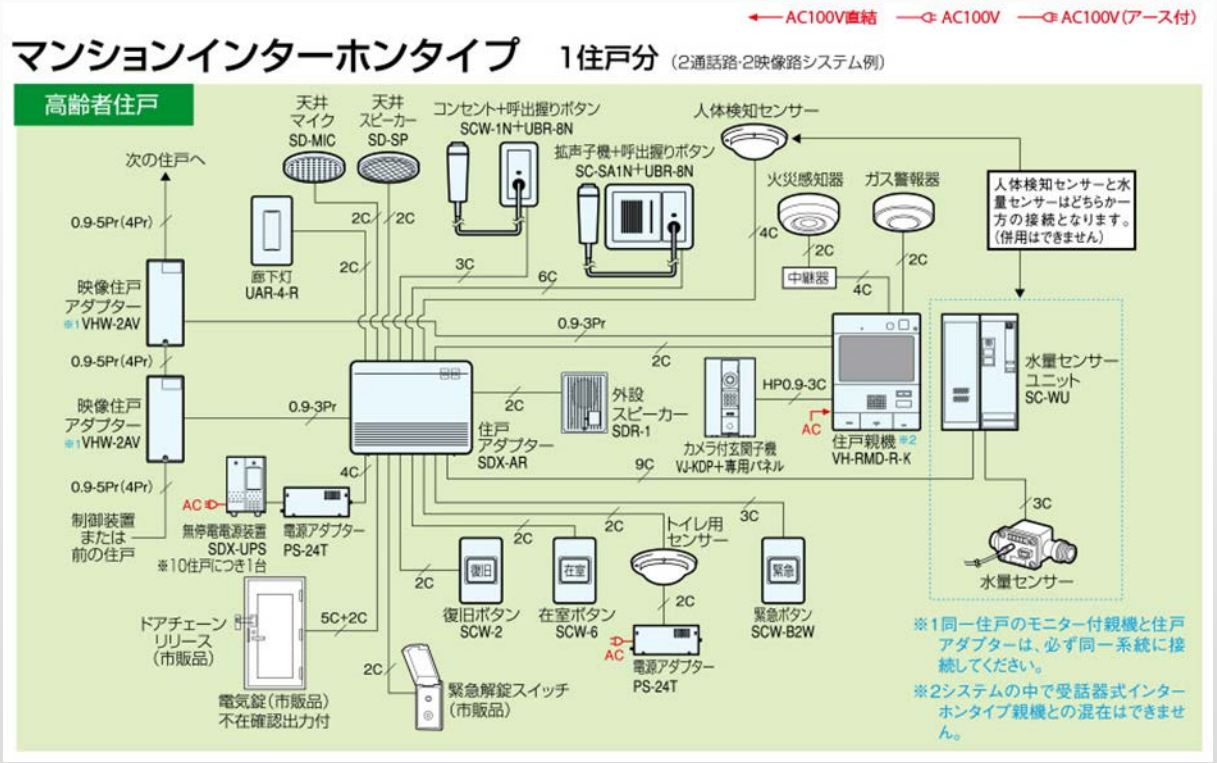
インフラ

https://www.ipa.go.jp/ikc/reports/20190329.html

はじめに

政府機関（国土交通省・厚生労働省）によってサービス付き高齢者向け住宅の登録制度が制定されている。この中で、安否確認（セーフティ）については定義されているものの、IoT連携に対する安全性（セーフティ）については指針が示されていない。

https://www.mlit.go.jp/jutakukentiku/house/jutakukentiku_house_tk3_000005.html

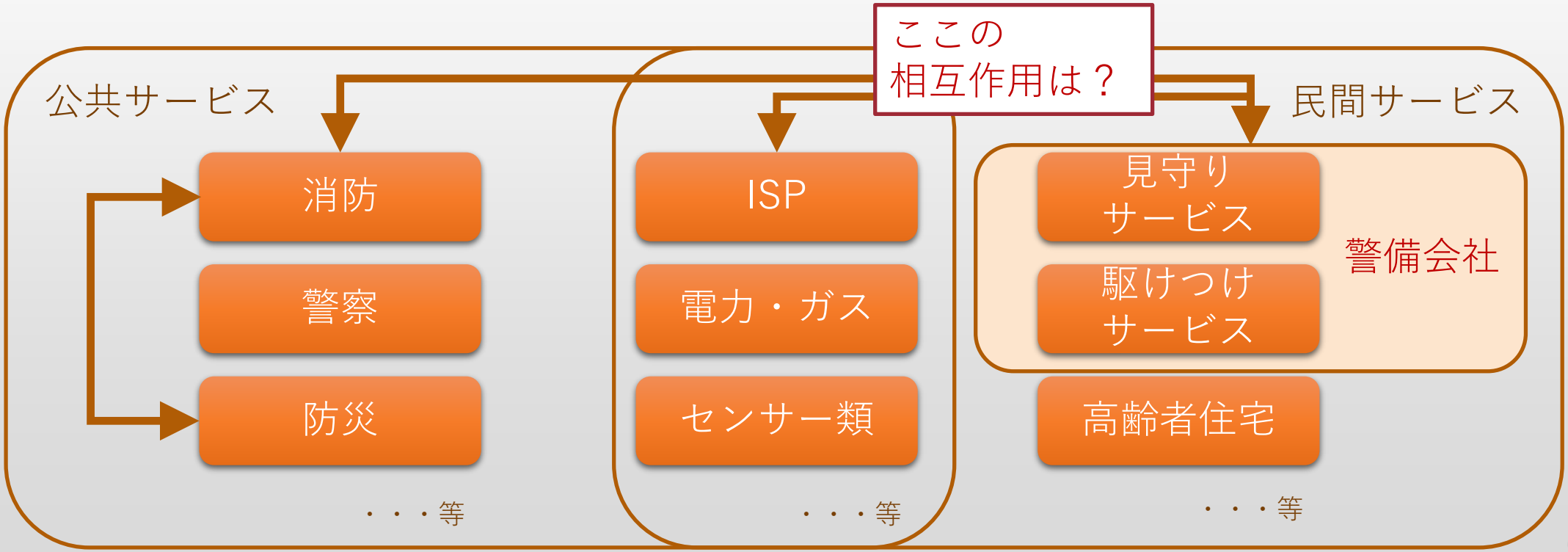


https://www.aiphone.co.jp/products/medical_welfare/fagus/system/images/img_system-draft_03.jpg

はじめに

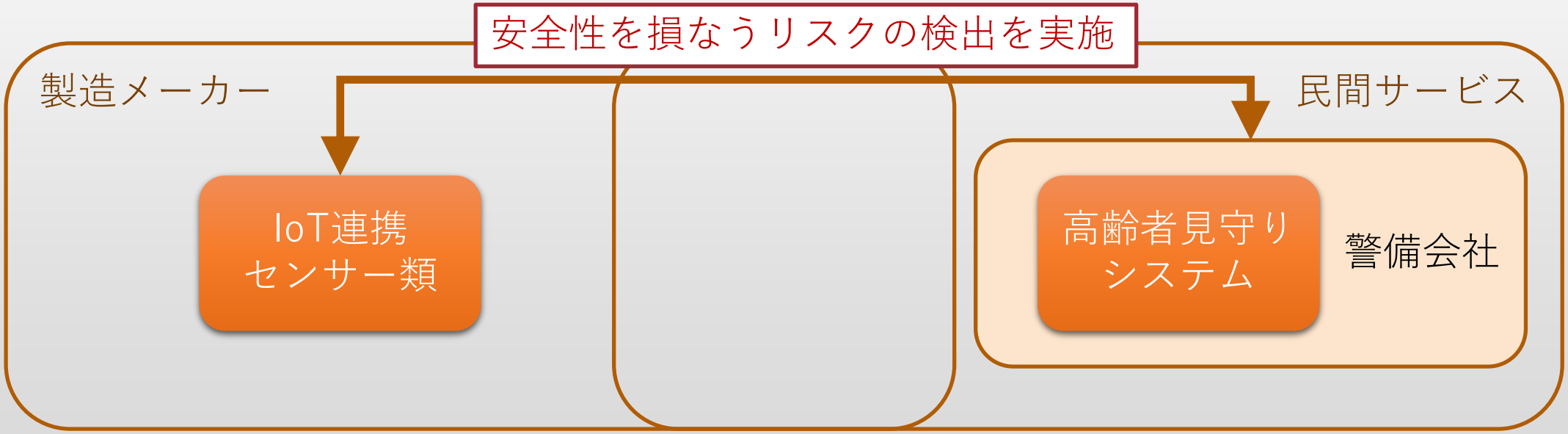
高齢者見守りサービスでは・・・

- 高齢者見守りサービス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

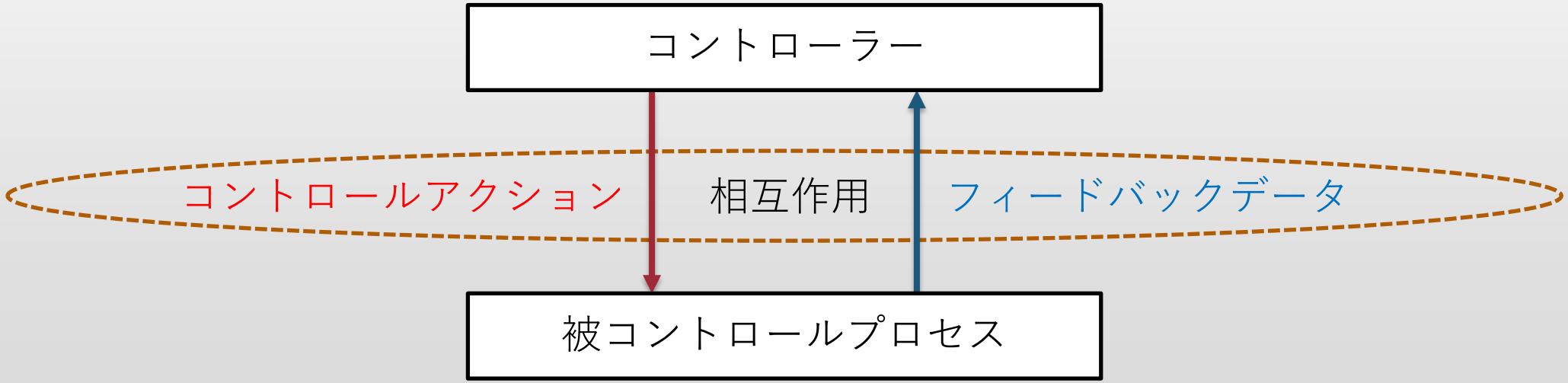
- 多種多様なサービスが連携／関与する特性を、STAMPの制御構造図と、STAMP S&Sの5階層モデルを用いてモデリング
- 高齢見守りサービスを例に、**民間サービスやIoTセンサー類とシステムが連携／関与する相互作用に着目した安全性分析を実施**
- この一環で、民間サービス間のIoT連携によって
  高齢者へ間接的にもたらされる、安全性を損なうリスクの検出を実施



関連研究

STAMP（System-Theoretic Accident Model and Processes）

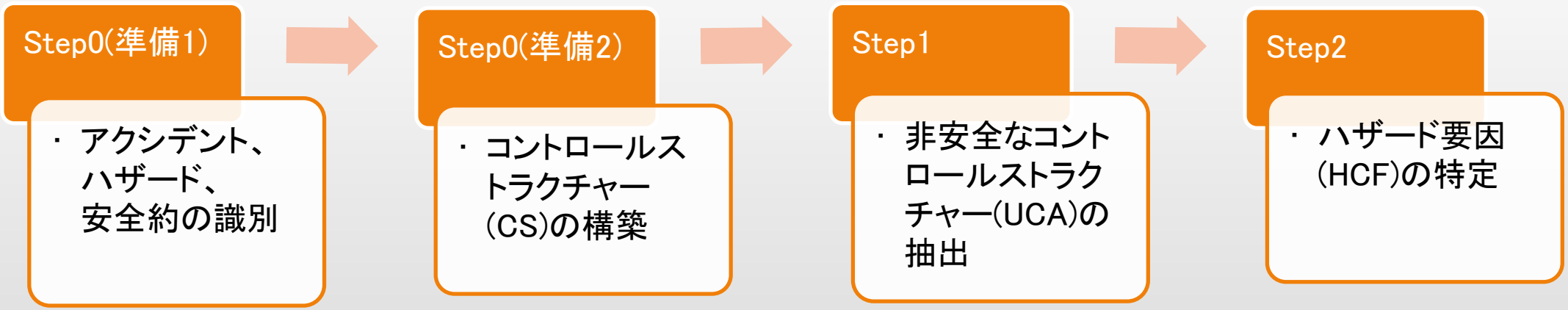
- システムの事故の多くは、構成要素の故障ではなく、システムの中で制御を行う制御要素と、被制御要素の相互作用が適切に働かないことによっておきているという前提をおく。
- 「制御要素（コントローラー）」と「被制御要素（被コントロールプロセス）」の「相互作用」に着目してメカニズムを説明する。
- 「アクションが働かない原因」＝「相互作用の不適切な作用」という視点を持つことで原因を具現化する。



関連研究

STPA（System-Theoretic Process Analysis）

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

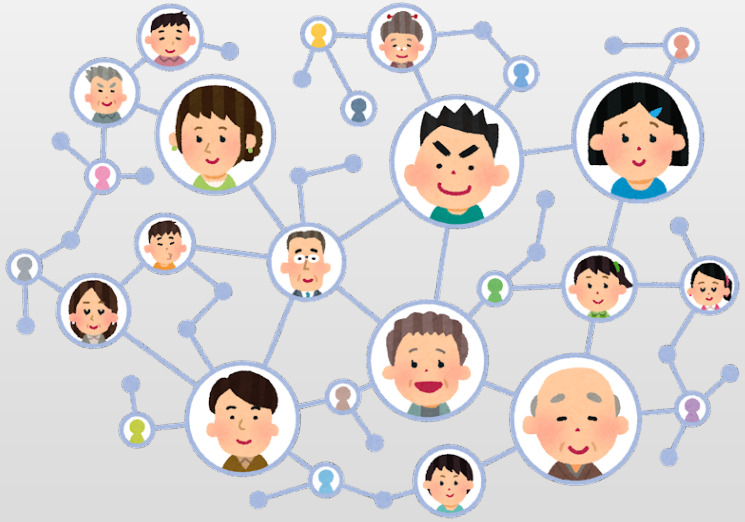
実験手順

手順１：高齢者見守りサービスをモデル化する

　高齢者見守りシステムとIoT連携センサー類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://www.ipa.go.jp/files/000052459.pdf



https://www.aiphone.co.jp/products/medical_welfare/fagus/

安全性分析の検証実験

手順２：モデル化した高齢者見守りサービスのリスクを分析する

STEP0：準備１

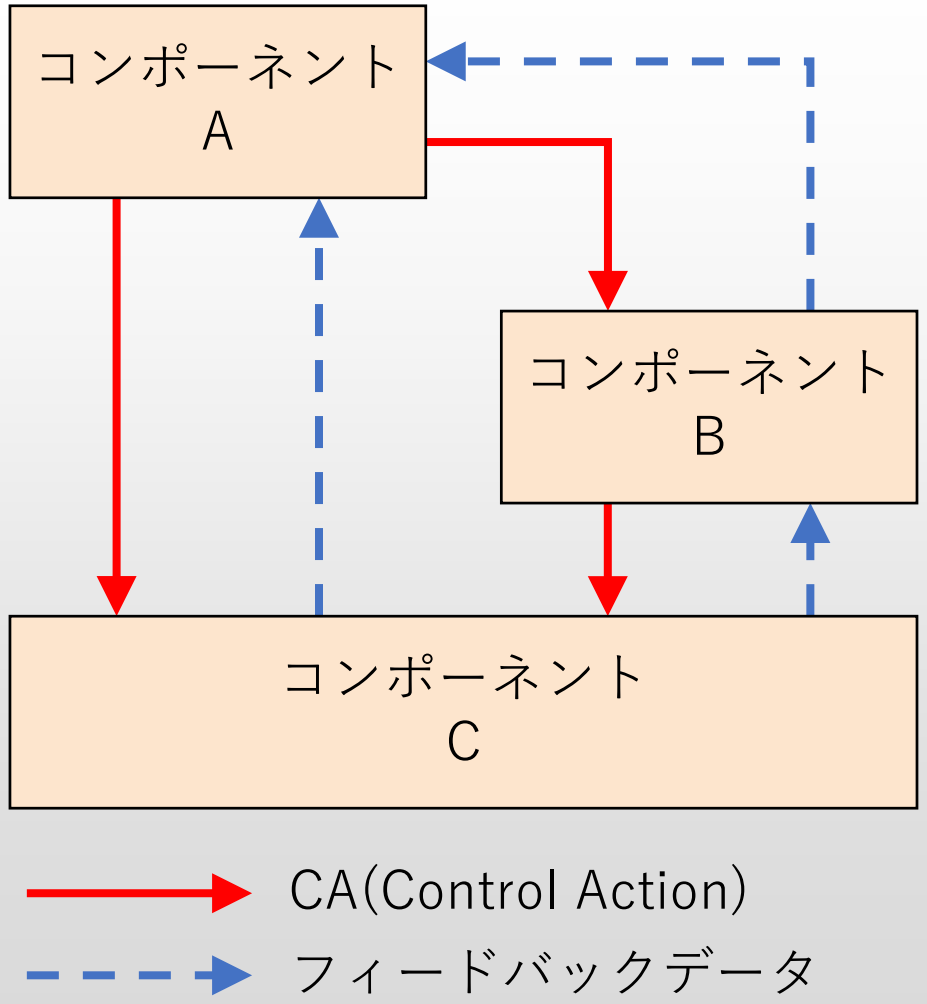
(1) 前提条件の整理
どの領域を重点的に分析するか、あるいは考慮しないかといった、前提を整理。

(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：UCA（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

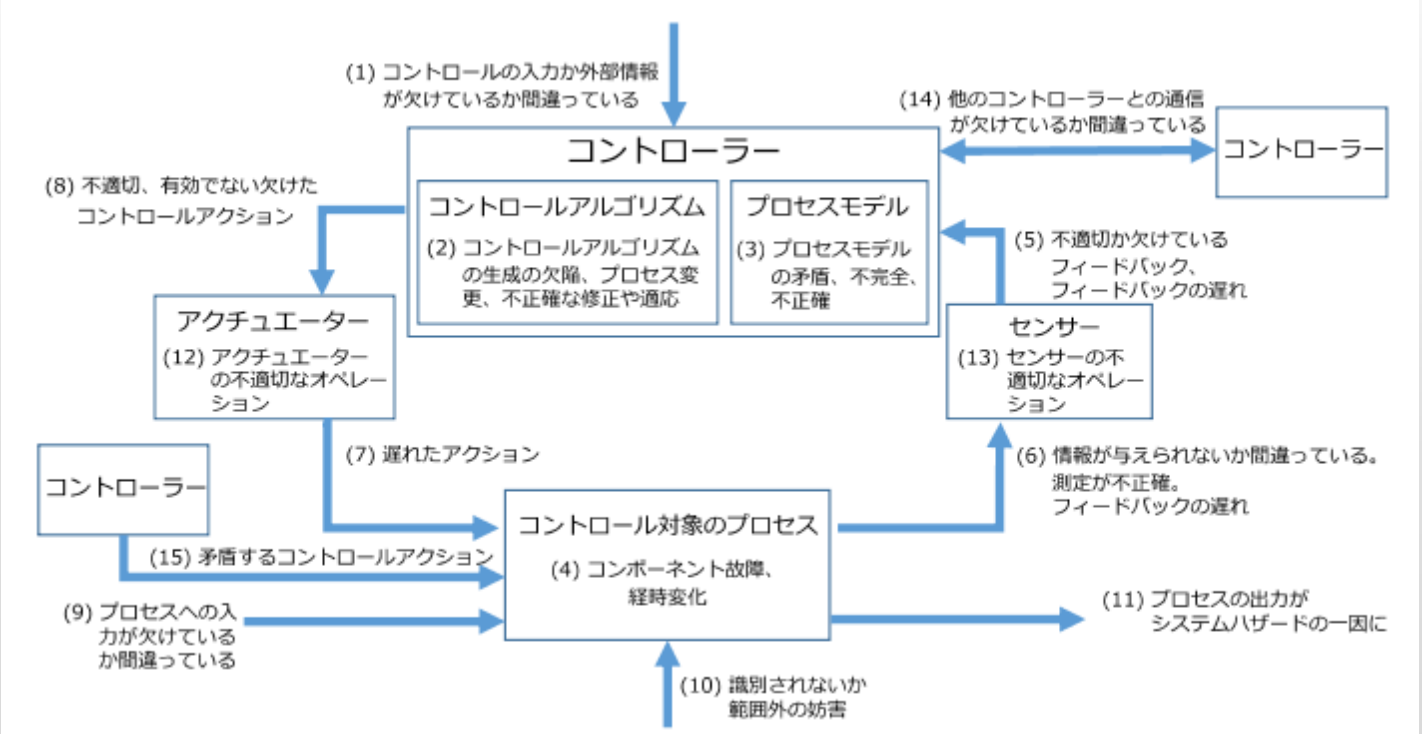
手順２

STEP２： UCAの発生要因 HCF(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

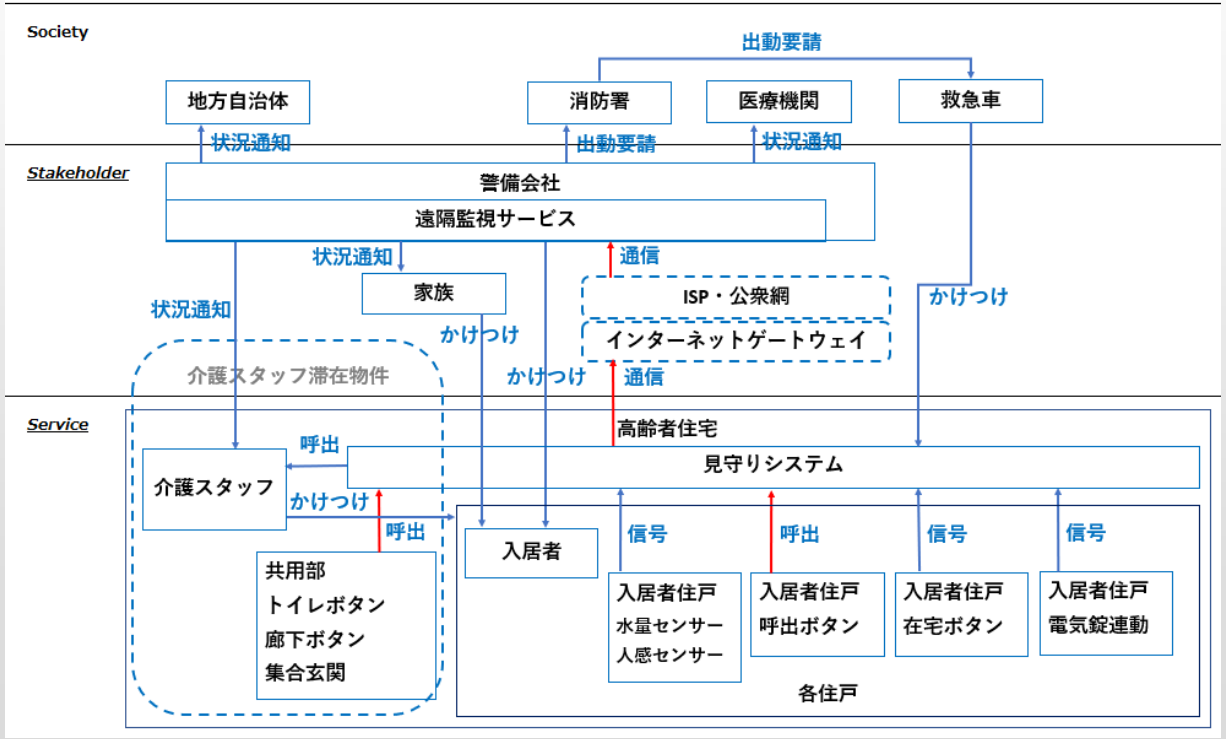
手順1　STEP0：準備1

　高齢者見守りサービスの中で、サービス提供者とセンサー類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4件、Stakeholderで5件、Serviceで8件）

今回の実験では特に人命に係る関係として、

「**IoT連携センサー類が高齢者の何らかの異常を検知する。見守りシステムに通知を送信し、クラウドサーバから警備会社に通知を送信する。訪問スタッフが現地を訪問し、状況を確認後に、消防署に救急車を依頼する。**」

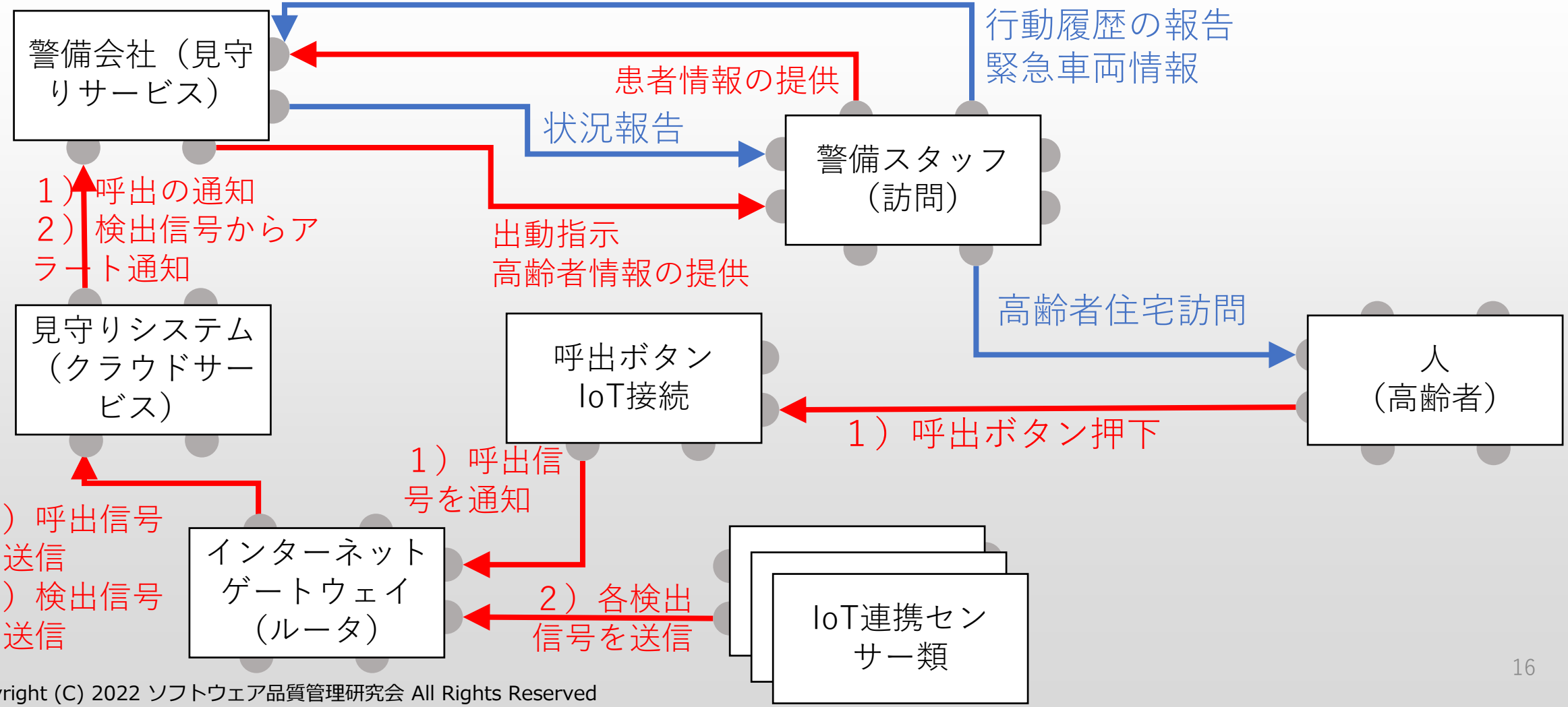
というシチュエーションとした。



安全性分析の検証実験

手順２　STEP0：準備2

準備2にて、前提条件から以下のように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毎に分け、**UCAを18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
呼出ボタン押下	人（高齢者）	呼出ボタン（IoT接続）	(UCA14-N-1) 呼出ボタンを押下されたが通知されない (UCA14-N-2) 呼出ボタンを押下できない	(UCA14-P-1) 呼出ボタンを押下されないが通知された	(UCA14-T-1) 呼出ボタンを押下されたが通知に遅延が発生した [SC1]	-

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単位で実施し、**HCFを16件、付随するシナリオを56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An STPA Primerで使いやすいヒントワードを主に活用した。

HCFの特定結果（一部抜粋）

HCF	ヒントワード	シナリオ
呼出ボタンを押下されたが見守りシステムから見守りサービスに通知されない	(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	クラウドサーバからの通信が遮断された クラウドサーバからの通信がドロップした クラウドサーバからのトラブルにより停止した
呼出ボタンを押下されたがインターネットゲートウェイへの通知に遅延が発生した	(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	通信経路の機器が故障し遅延した 通信経路の他通信により遅延した 通信経路にウィルス等で遅延した

考察

良かった点（1/2）

- 高齢者見守りサービスと高齢者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通知の遅延・不通知リスクがあることを検出できた。
  例：IoT接続センサー類の通信経路により通知が適切に行えず、見守りシステムに不通知になり、警備スタッフがかけつけができず、人命に関わる事故に繋がる、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。
  今回の5階層モデルでは、IoT接続センサー類は具体的なメーカー、モデルを特定していないため、system・softwareについては除外している。

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。

- コンポーネントが多いシステムを分析する際には、分析範囲を広くするため複数人での分析が有効となる。
  複数人による分析時は、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。

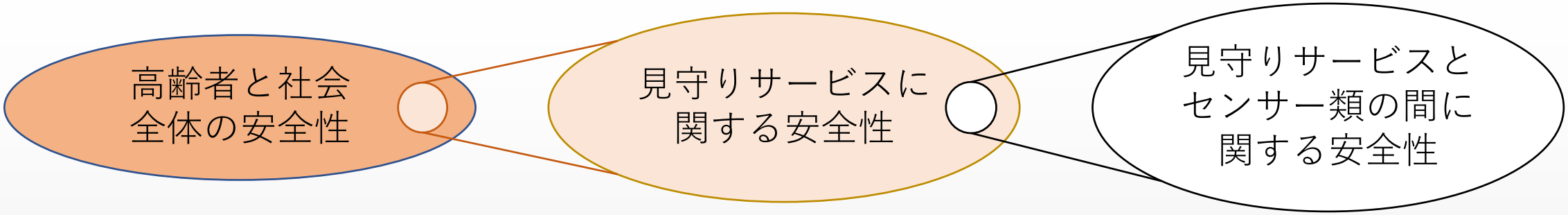
- 高齢者見守りサービスではコンポーネントが多様なため、分析は膨大な作業量になる。
  前提条件や分析対象の絞り込みを行い、「もっとも防ぎたいハザード」から
  優先順位をつけて分析を施すことが必要。ハザードの発生確率と発生時の影響度を
  勘案するとよい。

まとめ

- 高齢者見守りサービスにおける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IoT連携に着目した。そして、STAMPを活用して、安全性分析を行い、高齢者見守りサービス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、高齢者見守りサービスの開発にあたって考慮すべき、システム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

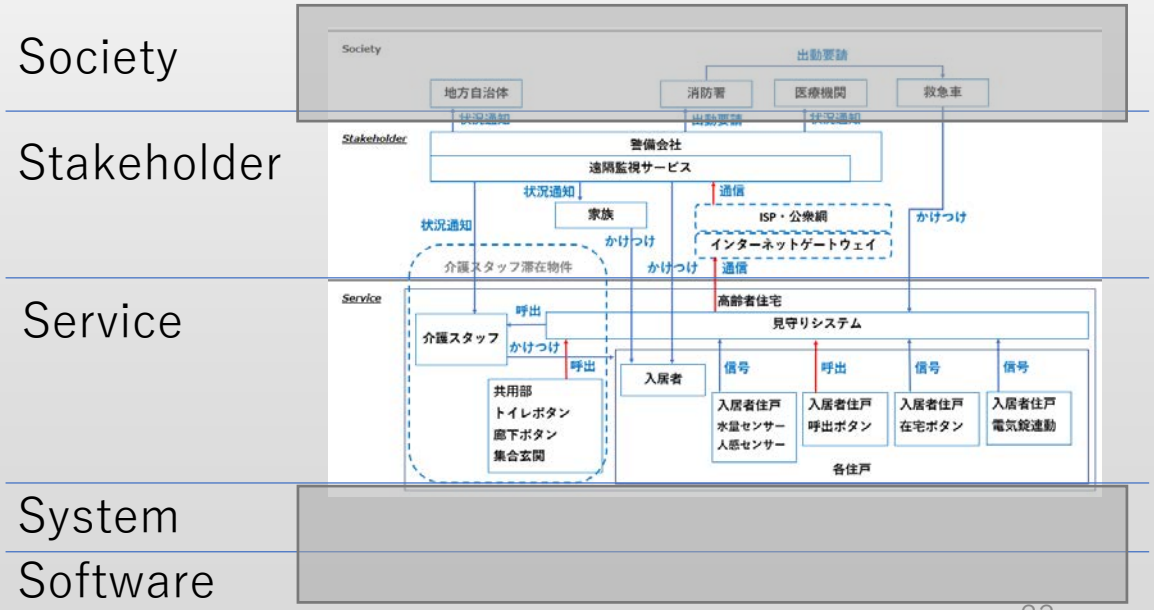
分析の対象範囲に関する課題



- 本研究における安全性分析の対象は、高齢化社会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高齢化社会全体へと広げていく必要がある。

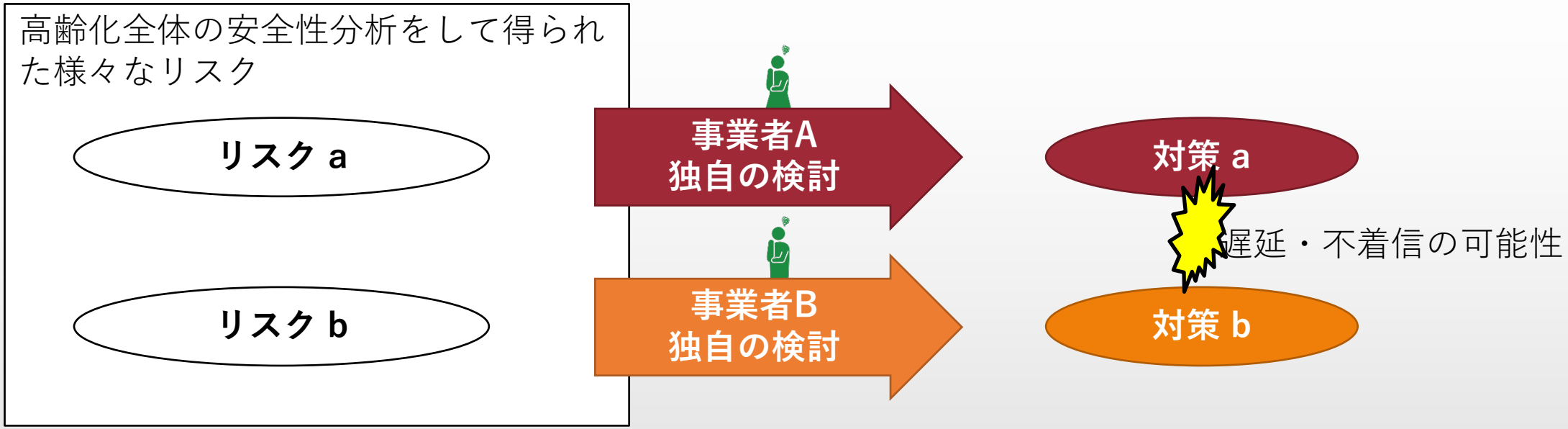
- 今回は、Societyの領域まで含めた分析はしなかった。今後、高齢化社会に対する安全性の分析を進める場合、この領域も含める必要がある。

- 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

- サービス付き高齢者向け住宅の登録制度の概要, https://www.mlit.go.jp/jutakukentiku/house/jutakukentiku_house_tk3_000005.html
- 独立行政法人 情報処理推進機構(IPA), STAMPガイドブック ～システム思考による安全分析～ Ver.1.0, https://www.ipa.go.jp/ikc/reports/20190329.html
- 高齢者向け集合住宅システム FAGUS［ファガス］, https://www.aiphone.co.jp/products/medical_welfare/fagus/
- ISO：ISO/IEC Guide 51:2014, https://www.iso.org/standard/53940.html
- ナンシー・G・レブソン著, 松原友夫 監訳・訳, 片平真史, 吉岡律夫,西康晴, 青木美津江 訳：『セーフウェア　安全・安心なシステムとソフトウェアをめざして』, 翔泳社, 2009年。
- 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

参考スライド