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

Safety analysis for IoT implementation of elderly monitoring system using STAMP/STPA

研 究 員：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）

研究概要
近年，老人ホームにおいても人感センサーなどを用いた IoT による見守りサービスを導入するケースが増えている．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．高齢者の居住の安定確保に関する法律は，国土交通省・厚生労働省の連携，サービス付き高齢者向け住宅の登録制度はあるが，IoT 技術の普及に伴って，各種見守りサービスが提供されており，多くの公共・民間サービスが存在する．各サービスについて既存のシステムとサービスについては、システム内連携、運用に関するリスクについて考慮されているが、IoT 連携に関する安全性の考慮がされていない．本稿では，従来のシステムから置き換わりが進むと予測される IoT を利用した見守りシステムについて，アクシデントモデルとその安全性解析手法である STAMP/STPA を活用し，各サービス間の IoT 連携に潜む安全性分析を行った．その結果，従来リスクに加えて通信経路，サーバ連携不良，機器へのセキュリティ対策など，サービス間の相互作用とセキュリティに関するリスクを検出した．

1. 背景

近年，高齢者住宅において人感センサーなどを用いた IoT による見守りサービスを導入するケースが増えている．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．高齢者の居住の安定確保に関する法律は，国土交通省・厚生労働省の連携，サービス付き高齢者向け住宅の登録制度[1]はあるが，IoT 技術の普及に伴って各種見守りサービスが提供されており，多くの公共・民間サービスが存在する．既存のシステムは機器と連携サービスについて，システム内連携，運用に関するリスクについて考慮されているが，IoT 連携に関する安全性の考慮がされていない[2]．

従来から提供されている高齢者見守りシステムとして，アイホン社製高齢者見守りシステム FAGUS［ファガス］がある[3]． 当該システム(図 1)はインターホンシステムに各種センサーを接続することで見守りシステムを構成している．当該システムは連携する機器間は専用線で接続し，集中統合型システムして設計されている．システム内の各センサー連携については動作確認がされた機器で構成されるなど，通信経路と連携動作が設計段階で検証，動作確認されている．運用については介護スタッフの駐在など呼出と異常検知時には即座に対応が可能な運用となっているサービス付き高齢者住宅向けの構成となる．本システムは，集中統合型であり今後は IoT 対応した分散協調型のシステムとして展開していくことが望まれる．

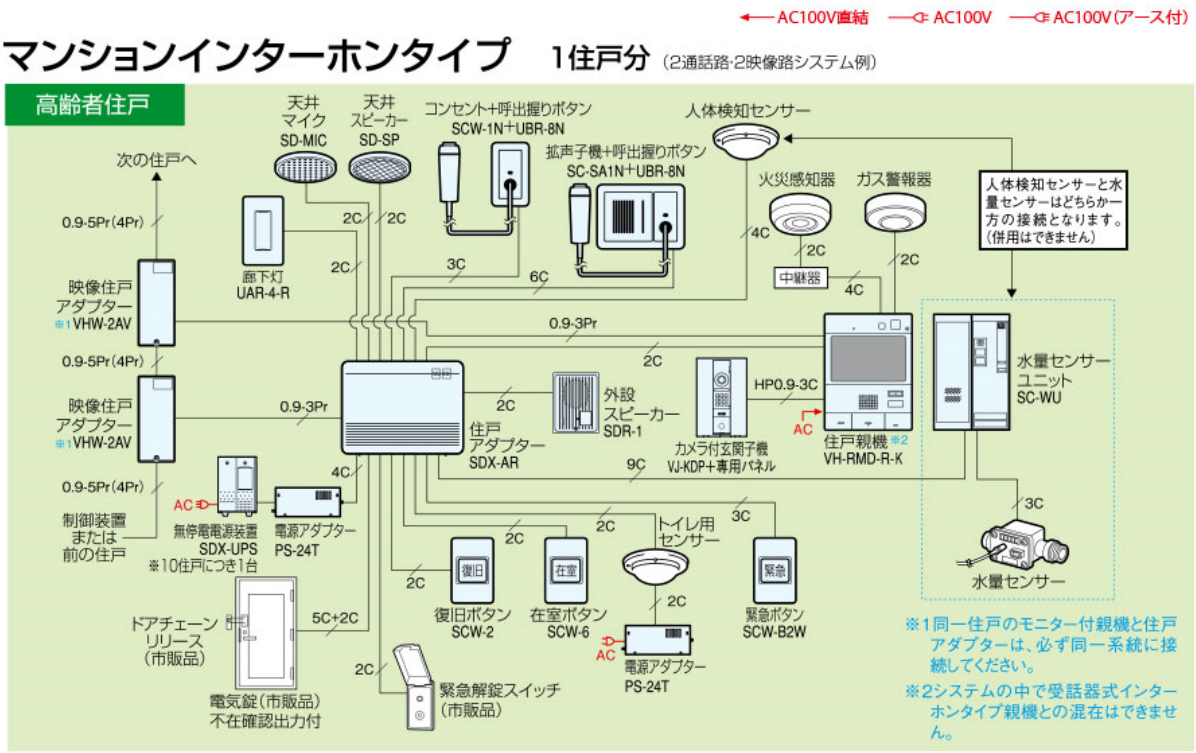

図 1　既存の高齢者見守りシステムの例（詳細は参考文献[3]を参照）

前述のような専用機器による構成から IoT の進展に伴い，その応用例として高齢者（独居）世帯の見守りサービスがある．高齢者世帯の監視はプライバシーに配慮した形で生活動作情報を得る必要があり，多様なセンサーと通信手段を持つ IoT 機器がこれを可能にしている．IoT を利用したサービスの価値は独立のベンダーが相互に情報を利用しあってサービスを提供するため，多様で付加価値の高いサービスが提供できることにある．分散協調型のシステム開発といえる．集中統合型のシステム開発と異なり，サブシステム相互の情報利用に矛盾が出てきてサービスが安全を脅かすことになると考えられる．何らかの被害が出た際の責任の所在があいまいになるといった問題点が指摘できる．

事例として，文献[2] では実際に提供された高齢者見守りサービスシステムの不具合報告がなされている．図 2 は，当該サービスの構成図となる．

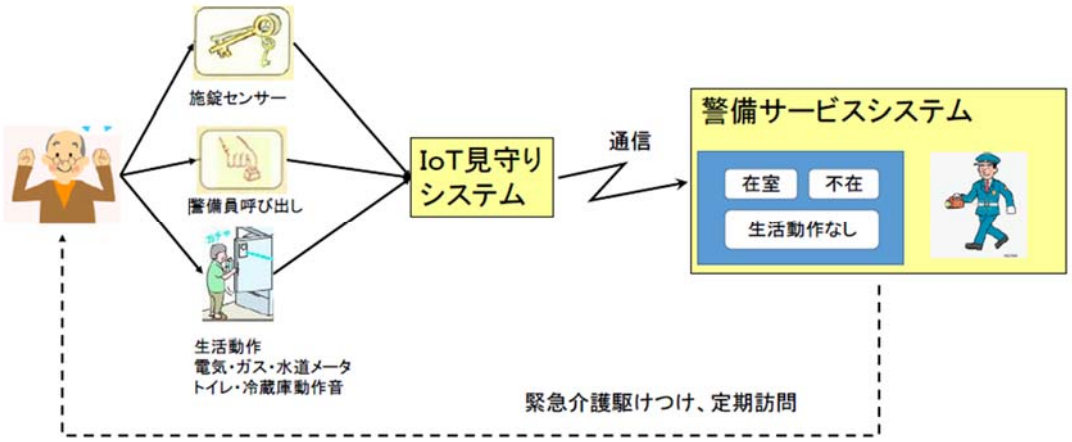

図 2　サービスの構成図（詳細は参考文献[2]を参照）

IoT 連携による高齢者見守りシステムは，セキュリティと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．安全性とは「許容不可能なリスクがないこと」[4]と定義され，人の生命や健康に関わる「事故や損失がないこと」[5]を指す．「安全・安心な高齢者見守りの実現」に向けて，高齢者見守りシステムのリスク分析・対応が重要である．

そこで我々は，多種多様なサービスが連携／関与する特性を STAMP（System-Theoretic Accident Model and Processes）の制御構造図（Control Structure Diagram:以降，CS 図と表記)と,金子らによって提唱されている STAMP（System-Theoretic Architecture Model and Processes）S&S[6]の 5 階層モデルを用いることでモデリングできるようになると考えた．

本稿では従来のシステムから置き換わりが進むと予測される IoT を利用した見守りシステムについて，アクシデントモデルとその安全性解析手法である STAMP/STPA を活用し，各サービス間の IoT 連携に潜む安全性分析を行った．その結果高齢者見守りシステムへ連携するセンサー類にもたらされるリスクと，セキュリティ上の安全性を損なうリスクの検出が出来た．

2. 関連研究・技術・製品

2.1. STAMP

Nancy Leveson が提唱した STAMP モデルでは，システムの様々な階層でコントローラと被コントロールプロセスに該当する要素が存在しており，それらの相互作用が適切に働くことによりシステムの安全が実現されるとする[7]．STAMP モデルは，アクシデントは相互作用が適切に働かないことによって起こるとしている．たとえコントローラも被コントロールプロセスも故障せずに,仕様通りに正しく動作していても,不適切な制御指示(Control Action：以降，CA と表記）が与えられることによって，最終的にアクシデントにつながるというモデルなのである．また，コンポーネント間の CA，フィードバックデータといった相互作用を分析するために，CS 図を構築する．CS 図はコンポーネント間の制御，被制御，情報のフィードバックを図示できるもので，制御の流れや情報の流れを容易に把握できると考える．

2.1.1. STPA (System-Theoretic Process Analysis)

Leveson らが提唱した STPA は STAMP アクシデントモデルを前提として，システムのアクシデントの可能性が潜在している状態（以降，ハザードと表記）とその要因を事前に分析するための安全性分析手法である[7]．従来は，FTA（Fault Tree Analysis）や FMEA（Failure Mode and Effect Analysis）の手法が用いられてきたが，これらは，単一コンポーネントの分析には有用であるが，相互作用が複雑なシステムの安全性分析においては十分ではないため，新しいアクシデントモデルによる分析手法が必要とされた．

STPA では，4 種類のガイドワード（ Not Providing , Providing causes hazard , Timing Too early/Too late , Duration Stop too soon/Applying too long）によって安全でない CA を抽出することが可能である．この手法を利用することで，サービス同士の連携においても，安全性を損なう連携を相互作用として抽出できるのではないかと考えた．

2.1.2. STAMP S&S

STAMP S&S は従来の STAMP を応用した金子らの提案である．S&S は，Safety，Security の他，Society，Stakeholder，Service，System，Software の 5 階層と，Scenario，Specification，Standard の複数の S による相互作用のモデルを示している[6]．その方法は分析対象を 5 層にモデル化し，自然環境や社会規範などの社会自体や公共・民間サービス・AI システムを含めた世界をシステム思考で捉え，対象間の相互作用を詳細化し，安全

性分析に役立てる方法である.

我々は，この手法の 5 層モデルを適用することで Society から Software に至るまでの階層および，各階層に属する様々な構成要素において，それらの間の関係を考慮した分析が可能になると考えた．5 層モデルの定義を表 1 に示す.

表 1　STAMP S&S の 5 層モデルの定義

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

すなわち，STAMP S&S の 5 階層モデルに高齢者見守りシステムを構成する各要素を割り当て，CS 図でその相互関係を明確にし，CA を抽出することによって安全性を脅かすリスクが分析できるのではないかと考えた.

3. 安全性分析方法の検証実験

本実験では，STAMP/STPA を用いて，従来から提供されている高齢者見守りシステムにおいて，置き換わりが進むと予測されるセンサー類の IoT 機器連携を中心としたシステムの安全性分析を行う．この一環で，IoT 機器間の連携によって高齢者見守りシステムへ間接的にもたらされる，安全性を損なうリスクを検証する．具体的な分析内容については，手順を追って説明する.

3.1. 実験の手順

3.1.1.　手順 1：高齢者見守りシステムの関係を構成する要素（Society, Stakeholder, Service, System, Software）を STAMP S&S モデルの考え方を用いて抽出する．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.

3.1.2.　手順 2：抽出した要素に対し，STAMP/STPA の手法を利用してリスク分析を実施する.

(1) Step0：(準備 1) アクシデント，ハザード，安全制約の識別

(a) 前提条件の整理

手順 1 で抽出した要素を踏まえた CS 図をベースに，どの領域を重点的に分析するか，どのような前提を置くかを整理.

(b) アクシデントハザード安全制約表の検討

重点的な分析対象となったコンポーネントに対し，発生してはならないアクシデントと，それを発生させるハザードを検討する．検討したハザードを発生させないために課すべき安全制約を導き出す.

(c) 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.

(2) Step0：(準備 2) CS 図の構築

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抽出し，CS 図を新たに作成する.

今回は，CS 図の作成に STAMP Workbench[8]を用いた.

(3) Step1：Unsafe Control Action（以降，UCA と表記）の抽出
ハザードにつながる CA を抽出.それぞれのコンポーネント間の CA に対し，過去のアクシデント事例に基づいた 4 つのガイドワードを用いて UCA を抽出する.
(4) Step2：UCA の発生要因（Hazard Causal Factor）（以降，HCF と表記）の特定
UCA を引き起こす HCF を，ドメインエキスパートでない人でも分析できる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のリスクに該当する.

3.2. 実験結果

手順 1 の結果，図 3 のように Society で 4 件，Stakeholder で 5 件，Service で 8 件の要素を抽出した.

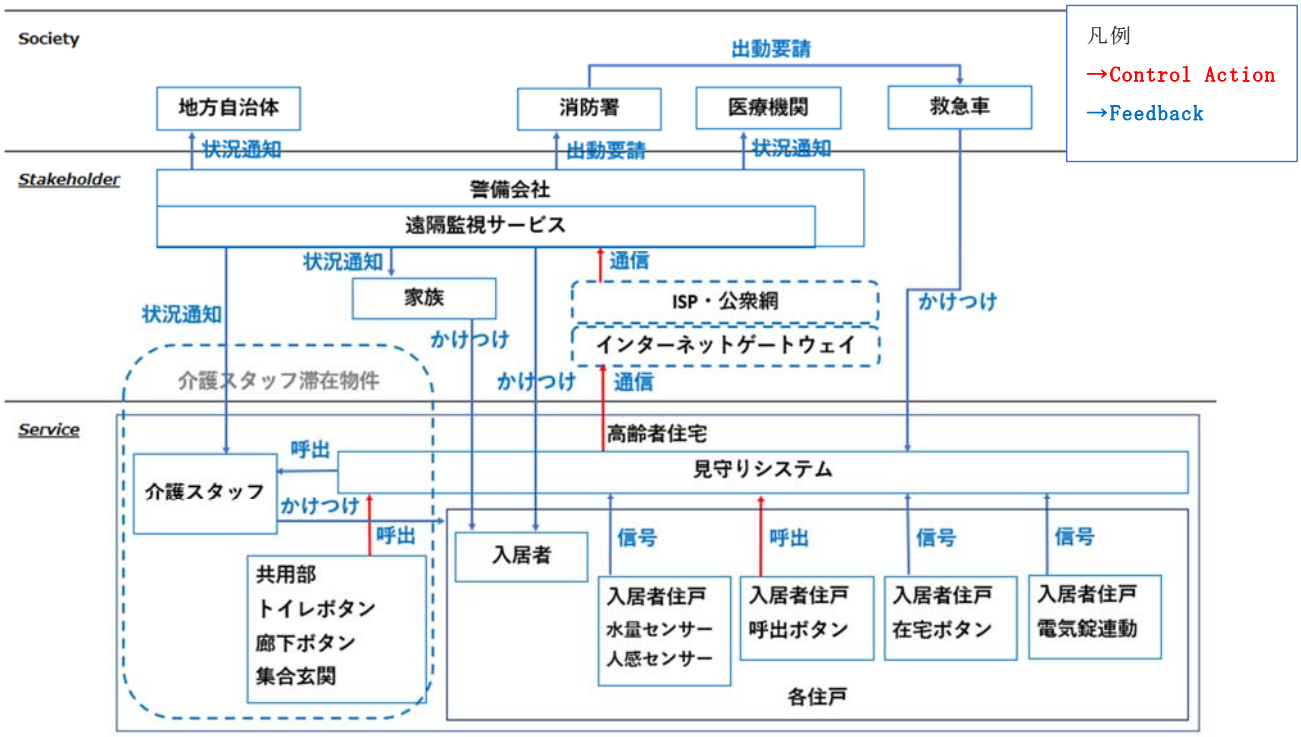

図 3　CS 図 整理前
（5 階層のうち Society，Stakeholder，Service 部分を抜粋．詳細は付録参照）

コンポーネント間の関係性を精緻に抽出すると,コンポーネント数が増えれば増えるほど関係性が複雑になるため，一度抽出した関係性のうち，特に人命に係る関係として,「センサー類は異常を検知しているが、高齢者見守りシステムは異常を検出できず、警備会社に通知ができない」というシチュエーションに絞り,通信障害，IoT 機器に対する攻撃によって通信を阻害されたりするリスクを分析することとした.その理由として,例えば,センサーは A 社,見守りシステム本体は B 社,警備会社は C 社というように会社を跨ぐような構成で責任の所在や取るべき対策も変わってくるなどの問題であると考えた.

次に，手順 2 の結果として以下の分析結果を得た.

Step0：準備 1 にて 5 層モデルを使用し，図 4 のように分析を進める上で必要な仮定や前提条件を整理した．高齢者見守りシステムに関連する公共・民間サービス提供者，高齢者見守りに関連した条件を多く整理した．整理した前提条件から公共・民間サービスやそれらに関連するシステムが連携／関与する部分に着目し，Stakeholder-Service 間のリスク分析を行うことにした.

ID	名前
Pre-4	Stakeholder - Service間 の通信に関するリスクを分析する

図 4　前提条件一部抜粋（詳細は付録参照）

Step0：準備 2 にて，前提条件から図 5 のように CS 図を作成した．

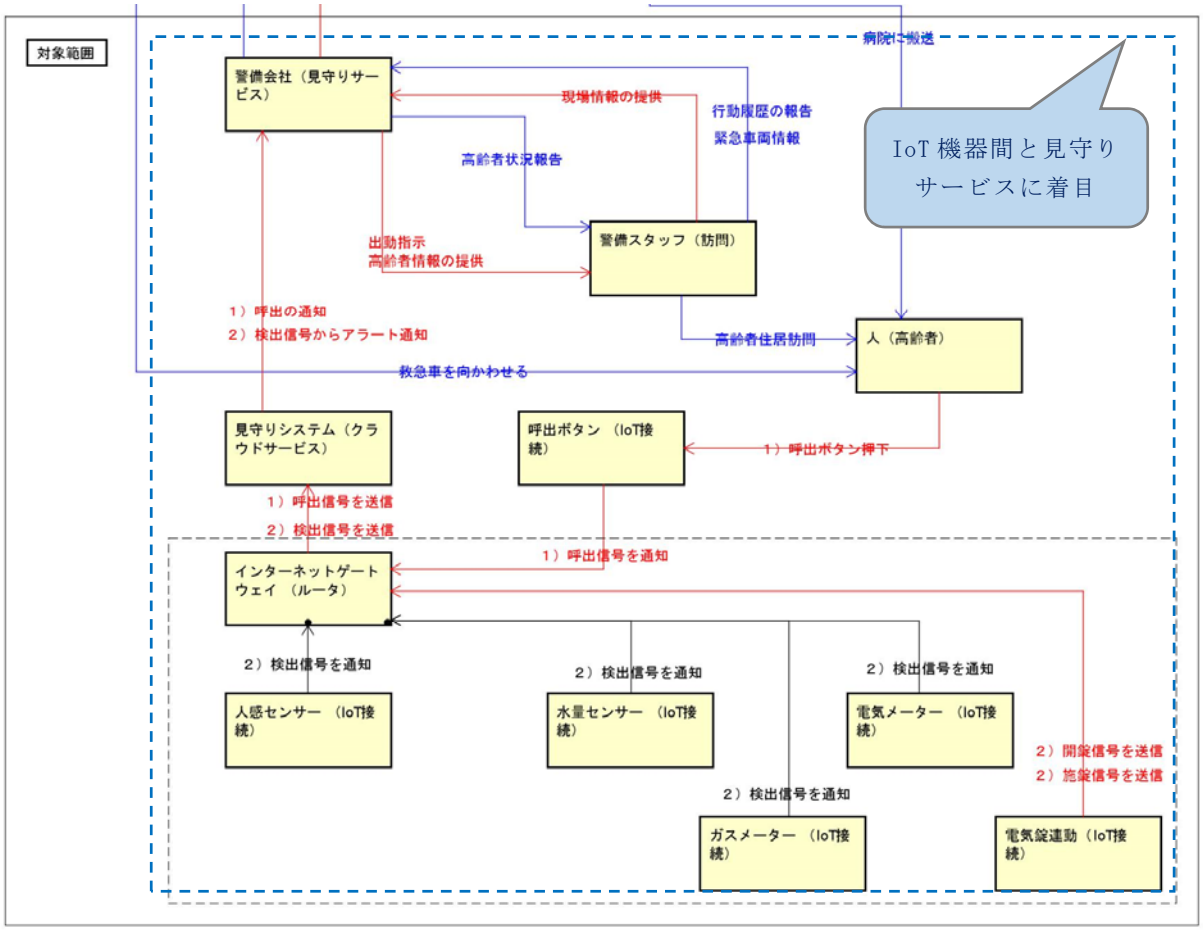

図 5　CS 図 整理後（詳細は付録参照）

Step1 にて，　表 2 のものを中心に UCA を 27 件抽出した．

表 2　UCA 表（詳細は付録参照）

No	CA	From	To	CA提供条件	Not Providing	Providing causes hazard	Too early / Too late
14	1）呼出ボタン押下	人（高齢者）	呼出ボタン （IoT接続）	高齢者が意図的にボタンを押下した時	(UCA14-N-1) 呼出ボタンを押下されたが通知されない [SC1] (UCA14-N-2) 呼出ボタンを押下できない [SC1]	(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]
15	2）開錠信号を送信	電気錠連動（IoT接続）	インターネットゲートウェイ （ルータ）	室外から鍵により開錠された時	(UCA15-N-1) 開錠が検出されたが通知されない [SC2]	(UCA15-P-1) 開錠が検出されないが通知された	(UCA15-T-1) 開錠が検出されたが通知に遅延が発生した [SC2]

Step2 にて，表 3 のものを中心に HCF を 16 件特定した．

表 3　HCF 表（詳細は付録参照）

ID	HCF	ヒントワード	シナリオ
HCF14-N-2-1	呼出ボタンを押せない	(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	高齢者が意識を失う 高齢者が体調不良により押すことができない 高齢者が呼出ボタンを紛失した、位置を忘れた 高齢者が破損した
HCF14-T-1-1	呼出ボタンを押下されたが見守りシステムへの通知に遅延が発生した	(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	呼出ボタンからの通知に遅延が発生した 呼出ボタンが故障して遅延が発生した 呼出ボタンの通信経路に遅延が発生した

HCF を特定する際，STPA では発想を促す目的でヒントワードを用いる．STAMP Workbench には，分析対象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おり，今回はその内の「An STPA Primer」を主として活用した．この結果，HCF に繋がるシナリオを特定することができた．

今回の分析では IoT 機器間の関係を分析することによって，直接的なコントローラ/被コントロールプロセス間だけでなく，間接的な影響による高齢者見守りシステムのリスクを検出することができた．例えば，センサー類と見守りシステムとの連携不良により，異常検出が適切に行われず，その結果検出不可に繋がるリスクがある．

高齢者見守りシステムにおいて多種多様なサービス提供者（行政・サービス提供者・関係者）が存在する様を明らかにした．また，公共・民間サービスやそれらに関連するシステムが連携／関与する部分に着目して安全性分析を行うことで，高齢者を監視するべきセンサー類から高齢者見守りシステムへの情報の通知不良で事故に繋がるなど，IoT 機器連携による特有のリスクを抽出できた．

3.3. 考察

STAMP S&S の 5 層モデルに基づいて高齢者見守りシステムの階層をモデリングすることにより，公共・民間サービスと IoT の関係性を精緻化することができた(**エラー！ 参照元が見つかりません。**)．但し，コンポーネントが増えれば増えるほど関係性が複雑になるため，いったん精緻化した関係性のうち，どこから分析の詳細化を図るかについては，CS 図を眺めながらよく吟味するために，優先順位付けにはハザードの発生確率と発生時の影響度を勘案すると良いと考える．

分析対象とするコントロールから，過去のアクシデント事例に基づいたガイドワード，ヒントワードを用いて UCA の抽出，HCF の特定を実施した．その結果この分析手法は 5 層モデルの上位層・下位層に依らず活用が可能であり，分析の初心者であっても比較的容易に分析を進めることができることを確認できた．但し，ガイドワードのセットは一律ではなく，分析対象のドメインや階層によって適切なワードを利用することで，より精緻な分析ができると考えられる．階層によっては適切なガイドワードを選択することが大事であると考える．

4. 今後の課題

本稿では，分析対象とした高齢者見守りサービスのセンサー類の組み合わせパターンが多く，CS 図に組み合わせるためにパターンを正しく抽出する仕組みと連携させていきたい．

分析の発散を防ぐ目的で，最初に分析対象を「高齢者見守りシステムのセンサー類にもたらされる，安全性を損なうリスク」に限定している．さらに，STAMP S&S の活用によって得られた，高齢者見守りシステムを取巻く Stakeholder，Service のうち、見守りシステムに対象を限定している.よって,実際に高齢者見守りシステム全体の開発を進める際は，こうした分析対象の限定を取り払い，広範な分析対象全てに対して安全性分析を実施していきたい．

また，STAMP/STPA は安全性分析手法であり，明らかになった非安全性に対する対策を検

討する手法が含まれていない．このため，高齢者見守りシステム全体に対して本実験と同様に安全性分析ができたとしても，公共・民間サービス提供者が妥当かつ一貫性のある対策を検討するための手段が必要と考えられる．しかし，Society，Stakeholder，Service の領域では，まだこうした手法の研究例はなく，対策立案に向けた新たな手法の検討を行っていきたい．

また，UCA の抽出，HCF の特定，およびハザードシナリオのいずれの分析フェーズにおいても，分析結果の文章構造は分析者の自由である．このため，複数人で分析を分担するような場合に，こうした文章構造に揺らぎが生まれ，分析の一貫性を維持しにくくなるという問題がある．分析結果の定型的な書き方を示すことで，誤解なく表現できる仕組みを検討する．

5. まとめ

本稿では，高齢者見守りシステムにおける公共・民間サービスやシステムが連携／関与する部分について，センサー類の連携に着目し，STAMP/STPA を活用して，安全性分析を行い，見守りシステム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 層モデルの適用によって，高齢者見守りシステムの開発時に CS 図を作成することで考慮すべき，IoT 連携するセンサー類の連携を明らかにすることができた．また，ガイドワード・ヒントワードを利用することによって，最終的に構成要素間の連携と安全性を損なうリスクを抽出することができた．

今後は 4 章で述べた課題に取り組んでいく予定である．

参考文献

[1] 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，2023 年 1 月 13 日アクセス確認

[2] 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，2023 年 1 月 13 日アクセス確認

[3] 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/，2023 年 1 月 13 日アクセス確認

[4] ISO：ISO/IEC Guide 51:2014，https://www.iso.org/standard/53940.html，2023 年 1 月 13 日アクセス確認

[5] 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

[6] 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

[7] 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，2023 年 1 月 13 日アクセス確認

[8] 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，2023 年 1 月 13 日アク