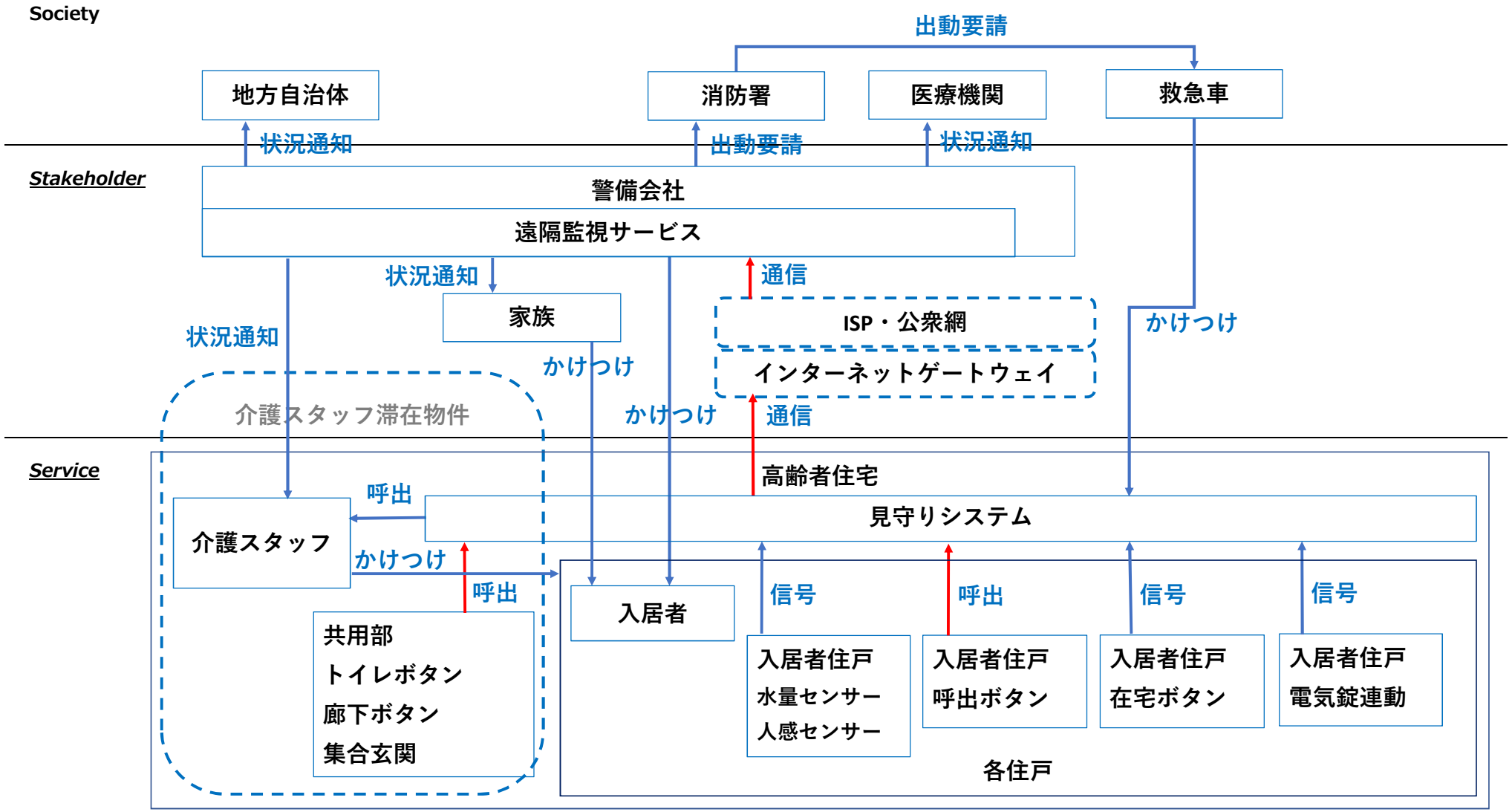
付録１．スマートシティのコントロールストラクチャー図（整理前）



付録２．前提条件

ID	名前
Pre-1	従来の見守りシステムではなく、クラウド上に見守りシステムを設置する
Pre-2	人命・財産にかかわる問題を取り扱う
Pre-3	対策の検討はしない
Pre-4	Stakeholder - Service間 の通信に関するリスクを分析する
Pre-5	地震、噴火、落雷、津波は発生しないものとする
Pre-6	火事、急病人などがあるものとする
Pre-7	車いすや、介助が必要な人がいるものとする
Pre-8	利益・ビジネスの継続性に関することは検討しない
Pre-9	運用に関する考慮不足は検討する
Pre-10	運用に関する人為的ミスは検討する
Pre-11	連携機器の故障は検討しない
Pre-12	連携機器の配線不良は検討しない
Pre-13	連携機器の連携仕様不備は検討する
Pre-14	監視カメラの映像を直接的に使用せず、ベッドなどの一定範囲検出で通知は可能とする
Pre-15	
Pre-16	

付録３．アクシデントハザード安全制約表

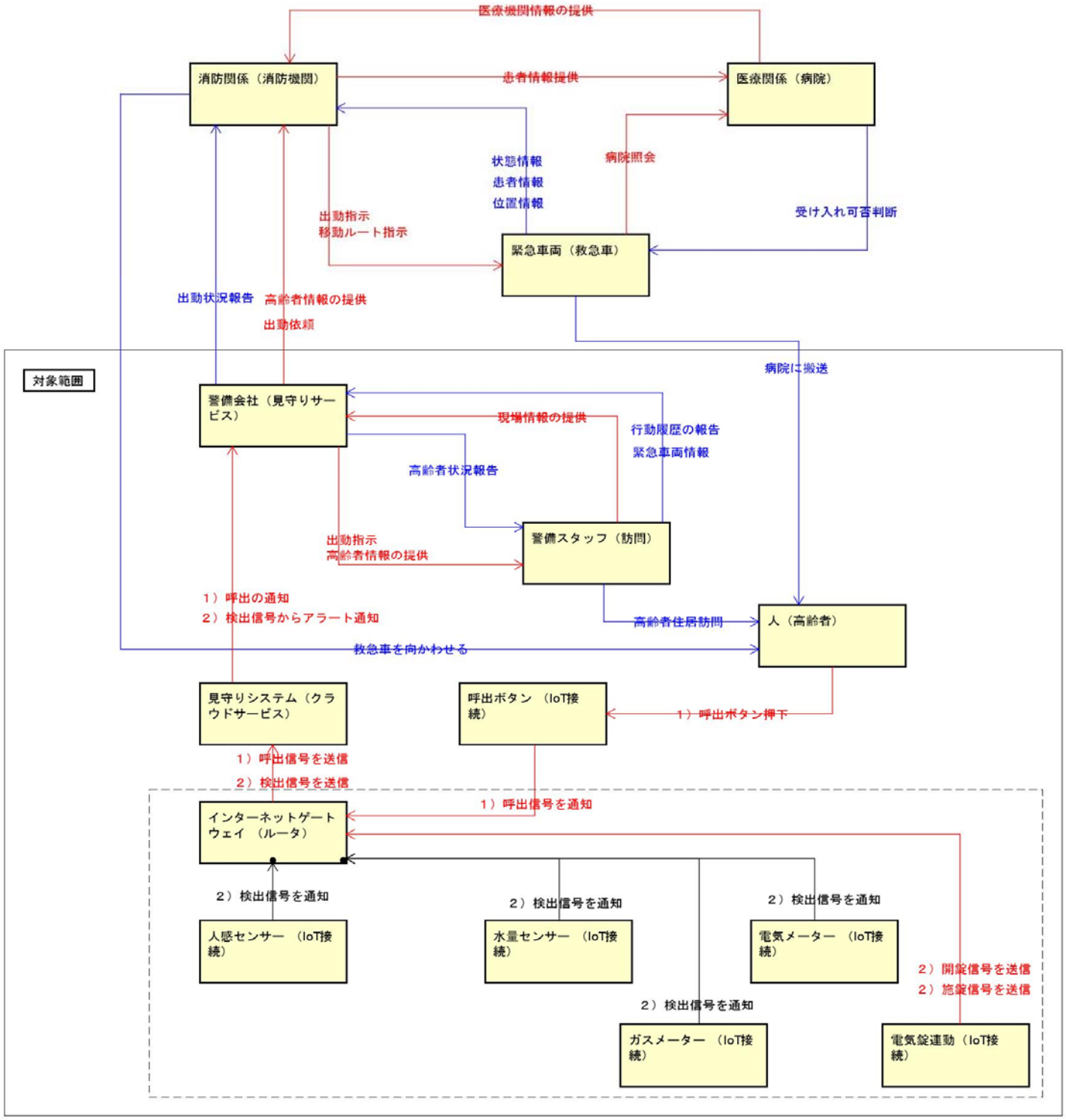
アクシデントID	アクシデント	ハザードID	ハザード	安全制約ID	安全制約
A1	高齢者が命に係わる状態になった時に見守りができない	H1	呼出ボタンで伝達されない	SC1	呼出ボタンから危険な状態を伝えられる
A1	高齢者が命に係わる状態になった時に見守りができない	H2	センサー類から伝達されない	SC2	センサー類から危険な状態を伝えられる
A1	高齢者が命に係わる状態になった時に見守りができない	H3	警備会社に通知されない	SC3	警備会社に危険な状態を伝えられる
A1	高齢者が命に係わる状態になった時に見守りができない	H4	警備スタッフに通知されない	SC4	警備スタッフに危険な状態を伝えられる

付録４．コンポーネント抽出表

対象	登場人物	責務	コントロールアクション	フィードバック	入出力	備考
true	消防関係（消防機関）	要・救護者の救助活動 病院への搬送	出動指示 (To: 緊急車両（救急車）) 移動ルート指示 (To: 緊急車両（救急車）) 患者情報提供 (To: 医療関係（病院）)	救急車を向かわせる (To: 人（高齢者）)		
true	緊急車両（救急車）	要・救護者の救助	病院照会 (To: 医療関係（病院）)	患者情報 (To: 消防関係（消防機関）) 位置情報 (To: 消防関係（消防機関）) 状態情報 (To: 消防関係（消防機関）) 病院に搬送 (To: 人（高齢者）)		
true	医療関係（病院）	要・救護者の受け入れ	医療機関情報の提供 (To: 消防関係（消防機関）)	受け入れ可否判断 (To: 緊急車両（救急車）)		
true	人（高齢者）	–	１）呼出ボタン押下 (To: 呼出ボタン（IoT接続）)			高齢者はIoT機器の扱いに慣れていない
true	警備会社（見守りサービス）	見守りシステムの監視 消防関係へ救助依頼	出動指示 (To: 警備スタッフ（訪問）) 高齢者情報の提供 (To: 警備スタッフ（訪問）) 出動依頼 (To: 消防関係（消防機関）) 高齢者情報の提供 (To: 消防関係（消防機関）)	高齢者状況報告 (To: 警備スタッフ（訪問）) 出動状況報告 (To: 消防関係（消防機関）)		検出信号の組合せから緊急度の判定が必要
true	警備スタッフ（訪問）	要・救護者の確認 消防関係へ救助依頼	現場情報の提供 (To: 警備会社（見守りサービス）)	緊急車両情報 (To: 警備会社（見守りサービス）) 行動履歴の報告 (To: 警備会社（見守りサービス）) 高齢者住居訪問 (To: 人（高齢者）)		訪問契約があれば対応可能

対象	登場人物	責務	コントロールアクション	フィードバック	入出力	備考
true	見守りシステム（クラウドサービス）	各センサーの情報蓄積 組合せによる判定	1）呼出の通知 (To: 警備会社（見守りサービス）) 2）検出信号からアラート通知 (To: 警備会社（見守りサービス）)			検出信号の組合せから判定するアルゴリズムが必要 １つの信号のみで判断すると誤判断になることがある
true	インターネットゲートウェイ（ルータ）	センサー類の信号をインターネットに送信	1）呼出信号を送信 (To: 見守りシステム（クラウドサービス）) 2）検出信号を送信 (To: 見守りシステム（クラウドサービス）)			セキュリティリスクとして、クラウドまでの通信のなりすまし、乗っ取りの可能性がある
true	呼出ボタン （IoT接続）	呼出信号を見守りシステムに送信	1）呼出信号を通知 (To: インターネットゲートウェイ （ルータ）)			
true	人感センサー （IoT接続）	検出信号を見守りシステムに送信			(出力)2）検出信号を通知	
true	水量センサー （IoT接続）	検出信号を見守りシステムに送信			(出力)2）検出信号を通知	
true	電気メーター （IoT接続）	検出信号を見守りシステムに送信			(出力)2）検出信号を通知	
true	ガスメーター （IoT接続）	検出信号を見守りシステムに送信			(出力)2）検出信号を通知	
true	電気錠連動（IoT接続）	開錠／施錠の信号を送信	2）開錠信号を送信 (To: インターネットゲートウェイ （ルータ）) 2）施錠信号を送信 (To: インターネットゲートウェイ （ルータ）)			

付録5．コントロールストラクチャ図（整理後）



付録６．UCA（Unsafe Control Action）表

No	CA	From	To	CA提供条件	Not Providing	Providing causes hazard	Too early / Too late	Stop too soon / Applying too long
1	出動指示	消防関係（消防機関）	緊急車両（救急車）					
2	移動ルート指示	消防関係（消防機関）	緊急車両（救急車）					
3	患者情報提供	消防関係（消防機関）	医療関係（病院）					
4	出動指示	警備会社（見守りサービス）	警備スタッフ（訪問）	呼出ボタンによる呼出された時 各センサーから出動が必要と判定した時	(UCA4-N-1) 呼出ボタンを押下されたが通知されない [SC1] (UCA4-N-2) 各センサーから出動必要と判定されたが通知されない [SC2]	(UCA4-P-1) 呼出ボタンを押下していないが通知される (UCA4-P-2) 各センサーに異常はないが通知される	(UCA4-T-1) 呼出ボタンを押下を押下したが通知までに遅延が発生した [SC1] (UCA4-T-2) 各センサーから出動必要と通知したが遅延が発生した [SC2]	
5	高齢者情報の提供	警備会社（見守りサービス）	警備スタッフ（訪問）	警備会社から消防関係に依頼する時	-	-	-	
6	出動依頼	警備会社（見守りサービス）	消防関係（消防機関）	現場情報から警備会社が必要と判定した時	-	-	-	
7	高齢者情報の提供	警備会社（見守りサービス）	消防関係（消防機関）	警備会社から消防関係に	-	-	-	
8	１）呼出の通知	見守りシステム（クラウドサービス）	警備会社（見守りサービス）	呼出の信号を受信した時	(UCA8-N-1) 呼出ボタンを押下されたが通知されない [SC1]	(UCA8-P-1) 呼出ボタンを押下していないが通知される	(UCA8-T-1) 呼出ボタンを押下を押下したが通知までに遅延が発生した [SC1]	
9	１）呼出信号を送信	インターネットゲートウェイ （ルータ）	見守りシステム（クラウドサービス）	各センター類からの信号を受信した時	(UCA9-N-1) 呼出ボタンが押下されたが受信されない [SC2]	(UCA9-P-1) 呼出ボタンを押下していないが受信された	(UCA9-T-1) 呼出ボタンを押下されたが受信までに遅延が発生した [SC1]	
10	１）呼出信号を通知	呼出ボタン （IoT接続）	インターネットゲートウェイ （ルータ）	呼出ボタンを押下した時	(UCA10-N-1) 呼出ボタンを押下されたが通知されない [SC1]	(UCA10-P-1) 呼出ボタンを押下されないが通知された	(UCA10-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]	

No	CA	From	To	CA提供条件	Not Providing	Providing causes hazard	Too early / Too late	Stop too soon / Applying too long
11	病院照会	緊急車両（救急車）	医療関係（病院）	救急車から搬送先を選定する時	-	-	-	
12	現場情報の提供	警備スタッフ（訪問）	警備会社（見守りサービス）	警備スタッフが現場到着時	-	-	-	
13	医療機関情報の提供	医療関係（病院）	消防関係（消防機関）	消防関係からの依頼された時	-	-	-	
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]	
16	2）施錠信号を送信	電気錠連動（IoT接続）	インターネットゲートウェイ （ルータ）	室内からサムターンにより施錠された時	(UCA16-N-1) 施錠が検出されたが通知されない [SC2]	(UCA16-P-1) 施錠が検出されないが通知された	(UCA16-T-1) 施錠が検出されたが通知に遅延が発生した [SC2]	
17	2）検出信号からアラート通知	見守りシステム（クラウドサービス）	警備会社（見守りサービス）	ゲートウェイからの信号を受信した時	(UCA17-N-1) ゲートウェイから信号を受信したが通知されない [SC2]	(UCA17-P-1) ゲートウェイから信号を受信していないが通知された	(UCA17-T-1) ゲートウェイから信号を受信したが通知に遅延が発生した [SC2]	
18	2）検出信号を送信	インターネットゲートウェイ （ルータ）	見守りシステム（クラウドサービス）	各センター類からの信号を受信した時	(UCA18-N-1) 各センサーから検出されたが受信されない [SC2]	(UCA18-P-1) 各センサーから検出されないが受信された	(UCA18-T-1) 各センサーから検出されたが受信に遅延が発生した [SC2]	

付録７．HCF（Hazard Causal Factor）表

ID	HCF	ヒントワード	シナリオ
HCF8-N-1-1	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
HCF8-T-1-1	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が遅延した	(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	クラウドサーバからの通信が遅延した クラウドサーバからの通信が外部からのアタックにより遅延した クラウドサーバからのトラブルにより遅延した
HCF9-N-1-1	呼出ボタンは正常に動作し、通知を送信しているが見守りシステムに通知されない	(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	インターネットGWからの通信が遮断された インターネットGWからの通信がドロップした インターネットGWの機器故障
HCF9-T-1-1	呼出ボタンは正常に動作し、送信しているが見守りシステムへ通知が遅延した	(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	インターネットGWからの通信が遅延した インターネットGWが外部からのアタックにより遅延した インターネットGWの機器故障
HCF10-N-1-1	呼出ボタンを押したが、インターネットゲートウェイに通知されない	(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	呼出ボタンからの通信が改ざんされた 呼出ボタンからの通信経路の機器故障 呼出ボタンの機器故障 呼出ボタンからの通信経路で破棄された インターネットGWの機器故障
HCF10-T-1-1	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
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

ID	HCF	ヒントワード	シナリオ
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
HCF15-N-1-1	開錠されたが見守りシステムへの通知されない	(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	電気錠からの通信が遮断された 電気錠からの通信が改ざんされた 電気錠からの通信経路で破棄された 電気錠が故障した
HCF15-T-1-1	開錠されたが見守りシステム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	電気錠からの通信に遅延が発生した 電気錠からの通信経路に遅延が発生した 電気錠が故障した
HCF16-N-1-1	施錠されたが見守りシステムへの通知されない	(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	電気錠からの通信が遮断された 電気錠からの通信が改ざんされた 電気錠からの通信経路で破棄された 電気錠が故障した
HCF16-T-1-1	開錠されたが見守りシステム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	電気錠からの通信に遅延が発生した 電気錠からの通信経路に遅延が発生した 電気錠が故障した
HCF17-N-1-1	各センサーから通知を受信したが、警備会社にアラート通知されない	(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	各センサーの組み合わせから、アラート通知が必要な検出結果だったが、誤検知により通知されなかった
HCF17-T-1-1	各センサーから通知を受信したが、警備会社にアラート通知が遅延した	(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	見守りシステムからの通信に遅延が発生した 見守りシステムからの通信経路に遅延が発生した 見守りシステムがトラブルにより遅延が発生した
HCF18-N-1-1	各センサーから送信されが、インターネットゲートウェイからクラウドサーバに通知されない	(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	インターネットGWからの通信が遮断された インターネットGWからの通信が改ざんされた インターネットGWからの通信経路で破棄された インターネットGWが故障した
HCF18-T-1-1	各センサーから送信されが、インターネットゲートウェイからクラウドサーバに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	インターネットGWからの通信に遅延が発生した インターネットGWからの通信経路に遅延が発生した インターネットGWが故障した

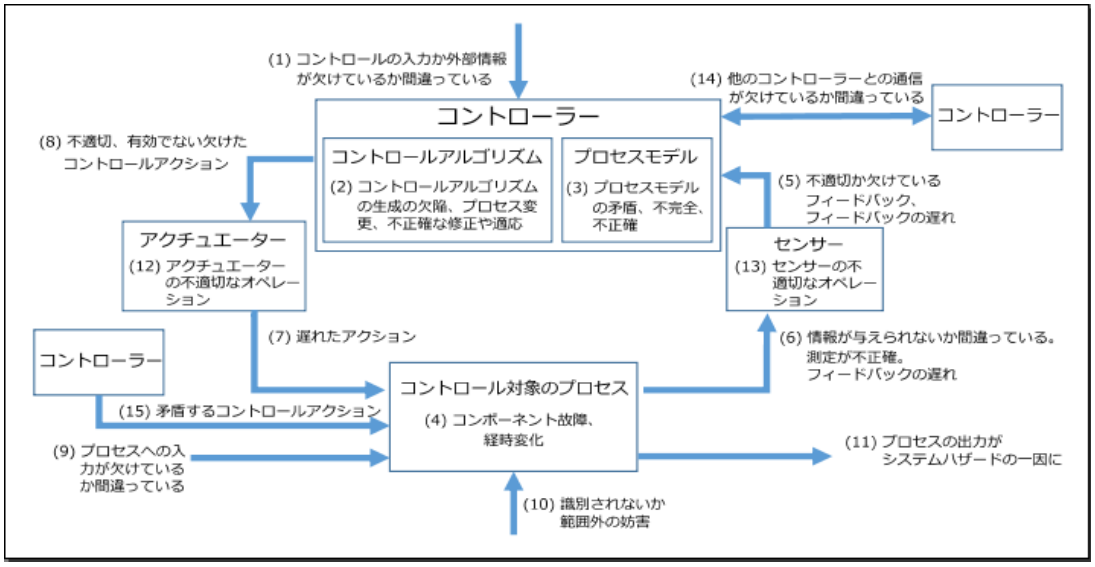
付録8. HCF特定ヒントワードセット

STAMP Workbench には、あらかじめ5種類のヒントワードセットが定義されている。

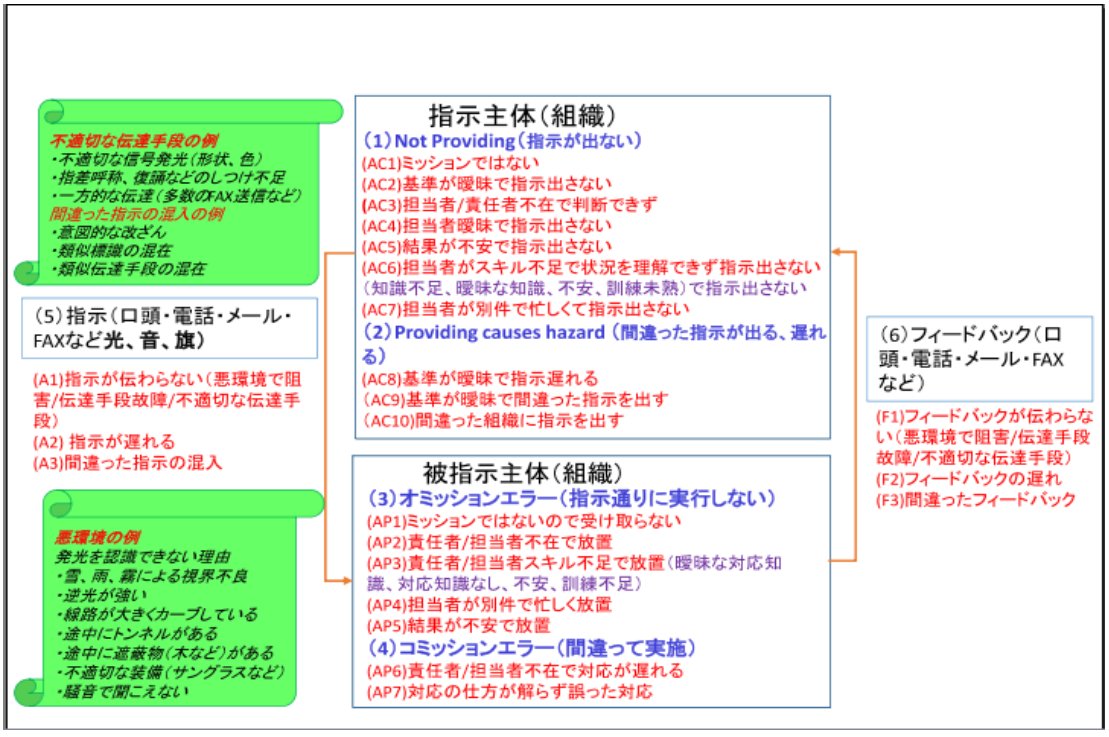
1	An STPA Primer
2	IPA - (人) 対 (人)
3	IPA - (人) 対 (機械)
4	IPA - (組織) 対 (人)
5	IPA - (組織) 対 (組織)

ヒントワードセットは、分析内容に応じてヒントワードを変更したり、新しいヒントワードを作成したりできる。
本稿に登場する、上記1、5のヒントワードの具体内容を以下に示す。

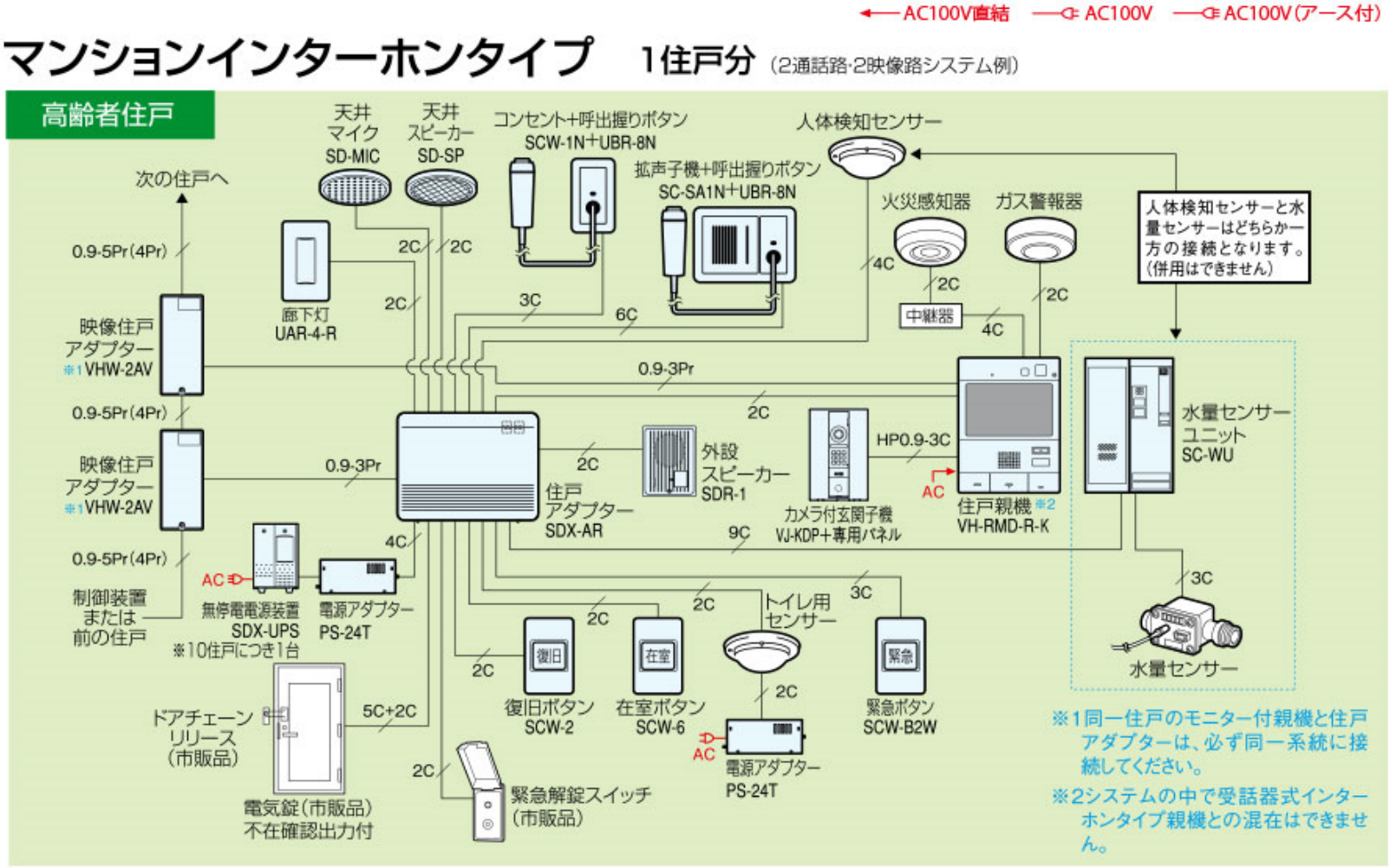
An STPA Primerのヒントワード



IPA - (組織) 対 (組織)のヒントワード



付録9. センサー類組合せ



呼出ボタンを押せないときのセンサーの組合せにより見守り可能か検討する

	パターン１	パターン２	パターン３	パターン４	パターン５	パターン６
呼出ボタン	×	×	×	×	×	×
電気錠　開錠	－	－	－	○	○	○
電気錠　施錠	○	○	○	－	－	－
人感センサー	検出あり	検出なし	検出なし	検出あり	検出なし	検出なし
水量センター	検出あり	検出なし	検出あり	検出あり	検出あり	検出なし
ガスメーター	検出あり	検出なし	検出あり	検出あり	検出あり	検出なし
電気メーター	検出あり	検出なし	検出あり	検出あり	検出あり	検出なし
判定	正常	異常	異常	異常	異常	正常

付録10. 用語集

本書で用いる略語

CS 図	コントロールストラクチャー図
CA	コントロールアクション
FB	フィードバック
UCA	Unsafe Control Action （非安全なコントロールアクション）
HCF	Hazard Causal Factor （ハザード誘発要因）

参考文献）https://www.ipa.go.jp/files/000072491.pdf

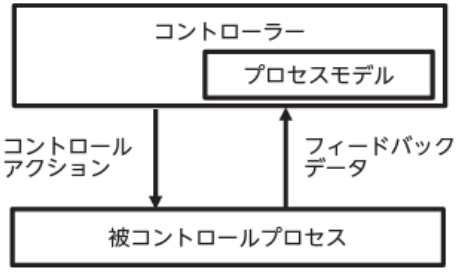


図 1.1-1　STAMP における相互作用のモデル

参考文献）https://www.ipa.go.jp/files/000051829.pdf

コントロールストラクチャー（Control Structure Diagram）
制御構造図。システムにおいて、安全制約の実現に関係するコンポーネント、およびコンポーネント間の相互作用から成る構造図。

コントロールアクション（Control Action）
コントローラーが被コントロールプロセスに対して行なう制御指示・制御動作・制御行動。

UCA（Unsafe Control Action）
非安全制御行動。事故・損失（アクシデント）につながる制御、制御行動、動作。

HCF（Hazard Causal Factor）
ハザード誘発要因。危険な状態（ハザード）を引き起こす原因。

参考文献）www.ipa.go.jp/files/000051829.pdf