Information Security Lab

IoTを含む医療機器システムの セキュリティ/セーフティ評価手法の提案と適用

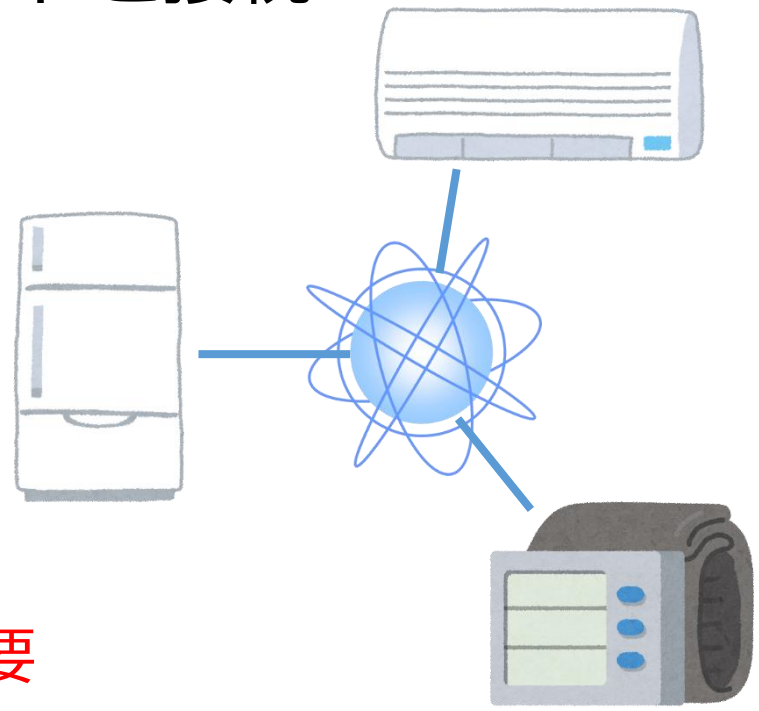
東京電機大学　早川拓郎　金子朋子　佐々木良一

目次

- IoTの現状
- ツリー分析とSTPAの課題
- 提案手法
- 試適用
- 今後の展望

IoT(モノのインターネット)の普及

- IoTの普及により様々な「モノ」がインターネットと接続
  - ➢もともと”セキュリティ”の考慮をされていない
- 機能安全によりセーフティを確保
  - ➢誤作動や停止が人の健康や命に関わる
- セキュリティの欠陥がセーフティの欠陥に直結
  - ➢セーフティとセキュリティを統合的に扱うことが必要



医療機器における脆弱性の例

- リモコンによる遠隔操作が可能なインスリンポンプに脆弱性(2016)

CVE番号	内容	備考
CVE-2016-5084	機密情報の平文通信 患者の治療情報やパスワードが暗号化されずに通信されている	患者の治療情報に個人を特定できるものは含まれていない
CVE-2016-5085	不十分なランダム値の使用 リモコン～ポンプ間の暗号鍵の値がいつも同じ値	リモートコントローラになりすました通信を行うために必要な情報を取得される可能性がある
CVE-2016-5086	キャプチャリプレイによる認証回避 リモコン～ポンプ間の通信プロトコルはキャプチャリプレイ攻撃への対策が不十分	あらかじめ取得した通信内容を使い、リモコンになりすましてポンプにコマンドを送られる可能性がある
CVE-2016-5686	スプーフィングによる認証回避 リモコン～ポンプ間の通信プロトコルはスプーフィング対策が不十分	遠隔の第三者によってポンプの操作に対する応答を偽装される可能性がある

Japan Vulnerability Notesより　https://jvn.jp/vu/JVNVU95089754/

- メーカーは注意喚起をするに留まる

IoTのセキュリティ対策

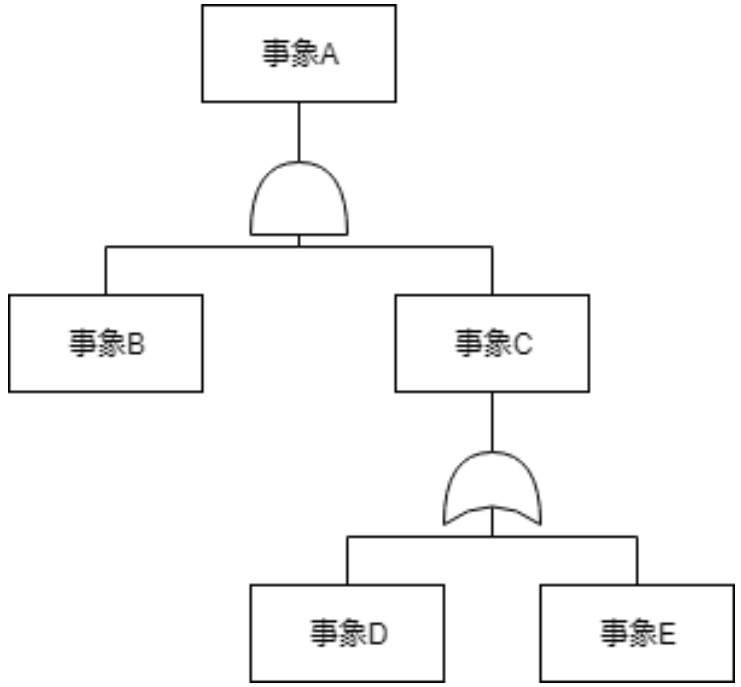
- IoTには流通後のセキュリティ対策が困難なものが存在
  - ➢設計段階でセキュリティを考慮する「セキュリティ・バイ・デザイン」の実践が必要

- セキュリティ・バイ・デザインの実践には、設計段階でシステムに対する脅威分析とリスクに基づく対策選定が必要

リスク　＝　事故の発生確率　×　影響の大きさ

従来の脅威分析手法の限界

- フォールトツリー解析やアタックツリー解析等の木構造解析がよく利用される
- 脅威の導出と事象の発生確率の算出が可能
- 木構造解析はIoTを分析するには不向き
  - 多数の要素と制御による相互作用の分析が困難



ツリー分析の例

STPAの課題点と本研究の目的

STPAの課題点

- アクシデントの影響の大きさや確率に基づくリスクの定量化が含まれない
- 対策選定の具体的な手順を含まない

本研究の目的

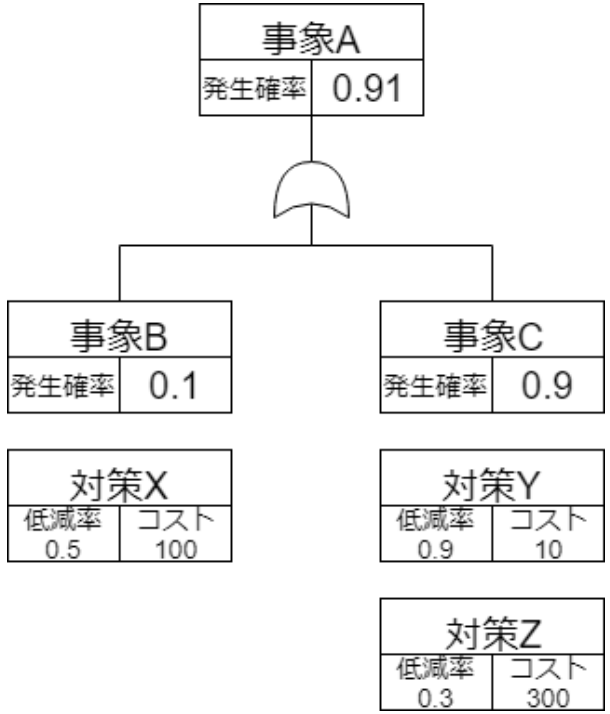
- IoTに対する新たな脅威分析・対策選定手法をSTPAをベースに開発する
- 提案手法は次の要件を含む
  - 制御構造が複雑に絡み合ったシステムを分析できること
  - セキュリティと安全性を統合的に分析できること
  - 対策選定のためにリスクの定量的分析を含むこと

⇒ STPAとディフェンスツリーの統合

ディフェンスツリーの概要

- アタックツリーに対策のモデルを加えたもの
- リスクの増減に基づき費用対効果の高い対策の組み合わせを導出

  例)予想される影響の大きさが1000の事象Aについて

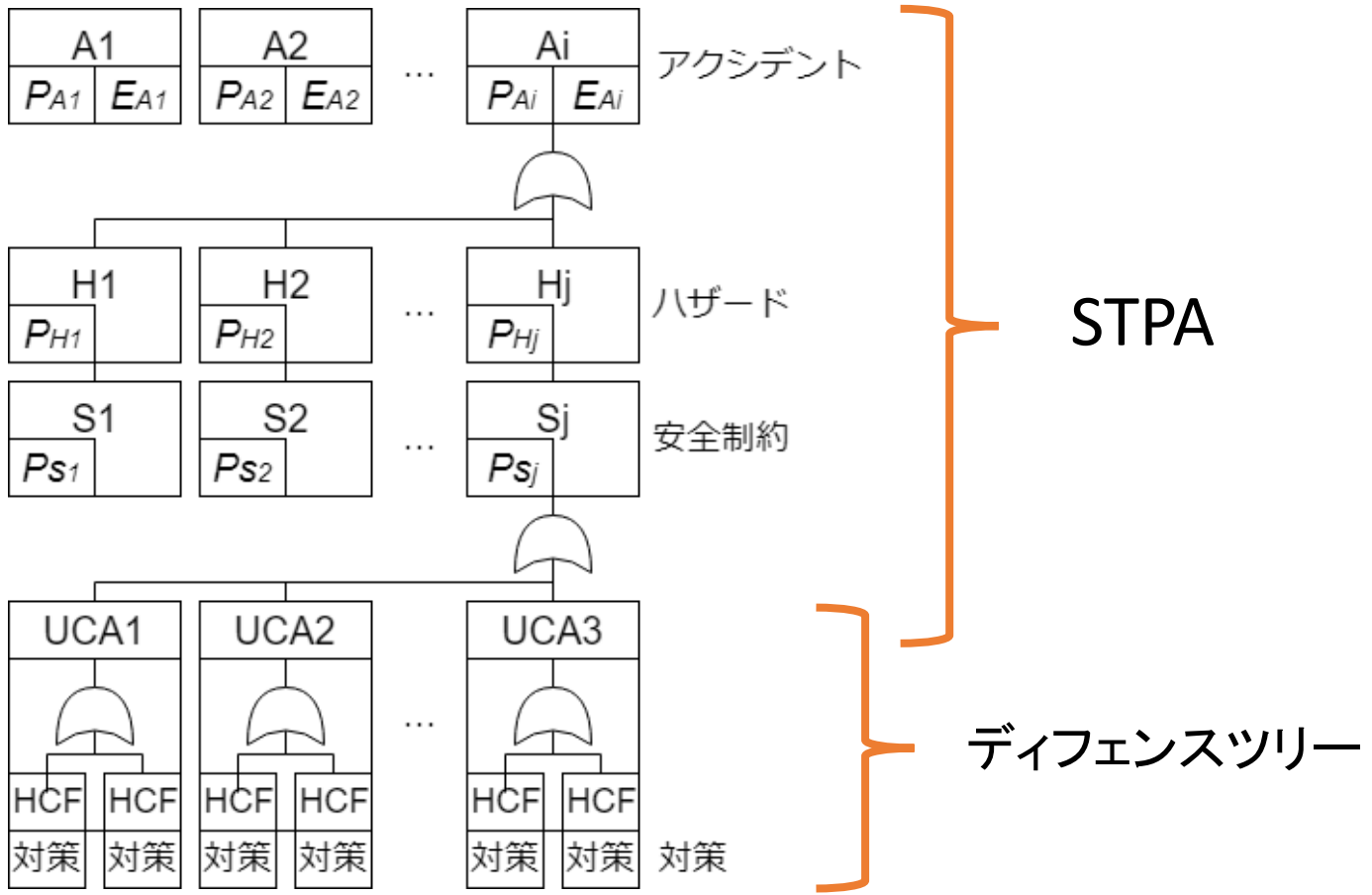


対策	事象Aの発生確率	トータルリスク
なし	0.91	910
X	0.905	1005
Y	0.829	839
Z	0.343	643
XY	0.8195	929.5
YZ	0.3187	628.7
ZX	0.3065	706.5
XYZ	0.28085	690.85

提案方式の概要

手順	内容
1	アクシデント，ハザード，安全制約の識別
2	コントロールストラクチャの構築
3	UCAの識別
4	ハザード誘発要因の特定
5	アクシデントの確率分析
6	対策選定

提案手法の手順



提案手法の全体像

インスリンポンプへの試適用

- 実在するインスリンポンプを参考にIoT化した
  仮想のインスリンポンプを分析
- 提案手法での対策選定の最適化が実用的な時間で可能かどうか検証
- 事象の発生確率や対策による低減率は仮の値を使用

インスリンポンプへの試適用

仮想インスリンポンプの機能

- インスリン投与機能
  - あらかじめ設定された基礎レートに基づく投与とボーラスの2種類の投与方法がある
- 血糖値測定器との連携機能
  - 血糖値測定器と短距離無線により連携することで血糖値を記録
  - 血糖値測定器からボーラスを遠隔指示できる
- 皮下グルコース値測定機能
  - 使用者に皮下に穿刺したセンサーにより皮下のグルコース濃度を測定する
  - センサーはトランスミッタにより測定値を短距離無線通信に変換して本体に送信する
- インターネットとの通信機能(仮定)
  - 本体はWi-Fiを通じてインターネット経由でサーバに血糖値情報を送信する
  - 医者はサーバの血糖値情報を参照して患者の治療を行う

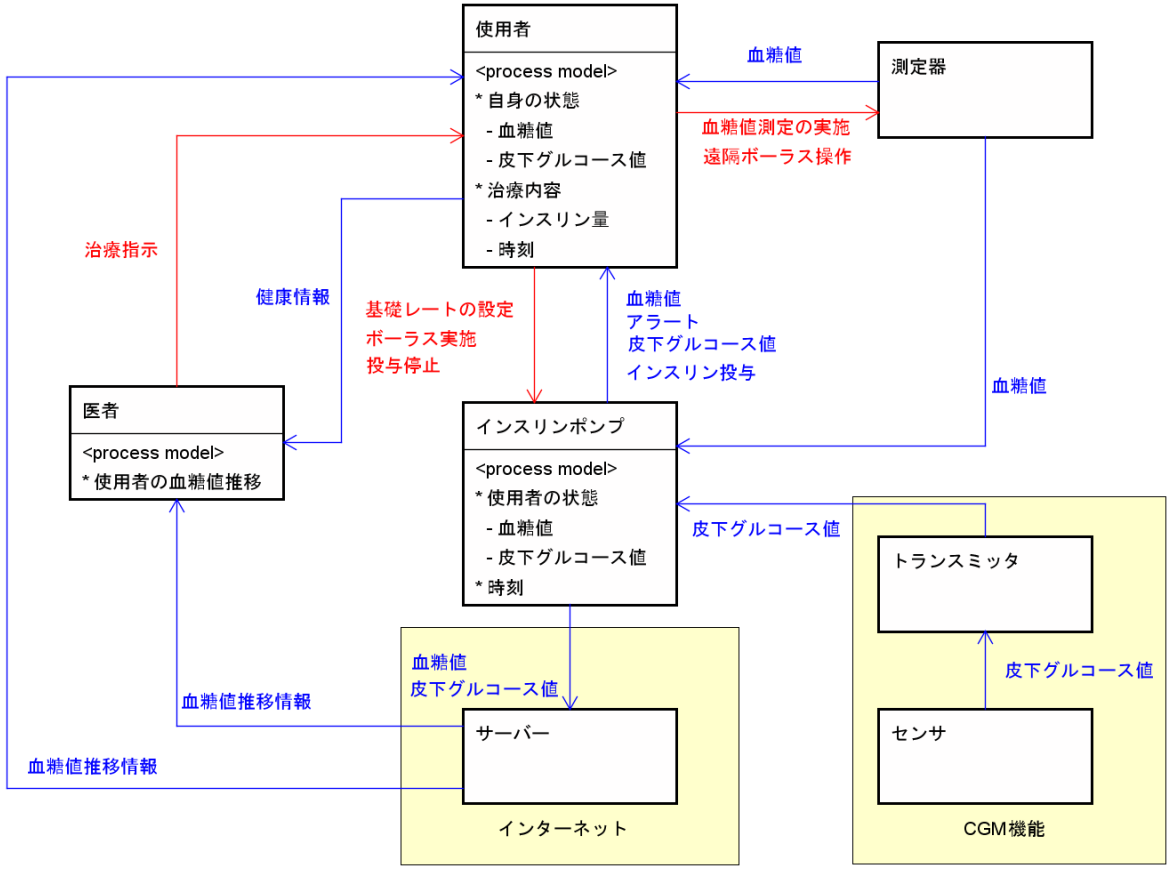
手順1

アクシデント、ハザード、安全制約の識別

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	使用者が健康を損なう	H1	使用者が高血糖になる	SC1	インスリンポンプは使用者が高血糖のときインスリンを投与しなければならない
A1	使用者が健康を損なう	H2	使用者が低血糖になる	SC2	インスリンポンプは使用者が低血糖のときインスリンの投与を停止しなければならない
A1	使用者が健康を損なう	H3	医者が使用者に対して不適切な治療を行う	SC3	医者は使用者の血糖値推移情報に応じた適切な治療を行わなければならない
A1	使用者が健康を損なう	H4	使用者の血糖値測定が行われない	SC4	使用者は定められた時刻に血糖値測定を行わなければならない
A2	使用者の個人情報が流出する	H5	通信経路が安全でない	SC5	通信経路はセキュリティが確保されていなければならない
A2	使用者の個人情報が流出する	H6	情報機器が安全でない	SC6	各種情報機器はセキュリティが確保されていなければならない

手順2

コントロールストラクチャの構築



手順3

UCAの識別

CA	From	To	CA提供条件	Not Providing	Providing causes	Too early / Too late	Stop too soon /
基礎レートの設定	使用者	インスリンポンプ	操作時	(UCA1-N-1) UCA [SC1][SC2]	(UCA1-P-1) UCA [SC1][SC2]	-	-
ボーラス実施	使用者	インスリンポンプ	操作時	(UCA2-N-1) UCA [SC1]	(UCA2-P-1) UCA [SC1][SC2]	(UCA2-T-1) UCA [SC1][SC2]	-
投与停止	使用者	インスリンポンプ	操作時	(UCA3-N-1) UCA [SC2]	(UCA3-P-1) UCA [SC1]	(UCA3-T-1) UCA [SC1][SC2]	(UCA3-D-1) UCA [SC1][SC2]
血糖値測定の実施	使用者	測定器	操作時	(UCA4-N-1) UCA [SC4]	(UCA4-P-1) UCA [SC5][SC6]	-	-
遠隔ボーラス操作	使用者	測定器	操作時	(UCA5-N-1) UCA [SC1]	(UCA5-P-1) UCA [SC1][SC2]	(UCA5-T-1) UCA [SC1][SC2]	-
治療指示	医者	使用者	診察時	(UCA6-N-1) UCA [SC3]	(UCA6-P-1) UCA [SC3] (UCA6-P-2) UCA [SC5][SC6]	-	-

手順3

識別したUCAの例(全17個)

UCAID	内容	違反安全制約1	違反安全制約2
UCA1-N-1	基礎レートの設定が行われない場合、適切な量のインスリンが投与されない。	SC1	SC2
UCA1-P-1	基礎レートの設定が不適切な場合、適切な量のインスリンが投与されない。	SC1	SC2
UCA2-N-1	ボーラス実施が行われない場合、必要なインスリンが投与されず血糖値が上昇する。	SC1	
UCA2-P-1	ボーラス実施の方法が誤っていた場合、適切な量のインスリンが投与されない。	SC1	SC2
UCA2-T-1	ボーラス実施のタイミングが適切でない場合、必要な時にインスリンが投与されない。	SC1	SC2
UCA3-N-1	投与停止が行われない場合、投与されるインスリンの量が過剰になり、血糖値が低下する。	SC2	
UCA3-P-1	投与停止が不適切に行われた場合、適切なインスリン投与が行われず、血糖値が上昇する。	SC1	
UCA3-T-1	投与停止が早すぎたり遅すぎる場合、適切なタイミングでインスリンが投与されない。	SC1	SC2
UCA3-D-1	投与停止が短すぎたり長すぎたりする場合、適切な量のインスリンが投与されない。	SC1	SC2

⋮

手順4

Excelによるツリー作成

アクシデントID	アクシデント	被害額	発生確率	リスク値	ハザードID	ハザード	安全制約ID	安全制約	違反確率
A1	使用者が健康を損なう	10000	0.73823	7332.251713	H1	使用者が高	SC1	インスリン	0.46994
A1	使用者が健康を損なう				H2	使用者が低	SC2	インスリン	0.32346
A1	使用者が健康を損なう				H3	医者が使用	SC3	医者は使用	0.24971
A1	使用者が健康を損なう				H4	使用者の血	SC4	使用者は	0.00848
A2	使用者の個人情報が流出する	10000	0.04363	436.2680003	H5	通信経路が	SC5	通信経路は	0.02206
A2	使用者の個人情報が流出する				H6	情報機器が	SC6	各種情報機	0.02206

総事象数	96
対策コスト最大値	11980
総リスク最大値	11328.85701
制約条件	6000
対策後総リスク	7768.519713
対策総コスト	5980

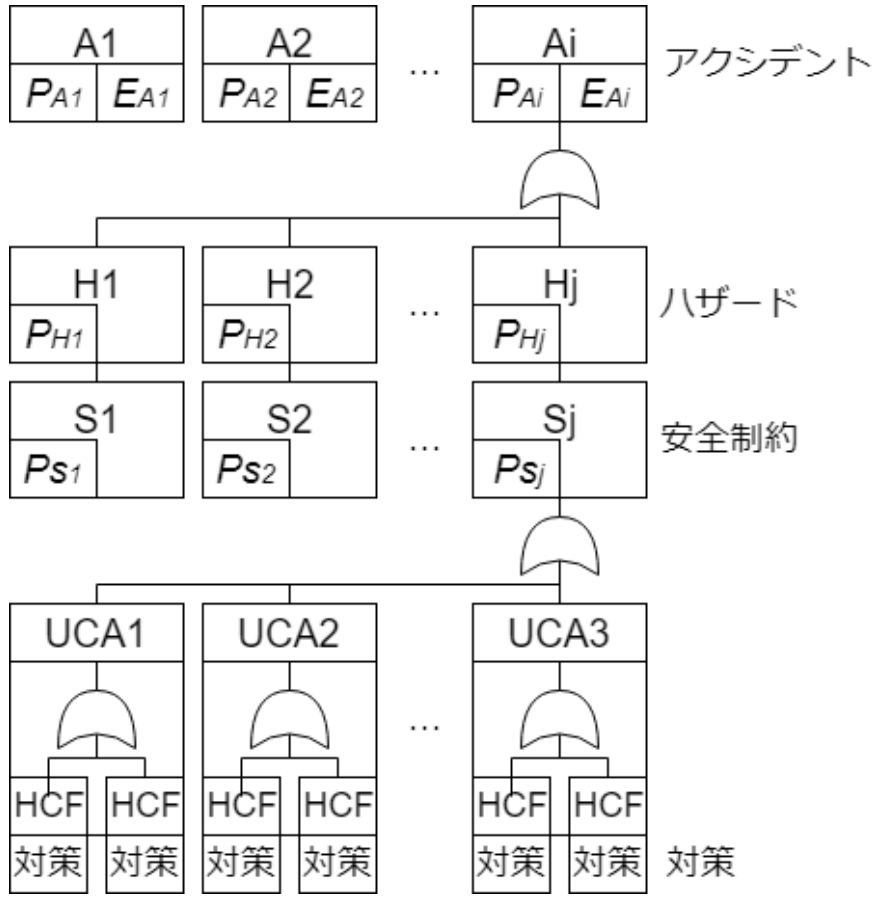
UCA	確率	ゲート	ワード	事象	確率	ゲート	事象	確率
UCA1-N-1	0.109891	OR	EN	インスリンポンプの電源喪失	0.001	AND	インスリンポンプの内部電源喪失	0.01
							電池切れ	0.1
			FA	インスリンポンプの故障	0.01			
			HE	操作忘れ	0.1			
UCA1-P-1	0.01593505	OR	HE	医者から不適切な医療指示を受けた	0.001			
			HE	操作ミス	0.01			
			S	使用者以外の第三者が故意に不適切な設定を行った	0.005			
			EN	インスリンポンプの電源喪失	0.001	AND	インスリンポンプの内部電源喪失	0.01
							電池切れ	0.1
			FA	インスリンポンプの故障	0.01			
			HE	操作忘れ	0.1			

UCA	確率	ゲート	ワード	事象	確率	ゲート	事象	確率
UCA1-N-1	0.057121675	OR	EN	インスリンポンプの電源喪失	0.0005	AND	インスリンポンプの内部電源喪失	0.005
							電池切れ	0.1
			FA	インスリンポンプの故障	0.007			
			HE	操作忘れ	0.05			
UCA1-P-1	0.007483011	OR	HE	医者から不適切な医療指示を受けた	0.001			
			HE	操作ミス	0.003			
			S	使用者以外の第三者が故意に不適切な設定を行った	0.0035			
			EN	インスリンポンプの電源喪失	0.0005	AND	インスリンポンプの内部電源喪失	0.005
							電池切れ	0.1
			FA	インスリンポンプの故障	0.004			
			HE	操作忘れ	0.03			

対策	低減率	コスト	実コスト	フラグ
	0.5	100	100	1
	0.6	200	0	0
	0.7	100	100	1
	0.5	30	30	1
	0.4	60	0	0
	0.3	80	80	1
	0.7	20	20	1
	0.5	80	80	1
	0.9	200	0	0
	0.4	100	100	1
	0.3	70	70	1

手順5、手順6

- EFTの下位事象の確率を推定すると、UCAの発生確率が求められる
  - ➢UCAの発生確率のOR演算により アクシデントの発生確率P_Aが求められる
- アクシデント発生時の影響の大きさを推定する
  - ➢通常は被害額の大きさを推定
- 各アクシデントのリスクの総和(トータルリスク)を最も低減する対策を選定



結果

STPAでの分析

項目	数
アクシデント	2
ハザード(=安全制約)	6
コンポーネント	7
コントロールアクション	6
安全でないコントロールアクション	17

ディフェンスツリーでの分析

項目	数
ツリー	17
最下位事象(ハザード誘発要因)	96
ソルバーによる求解時間	約1分程度

識別したHCFの例

- 遠隔通信を行う機器によるHCF
  - ➢測定機とトランスミッタは短距離無線により通信を行う
  - ➢なりすましや通信データの改ざんにより不正な投与が行われる可能性あり
- 時刻の同期によるHCF
  - ➢現状では利用開始時にユーザが手動で設定する前提
  - ➢NTPサーバと同期を行う場合、これを悪用した攻撃が発生する可能性あり
- 機内モードによるHCF
  - ➢機内モードのONにより全ての無線通信が停止する
  - ➢タイミングによってはスマートガード機能が機能しない可能性あり

考察

より現実に近い対策選定について

- 実際の対策選定では
  一つのHCFに対して複数の対策が存在する
  一つの対策が複数のHCFの発生確率に影響する
  可能性がある

➢これを考慮した上で求解が可能であるか検証が必要

分析の”漏れ”について

- 提案手法のツリー作成は分析者の主観による

➢分析者の技量によらず分析漏れがないことを担保できる手法の検討

今後の展望

- 具体的な対策内容と低減率の設定
  セキュリティ面の対策：「IoT開発におけるセキュリティ設計の手引き※1」
  セーフティ面の対策：実際のインスリンポンプに設定されているもの

- セキュリティ上のHCFの発生確率や対策による低減率の分散を考慮した分析の導入
  CrystalBallによるモンテカルロ法

- 対策選定の精度に関する評価

まとめ

- IoTにはセーフティも考慮したセキュリティ・バイ・デザインの実践が必要
  - セーフティとセキュリティの脅威を統合的に分析できる手法が必要

- STPAを拡張することで以下の要件を満たす提案手法を開発する
  - 制御構造が複雑に絡み合ったシステムを分析できること
  - セキュリティと安全性を統合的に分析できること
  - 対策選定のためにリスクの定量的分析を含むこと

- 提案手法を用いることでセキュリティ上の要因により機能安全だけでは防げない事故を設計段階で予測・対策できる