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

早川拓郎[1] 佐々木良一[1] 金子朋子[2] 高橋雄志[1] 大久保隆夫[3]

概要：IoT(モノのインターネット)の普及が進んでいる．従来スタンドアロンで用いられてきた機器がIoT ではインターネットに接続し，機器同士が連携することで新しい機能が実現される．しかし，IoT は機器の性質上，動作の停止や誤作動により人の命や環境に危険をもたらす可能性がある．したがって，IoT では従来別々の分野として扱われてきたセキュリティとセーフティを統合的に扱う必要がある．そこで，本稿では STPA(System-Theoretic Process Analysis) と呼ばれる安全解析手法を用いたセキュリティとセーフティの両方に対応可能なリスク分析手法を提案する．また，適用例として糖尿病向け医療機器であるインスリンポンプに対して分析を行った結果を示す．

Proposal and Application of Security/Safety Evaluation Method for Medical Device System Including IoT

TAKUO HAYAKAWA[1] RYOICHI SASAKI[1] TOMOKO KANEKO[2]
YUJI TAKAHASHI[1] TAKAO OKUBO[3]

1. はじめに

様々な”モノ”をインターネットと接続することで新たな機能や価値を実現する IoT(モノのインターネット)の普及が進んでいる．IoT の対象はエアコンや冷蔵庫などの家電から体温計やインスリンポンプのような医療機器まで多岐に渡る．これらの多くはもともとスタンドアロンでの動作を前提とした機器であり，インターネットと接続することでこれまで想定されなかったセキュリティ上の脅威に晒されることになる.また,例として挙げた医療機器のように，誤作動や停止が人の命や環境に危険をもたらす可能性のある IoT 機器も存在する．したがって，IoT では従来の機器では起こり得なかった，セキュリティ上の脅威が安全性に直接影響するという状況が起こり得る．例えば，2016 年には糖尿病患者向け医療機器であるインスリンポンプについて，第三者によるなりすましに繋がる脆弱性[1]が発見され，セキュリティ上の脅威が機器の誤作動や停止の原因となることが示された．しかし，この例でメーカーは機器への対策を行わず，ユーザへ使用法に関する指示を呼びかけるに留まった．このように，IoT 機器の中には流通後のセキュリティ対策が困難なものがあり，メーカーには安全性も考慮したセキュリティ･バイ･デザインの実践が求められる．

セキュリティ・バイ・デザインを実現するためには，設計段階であらかじめセキュリティ上の脅威を識別し，その影響の大きさに応じて各脅威への対策を立案する必要がある．従来，安全性の脅威分析には故障の木解析(Fault Tree Analysis，FTA)や故障モード影響解析(Failure Mode and Effect Analysis，FMEA)等が用いられてきた．これらの手法を用いることでシステムの脅威を識別するとともに，脅威の発生確率や影響の大きさからリスク値を求めることができる．また，リスク値を基に，より効果的な対策を選択することができる.しかし,これらの手法は戦後のミサイル，ロケット開発向けに作成された手法であり，現代のソフトウェアやネットワークを含むシステムの分析を対象としていない．したがって，IoT のようなシステムを分析するには不適当であると言える．また，セキュリティ上の脅威分析には FTA の派生形である攻撃木解析(Attack Tree Analysis, ATA)[2]が用いられる．しかし，ATA はセキュリティを対象とした手法であり，機器の故障を含む安全上の脅威を分析するには不適切である．したがって，IoT のセキュリティ・バイ・デザインを実現するには，複雑なシステムに適用でき，セキュリティとセーフティを統合的に扱うことのできる脅威分析が必要である．

本稿では IoT においてセキュリティとセーフティ両方の脅威を識別し，脅威の発生確率を定量的に算出する手法を提案する．加えて，提案手法の適用例として，糖尿病患者向け医療機器であるインスリンポンプが直接インターネットと接続して IoT として機能すると仮定して分析を行った．

1 東京電機大学
2 IPA
3 情報セキュリティ大学院大学

2. 関連手法

2.1 STPA(System-Theoretic Process Analysis)

近年，Leveson らにより FTA や FMEA に代わる安全解析手法として STPA(System-Theoretic Process Analysis) [3]が開発され，自動車や原子力プラントなどの様々な分野で利用が進んでいる．STPA は故障やヒューマンエラーを対象としていた従来の手法とは異なり，システム内の制御が安全制約を違反したときにアクシデントが起こると定義している．これにより，ソフトウェアという故障のない構成要素が重要となった現代のシステムにも対応することができる．また，STPA ではシステム構成全体を識別するため，従来の手法では困難だった，構成要素間の相互作用を考慮した分析を行うことができる．

STPA の手順の概要を以下の表 1 に示す．STPA は準備段階と対策検討を含めると 5 つの手順がからなる．準備 1 では損害を伴う望ましくない事象であるアクシデント，アクシデントに繋がる条件や状況であるハザード，ハザードが発生しないために必要な安全制約を識別する．例として簡単に自動車のアクシデント，ハザード，安全制約を識別したものを以下の表 2 に示す．準備 2 ではシステムの構成図であるコントロールストラクチャを構築する．コントロールストラクチャにはシステムの構成要素であるコンポーネント，あるコンポーネント(コントローラ)から別のコンポーネント(被コントロールプロセス)に行われる制御であるコントロールアクション，コントロールアクションに対するフィードバックが含まれる．また，コントローラはコントローラが認識している被コントロールプロセスの状態であるプロセスモデルを持つ．この他にシステムによっては情報の流れであるデータフローを記載する．自動車のコントロールストラクチャを簡単に作成した例を以下の図 1 に示す．STEP1 では準備 2 で作成したコントロールストラクチャに含まれるコントロールアクションから安全でないコントロールアクション(Unsafe Control Action，UCA)を導出する．導出はコントロールアクションに以下の 4 つのガイドワードを適用することで行う．

- 与えられないとハザード(N)
- 与えられるとハザード(P)
- 早すぎる，遅すぎる，誤順序だとハザード(T)
- 早すぎる停止，長すぎる適用だとハザード(S)

図 1 で示した「アクセルを踏む」というコントロールアクションについて UCA の導出を行った例を以下の表 3 に示す．STEP2 では UCA に繋がるハザード誘発要因(HCF)の特定を行う．特定はコントロールストラクチャから UCA に関連するコンポーネントを抜き出しコントロールループダイヤグラムを作成することで行う．IPA はハザードの識別に用いるヒントワードを示し，これを用いることで HCF の特定を行う方法を示した[4][5]．最後のまとめは STEP2 で特定した各 HCF に対する対策を検討する手順であるが，具体的な検討手順は示されていない．

表 1.STPA の手順

手順	内容
準備 1	アクシデント，ハザード，安全制約の識別
準備 2	コントロールストラクチャの構築
STEP1	安全でないコントロールアクションの識別
STEP2	ハザード誘発要因の特定
まとめ	対策の検討

表 2.アクシデント，ハザード，安全制約の例

アクシデント	ハザード	安全制約
A1．自動車と人がぶつかる	H1-1．運転手が信号を無視する	S1-1．運転手は赤信号の交差点を通過してはならない
	H1-2．自動車の速度が速すぎる	S1-2．運転手は法定速度を守らなければならない

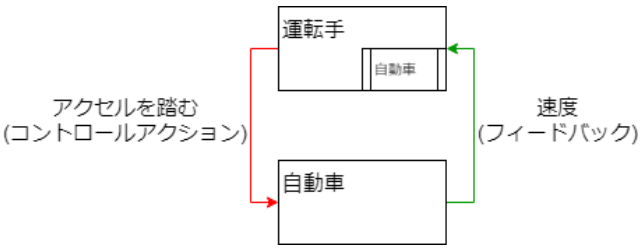

図 1.コントロールストラクチャの例

表 3. UCA 導出の例

ガイドワード	コントロールアクション(アクセルを踏む)
N	安全制約違反が発生しないためハザードは発生しない
P	運転手が赤信号の交差点でアクセルを踏む(S1-1 違反)
T	運転手が青信号に変わるより早くアクセルを踏む(S1-1 違反)
S	運転手がアクセルを踏むのが長すぎると速度が超過する(S1-2 違反)

STPA を用いることで従来の安全解析手法では困難であったソフトウェアやネットワークを含む複雑なシステムの分析を行うことができる．一方で，STPA はあくまでセーフティ向けの分析手法であり，情報の機密性の喪失のようなセキュリティ特有の脅威を識別することが困難である．STPA をセキュリティ向けに拡張した手法として Young ら

による STPA-sec[6]や STPA-sec に脅威分類 STRIDE による脅威分類を追加した金子らによる改良型 STPA-sec[7]が挙げられる．これらの手法は STPA の各手順にセキュリティの視点を追加することでセーフティ上の脅威に加え、安全性に影響するセキュリティ上の脅威の両方を識別可能にしている．しかし，Friedberg らは，STPA-sec では機密性の喪失のような安全性に直接的な影響を及ぼさない脅威を識別できないとし，セキュリティとセーフティの統合的な分析を実現した手法である STPA-SafeSec[8]を開発した．STPA-SafeSec では STPA では 1 層のものとして扱っていたコントロールストラクチャを物理層と機能層の 2 層に分けることによって，統合的な分析を可能としている．しかし，STPA-SafeSec をはじめとする STPA に関連する手法全てに共通して定量的な分析は含まれていない．したがって，脅威の発生確率や影響の大きさに基づいたリスク値を用いた定量的な対策選定を行うことができない．そこで，提案手法ではセキュリティとセーフティの統合的な分析と定量的な脅威分析を実現することを目標とする．

2.2 EFT(Extended Fault Tree)

脅威分析手法の例として，FTA やその派生形である ATA が挙げられる．これらの手法では発生が望ましくない事象を頂上事象とし，木構造を用いて原因となる事象をトップダウンに導出する．これにより，頂上事象の大まかな原因である中間事象と，細かい原因である下位事象を求めることができる．上位の事象は下位の事象と OR もしくは AND のゲートで接続され, OR は下位の事象のいずれかが, AND は下位の事象が全て起こったときに上位の事象が発生することを意味する．また，子事象の発生確率から親事象の発生確率を求めることができる．例えば，事象 x と事象 y について，x OR y を「(x, y)」，x AND y を「xy」とすると，それぞれの発生確率 P(x, y)，Pxy は以下の式で表せる．

$$P_{(x,\ y)} = 1 - (1 - P_x) \times \left(1 - P_y\right)$$
$$P_{xy} = P_x \times P_y$$

下位事象の発生確率が推定できれば，この式を用いて下位の事象から順に頂上事象の発生確率を求めることができる．

FTA が故障やヒューマンエラーなどの安全上の脅威を対象とする一方，ATA では特にセキュリティ上起こってはならない事象に繋がるセキュリティ上の脅威を導出することができる．しかし，逆に ATA では安全上の脅威を分析することはできない．そこで, 提案手法では Fovino らによる拡張故障の木(Extended Fault Tree, EFT)[9]を用いる．EFT ではセキュリティに対する攻撃はシステムの故障を利用することで行われるという考えに基づき，FT の下位事象と AT の頂上事象を接続する．したがって，EFT によって安全上起こってはならない事象に繋がる安全上の脅威とセキュリティ上の脅威を統合的に導出することができる．また, FTA や ATA と同様に先に述べた方法を用いて確率を扱った定量的な分析が可能である．

EFT の FT 部分は従来の FTA のものと同等である．一方，AT 部分には Masera らによって提案された AT[10]を用いる．この AT では通常区別しないノードの種類を以下の 3 種類に分類する．

- 脆弱性 － システムが持つ脆弱性
- 条件 － 環境条件
- オペレーション － 攻撃者が取る行動

前述の考え方に基づき，3 種類の分類のうちオペレーションノードと FT を接続することができる．EFT の例を以下の図 2 に示す．この例のうち AT 部分は点線で囲まれた部分である．また，脆弱性ノードを楕円形，条件ノードを長方形，オペレーションノードを六角形で示した．

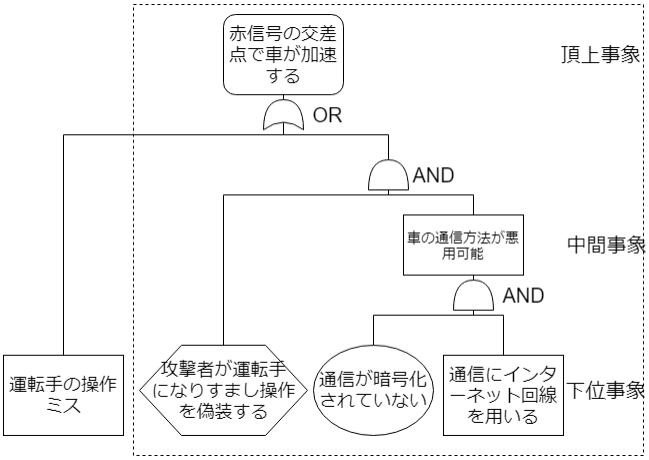

図 2.EFT の例

2.3 ディフェンスツリー

ディフェンスツリー[11]は ATA に対策の費用と効果を加えたモデルである．ディフェンスツリーを用いることでセキュリティ上の脅威に対する対策の費用対効果を求めることができる．これにより，より低コストで脅威の発生確率を低下させることのできる対策の組み合わせを導出することができる．相原らは EDC 手法[12]の中でディフェンスツリーを利用し，対策の予算を制約条件，リスク値を目的関数とすることで対策選定を組み合わせ最適化問題としてモデル化した．また，リスク値に対策コストを足したトータルリスクに応じて対策を選定する方法を示した．ディフェンスツリーの例を以下の図 3 に示す．図の例の場合，例えば事象 A の発生時の予想損害コストが 1000 だとすると，各対策を行った場合の総合リスク値は以下の表 4 のように変化する．したがって，この例では対策 Y と対策 Z を組み合わせることで最もリスクを低下させることができる．

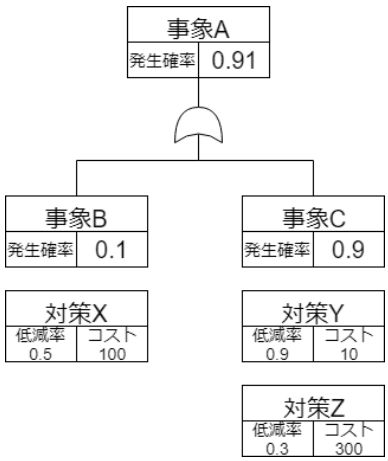

図 3.ディフェンスツリーの例

表 4.対策の組み合わせとトータルリスクの変化

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

3. 提案手法

3.1 概要

1 章で述べた通り，IoT で安全性を考慮したセキュリティ・バイ・デザインを実現するためにはセキュリティとセーフティの脅威を統合的に分析することのできる手法が必要である．また，対策選定の際には、脅威の発生確率や影響の大きさに基づいて算出したリスク(発生確率×影響の大きさ)の総和, すなわちトータルリスクをより低減させることのできる対策を選定する必要がある．そのためには，手法の中に定量的な分析を含む必要がある．IoT のような様々な構成要素が複雑に絡み合ったシステムにおいて，これらの必要を全て満たせる既存の脅威分析手法は存在していない. そこで, 本稿の提案手法では IoT のセキュリティ・バイ・デザインを実現するため，以下の要件を満たすことを目指す.

- セキュリティとセーフティを統合的に扱えること
- ソフトウェアやネットワークを含む複雑なシステムに対する分析が可能であること
- 確率とコストに基づく定量的な脅威分析を含み，対策選定を支援できること

これらの要件を満たすため，提案手法では STPA をベースとし，EFT とディフェンスツリーを組み合わせる．

3.2 分析手順

提案手法の手順は STPA の手順に準ずるが, STPA にはない定量分析の手順を含む。また、いくつかの手順に作業を加える．提案手法の手順を以下の表 5 に示す．STPA と比較して手順が変更されているのは, 手順 1, 手順 4 である。

表 5.提案手法の手順

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

(1) **手順 1:アクシデント，ハザード，安全制約の識別**

STPA と同様にアクシデント, ハザード, 安全制約の識別を行う．その際，STPA では考慮しない，機密性の喪失などのセキュリティインシデントをアクシデントとして識別し，安全制約についてもセキュリティ上のものを識別する．

(2) **手順 2:コントロールストラクチャの構築**

STPA と同様にコントロールストラクチャの構築を行う．

(3) **手順 3:UCA の識別**

STPA と同様に UCA の識別を行う．

(4) **手順 4:ハザード誘発要因の特定**

手順 3 で識別した UCA を頂上事象とする EFT を作成する．作成にあたり，まずはコントロールストラクチャから安全でないコントロールアクションと関連するコンポーネントを抜き出し，コントロールループダイヤグラムを作成する．続いて，コントロールループダイヤグラムに含まれるコンポーネント，コントロールアクション，フィードバックに対して以下の表 6 の 10 のヒントワードを適用し，頂上事象の子となる中間事象を作成する．セキュリティ上の脅威を識別するためのヒントワードとしては Microsoft の脅威分類である STRIDE[13]を用いる．この際，中間事象と頂上事象は OR ゲートで繋がる．その後，中間事象から下位事象を導出することで EFT とする．そして，EFT の下位事象をハザード誘発要因とし，下位事象から頂上事象に辿る流れをハザードシナリオとする．定量的分析を含まない脅威分析のみを行う場合はこの手順で分析を終了する．

表 6.中間事象導出のヒントワード

対象	ヒントワード	意味
セーフティ	EN	環境要因

	FA	機器故障
	BG	プログラムのバグ
	HE	ヒューマンエラー
セキュリティ	S	なりすまし
	T	改ざん
	R	サービス不能
	I	情報漏洩
	D	サービス不能
	E	権限昇格

(5) **手順 5:アクシデントの確率分析**

手順 4 で作成した EFT のすべて下位事象についてその発生確率を推定する．推定の際は統計データのある下位事象についてはその値を用いたり，関係者同士のリスクコミュニケーションにより決定した値を設定する．この値に絶対的な算出根拠は存在しないが，設定することで個々の下位事象がシステム全体にどの程度の影響をもたらすか確認できる．提案手法で作成する EFT の下位事象となる HCF の発生確率からアクシデントの発生確率を求める方法の全体像を示した図を以下の図 4 に示す．アクシデントの発生確率を求めるにあたり、まずは UCA の発生確率を求める．ある一つの UCA である UCAk の発生確率P_{UCAk}は通常の EFT と同様に求めることができる．次に、安全制約違反の確率を求める．安全制約違反は安全制約を違反する UCA のいずれか 1 つ以上が発生したときに起こると考えられる．したがって,安全制約 Sj を違反する UCA が UCA1 から UCAk まで存在する場合，Sj が違反される確率P_{Sj}は OR 演算により以下の式で表すことができる．

$$P_{Sj} = 1 - \prod_{n=1}^{k}(1 - P_{UCAn})$$

また，安全制約違反とハザードは 1 対 1 に対応しており、安全制約違反とハザードの発生は同義であるため，ハザード Hj の発生確率P_{Hj}はP_{Sj}に等しく，以下の式が成り立つ．

$$P_{Hj} = P_{Sj}$$

次に、アクシデントの発生確率を求める．アクシデントは対応するハザードのうちいずれか 1 つ以上が発生したときに起こると考えられる．したがって、アクシデント Ai に対応するハザードが H1 から Hj まで存在する場合、Ai の発生確率P_{Ai}は OR 演算により以下の式で表すことができる．

$$P_{Ai} = 1 - \prod_{n=1}^{j}(1 - H_n)$$

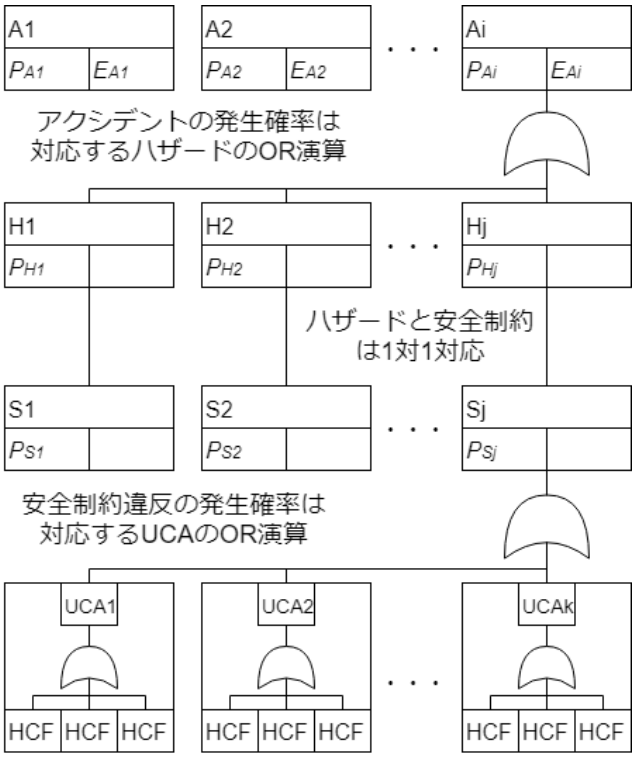

図 4.アクシデントの確立分析の全体像

(6) **手順 6:対策選定**

対策選定を行う場合，各アクシデントが発生した際に予想される影響の大きさを推定しておく．通常は被害額の値を用いる．アクシデントAにより予想される影響の大きさをE_Aとすると，ある一つのアクシデントA_iによるリスクR_{Ai}は以下の式で表すことができる．

$$R_{Ai} = P_{Ai} \times E_{Ai}$$

また，システムのアクシデントがA_1からA_iまで存在する場合，システムのトータルリスクR_Tは以下の式で表せる．

$$R_T = \sum_{k=1}^{l} R_k$$

したがって，対策を選定する場合は，より低いコストでR_Tの値がより低くなるように対策を組み合わせればよい．

4. 適用

4.1 適用対象

本稿では，提案手法の適用例として糖尿病患者向け医療機器であるインスリンポンプに対して，提案手法による分析を手順 4 まで行った．インスリンポンプは主に以下の 3

つの機能を持つ．

(1) **インスリンボーラス(投与)機能**

インスリンポンプの主な機能として，インスリンのボーラス機能がある．使用者はインスリンポンプの注射器部分(注入セット)を常に皮下に注射しておき，インスリンの投与が必要な際にはインスリンポンプ本体を操作してボーラス指示を行う．

(2) **持続グルコースモニタ(CGM)機能**

インスリンポンプはボーラス機能とは別に CGM 機能を持つ．CGM 機能を利用する場合，使用者は皮下にエンライトセンサと呼ばれるグルコース値を測定するセンサを皮下に穿刺する．エンライトセンサはトランスミッタにグルコース値送信し，トランスミッタは値を短距離無線信号に変換してインスリンポンプに送信する．これにより，使用者はインスリンポンプを通じて自身の皮下のグルコース値を確認することができる．

(3) **インターネットとの通信機能**

既存のインスリンポンプには使用者の所有するパソコンを経由してインターネット上のサーバに血糖値の推移等を含む血糖値情報を保存することのできるものがある．本稿ではこのようなインスリンポンプが IoT 化し，パソコンを経由せずに Wi-Fi 等を用いて直接インターネットと接続できる場合を想定する．インスリンポンプから送信された血糖値情報はインターネット上のサーバに保存される．使用者と使用者を診断する医者はサーバ上から血糖値情報を取得することができる．また，医者はサーバから得た血糖値情報を基に，使用者に対して治療指示を行う．

4.2 分析

(1) **手順 1:アクシデント，ハザード，安全制約の識別**

手順 1 でアクシデント，ハザード，安全制約を識別した結果を以下の表 7，8 に示す．各アクシデントには ID としてA_kを割り当てた．また，アクシデントA_kと対応するハザードには ID としてH_{k-l}を，ハザードH_{k-l}と対応する安全制約には ID としてS_{k-l}を割り当てた．

表 7.アクシデント

アクシデント	
ID	内容
A_1	患者の健康が損なわれる．
A_2	患者の治療情報が流出する．

表 8.ハザード，安全制約

ハザード		安全制約	
ID	内容	ID	内容
H_{1-1}	インスリンが過剰に投与される	S_{1-1}	インスリンポンプは低血糖時に投与を停止しなければならない
H_{1-2}	高血糖時にインスリンが投与されない	S_{1-2}	患者は高血糖時にインスリンポンプに投与指示しなければならない
H_{1-3}	適切な治療指示が与えられない	S_{1-3}	医者は患者の血糖値情報から適切な医療指示をしなければならない
H_{2-1}	通信が盗聴される	S_{2-1}	通信経路の安全が確保されなければならない
H_{2-2}	なりすましが行われる	S_{2-2}	インスリンポンプは認証した機器としか通信を行ってはならない

(2) **手順 2：コントロールストラクチャの構築**

4.1 節で述べた前提を基にコントロールストラクチャを構築した．構築したコントロールストラクチャを以下の図 5 に示す．コントロールストラクチャから識別できるコントロールアクションは 7 つであった．

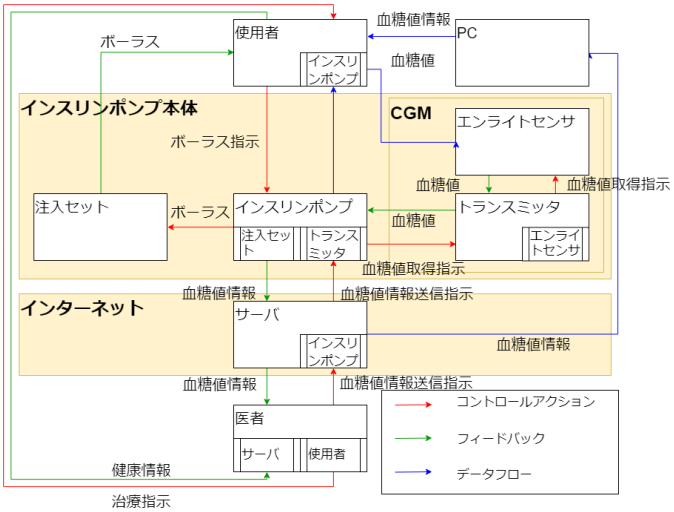

図 5.コントロールストラクチャ

(3) **手順 3:UCA の識別**

手順 2 で識別したコントロールアクションに対し，ガイドワードを適用して UCA を識別した．その結果を以下の表 9 に示す．また，各 UCA の内容を表 10 に示す．今回の例では 18 の UCA が識別できた．

表 9.UCA の識別

コントロールアクション	N	P	T	S
ボーラス指示	UCA1N	-	UCA1T	-
ボーラス	UCA2N	UCA2P	UCA2T	UCA2S

血糖値 取得指示	UCA3N	UCA3P	UCA3T	-
血糖値 取得指示	UCA4N	-	UCA4T	-
血糖値情報 送信指示	UCA5N	UCA5P	-	-
血糖値情報送信指示	UCA6N	UCA6P	-	-
治療指示	UCA7N	UCA7P	UCA7T	-

表 10.UCA の内容

UCAID	内容	違反する安全制約
UCA1N	高血糖時でも患者がボーラスを行わないと患者の健康が損なわれる.	SC1-2
UCA1T	使用者のボーラス指示が遅すぎると，使用者が高血糖になるため，健康が損なわれる.	SC1-2
UCA2N	高血糖時でもボーラスが行われないため患者の健康が損なわれる.	SC1-2
UCA2P	低血糖時にボーラスが行われると患者の健康が損なわれる.	SC1-1
UCA2T	ボーラスが遅すぎると，患者が高血糖になるため健康が損なわれる.	SC1-2
UCA2S	ボーラスが長すぎると患者の血糖値が低くなりすぎるため，健康が損なわれる.	SC1-1
UCA3N	患者が高血糖を認識できないため，患者の健康が損なわれる.	SC1-2
UCA3P	インスリンポンプになりすました他の端末が指示していた場合，なりすましによる情報漏洩が発生する.	SC2-2
UCA3T	血糖値取得指示が遅すぎると患者またはインスリンポンプが低血糖または高血糖を認識するのが遅れるため，患者の健康が損なわれる.	SC1-1, SC1-2
UCA4N	患者が高血糖を認識できないため，患者の健康が損なわれる.	SC1-2
UCA4T	血糖値取得指示が遅すぎると患者またはインスリンポンプが低血糖または高血糖を認識するのが遅れるため，患者の健康が損なわれる.	SC1-1, SC1-2
UCA5N	医者が患者の血糖値情報を得ることができないため，適切な治療指示をすることができない.	SC1-3
UCA5P	血糖値情報送信指示が盗聴された場合，情報漏洩が発生する.	SC2-1
UCA6N	医者が患者の血糖値情報を得ることができないため，適切な治療指示をすることができない.	SC1-3
UCA6P	血糖値情報送信指示が盗聴された場合，情報漏洩が発生する.	SC2-1
UCA7N	患者が医者からの適切な医療指示を得られないため，健康が損なわれる.	SC1-3
UCA7P	患者の治療指示が誤っていた場合，患者の健康が損なわれる.	SC1-3
UCA7T	患者の治療指示が遅すぎる場合，患者の健康が損なわれる.	SC1-3

(4) 手順 4:ハザード誘発要因の特定

手順 3 で識別した各 UCA について，コントロールループダイヤグラムと EFT を作成し HCF を特定した．作成した EFT は 18 個に及ぶため，例として UCA3N のコントロールループダイヤグラムと EFT を以下の図 6，7 に示す．この場合，セーフティの HCF は 5 個，セキュリティの HCF が 4 個特定された．

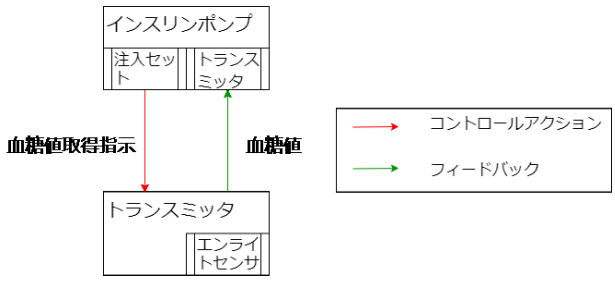

図 6.UCA3N のコントロールループダイヤグラム

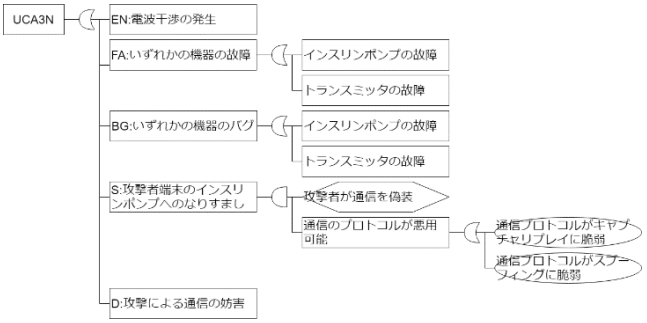

図 7.UCA3N の EFT

5. 結果と考察

実際に提案手法に関する考察は以下の通りである．

(1) **HCF の重複の発生**

今回の例では安全でないコントロールアクションが 18，その中の一つである UCA3N の HCF を 9 と多くの脅威を識別することができた．また、全体では 100 を超える HCF を特定した．一方で，現在の手順 4 の方法では作成するコントロールループダイヤグラムが複数の UCA に対して同じような内容になることがあり，EFT から識別される HCF に重複が起こることがあった．手順 4 の方法を改良し，HCF の重複を防ぐことを今後の課題としたい．

(2) **対策選定の手順化**

提案手法を用いることで既存の STPA 関連手法では求められなかった，アクシデントの発生確率を求められることを示した．また，アクシデントの発生確率と予想される影響の大きさから，システムのトータルリスクを求めることによって，より有効な対策を選定する方法を示した．しかし，今回の例だけでも，一人の分析者が計算を行うには膨大な数の HCF が導出されたため，現状の手順のみでは対策の選定が困難である．今後は対策選定の手順の具体化を行うことを課題としたい．

6. 評価

本稿での提案手法と既存の STPA 関連手法を比較した結果を以下の表 11 に示した．提案手法は IoT のセキュリティ・バイ・デザインに不可欠である，セキュリティとセーフティの統合的な脅威分析を含んでいる．また，既存の STPA 関連手法では実現していなかった，確率の定量的な分析を実現した．

表.11.STPA 関連手法と提案手法の比較

手法	①	②	③	④	⑤
STPA[3]	○	×	×	×	×
STPA-sec[6]	○	○	×	×	×
改良型 STPA-sec[7]	○	○	×	○	×
STPA-SafeSec[8]	○	○	○	×	×
提案手法	○	○	○	○	○

① セーフティの分析
② セキュリティの分析
③ セキュリティとセーフティの統合
④ 脅威分析手順を含む
⑤ 確率の定量分析を含む

7. おわりに

本稿では，IoT 機器の安全性を考慮したセキュリティ・バイ・デザインを実現するための手法を提案した．提案手法では既存の安全解析手法である STPA と EFT，ディフェンスツリーを組み合わせることによって，セキュリティとセーフティの統合的な分析を実現した．また，従来の STPA の関連手法では実現されていなかった，定量的な分析方法を示した．一方，提案手法で導出される脅威は多岐に渡り，確率やリスクの計算を人手によって行うのが困難であることが明らかになった．今後はさらに確率計算を含めた試適用を進め，対策選定手順の具体化を行う予定である．加えて，提案手法による分析と対策選定を支援するツールを作成する予定である．

参考文献

[1] Japan Vulnerability Notes, JVNVU#95089754 Animas OneTouch Ping に複数の脆弱性，入手先 <https://jvn.jp/vu/JVNVU95089754/> (参照 2018-05-01).

[2] B Schneier, ATTACK TREES，入手先 <http://tnlandforms.us/cs594-cns96/attacktrees.pdf> (参照 2018-05-01).

[3] N Leveson, Engineering a Safer World, Systems Thinking Applied to Safety, 2012

[4] 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～，入手先 <https://www.ipa.go.jp/files/000051829.pdf> (参照 2018-05-01)

[5] 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～(実践編)，入手先< https://www.ipa.go.jp/files/000058231.pdf> (参照 2018-05-01)

[6] W Young and N Leveson. “Systems thinking for safety and security, ” ACSAC '13, pp. 1-8, Dec. 2013.

[7] 金子朋子，高橋雄志，大久保隆夫，勅使河原可海 and 佐々木良一．”安全解析手法 STAMP/STPA に対するセキュリティ視点からの脅威分析の拡張停案，” CSS2017，Oct. 2017.

[8] I Friedberg, K McLaughlin, P Smith, D Laverty and S Sezer. “STPA-SafeSec: Safety and security analysis for cyber-physical systems, ” Journal of Information Security and Applications, vol. 34, pp. 183-196, Jun. 2017.

[9] I N Fovino, M Masra and A Cian. “Integrating cyber attacks within fault trees, ” Reliability Engineering and System Safety, vol. 94, pp. 1394-1402, Sep. 2009.

[10] M Masera and I N Fovino.” Through the Description of Attacks: A Multidimensional View, ” International Conference on Computer Safety, Reliability, and Security, pp. 15-28, Sep.2006.

[11] S.Bistarelli, F.Fioravanti and P.Peretti. ”Defense trees for economic evaluation of security investments, ” in Proc. ARES, pp. 416-423, Apl.2006.

[12] 相原遼，石井亮平 and 佐々木良一．”イベントツリーとディフェンスツリーを併用した標的型攻撃に対するリスク分析手法の提案と適用，”情報処理学会論文誌，vol.59，No3，pp. 1082-1094，Mar. 2018.

[13] Microsoft, The STRIDE Threat Model，入手先< https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20) > (参照 2018-05-13)