リモートメンテナンスを伴い フィードバックを有する医療用 IoT システムのリスクアセスメント手法

佐々木良一[1]，金子朋子[1]，髙橋雄志[1]，福澤寧子[2]

概要：近年，社会の情報システムへの依存度の増大に伴い，情報システムの安全性を評価し，不十分なら適切な対策案の組み合わせを求めるためのリスクアセスメント手法の重要性が増してきている．しかし，医療システムに多く見られる，リモートメンテナンスを伴いフィードバック機能を有する IoT システムを対象としたリスクアセスメント手法は提案されていなかった．そこで，フィードバック機能を持つシステムにリスクをもたらすハザード原因要因（HCF：Hazard Causal Factor）を，STAMP/STPA 法を改良した方式を用い，広く効率よくリストアップできるようにするとともに，そのようにしてリストアップされた HCF のうちリスクの大きなものを，拡張フォルトツリーを用いた準定量的分析によりリスクの大きさをレベル付けできるようにしている．次に，リスクの大きな HCF に対応するための対策を抽出し，Maintainability と Security，Safety の関係を，アンアベイラビリティを核として定量的に結び付けることにより，バランスよく対策案の最適組み合わせを求めることができるようにした．このようにして開発した手法と，そのための支援用プログラムを，インスリン注入システムに適用することにより，リスクが大きい HCF や対策案の最適な組み合わせを具体的に求めることができるとともに，方式の有効性を確認することができた．

Risk Assessment Method for Medical IoT System with Remote Maintenance and Feedback

RYOICHI SASAKI[1] ,TOMOKO KANEKO[1], YUJI TAKAHASHI[1],
YASUKO FUKUZAWA[2]

1. はじめに

近年，社会の情報システムへの依存度の増大に伴い，情報システムの安全性を評価し，不十分なら適切な対策案の組み合わせを求めるためのリスクアセスメント手法の重要性が増してきている．特に最近普及してきている IoT(Internet of Things)は，サイバー攻撃の影響が IoT 機器の Security 低下だけでなく，人命などの Safety への影響が生じる可能性が増大するといった特徴があるため，その重要性が高かった．しかし，IoT システムは制御系のように種々のフィードバックを含むシステムが多く，従来のやり方ではアセスメントが困難であった．このような問題を解決するための手法として MIT のナンシー・レブソンが開発した STAMP/STPA 法[1]呼ばれる手法がある．この手法はこの目的のためには優れたものであったが，Safety だけを扱うものでサイバー攻撃などの Security 要因が原因となって生じる安全の問題は扱えなかった．そこで，Safety だけでなく，Security も併せて扱える手法の開発が文献[2]に示すようにいろいろ行われてきており，著者らもこのための種々の手法の提案を行ってきた[3]-[7].

一方，IoT 機器は一般に寿命が長く，その機器を長く安心して利用するためにはメンテナンス（Maintenance）は不可欠である．また，IoT 機器は，広域に分散することが多いため，リモートメンテナンス（Remote Maintenance:以下 RM ともいう）が必要となることが多い．特に医療用 IoT 機器などにおいては，工学の専門家が現場にいないこともあり RM 機能を持たせようという動きが強い．このため，IoT 向けに RM に伴う Maintainability と Security and Safety をバランスよく実現するためのリスクアセスメント手法が必要になっており，著者らはそのための定量的手法を開発してきた[8].

しかし，この方式は，フィードバックを伴わないセンサーなどの IoT 機器を対象とするものであった．そこで今回，リモートメンテナンスを伴いフィードバックを有する医療用 IoT システムを対象としたリスクアセスメント手法（以降，SSFM: Risk Assessment Method on Safety and Security for IoT with Feedback and Remote Maintenance）を開発することとした．

この SSFM 手法は，フィードバック機能に対応するために STAMP/STPA 法を改良した方式[3]を基本的に用い，リスクをもたらすハザード原因要因（HCF：Hazard Causal Factor）を，広く効率よくリストアップできるようにすると

1 東京電機大学
2 大阪工業大学

ともに，そのようにしてリストアップされた HCF のうちリスクの大きなものを拡張フォルトツリー分析法（Extended Fault Tree :EFT）を用い準定量的分析によりレベル付けできるようにしている．次に，リスクの大きな HCF に対応するための対策を抽出し，Maintainability と Security ，Safety の関係をアンアベイラビリティを中心に定量的に結び付けることにより，バランスよく対策案の最適組み合わせを求める機能を持つ．このような方式の提案は従来なかったものである．

このようにして開発した SSFM 手法と，そのための支援用プログラム SSFMP（SSFM Program）を，インスリン注入システムに適用することにより，リスクが大きい HCF や対策案の最適な組み合わせを具体的に求めることができるとともに，方式の有効性を確認することができたので報告する．

2. 提案手法の概要

提案するリスクアセスメント手法は次のような手順で実施することとした．手順１－６を文献[3]の方式をベースとし，手順７－９を文献[8]の方式をベースとしている．

手順１　アセスメント対象の調査

手順２　リスク指標（起きては困る主要リスク等）のリストアップ

手順３　対象システムのコントロールストラクチャーの構築

手順４　コントロールストラクチャーを用い安全に影響を及ぼすＵＣＡ（Unsafe and Unsecure Control Action:アンセキュア・アンセーフティコントロールアクション）と影響を及ぼすリスク指標の明確化

手順５　リスク指標ごとにＵＣＡの原因となるＨＣＦの明確化

手順６　EFT（Extended Fault Tree：拡張フォルトツリー）上に各 HCF を位置づけ，準定量的分析を行うことによるリスクの大きなＨＣＦの明確化

手順７　リスクの大きなＨＣＦに対応した対策のリストアップ

手順８　アンアベイラビリティを核に各種のリスクを定量的に関連付け，対策コストの制約条件下にトータルリスク低減効果を最大化する対策案最適組み合わせ問題として定式化

手順９　定式化結果に基づき作成したプログラム SSFMP を用い対策案最適組み合わせを求解

手順１０　リスクコミュニケーションに基づく，採用対策に関する合意形成

文献[3]をベースとした方式を用いることにより，リスクをもたらすハザード原因要因（HCF : Hazard Causal Factor）を，広く効率よくリストアップできるようにするとともに，そのようにしてリストアップされた HCF のうちリスクの大きなものを準定量的分析によりランク付けできるようにしている．次に，文献[8]をベースにすることにより，リモートメンテナンスなどの効果も扱え，対策に関連する部分だけの定量化で済む効率的な定式化方法となっており，支援プログラム SSMFP を用いることにより効率的にバランスのよい対策案の最適組み合わせを求める機能を持つ．

3. インスリン注入システムの概要

本稿では，**図１**に示すようなインスリン注入を目的とした医療用 IoT システム（文献[９]を参考にして作成）を想定して提案するリスクアセスメント手法の適用を行った．

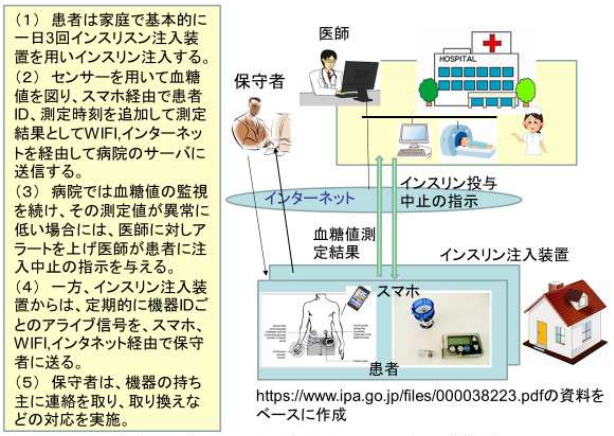

図１　インスリン注入システムの概要

4. 適用方法と結果

４．１　手順１　アセスメント対象の調査

アセスメント対象は上述したようなインスリン注入システムで，血糖値の値が基準値以下になると，医師にアラートを出して，インスリン注入停止の入力をさせる．また，リモートメンテナンスを行っており，インスリン注入装置からアライブ信号が来なくなったら異常と判断し，取り換えなどのメンテナンスを行うものとする．

４．２　手順２　リスク指標

ここでは，起きては困る主要リスクとして，次の 3 つをリストアップした．

（ａ）．生命にかかわる事象の発生

指標１：　インシュリンを誤って投入することにより血糖値が異常に低くなる

指標２：　インシュリンを誤って投入中止することにより血糖値が異常に高くなる

（ｂ）　重要情報の流出

指標３：　管理が不十分で患者の個人情報が漏洩

４．３　手順３　コントロールストラクチャーの構築

図１の対象を分析し，コントロールストラクチャーを**図２**のように想定した．

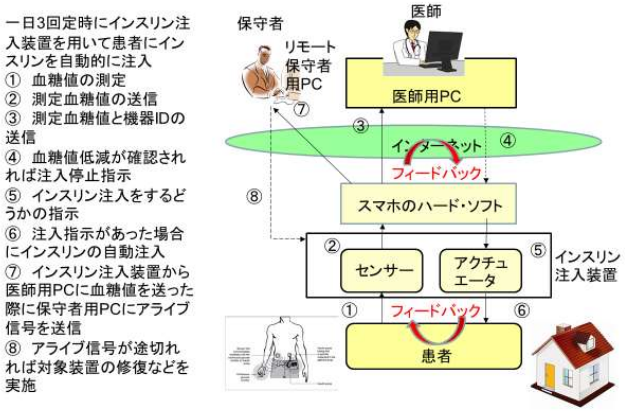

図2　コントロールストラクチャーの構築

４．４　手順４　ＵＣＡとその結果となるリスク指標の明確化

図２の①－⑥に示したコントロールアクションに対応して，非安全・非セキュアな結果となる UCA （Unsafe and Unsecure Control Action）を，A 表を用いて**表１**に示すようにして抽出する．Too Early や Too Late, Too soon や Too long など種々の制御の状態によって安全でない状態がリストアップできるのが STAMP/STPA の特長である．またここでは，血糖値上昇や血糖値異常低下など，どのリスク指標につながるかを記述し，あとで同一の結果となるツリーの要素を結合できるようにした．

この結果全部で 24 の UCA をリストアップした．

表1　UCA抽出結果の一例（A表使用）

分析者がいろいろ考えて記入　　STPAのガイドワード利用

コントロールアクション	Not Providing	Providing Causes hazard	Too early too late	Too soon too long
②センサー情報1送信血糖値	（UCA②N1）センサーから血糖値が与えられない＝＞血糖値が下がっているのに気つかない＝＞インスリン投入を続け血糖値異常低下（結果1）	（UCA②P1）血糖値を間違えて低くしたり低く改ざんする＝＞インスリン投入の中止＝＞血糖値上昇（結果2） （UCA②P2）血糖値を間違えて高くしたり高く改ざんする＝＞血糖値異常低下（結果1） （UCA②P3）センサーからスマホ間の通信のタッピング＝＞情報漏洩（結果3）	（UCA②L1）センサーから血糖値が与えられるのが遅すぎる＝＞血糖値が下がっているのに気つかない＝＞＝＞血糖値異常低（結果1）	—

A表（UCAの識別用）　　コントロールストラクチャー利用

４．５　手順５　ＵＣＡに対応したＨＣＦの明確化

何が UCA をもたらすかのＨＣＦ（Hazard Causal Factor：ハザード原因要因）をリストアップするのは容易ではない．特に，システムの故障やヒューマンエラー以外にサイバー攻撃などの影響も考慮してリストアップする方法は従来提案されてこなかった．そこで，**図３**の左側に示すような B１表と呼ばれるガイドテンプレートを考案し，関連するコントロールストラクチャーに，図３の右側の B2 表に示すように記入できるようにした．セキュリティに関する脅威の抽出には STRIDE 法[10]を用いてガイドするようにしている．これはシステムの故障やヒューマンエラー以外にサイバー攻撃などの影響も評価に組み込めるものとなっている．この結果 63 個の HCF を抽出した．

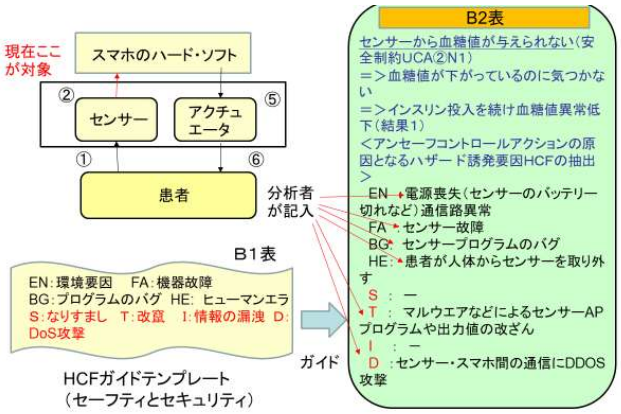

図3　ハザード誘発要因HCFの抽出結果の一例

４．６　手順６　リスクの大きなＨＣＦの明確化

同じ結果をもたらす UCA をリストアップし，その原因となる HCF を対応付けて，**図４**に示すような，EFT を作成する．

この拡張フォルトツリーは一番左側の項目（通常，最上位項目という）を手順２で設定したリスク指標とし，その次の次が同一の結果をもたらす UCA，その右が**図３**のガイドワードで抽出された原因である HCF である．ここでは，システムの故障やヒューマンエラー以外にサイバー攻撃などの影響も含むものとなっている．

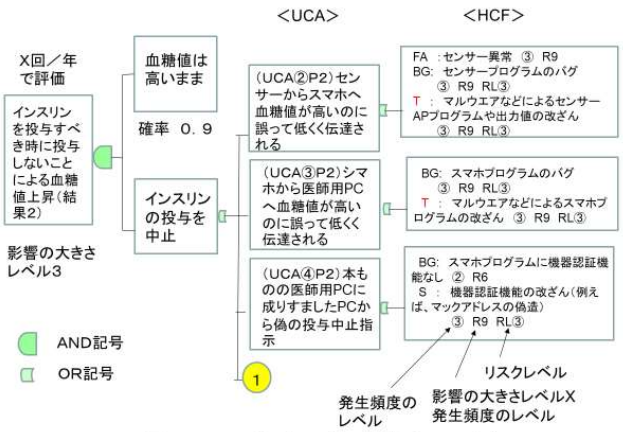

図4　EFT作成の作成結果の一例

それらの HCF の影響の大きさと発生頻度から，**図５**に関するような方法で，それぞれのリスクレベルを求める．このようにして求められたリスクレベルは表２に示すとおりである．

ここでは，リスクレベルが 4 以上のものに対し，対策を検討することとした．

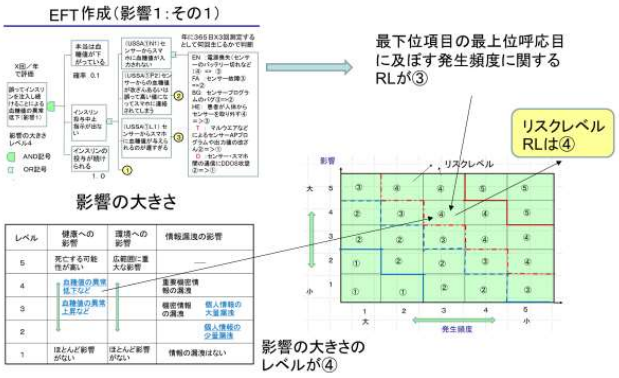

図5　リスクレベルの求め方

表2　各HCFのリスクレベル

影響＼頻度	②	③	④	⑤
④	R8(リスクレベル③) ②N1 BG,T,G ②P1 BG,T ③N1 FA,BG,T,D ③P1 BG,T ④L1 D ④ N1 BG,T ④N2 BG,T ④P1 BG,T ④L1 D ⑤N1 BG,T ⑥N1 BG ⑥P1 BG,T	R12(リスクレベル④) ②N1 EN,FA ②P1 FA ③N1 HE ③N1 HE ④N2 FA ⑤N1 FA ⑥N1 FA,HE	R16 (リスクレベル④) ①N1 HE ⑥N1 EN	R16 (リスクレベル⑤) なし
③	R6(リスクレベル②) ④P2 BG ⑤P1 BG S T ⑦L1 BG,S,T	R9(リスクレベル③) ②P2 FA, BG, T ③P2 BG, T ④P2 S ④P3 S ⑥N1 BG, T ⑦L1 EN,FA,D	R12(リスクレベル④) ⑥N1 EN,FA,HE	R15(リスクレベル④) なし
②	R4(リスクレベル②)	R6(リスクレベル②) ②P3 HE, S ③P3 S, T	R8(リスクレベル③) ②P3 I, ③P3 HE,	R10(リスクレベル③) ③P3 I

リスクレベル③以上に対し対策案を考案

表２より，次のようなことがわかる．

（１）リスクレベルが高い HCF は血糖値の異常低の部分に多い

（２）情報漏洩対応の HCF は一般にリスクが少ないが，暗号対策などをやっていないとリスクが大きくなる

（３）ヒューマンエラーや，環境条件でリスクが大きくなることが多い

４．７　手順７対策案最適組み合わせ問題としての定式化

ここまで扱ってきた EFT などでは，準定量的処理であり，復旧を考慮してないリライアビリティを扱っている．一方，RM の効果は，復旧を行うことにより，アベイラビリティを上げることを目指すためであり，しかも，効果を適切に把握するには定量的な扱いが必要である．そこで，EFT でもアベイラビリティ（あるいはアンアベイラビリティ）を扱えるようにするとともに，定量的な扱いを考える．そこで，**図６**に示すような EFT を考え，RM を実施することによるアンアベイラビリティ低減比率 H を導入し，ETF の構造に基づきリスクを計算できるようにした．

H＝１－　（MTBFa/（MTBFa＋MTTRa））　/（MTBFb/（MTBFb＋MTTRb））　　-- (1)

ここで

MTTRb：　対策前平均修復時間（時間）　　24 時間

MTBFb：　対策前平均故障間隔（時間）　　864 時間

（年に 10 回故障が発生と仮定）

MTTRa：　対策後平均修復時間（時間）　2 時間

MTBFa：　対策後平均故障間隔（時間）　864 時間

この時，H=0.915 となる．

また，RM のコストは全体で 1000 万円とし，100 の医院で使い，1 つの医院で 100 人のインスリン注入装置をメンテナンスの対象とすると

一インスリン注入装置当たりのコストは 1000 万円／（100X100）＝1000 円

となる．

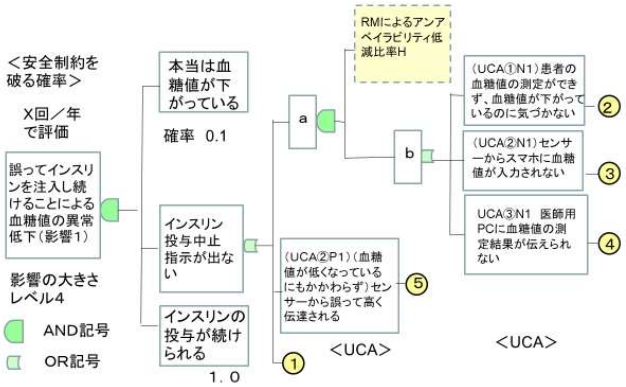

図6　RMの効果を導入したEFT

$$\text{Max} \quad \sum_{i=1}^{3} \Delta R_i \qquad ---(1)$$

$$\text{s.t.} \quad \sum_{i=1}^{3} \sum_{j=1}^{J_i} \sum_{k=1}^{K_j} C_{ijk} \cdot X_{ijk} \leqq CT \qquad ---(2)$$

$$X_{ijk} = 0 \text{ or } 1$$

ΔR1：血糖値が低いときにインスリン投与中止指示が出ないことによる血糖値異常低リスクの低減効果
ΔR2：血糖値が高いときに、インスリン注入指示が出ることによる血糖値異常高リスク低減効果
ΔR3：情報漏洩リスク低減効果
Cijk：指標iに及ぼすj番目のUCAiに対するk番目の対策案のコスト(円)
CT：対策コストの制約(円／年)
Xijl：0-1変数　Xijk=1の時対策案iを採用、Xijl=0なら不採用

図7　定式化結果

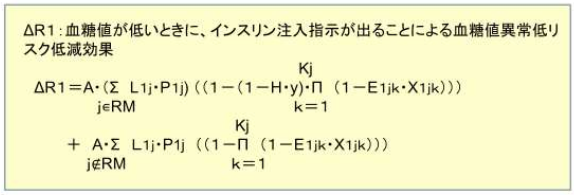

図8 ΔR1の求め方

また，システム全体を対象としたのでは，分析対象が，量的に膨大になる．そこで，全体システムのリスクの最小化を行うのではなく，RM 対策など各種対策候補に関連する部分だけに着目し，対策案のコストとアンアベイラビリティ低減効果などを考慮し，コスト制約下において対策効果を最大化を行うような定式化を行う．

定式化は，ETF の基づき，**図 7** に示すようなものとした．ここで，ΔR_1 は**図 8** に示すように定式化できる．ΔR_2，ΔR_3 も同様にして定式化できる．

４．８ 手順８ リスクの大きなＨＣＦに対応した対策のリストアップ

リスクレベルが４以上の**表 3** の左側の HCF に対し，**表 3** の右側に示すような対策案を考案した．また，それぞれに対策について，リスクの低減効果と対策コストを設定した．

対策案 ijk を，対策案を新たに順序づけし，1 であらわし，**表 3** の右に示すように Z_l としてあらわした(l=1,2,--,9)．

なお，ここでは，RM の実施も 10 番目の対策案とし，Z_{10} を０-１変数とし，RM を実施するなら X_{10}=1，実施しないなら Z_{10}=0 とし，既述したようにリスク低減効果を 0.915，一装置あたりのコストを 1000 円 （1000 万円/（100 医院・100 装置））とした．

なお，ここでは，対策２，3 のように１つの対策で複数の効果があるものも定式化している．

４．９ 手順９ 最適な対策案組み合わせの求解

対策案最適組み合わせ問題の解を求めるため，この問題専用に総当たり法を用いて解を求めるために Python を用いて，プログラム SSFMP を開発した（約 50 ステップ）．制約コストをいろいろ変化させて解を求めた結果は，**表４**に示すとおりである．

その結果次のようなことが言える．

（１）対策に 1000 円以上かけられるなら，RM を導入するほうが良い．

（２）通信路暗号化も重要性が高い．

（３）インスリン注入装置などの装着忘れを防止するための教育などのコスト効果もよい．

表３ リストアップされる HCF と対策案候補

結果	UCA	HCF	発生頻度	対策案	効果	コスト	RM
1	①N1	HE：インスリン注入装置の付け忘れ	④ RL4	X111：スマホ経由のアラート	0.7	500 円（ソフト追加料）	0 Z_1
	②N1	EN：電源喪失	③ RL4	X121:電源バックアップ	0.6	500 円（ハード追加料）	0 Z_2
	②N1	FA：センサー故障	③ RL4	X121：センサーの多重化	0.7	1000 円（ハード追加料）	0 Z_3
	②P1	FA：センサー異常	③ RL4	X131：センサーの多数決化	0.7	1000 円	x Z_4
	④N1	HE：医師の指示ミス	③ RL4	X141:チェック用ソフト	0.7	3000 円（ソフト追加料）	0 Z_5
	④N2	FA:医師用 PC の通算機能喪失	③ RL4	X51:：PC の２重化	0.7	3000 円（1 台 30 万円/100 人）	x Z_6
	⑤N1	FA：センサー異常でアクチュエータに対し注入指示が与えられない	③ RL4	X１61：センサーの２重化（X121 と共通）	ー	ー	x Z_3
2	⑥N1	EN：電源喪失	④ RL4	X211:電源バックアップ（X121 と同じ）	ー	ー	x Z_2
2	⑥N1	FA：アクチュエータ故障	④ RL4	X２２1:アクチュエータの２重化	0.6	5000 円（ハード追加料）	x Z_7
2	⑥N1	HE:患者への機器設置ミス	④ RL4	X231:教育	0.2	100 円（教育用時間 10 分）	x Z_8
3	③P3	I:スマホ－PC 間の通信の不正入手	⑤ RL4	X311:通信路暗号化	0.9	300 円（ソフト追加料）	x Z_9

RL は各 HCF のリスクレベル

表４ 対策案最適組み合わせ

制約条件(円)	最適値(円)	対策コスト(円)	対策案 1	2	3	4	5	6	7	8	9	10	備考
100	17999	100								0			
500	700000	500	0										
1000	1006500	1000										0	
1500	1069500	1400								0	0	0	
2000	1129000	1900	0							0	0	0	
3000	1199000	2900	0				0			0	0	0	

0 印は、採用すべき対策

４．１０ 手順１０ リスクコミュニケーションに基づく採用対策の見直し

今回の分析結果は，技術者が相談して，対策案や，コスト，リスク低減効果などを設定したものであり，今回はリスクコミュニケーションは実施してない．実際に適用しようとすると，関与者が集まって，リスクコミュニケーションを行い，最終的に採用すべき解を求めることとなる．

リスクコミュニケーションの対象者としては，次のよう

な人たちが考えられる．

（ａ）医用機器利用者

（ｂ）患者

（ｃ）リモートメンテナンス業者　他

また，リスクコミュニケーション用に対象者から出る可能性のある意見としては，

（ａ）評価指標の追加（例えば使い勝手）

（ｂ）対策案の追加

（ｃ）採用対策案から使い勝手が悪いものの排除

（ｄ）対策案の効果やコストに関する見積の修正依頼などが考えられる．

5. おわりに

今回，リモートメンテナンスを伴いフィードバックを有する医療用 IoT システムを対象としたリスクアセスメント手法 SSFM と，そのため支援用プログラム SSFMP（SSFM Program）を開発するとともに，インスリン注入システムに適用することにより対策案の最適組み合わせを求めた．その結果，リスクの大きな HCF として次のようなものがあることが分かった．

（１）　リスクレベルが高い HCF は血糖値の異常低の部分に多い．

（２）　情報漏洩対応の HCF は一般にリスクが少ないが，暗号対策などをやっていないとリスクが大きくなる．

（３）　ヒューマンエラーや，環境条件でリスクが大きくなることが多い．

また，対策案の最適組み合わせとしては次のようなことが言える．

（１）対策に 1000 円以上かけられるなら，RM を導入するほうが良い

（２）通信路に対する暗号化も重要性が高い

（３）インスリン注入装置などの装着忘れを防止するための教育などのコスト効果もよい．

今回の適用により，本方式は目的とするアセスメントを実施できることを確認できた．ただ，対象に応じて式の形を決定し，それに応じてプログラムの開発を行っているという問題があるので，プログラム開発経験のない人でも容易に最適化計算ができるように，式の形を容易に入力できる機能などの検討をしていきたいと考えている．

また，今後は，現実のシステムに関し適用し，リスクコミュニケーションなども実施し，合意形成を行いたいと考えられている．

謝辞

本研究は文部科学省の支援による東京電機大学私立大学研究ブランディング事業「グローバル IoT 時代におけるセキュアかつ高度な生体医工学拠点の形成」[12]の一環で実施したものである．本分析を実施するにあたり，柿崎淑郎准教授，稲村勝樹准教授，植野彰規教授，桑名健太准教授，土井根礼音助教をはじめとする本事業の参加メンバーに種々の有効な意見をいただいた．また，メトロポリタン州立大学の Jigang Liu 教授には研究の進め方に関する貴重なコメントをいただいた．記して感謝申し上げる．

参考文献

[1]　N. Leveson, “Engineering a Safer World, Systems Thinking Applied to Safety, The MIT Press, 2012

[2] Georgios Kavallieratos, Sokratis Katsikas , Vasileios Gkioulos “Cybersecurity and Safety Co-Engineering of Cyberphysical Systems—A Comprehensive Survey”Future Internet 2020, Vol.12,No.65, pp1-18

[3]　佐々木良一「IoT 時代のセキュリティとフォレンジックの技術課題と対応策」情報処理学会 DICOMO2019

[4]　Tomoko Kaneko , Yuji Takahashi ,Takao Okubo , Ryoichi Sasaki ” Threat analysis using STRIDE with STAMP/STPA” The International Workshop on Evidence-based Security and Privacy in the Wild 2018Nara, Japan

[5]　Takuo Hayakawa, Ryoichi Sasaki, Hiroshi Hayashi,Yuji Takahashi, Tomoko Kaneko, Takao Okubo, “Propoal and application of Security/Safety Evaluation Method for Medical Device System that Includes IoT” 2018 The 3rd International Conference on Network Security (ICNS2018) Taipei, Taiwan

[6]　林 浩史，髙橋 雄志，金子 朋子，早川 拓郎，佐々木良一「IoT システム向けリスク評価方式と支援ツール SS-Rat の開発」情報処理学会第 106 回 GN・第 24 回 CDS・第 21 回 DCC 合同研究発表会

[7]　永井康彦，福澤寧子：「STAMP/STPA 手法に基づく安全・セキュリティハザード統合分析方式の提案」，電子情報通信学会 SCIS2019, 2C3-1.

[8]　佐々木良一「メンテナビリティ・セーフティ・セキュリティを考慮した IoT システム向けリスク評価手法の開発」情報処理学会論文誌 2020 年 5 月号掲載予定

[9]　情報処理推進機構　「医療機器における情報セキュリティに関する調査」 2014 年，https://www.ipa.go.jp/files/000038223.pdf

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

[11]　東京電機大学研究ブランディング事業「グローバル IoT 時代におけるセキュアかつ高度な生体医工学拠点の形成」 https://www.dendai.ac.jp/about/tdu/activities/branding/