

IoT 時代のリスクコミュニケーション支援ツールの構想

佐々木良一[†]

サイバー攻撃が激化する中、どのような対策をどこまで実施すべきかを決定するのは簡単ではなく、どの程度のリスクがあるかのリスク分析や、どのぐらい安全にすべきかにかかわる組織としてのリスクコミュニケーションが必要になってくる。このような問題に対処するため報告者は早い段階から多重リスクコミュニケーター MRC (Multiple Risk Communicator) の開発と適用を実施してきた。しかし、IoT 時代を迎え、①セキュリティとセーフティの両方を考える必要があるとか、②制御システムのように多重のフィードバックを含むシステムを扱う必要がある、③影響の定量化が困難であるなどの理由により従来の方ではうまくいかなくなってきている。そこで、IoT 時代に適した広義のリスクコミュニケーションの手順を開発するとともに、それを支援するためのツールである MRC4IoT (MRC for IoT) の開発構想を固めた。本稿ではこの手順と開発構想を中心に報告する。

Development Concept of Risk Communication Support Tool in IoT Era

RYOICHI SASAKI[†]

1. はじめに

サイバー攻撃が激化する中、セキュリティ対策を実施するのは企業などの組織において常識になってきている。しかし、どのような対策をどこまで実施すべきかを決定するのは簡単ではなく、どの程度のリスクがあるかのリスク分析や、どのぐらい安全にすべきかにかかわる組織としてのリスクコミュニケーションが必要になってくる。このような問題に対処するため報告者は早い段階から多重リスクコミュニケーター MRC (Multiple Risk Communicator) の開発と適用を実施してきた[1]-[13]。

しかし、IoT 時代を迎え、①セキュリティとセーフティの両方を考える必要があるとか、②制御システムのように多重のフィードバックを含むシステムを扱う必要がある、③影響の定量化が困難であるなどの理由により従来の方ではうまくいかなくなってきている。そこで、IoT 時代に適したリスク分析やリスクコミュニケーションの手順を開発するとともに、それを支援するためのツールである MRC4IoT (MRC for IoT) の開発構想を固めた。

本稿では、まず MRC の開発と従来への適用に関する簡単な紹介をする。次に IoT 時代に必要なリスク分析やリスクコミュニケーション手順を示したのち、医療用 IoT システムを例に挙げて具体的にどのように適用するかを示す。最後にそれを支援するためのツールである MRC4IoT の開発構想を示す。

ここで、リスクマネジメントは図1に示すようにリスク

アセスメントとリスクコミュニケーションなどからなる。また、リスクアセスメントはリスクの特定とリスク分析、リスク評価から構成される。なお、本稿ではリスクアセスメントと狭義のリスクコミュニケーションを合わせて広義のリスクコミュニケーションという。

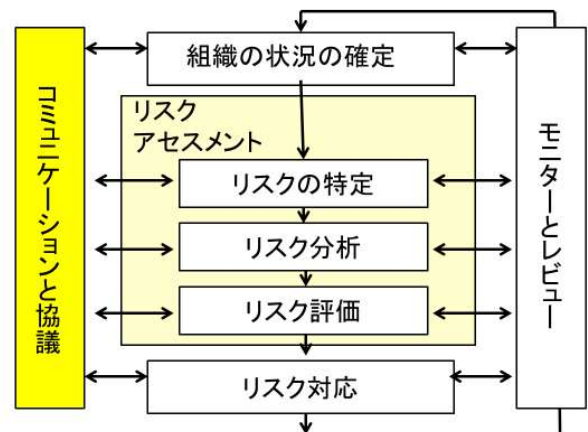


図1 リスクマネジメントのプロセスの流れ

2. 従来の多重リスクコミュニケーター MRC

セキュリティ対策の検討にあたってコストや使い勝手を考慮して対策をどこまで実施すべきかは重要な課題として残されていた。このような問題を解決するために報告者は広義のリスクコミュニケーションを支援する多重リスクコミュニケーター MRC の開発を行ってきた[1][2]。

MRC を開発するにあたっての基本認識は次のとおりで

[†] 1 東京電機大学 Tokyo Denki University

ある（図2参照）。

- (1) 多くのリスク（セキュリティリスク、プライバシーリスク、使い勝手リスクなど）が存在するためリスク間の対立を回避する手段が必要
- (2) ひとつの対策だけでは目的の達成が困難であり対策の最適な組み合わせを求めるシステムが必要
- (3) 多くの関与者（経営者・顧客・従業員など）が存在し、多くの関与者間の合意が得られるコミュニケーション手段が必要

このため次のような機能を持つMRCを開発した。

(a) 多くのリスクやコストを制約条件とし、残存リスク等を最小化する対策組み合わせ問題として定式化し

(b) 関与者の合意が得られるまで制約条件値などの値を変えつつ最適化エンジンを用い求解を行う。

このMRCは（イ）個人情報漏洩対策（含む：世田谷区役所の個人情報漏洩対策への実適用など）[3]や（ロ）内部統制問題[4]などに適用した。その結果、具体的な対策案の組み合わせに関し合意を得ることができ、その有用性を確認することができた。ここでのリスク分析にはフォルトツリー分析法に類似したアタックツリー分析法を用いていた。

その後、適用分野を増やすために次のような機能追加を行ってきた。

- (1) 標的型攻撃等多段にわたる攻撃のリスク分析を容易にするためのイベントツリー分析法とディフェンスツリー分析法を組み合わせるリスク分析法（EDC法）の開発[5]
- (2) 被害発生防止対策と復元対策の両方を考慮したレジリエンス対応機能を持つ対策案最適組合せ法[6]
- (3) 動的リスクを考慮した多重リスクコミュニケーター[7]
- (4) 経営者とのリスクコミュニケーションも考慮した多重リスクコミュニケーター[8]
- (5) 合意形成対象者が1000人を超すような問題へも適用できるリスクコミュニケーション手段[9]-[13]

今回の拡張はIoT（Internet of Things）システムに適した広義のリスクコミュニケーション法に関するものである。

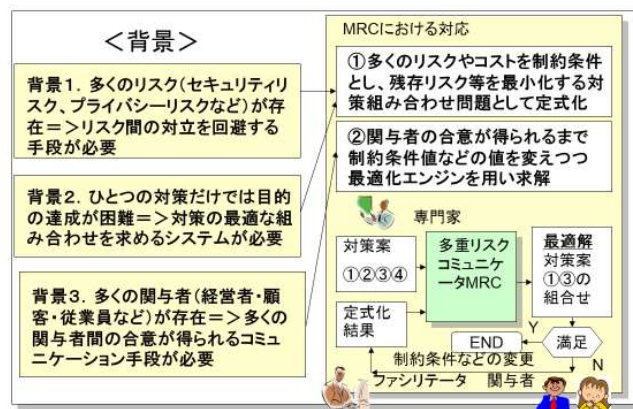


図2 多重リスクコミュニケーター(MRC)の開発

3. IoT時代のリスクコミュニケーション

3. 1 IoTシステムの特徴

現在IoTシステムのセキュリティが重大な問題となっている。この理由は次のように整理することができる。

- ① IoTが急速に普及していくことが予想される。2020年には530億個と総務省によって予測されている。
- ② IoTの機能喪失の影響が大きく、自動車事故のように人命が失われる場合もある。
- ③ 思いかけない接続によって予想しないリスクの発生も生じうる。
- ④ IoTシステムが被害にあうだけではなく、IoT装置が踏み台になった攻撃の可能性も大きい。
- ⑤ 現状のシステムでは性能の制約や自動アップグレードの困難性等の制約があり一般に対策が困難である。

ここで、一口でIoTといっても、センサーのような部品レベルから重要インフラの制御装置のように大規模なシステムレベルまでいろいろなものがあり、どのレベルのIoTについて議論しているのか確認しておく必要がある。すでに、総務省と経済産業省が協力して平成28年7月に「IoTセキュリティガイドライン」を制定し5つの指針・21の要点を明らかにしている[14]。しかし、これはIoT全般に対するものであり、セキュリティ対策などを明確にするためには、個別のリスク分析やリスクコミュニケーションが必要になる。

通常のITのリスク評価の用いられる指標は、コンピュータソフトのもたらす次の3つのセキュリティ指標である。

- ① 機密性の喪失（情報の漏えいなど）
- ⑥ 完全性の喪失（データの改ざんなど）
- ⑦ 可用性の喪失（システムダウンなど）

一方、IoTシステムの指標は図3に示すように、IoTシステムの主要な要素である制御対象のセーフティ指標と従来のセキュリティ指標を考慮する必要がある。

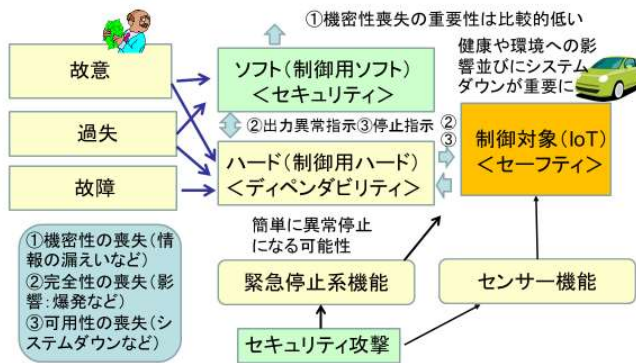


図3 IoTのリスク評価指標

3.2 IoT システムのリスクコミュニケーション手順の提案

IoT システムのリスク分析やリスクコミュニケーションを実施する上で必要な要件は以下のとおりであると考えられる。

(要件1) セーフティとセキュリティ両方のリスク指標が扱える。

(要件2) 多重のフォードバックを含む制御機能のリスク分析が可能である。

(要件3) 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む。

(要件4) 死亡者など生命の価値が評価指標になるが、金銭などに換算するのがむづかしいので準定量的な評価を前提とする。

これらの要件を満足するために開発予定の広義のリスクコミュニケーション手順は以下のとおりである。

- ② 事前準備：前提条件の整理
- ② 準備1：対象アクシデント・インシデントとその評価指標の明確化
- ③ 準備2：コントロールストラクチャーの構築
- ④ STAMP/STPA Step1 と同様な作業：USSA（非安全動作・非セキュア攻撃）の明確化
- ⑤ USSA 発生原因や攻撃手段の分析：USSA のコントロールストラクチャーへの書き込み
- ⑥ 追加分析作業：対象アクシデント・インシデント別フォルト・アンド・アタックツリー（FAAT）の完成
- ⑦ 対策の立案：フォルト・アンド・アタックツリー（FAAT）の最下位項目に対応した対策のリストアップ
- ⑧ 対策組み合わせの決定：採用すべき対策組み合わせに関する準定量的分析と合意形成

ここで、(要件2)の多重のフォードバックを含む制御機能のリスク分析を可能とするために、MITのナンシーレブゾンらが提案するSTAMP/STPA手法を用いている(図5[15]参照)。STAMP/STPA手法は優れた方法であるが、サイバー

攻撃の影響など従来セキュリティの分野で扱っていた脅威は扱ってこなかった。

■ STAMP/STPA

システムアプローチに基づく新たな安全解析手法

- STAMP (Systems-Theoretic Accident Model and Process) : システム理論に基づく事故モデル
- STPA (STAMP based Process Analysis) : STAMPに基づく安全解析手法

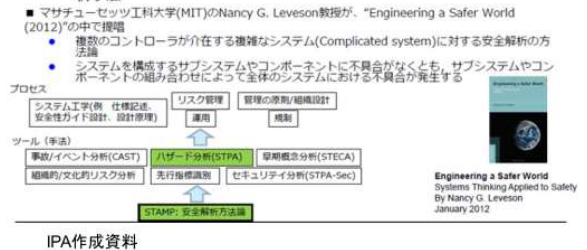


図4 STAMP/STPAの概要

3.3 広義のリスクコミュニケーション手順の例示

ここでは、図5に示すようなインシュリン注入を目的とした医療用IoTシステム(文献[16]を参考にして作成)を想定して手順の説明を行う。

- ① 事前準備：対象となるシステムの構成や機能などを明確化する。図5のようなものを作成するようなことを含む。現実のシステムは病院側からインシュリンの注入を指令するのではなく、患者が自分でインシュリンの注入を行うようであるが、ここでは適度の分析の複雑さを確保するため図5のような機能とした。
- ② 準備1：対象アクシデント・インシデントとその評価指標の明確化：一般には(1)生命や環境にかかわるアクシデント、(2)対象システムの異常停止、(3)重要情報の流出など影響の大きなアクシデントやインシデントを対象とすることとした。(1)(2)が従来セーフティの分野で扱われ、(3)はセキュリティの分野で扱われていたものである。この例では、(a)インシュリンを注入すべき時に注入しないことによる血糖値の上昇による健康障害、(b)インシュリンが必要以上に投与され健康障害(血糖値の異常低下など)、(c)医療ログデータの流出の3つとした。これは、セーフティとセキュリティ両方のリスク指標が扱えるという(要件1)を満足するものとなっている。
- ③ 準備2：図5の対象を分析しコントロールストラクチャーを図6のように想定した。
- ④ STAMP/STPA Step1 と同様な作業：図6の①ー⑦に示したすべての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USSA(Unsafe and Unsecure Control Action)を表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アクシデントやインシデント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。

- ⑤ USSA 発生原因の分析：何が USSA をもたらすかの原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 7 に示すようなコントロールワードを考案し、関連するコントロールストラクチャーに、図 8 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[20]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という（要件 3）を満足するものとなっている。
- ⑥ 追加分析作業：同じアクシデント・インシデントをもたらし USSA を表 2 に示すようにリストアップし、それぞれのアクシデント・インシデントに対し、図 9 に示すような、フォルト・アンド・アタックツリー（FAAT）を作成する。この FAAT は一番左側の項目（通常、最上位項目という）を対象アクシデント・インシデントとし、その次が同一の結果をもたらし USSA、その次が図 8 のガイドワードで抽出された原因をベース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含むものとなっている。
- ⑦ 対策の立案：フォルト・アンド・アタックツリー（FAAT）の最下位項目（図 9 では一番右側の項目）に対応した対策のリストアップを行う。その一例を図 10 に示す。このサイバー攻撃などセキュリティ側の対策のリストアップには、米国 NIST の「重要インフラのサイバーセキュリティを向上させるためのフレームワーク」[18]などを参考にすればよい。
- ⑧ 対策組み合わせの決定：採用すべき対策組み合わせに関する準定量的分析と合意形成。ここでは（要件 4）を満足するため次のような準定量的分析を行っている。
 - （a）図 9 のような FAAT の最上位項目の影響の大きさを 5 段階に分ける。ここでは表 3 のようなレベル設定を行った。
 - （b）図 9 のような FAAT の最下位項目の発生確率の大きさを 5 段階に分ける。ここでも CVSS[19]を使う方法などを検討しているが詳細は省略する。
 - （c）得られた影響の大きさの段階と発生確率の大きさの段階から、図 11 のようにしてリスクのレベルを設定する。
 - （d）一方、図 10 に示すような対策案に関し、コスト効果の大きさをランク付けする。
 - （e）リスクの大きさとコスト効果の大きさから、図

12 に示すような形で、対策採用推薦でレベルを決定する。対策推薦度レベルを求めた結果の一例を図 13 に示す。例えば、対策推薦度 3 以上あるいは対策推薦度 4 以上のものの組み合わせを採用することにしておけば、採用すべき対策案を求めることができる。また、各対策のコストを計算しておき、コスト制約に抵触するまで、対策レベル 5 から 4、3、2 の順に対策を選択していてもよい。

（f）関係者に参加してもらい、対策案のリストアップ、影響の大きさ、発生確率、リスクの分類方法、コスト効果の大きさに関し、意見を言ってもらい、そのようにした場合の対策案の組み合わせを示す。これらを繰り返すことにより対策案の組み合わせに関する合意を形成する。数値を色々変えても対策案の組み合わせはあまり変わらないことから予想以上に早く合意形成できることを従来の MRC の適用から経験している。

本稿で記述した手順は、図 5 で示した対象にはうまく適用しうることを確認できた。今後もう少し複雑な対象にも適用していきたいと考えている。

また、ここで述べたリスクコミュニケーション手順を容易に行えるようにするため MRC4IoT を開発する予定である。特に次の部分の支援ができるようにしていきたい。

- （1）手順④の STAMP/STPA Step1 と同様な作業のうち、表 1 のようなものの作成支援
- （2）手順⑤の USSA 発生原因の分析のうちの図 8 のようなものの作成支援
- （3）手順⑥の図 9 のような FAAT 作成支援
- （4）手順⑦の対策候補立案支援
- （5）手順⑧全体の支援

従来の MRC が定量評価を前提にしているのに対し今回の対象は、準定量的なものになっており大幅に変更が必要であるため、最初から作り直すべきだと考えている。MRC4IoT の開発において、広義のリスクコミュニケーションの手順を完全自動化しようとする膨大なものとなるため、実施作業のガイドをするということや、各手順で扱う情報の引継ぎの実現など作業の効率化を中心に支援していきたいと考えている。現状では、Excel をベースにマクロを使って MRC4IoT のプログラムを作成することを考えており、年内の完成を目指している。

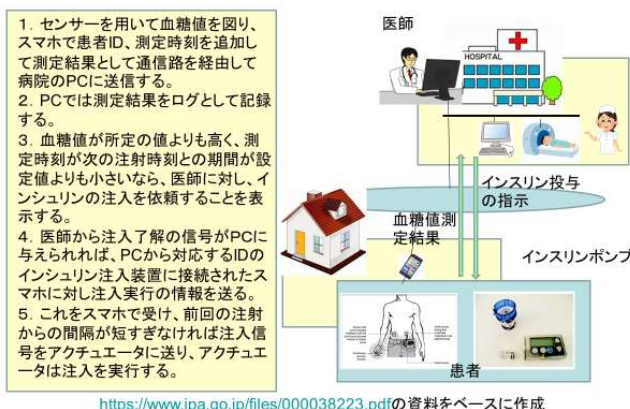


図5 インスリン注射システムの概要

セーフティ向け

- EN: Environmental Effect (環境要因)
- FA: Failure of machine (機器故障)
- BG: Bug of program (プログラムのバグ)
- HE: Human error (ヒューマンエラー)

セキュリティ向け (STRIDE法)

- S: Spoofing (なりすまし)
- T: Tampering (改竄)
- R: Repudiation (否認)
- I: Information disclosure (情報の漏洩)
- D: Denial of service (DoS攻撃)
- E: Elevation of privilege (権限昇格)

RとEは通常使わないのでガイドワード別原因一覧表からは外しておく

図7 セーフティとセキュリティに関するガイドワード

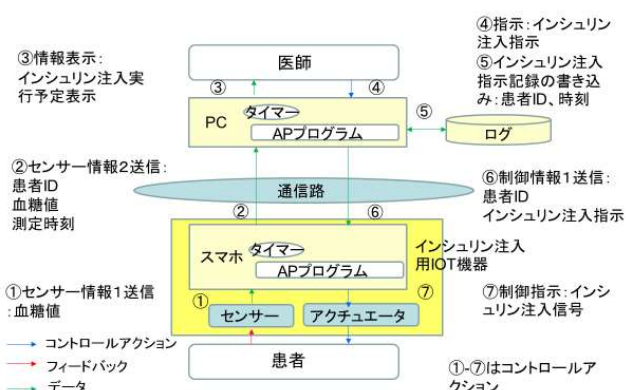


図6 準備2: コントロールストラクチャーの構築

表1 STAMP/STPA Step1同様作業

コントロールアクション	Not Providing	Providing Causes hazard	Too early too late	Too soon too long
①センサー情報1送信: 血糖値	(USSA①N1) センサーから血糖値が与えられない=>血糖値上昇	(USSA①P1) 血糖値を間違えて低くしたり高く改ざんする=>血糖値上昇 (USSA①P2) 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	(USSA①L1) センサーから血糖値が与えられるのが遅すぎる=>血糖値上昇	—
特徴: どのアクシデント・インシデントにつながるか表示しておく				

USSA: Unsafe and Unsecure Control Action (STPAではUCAと呼んでいたもの)
① - ⑦について同様に作成

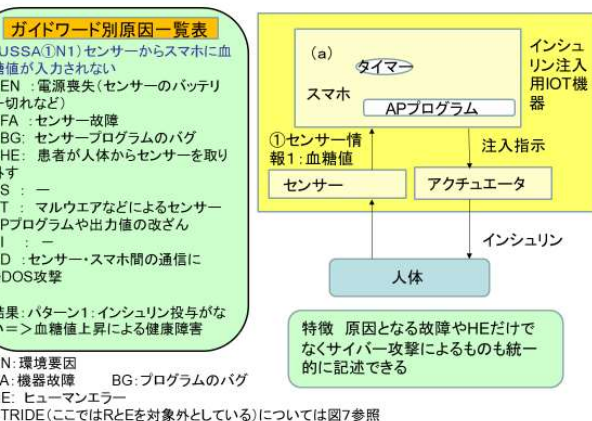


図8 USSA発生原因の分析

表2 アクシデントパターン別原因事象

アクシデント・インシデント	原因事象	備考
1	インシュリンが過剰に投与され健康障害(血糖値の異常低下など)	①P2, ②P3, ⑥P2, ⑥P3, ⑦P1
2	インシュリンを注入すべき時に注入しない(血糖値の上昇など)	①N1, ①P1, ①L1, ②N1, ②P2, ②P4, ②L1, ③N1, ③P1, ③L1, ③S1, ④N1, ④P1, ④L1, ⑥P1, ⑥L1, ⑦N1, ⑦P2
3	医療ログ情報の流出	⑤P1

アクシデント・インシデント別のFAAT (Fault and Attack Tree) の作成が容易となる

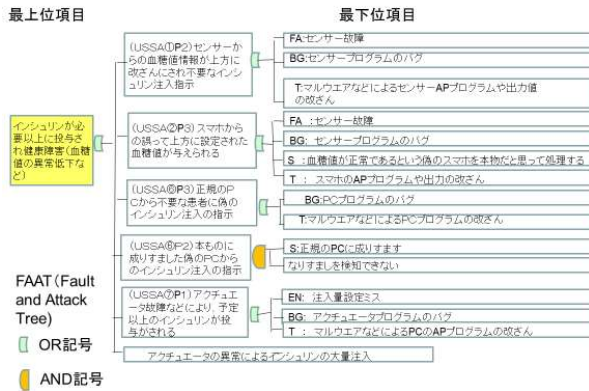


図9 FAAT作成結果の一例

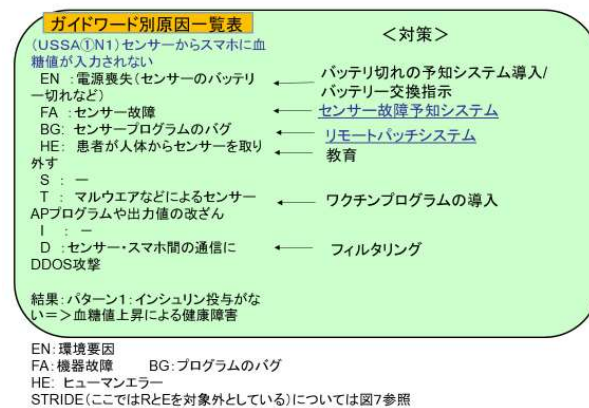


図10 対策案の例

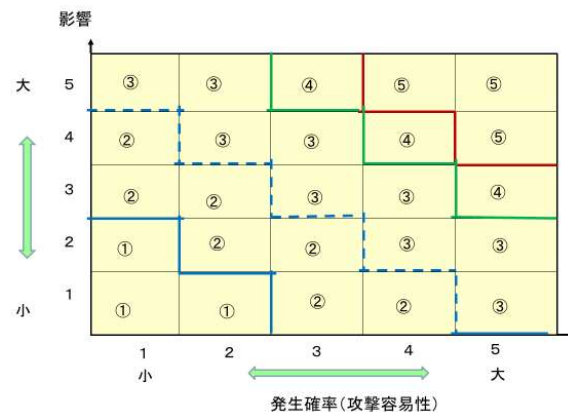


図11 リスクの大きさのレベル付け案

表3 影響の大きさ

レベル	健康への影響	環境への影響	情報漏洩の影響
5	死亡する可能性が高い	広範囲に重大な影響	—
4	(血糖値の異常低下など)	↑	重要機密情報の漏洩
3	(血糖値の異常上昇など)	↑	機密情報の漏洩 個人情報の大量漏洩
2	↑	↑	個人情報の少量漏洩
1	ほとんど影響がない	ほとんど影響がない	情報の漏洩はない

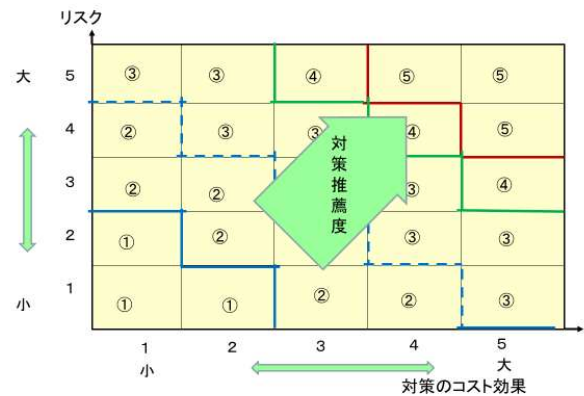


図12 リスクと対策効果の2次元図

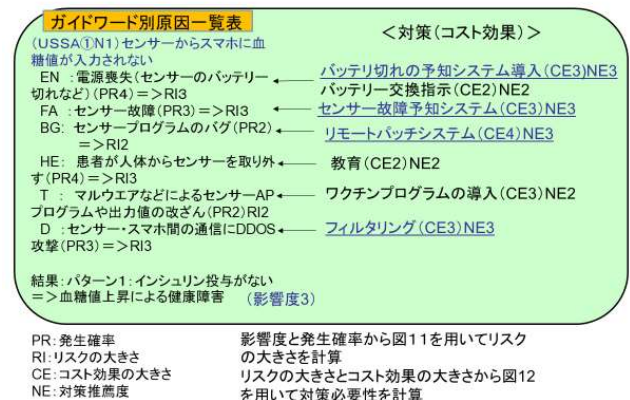


図13 対策推奨度の分析の例

4. おわりに

報告者らが開発したIoT時代に必要な広義のリスクコミュニケーション手順を医療用IoTシステムを例に挙げて具体的にどのように適用するかを説明した。あわせてそれを支援するためのツールであるMRC4IoTの開発構想を示した。

今後は、ほかの例にも適用することによって手順を見直したうえで、MRC4IoTの開発を進めていきたいと考えている。

謝辞

本研究を実施する上で、IoT のリスク分析の方法に関する有益な示唆を与えてくれた情報セキュリティ大学院大学の久保隆夫教授、IPA の金子朋子氏、東京電機大学の猪俣敦夫教授、高橋雄志氏、早川拓郎氏に深く感謝申し上げます。本研究は文献[17]の研究を協力して実施する中から、広義のリスクコミュニケーションの観点から発展させたものである。

参考文献

- 1) 佐々木良一, 日高悠, 守谷隆史, 谷山充洋, 矢島敬士, 八重樫清美, 川島泰正, 吉浦裕 「多重リスクコミュニケーターの開発と適用」, 情報処理学会論文誌, Vol. 49, No. 9, pp. 3180-3190, 2008
- 2) Ryoichi Sasaki, “Consideration on Risk Communication for IT Systems and Development of Support Systems” Journal of Information Processing, Vo.20 (2012) -4, pp814-822 <https://www.jstage.jst.go.jp/browse/ipsjip/>
- 3) 谷山充洋, 日高悠, 荒井正人, 甲斐 賢, 伊川宏美, 矢島敬士, 佐々木良一「多重リスクコミュニケーターの企業向け個人情報漏洩問題への適用」日本セキュリティ・マネジメント学会誌, Vol. 23, No. 2, pp34-51, 2007
- 4) 守谷隆史, 千葉寛之, 佐々木良一 「内部統制のための多リスク・多関与者を考慮した費用対効果の評価法の提案と適用」, 日本セキュリティ・マネジメント学会学会誌, 第 22 巻第 3 号, pp. 3-14, 2008
- 5) 相原遼, 石井亮平, 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, No. 3, pp1082-1094, 2017
- 6) Ichiro Matsunaga, Ryoichi Sasaki, ” Development and Evaluation of a Continuity Operation Plan Support System for an Information Technology System” International Journal of Cyber-Security and Digital Forensics (IJCSDF) 4(2): 327-338, 2015
- 7) 梅原悠平, 安藤駿, 佐々木良一「IT リスクの動的特性を考慮した対策案組み合わせ最適化技術の提案と評価」日本セキュリティ・マネジメント学会誌, 30 巻第 3 号 2017 年 3 月 pp11-21
- 8) Shota Fukushima and Ryoichi Sasaki, “Proposal and Evaluation of Method for Establishing Consensus on Combination of Measures Based on Cybersecurity Framework”, International Journal of Cyber-Security and Digital Forensics (IJCSDF) 5(3): 155-165, 2016
- 9) 佐々木良一, 杉本尚子, 矢島敬士, 増田英孝, 吉浦 裕, 鮫島正樹, 船橋誠壽「ITリスク対策に関する社会的合意形成支援システム Social-MRC の開発構想」情報処理学会論文誌 Vol. 52, No. 9, pp 2562-2574, 2011
- 10) Ryoichi Sasaki, Shoko Sugimoto, Hiroshi Yajima, Hidetaka Masuda ,Hiroshi Yoshiura, Masaki Samejima” Proposal for Social-MRC: Social Consensus Formation Support System Concerning IT Risk Countermeasures” International Journal of Information Processing and Management Vol.2, No.2 pp48-58, 2011
- 11) 大河原優, 高草木一成, 矢島敬士, 増田英孝, 小林哲郎, 佐々木良一「IT リスク対策に関する社会的合意形成支援システム Social-MRC の情報フィルタリング問題への試適用と考察」日本セキュリティマネジメント学会誌 25 巻第 3 号 pp15-23, 2012
- 12) 安藤駿, 猪瀬裕介, 増田英孝, 佐々木良一「マイクロブログ中のリスクコミュニケーションに関する有益な意見を自動的に抽出する手法の提案と評価」情報処理学会論文誌, Vol. 55, No. 9, pp2149-2158, 2014
- 13) Masaki Samejima, Ryoichi Sasaki, ” Chance-Constrained Programming Method of IT Risk Countermeasures for Social Consensus Making” IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS: SYSTEMS, VOL. 45, NO. 5, MAY 2015 pp725-733
- 14) 「IoT セキュリティガイドライン v.1.0」IoT 推進コンソーシアム, 総務省, 経済産業省 2016 年 7 月 http://www.soumu.go.jp/main_content/000428393.pdf
- 15) 例えば「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～」2016 <https://www.ipa.go.jp/sec/reports/20160428.html>
- 16) 「医療機器における情報セキュリティに関する調査」2014 IPA <https://www.ipa.go.jp/files/000038223.pdf>
- 17) 早川 拓郎, 佐々木 良一, 金子 朋子, 高橋 雄志, 久保隆夫, 猪俣敦夫「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」情報処理学会 DICO02018
- 18) 米国国立標準技術研究所 (IPA 翻訳)「重要インフラのサイバーセキュリティを向上させるためのフレームワーク」2014 年 2 月 <https://www.ipa.go.jp/files/000038957.pdf>
- 19) IPA 「共通脆弱性評価システム CVSS 概説」<https://www.ipa.go.jp/security/vuln/CVSS.html>
- 20) 久保隆夫「脅威分析法 組み込みの安全性とセキュリティを保証するために」2015 <https://www.ipa.go.jp/files/000046476.pdf>