情報処理学会論文誌 Vol.61 No.5 1096–1103 (May 2020)

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

佐々木 良一[1,a)]

受付日 2019年8月30日, 採録日 2020年2月4日

概要：IoTシステムのリスク評価は，セキュリティだけでなく，セーフティも含めて評価する必要があるといわれてきており，報告者らもセキュリティとセーフティを両方考慮したリスク評価手法を開発してきた．最近ではさらにリモートメンテナンスが取り入れられつつありメインテナビリティ（M）とセーフティ（S），セキュリティ（S）を良いバランスで対象システム上に実現していくことが重要になってくる．著者らはこれをMSSコンセプトと名付け，このコンセプトを実現するためのリスク評価の方法と対策案の最適な組合せを求める方式の開発を行ってきた．今回，これを可能とする方式を初めて実現するとともに対応するプログラムを開発した．また，これを医療用の敷布型マルチバイタルIoTモニタシステムに適用した結果，リモートメンテナンスを導入する際に，情報漏洩対策を同時に実施しないと全体のリスクが増大することを明確にした．また，対策コストの種々の制約条件下で，「対策のメリット＋ディメリットの減少値」を最大化する対策案の最適な組合せを具体的に求めることができ，それらの対策の組合せを用いると比較的安いコストでメリットの方が大きくなることを明らかにした．これにより，医療用IoTシステムに対しては，MSSコンセプトに基づく対策案の最適な組合せを求めることが可能である見通しを得た．

キーワード：IoT，セキュリティ，セーフティ，メンテナビリティ，リスク評価

Development of Risk Assessment Method Considering Maintainability, Safety and Security for IoT Systems

Ryoichi Sasaki[1,a)]

Received: August 30, 2019, Accepted: February 4, 2020

Abstract: It has been said that the risk assessment of IoT systems needs to be assessed not only for security but also for safety. Therefore, the author has developed risk assessment methods that consider both security and safety. Recently, remote maintenance is being introduced into IoT systems, and it is important to realize maintainability, safety, and security on the target system in a good balance. The author named this MSS concept, and has developed a risk assessment method and a method for finding the optimal combination of countermeasures to realize this concept. This time, for the first time, we have realized a method that makes this possible and developed a corresponding program. As a result of applying this to a medical-use multi-vital IoT monitor system, it has been clarified that the overall risk will increase if information leakage measures are not performed at the same time when remote maintenance was introduced. In addition, under various constraint conditions of countermeasure costs, it is possible to specifically find the optimal combination of countermeasure proposals that maximizes “the merit of countermeasures + the reduced value of demerits”. It was clarified that the merit becomes larger at a relatively low cost. As a result, for medical IoT systems, it was possible to find the optimal combination of countermeasures based on the MSS concept.

Keywords: IoT, security, safety, maintainability, risk assessment

1. はじめに

自動車や家電品，医療用機器など従来ネットワークにつ

[1] 東京電機大学
Tokyo Denki University, Adachi, Tokyo 120–8551, Japan
[a)] r.sasaki@mail.dendai.ac.jp

ながっていなかったいろいろな「もの」がインターネットにつながる IoT（Internet of Things）時代が到来しつつある．IoT 時代のリスク評価は，次の理由によって従来の方法の適用では困難である．

① 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を扱う必要があり，従来のアタックツリーのようなものだけではモデル化が困難である．

② サイバー攻撃の増加による IoT 機器のセキュリティ低下が原因となり，人命などのセーフティへの影響が生じる可能性が増大する．

① の問題に対応するために，MIT のナンシー・レブソンによって STAMP/STPA [1] が提案されており，目的の達成のために適切な方法であるといってよい．しかしこの方法は，機器故障やヒューマンエラーによるセーフティへの影響を考慮するだけで，サイバー攻撃のようにセキュリティに関連する事象が原因となりセーフティへ影響を扱うものではなかった．すなわち，② の問題には適用できなかった．

そこで，著者らは，① の問題とともに ② のような問題を解決するための基本的アプローチ方式 [2] を確立するとともに，準定量的な評価に基づき対策案の組合せを求める方式 [3] およびその支援ツール [4] を開発してきた．あわせてこの定量的評価法とそれに基づき対策案の最適な組み合わせる方法 [5] についても開発してきた．

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．RM を導入すると対象とする監視が強化されるので IoT 機器のアンアベイラビリティが下がり，人命などのセーフティが向上する．一方，RM により情報がネットワーク経由で外部に送られるので，そのままでは不正侵入の確率が向上し，個人情報漏洩などのセキュリティの低下が予想される．また，不正侵入後，対象とする IoT 機器に対する攻撃が発生し，セーフティが低減する可能性がある（図 1 参照）．

このため，従来，著者らが扱ってきたセーフティ（Safety）とセキュリティ（Security）の関係に新たに RM のメンテナビリティ（Maintainability）を追加し，3 者の相互の関係を定式化し，良いバランスで対象システム上に実現していくことが重要になってくると考えた．著者らはこれを MSS コンセプトと名付け，このコンセプトを実現するためのリスク評価法と対策案の最適な組合せを求める方法の開発を行ってきた [6]．

メンテナビリティとセーフティ，セキュリティの 3 つを考慮した対策方法の研究は少しずつ発表されてきているが

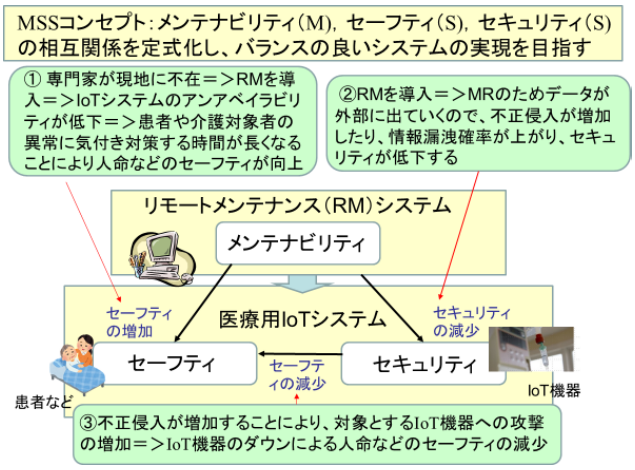

図 1 MSS コンセプトの概要
Fig. 1 Overview of MSS concept.

（たとえば文献 [7], [8]），これらは定性的検討であり，本提案方式のようにアンアベイラビリティを仲介として 3 つの関連を式で結び付け，定量的な評価を行い，さらに最適な対策の組合せを求めるようにする方法についての研究は見当たらない．

本論文では，この方式と医療用 IoT 機器への適用結果を報告する．

2. MSS コンセプトに基づくリスク評価方式の提案

2.1 リモートメンテナンス（RM）の概要

ここで RM とは，インターネットなどのネットワークにつながったサーバやパソコン，IoT 機器などを遠隔地から，監視，保全，異常検知，修復などをすることである．監視によって機器故障などの異常を早期に検知することができる．ハードウェアの保全には時間がくると構成要素を取り換える定期保全と状態の監視によって随時取り換える予防保全などがある．また，ソフトウェアやファームウェアはリモートでの修復が可能であるが，ハードウェアは困難である．

なお，医療用機器のソフトウェアを，ダウンロードなどにより製品出荷後に無認可で変えるのは，医薬品医療機器法に抵触する可能性があるので慎重でなければならないといわれている．

2.2 方式の概要

IoT 機器は，広域に分散することが多いため，RM 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，先にも記述したように，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．

しかし，RM の導入にともない，機器故障の検知までの時間を短縮し患者や被介護者が異常状態にあることを気づかない確率を小さくするというセーフティ上の効果がある

一方，ネットワーク上を情報が流れることによる情報漏洩などセキュリティ上の悪影響も予想される．また，不正侵入後，対象とするIoT機器に対する攻撃が発生し，結果として生命などのセーフティが低減する可能性がある．したがって，果たしてRM機能を導入すべきか，導入するとしたら，どこまでの情報漏洩対策をすべきかを明確にしておく必要がある．

本節ではそのための評価方法の概要（図2参照）について説明する．

＜フェーズ1＞リモートメンテナンス導入によるメリットとディメリットの明確化

メリットとしては，① アンアベイラビリティの低減による効果（E）と ② 波及効果（Eh）が考えられる．医療用IoT機器などのアンアベイラビリティを低減することにより，患者や被介護者の状態の検知確率が増大し，患者の安全の向上に役立つ．なお，RMの実施が原因となって，不正侵入があり，IoT機器に対し攻撃を仕掛けることにより，その機器のアンアベイラビリティが上がることもある．これはディメリットであるが，アンアベイラビリティの計算は，後述する式(6)を用いて，メリット，ディメリットの両方の要因を一緒に考慮できるようにしている．そしてメリットの方が一般に多いと考えられるので，ここでは両方合わせて計算した結果をメリット（E）として扱うこととした．

一方，ディメリットとしては，① リモートメンテナンス業の保守者による情報の不正使用，② 保守者に成りすましての情報入手，③ 通信路上からの侵入による情報漏洩などのセキュリティ上のリスク（L）とリモートメンテナンスの実施のためのコスト（Cr）がある．

これらの，メリットやディメリットの計算においては比較を容易にするために，リスクベースで統一的に扱い，単位はできるだけ円であらわすようにする．

＜フェーズ2＞最適な対策案の組合せの選出

メリットとディメリットを比べディメリットの方が大きい場合には，ディメリットとして生じたセキュリティ上の問題に対する対策案をリストアップし，対策コストなどを制約条件とし，「メリット＋ディメリット低減分」を最大化する対策案の組合せを求める．

この方式は，メンテナビリティとセーフティ，セキュリティの関連を考慮したものであり，1章で述べたMSSコンセプトを実現するものとなっている．

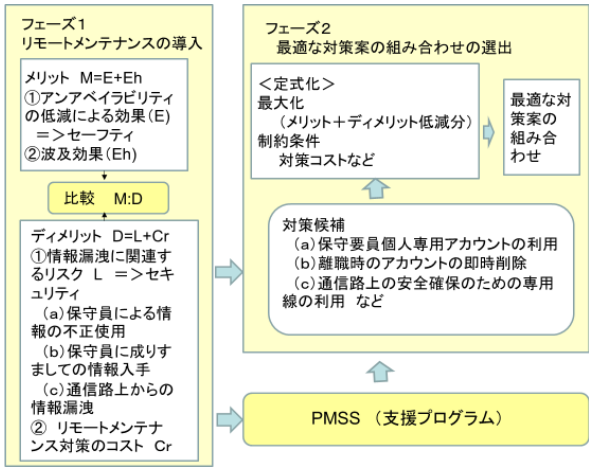

図2 提案手法の概要

Fig. 2 Overview of proposed method.

3. 医療用IoTシステムへの適用

3.1 対象システムの概要

ここで対象とするIoT機器は，本学の植野彰規教授が開発中の図3に示すような敷布型マルチバイタルIoTモニタである[9]．これは，敷布の下にセンサを設置し，心電図や，離床着床の状態，呼吸の状態，血圧などを測定することによって，病院の患者や，介護施設の被介護者の健康状態を監視できるようにするものである．ここではこのIoT機器を含むシステムを介護施設で使うとした場合を対象として手法を適用した．その処理フローは以下のとおりである（図4参照）．

① 敷布型マルチバイタルIoTシステムのセンサで被介護者の心電図信号や血圧，呼吸の状態，離床着床の状態などを測定し，機器IDとともに，無線LANなどを用

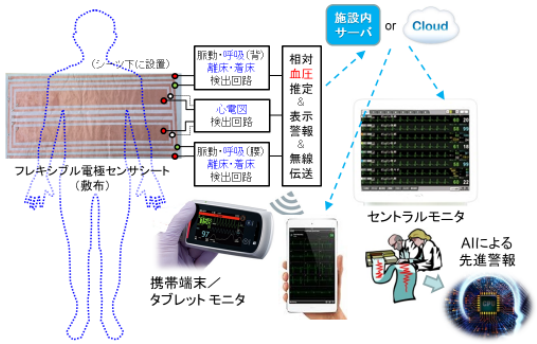

図3 敷布型マルチバイタルIoTモニタ

Fig. 3 Under sheet multi-vital IoT monitor.

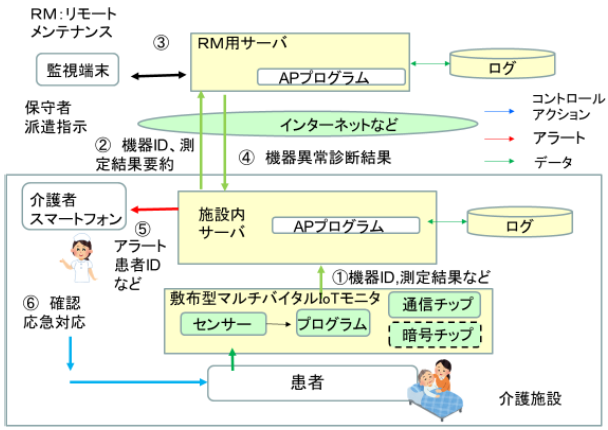

図4 RM対策後のシステムの構造

Fig. 4 System structure after RM.

いて施設内サーバに送信する．

② 施設内サーバでは，測定結果を要約したものを，機器 ID とともに，RM サーバに送信する．

③ RM サーバでは，敷布型マルチバイタル IoT システムのセンサからアライブ信号がこないような場合や，体温が 70 度 C というようにありえない値を示す場合にはセンサ故障と判断し，保守者にアラートを上げる．また，施設内サーバにどの IoT 機器がどんな異常状態かの情報を送る．

④ 施設内サーバでは被介護者のバイタルデータの測定結果や RM サーバからインターネット経由で送られてきたセンサ故障の診断結果に基づき，被介護者に異常があるかどう判断する．

⑤ 施設内サーバでは，IoT 機器故障でなく被介護者に異常があると判断すると，対応する介護者のスマートフォンに，機器 ID と対応する部屋 No，被介護者 ID，異常の種類などを含むアラートを，無線 LAN などを用いて送信する．

⑥ 介護者は被介護者異常のアラートがくると，被介護者の所に駆けつけ対処を行う．

3.2 フェーズ 1 の定式化

RM を導入することによりアンアベイラビリティが変化すると考えられる．この変化には，アンアベリラビリティを減らし患者などのセーフティを増大する要因と，アンアベリラビリティを増加させ患者などのセーフティを増加する要因がある．前者は，患者の状態の監視が行き届くことによって生じ，後者は，RM を導入することによって，ネットワーク経由での不正侵入が増え，IoT 機器を故障させることによって生じる．これらの影響は次のようにして計算することができる．

＜メリット＞

RM 導入によるメリットは次のように定式化することができる．

$$\mathrm{M} = \mathrm{E} + \mathrm{Eh} \tag{1}$$

ここで

E：RM を導入することによるアンアベイラビリティ低減によるメリット

Eh：RM を導入することによる派生的効果．たとえば，人件費の減少などが考えられる．

アンアベイラビリティに注目したのは，その低減がリモートメンテナンスの本来の目的とするものであるからである．

故障率が λ，修復率が μ，とすると運用開始後 t 時間におけるアンアベイラビリティは文献 [10] の式 4.90 より

$$\mathrm{U}(t) = \frac{\lambda}{\lambda+\mu}\left(1 - \mathrm{e}^{-(\lambda+\mu)t}\right) \tag{2}$$

で求めることができる．$t = \infty$ では，

$$\mathrm{U}(\infty) = \lambda/(\lambda+\mu) \tag{3}$$

ここで，

$$\lambda = 1/\mathrm{MTTF}, \quad \mu = 1/\mathrm{MTTR} \tag{4}$$

であるので次式が成立する．

$$\mathrm{U}(\infty) = \mathrm{MTTR}/(\mathrm{MTTF} + \mathrm{MTTR}) \tag{5}$$

MTTF：平均故障時間（時間）

MTTR：平均修復時間（時間）

このとき RM を導入することによるアンアベイラビリティの変化 ΔU は次式で計算できる．

$$\begin{aligned}\Delta\mathrm{U} = {} & (\mathrm{MTTRb}/(\mathrm{MTTFb} + \mathrm{MTTRb})) \\ & - (\mathrm{MTTRa}/(\mathrm{MTTFa} + \mathrm{MTTRa}))\end{aligned} \tag{6}$$

MTTRb：対策前平均修復時間（時間）

MTTFb：対策前平均故障時間（時間）

MTTRa：対策後平均修復時間（時間）

MTTFa：対策後平均故障時間（時間）

ここで，

$$\mathrm{MTTRa} = \mathrm{MTTRb} - \Delta\mathrm{T} \tag{7}$$

ΔT：RM 対策を実施した場合に短縮した機器の修復時間（時間）

修復のためには，リモートからの故障発見を行い，そののち，修理する．ここでは，敷布型マルチバイタル IoT モニタという，ハードを対象としているので，リモートで修理時間を短縮することはできず，短縮できるのは，故障の発見までの時間だけである．この時間は，機器からのアライブ信号を RM で検知できるようにしておくことで，故障発見までの期間を，大幅に低減できる．

なお，今回対象としたのは医療用 IoT 機器であるので簡単にソフトウェアやファームウェアはリモートで変更できないと考え，これらの RM による変更やそれにともなって起こる可能性のある誤操作のリスクは対象外とした．

次に対策後平均故障時間 MTTFa は，次のようにして求めることができる．

$$\mathrm{MTTFa} = (1/\lambda\mathrm{a}) \tag{8}$$

ここで，λa は，RM 導入後の故障率であり次式で求めることができると考えた．式の後半は不正侵入による IoT 機器の故障率の増加を表している．

$$\lambda\mathrm{a} = \lambda\mathrm{b} + \sum_{k=1}^{K} \mathrm{P}_k \cdot \mathrm{q}_k \cdot (1 - \mathrm{F}_k) \tag{9}$$

λb：RM 導入前の故障率（$\lambda\mathrm{b} = 1/\mathrm{MTTFb}$）

P_k：侵入経路 k からの侵入頻度（回/時間）

q_k：侵入経路 k から侵入し，監視対象となる IoT 機器を故障させる確率

このようにして，アンアベイラビリティの変化値 ΔU が求められるようになると，その価値 E は次のように求めることができる．

$$E = S \cdot \Delta U \tag{10}$$

S：アンアベイラビリティを 1 単位低減することによる価値（円）

以下，具体的な数値の設定を行う．この前提としては，1 つの介護施設を想定し，1 年あたりでコストなどを推定する．これらの値は，つねに不確実性をともなうが，意思決定を行う組織の関与者がリスクコミュニケーションを行い，納得したものを用いることで対応できる．

ここでは，実験的にやっているので，とりあえず 2 人の技術者が相談して値を決め計算を行い，その後，第三者の意見も聞いて数値の修正を行い，解を再度求め議論することとした．

今，式 (6) に関連して IoT 機器が年に 10 回ダウンすると仮定すると $MTTFb = 365 \cdot 24/10 = 876$ 時間平均修復時間 MTTRb は現状で 24 時間とし，故障の発見までの時間と修理に要する時間からなり，故障発見までの時間が現状 3 時間だとするとこれを大幅に低減できるので $\Delta T = 2.9$ 時間とした．

今，式 (9) に関連して攻撃経路として，下記のように ① メンテナンス業の保守者による入手データの不正利用攻撃，② メンテナンス業者に成りすました第三者よる攻撃，③ 第三者による通信路上からの侵入による攻撃．

P_1：メンテナンス業の保守者による不正を意図しての操作頻度

$P_1 = 1$ 回/年 $= 1/365 \times 24$ 回/時間

P_2：メンテナンス業者に成りすましての侵入頻度

$P_2 = 1$ 回/年 $= 1/365 \times 24$ 回/時間

P_3：第三者による通信路上からの侵入頻度（暗号をかけてない前提）

$P_3 = 10$ 回/年 $= 10/365 \times 24$ 回/時間

q_1：保守者が不正侵入して IoT 機器を壊す確率

保守者が不正侵入して IoT 機器をわざわざ壊すことはありえないと考え

$q_1 = 0$

q_2：保守者に成りすまして侵入した後 IoT 機器を壊す確率　$q_2 = 0.1$

q_3：第三者が侵入して IoT 機器を壊す確率

$q_3 = 0.1$

また，F_k はセキュリティ対策を実施することによる経路 k からの侵入頻度低減率であり，対策前は $F_k = 0$ である．なお，対策後は後述の式 (16) で求めることができる．

このとき，式 (6)–(9) ならびに設定した値より，$\Delta U = 0.000627$ であった．

ここで，式 (10) に関連し，S = 5,000 万円とした．これは，

$$S = N \cdot MM \cdot PIK \tag{11}$$

N：施設内の被介護者の数 (50 人)

MM：人命への補償額 (1 億円/人)

PIK：被介護者が，緊急対応が必要な危機状況になる確率（1%/年）

から求めたものである．

この結果，E = 3.1 万円であった．

波及効果 Eh については，いろいろなものが考えられる．ここでは介護者の無駄な作業の低減によるコスト低減を取り上げ今回は Eh = 300 万円とした．RM を導入することにより，IoT 機器異常の発見が容易となる．それにより機器異常に基づく被介護者異常の誤アラートを低減でき介護者の無駄な作業を防止できるからである．この値については，推定が簡単でないのでとりあえずの値を与え後で，関係者の意見を入れ，値を変化させ，影響を検討することとした．

この結果，M = E + Eh = 303.1 万円であった．

＜ディメリット＞

ディメリット D は次のようにして計算できる．

$$D = L + Cr \tag{12}$$

Cr：リモートメンテナンスの対策コスト（円）

ここで，全体で年間 1,000 万円のコストが必要であるとして，1 つの RM システムで 100 の介護施設を対応していると想定し，1 施設あたり 10 万円とした．

L：RM を導入することによる情報漏洩確率増加にともなうリスク（円）

これは前述した 3 つの攻撃経路を想定し次式を用いて計算した．

$$L = L1 + L2 + L3 \tag{13}$$

L1：リモートメンテナンス業の保守者の不正によるリスク

L1 = P1 · Q1 = 100 万円/年

P1：先に説明したとおりでありメンテナンス業の保守者による不正　1 回/年

Q1：1 回あたりの攻撃によるメンテナンス関連情報の漏洩が原因となる介護施設の損害額　100 万円/回

L2：メンテナンス業者に成りすました第三者によるリスク

L2 = P2 · Q2 = 100 万円/年

P2：先に説明したとおりでありメンテナンス業者に成りすました第三者よる攻撃　1 回/年

Q2：1 回あたりの第三者による情報漏洩が原因となる介

$$\text{Maximize} \quad M+\sum_{k=1}^{K} L_k\cdot\left(1-\prod_{j=1}^{J}(1-R_{kj}\cdot Y_{kj})\right)$$

$$\text{Subject to} \quad Cr+\sum_{k=1}^{K}\sum_{j=1}^{J} C_{kj}\cdot Y_{kj} \leqq CT$$

$$Y_{kj} = 0 \text{ or } 1 \quad (k=1, 2,\text{--}K;\ j=1,2,\text{--},J)$$

M：メンテナンスによるメリット M=E+Eh
E=ΔU･S
ΔU：式(6)及びその説明を参照
Eh： 波及効果 （円）
S： 単位アベイラビリティ低減当たりのセーフティ上のメリット(円)
Lk：漏洩源kからの情報漏洩に関する対策前リスク(円)
Rkj：漏洩源kに対するj番目の対策案による漏洩遮減率(無単位)
Ckj：漏洩源kに関するj番目の対策案のコスト(円/年)
CT：対策コストに関する制約値(円/年)
Cr：リモートメンテナンスのコスト(円/年)＝10万円
Ykj 漏洩源kに関するj番目の対策案の採用･不採用を表す0－1変数

図 5 定式化法
Fig. 5 Formulation method.

護施設の損害額 100 万円/回

L3：インターネットにつながることによるタッピング機会の増大が原因となって第三者による情報の盗み出しや情報の改ざんなどの不正リスクが増大

$L3 = P3 \cdot Q3 = 1{,}000$ 万円/年

P3：先に説明したとおりであり第三者による通信路上の攻撃 10 回/年（暗号をかけてない前提）

Q3：1 回あたりの攻撃による情報漏洩などが原因となる介護施設にとっての損害額 100 万円/回

よって $L = 12{,}000$ 円である．

これ以外にディメリットとしてレピュテーションリスクなどもありうるが，状況に大きく依存し，複雑になるので今回は対象外とした．

＜メリットとディメリットの差＞

メリットとディメリットの差を求めると

$$Sa = M - D = 303.1 \text{ 万円} - 1{,}210 \text{ 万円} = -906.9 \text{ 万円}$$

となる．

この結果から分かるように，メリットとディメリットでは，ディメリットが 4 倍ほど大きい．そこで，情報漏洩リスク低減対策の最適な組合せを求めることにした．

3.3 フェーズ 2 の定式化

情報漏洩対策の最適な組合せを求めるため図 5 に示すような組合せ最適化問題として定式化する．

ここで，

M：メンテナンスによるメリット 求め方は 3.2 節で示したとおりである．

L_k：漏洩源 k からの情報漏洩に関する対策前リスク（円）これも求め方は 3.2 節で示したとおりである．

R_{kj}：攻撃経路 k に対する j 番目の対策案による侵入低減率（無単位）．

C_{kj}：攻撃経路 k に関する j 番目の対策案のコスト（円/年）値については表 1 を参照．

表 1 パラメータの値
Table 1 Values of parameters.

漏洩源	対策案	対策案No.	Rkj	Ckj
漏洩源1（保守員）	保守要員個人専用アカウントの利用	11	0.9	5000円
	離職時のアカウントの即時削除	12	0.2	1000円
	アクセスログの収集と確認	13	0.7	20万円
漏洩源2（保守員へのなりすまし）	保守員のパスワードの厳密な管理	21	0.8	1000円
	2要素認証などによる個人認証	22	0.9	5万円
	PCのRMサーバへのなりすまし防止	23	0.8	1万円
漏洩源3（通信路）	専用線の利用	31	0.99	50万円
	RMサーバと施設内サーバ間の暗号化	32	0.95	1万円

CT：対策コストに関する制約値（円/年）ここでは，10 万円，11 万円，12 万円，13 万円と変化させてそれぞれにおける解を求めることにした．

Cr：リモートメンテナンスのコスト（円/年）ここでは 10 万円を採用した．

Y_{kj}：攻撃経路 k に関する j 番目の対策案の採用・不採用を表す 0–1 変数．$Y_{kj} = 1$ のとき対策案 kj を採用．$Y_{kj} = 0$ のとき不採用とする．

なお，ΔL は

$$\Delta L = \sum_{k=1}^{K} L_k \cdot \left(1 - \prod_{j=1}^{J}(1 - R_{kj} \cdot Y_{kj})\right) \tag{14}$$

であり，k については算術和であらわし，j については論理和の値を求める式で定式化している．

また，

$$\Delta C = \sum_{k=1}^{K}\left(\sum_{j=1}^{J} C_{kj} \cdot Y_{kj}\right) \tag{15}$$

とする．この式により，採用するさまざまな対策案のコストの合計が計算することができる．

このとき，式 (9) の直後で述べたセキュリティ対策を実施することによる経路 k からの侵入頻度低減率である F_k は次式で計算することができる．

$$F_k = 1 - \left(\prod_{j=1}^{J}(1 - R_{kj} \cdot Y_{kj})\right) \tag{16}$$

このうち，具体的な対策案候補として採用したのは重要性が高いと考えられる次の 8 つである．

① リモートメンテナンス業者による不正に対する対策
（対策案 11）保守要員個人専用アカウントの利用
（対策案 12）離職時のアカウントの即時削除
（対策案 13）アクセスログの収集と確認

② リモートメンテナンス業者に成りすました第三者による不正に対する対策
（対策案 21）リモートメンテナンス業者に成りすました侵入を防止するため，パスワードの厳密な管理を実施

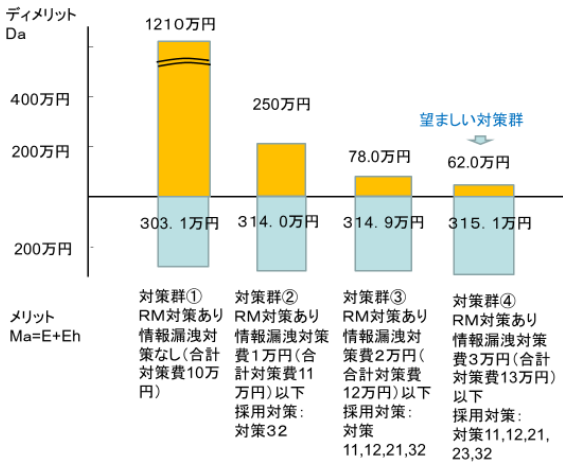

図 6 対策案群の比較

Fig. 6 Comparison of optimal countermeasures.

（対策案 22）リモートメンテナンス業者に成りすました侵入を防止するため，2 要素認証などによる個人認証を実施

（対策案 23）PC の RM サーバへの成りすましを防止するため機器接続の制限

③ 通信路からの侵入に対する対策

（対策案 31）通信路上の安全確保のための専用線の利用

（対策案 32）通信路上の安全確保のための組織内サーバサーバ間の暗号化

それぞれの対策のパラメータ R_{kj} や C_{kj} の値は，大学に属する 2 人の技術者が相談して決定したものであり表 1 に示すとおりである．

本提案方式は，以上述べたようにメンテナビリティ，セーフティ，セキュリティの 3 つの関連をアンアベイラビリティを仲介として式で結び付け，一元的な定量評価を行い，さらに最適な対策の組合せを求めるようになっており従来なかったアプローチである．

3.4 求解結果

この定式化結果から解を求めるため，求解プログラム（PMSS：Program for risk assessment considering Maintainability, Safety and Security）を，Python を用いて開発した．現段階では，総あたり法で最適解を求めるようにしている．

このプログラムを用い，制約条件値を，10 万円，11 万円，12 万円，13 万円と変化させて入力した場合の最適解を求めた．それぞれの条件におけるメリット，ディメリットの差は図 6 に示すとおりである．

なお図 6 で対策後のメリット Ma は

$$\mathrm{Ma} = \mathrm{E} + \mathrm{Eh} \tag{17}$$

対策後のディメリット Da は

$$\mathrm{Da} = (\mathrm{L} - \Delta\mathrm{L}) + \mathrm{Cr} + \Delta\mathrm{C} \tag{18}$$

で示している．

この条件の範囲では制約条件の値を 13 万円と設定した場合が，（メリット − ディメリット）の値が最も大きくなることが分かる．

また，このときに採用すべきとなった対策案は図 6 に示すように対策 11，対策 12，対策 21，23，対策 32 の 5 つである．

この対策案の最適な組合せは，制約条件値を 15 万円まで上げてみても変化がなかった．なお，制約条件値が 11 万円のときの対策案の最適な組合せは，図 6 に示すように対策案 32 のみの場合であり，12 万円のときの最適な組合せは，対策案 11 と対策案 12 と対策案 21 と対策案 32 の組合せの場合であった．

3.5 条件を変えた場合の求解結果

大学に属する技術者 2 名に，新たに企業人 1 名を加えパラメータの値の見直しを行った．その結果，式 (7) の PIK の値を 0.01 としたが，介護施設にいる人の年齢を考慮すると小さすぎるのではないかという意見があったので 0.05 とした．また，式 (1) の Eh の値を 300 万円としたが大きすぎるという意見があり，10 万円とした．このように値を変えたうえで支援プログラム PMSS を用いて最適解を求めてみた．その結果対策コストの制約値を 13 万円とした場合の最適な組合せは 3.4 節で述べた 5 つであり，目的関数の最大値は変わるが採用すべき解に変化はないことが分かった．

このように支援プログラム PMSS があるので，制約条件に関する入力値を変えるとただちにその制約条件に沿った，対策案の最適の組合せを求めることができた．また，組織の関与者とのリスクコミュニケーションに基づき，パラメータの値を変えたうえで最適な対策の組合せを求めることも容易にでき，関与者間で合意が得られるまでこの過程を続ければよいことが分かった．

本プログラムは直接的には医療用 IoT システム向けのものであるが，アンアベリラビリティの低減が及ぼすセーフティへの影響の定義や計算式の形を少し変えるなどによって，他の IoT システムにも適用が可能であると考えている．

4. まとめ

IoT の普及にともない，IoT システムのリスク評価が重要性を増している．医療用 IoT システムのリスク評価においては，セキュリティだけでなくセーフティやメンテナビリティを考慮したリスク評価を行い，メンテナビリティ・セーフティ・セキュリティのバランスの取れたシステムの実現が必要となる．著者らはこれを MSS コンセプトと名付け，このコンセプトを実現するためにリスク評価と対策案の最適な組合せを求める方法の研究・開発を行ってきた．今回，報告者らはそこで，このための定式化方式を提案するとともに，この定式化結果から解を求めるための求解プロ

グラム（PMSS：Program for risk assessment considering Maintainability, Safety and Security）を，Python を用いて開発した．

この定式化方式と求解プログラムを敷布型マルチバイタル IoT モニタシステムに適用した結果，リモートメンテナンスを行うと，個人情報漏洩対策を実施しないと全体のリスクが増大するので何らかの個人情報漏洩対策と組み合わせるほうが望ましいことを明確にした．また，対策コストの制約条件下で，対策のメリットとディメリットの減少の和を最小化する対策案の最適な組合せを具体的に求めることができ，それらの対策の組合せを用いると比較的安いコストでメリットの方が大きくなることを明らかにした．

以上の適用により，少なくとも医療用 IoT システムに対しては，MSS コンセプトに基づく対策案の最適な組合せを求めることが可能であると明らかになった．

今回も，パラメータの値をいろいろに変化させて計算を行い，最適な対策案の組合せを求めたが限定的である．実際の適用に当たっては，意思決定関与者の意見を聞きつつ，リスクコミュニケーションを行い対策案の最適な組合せを求めていけばよいが，今回のように実験的に適用するにはさらにいろいろなケースで解を求め傾向を明確にすることが望ましく今後の課題である．

また，他の医療用 IoT システム，別の IoT システムに適用し，対策案の最適な組合せを求めるとともに，方式やプログラムの改良を図っていきたい．

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」[11] 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に種々の有効な意見をいただいた．感謝申しあげる．

IoT システムのリスク評価の方法論について貴重な議論いただいた情報セキュリティ大学院大学大久保隆夫教授，NTT データ金子朋子氏，東京電機大学高橋雄志氏，林浩史氏，早川拓郎氏にお礼申しあげる．

また，一般社団法人セキュア IoT プラットフォーム協議会のメンバには IoT システムの現実的使い方やレイヤーリングに関する示唆をいただいた．記して感謝申しあげる．

参考文献

[1] IPA：はじめての STAMP/STPA—システム思考に基づく新しい安全解析手法 (2016), 入手先 ⟨https://www.ipa.go.jp/sec/reports/20160428.html⟩.
[2] Kaneko, T., Takahashi, Y., Okubo, T. and Sasaki, R.: Threat analysis using STRIDE with STAMP/STPA, *The International Workshop on Evidence-based Security and Privacy in the Wild 2018* (2018).
[3] 佐々木良一：IoT 時代のリスクコミュニケーション支援ツールの構想，情報処理学会 DICOMO2018 (2018).
[4] 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 (2019).
[5] Hayakawa, T., Sasaki, R., Hayashi, H., Takahashi, Y., Kaneko, T. and Okubo, T.: Proposal and Application of Security/Safety Evaluation Method for Medical Device System that Includes IoT, *ICNCC 2018*, pp.157–164 (2018).
[6] 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 (2019).
[7] Tedeschi, S., Mehnen, J., Tapoglou, N. and Roy, R.: A Secure IoT Devices for the Maintenance of Machine Tools, *Procedia CIRP*, Vol.59, pp.150–155 (2017).
[8] Tedeschi, S., Mehnen, J., Tapoglou, N. and Rajkumar, R.: Security Aspects in Cloud Based Condition Monitoring of Machine Tools, *4th International Conference on Through-life Engineering Services* (2015).
[9] Uesawa, H., Takehara, T. and Ueno, A.: Non-contact measurements of diaphragm electromyogram, electrocardiogram and respiratory variations with sheet-type fabric electrodes for neonatal monitoring, *2018 IEEE EMBS International Conference on Biomedical & Health Informatics* (*BHI*) (2018).
[10] 熊本博光：モダン信頼性工学，コロナ社 (2005).
[11] 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，入手先 ⟨https://www.dendai.ac.jp/about/tdu/activities/branding/⟩.

佐々木 良一 （正会員）

1971 年日立製作所入社．システム開発研究所にてシステム高信頼化技術，セキュリティ技術，ネットワーク管理システム等の研究開発に従事．2001 年 4 月より 2018 年 3 月まで東京電機大学教授．現在，東京電機大学総合研究所特命教授兼サイバーセキュリティ研究所長．工学博士（東京大学）．著書に，『IT リスクの考え方』岩波新書 2008 年等．日本セキュリティ・マネジメント学会会長，内閣官房サイバーセキュリティ補佐官等を歴任．本学会フェロー．