Vol.2019-GN-106 No.35
Vol.2019-CDS-24 No.35
Vol.2019-DCC-21 No.35
2019/1/25

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

林 浩史[†1]　髙橋 雄志[†1]　金子 朋子[†1]
早川 拓郎[†1]　佐々木 良一[†1]

概要： IoT 機器の急速な普及に伴い，IoT 機器を含むサービスシステムのサイバーセキュリティが重要な課題となっている．IoT 機器はその性質上，サイバーセキュリティとセーフティが一体不可分であり，従来の IT 環境とは異なる特徴を持っている．また，セキュリティ・バイ・デザインの考え方が，IoT 機器のセキュリティ対策にとっても，有効であるが，それを支援する評価方式やツールは整備途上である．本稿では，このような特徴や課題を考慮し，IoT 機器のセーフティ・セキュリティリスク評価を行う方式を提案する．まず分析方式として，リスク指向アプローチを採用した．これによりリスク対策の優先度比較や費用対効果の分析が可能である．また，分析者の負担や分析期間の軽減を目的とし，準定量表現を採用した．セーフティとセキュリティが融合する環境に対するリスク分析を行うため，STAMP/STPA を拡張して活用し，その結果を木構造による発生可能性分析に活用した．STAMP/STPA の分析結果から複雑な因果関係を整理して樹形図を構築し，分析や対策案の策定を支援，その残留リスクや費用対効果を算出する方式を提案し，併せてそれらの作業を容易に行うための分析支援ツール SS-Rat を開発した．これにより，分析者の負担が軽減し，IoT 機器の特徴を考慮した方式で，セキュリティ・バイ・デザインが実現できることを目標とした．インシュリンポンプを対象とした分析を行い，その効果を検証した結果，従来方式では識別できていなかった脅威が識別された他，ツールを活用することで分析に要した期間を短縮できることが確認された．

キーワード：IoT 機器，リスク分析，セキュリティ・バイ・デザイン，STAMP/STPA，リスク指向

Proposal of an IoT Risk Assessment Framework and its assistant tool SS-Rat

HIROSHI HAYASHI[†1]　YUJI TAKAHASHI[†1]　TOMOKO KANEKO[†2]
TAKURO HAYAKAWA[†1]　RYOICHI SASAKI[†1]

Abstract: Cybersecurity for IoT device is identified as an important topic. Both of Cybersecurity and Safety should be discussed at once for IoT device by their characteristics. The methodology of Security-by-design can work well for IoT device development as well, but it is still on the half way to develop the analysis method and assistant tools suitable for IoT device. We would like to propose the Risk Analysis method with the consideration of these characteristics of IoT Device and its systems. We considered to use Risk-Base-Approach with Semi-Quantitative description to enable comparison between several ways of countermeasure and quick and effective analysis. To consider both of Security and Safety, we considered to use STAMP/STPA with some extension. The tree share analysis is also used to calculate likelihood of hazard and threat. We developed assistant tool named SS-Rat to make analysts' effort lighter to realize Security-By-Design process. We could find several positive results to confirm the effect of our proposed method and assistant tools by trial using Insulin-Pump.

Keywords: IoT, Risk analysis, security-By-Design, STAMP/STPA, Risk-Base Approach

1. はじめに

近年，様々な分野で IoT 機器が開発・活用されている．IoT 機器の多くは従来組み込み機器として製造販売されていたデバイスに通信機能を付加することで，さらなる利便性の向上や付加的な機能の実装が行われたものである．従来の組み込み機器は，その目的に合わせて必要最小限のハードウエアおよびソフトウエアで構成されていた．しかし，通信機能を持ち，関連周辺機能を取り込むことで，多機能化が行われるようになった．この結果，IoT 機器は複雑化しサイバーセキュリティの担保の難易度が上がった．

IoT 機器やこれに関連するネットワーク，サーバーなどのサイバーセキュリティ（以下セキュリティ）を担保するためには，設計開発段階から，セキュリティ対策を考慮する，いわゆるセキュリティ・バイ・デザイン（以下 SBD）が有効なアプローチのひとつであると考えられる．我々は，IoT 機器のセキュリティの担保が，日常生活に非常に大きな影響を与えるものであると考え，この SBD を，できるだけ容易にかつ効率的に実施する手段や方法論について研究を行っている．

IoT 機器は，その機能や目的から，動作不良が，利用者の安全に関わる場合も少なからず発生する．このことから，IoT 機器のセキュリティは，情報資産の保護や改ざん防止を目的としたものに加え，デバイスが正常に動作することを担保する目的でも重要な要素となると考えられる．セキュリティ・アセスメントや脅威・脆弱性分析などは，SBD

†1 東京電機大学
Tokyo Denki University

Vol.2019-GN-106 No.35
Vol.2019-CDS-24 No.35
Vol.2019-DCC-21 No.35
2019/1/25

を実施する上で，重要なプロセスである．セキュリティ・アセスメントに用いる分析方式は数多く提案されているが，その多くは IT 機器に関するものであり，安全と安心がともに求められる IoT 機器での活用については，不十分な場合もある．

またセキュリティ分析は，工業製品の開発工程のひとつであるにもかかわらず，実施者の知識や経験などの個人の属性に結果が依存する場合があり，このような工程がプロセスに含まれることは，その発展過程において解消すべき課題のひとつであると考えられる．本稿では，このような IoT 機器が抱える課題に着目し，安全と安心（セーフティとセキュリティ）を同時に分析し，分析者による結果の違いを可能な限り低減するような方式を提案する．合わせて，開発工程の中で分析を繰り返し実施できるように，開発者自身が低負荷で活用できるような，セキュリティ・セーフティ分析支援ツール Safety/Security–Risk Analysis Tool（以下，SS-Rat）の開発を報告する．

なお，本稿の構成は以下の通りである．2 章にて提案方式とそれにより解決したい課題について述べる．3 章にて課題解決のため開発したツールについて記載し，4 章で提案方式の適用とその検証について報告する．5 章にて評価および今後の展開について述べた後，6 章でまとめる．

2. 提案方式と課題解決

本稿では，IoT 機器のセーフティとセキュリティの分析を同時に実施し，比較検討を行うための方式を提案する．

本提案で解決したい課題は以下の通りである．

① セーフティとセキュリティを同時に分析し，かつそれらを比較検討できる指標が提供できること
② 分析実施者の経験や知識にできるだけ依存しない分析結果が得られること
③ 開発や設計の早期から分析を低負荷に繰り返し実施できること

上記課題解決のため我々は，以下の方式の検討を行った．なお，本稿で取り扱うセーフティとセキュリティについて以下の定義を用いる．

- [セーフティ]: 偶発的なミス、故障などの悪意のない危険に対する安全
- [セキュリティ]:悪意をもって行われる脅威に対しての安全

2.1 STAMP/STPA の利用

まず，我々は，IoT 機器単体の分析を行うのではなく，それを取り巻くネットワークやサーバーなどを含むシステム全体で分析すべきであると考えた．IoT 機器はネットワークと接続することで，その価値が上がる一方，フィードバック系を含むため，より多くの脅威にもさらされる．そこで，分析方式の中に，フィードバックを含むシステムに着目して分析を行うことを基本的な考え方としている STAMP/STPA （ Systems-Theoretic Accident Model and Processes/ System-Theoretic Process Analysis） [1]を採用することとした．MIT ナンシーレブソンが提案した STAMP/STPA は，複数のコンポーネントが協調して動作するシステムにおいて，個々のコンポーネント・機能が正常に動作していても，その間のコミュニケーションや情報の授受に問題が発生した場合には，システム全体としての障害につながるという考え方に基づいている．従来の分析方式では，主にコンポーネント内での障害に着目するものが多かったため，STAMP/STPA を活用することで，システム構成要素の協調動作を考慮した解析が可能となる．

リスク分析を行う方式は数多く提案されている．ETSI の TVRA（Threat, Vulnerability, Risk Analysis）[2]やコネクテッド･カーの分析などで用いられる TARA（Threat Analysis and Risk Assessment）[3]などである．しかし，これら方式は，分析者の知識や力量によって，結果に違いが出てしまう．特に脅威シナリオの作成を行うステップにおいて識別される脅威は，分析者の知識や経験により大きな違いが現れる．この点においても STAMP/STPA を用いることで効果が期待できると考えている．提唱者のナンシーレブソンは，STAMP/STPA によって，より網羅性の高い HCF（Hazard Cause Factor）を抽出することが可能であるとしている．すなわち STAMP/STPA を利用することで，分析者によらずより抜け漏れの少ない分析が期待できる．

また，IoT 機器のセーフティとセキュリティは密接に関連しており一体不可分な状態である．このことから，セーフティとセキュリティは同時に分析される必要がある．

提案方式では，この問題を解決するため，STAMP/STPA でセキュリティを取り扱うための拡張を行った．

STAMP/STPA-Sec[4][5]や STAMP/STPA- SafeSec[6]のような拡張が行われた事例があるが，これらには脅威分析が具現化されていないか、または含まれていない[7][8][9]. 国内でも，大森らによりセーフティとセキュリティを同時に扱う取り組みがなされている[10]. 我々は，サイバーセキュリティをシステムの機能の一部であると位置づけ，分析対象であるシステムがもつべき機能のひとつとしてセキュリティ耐性を想定する．これにより，この機能が「実装されていない」または，「十全に動作しない状態」がインシデントにつながると位置づけた．また，セーフティとセキュリティの HCF を同時に取り扱うことができるよう，本稿の著者の一人である佐々木によるヒントワードの拡張モデル[11]を採用した．

- 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[10]）

Vol.2019-GN-106 No.35
Vol.2019-CDS-24 No.35
Vol.2019-DCC-21 No.35
2019/1/25

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）

このヒントワードは，IoT 機器やその原型である組み込み機器で用いられる概念を活用しているため，提案方式の想定活用主体である IoT 機器開発者にとって馴染みのあるものであり，本稿での提案趣旨に合致している．これにより，HCF を故障のシナリオのみならず，脅威のシナリオとして取り扱うこが可能となると考えた．

2.2 準定量表現での分析

抽出された故障や脅威のシナリオは，その重要度などの観点で比較され，実施優先順位を付けられる必要がある．そこで我々は，リスク指向アプローチを採用した．リスク指向アプローチは，ある「アクシデント・インシデントのリスク」をその「発生可能性」と，「発生したときのインパクト」の積と定義し，このリスク値を利用して比較検討を行う評価方式である．

$$Risk_i = Likelihood_i \times Impact_i \quad -(1)$$

ここでiはアクシデントまたはインシデントである．

まず，アクシデント・インシデントが発生したときのインパクトを定義する．本稿ではアクシデント・インシデントを以下の 3 指標を用いて評価することとした．

- 利用者や関係する人の安全や健康への影響
- 環境など回復に時間を要するものへの影響
- 個人情報・ノウハウのなどの機密情報の漏洩

なお，この指標については，分析対象や分析の目的などに合わせて変更することが可能である．

次に，アクシデント・インシデントの発生可能性について定義を行う．「発生可能性」は，その構成要素に分解し，「構成要素の発生可能性」の論理和として定義することが可能である．ある事象iの発生可能性P_iは，その構成要素jの発生可能性p_{ij}を用いて以下のように書くことができる．

$$P_i = 1 - \prod_j (1 - p_{ij}) \quad -(2)$$

これにより，STAMP/STPA で分析した結果得られる HCF を最下位要素として定義し，HCF の上位層として，UCA(UnSafe Control Action)，さらに上位に安全制約–アクシデント・インシデントが定義されている論理和の木構造を構築することで，アクシデント・インシデントの発生可能性を定義することが可能である．なお，式（2）の成立要件は，その構成要素jが十分抽出されていること（式（3））である．

$$1 - \prod_{j=1}^{n} (1 - p_{ij}) \gg 1 - \prod_{n+1}^{\infty} (1 - p_{ij}) \quad -(3)$$

ここでnは抽出された要素数である．本提案では，構成要素jとして STAMP/STPA で分析した HCF を用いる．STAMP/STPA による分析は網羅性が重視されているため，本方式は式 （3）の要件を具備していると考えている．

なお提案する方式ではリスク，発生可能性，インパクトを[リスクレベル]，[発生可能性レベル]，[インパクトレベル]として 5 段階で準定量値（レベル）して取り扱うこととした．早川ら[12]は定量表現を用いて分析を行っているが，我々は，分析の目的と分析者の入力負担の観点から，準定評表現を採用した．

また，リスクについては式（1）を直接使うことはせず，図 1 のような分析者が設定したマトリックスを用いて表現することとした．これは，分析対象によって単純な積ではない指標を用いる必要がある場合があるためである．

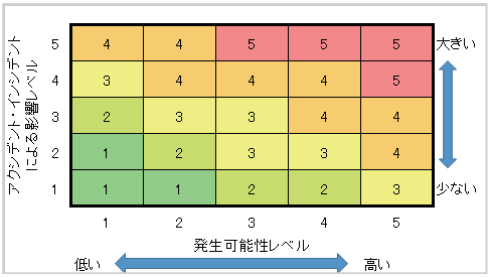

図 1 リスクレベル定義マトリックス

2.3 提案分析方式

提案方式を時系列にしめす．まず図 2 で分析の流れをフローチャートとして示す．

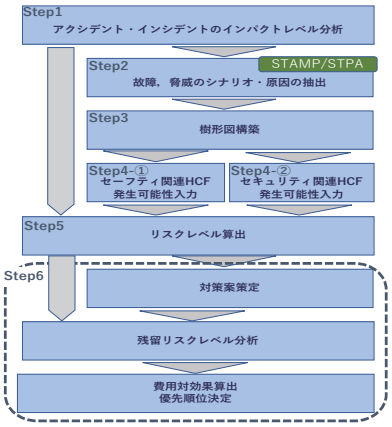

図 2 フローチャート

Step 1. インパクトレベル分析

アクシデント・インシデントのインパクトレベルの定義を行う．本稿の場合，インパクトとは，アクシデント・インシデントが発生した場合に想定される被害または悪影響である．なお，評価においては，できる限り評価者による分析結果の違いを少なくするため，数値ではなく，文章での選択を行うべきであると考える．今回我々は，図 3 のような評価指標を用いた．

本方式では費用対効果算出のため，各安全制約cの違反に起因する総合的なインパクトレベル$Total\ Impact_c$を各指

Vol.2019-GN-106 No.35
Vol.2019-CDS-24 No.35
Vol.2019-DCC-21 No.35
2019/1/25

標を軸として張った空間の原点からの距離として定義した．

$$Total\ Impact_c = \left[\sqrt{\sum_x \left|Impact_{x,j}\right|^2}\right] \quad -(4)$$

xは健康，環境，情報漏えいの各指標であり，当該安全制約cに紐付けられた軸x上のインパクトを$Impact_{x,j}$としたa．

情報漏えいの影響	レベル
情報漏洩しない	1
重要	
機密	
重要	
—	

環境への影響	レベル
ほとんど影響ない	1
限定	
—	
広範	
回復	

健康への影響	レベル
軽傷または通院で完治	1
比較的短期の入院は必要な状態	2
重症または長期療養が必要な状態	3
完治しない　または後遺症が残る	4
死亡する可能性が高い	5

図 3 インパクト評価指標

Step 2.　故障，脅威のシナリオ・原因の抽出

STAMP/STPA を用いて，IoT システムの分析を行う．ここでセキィリティを同時に分析するため以下の拡張を行う．

- アクシデント識別工程においてインシデントも識別
- 故障やミスにより発生するハザードと同様に，意図的なサイバー攻撃によるものを考慮
- UCA(UnSafe Contrl Action)と同時に UnSecure Control Action を識別
- 拡張したガイドワードを用いて HCF(Hazard Cause Factor)および脅威原因（Threat Cause Factor）を抽出

まず，「システムに起こってほしくない状態」であるアクシデントおよびインシデントを識別する．

IoT 機器を取り扱う場合，アクシデントとインシデントは非常に近い意味で捉えることができる．すなわち，システムの一部に機能不全が発生し，その結果サービスが停止する事態に陥った場合，これが部品の故障やソフトウエアの不備によるものであれば，アクシデントと解釈されるが，一方でサイバー攻撃によるものであればそれはインシデントとして解釈される．また，情報漏えいなどのように，システムが提供するサービスには影響を与えず，内包する情報資産が毀損されるような例もここで識別する．

次に，「アクシデント・インシデントに至る可能性のある状態」として定義されるハザードを識別する．提案方式では，セキュリティを機能と考え，インシデントに至る原因として，セキュリティ機能が不全を起こしているまたは機能が実装されていないことを想定して分析を行う．

安全制約は，ハザードや脅威がアクシデント・インシデントに至ることの無いようにするための仕組みや機能であり，本方式で具体化・詳細化を行う対象である．

次に，コントロールアクションの識別を行う．ここでも拡張として，機密情報などの情報資産の授受もコントロールアクションとして記述する．UCA についても同様であり，ここでは UCA を“UnSafe - UnSecure” Control Action として捉える．例えば，ある Control Action において本来送信されるべきでない情報資産が送信されてしまうようなケースは，P: Providing causes hazard として記述される．これは，「機密情報を送信しないようにする機能」を有しているべきシステムが，この機能の不全によりまたは，この機能が実装されていないために，機密情報を送信してしまうケースと考えることができる．

我々は，標準のヒントワードに変えて，佐々木らによって提案されている 6 種類（2.1 節参照）を採用をした．これにより，部品の故障やソフトウエアの不備によるものに加え，サイバー攻撃によりものを考慮することが可能である．

Step 3.　因果関係の整理と樹形図化工程

図 4 の樹形図のように，STAMP/STPA の分析結果は，アクシデント・インシデントを頂点として，HCF に至る木構造として表現できる．なお，安全制約は，複数のハザード，アクシデント・インシデントに効果があるものがあり，また一つの UCA が複数の安全制約違反を引き起こす可能性もあることから，この構造は N:N:N の関係を持つ複雑なものであると考えられる．これを木構造とした場合には，枝や葉にあたる UCA や HCF 部分に，同じ要素が複数回現れる構造となる．

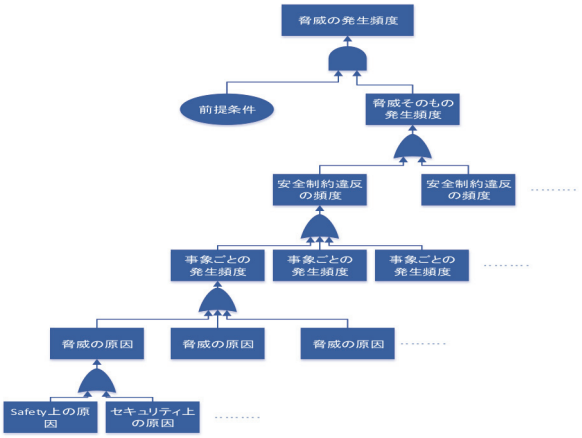

図 4 樹形図

Step 4.　発生可能性

本方式では，HCF は，アクシデント・インシデントを構成要素に分解したときの最小単位である．HCF（ハザードの原因となるファクター）は，具体的な故障や脅威のシナリオであり，準定量表現で発生可能性の定義が可能なレベルであると考えている．我々は，セーフティおよびセキュリティについて，それぞれの HCF 発生可能性を単位時間あたりの発生回数として定義する方式を提案する．なお，STAMP/STPA で設定した前提条件は，その効果を 0. 0～1. 0 で設定し，安全制約の発生可能性に一律に論理積演算を行って考慮した．

a [ ]は整数化

Vol.2019-GN-106 No.35
Vol.2019-CDS-24 No.35
Vol.2019-DCC-21 No.35
2019/1/25

① セーフティに関連するもの

本方式において，セーフティに関連するハザードは，部品の故障などに起因するものとして評価をされる．例えば，ある部品の単位時間あたりの故障の可能性は，MTBF（Mean Time to Failure）の逆数として表現される．

このように分析者が日頃使っており，部品の仕様書などから比較的入手が容易な情報であるMTBFや部品の耐用年数など情報を入力パラメータとして活用することが望ましいと思われる．本稿ではMTBFを用いた．

② セキュリティに関連するもの

セキュリティ関連HCFの発生可能性は，ITを含む一般的なサイバーインシデントの発生可能性をベースに，悪用される脆弱性のCVSS値を考慮して算出する方式を提案する．

$$p_{HCF} = p_{cyber} \times v \quad -(5)$$

ここで，p_{HCF}は，セキュリティ関連HCFの発生可能性，p_{cyber}は一般的なサイバーインシデントの発生可能性，vは，HCFの特徴を考慮したファクターである．

TARAなどの既存の準定量分析方式において，脅威の発生可能性レベルとして，その脅威に悪用されると想定される脆弱性のCVSS攻撃容易性値を活用する方式が提案されている．我々はこの方式を活用し，個別のHCFの特徴から抽出したCVSS攻撃容易性値をファクターとして活用する．CVSS v3b[b]では攻撃容易性fを，以下のように定義している．

$$f = 8.22 \times v_{AV} \times v_{AC} \times v_{PR} \times v_{UI} \quad -(6)$$

ここで，$v_{AV}, v_{AC}, v_{PR}, v_{UI}$は，それぞれ「攻撃元区分」，「攻撃条件の複雑さ」，「攻撃に必要な特権レベル」，「攻撃へのユーザの関与レベル」である．ここで，fの最大値，最小値をそれぞれf_{max}, f_{min}とすると，規格化されたfであるf'は以下のように書くことができる．

$$f' = \frac{f - f_{min}}{f_{max} - f_{min}} \qquad 0 \le f' \le 1 \quad -(7)$$

インシデントがCVSSについて偏りなく分布していることを仮定すると，統計処理等で一般に用いられる仮定を活用し，vを以下のように定義することが可能である

$$v = -\ln(f') \qquad -(8)$$

これにより，HCFの特徴を考慮して，発生可能性を仮定することが可能となる．なお，厳密な数値としての，一般的なサイバーインシデントの発生可能性p_{cyber}の入手は難しいが，分析対象環境でのインシデント発生実績値や，公開情報からの概算値を利用することも可能である．本稿の検証においては，JPCER/CC[c]のレポートJPCERT-IR-2017-01, JPCERT-IR-2017-03, JPCERT-IR-2017-04, JPCERT-IR-2018-01から国内でのインシデント件数を活用した．

Step 5. リスクレベルの算出

Step1で，アクシデント・インシデントに関するインパクトレベルを算出し，Step2～4で発生可能性を算出した．これにより，リスク指向アプローチによる方式を用いて，アクシデント・インシデントのリスクレベルを算出する．算出には，図1のマトリックスを利用した．

Step 6. 対策

リスクアセスメントの目的として，リスクを評価した後の対策案の策定，その対策に対する残留リスクの評価およびその効果を考慮した実施有無・優先順位の検討がある．

提案方式では，対策策定補助，残留リスクの評価方式，および費用対効果の検討方式についても提案を行う．

まず，対策案は，抽出された各HCFについて検討する方式を提案する．HCFは故障やサイバー攻撃に関するシナリオであり，前のStepまでで，故障が想定される部品や，発生が想定される脅威が抽出されている．したがって，それに対する対策案として，部品の交換や脅威に対する防衛策を具体的に記載することが可能である．本方式では対策案を実施した結果を，Step4で定義した発生可能性レベルの変化値として考慮する．なお，構築した分析用樹形図は，同じHCFが複数箇所に登場する構成であるため（Step 3参照），同じHCFには同じ対策案が設定される必要がある．同様に，複数のHCFに効果のある対策案を策定することも可能であるため，対策案の効果に関する比較検討を行う場合には，これ考慮する必要がある．

IoT機器などの工業製品に関するセキュリティを考えるとき，費用，開発期間など様々な制約条件により，策定された対策案をすべて実施することは非現実的である．多くの場合，対策には優先順位を設定して実施する．提案方式では，準定量分析によって得られた結果を，この優先順位の検討のために材料として活用する．対策案iの効果$\delta Risk_i$を以下のように定義する．

$$\delta Risk_i = Risk_{initial} - Risk_i \qquad -(9)$$

ここで，$Risk_i$は対策案iのみを実施したときの分析対象全体のリスクベルである．また$Risk_{initial}$は全く対策を行っていない初期分析時点でのリスクレベルである．費用対効果は，この$\delta Risk_i$を得るために支払う費用として対策案iごとに定義する．

3. ツール開発

3.1 ツール開発の目的

2章で定義した課題③の解決には，分析補助のためのツールが有効である．STAMP/STPAの分析結果として多数のHCFを得ることができる一方で，樹形図構築や，同一のHCFの発生可能性パラメータ，対策案管理など，煩雑な作業が発生する．そこで，支援ツールSS-Ratを開発した．

3.2 ツールの構成

ツールは，以下の特徴をもつ

① STAMP/STPA Workbenchの活用

b Common Vulnerability Scoring System: https://www.first.org/cvss/

c Japan Computer Emergency Response Team Coordination Center

Vol.2019-GN-106 No.35
Vol.2019-CDS-24 No.35
Vol.2019-DCC-21 No.35
2019/1/25

Step2 HCF の抽出工程には，IPA d が提供している STAMP/STPA Workbench を利用する．STAMP/STPA Workbench は，STAMP/STPA 分析支援ツールであり，多くのユーザが活用している．このツールを利用することで，ユーザは今までに分析した結果を活用することができる．

② SS-Rat

SS-Rat は，Step1 および Step3-6 の支援ツールであり，マイクロソフトエクセルのマクロ機能により実装されている．

本稿で想定する利用者は IoT 機器のサイバーセキュリティに従事する技術者などである．このような利用者の環境は，セキィリティ対策が通常より厳しくに行われることが多く，特殊なソフトウエアのインストールを制限する企業も少なくない．そのため，できる限り既存環境で動作する形態を選択した．

3.3 動作環境

ツールは，表 1 の環境で利用可能である．

表 1 SS-Rat の動作環境

動作環境	● Windows7 以上 動作確認環境 Windows 10 ● Microsoft Excel 動作確認環境 Excel2016
開発言語	VBA
ソフトウエア規模	約 5000 ステップ

4. 提案方式の適用と検証

本稿では，提案方式およびツールの適用事例として，インシュリンポンプを取り上げる．インシュリンポンプとは，糖尿病患者が常に携帯・装着し，必要に応じて体内にインシュリンを注入する医療機器である．インシュリンポンプシステムで測定された血糖値は，ネットワークを通じて医療機関に送信され，主治医が血糖値などの情報を元に診断を行い，インシュリン注入の指示をだす．この指示が再度ネットワークを通じてインシュリンポンプに伝達され，インシュリンが，患者の体内に注入される．このシステムは，取り扱う情報が医療情報であり，情報の改ざんなどのサンバー攻撃，機器や部品の故障による誤動作が発生した場合のインパクトが，患者の生命・健康に直結する．また，取り扱う情報が要配慮個人情報であるため，情報漏えいの観点からも分析・対策が必要である．本方式の検証として，インシュリンポンプシステムに関する分析を行い，提案手法により有効な結果を得ることができることを示す．

続いて，提案方式を用いた場合と従来方式を用いた場合での抽出された脅威シナリオの違いを検討することで，従来方式との差異，優位性などを検証する．

最後に，本分析方式を手作業で行った場合と，ツールを用いた場合での違いを作業時間の観点から検証する．

4.1.1 アクシデント・インシデント設定と HCF 抽出

STAMP/STPA Workbench を用いて，インシュリンポンプの分析を行った結果，図 5 のようなコントロールストラクチャ図を作成し，3 個のアクシデント・インシデントに対して，11 個のハザード･脅威，13 個の安全制約が定義された．

医師，患者を含め 8 のコンポーネントと 15 のコントロールアクション（CA）が識別された．

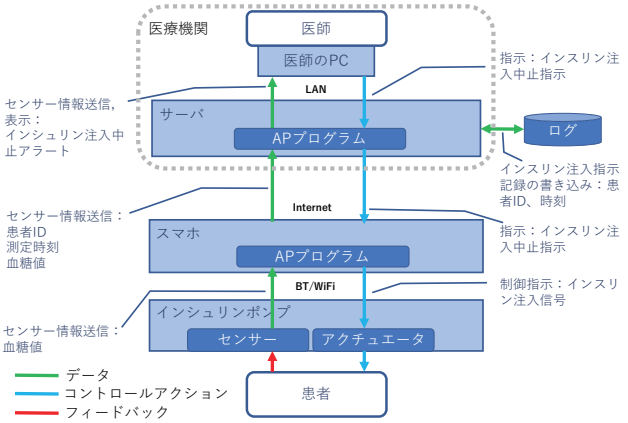

図 5 インシュリンポンプシステムの
コントロールストラクチャ

各 CA について，ガイドワードを適用した結果 57 個の UCA が識別され，各 UCA について，拡張したヒントワードを適用することで，266 個（類似のものを含む）の HCF が識別された．（3 章 Step2 参照）

4.1.2 インパクトレベル分析

STAMP/STPA で識別されたアクシデント・インシデントについて，そのインパクトレベルを図 6 で示すように「安全」「環境」「情報漏えい」の観点で分析・選択した．（3 章 Step1 参照）

図 6 アクシデント・インシデントのインパクト定義

4.1.3 因果関係整理と樹形図化

ハザードと安全制約は，N:1 の関係を持っている．SS-Rat は，安全制約をキーとして，ハザードと，このハザードに紐づく UCA を自動的に整理する．整理した結果は図 7 で示すようになった．図 7 は，木構造分析の上位 2 レイヤーまでを表示している．（3 章 Step3 参照）

d 独立行政法人 情報処理推進機構

Vol.2019-GN-106 No.35
Vol.2019-CDS-24 No.35
Vol.2019-DCC-21 No.35
2019/1/25

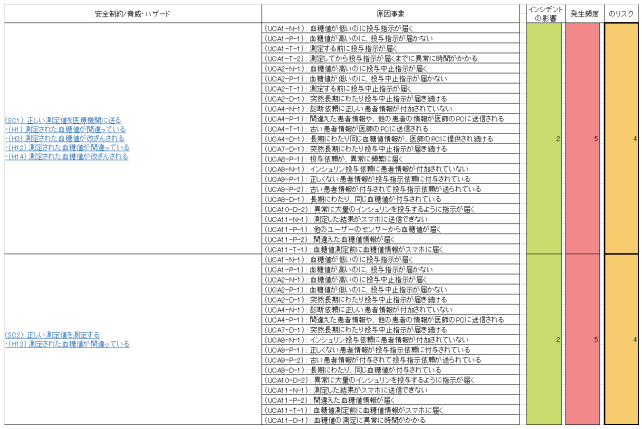

図 7　安全制約と UCA のマッピング

4.1.4 発生可能性

発生可能性分析画面では，各「安全制約違反の発生可能性」を頂点とした木構造が表示される．分析者は，図 8 のように，各「故障・脅威の原因（HCF）」について，セーフレベルまたはセキュリティレベルの設定を行う．セーフレベルを設定する場合には，セーフレベルの選択肢から該当するものを選択し，セキュリティレベルでは，攻撃に悪用されることが想定される脆弱性の特徴として，CVSS の各項目を選択する．なお，分析者は，CVSS に関する専門的な知識は必要なく，「攻撃元区分」，「攻撃条件の複雑さ」，「攻撃に必要な特権レベル」，「攻撃へのユーザの関与レベル」などの悪用される脆弱性の特徴を選択する．(3 章 Step4 参照)

図 8 発生可能性設定画面例

なお，SS-Rat は，同一の HCF が複数現れた場合，これを自動的に検出する．別の安全制約などで入力済のセーフレベルやセキュリティレベルが存在する場合，自動的に該当箇所の転記が行われ，ユーザは重複内容を検索する必要も，改めて入力する必要はない．

4.1.5 リスクレベル

セーフレベル，セキュリティレベルの選択が終了すると，「故障・脅威の原因（HCF）」，「ケース毎の発生可能性（UCA の発生可能性）」「安全制約違反の発生可能性」が自動的に計算され，「アクシデント・インシデントの影響」を用いて，「安全制約毎のリスクレベル」が算出・表示される．(3 章 Step5 参照)

4.1.6 対策案策定

対策案は，HCF 毎に設定する．策定された対策案は SS-Rat 内の DB で管理され，対策案設定処理では，策定した対策案を選択する．これにより対策案の再利用性向上や複数 HCF に効果がある場合の費用対効果への影響を考慮する．

対策案策定（対策案 DB 入力）機能では，「対策実施後のセーフレベル，セキュリティレベルの設定」および，「発生頻度の減衰値指定」が可能である．「発生頻度の減衰値指定」は取扱説明書の改善・充実，訓練の実施，業務プロセスの改善など，人的，付加的要素，システム外要素の改善により発生可能性を抑制するような対策を想定している．

また，費用対効果を計算するため，この対策実施にかかる費用概算の入力を行う．（3 章 Step6 参照）

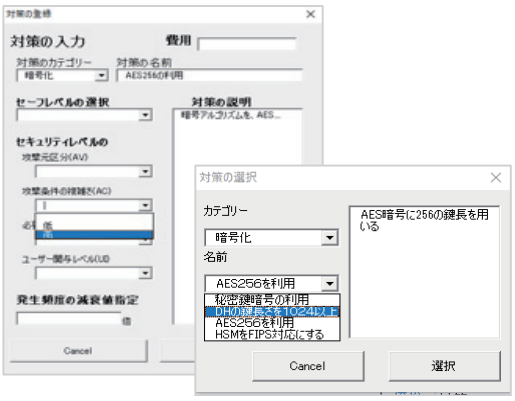

図 9　対策案策定と選択

4.1.7 残留リスク，費用対効果

対策案設定後，SS-Rat は自動的に分析結果をまとめ，「対策前の総合リスクレベル」（図 9①），「策定したすべての対策案を実施した場合の総合リスクレベル」（図 9②）を表示する．さらに，対策実施のための予算を設定（図 9③）することで，SS-Rat が費用対効果の高い順に予算の範囲内で対策案を自動的に選択し，「予算内で対策を実施した場合の総合リスクレベル」（図 9④）と，その時選択された対策案一覧（図 9⑤）を出力する．

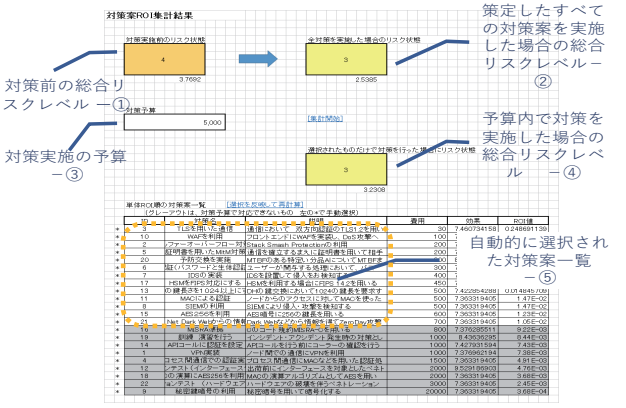

図 10　費用対効果と優先順位設定

4.2 分析を行った「主要な結果」

本稿提案の方式の効果を検証するため，同一のシステムに

Vol.2019-GN-106 No.35
Vol.2019-CDS-24 No.35
Vol.2019-DCC-21 No.35
2019/1/25

対して STRIDE を用いた脅威分析を行った．この方式は，脅威分析の方式として一般的に行われているものである．なお，STRIDE はセキュリティに特化した考え方であるため，本方式の分析結果についてもセキィリティに関連するもののみを抽出して比較を行う．STRIDE を使って分析を行った結果，33 個の脅威が識別された．一方で提案方式では 123 個（類似のもをの含む）の脅威が識別された．従来方式では、識別が難しい,「サーバー–スマホ間の MitM で，投与指示受信を何回か否認し，正規の投与指示を複数回発行させて，まとめてアクチュエータに送信することで大量のインシュリンを投与する」ようなケースなども含まれていた．また，その他に患者・医師のオペレーションミスによるものや，「患者がセンサーを勝手に取り外してしまう」ような想定外の使い方によるもの，マルウエアによるスマホアプリやサーバーの改ざんも，多く識別された．このことから，通信時の認証や暗号化処理が，情報資産保護だけではなく，セーフティの観点からも有効であること，マニュアル整備や研修などシステム外対策が有効であることなどが認識された．以上より本稿提案の目的の観点から，従来方式と比較して，優位な結果が得られたと考えている．

次に，ツールの効果について比較検討を行った．ツールを使わずに，同分析を行った場合，因果関係の整理や樹形図の構築作業が非常に煩雑であり，複数の安全制約に影響を与える UCA の検出などに多くの時間がさかれ，5 人日の工数を要した．一方，ツールを使った場合には，約 1 人日程度で分析することができた．

5. 評価および今後の発展

5.1 評価

本稿では，2 章に示す 3 つの課題の解決のため，方式の提案および検証を行い，その支援ツールである SS-Rat を開発した．検証結果から，提案方式について，次のようなことが確認できた．

① IoT 機器の特徴である，セーフティとセキュリティを同時に取り扱うことができる
② 故障や脅威のシナリオである HCF をより網羅的に識別できる方式であり，分析実施者の経験や知識に依存する要素を排除しやすい

また，支援ツール SS-Rat についてはさらに評価実験が必要であるが，今回の適用の範囲では，分析に要する工数を 80%程度短縮でき，工数低減に有効なものである見通しを得た．

5.2 今後の展開

ひとつの HCF について，複数の対策案を策定し，実施することも可能であるが，本ツールでは未対応である．さらに，複数の対策案を行った場合には相乗効果や阻害関係による効果減少などが想定される．現時点ではこれらの効果は未考慮であり，今後の課題として検討を進める必要があると考えている．

また，本稿では，STRIDE による脅威分析と比較したが，TVRA，TARA などの他の方式と比較してその優位性を検証するとともに，改良を重ねる必要があると考えている．

6. まとめ

本稿では IoT 機器とその周辺システムに関するセーフティ・セキュリティ分析の方式を提案し，インシュリンポンプを対象とした分析事例を用いて検証を行った．IoT 機器は日々進化し続けており，機能・性能，用途などによって，その特徴も様々である．また，分析の目的や注意・注目すべき点も異なる．そのため，多くの分析事例を蓄積し，さらなる検討や拡張が必要である．

我々は，今後も本分析方式と支援ツール SS-Rat を研究活動や実業務で活用し続け，実施例を蓄積し，適用範囲を広げるとともに，方式およびツールの改善・改良を継続して行きたいと考えている．

参考文献

[1] Nancy G． Leveson:Engineering a Safer World: Systems Thinking Applied to Safety (Engineering Systems), The MIT Press, 2012.
[2] ETSI TS 102 165-1 V5．2．3 (2017-10) CYBER; Methods and protocols;Part 1: Method and pro forma for Threat, Vulnerability, Risk Analysis (TVRA)
[3] J3061_201601 Cybersecurity Guidebook for Cyber-Physical Vehicle Systems
[4] William Young Jr, Security Tutorial Part 1 A Systems Approach to Security, 5th STAMP Workshop in BOSTON
[5] William Young Jr, Understanding STPA-Sec Through a Simple Roller Coaster Example
[6] Ivo FriedbergMcLaughlin,Paul Smith,David Laverty,Sakir SezerKieran.(2017). STPA-SafeSec: Safety and security analysis for cyber- physical systems. Journal of Information Security and Applications.
[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]金子朋子，高橋雄志，大久保隆夫，勅使河原可海,佐々木良一．” 安全性解析手法 STAMP／STPA への脅威分析（＝STRIDE）の適用，”,CSEC 研究会,Mar8.2018
[9]Tomoko Kaneko, Yuji Takahashi, Takao Okubo and Ryoichii Sasaki, ”Threat analysis using STRIDE with STAMP/STPA,” The International Workshop on Evidence-based Security and Privacy in the Wild 2018
[10]SQiP 研究会演習コースⅢ,”セーフティ＆セキュリティ開発のための技術統合提案～STAMP/STPA とアシュアランスケースの統合～”, www.juse.jp/sqip/library/shousai/?id=378
[11]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
[12] 早川拓郎「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 DICOMO201
[13]Microsoft,The STRIDE Threat Model, (参照 2018-05-13)