

# セーフティとセキュリティの手法を含んだリスク管理手法についての調査

五郎丸秀樹<sup>†1</sup>

**概要:** 概要: 近年, IoT や CPS 技術の広まりによって情報システムは人々の普通の生活に欠かせなくなるほど社会に浸透しシームレスに様々なサービスを使えるため利便性が高まってきている。しかし利便性が高まった反面, サイバー攻撃による被害が拡大し易くなり, 標的型攻撃やハイブリッド攻撃など技術的だけではなく人的な脆弱性にも攻撃が行われている。そして Stuxnet やサプライチェーン攻撃のようにネットワークから切り離された制御系システムでさえもサイバー攻撃対象になっている。その結果, セーフティだけでなくセキュリティの面も含めたリスク管理が必要となり, FMVEA, FACT Graph, SAHARA, STPA-SafeSec などセーフティとセキュリティの手法を組合わせた新たな手法が出現した。本稿では, これらの手法について調査を行い, 手法の違いや共通点などの特徴を示すと共に, その問題点や課題を明らかにする。

**キーワード:** IoT, CPS, リスクマネジメント, セキュリティ, セーフティ

## A Survey of Risk Management Method with Safety and Security Analysis

HIDEKI GOROMARU<sup>†1</sup>

**Abstract:** In recent years, with the spread of IoT and CPS, information systems have become essential in people's daily life and the convenience of various services has been improved through their seamless use. However, the damage of cyber-attacks has become widespread easily for the high convenience. Attacks to not only technical vulnerabilities but also human vulnerabilities have increased, such as APT or hybrid attacks. Even offline control systems are targeted by cyber-attacks such as Stuxnet or supply chain attacks. As a result, it has been to need the risk management for safety and security, and new methods, which have safety method and security method such as FMVEA, FACT Graph, SAHARA and STPA-SafeSec, have appeared. In this paper, we identify about the difference of measures or things in common of methods after investigating these methods, and clarify the problems and issues.

**Keywords:** IoT, CPS, Risk Management, Security, Safety

### 1. はじめに

近年, IoT (Internet of Things)[1][2]および CPS(Cyber Physical System)[3]技術が産業界に広まり, 必要な情報を必要な時に提供することで人間社会へ還元し新たな価値創造をおこなう Society5.0 が叫ばれている[4]. 各業界や各分野で独自に発展してきた独自のネットワーク・通信プロトコル・機器を使用した独自システムは, 情報システムの広がりに伴い標準化そして汎用化されたシステムへと変わり, 機器間およびサービス間の連携が容易になることで新たなサービスがクラウドやスマートフォンを経由して簡単に実施可能となり, システムの保守などのコストが削減され利便性が向上していった。

その反面, 機器の故障やマルウェアなどによる攻撃に対して被害が拡大しやすくなり, 小さなインシデントやアクシデントがシステムやネットワーク全体へと波及し, 政府や銀行や発電所などの重要機関やインフラの各サービスが停止したり住民の安全が脅かされたりするなど国家や世界

規模の影響へと広がる可能性が高まった。そしてネットワークに接続しないシステムであっても安全とは言えず, Stuxnet[5]やサプライチェーン攻撃[6]により閉じたネットワークであってもサイバー攻撃を受ける可能性があることが証明され, 制御系システムはセーフティだけでなくセキュリティも考慮することが迫られている[7][8][9].

しかしセーフティおよびセキュリティの対策のためにセーフティ対応機能とセキュリティ対応機能を調整なしに開発し別々に組み込むと, 一方の機能がもう一方の機能の新たなリスクになる場合があり, 機能の不整合がシステムに残る可能性がある[10]. 不整合の有無の確認や新たな仕様変更などでセーフティの専門家とセキュリティの専門家との間の調整が必要になる。そこで調整を支援するためセーフティだけでなくセキュリティの手法も含めた様々なリスク管理手法が出現した。

本稿では, まず用語の意味を理解するため, セキュリティとセーフティに関連する用語の定義をおこない, 分野の現状の調査をおこなう。各手法の違いや共通点などの特徴を把握し, セキュリティとセーフティに使用する手法の既存の問題点と課題を示す。そして, 新たな分類を実施し,

<sup>†1</sup> 日本電信電話株式会社  
NIPPON TELEGRAPH AND TELEPHONE CORPORATION

今まで気づけなかった新たな問題点や課題を明らかにする。

## 2. 用語の定義

セーフティとセキュリティの両特性を含むシステムを開発する方法論は「Safety and Security Co-engineering」と呼ばれている[8]。ここではセーフティとセキュリティを「SaS (Safety and Security)」[11]と呼ぶこととする。SaSの研究が進むにつれてSaSで使用されている用語の定義が従来の定義とは異なってきているため、現在SaSで使用されている関連用語について紹介する。

### 2.1 セーフティ・セキュリティ・リスクマネジメント

これまでの標準規格では、セーフティは「許容不可能なリスクがないこと」[12]、セキュリティ（ここでは「情報セキュリティ」とする）は「情報の機密性、完全性および可用性を維持すること。さらに、真正性、責任追跡性、否認防止および信頼性のような特性を維持することを含めてもよい」[13]と定義されている。しかしSaSでのセーフティとセキュリティの違いはこれらの定義では判りにくい。Abulamddi (2016)[11]は、セーフティとセキュリティの違いを下記(1)(2)のように述べている。

#### (1) 発生源と影響先

- ・ セーフティはシステムから発生し環境に影響を与える可能性がある危険を扱う
- ・ セキュリティは環境から発生してシステムに影響を与える可能性があるリスクに関係している

#### (2) 意図の有無

- ・ セーフティは意図しないハザードを扱う
- ・ セキュリティは意図的な脅威を扱う

またChockalingamら(2017)[14]はリスクマネジメントも含めた上記(2)と同様の定義を行っている。

- ・ セーフティコミュニティは、自然災害、技術的欠陥及び人的過誤によって引き起こされる意図的でない又は悪意のない脅威に対処するもの
- ・ セキュリティコミュニティは、意図的な人間の行動によって引き起こされる意図的/悪意のある脅威に対処するもの
- ・ リスクマネジメントは、意図的でない/悪意のない脅威と、意図的である/悪意のある脅威の両方に対処するもの

上記の(1)(2)の定義について異論も存在する。例えばISO/IEC27005:2011aでは附属書Cにて、故意（意図的）によるもの（例：盗難、盗聴）だけでなく、偶発的なもの（例：故障、ミス）、環境的なもの（例：地震、洪水）も情報セキュリティの脅威に含めており(1)(2)の定義とは異なる。同様にリスクマネジメントの標準規格であるJIS Q31000:2019 (ISO 31000:2018)でのリスクマネジメントの定義は「リスク

（目的に対する不確かさの影響）について、組織を指揮統制するための調整された活動」[15]となっており上記の定義とは異なる。しかし、セーフティとセキュリティの違いや共通点を説明する上では非常に判りやすく、セキュリティ自体の定義も流動的（例えば、セキュリティの一種であるサイバーセキュリティの定義は流動的である[16]）であるため、本稿のSaSではリスクマネジメント（リスクマネジメントはリスクアセスメントを含む[15]）の定義も含めた(2)の定義を使用することとする。

### 2.2 SIS

SaSには、SIS (Security Informed Safety : セキュリティを考慮した安全性)と言う概念があり [17][18][19]、そのねらいは「安全性技術者 (safety engineer) がセキュリティについての認識を深めることと、そのためにプロセスと知識を提供すること」である[17]。S4S(Security for Safety)[18]の考え方にも通じる。この概念自体はわかりやすいが、具体的に手法の分類に適用しようとすると難しい。セキュリティ手法とセーフティ手法および両方を含む手法 (SaS) を分類した場合、

- ① 他分野を不使用（セーフティとセキュリティは別々）
- ② 他分野情報を使用（SIS）
- ③ 両分野を使用（セーフティとセキュリティの両方）

に分けることができる。①に関しては従来のセーフティまたはセキュリティの手法であるので問題はないが、SaSの任意の手法を②と③のどちらに分類すべきなのか基準が不明瞭である。特にセキュリティの手法はセーフティの手法を参考に改良したものも多い [20]。例えば、FMEA[21]とSTRIDE[22]を組み合わせたFMVEA[23]は②と③のどちらに属するのか迷う。FMVEAの処理はセーフティ処理とセキュリティ処理で分けて処理し整合しているのが③であるが、セキュリティ処理は元々セーフティの手法であるFMEAをSTRIDEと組み合わせてセキュリティ処理に使用しているので②とも言える。本稿ではSISは概念としては使用するが、具体的な手法の分別には使用しないこととする。

## 3. 現状の把握

本章ではSaSの動向を把握することとする。研究分野だけでなく応用分野としての業界、そして標準化活動など幅広く各種の動向を確認し現状を把握していく。

### 3.1 関連研究の動向

SESAMO (2013)では、SaSシステムにおける各コンポーネント間の相乗効果とトレードオフの分析結果を公表している[10]（例：暗号化/復号化の相乗効果は故障検知用のチェックサム、トレードオフは遅延⇄セキュリティレベル）。またSESAMO (2014)では、SaSの収束への道は統一されたプロセスよりもむしろ別々のセーフティ解析とセキュリティ解析のプロセス間の相互作用の接点の定義にあると結論

a 最新版は ISO/IEC 27005:2018

を出している[24]. つまり並行して実施したセーフティ解析とセキュリティ解析のそれぞれの結果を適宜整合する, ということである. 最終的な目標はセーフティとセキュリティの統一プロセスであるが, 他の標準化コミュニティに対する現実的なアプローチが必要であり, いくつかの標準化団体で採用されている明確に定義された相互作用の接点で整合することが現在の現実的なアプローチであることを述べている.

Cherdantseva ら(2015)[25]は, 2004 年から 2014 年間の SCADA のリスクアセスメントをカバーする論文の数を調べたところ, 1 年あたり 0~4 件の間で変動し, 経時的な論文数の顕著な増加は見られないことを報告した. 特徴として, リスクアセスメントでは定性的よりも定量的な手法が大部分であり, かつ確率的なものが殆どであった. また数学的に解析する数式ベースのものよりもグラフィカルに解析するモデルベースのものが大部分であり, かつ肯定的結果に焦点を合わせたゴール指向 (例: GSN (Goal Structuring Notation) [26]) よりも否定的結果に焦点を合わせた攻撃・故障指向 (例: ATA (Attack Tree Analysis) [27], FTA(Fault Tree Analysis)[21]) が殆どであった.

Abulamddi (2016)[11]は, 複数の論文をサーベイし, セーフティとセキュリティの手法 (HAZAP[28]やグラフモデル [11]の改良について) とセーフティ手法 (スイスチーズモデル[11], AcciMap[29], STAMP[29]) を紹介した. グラフモデルの 1 つであるミスユースケース[30]はユーザインタラクションに関連した故障モード分析において FMEA よりも容易で混乱が少ない利点があるが, システム内部動作関連の故障モードの詳細分析には FMEA の方が適していることを述べている. その中でセキュリティ要求とセーフティ要求に対して, 体系的かつ概念的な技術とアプローチの統合を必要とし, そのモデルとツールは様々な観点から注目されていることを述べている (例: アーキテクチャのフレームワーク, セーフティとセキュリティの両方における定義と用語の間のギャップを狭くすること, システムの開発ライフサイクルで使用される技術要件とツールを絞り込むこと).

MERgE ITEA2 Project (2016) [18]は, 1989 年から 2016 年までのセーフティとセキュリティの両方の技術専門分野を明示的に扱った論文のみを対象とした調査を行った. 2000 年までは活発ではなかったが 2001 年の米国同時多発テロの翌年から増え始め, 2010 年の Stuxnet の影響で 2012 年から更に増加しセーフティおよびセキュリティの専門家がお互いを無視することができなくなっている状態である. セーフティとセキュリティの関連問題に対して論文を調査したところ, ①自専門分野だけで個別に論じたもの, ②セーフティとセキュリティの相互交流でセーフティまたはセキュリティを改善したもの, ③両専門分野を仲間と考え偏見なしに論じたもの, の 3 つに分けた. ①は「セキュリティ

のないセーフティ工学」または「セキュリティを分けたセーフティ工学」を論じたものである (セキュリティのないセーフティシステムが攻撃を受けても, フェールセーフな状態に入る傾向があり安全である等). 分野固有 (交通, 産業, 自動車等) で採用されたものが多い. ①は改善の余地があると主張しているが, 具体的な方策は述べられていない. そのため①は推奨できないにも関わらず論議が減らないことに驚いている. これは②③を含めて全体的に研究が活発であることを示している.

Chockalingam ら(2017)[14]は, 近年セーフティとセキュリティの研究者の間でリスクマネジメント分野において協力する動きがあるが, 包括的なレビューが足りないことを指摘した. そこで統合化したセーフティとセキュリティのリスクアセスメントの手法の主な特徴が何であるかを研究課題として取り組んだ. セーフティとセキュリティの関連の論文を検索した後に, 制御システムを含む少なくとも 1 つの実例にすでに適用されていると思われるもの, リスクアセスメントのプロセスを含んでいるものを選別し, 7 つの統合手法を厳選し分析した. この中で, EFT[31], Extended CFT[32], FACT Graph[33]は FTA と ATA を含んだ手法である. 2016 年までの引用数は EFT(63 件)が最も多く次に Extended CFT(17 件)である. リスク管理のプロセスをリスク特定・リスク分析・リスク評価とした場合, リスク評価を行っている手法は 1 つだけであり, 殆どの手法がリスク特定およびリスク分析に集中していることを述べている.

Lisova ら(2018) [19]は, 2012 年から 2017 年までのセーフティとセキュリティの関連の論文を検索して 13,711 件抽出しタイトル・概要・内容を調査して厳選しセーフティとセキュリティの相互作用に対処する分析方法と対処方法を含んだ 33 の論文を特定した. 論文の全体の数は 2012 年から 2017 年まで増え続けている. セキュリティ情報に基づくセーフティの研究は 2015 年がピークであるが 2017 年に再び増加し, セーフティとセキュリティを組合せた研究は 2017 年まで増え続けており, セーフティとセキュリティの統合に関する研究は発展途上であると結論付けている.

これらの研究報告から, 詳細な研究内容については多少の増減があるもののセーフティとセキュリティの関連研究全体はまだ活発な状態であること, セーフティとセキュリティの各専門家間のコミュニケーションが必要でありセーフティとセキュリティの新たな統合手法や, 解析結果の整合方法についてはまだ議論の余地はあること, また統合手法としては FTA と ATA を含んだ手法が多いことがわかった.

### 3.2 業界の現状

SaaS の研究を最もけん引している分野は自動車分野(輸送分野)であり, 電力および公益事業分野, 医療分野と続いている[18] [19]. Lisova ら(2018)は, 標準との関連性はほとんどすべての場合, 対象とするアプローチの適用分野に直

接関連している。特に多くの論文が自動車分野における SaS 問題に取り組むことを目的とし自動車分野における電気・電子システムの機能安全のための国際規格である ISO26262 規格を使用し、続いてあらゆる分野および産業制御システム分野に適用可能な一般的アプローチを採用していることを指摘している[19]。自動運転技術の発展、かつインシデントやアクシデントが人の命や身体の危機に直結する分野でもあるため[34]、自動車分野を中心に研究が進められていることがわかる。

### 3.3 標準化の動向

SaS に関連する国際標準化団体として、セーフティ分野では、制御系安全を扱う IEC/TC65, 機械安全を扱う IEC/TC44, ISO/TC199 がある[35]。セキュリティ分野では ISO/IEC JTC1 SC27, ISO/IEC JTC1 SC41 がある。全体的に SaS に関してはセーフティの規格での動きは活発であるが、セキュリティの規格では大きな動きは見られない。ここでは SaS に関して活発に動いている IEC/TC65 と IEC/TC44 について述べる[7]。

#### (3) 制御系安全を扱う IEC/TC65,

機能安全の IEC61508:2010 を手本に制御セキュリティとして IEC62443 にコンポーネントレベルのセキュリティが下記のように入っている。

- サイバーセキュリティを対象とする IEC 62443-2-1 (CSMS 認証)
- 組込デバイスのセキュリティを対象とする IEC 62443-4-1, 2 (EDSA 認証)

しかし機能安全と制御セキュリティには類似点だけでなく相違点もあるため、日本が提案国になり安全・セキュリティ連携規格の開発に着手 (IEC TR63069: 一般的制御システムにおける安全とセキュリティの分析・対応)した。これは SaS の並行分析を目指したものである。

#### (4) 機械安全 (IEC 側) を扱う IEC/TC44

セキュリティの機械の SRCS (Safety Related Control Systems)への影響は TC44 が主体となって作るべきだと考えており、IEC TR63074 (安全性に関する機能安全に関するセキュリティコントロールシステム関連) という規格に着手している[7][36]。これは安全分析そしてセキュリティ分析という SaS の順次分析を目指したものである。

## 4. SaS 統合手法の種類

3 章での論文からセキュリティおよびセーフティの手法を調べ、その中から代表的な手法を3つのグループに分けて下記に記す。

### (1) セーフティ分野の手法

- ・ FMEA (Failure Mode and Effects Analysis)[21]
- ・ FTA (Fault Tree Analysis)[21]
- ・ CFT (Component Fault Tree)[37]
- ・ HAZOP (HAZard and OPERability Study)[38]

- ・ What-If[38]
- ・ LOPA[38]
- ・ AcciMap[29]
- ・ FRAM[39]
- ・ STAMP-STPA[40]

### (2) セキュリティ分野の手法

- ・ ATA (Attack Trees Analysis)[27]
- ・ STRIDE[22]
- ・ Misuse cases[30]
- ・ NIST SP800-30[41]
- ・ ACT (Attack-Countermeasure Trees)[42]
- ・ STPA-Sec[46]

### (3) SaS 分野の手法

- ・ FMVEA[23]
- ・ Extended CFT[32]
- ・ EFT[31]
- ・ SAHARA[43]
- ・ CHASSIS[44]
- ・ FACT Graph[33]
- ・ Unified Security and Safety Risk Assessment method (Extended NIST SP800-30)[45]
- ・ STPA-SafeSec[46]
- ・ その他(BDMS, MILS, D-MILS, AADL, SysML, GAE, BPMN, BBN, SafSec, S-cube, NFL, IFD (Information Flow Diagram), extended TVRA (Threat Vulnerability and Risk Assessment)等)[14][18][19][25]

上記の(3)が本稿の対象の手法である。この手法の種類には SIS の手法、形式手法や包括的アプローチ、要求工学アプローチ (要求の抽出, 解析, および SaS 間の不整合解決) なども含んでいる。

## 5. SaS 手法の既存の問題と課題

4 章で上げた SaS 統合手法の既存の問題と課題について述べる。

### 5.1 SaS の最適な解析が並行か統合かの検討が不十分

Lisova ら(2018) [19]は、SaS でのセキュリティとセーフティの解析のやり方について下記の分類をしている。

#### 1. 統一 (Unified) アプローチ

解析中にそれらの相互依存性を扱うセーフティとセキュリティの共同解析 (例: SAHARA, extended NIST SP800-30, FMVEA, CHASSIS, STPA-Sec)

#### 2. 並行 (Parallel) アプローチ

セーフティ解析とセキュリティ解析を並行(別々に分けて解析)して行う (調和させるための整合活動を必要とする) (例: IFD, extended TVRA)

SaS の解析は並行よりも統合の方が良いといわれているが、本当にそうであるのか議論されていない。並行の場合、新

たなハザードや脆弱性をもたらす矛盾する要件につながる可能性があり、またセーフティとセキュリティの相互依存から生じるハザードや脅威を見逃す可能性があるが、具体的に統合と並行の差について述べた論文は見つけられなかった。ISO 26262 と SAE J3061 への準拠など、規格への準拠が最も重要である分野では、特に詳細まで分析する場合、SaS 統合手法を使う上での制約があり統合ではなく並行にせざるを得ないが[24]、もし並行で問題がなければ無理に統合する必要はない。また規格に特化したソリューションやフレームワーク、または意思決定者がいくつかの選択肢があるのであれば、その中から最良の選択肢を選択することを助けるための多基準意思決定支援 (MCDA) 技術などを使用することも提案されているが、その効果については今後の検討課題である。

### 5.2 社会的な問題へ対応した手法の機能がいない

セーフティでは、技術的な事故、ヒューマンエラーを含む個人的な事故、組織事故 (社会的問題も含む)、機能共鳴事故に対応する手法が生み出されてきた[11]。またセキュリティでは、標的型攻撃やハイブリッド攻撃などサイバー戦争に関わるソーシャルエンジニアリングを駆使した社会的な問題 (個人、組織も含む) も出てきている[47]。セーフティでもセキュリティでも社会的な問題に対応せざるを得なくなっているが、論文を見ても技術的な問題が主であり、社会的な問題に対応する手法については殆ど議論されていない。セーフティでは AcciMap が社会的問題に対処した機能を持つ手法であるが、セキュリティの社会的問題を考慮した機能を持つ手法は見つけることができなかった。代わりにセキュリティでは国や関連機関の責任を明確化した法律の制定 (例: サイバーセキュリティ基本法[48]) や組織の枠組み (例: 金融 ISAC[49]) でセキュリティの社会的問題に対処している。リスク特定の対象範囲外と言って切り捨てることも可能であるが、技術の問題が背後要因を辿ると個人、組織、社会の問題に行き着く場合もある。根本的に解決するには技術だけでは不十分であり上流の社会的問題に対処せざるを得ない場合もある。Bloomfield ら (2018)は、鉄道分野と自動車分野における codes of practice (CoPs) を開発し、「構成するすべての組織がトランスポーションシステムのユーザと社会全体に対して安全性リスクを最小化すること」ということで社会全体を含めたリスクにまで言及している[17]。社会的問題を考慮した手法について更に検討が必要である。

### 5.3 動的リスクアセスメントに関する手法の機能がいない

SaS の不整合解決の方法について議論していたが、セキュリティ重要システムを特徴づける効率的な「システム更新処理に対するサポートの評価」を欠いていることを指摘している論文が複数存在している[14][19]。セキュリティの動的な性質とそのセーフティへの影響に関するこのような重要な問題に焦点を当てていないこと、将来的により効果

的にするために対処される必要がある動的リスクアセスメントを実行するためにリアルタイムのシステム情報を考慮に入れた機能を手法に持たせる必要がある。

### 5.4 未検討の分野があり SaS の検討範囲が不十分

Lisova ら(2018)[19]は SIS (Security Informed Safety : セキュリティを考慮した安全性) の対称となる「セーフティを考慮したセキュリティ (Safety informed Security)」アプローチの研究を見つめることが出来なかった。そのため「セキュリティに対するセーフティの影響の分析をカバーしておらず、多くの研究が提案アプローチと方法論の広範な評価を欠いていることを示している」と結論している。この結果より、SaS の分野は他にもまだ未検討の分野がある可能性がある。

## 6. 新たな問題と課題の抽出

5.4 節から SaS の分野にはまだ未検討の分野が残っている可能性があるため、さらに調査する価値がある。そこで新たな分類方法を考えこととした。Cherdantseva ら(2015) [25]は、SaS のリスク評価方法の分類の一つとして下記を提示している。

- ・ 数式ベース (リスクの数学的モデル)
  - ・ モデルベース (グラフィカルモデル)
- そして上記のモデルベースを2つに分けていれる。
- ・ 肯定的結果に焦点を合わせたゴール指向 (例: GSN)
  - ・ 否定的結果に焦点を合わせた攻撃・故障指向 (例: ATA, FTA)

ここで注目したことは、ゴール指向はアシュアランスケース[26]であり保証のための構造化された議論の記述法という認識であるが、Cherdantseva らはゴール指向を肯定的アプローチ、攻撃・故障指向を否定的アプローチと新たな見方を提供したことである。この分類を FTA のようなトップダウン、FMEA のようなボトムアップおよび HAZOP のようなガイドワードの観点をいれてさらに分類すると表 1 のようになる。

表 1 手法が存在しない分野

アプローチ	トップダウン	ボトムアップ	ガイドワード
肯定的	GSN,D-Case 等	①存在しない	②存在しない
否定的	FTA, ATA 等	FMEA , FMVEA 等	HAZOP, STRIDE 等

表 1 から、①肯定的かつボトムアップの手法、および②肯定的かつガードワードの手法が抜けていることを今回発見した。つまり①②の分野は未検討の分野であり今後の検討が必要である。①②の分野の肯定的アプローチは興味深いものであり、似た考え方としてホルナゲル[50]のレジリエンス工学の Safety- I と Safety- II がおり下記の通りであ

る。

- ・ Safety-I 「物事が悪い方向へ向かわない状態」
- ・ Safety-II 「物事が正しい方向へと向かうことを保証する」

Safety-I を否定的アプローチ, Safety-II を肯定的アプローチと同じであると仮定すると, ①や②の手法を実施することで正しい方向への保証を行いながら新たな価値が出てくる可能性がある。様々な悪い要因が含まれている場合でも良い要因を増やすことで容認できない状態に行かないように制御していくということである。

例えば①の手法としては, サプライチェーン攻撃のようにシステムにマルウェア等の悪意のある要因が含まれていても, それを防御する安全施策を下位レベルから複数用意し, 活動を制御することで安全を保つというやり方が考えられる。②の手法では, セーフティやセキュリティを保持しようとするキーワードを基に, リスク分析やリスク対応に役立てることなどが考えられる。また, これらの手法をリスクマネジメントのプロセスのどの部分に適用することが適切なのか, 統合することでより相乗効果が出てくるのか, など様々な検討が必要である。

## 7. おわりに

SaS 関連の手法の種類が非常に多く, 現在でも新たな手法が出現している。既存の SaS 間の問題や課題も解決できていないところも残っており, 同時に未検討の分野も存在している。これらの分野について新たな検討が必要となる。今後はこれらの問題や課題を検討し新たな手法を提案していくことを考えている。

## 参考文献

[1] “That 'Internet of Things' Thing”.  
<http://www.rfidjournal.com/articles/pdf?4986>, (参照 2019-01-18).

[2] Brian Russell, Drew Van Duren. Practical Internet of Things Security. Packt Publishing, 2016.

[3] Khaitan et al. Design Techniques and Applications of Cyber Physical Systems: A Survey. IEEE Systems Journal, 2014.

[4] “Society 5.0”. [http://www8.cao.go.jp/cstp/society5\\_0/index.html](http://www8.cao.go.jp/cstp/society5_0/index.html), (参照 2019-01-18).

[5] “Five nightmarish attacks that show the risks of IoT security”, <http://www.zdnet.com/article/5-nightmarish-attacks-that-show-the-risks-of-iot-security/> (参照 2019-01-18).

[6] “サプライチェーンマネジメントとは? 攻撃リスクを回避する7つの対策”. <https://blogs.mcafee.jp/scrm-risk-prevention>, (参照 2019-01-18).

[7] 神余浩夫. ②機能安全と制御セキュリティの標準化動向. 情報処理学会学会誌, Vol.58 No.11 Nov. 2017.

[8] 田口研治. ①IoTの伸展に伴うセーフティとセキュリティのリスクと課題. 情報処理学会学会誌, Vol.58 No.11 Nov. 2017

[9] 金川信康, 山田 勉. 社会インフラストラクチャを支える制御システムにおけるセーフティとセキュリティ. 情報処理学会学会誌, Vol.58 No.11 Nov. 2017.

[10] SESAMO. Security and Safety Modelling. D2.1-Specification of Safety and Security Mechanisms, version 01, 2013.

[11] MOHAMMED F. H. ABULAMDDI. A SURVEY ON CHNIQUES

REQUIREMENTS FOR INTEGRATING SAFETY AND SECURITY ENGINEERING FOR CYBER-PHYSICAL SYSTEMS. JCSES, Vol.7, No.6, 2016.

[12] 日本工業規格. 安全側面-規格への導入指針. JIS Z8051:2015 (ISO/IEC Guide51:2014), 2015.

[13] 日本工業規格. 情報技術-セキュリティ技術-情報セキュリティ管理策の実践のための規範. JIS Q27002:2014 (ISO/IEC 27002:2013), 2014.

[14] Sabarathinam Chockalingam. et. al.. Integrated Safety and Security Risk Assessment Methods: A Survey of Key Characteristics and Applications. Cornell University Library, 2017.

[15] 日本工業規格. リスクマネジメント-指針. JIS Q31000:2019 (ISO 31000:2018), 2019.

[16] “ISOIEC 27000 ファミリー規格の最新動向”.  
[https://www.jnsa.org/seminar/2018/1207/data/2018\\_resume1.pdf](https://www.jnsa.org/seminar/2018/1207/data/2018_resume1.pdf), (参照 2019-03-21).

[17] “セキュリティを考慮した安全性”.  
[https://www.bcm.co.jp/bcm/wp-content/uploads/2018/10/yamamoto\\_03.pdf](https://www.bcm.co.jp/bcm/wp-content/uploads/2018/10/yamamoto_03.pdf), (参照 2019-03-20).

[18] MERgE ITEA2 Project. Recommendations for Security and Safety Co-engineering. MERgE ITEA2 Project # 11011, 2016.

[19] Elena Lisova et. al.. Safety and Security Co-Analyses: A Systematic Literature Review. IEEE SYSTEMS JOURNAL, 2018.

[20] Piètre-Cambacedes, et al.. Cross-fertilizations between safety and security engineering. Reliability Engineering & System Safety, Elsevier, Vol. 110, pp. 110-126, 2013.

[21] 鈴木順二郎他. FMEA・FTA 実施法. 日科技連出版社, 1987.

[22] Shawn Hernan et. al.. Uncover Security Design Flaws Using The STRIDE Approach. MSDN Magazine, 2006.

[23] Christoph Schmittner et. al.. Security Application of Failure Mode and Effect Analysis (FMEA). Springer-Verlag, SAFECOMP 2014.

[24] SESAMO. D4.2-Integrated Design and Evaluation Methodology Version 01, 2014.

[25] Yulia Cherdantseva. et. al.. A review of cyber security risk assessment methods for SCADA systems. elsevier, computers & security56 (2016) 1-27, 2016.

[26] “アシュアランスケース入門”.  
<https://www.ipa.go.jp/files/000043906.pdf>, (参照 2019-03-20).

[27] “Attack Trees”.  
[https://www.schneier.com/academic/archives/1999/12/attack\\_trees.html](https://www.schneier.com/academic/archives/1999/12/attack_trees.html), (参照 2019-03-20).

[28] 日本規格協会. リスクマネジメント-リスクアセスメント技法. JIS Q31010:2012, 2012.

[29] 小松原明哲. 事故分析のためのヒューマンファクターズ手法. 海文堂出版, 2016.

[30] “Capturing Security Requirements through Misuse Cases”.  
<http://www.nik.no/2001/21-sindre.pdf>, (参照 2019-03-20).

[31] Shengwei Yi et. al.. A safety-security assessment approach for Communication-based train control (CBTC) systems based on the extended fault tree. 27th ICCCN, 2018.

[32] Max Steiner et. al.. Combination of Safety and Security Analysis – Finding Security Problems That Threaten The Safety of a System. HAL Id: hal-00848604, 2013.

[33] Giedre Sabaliauskaite et. al.. Aligning Cyber-Physical System Safety and Security. Springer, CESAMES2014 pp.41-53, 2014.

[34] IPA. セーフティ設計に関する実態調査結果, 2015.

[35] “機能安全を実現する安全制御システムにおけるセキュリティについての標準化の動き”.  
[http://www.jmf.or.jp/content/files/hyoujunka/hyo201711\\_04.pdf](http://www.jmf.or.jp/content/files/hyoujunka/hyo201711_04.pdf), (参照 2019-03-20).

[36] “IEC 規格ドラフトの状況”.  
[https://jema-net.or.jp/Japanese/standard/iec\\_draft.html](https://jema-net.or.jp/Japanese/standard/iec_draft.html), (参照 2019-03-20).

[37] B. Kaiser et. al.. Bdd complexity reduction by component fault

- trees. ESREL 2005, Balkema Publishers, pp.1011-1019, 2005.
- [38] 日本規格協会. リスクマネジメントーリスクアセスメント技法. JIS Q31010:2012, 2012.
- [39] エリックホルナゲル著, 小松原明哲訳. 社会技術システムの安全分析 FRAM ガイドブック. 海文堂, 2013.
- [40] “はじめての STAMP/STPA”.  
<https://www.ipa.go.jp/files/000051829.pdf>, (参照 2019-03-20).
- [41] “NIST Special Publication 800-30Revision 1 リスクアセスメントの実施の手引き”. <https://www.ipa.go.jp/files/000025325.pdf>, (参照 2019-03-20).
- [42] Arpan Roy et. al.. ACT: Attack Countermeasure Trees for Information Assurance Analysis. In Proceedings of INFOCOM IEEE Conference on Computer Communications Workshops, pp.1-2, 2010.
- [43] Georg Machera et. al.. Threat and Risk Assessment Methodologies in the Automotive Domain. Elsevier, Procedia Computer Science 83, pp.1288 – 129, 2016.
- [44] “Addendum to: “Combined Assessment of Software Safety and Security Requirements An Industrial Evaluation of the CHASSIS Method””.  
<http://bora.uib.no/bitstream/handle/1956/16161/CHASSIS-appendix-final-11.pdf?sequence=1&isAllowed=y>, (参照 2019-03-20).
- [45] Yean-Ru Chen et. al.. Unified Security and Safety Risk Assessment- A Case Study on Nuclear Power Plant. IEEE, 2014 International Conference on Trustworthy Systems and their Applications, 2014.
- [46] Ivo Friedberg et. al.. STPA-SafeSec: Safety and security analysis for cyber-physical systems. ELSEVIER, Journal of Information Security and Applications 34, pp.183-196, 2018.
- [47] “サイバー攻撃と詐欺を掛け合わせた「ハイブリット攻撃」その手法と具体的対策とは”.  
<https://cybersecurity-jp.com/cyber-terrorism/25141>, (参照 2019-03-20).
- [48] “サイバーセキュリティ基本法”.  
[http://elaws.e-gov.go.jp/search/elawsSearch/elaws\\_search/lsg0500/detail?lawId=426AC1000000104](http://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=426AC1000000104), (参照 2019-03-20).
- [49] “一般社団法人 金融 ISAC”. <http://www.f-isac.jp/index.html>, (参照 2019-03-20).
- [50] “Safety- I から Safety- II へーレジリエンス工学入門ー”.  
[http://www.orsj.or.jp/archive2/or59-08/or59\\_8\\_435.pdf](http://www.orsj.or.jp/archive2/or59-08/or59_8_435.pdf), (参照 2019-03-20).