



# ① IoT の進展に伴うセーフティとセキュリティのリスクと課題

田口研治（国立研究開発法人産業技術総合研究所／（株）シーエービテクノロジーズ）

## IoT 進展に伴うリスクと課題

現在、世界中でモノがインターネットにつながる IoT（Internet of Things）システムが開発され稼働している。しかし、IoT 機器の中には、サーバに不正な通信を大量に送ることでサービスを不能にする DDoS（Distributed Denial of Services）攻撃の踏み台として利用されるなど、さまざまなインシデントが発生している。IoT 機器の中には、自動車、航空機、プラント制御など、安全性が重要視される（Safety Critical）システムがある。これらのシステムに対して、セキュリティ上の不具合（脆弱性）に対する攻撃により、不正な動作を引き起こし、システムの安全性が侵害され、資源、環境、人への損害が生じることが重大な問題となっている。

IoT 機器を導入することにより、より安全な環境を構築することは可能である。たとえば、故障の早期検知のためのモニタリング機能を IoT 機器により実現することで、故障の検知を可能にするのは 1 つの例である。それに対して、IoT 機器の脆弱性から、安全性への侵害が起こることが危惧されているように、両者は互いに影響しあう関係といえる。相互の関係を考慮し、両システム特性を満たすシステムを開発するための方法論「安全とセキュリティのコエン지니어リング（Safety and Security Co-engineering）」の開発が必須である。本稿においては、安全とセキュリティの両者を扱う際の課題、その解決へのアプローチを、システム開発の初期段階に絞って解説をし、さらに今後の展望について示す。

## 安全機構

自分の PC がウィルスに感染し、標的型攻撃の対象になった経験や、利用しているサーバのアカウントを乗っ取られた経験がある読者は相当数いると思われる。このような場合は、システムの安全性が侵害されたとはいわない。安全性が重要視されるシステムにおいては、故障やヒューマンエラーによる誤操作などによりハザード（たとえば、電車の脱線、衝突や、航空機の墜落）が生じないように、さまざまな安全機構が設計、実装されている。代表的なものとしては、冗長系（主要な装置である、記憶回路、通信経路などを多重化）や、1oo1D（1 out of 1 channel architecture with diagnostics）といった制御用チャンネルと故障診断用チャンネルに 1 つの出力を持つ安全機構がある。このような安全機構を用いると、制御用チャンネルにおいて故障が発生しても、故障診断用チャンネルで故障を検出することが可能になる。しかし、セキュリティ上の攻撃により、自動車の制御が奪われた場合には、必ずしも安全機構により防ぐことができないため、セキュリティ機構を導入するのが通常の対処方法である。

## インシデント例

2000 年、オーストラリア、マルーチーにおける下水処理場において起こったセキュリティのインシデントにおいては、3 カ月の間、インシデントの発生は検知されていたが、セキュリティの侵害であることが分からず、安全上の重大な被害が生じた。下水処理場の監視制御用の SCADA（Supervisory Control And Data Acquisition）システムは、汚水処理の管理のための 300 ノード（142 のポンプス

ーション) から構成され、無線による制御を行っていた。犯人は、ラップトップ PC と無線送信機、盗んだ SCADA 制御ソフトを利用して、システムの制御を妨害していた。この例では、システム制御に関する障害に対して、それがセキュリティからの侵害によることが判明するまで時間がかかった、と考えられる。

自動車業界においては、セキュリティ上の問題から起こった最初のリコールとして記憶されているのが、FCA (Fiat Chrysler Automobiles) 社のジープのリコールである。元々は、C. Miller と C. Valasek<sup>1)</sup> による遠隔からのハッキングにより自動車の制御が奪われたレポートに起因するものである。このハッキングにおいては、車の外部から遠隔操作に成功している。後述するが、この例は、セーフティとセキュリティの関連で見ると、別の様相が見えてくる事例である。

## 🔒 安全性とセキュリティの関係

自動車は、ECU (Electronic Control Unit) により制御されており、1 台の自動車に 50 ~ 100 の ECU が利用されている。ECU はエンジン制御、サスペンション制御、エアコンなど、さまざまな用途に利用されている。前述のジープの遠隔ハッキングの事例においては、制御の乗っ取り方法としては、1 つの ECU になりすますために、その ECU を診断セッションに推移させ、動作を止め、その後、その ECU のメッセージのなりすましを行った。

しかし、このハッキングの方法の制限としては、診断セッションに遷移するのは、自動車が低速時だけであった。つまり、ECU には、車が高速に走行している際に、あやまって診断モードに落ちないように安全機構を持っており、そのために、車速がどのようなときでもハッキングが成功したわけではなかった。すなわち、安全機構により、セキュリティからの侵害をある程度防ぐことができた事例である。

安全性とセキュリティは、システムの非機能特性として、互いに相反する場合があります。双方を満足するシステムを開発するためには、開発におけるさま

ざまな段階において、配慮が必要になる。ヨーロッパの研究プロジェクト SESAMO (Security and Safety Modelling)<sup>2)</sup> においては、安全要求とセキュリティ要求の相互干渉に対する分析から、そのトレードオフと統合 (両者の特性を利用して、双方に役立つようにすること) について研究が実施された。そこでは、暗号化・復号化、署名生成と検証、ノード認証、アクセス制御・トラフィックフィルタリング、といった 18 の代表的なセキュリティ機能に対して、双方の影響分析を行っている。以下の表-1 に、暗号化・復号化に対する分析例を示す。

制御システムにおいては、セーフティ確保のために与えられた、処理時間に対するリアルタイム制約が存在する。しかし、通信データの盗聴、なりすまし、改竄を防ぐために暗号技術を導入すると、リアルタイム制約を満たさない可能性がある。表-1 において、遅延とされている記述がそれにあたる。それに対して、暗号化・復号化は秘密鍵の長さにより、セキュリティの強度が異なる点は、セキュリティのレベルという点で示されている。両者のトレードオフとしては、安全側から見ると、処理の遅延が問題となり、セキュリティ側から見ると、セキュリティ上の強度の問題があることが示されている。両者の統合に関しては、暗号学的チェックサムは、符号誤りの検知に利用可能なので、セキュリティ機能が安全機能としても利用可能であることを示している。

IoT 機器を開発する場合には、このような安全性とセキュリティのトレードオフを分析し、バランスの取れた機器の開発が望ましいことはいうまでもないが、それにより、IoT 機器を用いたシステムが全体として、安全性とセキュリティの担保が可能かどうかは別の課題である。

|        | セーフティ                          | セキュリティ                               |
|--------|--------------------------------|--------------------------------------|
| トレードオフ | 遅延<br>暗号・復号化のための計算量は暗号鍵の長さに依存。 | セキュリティのレベル<br>セキュリティのレベルは、暗号鍵の長さに依存。 |
| 統合     | 暗号学的チェックサムはフォルトの発見に役立つ。        |                                      |

表-1 SESAMO のトレードオフと統合の例

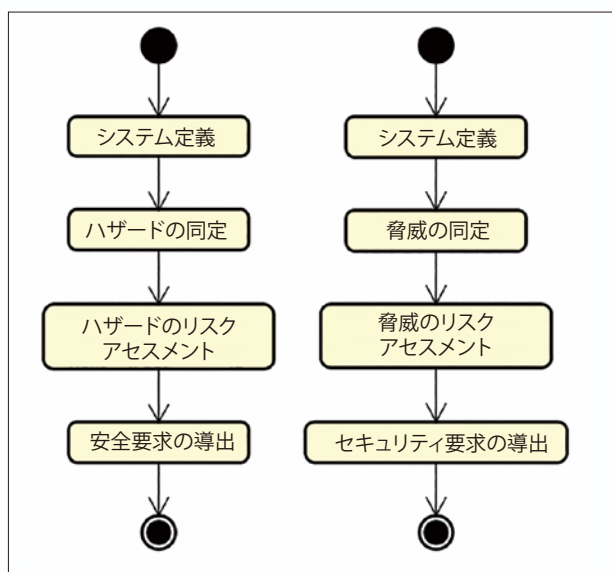


図-1 安全とセキュリティの初期段階（基本形）

## 解決へのアプローチ

安全性とセキュリティの相互影響を考慮・分析し、双方の特質を活かしたIoT 機器を開発するための課題のうち、「開発ライフサイクルの統合」と「安全・セキュリティ分析」について解説を行う。

### 開発ライフサイクル

安全性が重要視されるシステムにおいては、機能安全規格が策定されており、それらに規定された開発ライフサイクルに準拠する必要がある。さらに、サイバーセキュリティに関する規格が徐々に整理されている（例：自動車の機能安全 ISO 26262, サイバーセキュリティ J3061, 航空機の安全 ARP 4754A, セキュリティ DO-326A）。

しかし、それらの規格においては、安全側の開発ライフサイクルとセキュリティ側の開発ライフサイクルをどのように統合するか（同時に実施するか）については明確でない場合が多い。双方の開発ライフサイクルをどのように統合するかにより、製品の品質、開発コスト、開発期間などに大きな影響が出ることが予想される。

プロセスの統合において考慮すべき点を、図-1で示される、開発ライフサイクルの初期において実施される安全分析と脅威分析の段階を例に示す。

図-1の右側がセキュリティ側の脅威分析における一般的な開発の流れであり、「システム定義」において、システムに関する情報（機能仕様、アーキテクチャ情報、他）を入手し、それから「脅威の同定」を行い、そのリスクを何らかの評価基準により実施し、セキュリティ要求を導出するものである。

左側は安全分析を行うものであり、システムに関する情報は、セキュリティ側と同様な情報が与えられ、その後、故障の原因となるハザードに対する、「ハザードの同定」を行い、そのリスクを何らかの評価基準によりアセスメントをし、そのハザードに対抗する安全要求を導出するものである。

筆者らは、安全とセキュリティの開発ライフサイクルを統合する際のさまざまな場合を考慮し、パターン化を行った<sup>3)</sup>。パターン化の観点には、成果物が参照される場合の参照関係があるかどうか、片方の開発段階において他方が含まれるかどうか、相互の影響により異なる成果物を生成するかどうか、といった点である。

- 1) 片方がもう片方を参照（片方向参照型）
- 2) 片方がもう片方を包含（従属型）
- 3) ある時点で、双方の成果物に対してトレードオフの実施（相互関連型）

以下に、1) と 3) について示す。図-2の片方向参照型においては、安全とセキュリティの双方において、唯一影響を及ぼす個所として示されているのが、安全で同定されたハザードをセキュリティ側で参照し、脅威の同定に利用する個所である。

つまり、安全側で同定されたハザードに対して、そのハザードを引き起こす脅威があるかどうかを分析するために行われる。本プロセスパターンは、DO-326A に示されているものである。

次に示すプロセスパターン（図-3）は、前章で解説した SESAMO<sup>2)</sup>におけるトレードオフの関係を示したものであり、安全要求とセキュリティ要求が導出された後に、双方のトレードオフを実施することが示されている。このようなトレードオフは、要求間だけではなく、さまざまな開発段階において現れる。

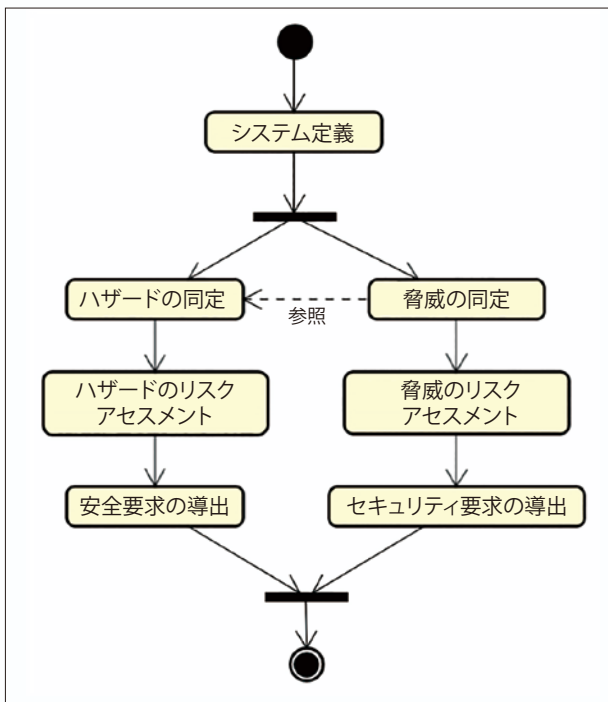


図-2 片方向参照型

では、このようなプロセス統合をするための分析手段、方法論はあるのだろうか。SESAMO においては、プロセス間で関連があるポイントをコネクションポイントと呼び、分析することを提案している。また、J3061 においては、コミュニケーションポイントと呼ばれているものである。これらは概念的なフレームワークを示したものであり、プロセスを統合する方法論を提示したものでない点は理解しておく必要がある。

実際に分析ができたとしても、そのプロセスを支援するための手法や方法論があるかどうか（たとえば、ハザードと脅威の関連の分析や、トレードオフの方法）、誰が実施するのか（安全側の人間か、セキュリティ側の人間か）などのさまざまな課題がある。

### 🔒 安全分析とセキュリティ分析

本章では、安全分析とセキュリティ分析の統合手法と、関連するリスクアセスメント方式の例を示す。

システムの安全性を保証するためには、どのようなハザードがあるかを分析し、そのリスクを評価するのが基本である。そのための手法としては、故障木 (FT (Fault Trees)) や、FMEA (Failure

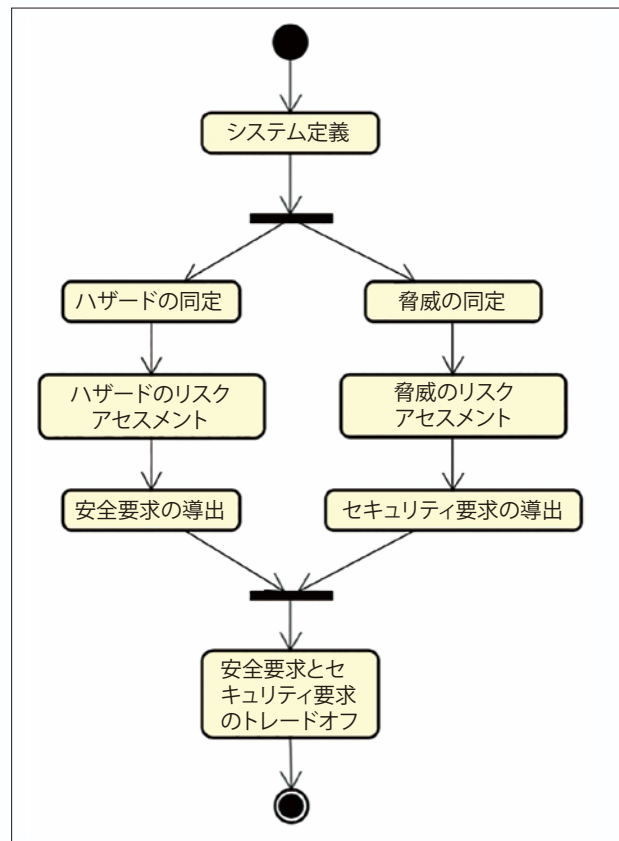


図-3 相互関連型

Modes and Effects Analysis) が知られている。故障木は、故障の原因、その組合せを、AND-OR 木 (AND と OR ゲートで記述されるブール代数式) で分析するものである。セキュリティにおいては、システムの脆弱性の分析や、脆弱性を用いた攻撃の分析を、FT と類似した攻撃木 (AT (Attack Trees)) により分析する手法がある。

安全側で同定されたハザードが実は、セキュリティ上の攻撃に起因する場合の分析に、FT と AT を組み合わせる手法が提案されている<sup>4)</sup>。図-4 は、FT の中に AT が記述されていることを示している。

ここで重要な点は、FT の一部として、ゲート記号 (図-4 における A) の下に、AT が現れる形はあるが、AT の中に FT は決して現れない (攻撃という、人為的な事象の原因に機械故障などが原因にならない) 点である。

FT と AT を統合した分析が可能なツール<sup>5)</sup> を用いて衝突事故に関する FT と AT を統合した分析例を示す (AT の部分はノードが二重線で表示)

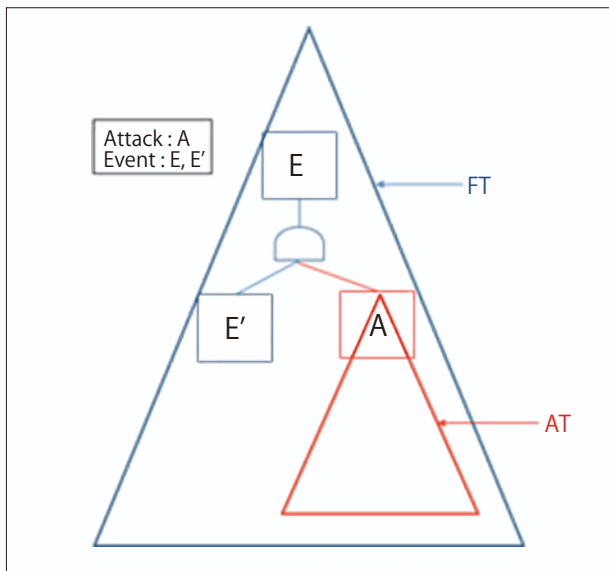


図-4 故障木と攻撃木を組み合わせた分析

(図-5). 本例は、衝突事故の原因として、ハードウェア故障（通信機器の故障）と、攻撃（なりすまし）がある場合を示している。

安全とセキュリティに関するリスクについては、独立していると考えられる場合、相互の影響を考える立場などさまざまであり、まだ定説は存在しない。

FTとATにおけるリスクアセスメント計算の例としては、FTではANDゲートは乗算、ORゲートは加算で計算されるが、ATでは、各々がmin, maxで計算されるやり方が、欧州におけるV2X（車とその他との通信）のセキュリティに関する研究プロジェクトEVITA<sup>6)</sup>において提唱されている。

それに対して、FTとATを統合した場合（図-5）において、リスクアセスメント計算を独立で行う方式としては、ATとFTの両方の値を対として各ノードで持ち、ゲートの演算を分配するやり方がある<sup>5)</sup>。

安全のリスクは、頻度×深刻度として計算されるのが一般的であるが、機能安全規格においてはISO 26262の、ASIL（Automotive Safety Integrity Level）などの評価基準が利用されている。セキュリティにおける評価基準は、情報システムに関する共通脆弱性評価システム（CVSS：Common Vulnerability Scoring System）や、セキュリティ規格

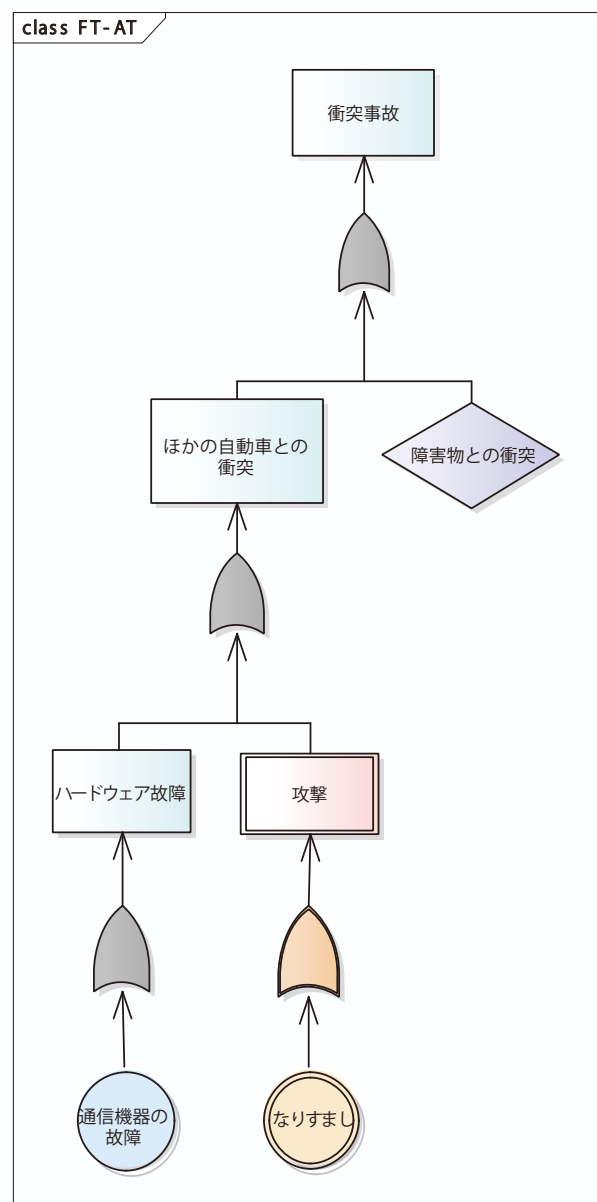


図-5 FTとATの統合による分析

であるISO/IEC 15408におけるCC/CEM（セキュリティ評価基準）などがある。

リスクグラフを用いて双方を統合したものが、EVITAで提案されている（表-2）。そこでは、ASILにおける評価軸である、運転手（もしくは歩行者）によるハザードに対する回避可能性、ハザードが発生した場合の被害の深刻度と、CC/CEMを元にした攻撃に対するリスクアセスメント評価である攻撃能力の組合せから、リスク値（ $R_i$ ）（ $i=0,1,2,3,4,5,6$ ）を決定している。

| 回避可能性 | 深刻度 (安全) | 攻撃能力 |     |     |     |     |
|-------|----------|------|-----|-----|-----|-----|
|       |          | A=1  | A=2 | A=3 | A=4 | A=5 |
| C=1   | S=1      | R0   | R0  | R1  | R2  | R3  |
|       | S=2      | R0   | R1  | R2  | R3  | R4  |
|       | S=3      | R1   | R2  | R3  | R4  | R5  |
|       | S=4      | R2   | R3  | R4  | R5  | R6  |
| C=2   | (省略)     |      |     |     |     |     |
| C=3   |          |      |     |     |     |     |
| C=4   |          |      |     |     |     |     |
| C=5   |          |      |     |     |     |     |

表-2 セキュリティと安全の統合リスク評価

## 今後の展望

本稿においては、IoT 機器に対する安全性とセキュリティの統合に関して、開発ライフサイクルと安全分析・脅威分析の観点からその課題と提案されているアプローチについて概観した。紹介したアプローチを含んだ研究開発は、現在、セーフティとセキュリティのコエンジニアリングという名称で、活発化している。その理由は、従来、安全が重要視されるシステムに対するセキュリティ侵害が現実のものとなり、安全性に重要な影響が出ることが認識され、両者を統合するための新たな方法論を開発する必要があることが広く認識されたことからである。現時点では、両方を理解しているエンジニア、研究者が少ないのが現状である。しかし、そのような状況も、徐々に改善されつつある。

このような新たな技術課題に対して、従来からの開発ライフサイクルや開発手法に対する影響や、両者を配慮した開発に対して、否定的な見方を持つ場合も考えられる。しかし、実際にさまざまな製品において相互の影響は無視できないものであり、製品の品質の向上や、新製品、新機能の開発の好機と捉え、取り組まれることを望むものである。

### 参考文献

- 1) Miller, C., et al. : Remote Exploitation of an Unaltered Passenger Vehicle (2015).
- 2) SESAMO : Security and Safety Modelling, D2.1-Specification of Safety and Security Mechanisms, version 0.1 (2013).
- 3) Taguchi, K., et al. : Safe & Sec Case Patterns, SAFECOMP Workshops ASSURE, pp.27-37 (2015).
- 4) Fovino, I. N., et al. : Integrating Cyber Attacks Within Fault Trees, J. Reliability Engineering and System Safety, pp.1394-1402 (2009).
- 5) <https://www.gaio.co.jp/iso/seculia>
- 6) Deliverable D2.3 : Security Requirements for Automotive On-board Networks based on Dark-side Scenarios (2008). (2017 年 7 月 31 日受付)

田口研治 ■ [kenji.taguchi@cav-tech.co.jp](mailto:kenji.taguchi@cav-tech.co.jp)

Uppsala 大学 (PhD in computer science). (株) シーイーブイテクノロジーズ代表取締役社長 (産業技術総合研究所招聘研究員併任). 車載セキュリティ, 特に脅威分析 (とツール開発) 等に従事.

