技術特集

組込みセキュリティ

組込みシステムセキュリティ委員会
副委員長　牧野　進二

1. はじめに

IoTによって現実社会(Physical)とサイバー空間(Cyber)を繋げることで得られるデータを活用し、新たな付加価値を創出することが求められている。例えば日本政府が進める「Society5.0、Connected Industries」では、データ主導の社会を作ることを目標に掲げている。

一方で、ここ数年でサイバー攻撃による事故が増加しており、2016年に起きたマルウェア MiraiによるDDoS攻撃、2016年に発生したCrashOverRideのサーバー攻撃によるウクライナでの停電、2017年に起きたランサムウェア WannaCryによる工場の生産ラインの停止などが記憶に新しい。

データ主導の社会にはセキュリティ対策が不可欠である。実際、自動車分野ではISO26262 SAE J3061、ISO/SAE21434など、産業機器ではIEC62443が策定され、組込み開発においてもセキュリティ対策が求められる時代になっている。

セキュリティに対する対策や事故発生時の対応の強化は世界的な動きである。例えば北米、欧州、中国ではセキュリティ関連の法律が施行がされているし、東南アジアなどでも法案の立案がされている。

日本も同様である。内閣府、経済産業省、総務省、厚生労働省などが、国内のセキュリティ対策の意識を高めるためのガイドラインや省令の改正を行っている。例えば経済産業省は、NIST(アメリカ国立標準技術研究所)の規格を参考としたサイバー・フィジカル・セキュリティ対策フレームワークを提唱している[1)]。

本特集では第1部でIoTとセキュリティについて概観した後、第2部でセキュリティを巡る世界・国内の動向、第3部で組込み製品開発にセキュリティ設計をプロセスとして組込む際の留意点を説明する。さらに第4部で運用視点でのIoTシステムのセキュリティ対策を述べる。最後の第5部では、組込み製品開発の設計をサポートするツール類を紹介する。

表1　IoTの４つの構成要素

構成要素	内　容	例
モノ（デバイス）	主体となる要素。物理的にセンサーを取り付けることができる物体を指す	クルマ、家電、スマホ、時計、工場の治具、フォークリフトなど
センサー	モノやモノの周辺の状態を感知し、データとして様々な状態を感知するセンサーを指す	モノの存在の有無、位置、重さ、圧力、速度、音声、振動、温度、湿度、匂い、電磁気、光など
通信手段	センサーが取得したデータを利用する機器に送る通信手段を指す。高速・大容量、低遅延、多数同時接続、長距離、低消費電力なものが求められる	Wi-Fi、Bluetooth、3G、4G LTE、5G、LPWA、Wi-SUN など
アプリケーション	センサーからのデータを統計分析し、人に利用し易いようにする情報処理を指す	データの抽出、整理、解析、最適化など

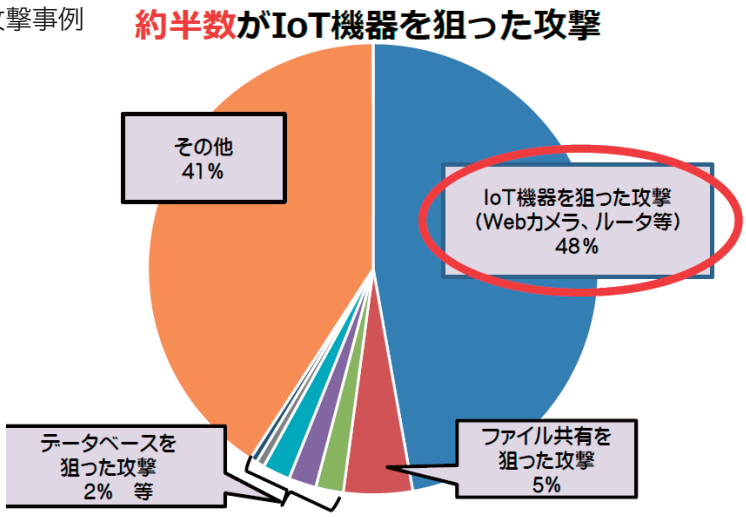
参考文献2)：Techfirm Blog：IoT(Internet of Things)とは？ わかりやすく解説！

1.1. IoT(Internet of Things)

従来のインターネット利用は、IoP(Internet of People)だった。人とPCやスマートホンなどをネットワークに繋げ、PtoP(Person to Person:人同士が繋がるためのインターネット)の利用が主流だったといえる。SNSが代表例である。

一方、本特集で議論の中心となるIoTでは、センサーと通信機能が組込まれたモノがインターネット上で繋がり、モノ同士の繋がるM2M(Machine to Machine)による情報・機能の補完、共生が主流となる。IoTの目的としては、第1に監視・管理対象の機器のデータを収集し状態を把握すること、第2にデータの蓄積・分析から知見を獲得して、新たなサービスやソリューションにつなげることが挙げられる。ここで取り上げるIoTは4要素で構成される(表1)[2]。

図1 IoT攻撃事例



(注1) NICTERで観測されたパケットのうち、サービスの種類(ポート番号)ごとに割合の多い上位から30位までを分析したもの。

(注2) IoT機器を狙った攻撃は多様化しており、ポート番号だけでは分類しにくいものなど、「その他」に含まれているものもある。

出典:総務省、IoTセキュリティ総合対策プログレスレポート2019[7]

1.2. IoTとセキュリティ

モノとモノが繋がりデータ活用が進むことで、利便性は高まる。Society5.0などデータ主導社会では、データそのものに価値が出てくる。データに価値があるとなれば、データを生み出すIoT機器は悪意のある攻撃の格好の対象になる。

1.2.1. IoTセキュリティの事例

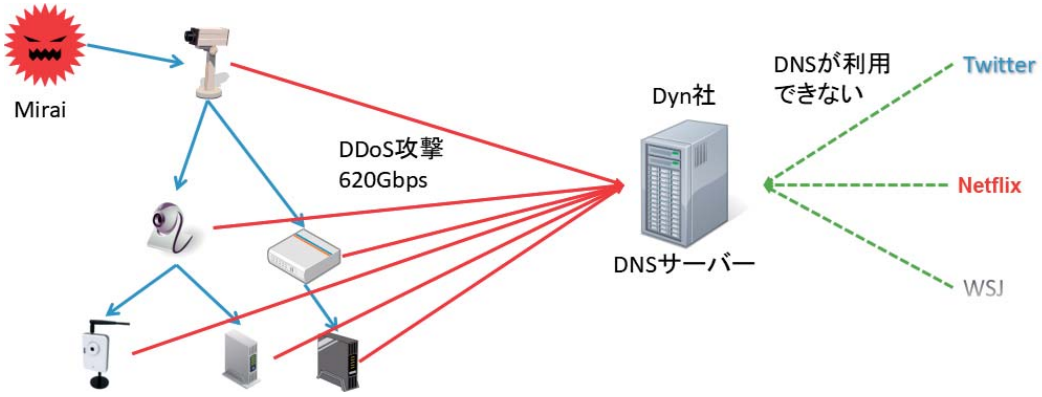
NICT(情報通信研究機構)のNICTER(Network Incident analysis Center for Tactical Emergency Response)システムによる2019年のサイバー攻撃の観測によると、半数以上がIoT機器を狙ったものだった(図1)[7),8)]。

記憶に新しいところでは、2016年10月に流行したマルウェアMiraiがある。監視カメラやWi-Fiストレージ ポケドラ、ルーターなどのIoTデバイスがボット化され、米Dyn社のDNSサービスを狙った大規模なサイバー攻撃(DDoS攻撃)に利用された。DNSサービスが使えないために、TwitterやNetflixなどのサービスで障害が発生した(図2)。

Miraiは、Linux OS搭載機器で保守ポートとして開いていたtelnetを狙ったマルウェアである。パスワードのリスト攻撃で、監視カメラなどのIoT機器に侵入をした。侵入後、reboot、netstat、cp、mv、kill、killall、wget、ftpgetなどの主要コマンドを無効化し、攻撃マルウェアをダウンロードしバックドアを仕掛けた。侵入できる機器を次々に探し出し、ボットは増殖した。攻撃者がボット化したIoT機器に対してバックドアから命令を出すことで攻撃が始まった。

ここで留意しなければならないのは、telnetの問題だけではなく、ボット化に気づかなかったことである。IoTデバイスの場合、ネットワークに繋がっていればサイバー脅威にさらされると認識しなければならない。telnetの問題はIoTデバイス開発時のセキュリティ設計(セキュリティ・バイ・デザイン)で対策をし、ボット化は保守運用の部分で対策することが必要である。

図2 IoT攻撃例 (Miraiの例)

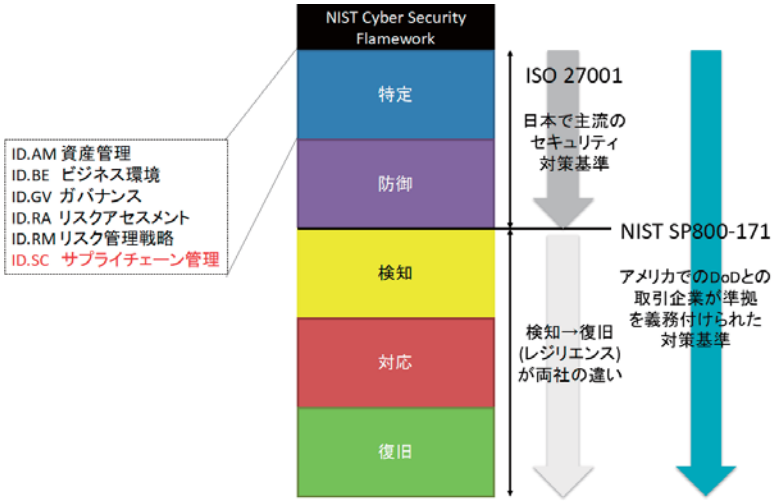


2. 世界・国内のセキュリティ動向

2016年以降、欧州、米国など主要国では、サイバーセキュリティに対する法律やガイドラインが策定されている。米国のセキュリティ会社が2016年に、携帯電話のファームウェアに不正プログラムを発見したことがキッカケとなった。

この不正プログラムは中国企業が開発したもので、ユーザーの同意なしに72時間おきに携帯電話内の情報を中国のサーバーに送っていた。このほか2017年に起きたランサムウェアWannaCryの蔓延がある。感染した欧州企業からサプライチェーン経由で広がった。このような事例の反省を踏まえ、調達要件やサプライチェーンを重視した法律、ガイドラインが2017年以降に策定された。

図3 NIST SP800-171におけるサプライチェーンの対応



2.1. 米国の動向

2017年5月の「サイバーセキュリティ強化のため大統領令」以来、米国では様々なガイドラインが策定されている。NISTが2014年から検討してきた「Cybersecurity Framework」が2018年にNIST SP800-171 Rev.1として更新された。ISO27000の「特定」「防御」に加え、「検知」「対応」「復旧」が追加されている（図3）。国際標準化に向けた活動も始まり、2019年にDoD（アメリカ合衆国国防総省）の調達要件として義務付けられた。今後は重要インフラ企業やその他の製造分野に広がると予想される。NIST SP800-171の特徴としては、特定段階でサプライチェーン全体で対策を実施することや、必要に応じて監査を行うことが要求されている点が挙げられる（図3）。

2.1.1. 対ボットネットに対する取組み

IoTデバイスのボット化への対策として、2018年5月に商務省（DoC）、国土安全保障省（DHS）が報告書をまとめた。報告書に基づき、11月に「対ボットネット強靭化ロードマップ」を公開した。ボットネット撲滅活動を5つの取り組みに分類した上で、官民が行うべき個別タスクを整理した。ロードマップの公表に合わせ、CSDE（The Council to Secure the Digital Economy）が５つの取り組み・タスクを示し、「国際アンチボットネットガイド」として公表した（表2）[13]。

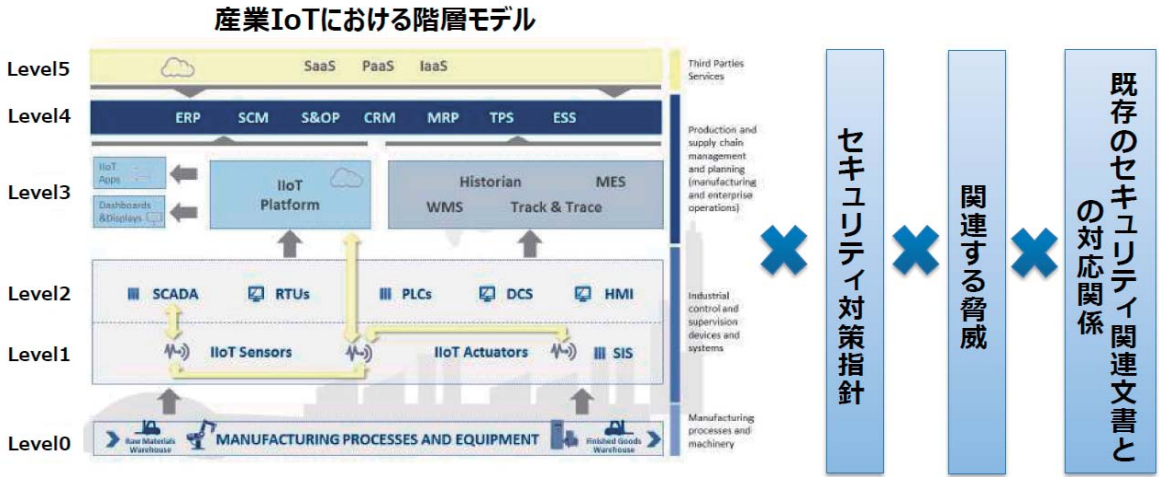
2.2. 欧州の動向

欧州では2017年に、ネットワークに繋がる機器を対象とした認証フレームワークの議論が始まっている。IoTデバイスのセキュリティに関する課題を洗い出し、解決に有用な考え方やツール（既存の規格、ガイドライン、研究資料等）を具体的な産業分野（スマートホーム、スマートカー等）を念頭に整理したものである[13]。さまざまな議論の後に

表2 ロードマップにおける５つの取り組み・タスク

項番	項　目	内　容
1	IoTデバイスのセキュリティ向上	信頼性の高いIoT機器の強固な市場開拓。エコシステム全体にわたるIoTセキュリティの持続的な適用
2	企業のサイバーセキュリティリスクマネジメント	NIST CSFを用いたプロファイル作成。ネットワークアーキテクチャの高度化。企業のベストプラクティスの連邦政府への適用。OTのサイバーセキュリティ対策
3	インフラ	ルーティングのセキュリティ向上。実践的な情報共有の推進。情報共有プロトコルの開発。インフラセキュリティ向上のための研究開発
4	セキュリティ技術の開発・移り変わり	セキュアなソフトウェア市場の構築。国際協調。革新的な技術開発
5	啓発と教育	IoT機器のセキュリティに対する消費者の信頼を促進。IoT機器のサイバーセキュリティの脅威に対する労働者の教育

図4 欧州の産業IoTにおける階層モデル　　出典：参考文献13のp.19



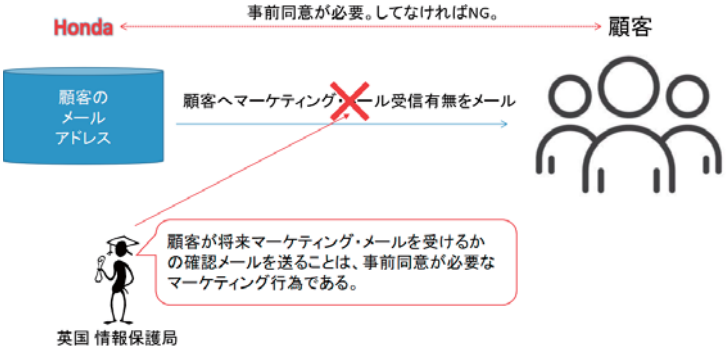
ENISA（欧州ネットワーク・情報セキュリティ機関）は、2018年11月に「Good Practices for Security of Internet of Things in the context of Smart Manufacturing」（図4）を公表した。

図4に示す通り、産業IoTのセキュリティ確保に向けてポリシー、組織、技術という３つの側面で対策指針を整理している。同時にサイバーセキュリティの共通理解を促すための用語定義、守るべき機器、サービスの分類、産業IoTにおける脅威も分類し、セキュリティ対策ごとに既存のセキュリティ関連文書との対応づけも行った。

2019年に施行されたEUサイバーセキュリティ法（EU Cybersecurity Act）では、サイバーセキュリティ認証制度（罰則などの一部規定は2021年6月以降から適用）が存在する。EU内でネットワークに接続するIoT機器を販売する際に、安全を示す「セキュリティ証明書」の取得を求めている。個人情報保護のGDPR（EU一般データ保護規則）と同様、施行されれば日本企業への影響は小さくない。

欧州での情報の取り扱いについても注意が必要である。特に個人情報の取り扱いは、2016年に発令されたNIS指令（The Directive on Security of Network and Information Systems）の存在を忘れてはならない。GDPR施行の前までに、EU各国に対してNIS指令に基づく国内の法整備を求める指令である。EU域外の企業に対する罰則がゆるいこともあり、日本ではGDPRに目が行きがちだが、NIS指令をおろそかにしてはならない。GDPRはEUの統一ルールなのに対して、NIS指令はEU域内のミニマムスタンダードであり、実際の法令や運用、強制執行措置は各国に委ねられている。各国での法令を理解することが必要である。

図5 英国での個人情報の取り扱い事例



欧州の動きは各国各様である。EUの規格と法案だけでなく、各国の規格と法案を把握することが欠かせない。GDPRに代表されるように、特にプラバシーに対する規制は厳しい。例えばホンダ技研工業は、2016年に13000ポンド（約190万円）の罰金が科された（図5）。

この事例でホンダは、マーケティング情報を受け取ることに対する明確な許諾を、顧客から事前に得ていなかった。ホンダが顧客にマーケティング情報の許諾を得るためメールを送ったところ、英国情報局から「顧客がマーケティング情報の受け取りたいかどうかの確認自体が、顧客に対するマーケティング活動であり、事前同意が必要」と判断された。卵が先か、鶏が先かの議論になるが、欧州では国によって個人情報の取り扱いが異なっている事例と言える。日本で考えている以上に、欧州ではプライバシー保護が重要視されていることを忘れてはならない。

GDPRが施行され、欧州に拠点をもたない日本企業などに対しても、制裁金を科すなどの厳しい規則が適用されると予想される。万が一、情報漏洩などの事故・事件を発生させてしまった場合には厳しい制裁が行われるだろう。図6には、北米と欧州を含め各地域で施行されているセキュリティ関連の法律の例を示した[11]。参考にして欲しい。

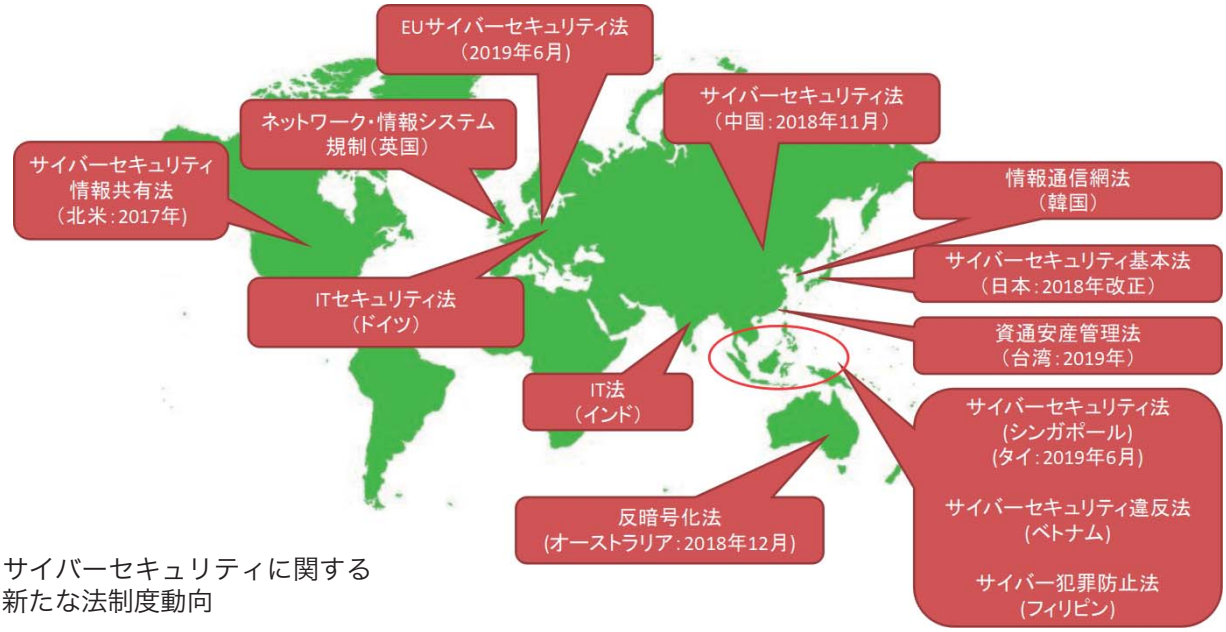


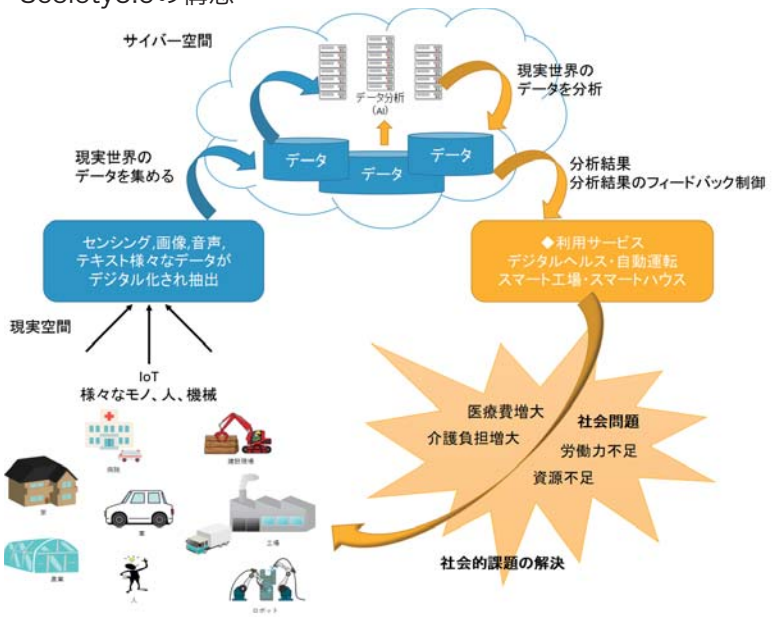
図6 サイバーセキュリティに関する新たな法制度動向

2.3. 国内の動向

日本では、Society5.0（図7）に向けたセキュリティに関するガイドラインや法案などが各省庁から公表されている。Scociety5.0は、2017年6月に日本政府が閣議決定した「未来投資戦略2017」で次のように定義されている。「先端技術をあらゆる産業や社会に取り入れ、“必要なモノ・サービスを必要な人、必要な時、必要なだけ提供する”ことにより様々な社会課題を解決する試み」である。デジタル技術の応用によって、データを使って社会的な課題を解決する「データ主導社会」の実現を目指している。

Society5.0ではIoT機器（組込み機器）の利用が重要な要素となっているが、機器は繋がることによって大きな脅威にさらされる。セキュリティへの配慮が欠かせない[15]。

図7 Scoiety5.0の構想



2.3.1. 総務省

総務省は2019年4月に電気通信事業法の省令改正を行った[14]。Miraiに代表されるマルウェアへの対策やNIST規格にIoT機器を対応させるための改正である。

具体的には、①不特定多数からのアクセスを遮断できる機能、②IDやパスワードに対して初期値からの変更を促す機能、③ソフトウェアを常に更新できる機能を義務付ける。施行は2020年4月から。2020年4月以降に出荷されるIoT機器には不可欠な機能となる。

2.3.2. 厚生労働省

厚生労働省は、医療情報システムの安全管理に関するガイドラインを公表している。このガイドラインでは、医院内のモバイル機器や、遠隔医療やデータ管理向けの医療機器をIoT機器として取り扱うように求めている（表3はガイドラインの抜粋）。具体的な対応方法は、総務省や経済産業省などが公表しているガイドラインを参照することを推奨している[16]。

2.3.3. 経済産業省

政府が進めるSociety5.0の推進には、DX（Digital Transformation）の実現が不可欠である。DXの推進では、機器間のデータの取り扱い方法や機器の開発手法のルール化が欠かせない（図8）。とりわけデータの取り扱いでは、セキュリティ対策の視点が必須となる。

経済産業省はDX推進するにあたり、

表3 医療情報システムの安全管理に関するガイドラインより抜粋

No	改定テーマ	主な改定内容
1	電子カルテの代行入力を時間経過で自動確定することへの言及	・診療録等の代行入力を行う際、時間経過で自動的に記録確定する運用がみとめられないこと明確化 ・記録の作成にかかわる当事者の役割を明確化
2	「製造業者による情報セキュリティ開示書」ガイドVer2.0への言及	・保健医療福祉情報システム工業会(JAHIS)標準及び日本画像医療システム工業会(JIRA)規格となっている「製造業者による医療情報セキュリティ開示書」ガイド(MDS)に言及
3	モバイルデバイスへの対応	・機器管理の運用管理規定の設定、データ暗号化、業務に不要なアプリのインストールはしない、公衆無線LAN利用時の基準設定BYODは原則禁止、覗き見防止策など
4	標的型攻撃への対応	・サイバー攻撃の具体例、連絡先、対処項目を追加 ・数世代分のデータのバックアップを推奨など
5	TLS1.2によるオープンネットワーク接続への言及	・インターネット等のオープンネットワークに接続する際は、TLS1.2に限定し、「SSL/TLS暗号設定ガイドライン」における「高セキュリティ型」の要求設定に則るべき旨を追記
6	小規模医療機関が順守すべき項目の明確化	・ガイドラインの本文の変更に伴い、医療機関の規模別運用管理の実施項目の見直し
7	医療情報システムの対象範囲の検討	・電子的な医療情報を取り扱う介護事業者及び医療情報連携ネットワーク運営事業者をガイドラインの対象として追加
8	IoTセキュリティへの対応	・総務省、経済産業省、IoT推進コンソーシアムが策定した「IoTセキュリティガイドライン」等、各種ガイドライン及び医療現場の状況を鑑み、修正
9	2要素認証の採用	・医療情報システムの2要素認証について、医療現場への影響を考慮し、猶予期間を設けて段階的に移行を進めること等を記載 ※猶予期間は、第5版公開から10年後を目処。
10	電子署名の採用	・平成28年度の診療報酬改定において、電子的診療情報提供書の算定要件に保健医療福祉分野の公開鍵(HPKI)による電子署名の採用が盛り込まれたことに合わせて修正

出典:「厚生労働省、医療情報システムの安全管理に関するガイドライン、2017年」の抜粋

表4 CPSFの各層の役割と定義

階層	特性	機能・役割	分析対象	分析対象の具体的イメージ
第1層	各組織の適切なガバナンス・マネジメント	・各組織のセキュリティマネジメント [信頼性の基点]組織・マネジメント	・組織で管理されるモノ、システム等 ・組織内で流通するデータ等	・社員、従業員 ・企業のIT資産 等
第2層	フィジカル空間とサイバー空間の繋がり拡大	・フィジカル空間とサイバー空間との間のデータのやりとり [信頼性の基点]ルールに沿って正しくフィジカル空間とサイバー空間とを転写する機能	・データを転写するモノ・システム ・転写されるデータ等	・センサ ・アクチュエータ ・3Dプリンタ ・監視カメラ 等
第3層	サイバー空間で組織を超えた多様・大量のデータの流通・処理	・データの送受信、加工、分析、保管 [信頼性の基点]データ	・データを送受信/加工・分析/保管するモノ・システム等 ・組織を超えて流通するデータ等	・サーバ ・ルータ ・スマートメータ ・オープンデータ 等

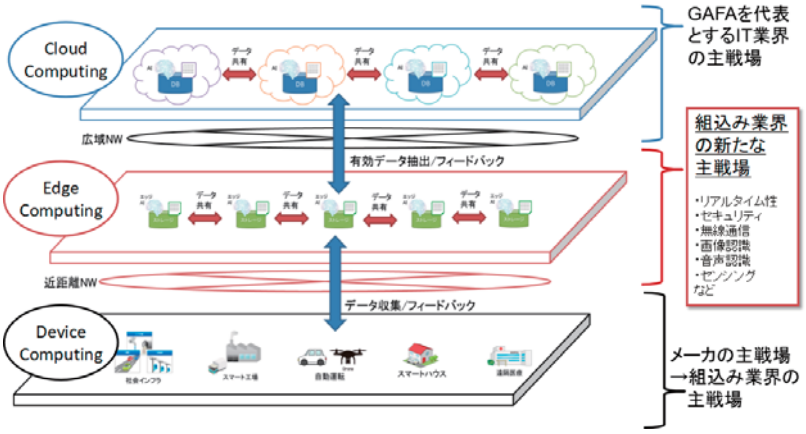
出典:参考文献 17を要約した

CPSF(Cyber Phisical Security Framework)のガイドラインを策定した(表4)。CPSFでは階層構造を定義し、各層におけるセキュリティ対策を定義している。最も重要されているのがサプライチェーンである。会社間の調達要件やソフトウェア開発にあたってのセキュリティ対策のポイントがガイドラインとして公表されている[17]。

CPSFの第1層では、IoT機器を開発するにあたっての調達ルールなど組織間のセキュリティマネジメントを定義する。サプライチェーンでのセキュリティマネジメントを重要視したとも言える。第2層は、フィジカル空間とサイバー空間でのデータの取り扱い方を定義する。IoT機器とクラウドサービスなどとの間のデータのやり取りを対象とする。第3層が定義するのは、サイバー空間の間でのデータの取り扱い方法である。各層で、OSS(Open Source Software)の取り扱いや脆弱性対策などを重要視しているのもCPSの特徴の一つである。

国内外の動向を踏まえると、IoT機器を開発する会社におけるセキュリティ対策は経営問題といえる。現場だけのものではなく、経営課題として捉え会社や組織としての対応が求められている。セキュリティ対策はコストではなく、経営戦略として捉えるべきである。セキュリティ対策をなおざりにするようでは、日本IoT機器のガラパゴス化は避けられない。輸出が難しいなど、ビジネスに大きな影響が出ることを認識して欲しい。

図8 DX(Digital Transformation)のイメージ



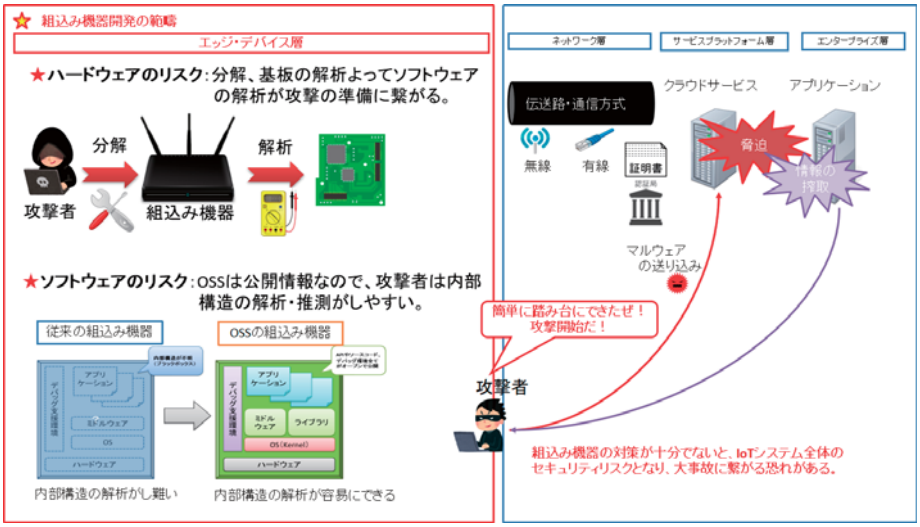
3. IoT製品開発におけるセキュリティ設計

IoT製品開発においては、設計段階でのセキュリティへの配慮が重要となる。設計段階でセキュリティ対策をすることで、運用コストを抑えられるメリットがある。セキュリティ設計をするには、IoT製品の開発における脆弱性となるポイントを押さえなければならない。

3.1. IoT製品における脆弱性ポイント

IoT製品には、ハードウェア、ソフトウェアの大きく2つの脆弱性ポイントが存在する(図9)。ハードウェアでは、IoT機器が分解され、内部を解析・分析されることを想定すべきである。つまり機器の構成やファームウェアの吸い出しなどによって、脆弱性を発見されるというリスクがある。ソフトウェアではOSSへの対応がポイント

図9　IoT機器の脆弱性ポイント



になる。IoT機器ではOSSが利用されていることが多く、ソースコードが公開されている。ソフトウェアの脆弱性を突いた攻撃が容易なのは間違いない。

IoT製品におけるセキュリティ事故の大半が、上記の脆弱性部分を突いている。ボット化されて踏み台にされたり、情報資産を狙った金銭目的の攻撃に利用されていることを忘れてはならない。

3.2. セキュリティ設計

セキュリティ設計とは、どのようなことか？。一般的にセキュリティ対策は、脅威に対する分析を行った上で、この脅威において脆弱となる部分に対策を施すことを意味する。V字モデルの開発では、上流設計段階での対応が重要である。

図10にV字開発におけるセキュリティ設計のポイントを示した。SbD（Security by Design）と呼ばれ、上流工程でセキュリティ対策を盛り込む手法である。上流工程で対策された内容を下流工程で確認し、セキュリティ設計が有効であることを確認する。

IoT製品の場合には別の視点も必要となる。IoT機器単体での対策はもちろんだが、IoTシステム全体を俯瞰することが欠かせない。単体のシステムだけを対象にするのではなく、IoTシステム全体としてセキュリティ対策を施す。こうすることでIoT機器単体で対応できない部分をカバーすることが可能となる。この場合、システム全体を俯瞰できるアーキテクトとしてのスキルが必要になるのは言うまでもない。

3.2.1. 脅威分析

脅威分析は２つ存在する（図11）。１つは要求定義段階での被害分析。もう１つは設計段階での攻撃分析である。被害分析では、情報資産（守りたい資産）が何であるかを特定し、その情報資産が盗まれたり改ざんされたりした場合の被害を推定する（被害識別）。攻撃分析では、設計仕様がある程度固まった後、対象の機器に対して想定される攻撃手法を定義する。想定された攻撃手法から、攻撃される可能性の有無を分析する。最終的には、被害識別した結果と攻撃の可能性を考慮してリスク評価を実施する。リスクが高いものに対しては、脆弱性が存在する部分に対策を行うこととなる。

セキュリティ設計における脅威分析で難しいのは、「人」に関する部分である。脅威は人(第三者)の悪意によって引き起こされる。この脅威をもたらす人をどう想定するかによって、脅威分析の優劣が決まる。設計者だけではなく、IoT製品の関係者が一緒になって考える必要がある。

3.2.1.1. 被害分析手法

被害分析で利用される代表的な手法を紹介する（表5）。ポイントは2つあ

図10　セキュリティ設計（Security by Design）

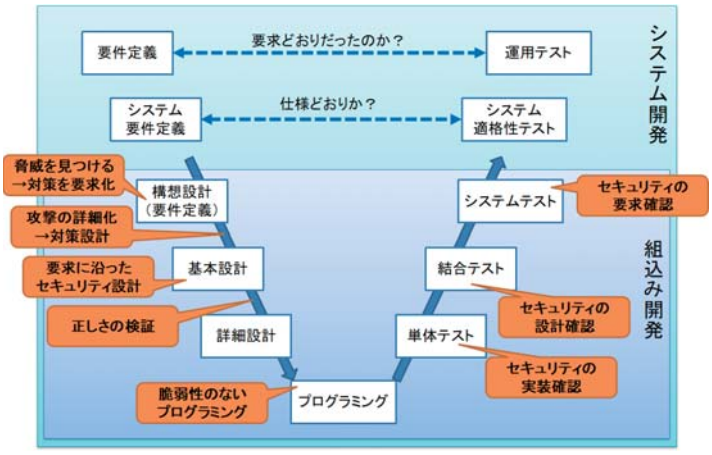


図11　脅威分析のポイント

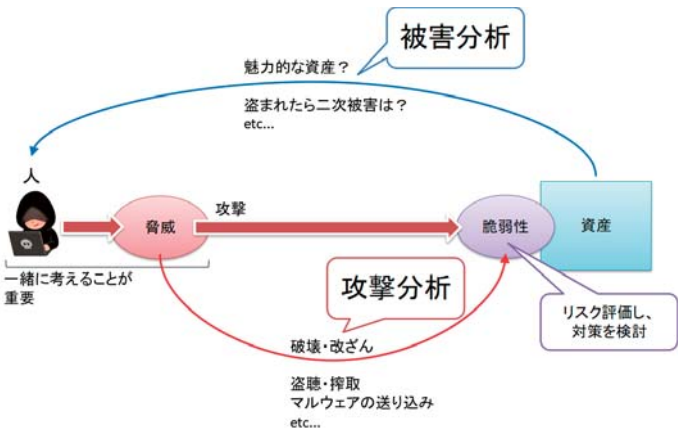


表5 被害分析の代表的な手法

No	被害分析手法名	概　要
1	KAOSを用いた手法（ゴール指向）	FTA（Fault Tree Analysis）の応用となり、攻撃者の目標を分解し、攻撃者のゴールを分析する
2	Liuらの手法	ステークスホルダーを含むシステムに関わるアクターを全て攻撃者になりえると仮定し、攻撃者のゴールを分析する
3	ミスユースケース	2000年 Sindere Opdahiが提案。UMLのユースケース図を拡張し、脅威とその関係者、対策の関係を明確にする

表6 攻撃分析の代表的な手法

No	被害分析手法名	概　要
1	脅威モデリング	Microsoftが考案した脅威分析手法。一般的に最も使われている手法。DFD（Data Flow Diagram）を用い、STRIDEといったガイドキーワードを用いて、脅威の抽出、評価をする。アーキテクチャが明確なときに、脅威抽出の手法としては有効と言われている
2	解析型セキュリティ分析	Where、Who、When、Why、Whatの5Wを用いて、資産（Asset）に対して、攻撃者（Agent）が、有害なアクション（Attack）を実行することをツリー状に検討することで、網羅的に脅威を抽出する。トップダウンでアプローチする手法と言われている

表7 リスク評価の代表的な考え方

No	リスク評価名	概　要
1	CRSS方式	CVSS based Risk Scoring Systeの略。CVSSと言われる共通脆弱性評価システムのリスク評価方法を応用したもの
2	RSMA方式	Risk Scoring Methodology for Automotive systemの略。「リスク値」を「影響度」と「発生可能性」のリスクレベル判定表によって決定する方式である。「影響度」は“セーフティ”、“個人情報／プライバシ”、“財産／企業価値”の3種類の被害分類に分けた上でレベルを決定する
3	ETSI方式	欧州電気通信標準化協会（European Telecommunications Standard Institute）のリスク評価手法。「発生可能性」を「動機」と「技術的困難さ」に細分化して評価し、これに「影響」の評価を行い、それぞれ3段階で評価した値の積で、リスク値のクラス分けを行う
4	CCDS方式	「リスク値」を攻撃の「難易度」とユーザへの「影響度」についてランク付けして判定する方式を用いている。CVSSの情報を参考とし、初動段階において、早期評価、開発を行う事を目的として、「難易度」と「影響度」を基本軸としている

る。第1に重要なのは、システムの分析が行いやすい手法を選ぶことである。第2は、情報資産を定義できる手法を選択することである。表5に示した手法はいずれも、情報資産に対してどのような被害が想定されるか分析することを目的としている。機能安全の分析手法であるFTA（Fault Tree Analysis）と同様と考えることができる。異なるのは、セキュリティ設計の分析が情報資産を対象としている点である。

被害分析では、攻撃者の目的を想定しながら、攻撃者のゴールを分析する。被害分析を実施する段階では、設計仕様やアーキテクチャが決まっていないケースもある。こうした場合は、ある程度設計仕様を想定して脅威や攻撃などを識別することになる。

3.2.1.2. 攻撃分析手法

攻撃分析で利用される代表的手法を紹介する（表6）。攻撃分析においては、「何がこまる？＝脅威の識別（網羅的）」「どうやって攻撃される？＝攻撃の手段の詳細化」で攻撃の可能性評価を行う。被害分析で洗い出された情報資産に対して、「攻撃が起きるのか？＝リスク評価」することとなる。表6に示した手法はいずれも情報資産（データなど）を重要視し、どのような攻撃が想定されるのかをツリー構造で分析する。

3.2.1.3. リスク評価

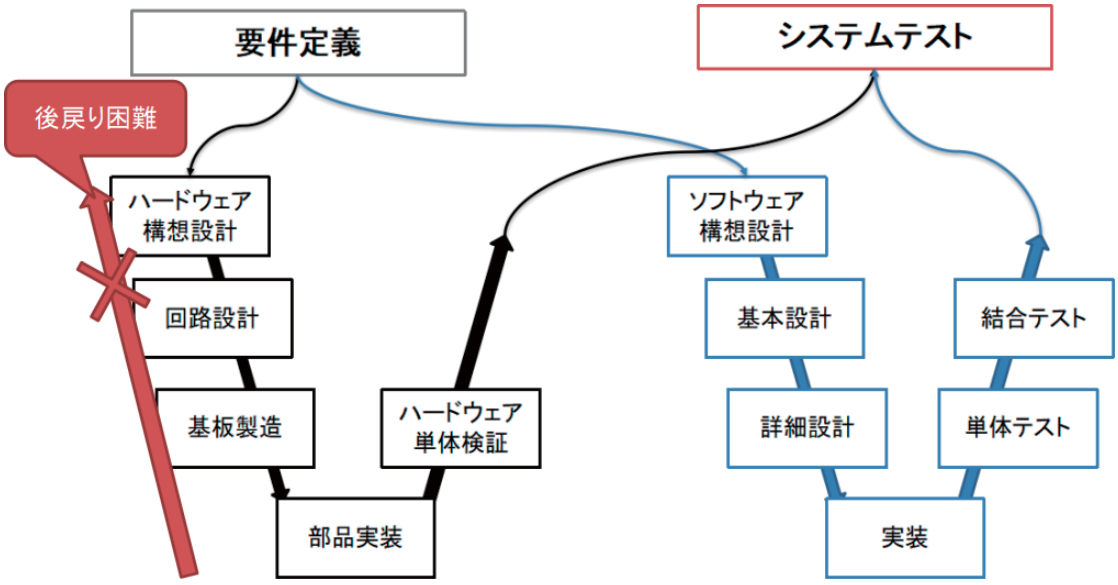
リスクの評価は、「アタックツリー」と呼ばれる２分木のツリーを用いるのが一般的である。アタックツリーでは、「その脅威が本当に起きるのか？」「脅威が起こることにより、影響が（リスク）があるか」を明確にする。FT（Fault Tree）に応用すること可能とされている。

リスクの評価にあたっては、リスクの重要度が判断できるように、重要度を数値化することが一般的な方法とされている。代表的なリスク評価の数値化手法を表７に示した。CRSS（Common Vulnerability Scoring System）方式が一般的だが、手法によって考え方に特徴があるので、利用しやすいものを選んで欲しい。

3.2.2. 組込み製品開発における留意事項

組込み製品開発では、ハードウェアとソフトウェアの開発を一緒に進める

図12　組込み開発におけるセキュリティリスク



ことが一般的である。要求定義段階で、セキュリティ対策を踏まえた要求仕様を検討することが欠かせない。ハードウェア開発がある程度の工程まで進んでしまうと後戻りが難しいためである。要求定義段階で、ハードウェアとソフトウェアのアーキテクチャ候補となるものを列挙し、リスク評価をすることが重要である(図12)。

多くの場合、要求定義段階で性能要求とコスト(特にハードウェア)のトレードオフでアーキテクチャが決定される。コストが優先され、セキュリティ機能が実現できないこともある。こうしたときに、対策が難しい事柄に対してはリスクの残存を「受容」することも必要となってくる。

3.2.2.1. 脅威分析の留意点

バグをゼロにできないのと同様で、リスクをゼロにするのも困難である。単体システムでソフトウェアに対して無理なセキュリティ対策を行うことは、性能の劣化やコストの増加に繋がる可能性がある。単体システムの脆弱性に対するリスクを「受容」した部分に対しては、他のシステムやシステム全体でカバーすることを想定したアーキテクチャ設計が必要となる。

3.3. セキュリティテスト設計

セキュリティ対策では、4つのテストを想定しなければならない。機能テスト、脆弱性スキャン、ファジングテスト、ペネトレーションテストである(表8)。テストは、上流設計で設計した内容を確認する工程である。テスト項目の漏れがセキュリティ事故に繋がることもあるので、セキュリティテスト設計の重要性は大きい。

特にファジングテストとペネトレーションテストの確立を自社で行うには、専門的なスキルとツール開発が必要となる。より高度なセキュリティ技術が要求されるため、自社単独では難しいことが想定される。最初のうちは、専門機関や企業が提供してくれるツールなどを利用する方が良いだろう。

表8　セキュリティテストの概要

No	項　目	内　容
1	機能テスト	ターゲットシステムの全てのセキュリティ関連機能の堅牢性と機能の正常な作動に焦点にテストを実施。このステップではセキュリティ脆弱性につながる実装エラー、仕様書との不一致、未定義機能を見つけることを目的にする
2	脆弱性スキャン	ターゲットシステムに対して既知の通常のセキュリティ脆弱性の検査が行われる。例えば、既知のセキュリティエクスプロイトや不適切な設定による既知の脆弱性を検出する
3	ファジングテスト	未知のセキュリティ脆弱性を見つけ出すことに焦点にテストを実施する。このステップはファジングと呼ばれており、ターゲットシステムに対して不正形式あるいは仕様書とは異なるインプットを送信しモニタリングして、異常検知をする
4	ペネトレーションテスト	ターゲットシステムのソフトウェアとハードウェアの両方に侵入テストを行うことによるシステム全体のテストに焦点にテストを実施する。試験者が優れた攻撃者を模倣して既知のセキュリティ脆弱性の全てを試す。試験者は長年のハッキングの経験を生かし、リバースエンジニアリングや重要なデータの抜き出し、ソフトウェアとハードウェアを結び付けるアプローチを行い、より洗練された攻撃を実行しなければならない

4. IoTシステム運用時のセキュリティ対策

設計段階で脆弱性対策を行うことは、コスト面で重要である。図13はセキュリティと製品ライルサイクルの関係を示している。設計段階での脆弱性対策は、既知の脆弱性に対応するものである。しかし運用段階で、攻撃者が新たな攻撃手法を開発する可能性もある。これが新規の脆弱性につながることも想定しなければならない。運用から破棄までの製品ライフサイクルを見据え、運用での脆弱性対策を忘れてはならない。

4.1. セキュリティ事故の判例

設計段階で見つかっていない脆弱性が、運用段階で見つかることがある。図14は運用段階で脆弱性対策を怠ったために裁判になった例である。IPA（情報処理推進機構）からSQLインジェクションに対する注意喚起があったにもかかわらず、対策を怠ったため個人情報（カード情報）が流出した。判決に記載されている通り、IPAなどからの注意喚起があった場合には速やかな対策が必要となる。IoT機器では運用段階での脆弱性対策のコストを見込んでいないことが少ないない。しかしセキュリティ事故が生じると、損害賠償を求められるだけではなく、社会的な地位を失いかねない。

図14　セキュリティ対策をしなかった場合の判例

判決の内容

（1）被告が展開する事業の一環として、ウェブアプリケーションを提供していることから、原告がその専門的知見を信頼して委託契約を締結したと推認できること。
（2）被告に求められる注意義務の程度は比較的高度なものと認められる。
（3）SQLインジェクション対策がなされていれば、第三者によるSQLインジェクション攻撃により、個人情報が流出する事態が生じる得ることが予見できた。
（4）経済産業省及び、独立行政法人 情報処理推進機構（IPA）が、ウェブアプリケーションに対し、SQLインジェクション対策をするよう注意喚起していたことから、個人情報が流出する事態が生じ得ることを予見することは容易であったといえること。
（5）SQLインジェクション攻撃への対策をとることは、多大な労力や費用がかかる証拠はなく、流出という結果を回避することが容易であったといえること。

4.2. サプライチェーン

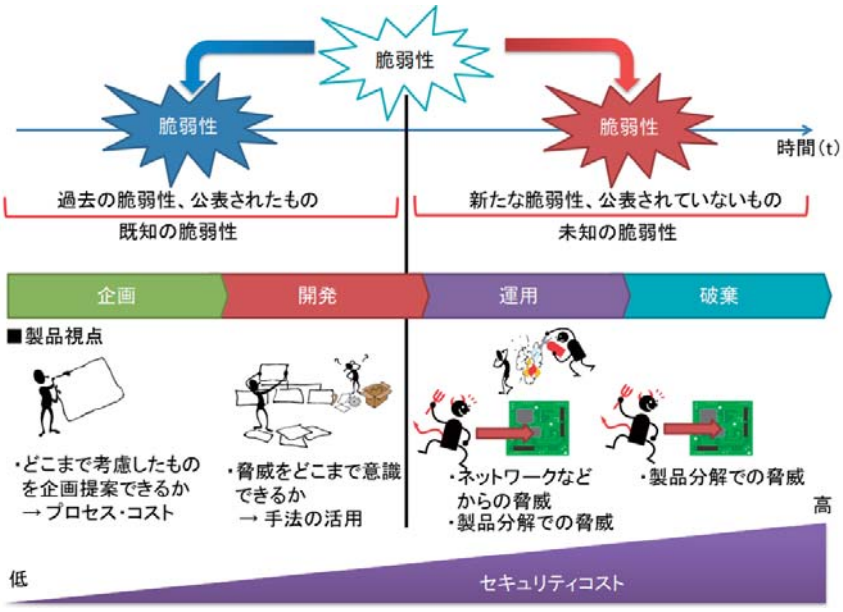
昨今の組込み機器は、多機能化や高機能化のために開発量が多くなっている。このため1社のみで対応することが難しく、複数社にまたがった開発が主流となっている。図15に、こうした状況を考慮したセキュリティ対策の考え方を示した。IoT機器開発のサプライチェーンに加わる会社や自社内の部門においてセキュリティ意識を高めるだけではなく、脆弱なシステムとならないように開発を管理・運用することが肝要である。

4.2.1. セキュリティゴールの設定

セキュリティのゴールの設定に当たっては、発注元と受注側の企業の意識合わせが重要となる。要件定義段階で、発注元がセキュリティゴールを設定し、受注側との意識を合わせなければならない。こうすることで、システム全体でセキュアな開発が可能になる。発注元がセキュリティゴールを設定しないと、受注側のセキュリティ意識にバラツキが出る。システム全体を見た場合に脆弱性を抱えかねない。発注元のセキュリティ意識が低いと判断した場合に受注側は、ぜひ確認をとって欲しい。

民法が改正され、2020年から瑕疵担保期間は最長5年となる。5年間に新たな脆弱性が発見された場合、発注元へ

図13　セキュリティと製品ライフサイクル

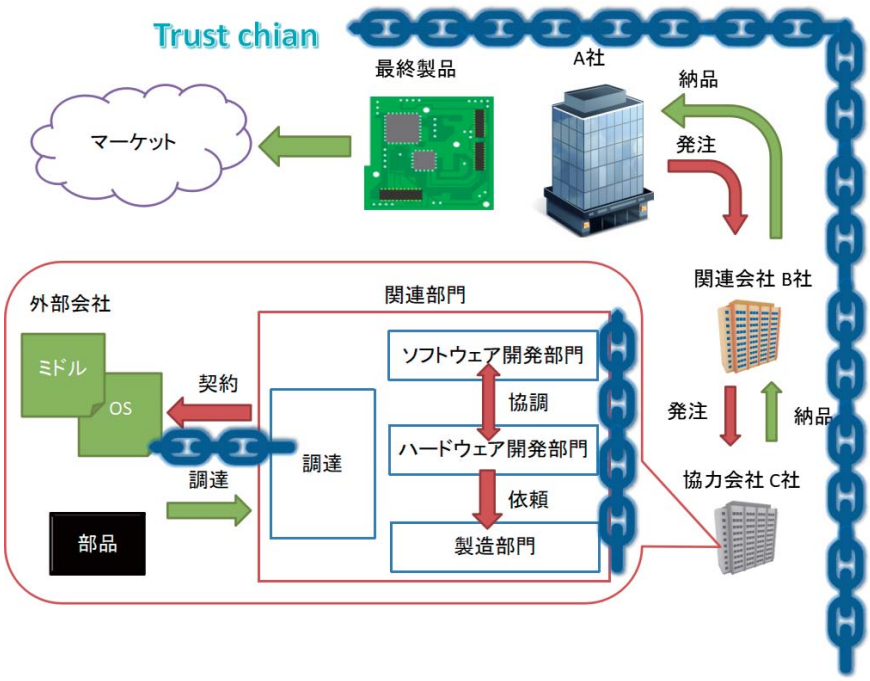


の対応が不可避である。セキュリティ対策の運用コストを想定することが重要になる。

図16の左側は、発注元がセキュリティゴールを明確に示していない事例である。受注側にセキュリティ意識がない場合、セキュリティ対策がなされずに開発が進められるケースが出てくる。IoT機器は脆弱性を抱えかねない。

一方で図16の右側は、発注元がセキュリティゴールを明確に示した事例である。発注元がセキュリティゴールを示すことで、受注側のセキュリティ意識は高まる。セキュリティ対策をとった開発プロセスが推進がされる。

図15　サプライチェーンのイメージ



4.2.2. 調達要件の明確化

2016年に起きた中国企業の情報漏えい事件を踏まえ、NTIA（米国商務省電気通信情報局）は2018年にSBOM（Software Bill of Material）を推奨するようになった。SBOMでは、開発したものが「どのように調達されたものなのか」「どのように開発されたものなのか」などの調達要件を明確にすることを求めている。

図17は、経済産業省の「サイバーフィジカルセキュリティ対策フレームワーク」で提言されているOSSの取り扱い例である。OSSの品質やセキュリティなどは利用する側が担保しなければならない。OSSを利用した開発では、「どのようなOSSを使っているのか」「ソフトウェアを外部調達していないか」など、ソフトウェアの構造や成り立ちを明確にし調達要件としてまとめることを推奨している。

米国に輸出する機器などでは今後、SBOMで調達要件を明確にすることが求められるだろう。特にOSSを利用した開発の場合には、OSSの安全性を評価する仕組みなどが必要となる（図17）。

4.2.2.1. OSSの利用

組込み機器やIoT機器にOSSを利用することが多くなっている。OSSを使った開発は、開発部分を減らすことができ、多くの機能を利用できるので便利である。しかし欠点もある。OSSの情報は、広く一般に公開されているので脆弱性に繋がることが少なくない。OSSを利用する場合、自己責任でセキュリティ対策を施す必要があり、利用方法や開発方法に工夫が欠かせない。

運用段階でも、新たな脆弱性が見つ

図16 セキュリティゴールのイメージ

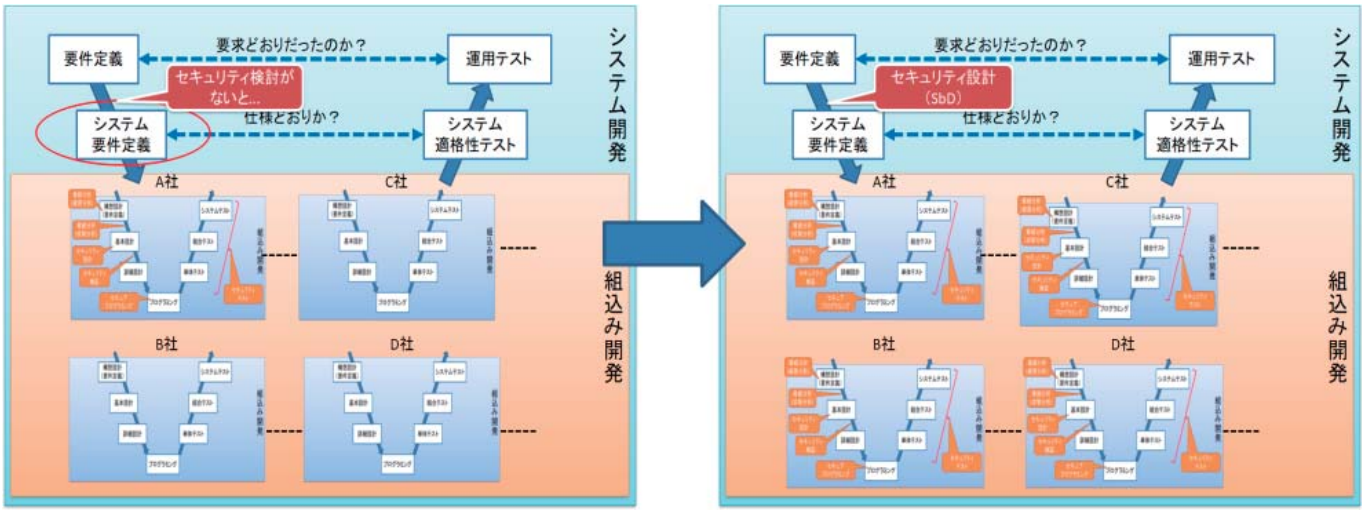
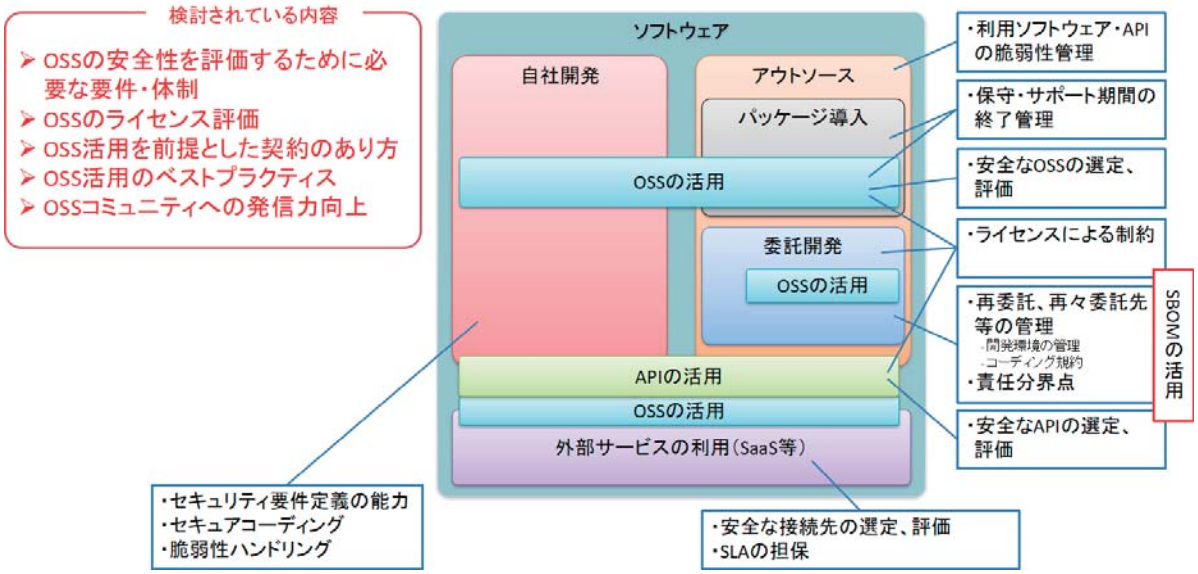


図17　SBOMのイメージ



かることは避けられない。運用段階での脆弱性管理を想定した運用ルールを定めなければならない。図18はOSSを利用する前に脆弱性診断をした例である。OSS利用時には、まず選定前に診断を行い、CVSS（Common Vulnerability Scoring System）にもとづいたリスク評価を行う。次にバージョンの選定と、CVE（CommonVulnerabilities and Exposures）の情報に基づいたセキュリティ設計の工数を見積もることが必要となる。運用時にも脆弱性診断を定期的に実施し、対策を続けることが重要となる。

4.2.2.2. BSPの選定

LinuxやAndroidなど、OSSのBSP（Board Support Package）は、多くはSoCベンダーから提供されている。開発時のセキュリティ要件によって、採用するBSPのバージョンを選定しなければならない。特にカーネル・バーションが古いと暗号化や強制アクセス制御などの利用が制限される場合がある。SoCにセキュアブートなどの機能がない場合にも、ブートローダの開発で対応をしなければならないケースが出てくる。

またSoCベンダーが配布しているBSPのメンテナンスがされていないこともある。セキュリティ要件が実現できないことも少なくない。セキュリティ要件を満たせない場合、脅威分析を実施したのちにリスクが「受容」できるレベルなのかを判断しなければならない。結局、開発が後戻りしたり、発注元の企業との調整が発生したりと工数増大に繋がる。

セキュリティ要件が実現できるSoCベンダーのBSPを選定し、開発の後戻りを避けるには、要件定義段階においてセキュリティを意識したアーキテクチャ設計が必要である。要件定義段階で利用できそうなOSSのセキュリティ機能（表9）を把握し採用することがポイントになる。

表10は、SoCベンダーが配布しているBSPを実際に脆弱性診断した結果である。選定時の参考にしてほしい。

ここで示している数値はあくまでも参考値だが、アーキテクチャ設計段階で脆弱性診断をすることで、採用するSoCベンダーやBSPのバージョンなどの選定に役立てることができる。通常の組込み開発では、ハードウェア部門が先導してSoCベンダーを選定してしまうのが一般的である。セキュリティの対応にあたっては、ソフトウェア主導でSoC上で動作するBSPやミドルウェアを選定し、SoCを決めることがセキュアな

図18　OSS利調達時の脆弱性診断イメージ

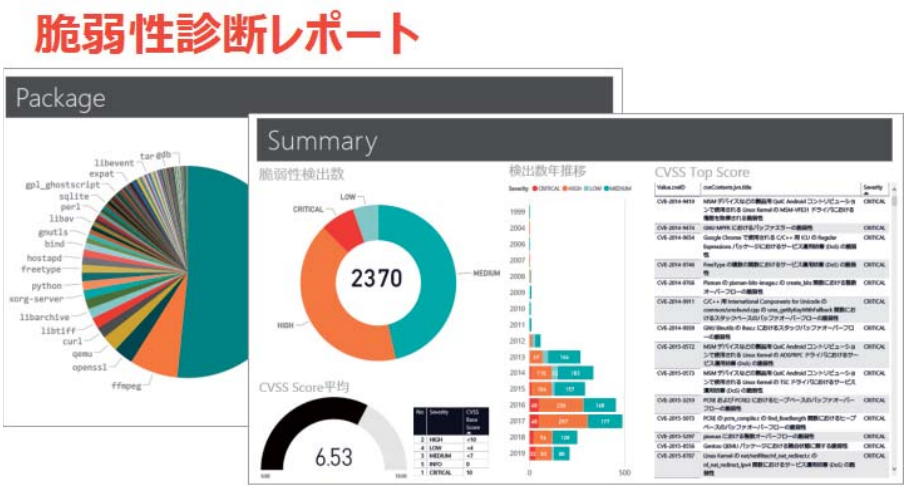


表9 OSSの主要なセキュリティ機能

No	セキュア機能名	内　容
1	セキュアブート FIT	SoCでセキュアブートを利用できない場合、u-bootでソフトウェア的にセキュアブートを実現する機能
2	改ざん検知 IMA	Integrity Measurement Architectureの略。カーネル上に組み込まれたモジュールを利用して、実行ファイルを測定して記録し、実行ファイルが不正に改変されていないかをチェックするもの
3	強制アクセス制御	ラベル方式：SE Linux、SMACKパス方式：Tomoyo Linux、AppArmorがある。プログラムを「改変されないように」するために対象ファイルやデータに対するアクセス権を制御する機能である。アクセス制御には、セキュリティポリシーの設計が必要となる

設計を進めるうえで重要になる。

OSSを使う場合には、人の作ったソフトウェアを利用する意識を持ってセキュリティ対策に意識を向けてほしい。OSSは他者が作ったものだが、自社の責任で利用することを意識しなければならない。

4.2.2.3. 商用パッケージの採用

OSSの場合には、セキュリティ対応に対する工数がかかるイメージであるが、商用パッケージを採用したとしても、OSベンダーが対策していない可能性もある。2019年に見つかった「通称：URGENT/11」という商用OSの脆弱性も見つかっており、商用OSを採用する場合にも、脆弱性の検査が必要なってきている。商用OSや商用のライブラリ（マルチメディア機能など）を採用する場合にも調達要件として、脆弱性診断をする運用ルールの確立が求められてきている。

表10 SoCベンダーのBSP脆弱性情報

No	社名	CVE 総数	CRITICAL	HIGH	Kernel Version
1	A社	1861	202	1438	4.14.06
2	B社	756	53	382	4.1.44
3	C社	1243	117	599	3.10.31
4	D社	424	35	222	4.14.96

5. 組込み製品セキュリティ設計を支援するツール

組込みシステムセキュリティ委員会には、セキュリティ製品を取り扱っている企業が多く参加している。開発や運用を支援するツールやサービスを以下で紹介をする。紹介したツール類や教育に関しては、JASA事務局か当委員会に問い合わせてほしい。

5.1. Cybertrust

超長期サポートのOSSソリューションを軸に、証明書サービス、セキュア・プラットフォームなど、セキュリティ関連の幅広いソリューションの提供を行っている。

5.2. ユビキタスAIコーポレーション

QuickBoot、セキュリティソリューションと幅広い組込み開発向けのプロダクトを揃えている。近年は、セキュリティ分野に注力しており、製品のライフサイクルを通じたセキュリティソリューションの提供と手厚いサポートを提供している。

5.3. マクニカ

幅広いセキュリティソリューションを提供している。V字モデルで利用できる幅広いソリューションや多くの技術に精通したFAEによる手厚いサポートを提供する。

5.4. Connectfree

ET2019 横浜で紹介したベンチャー企業である。セキュアなコンパイラやOSをはじめとした、低レイヤから信頼のおけるソフトウェアの構築を可能にする製品を提供している。セミナーや企業サポートなどを通して、セキュア組み込みシステムの構築を行なっている。

5.5. 情報セキュリティ大学院大学

セキュリティ教育を展開している社会人向けの大学である。IoTセキュリティコースは、組込み開発初心者がIoTセキュリティ設計技術者になるためのコース。初心者でも、IoTセキュリティ設計のスキルを身に着けることができる。図19に示すようなコースを展開している。基礎の基礎を覚えるには最適なカリキュラムなので、これからセキュリティ設計のスキルを身につけたい場合は利用して欲しい。

Cybertrust

No	ソリューション名	内　容
1	Secure IoT Platform	IoT機器のライフサイクルを管理するソリューション。機器にユニークな【信頼の基点】を複製や変更が不可能な方法で格納し、【信頼の基点】を元に機器を特定し、いつ、どの機器が、何を行ったかを証明するトラストサービスである
2	EM+PLS	IEC62443対応を支援するサービス。産業機器向けのIoT機器に対して、Linux OS、脆弱制対応のパッチを提供を超長期間サポートし、IoT機器の認証情報の管理を行い、なりすまし防止、安全なリモート更新機能の提供や脆弱性診断ツールを使ったIoT機器の脆弱性を定期的に診断するトータルソリューションを提供している

ユビキタスAIコーポレーション

No	ソリューション名	内　容
1	beSTORM X	Beyond Security社とユビキタスAIコーポレーションが開発した多種のプロトコル/プラットフォームAPI/機器へのファジングテストとペネトレーションテストが可能な検証用のフレームワーク
2	CodeSonar	MISRA C/C++、CERT C/C++等各種セキュアコーディング規約対応する高精度バグ検出ツールです。C/C++/Javaで書かれたソースコードを、コンパイル時に静的に深く解析し、さまざまな種類の重大なバグとセキュリティ上の脆弱性を検出し、ソフトウェアの品質を向上させる
3	Edge Trust	凸版印刷が金融向けに提供し、高い実績を誇るICカード向けのデバイスID/証明書管理サービスを応用したIoT機器向けのデバイス管理サービスとユビキタスAIコーポレーションのIoT機器セキュリティ実装とAgentソフトウェアを組み合わせることで、製品ライフサイクルのトラストチェーンを確立する
4	Ubiquitous Securus	SoCやMCUに内蔵されているセキュアハードウェアを使用し、秘匿データの保護・管理することで、セキュアな 組込み機器の開発・製造を実現できる

マクニカ

No	ソリューション名	内　容
1	Spirent(スパイレント)	信頼あるホワイトハッカーチームがリスクアセスメント、ソースコードレビュー、ペネトレーションテストでの模擬攻撃などのセキュリティサービスを提供する
2	Mocana TrustPoint (トラストポイント)	各種組込みOSに対応可能な、暗号化通信、相互認証、署名検証、改竄検知等を実現する、オープンソースを一切含まないソフトウェア提供をする。暗号化エンジンはFIPS 140-2 レベル1対応済み
3	Mocana TrustCenter (トラストセンター)	サーバーサービスとして、デバイス証明書のゼロタッチ実装、失効・更新管理を実現するほか、更新プログラムへのサイニング機能により、サプライチェーンに沿った安全な機器アップデートをサポートする
4	THALES	暗号鍵を最高レベルの耐タンパ(改ざん)性を備えたセキュリティ対策の最後の砦と呼ばれるHSM（ハードウェアセキュリティモジュール）を利用することで、製造時、運用時での暗号鍵の管理をする
5	VDOO Vision	Firmwareのバイナリに対する脆弱性診断を実施し、CVEなどの脆弱性情報、セキュリティ規格・ガイドラインの対応可否が診断可能となる。設計段階での診断により、サプライチェーンリスク対策も可能となる
6	VDOO ERA	Firmwareにエージェントを組込むことで、運用時における改ざん検知、ゼロティ攻撃対策、バッファオーバーフローなどの特定攻撃からの保護が可能となる

Connectfree

No	ソリューション名	内　容
1	Zen言語	C言語に代わるセキュアな言語として注目を集めている。コンパイル時に高速化したCPUの計算能力を利用することで多くの安全性の検査を行うような、言語工程での安全性保証が広い言語体系になっている。安全性の検査だけでなく、様々な組み込み環境にアプリケーションを移植可能にする柔軟な運用性を持ち合わせる
2	KIYOMIZU	C言語を始めとする多言語に対応した実行コードの安全性を証明するサービスである。ソースコードから生成された中間表現を解析することで、不正なメモリ操作、バックドアの判定などの診断を行いソフトウェアの安全性を証明する
3	RISC-Vサポート	日本初のRISC-V Platinum MemberとしてのRISC-Vに関する知見を活かし、ソフトウェア開発環境の構築からはじまり、RISC-Vを用いた製品開発をサポートする

図19　情報セキュリティ大学院大学

IoT-1：組込システムの基礎　(1 day, 4 units)

IoTデバイスを開発するために基礎となるハードウェアとソフトウェアの基礎知識を習得します。ハードウェアでは、組込デバイスを構成する要素であるマイクロコントローラ、デバイスインタフェース、センサー、Wi-Fiモジュールを学修し、簡単な実験回路が作れることを目指します。ソフトウェアでは、デバイス(センサー)を制御する簡単なリアルタイムプログラムを作成し、クラウドコンパイラmbedを用いた組込システム開発の基礎を習得します。このコースには、セキュリティの要素はあまりありません。PCの準備が必要です。

IoT-2：IoTアーキテクチャ　(2 days, 8 units)

IoTのビジョンとアーキテクチャを従来型のITと比較しながら考察し、その違いによって生じるIoTのセキュリティリスクを理解し、システムに存在するリスクや脅威を予測する方法を学修します。IoTの法制度、規格や認証制度、また、IoTシステムサービスを運用する基礎知識を習得します。IoTシステムの信頼の基点となる暗号鍵の秘匿法をセキュアIoTデバイス演習で習得します。

IoT-3：IoTシステムの脅威分析と脆弱性検査演習　(2 days, 8 units)

IoTシステムのセキュリティを開発・展開前に十分に検討することができるように、リスクを想定し、対策する計画を立てる脅威分析技術やそのツールを学修します。演習では、いくつかのIoTデバイスから構成されるスマートホームを想定し、実際に脅威分析を行います。更に、疑似環境を用い、脆弱性検査ツールを駆使しながら、そこに潜む脆弱性を検出するまでの技術を習得します。

IoT-4：IoTシステムの脆弱性検査発展演習　(1 day, 4 units)

IoTシステムのセキュリティ対策が脅威分析を行った通りに実施されているか確認出来るように、疑似環境への検査手順を検討して検査ツールを使って実際にIoT機器を検査して脆弱性を検出するとともに脆弱性を利用した脅威を再現するまでの技術を習得します。PCを各自で持参ください。

6. 最後に

2019年4月に「組込みエンジニアの教科書」という本を共著で出版した[15)]。この書籍では、組込み技術者が持たなければならないスキルを纏めた。例えばobjdumpやアセンブラ言語の解析など、組込み開発時のデバッグ方法に関する調査や実践を記載した。このときに組込み技術者は元来、いろいろな解析技術を持っていることを改めて認識した。JASA会員の方々が持つ組込み技術を生かし、セキュリティ対策をするホワイトハッカーになれるように、組込みシステムセキュリティ委員会は今後も情報発信を続ける予定である。

参考文献 1)：経済産業省：サイバー・フィジカル・セキュリティ対策フレームワーク (https://www.meti.go.jp/committee/kenkyukai/shoujo/sangyo_cyber/wg_1/pdf/001_06_00.pdf)
参考文献 2)：Techfirm Blog ： IoT （Internet of Things） とは？わかりやすく解説！ (https://www.techfirm.co.jp/blog/iot-definition#chap4)
参考文献 3)：株式会社 XERA：IoT とは？今さら聞けない IoT の本質を 15 の図でスッキリ学ぼう！ (https://xera.jp/entry/iot)
参考文献 4)：IT 用語辞典 e-Words：IoT【 Internet of Things 】モノのインターネット / インターネットオブシングス (http://e-words.jp/w/IoT.html)
参考文献 5)：KOMATSU：SMART CONSTRUCTION(https://smartconstruction.komatsu/introduction/ictkenki.html)
参考文献 6)：総務書：令和元年版 情報通信白書 (https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r01/pdf/01honpen.pdf)
参考文献 7)：総務省：IoT セキュリティ総合対策プログレスレポート 2019(https://www.soumu.go.jp/main_content/000623344.pdf)
参考文献 8)：足立照嘉、サイバー犯罪入門、幻冬舎 (https://www.gentosha.jp/store/ebook/detail/5748)
参考文献 9)：欧州 NIS 指令が医療規制対応にもたらすインパクト (https://monoist.atmarkit.co.jp/mn/articles/1803/16/news016.html)
参考文献 10)：【EU】サイバーセキュリティ法「NIS 指令」、重要な公共事業・IT 事業者の義務的体制整備進む (https://sustainablejapan.jp/2018/05/11/eu-nis-directive/32028)
参考文献 11)：JCIC:2019 年の海外法制度の展望 (https://www.j-cic.com/column/Cybersecurity-Privacy-Law.html)
参考文献 12)：経済産業省：サプライチェーンサイバーセキュリティ等に関する海外の動き 平成 30 年 (https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/pdf/003_04_00.pdf)
参考文献 13)：経済産業省：サプライチェーンサイバーセキュリティ等に関する海外の動き 平成 31 年 (https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_denryoku/pdf/004_03_04.pdf)
参考文献 14)：総務省：電気通信事業法に基づく端末機器の基準認証に関するガイドライン (第 1 版) (https://www.soumu.go.jp/main_content/000615696.pdf)
参考文献 15)：渡辺登、牧野進二、組込みエンジニアの教科書シーアンドアール研究所 (https://www.c-r.com/book/detail/1308)
参考文献 16)：医療情報システムの安全管理に関するガイドライン 第 5 版 (https://www.mhlw.go.jp/file/05-Shingikai-12601000-Seisakutoukatsukan-Sanjikanshitsu_Shakaihoshoutantou/0000166260.pdf)
参考文献 17)：経済産業省：サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）のポイント (https://www.meti.go.jp/press/2019/04/20190418002/20190418002-1.pdf)