組込みシステム技術協会機関誌
vol.73
Bulletin JASA
2020 Apr.

技術特集
組込みセキュリティ

一般社団法人
組込みシステム技術協会
Japan Embedded Systems Technology Association

JASAホームページ（https://www.jasa.or.jp/）をリニューアル。3本柱「ビジネスマッチング」「技術高度化」「人材育成」を中心に協会の活動を積極的に発信します

Contents

Bulletin JASA Apr. 2020 Vol.73

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

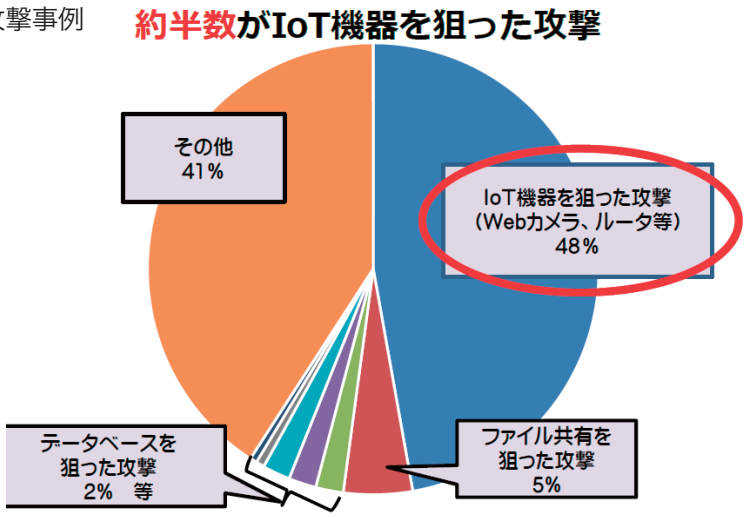
参考文献2)：Techfirm Blog：IoT(Internet of Things)とは？ わかりやすく解説！

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

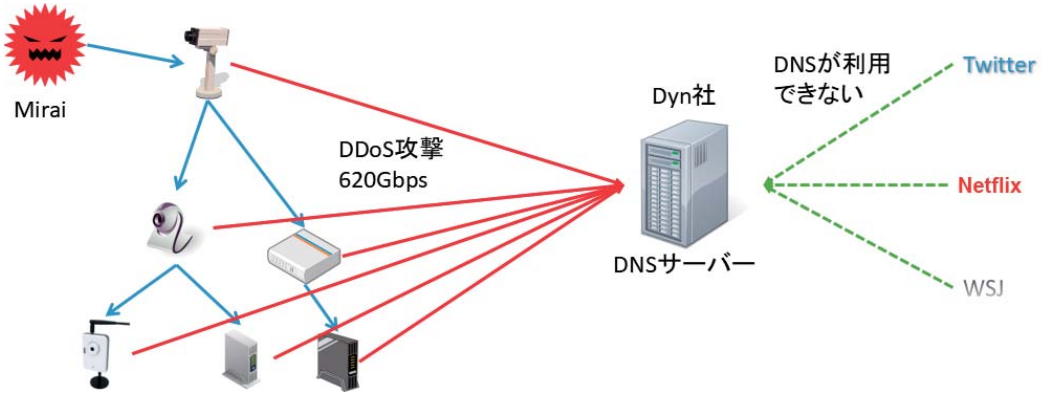
NICT(情報通信研究機構)のNICTER(Network Incident analysis Center for Tactical Emergency Response)システムによる2019年のサイバー攻撃の観測によると、半数以上がIoT機器を狙ったものだった(図1)[7),8)]。

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)

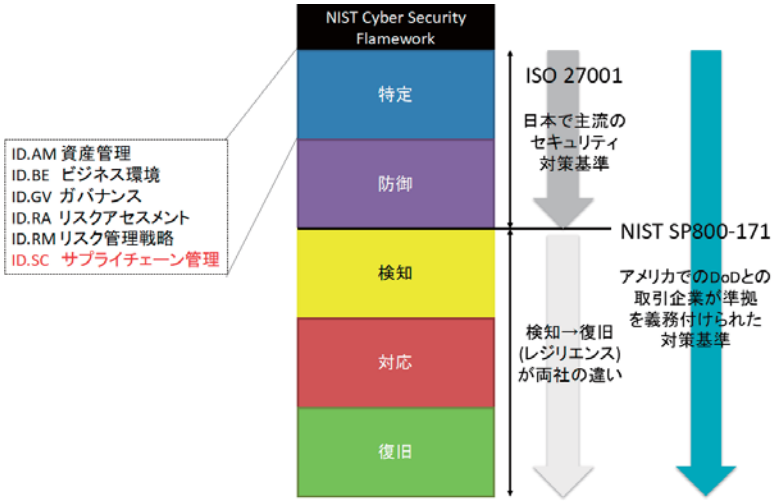


2. 世界・国内のセキュリティ動向

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]。

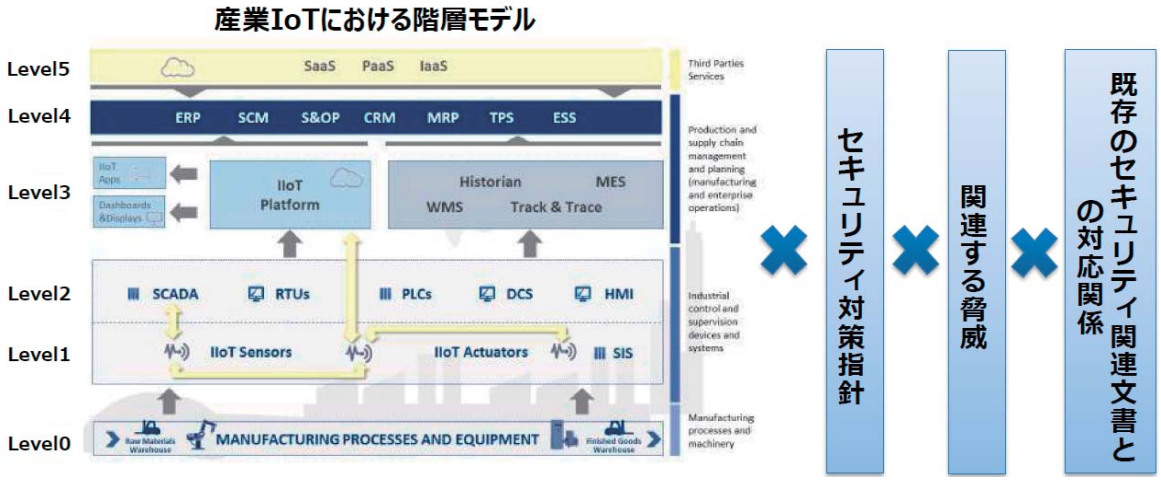
2.2. 欧州の動向

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



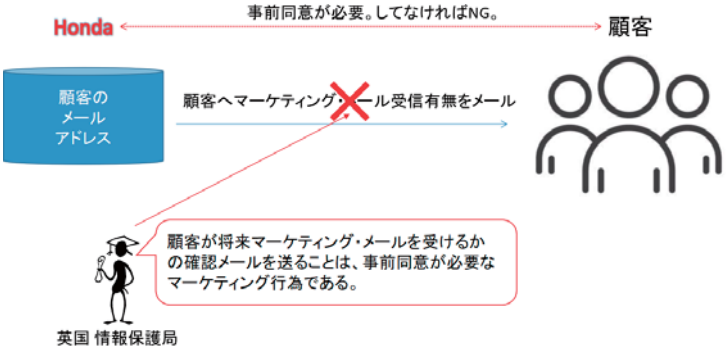
ENISA（欧州ネットワーク・情報セキュリティ機関）は、2018年11月に「Good Practices for Security of Internet of Things in the context of Smart Manufacturing」（図4）を公表した。

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。

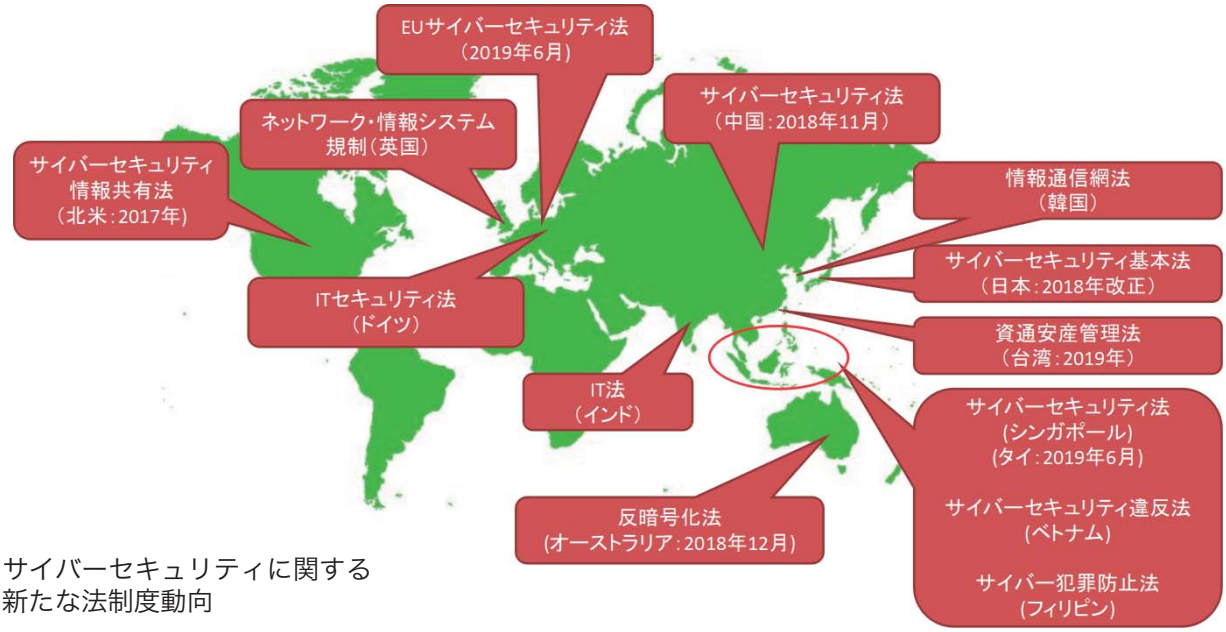


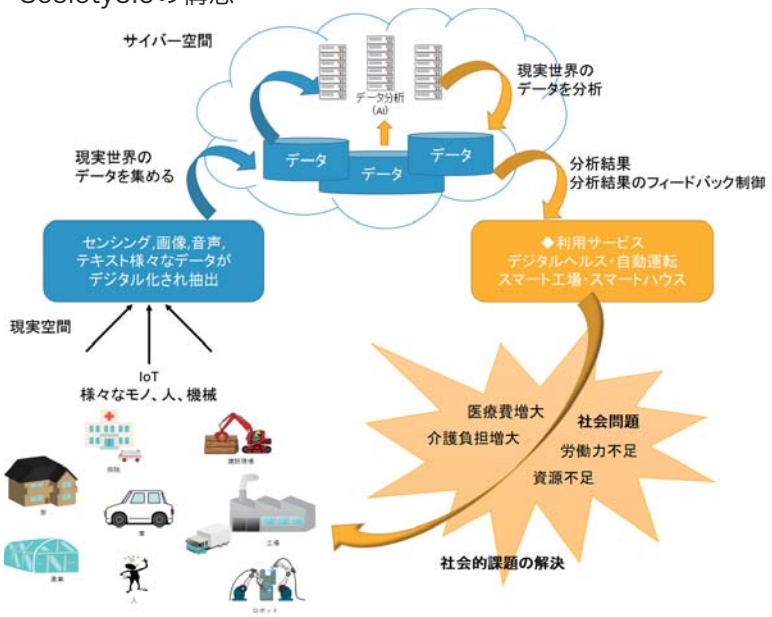
図6 サイバーセキュリティに関する新たな法制度動向

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

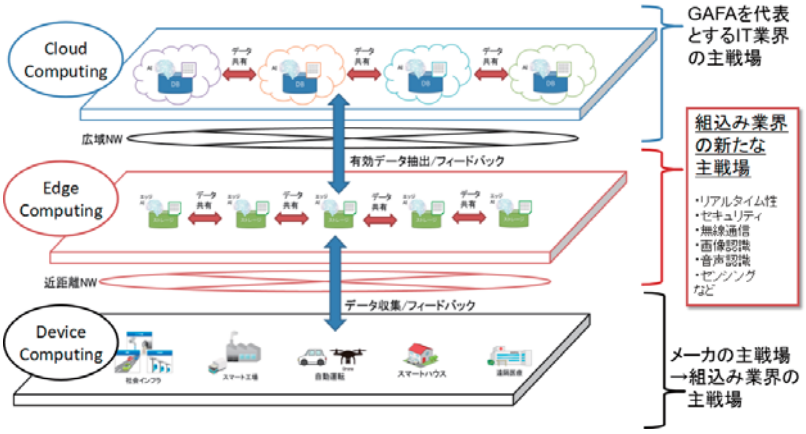
出典:参考文献 17を要約した

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



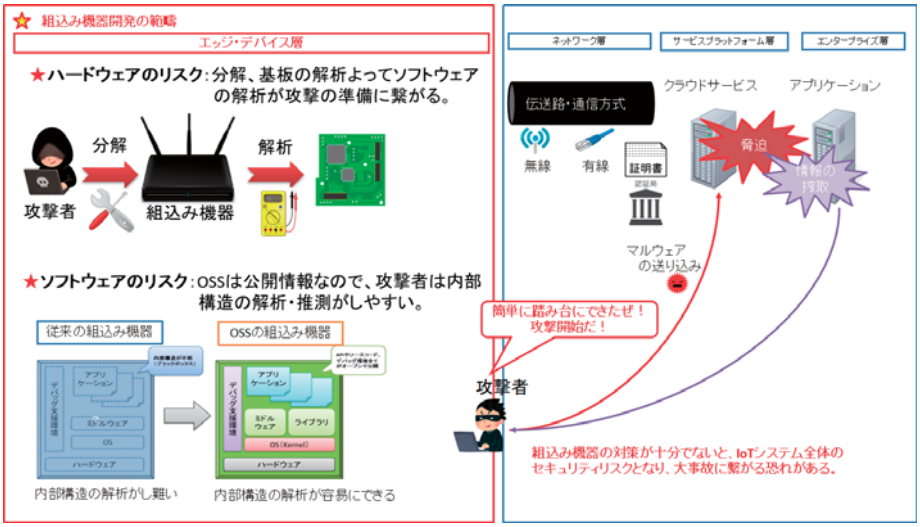
3. IoT製品開発におけるセキュリティ設計

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）

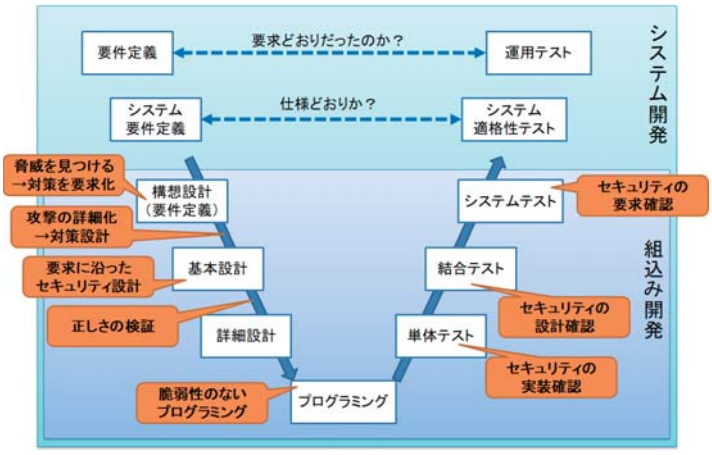


図11　脅威分析のポイント

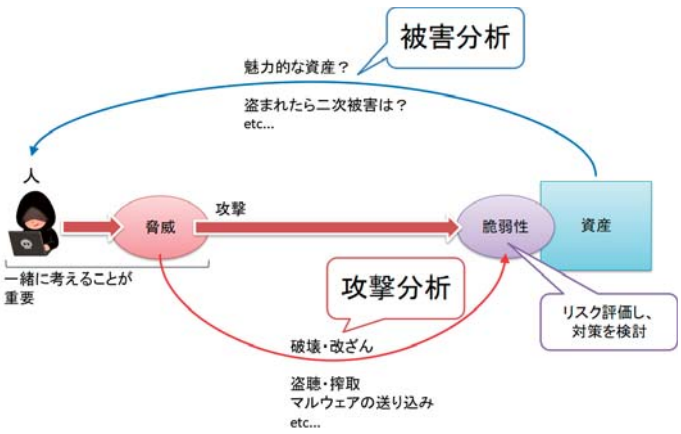


表5 被害分析の代表的な手法

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

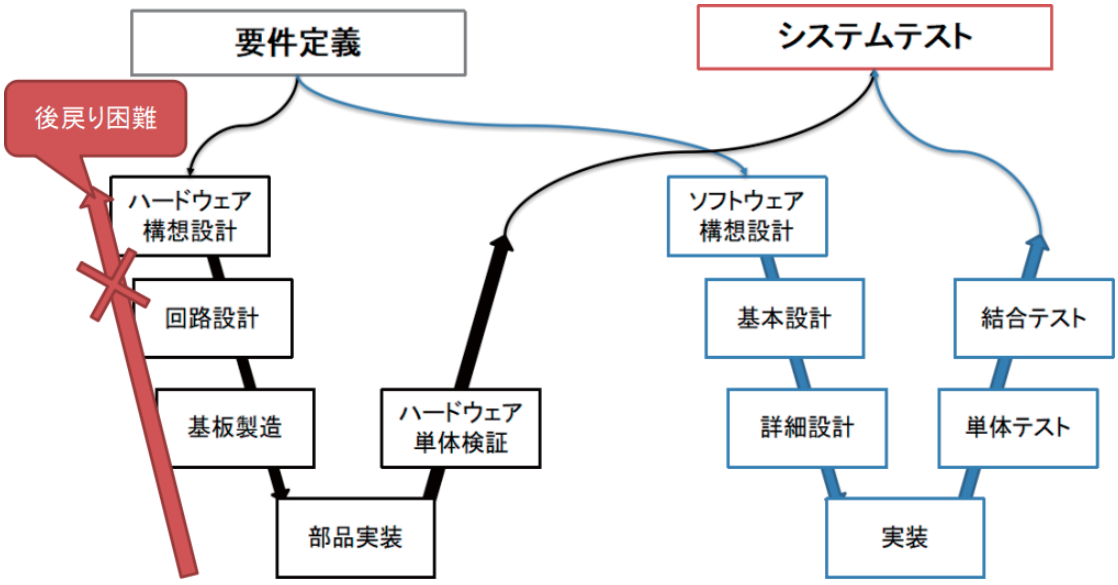
リスクの評価は、「アタックツリー」と呼ばれる２分木のツリーを用いるのが一般的である。アタックツリーでは、「その脅威が本当に起きるのか？」「脅威が起こることにより、影響が（リスク）があるか」を明確にする。FT（Fault Tree）に応用すること可能とされている。

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

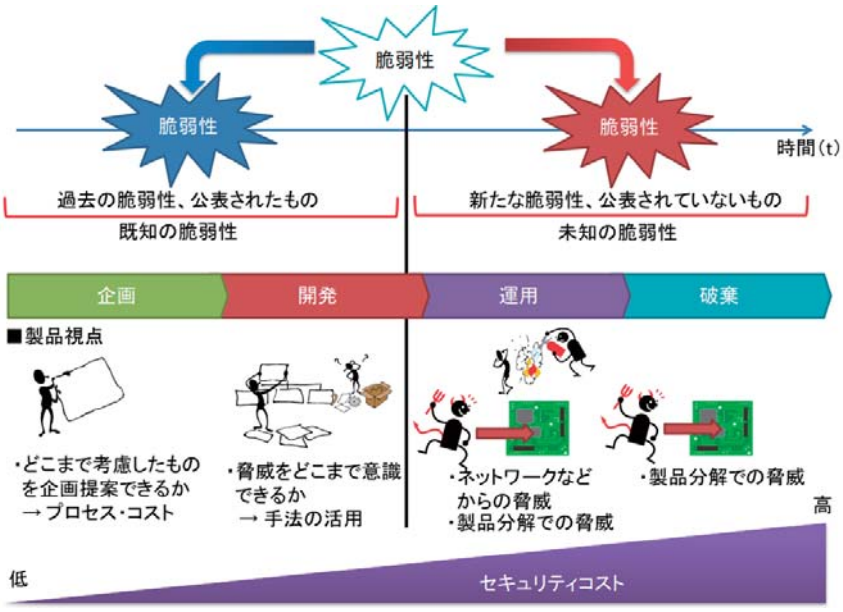
昨今の組込み機器は、多機能化や高機能化のために開発量が多くなっている。このため1社のみで対応することが難しく、複数社にまたがった開発が主流となっている。図15に、こうした状況を考慮したセキュリティ対策の考え方を示した。IoT機器開発のサプライチェーンに加わる会社や自社内の部門においてセキュリティ意識を高めるだけではなく、脆弱なシステムとならないように開発を管理・運用することが肝要である。

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

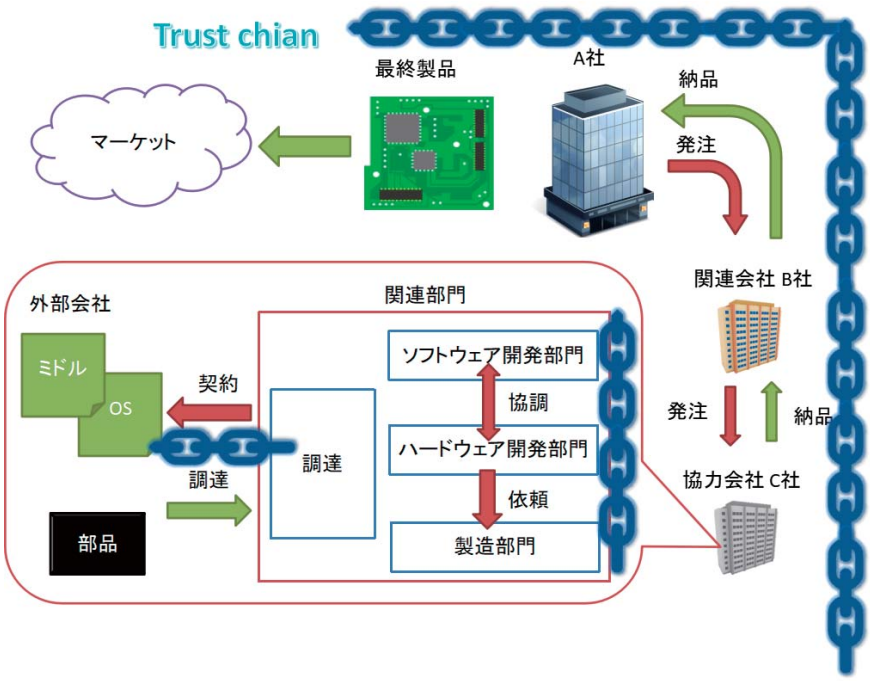


の対応が不可避である。セキュリティ対策の運用コストを想定することが重要になる。

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

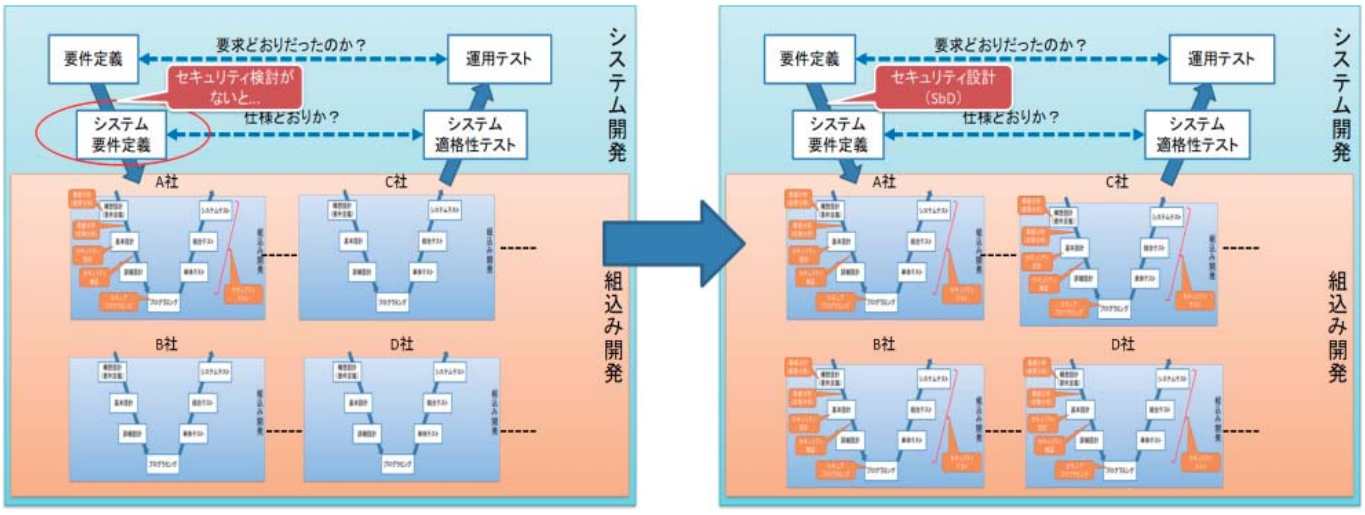
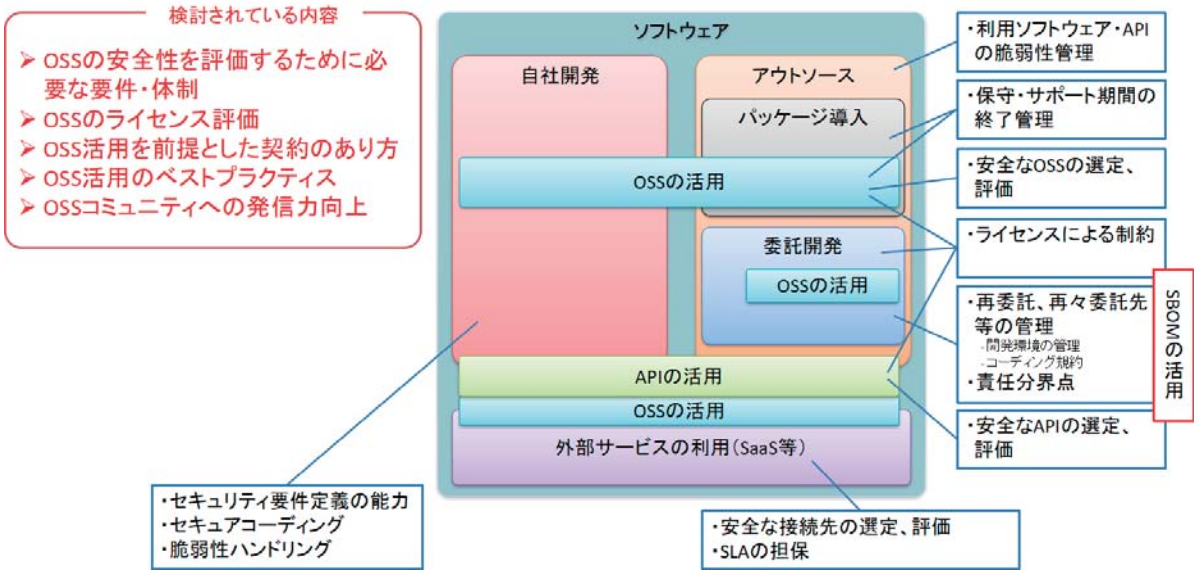


図17　SBOMのイメージ



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

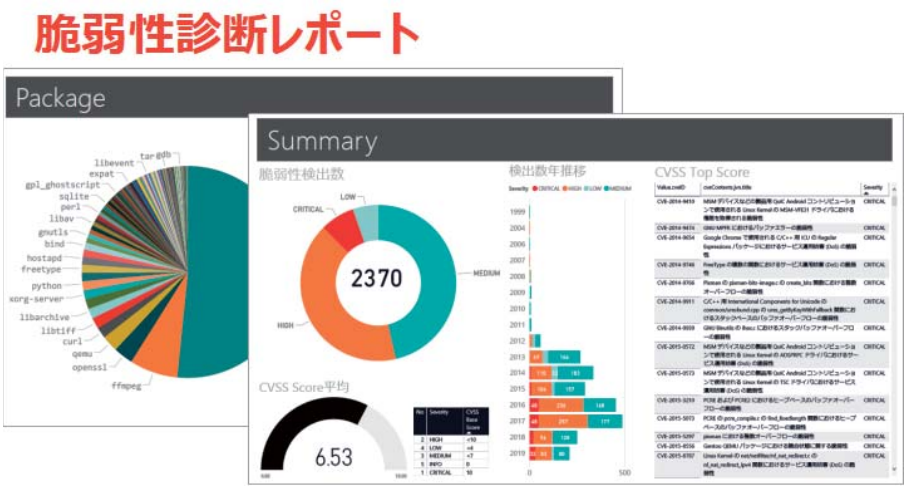


表9 OSSの主要なセキュリティ機能

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)

三幸電子株式会社

70年前から産業分野のシステムニーズに応え続ける開発力で新機軸となるサイネージ事業も好調に拡大中

名古屋市を拠点として、システム開発や店舗経営など多角的な事業を展開する三幸電子。古くからのJASA会員である同社の計測器製造から始まった開発の歴史は、デジタル化、オートメーション化の進展に合わせ高まった、さまざまな分野のシステム化ニーズに応えてきたものでもある。そのノウハウは、新たな柱として期待されるサイネージ事業に受け継がれている。一方で賃貸・飲食事業を展開し、街づくりにも貢献中だ。多角化にあっても「精神は組込み企業そのもの」として事業を推進する同社の代表取締役・香川利光氏に話を伺った。

代表取締役　香川　利光氏

計測器の製造受注を機に創業

産業用システム、LEDサイネージの開発からビル・マンション物件の賃貸、カフェや飲食店経営などにおよぶ事業の多角化で成長を続ける三幸電子。代表取締役の香川利光氏は「何がメインかわからないような状態ですが」と笑いながらも「計測器の製造が事業の始まりで、まさにシステムハウスそのものでした」と振り返る。もともと大学の非常勤講師や電機系企業に関わっていた創業者の元に、計測器がつくれるならと依頼されたことがきっかけ。1950年ごろに遡る話だが、なにせ電子部品がなかなか手に入らなかった時代、「進駐軍の払い下げの部品を使ってつくることもあったようです」

当時、計測器は大学の研究室や航空機関係の企業など多くの需要があった。必要だが手に入らない、そうした願いに応え副業的に始めたものが、賄えきれないほど注文が入るようになり事業化したという。

当初は受注生産だったが、80系68系といった8ビットCPUの登場を受け計測器の標準化に着手。制御装置や演算装置といったコンピュータの各種装置を1組の共通の線で共用するバスライン方式で構成し、注文に応じ組み合わせることで製造を続けた。「工業用としてリアルタイムOSを自社開発し、アプリケーションを乗せていきました。地域的に多い自動車関連や、工場のライン設備を集中監視して進捗管理や不良率の改善につなげるシステムなど提供しました」

当時発足された任意団体「中部システムハウス工業会」に参画し、会員企業とともにマイコン応用を事業としていく活動を開始、コンピュータ部門を立ち上げて製品化に拍車を掛けていった。その団体が現JASA中部支部となるもので、JASA設立時からの会員である。

ノウハウを活かし多ジャンルのシステム化に対応

計測器製造で培った計測技術は、工場の汚染物質量の計測などロガーシステムの開発へも広がった。以後、得られたノウハウはさまざまな分野のシステム化に活かされていくことになる。

そのひとつがパチンコ遊技機やホールのデータ管理。遊技業界は80年前後からデジタル化、コンピュータ化が急速に進み、1台1台から取得するリアルタイムの測定データを本部で集中管理するなどシステムニーズが高まった。商社からの依頼に「実績のあった生産管理システムとぴったり合っていた」としてシステム化に対応していった。

ホールシステムでは、客が得た出玉を店に預けておき後日再プレイができる「貯玉」の管理システムにも着手した。「出玉を預かり払い出しを遊技機でリアルタイムに行う。出玉はお金と一緒ですから、ホールにはATM機が1000台あるイメージ。要はバンキングシステムと同じです」。また顧客管理のノウハウも得て、ホテルのルーム管理や飲食店でのオーダーシステムなど、クラウドコンピューティングに通じるシステム化の実績も積んできた。

賃貸・飲食事業で業績拡大、街づくりにも貢献

「いまは顔認証で顧客管理ができないか進めている」と新たなチャレンジも始まっているが、多分野に広がるシステム開発には「昔から解決策を日々考え続けて

❶本社内のショールームでは取締役の香川俊宗氏が自社のサイネージを紹介してくれた。❷柱に設置できる曲面タイプのサイネージ。❸設置スペースに合わせて上にも左右にもつなぎ合わせて拡張できるタイプ。誰でも簡単に接続できる点も大きな特徴だ。

いまに至っている」と香川氏が評すベテラン世代の力が大きく働いているようだ。

「マイクロコンピュータができた頃から開発にかかわっている社員は、メモリやI/Oが足りないとか処理能力が足りないといった状況に悩み抜き対処してきたことで、クリエイティブな発想力が備わっています。お客さんからの無理な依頼に頭を悩ませることと同じで、それを解決する能力が基本的にシステムの設計力の基になっています」。若い世代になるほど開発環境が満たされ、そうした発想力が自ずと養われなくなってしまう傾向がある。そういう点では、「次の世代にどう継承していくかはひとつの課題」と香川氏は口元を引き締める。

また悩ましかった点が、案件の規模の大小で業績に浮き沈みが出てしまうこと。「通年で見れば悪くなくても、時期により開きが出てしまい平準化が難しい状況でした」。その打開策としての展開が賃貸事業、飲食事業へとつながっていった。

「昔は滞在する場所がなく駅裏と言っていた、名古屋駅の新幹線ホーム側に建てた飲食ビルやホテルも盛況です」と香川氏は街づくりの一環としての役割を口にする。飲食店は店子が見つからなかったため自社で始めた経緯があるそうだが「最初に声を掛けた相手が後になって後悔していました」というほどで、連日賑わいを見せているようだ。

新機軸となる サイネージ事業が成長中

現在のメインとなりつつあるのがサイネージ事業。これからの新機軸として「2年ほど前に恐る恐る始めた」そうで、香川氏はその経緯を次のように話す。「電子機器の価格は急落し、端末はスマートフォンで済みサーバはクラウドで済むといった状況で、かつて数億円の開発規模だったシステムが月額数百円、数千円で使えるようになった。この先、我々に何が残るのか考えると、せいぜいソフトウェアの使用料くらい。そこで新たな事業をということで、端末の領域に戻り事業化しました。デジタル情報の出力ということでは液晶もありますが、屋外で見たい、大きな画面で見たいといった、サイネージなら対応可能となるニーズは多々あります」

設置場所やスペースなど案件ごとに異なるため、ほとんどがカスタム品になるという。上や横につなげスペースに合わせて拡張できるユニットタイプ、丸い柱に設置可能な曲面タイプなどオリジナリティのある多彩なサイネージが開発されている。「ニーズに応えるために必要な素材は世界中を探してでも見つけて仕入れます」という香川氏の言葉からも、同社の真骨頂がうかがい知れる。

もうひとつ同社の特徴を表すものが公式広報キャラクターとして活躍中の「シンシア」。もともとは社内の意識改革として“性能だけではない、外見の重要さ”を認識してもらうためのアイデアだという。構図も含め考案した取締役の香川俊宗氏は「ハードウェアやシステムが均一化し、どのメーカーがつくっても横並びになるなか、差別化する要素はソフトウェアやコンテンツになる。それも見せ方の工夫ひとつで変わってきます。性能だけではないことのアピールのひとつの手段として具現化したものです」と説明してくれた。

さまざまな分野での実績を重ねていきながらも「精神は組込み業界の企業そのもの」と語る香川氏。だからこそJASA会員として、同じ会員企業と共有できる場は何より貴重に感じているという。「JASAの一番の魅力は同業者の生の声が直接聞けること。いま困っていることや開発しているものなど会話を通じて生きた情報が入ってくることです。もっともそうした情報が統計になったり白書になったり世に出回るとあまり価値もなくなりますが、みんなが情報交換できる場が持てることに会の意味があると思っています」とコメントをいただいた。

●「会社訪問」のコーナーでは、掲載を希望される会員企業を募集しています。お気軽にJASAまでお問い合わせください。

専務理事・武部桂史　＜遊び・情熱・そして目的を持て＞

JASAフィールドワーク

2018年がDX元年、2020年が5G元年。すでに、AI、IoTが事業推進に当たり前になっている時代になり、第4次産業革命がどうなっていくのか楽しみに思っていました。しかし、新型コロナウイルスで、産業界は大きなダメージを被りました。展示会、東京マラソンでの一般参加などの中止が多く発表され、テレワーク、時差通勤などの新しい取り組みが進んでいます。新しいニーズが生まれており、これにいかに対応するかを、常日頃から追い求めていく姿勢が必要です。今回は、チャレンジ精神あふれる、技術本部応用技術調査委員会の活動を語ってもらいます。

技術本部応用技術調査委員会

(株)アックス
代表取締役会長兼社長
竹岡 尚三

●活動方針

AI、アジャイル開発、RISC-Vなど先端的な分野への早期の取り組みと、OSSなど、組込み業界に馴染みにくい分野へ、細く長い取り組みを行っています。WG活動参加者のスキルアップのみではなく、WG活動から業界を牽引する大きなムーブメントにつなぐ下地作りに貢献できるように活動しています。本委員会下のWG活動から、委員会に格上げになった活動も多くあります。

●委員長としての意気込み

AI、エンタープライズ、IT分野などの先端技術や先端開発手法を組込み分野で生かそうとする人々の自由闊達にして愉快なる活動を全力で支援しています。

OSS活用WG

(株)アックス　代表取締役会長兼社長
竹岡 尚三

●WGの目標・運営の思い

オープンソース・ソフトウェア（無料ソフトウェア）という、営利企業にとっては諸刃の剣であるものの取り扱いについて、長く取り組んでいます。OSSは現在では、OS、コンパイラ、ミドルウェア、ロボット、AIなど、どの分野でも使用しなければ先端的なものづくりができない状態です。OSSライセンスやOSSの品質、製品開発時の取り扱いについて議論、調査、評価を行っています。OSSコンソーシアムという他のNPOと共同活動をしており、組込み女子活動を積極的に行っています。

●どのようなメンバー・開催頻度

メンバーとしては、OSSライセンス調査、OSS普及活動、OSSの実製品への取り込み開発、OSSのセキュリティ問題に興味がある人がいます。定例会の開催頻度は2ヶ月に1回の夕方。現在は、RISC-V用OSS調査と「組込みOSS鳥瞰図作成」と取り組んでいます。

●楽しいイベント・成果など

OSSコンソーシアムとの共同セミナ（外部対象）は年に3回ほど平日の日中に開催。過去には自動運転、ドローンなどの先端テーマで、著名講師を招いて開催しており、毎回好評です。

OSSコンソーシアムとの共同開催の女子ハンダ付け会（外部対象ハンズオン）は、年に1～3回程度、主に土曜日午後開催。女子ハンダ付け会は、社会人として組込み業界やIT業界で活躍している女性がハードウェアの入門として参加され、大変好評です。

過去の成果は、仮想化基本ソフトウェア（仮想マシン・モニタ）の組込み向け指標づくり、OSSに対するFuzzテスト試行など。

アジャイル研究WG

東海ソフト（株）
秋谷 勤

●WGの目標・運営の思い

～組込みソフトウェア開発業界がハッピーになりますように～

参加しているメンバーが各社で抱えている問題点を解決するため、既存のやり方にとらわれず、Web系で成果をあげているアジャイル開発の考え方も取り入れたいと活動を開始。アジャイル開発の考え方を学び、それを自社の課題に適応し、その試行結果を議論することで、更なる改善に繋げることを目的としています。

●どのようなメンバー・開催頻度

ベンダー企業の方、メーカーの方や開発者、品質保証、営業、企画など幅広いメンバーが参加しております。各々の視点による課題・不満があり、お互いがその視点を議論しあえる場となっています。

開催頻度は月1で議論を行っています。議論内容は1年の議論テーマを決め、そのテーマに沿った実際の現場での経験を説明し、改善方法などを模索するようにしています。

●楽しいイベント・成果など

年に1～2回、アジャイル経験が豊富な方たちと議論する会を設け、アジャイル研究会での議論の内容や、アジャイルでの疑問点などを話し合い、具体的なフィードバックを得ています。また、毎年ETにて経験発表を行っています。ETでは研究会以上に幅広い方たちに発表することで多くのフィードバックを得て、毎年WG自体の改善も行っています。

OpenEL WG

アップウィンドテクノロジー・インコーポレイテッド
代表取締役
中村 憲一

●WGの目標・運営の思い

OpenEL（Open Embedded Library）は、アクチュエータの制御やセンサからデータの取得を行うソフトウェアの実装仕様を標準化する組込みシステム向けのオープンなプラットフォームです。OpenEL WGでは、OpenEL仕様の策定、OpenELの国内外に

おける普及、OpenELの国際標準化の可能性の調査を行っています。

OpenELを国際標準とするためには、優れた仕様だけでは不十分であり、多くのユーザーに使っていただく必要があります。そのためには、多くのユーザーが使用しているプラットフォームに対応するのが得策であると考え、2020年度はETロボコンのプラットフォームとして採用されているLEGO社のEV3などへの対応を行います。また、ETロボコンに限らず、高度化する組込みシステム開発において品質と効率を上げるモデルベース開発が求められており、上流から下流まで一気通貫して開発できることが重要になっています。これを実現するためには、各レイヤーのツールベンダーの協力を得る必要があります。そして、各ツールでOpenELをサポートしていただくことにより、レイヤー間のインターフェースが統一されるため、モデルからソースコードを自動生成し、さらに自動テストまで行うことが可能になります。ゆえに、OpenELが組込みシステム開発において上流から下流まで一気通貫したソリューションを提供する核となるのです。さらに、組込みシステムセキュリティ委員会と連携し、セキュリティ対応を目的として仕様を強化することも検討しております。

いくら世界に勝る技術力があってもルール作りで負けてはビジネスになりません。また、ルールは政府に作ってもらうものではありません。そこで、本WGでは、自分たちの手でOpenELというルールを作り、オープンイノベーションを起こします。我々と一緒にゲームチェレンジャーとなって、世界市場を狙いましょう。メーカー、デバイスベンダー、ツールベンダー、OpenELを顧客に提案したい方々だけではなく、OpenELを勉強したい方々やOpenELをすぐに使ってみたい方々の参加も歓迎いたします。

●どのようなメンバー・開催頻度

デバイスベンダー、ツールベンダー、教育機関をはじめ各レイヤーの皆様に集まっていただき、毎月WGを開催しています。

●楽しいイベント・成果など

OpenEL 3.1の仕様書やサンプル実装をGitHubで公開しております。

https://github.com/openel

Windows、Mac、Linuxで動作するデバイスシミュレータを実装しておりますので、アクチュエータやセンサを用意しなくても、サンプルプログラムを動作させることが可能です。まずは、ダウンロードいただき、OpenELを試していただければと思います。

AI研究WG

(株) Bee
最高技術責任者
中村 仁昭

●WGの目標・運営の思い

AIのわかる組込み技術者の育成と、エッジデバイスAIの可能性について調査研究を行なっています。技術者の育成はセミナー形式で実施し、デモの選定と作成、発表までを1年間で行ない一般的なAI周辺の知識を学べるようにしています。また、エッジデバイスAIの可能性についてWG活動では最新のニュースについてキャッチアップと、個々のテーマについて議論、調査および評価などを行なっています。

●どのようなメンバー・開催頻度

基本的にAIに興味がある組込み技術者がメンバーとなり、セミナーなどを通してもっとエッジデバイスAIを追求したいメンバーがWG活動の中心となっています。セミナーは年5回、WG活動は年6回のペース、隔月で実施しています。

●楽しいイベント・成果など

セミナーのデモ発表会でプレゼンやデモ実施を行なっています。色々質問が来たり、用意された素材でなくその場で取った写真などでデモしてみたり、なかなかの盛り上がりで楽しいです。またWG活動ではAI関連のコンペにみんなで参加して結果を競ったりなども行なっています。

RISC-V WG

(株) 日立産機システム
小檜山 智久

●WGの目標・運営の思い

RISC-Vはハード、ソフトともにオープンソースかつロイヤリティフリーであり、加えて組込み機器で今後ますます重要となるセキュリティ機能の技術開発も進んでいることから、JASAとして押さえておくべき重要技術の1つと考えています。一方、使いこなしにはノウハウの積み重ねが必要です。これを会員各社が個別に行うと、ノウハウ取得までのリソース投資が各社個別に必要となることから、会員が相互に利用可能な共通プラットフォームの早期開発が望まれます。そこで、RISC-V WGでは次のような方針で取り組むことにしました。

1. 会員の協力で、会員が自由に活用可能なRISC-Vプラットフォームを開発する。
2. 開発したRISC-Vプラットフォームの活用・普及活動を行い、応用範囲を広げる。
3. 上記活動を通じRISC-Vコミュニティに貢献するとともにJASAのプレゼンス向上を図る。

●どのようなメンバー・開催頻度

JASAのメンバーでRISC-Vに興味を持つ方々が参加しています。FPGA実装、開発環境の移植、アプリケーションの開発など、幅広い分野のエキスパートの参加をお待ちしています。WGは毎月開催し、内外の有識者による講演、勉強会をはじめ、各社の取り組み事例やプロジェクトの進捗報告などを予定しています。

●楽しいイベント・成果など

今年度はリファレンスのFPGAボードを決め、RISC-Vの実装とArduino開発環境の移植、ブートローダの準備まで進めるのが目標です。出来上がったプラットフォームを使った作品を11月のET展に出展したいと考えています。

あとがき

オープンイノベーションで、世界中の知財がハイスピードで動いており、この委員会は、アンテナ高く情報収集をしています。ご興味ある方は積極的に参加してください。

世界中に拡散したコロナウイルスによって、会社経営に激震が走っています。製造業に関しては、その原材料などが計画通りに入手できない。物流がスムーズにいかなく、受注があっても納品できない。ソフト開発においては、まだ準備不足のテレワーキングなど新しい形での開発を余儀なくされており、効率はもちろん品質確保にも課題が残っています。

3.11以降、BCPについて、様々な取り組みが実施されてきましたが、自給率などの課題は、再度明確になりました。一方、テレワークなどは、IoTの応用時代を加速させています。工場を複数持つ企業では、従来であれば、一元管理、集中管理を目指して、システム構築を実施してきましたが、IoT、5G、AIを活用して分散、有機的に機能するシステムづくりはサバイバルの重要なポイントと考えられます。

問題点、困ったこと、協力要請をできるだけ早く発信して、助け合いながら、この危機的な時期を協会を上げて乗り切りましょう。

ビジネス創出人材育成コンテスト IoTイノベーションチャレンジ2020

IoTイノベーションチャレンジ実行委員会

参ス

今年で3回目を迎えるIoTイノベーションチャレンジで参加チームとスポンサーを募集しています。IoTイノベーションチャレンジは、JASAが主催する、これからの組込み業界を牽引できる人材の発掘・育成を目的としたアイデアソンです。

企業・団体・教育機関から参加チームを募り、いま産業界や社会に解決を求められている喫緊の課題「SDGs（Sustainable Development Goals：持続可能な開発目標）」が掲げる17のゴールから課題を抽出し、IoTを活用したソリューションを企画します。グループディスカッションなどを通して、ビジネスをデザインする能力と組込みシステム全体を俯瞰して捉えるセンスを養ってもらいます。

IoTイノベーションチャレンジの特徴の一つは、第一線の専門家による充実したセミナー・ワークショップです。参加者の通常の業務だけでは得られにくい、ビジネス、イノベーション、IoT要素技術、アーキテクチャといった、ビジネスの企画・検討に必要な内容に関する広範囲の教育を、6日にわたって受講することができます。

2019年の結果報告

2019年のIoTイノベーションチャレンジには41チームが参加しました。一流講師陣による6日間19コマのセミナー/ワークショップ、ベンチャー企業経営者によるトークセッション、相談会、書類審査、プレゼンテーション審査を経て、7チームが11月の決勝審査に進出しました。

決勝審査はEmbedded Technology 2019・IoT Technology2019展のメインステージです。5分間の熱気あふれるプレゼンテーションと、審査員との質疑応答が繰り広げられ、ダイキン情報システム(株)とダイキン工業（株）のチーム創発が優勝、(株)エクスモーションのChelsyが準優勝、(株)ビッツ東北事業所のSparrowが第3位、そして(株)シーエーシーの[ΣCAC]が特別賞をそれぞれ受賞しました。

2020年の新企画

昨年までのIoTイノベーションチャレンジでは、多くのチームが「課題設定」の難しさを挙げていました。この声に応えるべく、NPO法人人間中心設計推進機構による新たなワークショップ“開発チームのみんな！「街に出よう！」”を開催します。実際に利用現場を観ることで、課題の発見やソリューションの創発につなげる手法を学びます。

チーム・ビルディング・ワークショップも拡充します。チームメンテナンスツール「Monica」を使ったセッションと、レゴ シリアスプレイ組織論の3つのセッションを行います。

IoTイノベーションチャレンジには新しいビジネスを考える技術者が集まります。ビジネスのデザインのヒントが数多くあります。企業にとって宝の山です。ぜひ、参加をご検討ください。

またIoTイノベーションチャレンジはスポンサーの皆さまに支えられたコンテストです。スポンサーにはセミナーの受講資格などの特典があります。多くの企業にスポンサーとして手を挙げていただきたいと思います。特典に応じてダイヤモンドスポンサー、プラチナスポンサー、パールスポンサー、エンジェルスポンサー、プライズスポンサーと5つの枠をご用意しております。

●詳細資料は、こちらをご覧ください。
iot-innovation-challenge.net

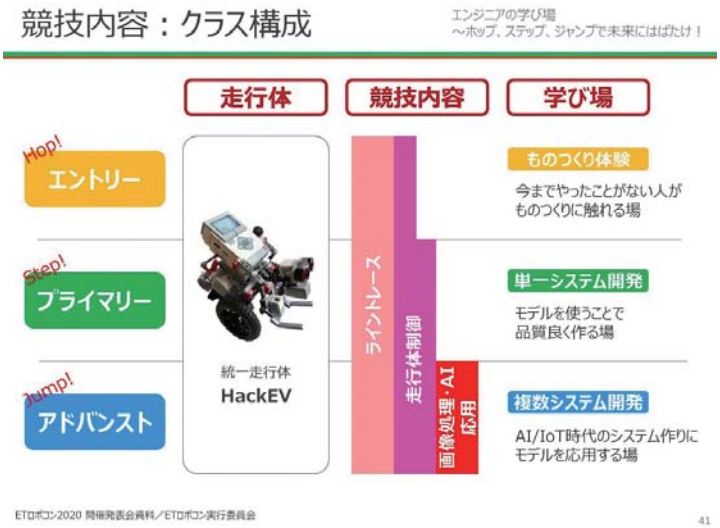
1月28日、CES2020報告会を開催しました。これまで3年連続でCESを見てきて、その変遷とこれからの方向性のようなものをお話しました。今年はソニー、トヨタ自動車からクルマ関係の目新しい発表がありましたが、他に斬新な発表がなかったため、相対的に目立ったと理解したほうが良いでしょう。どちらも自社製品をユーザ視点で使ったらどうなるか確認してみたい、という思いは共通です。

2年前は目新しい技術が目白押しで感激しました。故に若い人にも見てほしいと、ETロボコン ガレッジニア部門 最優秀チームにもCESに参加いただきましたが、去年はそれがだんだん当たり前になっていき、今年はすでに限定的にサービスイン、もしくは提供中となり、目立つも

加チーム
&
ポンサー
募集中

ETロボコン2020に参加しませんか

ETロボコン実行委員会



AI（人工知能）やIoT（モノのインターネット）などの新しい技術への注目度が増しています。世の中の変化のスピードが速い時代をどうやって渡り合うか、『これまで通りの開発手法や、モデルを書くだけでいいのか』とETロボコンは自問自答を繰り返し、早いもので19年目を迎えました。2020年の新しい取り組みとして、プログラムやモデリング未経験者向けに「エントリークラス」を新設。組込みエンジニアはもちろん、エンジニア以外の職種や他業界からも積極的に参加してもらい具体的な題材を体験する「学ぶ場」を提供し、体験しながら学ぶ価値を感じてもらうためです。従来から存在する「モデルを使うことで品質を良くする場」を体験できるプライマリークラス、「課題をモデルにて攻略し、AIによる画像認識の新しい技術を使う場」を体験できるアドバンストクラス、初心者からベテランまで幅広い層がそれぞれのレベルに合わせて体験できる「場」で、相互に刺激しながらやりがいと成長を実感し、組織と共に自分も成長することができるのがETロボコン最大の見どころ、今こそ「人財育成と組織の醸成」に大きく舵を切る決断をしませんか？

※ETロボコンとは、一般的なロボットコンテストと異なり「ソフトウェア重視の教育コンテスト」である点が特徴で、共通のロボットによるコース走行のタイム成績に加え、高品質な組込み開発に欠かせない設計技法（モデリング）も評価対象となる。2019年には組込みエンジニアへの教育効果が評価され、社会の情報化促進に貢献した団体に与えられる令和元年度「情報化促進貢献個人等表彰」経済産業大臣賞を受賞した。

CES2020報告会

ETロボコン共同企画委員長　江口 亨

のが少なくなった気がします。AIや5Gのようなバズワードを全面に出す展示は影を潜めました。代わりに、これまで規模が小さかったHealth/Wellnessに関する出展が目立ってきて、単に体を動かしてトレーニングを数値化するだけでなく、ゲーム性を持たせて楽しく運動するマシンが登場。また、IoTの単語はSmart Homeに差し替わり、技術ではなく目的を目指す言葉に交代しています。

ソニーの試作車VISION-S


スキー大回転風のトレーニングマシン

トランプ大統領の影響か、中国からの出展パワーが幾分落ちました。話題のHUAWEIは大人しくTCLも控え気味。代わってLG、Samsungの曲がる・大型高精細ディスプレイが幅を利かせています。ですから中国勢の本気を見に、6月に上海で開催されるCES Asiaに行く段取りをつけましたが、この新型コロナウイルス騒ぎで開催されるのか、開催されたとしても日本から入国できるのか、今から心配しているところです。

ET・IoT Technology NAGOYA 2020 開催報告

2020.2.5-6
吹上ホール（名古屋市中小企業振興会館）

ものづくり名古屋で最新の組込み×エッジテクノロジーを紹介

2月5日（水）、6日（木）に名古屋市・吹上ホール（名古屋市中小企業振興会館）で、協会主催のET・IoT Technology NAGOYA2020が開催された。TECH Biz EXPO（主催：名古屋国際見本市委員会、名古屋産業振興公社）、フロンティア21エレクトロニクスショー（主催：中部エレクトロニクス振興会）との同時開催としては、今回で2回目となる。

自動車産業をはじめとした“ものづくり”の一大拠点である名古屋圏らしく、組込み関連はもちろん、電気・電子系、機械系、部品系、製造装置系などの基盤技術が一堂に会した展示会となった。初日の開場前から多くの来場者が吹上ホールの外に列をつくり、中部圏の技術者や企画担当者の関心の高さを窺わせた。出展規模は137社・団体と2019年を上回った。製品やソリューションの展示と30以上の専門セミナーにより、2日間の会期中に1万201人の来場者を集めた。

ET・IoT展では、IoTやエッジ、組込みAI、セキュリティ、開発・設計に関連したソリューションや製品の展示のほか、それぞれ3件の基調講演と技術本部による専門セミナーで、JASAならではの情報発信を行った。展示会場で熱心に説明員の話に耳を傾ける来場者や、旬な話題を取り上げた基調講演や専門セミナーで熱心にメモを取る受講者の姿が印象的だった。

基調講演では、（株）DeepXの那須野薫代表取締役、エヌビディア合同会社の齋藤弘樹事業部長、Idein（株）の中村晃一代表取締役が登壇し、AI関連の最新動向を紹介した。いずれも多くの出席者が会場を埋め、旬の情報に聞き入っていた。

このほか好評を博したのが、主催者企画の出展者向けネットワークイベント「中部地域自動車業界技術者との情報交換会」である。トヨタ自動車をはじめ、デンソー、アイシン精機、豊田自動織機、東海理化の第一線に立つ技術者が、電動化や自動運転といったCASE関連の動向と将来展望、現状の課題について講演するとともに、出席者の質問に答えた。他では聞けないディープな話題の数々は、珠玉の情報になったのは間違いない。

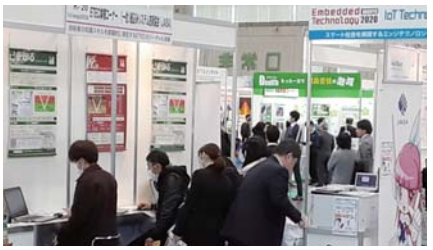
ネットワークイベントの後には名刺交換会（懇親会）が催された。トヨタグループの講演者との情報交換や人脈作りの場として、さらに盛り上がりを見せた。

JASAでは，組込み×エッジテクノロジー総合展として「ET・IoT Technology」を横浜（11月）、大阪（7月）、名古屋にて開催している。最新情報は公式サイトをご覧いただきたい。
https://www.jasa.or.jp/expo/

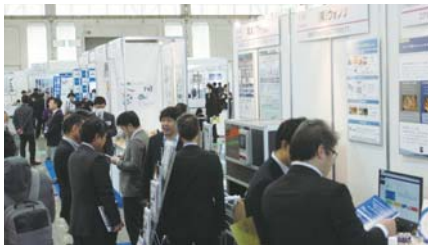
DeepX
那須野 薫 氏

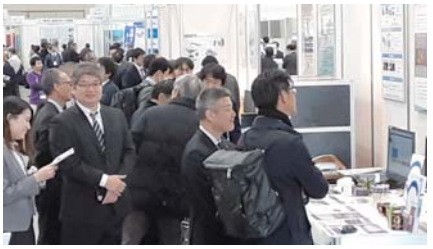
エヌビディア
齋藤 弘樹 氏

Idein
中村 晃一 氏



JASA中部支部・青木義彦支部長も出席した開会式の様子（左）。
JASAブースでは協会活動とETECをアピール（右）。





25社・団体が参加した出展ブースの様子。展示テーブルスタイルのコンパクトな設計に、各社から“今年のイチオシ”となる最新のソリューションが展示紹介された。

セミナー会場の様子。終了後は質問など講師と積極的に接する聴講者が多く、貴重な交流時間となっていた。JASAでは3つの委員会・WGが研究成果を発表、多くの聴講者で賑わった。

九州企業視察および九州支部交流会開催報告

関東支部
支部長　神山 裕司

九州－関東支部間の協業を促進

去る1月23日(木)、24日(金)に関東支部主催にて、九州企業視察および九州支部交流会を開催致しましたので報告します。

本視察の目的は、関東支部会員への九州地区ビジネスに関する情報提供と共に支部間交流を深めることで会員各位の新たなビジネス開拓のキッカケとなることを企図しました。

[開催概要]
日程：2020年1月23日(木)、24日(金)
会員参加人数：関東支部14名、九州支部5名
視察企業：株式会社三松、
　　大分朝日放送株式会社



初日は、工場のIoT化に取り組まれ九州内外で注目を集めている株式会社三松を視察しました。代表取締役 田名部徹朗様より、「三松スマートファクトリー構想」をご説明頂きました。三松は金属部品と機械組立の事業を主として創立された企業ですが、現在は半導体・液晶製造装置から微細な電子部品に至る金属部品の加工だけでなく、モノづくりに関わる製造・アッセンブリ・設計と事業を拡大し、1日30件を超える依頼を受け生産しているとの事です。オーダーに対して、「一個からでもお作りする」「品質にこだわる」「納期をきちんと守る」を信念としています。

受注量・製品・サービスが増えるにあたり「生産の改善活動」を進めてきた結果が、工場のIoT化へと繋がったそうです。社員の平均年齢が35歳と若く社内教育が整備されており、「三松大学」と呼ばれる技術教育で社員が一人三役を担えることを推進しています。忙しい部門の業務を全社員一丸となってフォローできることが工程毎のタイムラグを埋め、納期厳守に繋がっています。参加者からは普段見ることのない製造業の現場管理・生産管理状況を視察ができ、とても有意義であったとの感想を頂きました。

その後、博多へ移動し光安九州支部長を含めた九州支部会員5名、九州大学の福田主幹教授、特定非営利活動法人QUEST(旧名称「九州組込みソフトウェアコンソーシアム」)の芦原副理事長を含む4名の理事の方々に参加頂き、総勢24名にて支部間交流と九州地域の組込みの状況についてのヒアリング及び情報交換を行いました。各テーブルにて活発かつ熱いディスカッションが行われ、支部間交流の意義が表れました。

2日目は、全国の放送局に先駆けフルハイビジョンの4倍の画素数となる「4K」に対応した編集センターを開設し注目を集めている、大分朝日放送株式会社を視察致しました。初めに役員待遇技術担当の塩川技術局長より御挨拶頂いた後、技術局澤村副部長より大分朝日放送の取組みについてご説明頂きました。



その後、澤村副部長と泥谷総務局長の2班に分かれて局内を案内頂きました。大分朝日放送は撮影から編集，音声処理，プレビューまで一貫した4Kシステムを導入し、この4Kシステムを武器に海外進出や日本国内ケーブルテレビとの連携ビジネスを拡大しています。この取組みは、総務省のモデル事業としても認められています。また地元への貢献を目指しており、「JIMOTTO(じもっと)」をスローガンに各種イベントや事業展開を行っています。イベント運営は「全社体制」をモットーに、全従業員がスタッフとして“おもてなし”する「OAB感謝祭」などを実現しています。このイベント運営のノウハウ活かし、大分県や大分市から委託を受けて婚活事業で地元の活性化を図るなど、放送局として珍しい取組みです。

また「全社体制」のモットーはイベントのみならず、地震や台風などの緊急事態の報道の際にも営業，総務，報道など部門の垣根を越え、各社員が自身の手伝える業務を分担し、迅速な報道を行うことにも生かされています。

2日間、駆け足での福岡/大分の視察ではありましたが、普段、あまり接することのない製造工場や放送局を実際に視察することができ、とても有意義な経験となりました。快く企業視察を受け入れて頂きました株式会社三松と大分朝日放送株式会社の両社に感謝するとともに、両社の社員の方々の暖かな配慮や明るい挨拶に、自分達の足元を見直す機会ともなりました。

横田英史の 書籍紹介コーナー

ザ・ワン・デバイス
～iPhoneという奇跡の“生態系”はいかに誕生したか～

ブライアン・マーチャント、倉田幸信・訳
ダイヤモンド社　2,200円（税込）

ちょっと風変わりなiPhone開発物語。ジョブズの気分に左右され、意外にも行き当たりばったり的だった開発プロセスを明らかにする。ハードとソフトの開発過程だけではなく、Liイオン電池の原料の採掘現場、中国深センのフォックスコンの工場やiPhoneの部品のブラックマーケットに潜入したりと、多角的な取材を敢行している。

好奇心旺盛な雑誌記者らしい視点は悪くない。本書のカバー範囲は広く、ARMチップ、マルチタッチのユーザインタフェース、タッチスクリーン、ゴリラガラス、カメラの手ぶれ補正、センサー類（加速度、近接、磁気、GPS）について、それぞれ1章を割く。手ぶれ補正技術の開発者として日本人が登場する。凄いのはフォックスコンの工場に潜入したレポートだ。セキュリティが厳重な工場に潜り込んだ経緯や想像を絶する内部の実態を明らかにする。

イノベーションは、万能ではない

西村吉雄
日経BP　2,750円（税込）

イノベーションは経済的な発展に必ずしもつながらないことをデータと歴史的事実を踏まえつつ明らかにし、「イノベーション万能論」に警鐘を鳴らす。ICTの領域でイノベーションは起こっているのに、経済成長につながっていない。「何故か」について検証する。バックデータを駆使する手法は、安定感と説得力をもたらしている。

筆者は「イノベーションとは何か」から説き起こし、研究→開発→生産→販売→市場と連鎖するリニアモデルの限界、中央研究所の終焉、企業家/シリコンバレーの台頭などを切り口に、成長を生み出すものは何かについて論じる。

第3部「ICTイノベーションズ」で取り上げるのは半導体と電気通信。前者ではマイクロプロセッサ、後者ではインターネットをイノベーションの事例として紹介する。筆者が得意とする半導体の章は読み応えがある。

AI時代の労働の哲学

稲葉振一郎
講談社　1,760円（税込）

「AIの発展が社会に、とりわけ労働に及ぼすインパクトについて考える際に、我々はどのような知的道具立てを既に持っているのかを点検」した書。筆者はAIのインパクトを、「資本主義経済のもとで機械化によって仕事が奪われるインパクト」についてのカール・マルクスなどの議論と対比しながら筆を進める。資本主義とは何かにまで言及しており興味深い。

「AIの労働に対するインパクトは、資本主義のもとでの技術革新（機械化）や組織変革と変わらない」「AIがもたらす本質的な新しい問題はない」「AIが我々の社会の構造を根本的に変えるとは思えない」というのが筆者の結論である。ただし、AIが自律的な判断・行動能力を備え、道具から離れ「人」と「モノ」との中間にある存在になり始めたら、従来の伝統的な道徳や法の枠組みを揺るがす可能性があるとする。

マーケティングのSONY
～市場を創り出すDNA～

立石泰則
岩波書店　2,640円（税込）

ソニーの強さを営業やマーケティングの視点から描いたノンフィクション。ソニーの取材を30年近く続けているノンフィクション作家による丹念な取材がベースになっており、読み応え十分だ。

筆者の問題意識は、なぜ日本の家電産業が欧州と同じ衰退の道を選んだのかという点にある。本書は、その過程を描き、衰退の理由を解明するライフワークの第1弾と位置づける。経営の判断が現場にどのような影響を与え、現場がどう対応したかをソニーを題材に検証しており興味深い。

筆者は黎明期から、ソニー神話が生まれた時期、ソニーショックの迷走期、もがきながら再浮上中の現在まで、マーケティングの変遷を追っている。ソニーの創業者の一人である盛田昭夫に始まる「市場を作り出すDNA」をうまく描き出しているのは流石である。盛田が語った「マーケティングはエデュケーションである」は卓見だ。

横田 英史（yokota@et-lab.biz）
1956年大阪生まれ。1980年京都大学工学部電気工学科卒。1982年京都大学工学研究科修了。
川崎重工業技術開発本部でのエンジニア経験を経て、1986年日経マグロウヒル（現日経BP社）に入社。日経エレクトロニクス記者、同副編集長、BizIT（現xTECH）編集長を経て、2001年11月日経コンピュータ編集長に就任。2003年3月発行人を兼務。
2004年11月、日経バイト発行人兼編集長。その後、日経BP社執行役員を経て、2013年1月、日経BPコンサルティング取締役、2016年日経BPソリューションズ代表取締役に就任。2018年3月退任。
2018年4月から日経BP社に戻り、日経BP総合研究所 グリーンテックラボ 主席研究員、2018年10月退社。2018年11月ETラボ代表、2019年6月当協会理事、現在に至る。
記者時代の専門分野は、コンピュータ・アーキテクチャ、コンピュータ・ハードウエア、OS、ハードディスク装置、組込み制御、知的財産権、環境問題など。
＊本書評の内容は横田個人の意見であり、所属する団体の見解とは関係がありません。

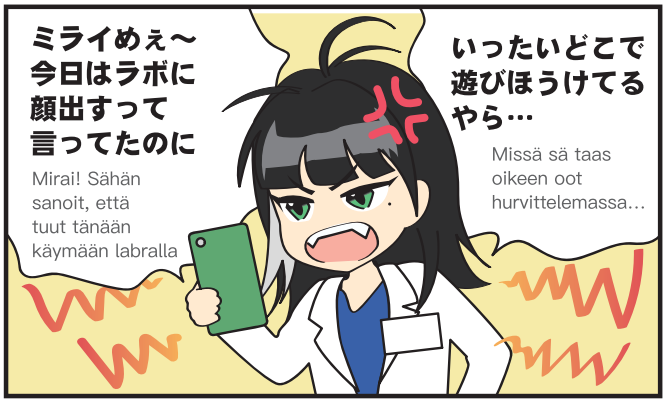
クミコ・ミライ ハンダフルワールド 第11話

Kumiko Mirai ihmeellinen maailma osa 11

フィンランド語訳：アラヤ株式会社
（翻訳者：シリヤ イヤス）の提供です。
Suomenkielisen käännöksen tarjoaa: Alaya Inc.
(Kääntäjä: Silja Ijas)

この漫画はダイナフォントを使用しています。
Tässä mangassa käytetään DynaFont-kirjasintyyppiä.

慌てミライ① Hötky-Mirai ①



Jatkuu oikealla
右へつづく

慌てミライ② Hötky-Mirai ②

あせったジャサ〜〜博士にはお詫びにスタンププレゼントしたジャサ！（ミライちゃん）
Tulipa taas hötkyiltyä…
Lähetin proffalle anteeksipyyntönä tarrat lahjaksi! (Mirai)

JASA 会員一覧

（2020年4月）

北海道支部

HISホールディングス株式会社	http://www.hokuyois.co.jp/
株式会社技研工房	https://www.giken-k.biz/
株式会社コア 北海道カンパニー	http://www.core.co.jp/
北都システム株式会社	https://www.hscnet.co.jp/
株式会社北斗電子	http://www.hokutodenshi.co.jp/

東北支部

株式会社イーアールアイ	http://www.erii.co.jp/
株式会社コア 東関東カンパニー	http://www.core.co.jp/
株式会社セントラル情報センター 東北支社	https://www.cic-kk.co.jp/
国立大学法人東北大学 情報科学研究科教授 青木研究室	http://www.tohoku.ac.jp/
株式会社ビッツ 東北事業所	https://www.bits.co.jp/

関東支部

一般社団法人IIOT	https://www.iiot.or.jp/
IARシステムズ株式会社	https://www.iar.com/jp/
株式会社アイ・エス・ビー	https://www.isb.co.jp/
一般社団法人iCD協会	https://www.icda.or.jp/
一般社団法人ICT CONNECT 21	http://ictconnect21.jp/
一般社団法人IT検証産業協会	https://www.ivia.or.jp/
アストロデザイン株式会社	https://www.astrodesign.co.jp/
株式会社アックス	http://www.axe.bz/
アップウィンドテクノロジー・インコーポレイテッド	http://www.upwind-technology.com/
アドバンスデザインテクノロジー株式会社	http://www.adte.co.jp/
アドバンストシステムズ株式会社	http://www.asco.jp/
株式会社アドバンスド・データ・コントロールズ	http://www.adac.co.jp/
株式会社アフレル 東京支社	https://afrel.co.jp/
アンドールシステムサポート株式会社	https://www.andor.jp/
株式会社イーテクノロジー	https://e-technology.co.jp/
イマジネーションテクノロジーズ株式会社	https://www.imgtec.com/
株式会社インサイトワン	http://www.insight-one.co.jp/
株式会社インフォテック・サーブ	http://www.infotech-s.co.jp/
株式会社ウェーブ	https://www.waveco.co.jp/
ウットゥンガ株式会社	https://www.utthunga.com/
株式会社エクスモーション	https://www.exmotion.co.jp/
株式会社SRA	https://www.sra.co.jp/
STマイクロエレクトロニクス株式会社	https://www.st.com/
株式会社NS・コンピュータサービス エンベデッド本部	https://nscs.jp/
株式会社NTTデータ・ニューソン	https://www.newson.co.jp/
株式会社エヌデーデー	https://www.nddhq.co.jp/
株式会社エンファシス	http://www.emfasys.co.jp/
株式会社エンベックスエデュケーション	https://www.embex-edu.com/
オープンテクノロジー株式会社	http://www.open-tec.co.jp/
ガイオ・テクノロジー株式会社	https://www.gaio.co.jp/
株式会社金沢エンジニアリングシステムズ	https://www.kanazawa-es.com/
合同会社Keychain	https://www.keychain.io/
株式会社ギガ	https://www.giga.core.co.jp/
キャッツ株式会社	https://www.zipc.com/
一般社団法人行政情報システム研究所	https://www.iais.or.jp/
京都マイクロコンピュータ株式会社	http://www.kmckk.co.jp/
特定非営利活動法人組込みソフトウェア管理者・技術者育成研究会	http://www.sessame.jp/
一般社団法人組込みマルチコアコンソーシアム	https://www.embeddedmulticore.org/
株式会社グレープシステム	https://www.grape.co.jp/
株式会社クレスコ	https://www.cresco.co.jp/
株式会社グローセル	http://www.glosel.co.jp/
グローバルイノベーションコンサルティング株式会社	https://www.gicip.com/
株式会社コア	http://www.core.co.jp/
株式会社コスモ	http://www.cosmo.co.jp/
株式会社コンセプトアンドデザイン	https://www.candd.co.jp/
一般社団法人コンピュータソフトウェア協会	http://www.csaj.jp/
サイバートラスト株式会社	https://www.cybertrust.co.jp/
佐鳥電機株式会社	http://www.satori.co.jp/
CICホールディングス株式会社	http://www.cic.kk.co.jp/
株式会社CSAホールディングス	http://csa-h.co.jp/
CQ出版株式会社	http://www.cqpub.co.jp/
JRCエンジニアリング株式会社	http://www.jrce.co.jp/
株式会社ジェーエフピー	http://www.jfp.co.jp/
株式会社JTBコミュニケーションデザイン	https://www.jtbcom.co.jp/
一般社団法人J-TEA	http://www.j-tea.jp/
ジェネシス株式会社	http://www.genesys.gr.jp/
株式会社システムクラフト	http://www.scinet.co.jp/
株式会社システムサイエンス研究所	http://www.sylc.co.jp/
一般社団法人重要生活機器連携セキュリティ協議会	http://www.ccds.or.jp/
一般社団法人情報サービス産業協会	https://www.jisa.or.jp/
一般社団法人スキルマネージメント協会	http://www.skill.or.jp/
株式会社ストラテジー	http://www.k-s-g.co.jp/
株式会社ゼロソフト	https://www.zerosoft.co.jp/
株式会社セントラル情報センター	https://www.cic-kk.co.jp/
ソーバル株式会社	https://www.sobal.co.jp/
株式会社Sohwa & Sophia Technologies	http://www.ss-technologies.co.jp/
一般財団法人ソフトウェア情報センター	http://www.softic.or.jp/
第一生命保険株式会社	http://www.dai-ichi-life.co.jp/
一般社団法人体験設計支援コンソーシアム	http://www.cxds.jp/
ダイナコムウェア株式会社	https://www.dynacw.co.jp/
大旺工業株式会社	http://taiyo-kg.co.jp/
株式会社チェンジビジョン	http://www.change-vision.com/
TISソリューションリンク株式会社	https://www.tsolweb.co.jp/
dSPACE Japan株式会社	https://www.dspace.com/ja/jpn/home.cfm
株式会社DTSインサイト	https://www.dts-insight.co.jp/
株式会社D・Ace	http://d-ace.co.jp/
ディジ インターナショナル株式会社	http://www.digi-intl.co.jp/
TDIプロダクトソリューション株式会社	http://www.tdips.co.jp/
株式会社テクノプロ	https://www.technopro.com/
テクマトリックス株式会社	https://www.techmatrix.co.jp/
デジタル・インフォメーション・テクノロジー株式会社	http://www.ditgroup.jp/
デンセイシリウス株式会社	https://www.denseisirius.com/
株式会社電波新聞社	https://www.dempa.co.jp/
東京電機大学 未来科学部	http://web.dendai.ac.jp/
東芝情報システム株式会社	https://www.tjsys.co.jp/
東信システムハウス株式会社	http://www.toshin-sh.co.jp/
東横システム株式会社	http://www.toyoko-sys.co.jp/

株式会社トーセーシステムズ	https://www.toseisystems.co.jp/
特定非営利活動法人TOPPERSプロジェクト	http://www.toppers.jp/
トロンフォーラム	http://www.tron.org/
株式会社永栄	http://www.nagae-jp.com/
株式会社ニッキ	http://www.nikkinet.co.jp/
株式会社日新システムズ 東京支社	https://www.co-nss.co.jp/
日本システム開発株式会社	http://www.nskint.co.jp/
日本生命保険相互会社	https://www.nissay.co.jp/
日本ノーベル株式会社	https://www.jnovel.co.jp/
日本プロセス株式会社 組込システム事業部	https://www.jpd.co.jp/
日本ローターバッハ株式会社	https://www.lauterbach.com/jindex.html
NextDrive株式会社	https://jp.nextdrive.io/
ノアソリューション株式会社	http://www.noahsi.com/
パーソルテクノロジースタッフ株式会社	https://persol-tech-s.co.jp/
ハートランド・データ株式会社	https://hldc.co.jp/
株式会社ハイスポット	http://www.hispot.co.jp/
株式会社パトリオット	http://www.patriot.co.jp/
ハル・エンジニアリング株式会社	http://www.haleng.co.jp/
株式会社ビー・メソッド	http://www.be-method.co.jp/
株式会社ピーアンドピービューロゥ	https://www.pp-web.net/
BTC Japan株式会社	http://www.btc-es.de/
ビジネスキューブ・アンド・パートナーズ株式会社	http://biz3.co.jp/
株式会社日立産業制御ソリューションズ	http://www.hitachi-ics.co.jp/
株式会社ビッツ	https://www.bits.co.jp/
株式会社富士通コンピュータテクノロジーズ	http://jp.fujitsu.com/group/fct/
株式会社ブライセン	https://www.brycen.co.jp/
フラットーク株式会社	http://www.flatoak.co.jp/fltk/
ベクター・ジャパン株式会社	http://www.vector.com/jp/ja/
株式会社ボード・プランニング	http://www.b-planning.com/
マルツエレック株式会社	https://www.marutsu.co.jp/
三井住友信託銀行株式会社	https://www.smtb.jp/
株式会社メタテクノ	https://www.meta.co.jp/
モバイルコンピューティング推進コンソーシアム	http://www.mcpc-jp.org/
ユークエスト株式会社	https://www.uquest.co.jp/
ユタカ電気株式会社	http://www.yutakaelectric.co.jp/
株式会社ユビキタスAIコーポレーション	https://www.ubiquitous-ai.com/
株式会社来夢多゛	http://www.ramuda.co.jp/
リネオソリューションズ株式会社	https://www.lineo.co.jp/
早稲田大学 グローバルソフトウェアエンジニアリング研究所	http://www.washi.cs.waseda.ac.jp/

中部支部

アイシン・ソフトウェア株式会社	https://www.aisin.co.jp/group/aisin-software/
株式会社ヴィッツ	https://www.witz-inc.co.jp/
株式会社ウォンツ	http://www.wantsinc.jp/
有限会社OHK研究所	
株式会社OTSL	http://www.otsl.jp/
株式会社コア 中部カンパニー	http://www.core.co.jp/
三幸電子株式会社	http://www.sanko-net.co.jp/
株式会社サンテック	http://www.suntec.co.jp/
シリコンリナックス株式会社	http://www.si-linux.co.jp/
東海ソフト株式会社	http://www.tokai-soft.co.jp/
東洋電機株式会社	http://www.toyo-elec.co.jp/
ハギワラソリューションズ株式会社	http://www.hagisol.co.jp/
萩原電気ホールディングス株式会社	https://www.hagiwara.co.jp/
株式会社バッファロー	http://buffalo.jp/
株式会社マイクロブレイン	http://www.microbrain.ne.jp/
株式会社明理工業	http://www.meiri.co.jp/
株式会社ユタカ電子	http://www.yutakadenshi.co.jp/

北陸支部

株式会社アフレル	https://afrel.co.jp/

近畿支部

株式会社暁電機製作所	https://arunas.co.jp/
株式会社アクシアソフトデザイン	http://www.axia-sd.co.jp/
株式会社アレクソン	https://www.alexon.co.jp/
アンドールシステムサポート株式会社 大阪事業所	https://www.andor.jp/
イーエルシステム株式会社	http://www.el-systems.co.jp/
株式会社エイビイラボ	http://www.ab-lab.co.jp/
株式会社M's STYLE TECHNOLOGY	http://www.msstyletech.co.jp/
一般財団法人関西情報センター	http://www.kiis.or.jp/
組込みシステム産業振興機構	http://www.kansai-kumikomi.net/
株式会社コア 関西カンパニー	http://www.core.co.jp/
コネクトフリー株式会社	https://connectfree.co.jp/
株式会社Communication Technologies Inc.	https://www.cti.kyoto/
株式会社システムクリエイティブ	http://sc.poi.ne.jp/
株式会社システムプランニング	http://www.sysplnd.co.jp/
スキルシステムズ株式会社	https://skill-systems.co.jp/
株式会社ステップワン	http://www.stepone.co.jp/
株式会社窓飛	http://www.sohi.co.jp/
株式会社ソフトム	http://www.softm.co.jp/
株式会社ソフト流通センター	http://www.k-src.jp/
太洋工業株式会社	http://www.taiyo-xelcom.co.jp/
株式会社たけびし	http://www.takebishi.co.jp/
有限会社中野情報システム	http://nakanoinfosystem.com/
株式会社日新システムズ	https://www.co-nss.co.jp/
日本メカトロン株式会社	http://www.n-mec.com/
ハートランド・データ株式会社 大阪支店	https://hldc.co.jp/
株式会社ハネロン	http://www.haneron.com/
株式会社Bee	http://www.bee-u.com/
株式会社ビッツ 関西事業所	https://www.bits.co.jp/
株式会社星光	http://hoshimitsu.co.jp/
株式会社ルナネクサス	http://www.luna-nexus.com/

九州支部

株式会社エフェクト	http://www.effect-effect.com/
九州IT融合システム協議会（ES九州）	http://www.isit.or.jp/progect/es-kyushu/
株式会社コア 九州カンパニー	http://www.core.co.jp/
ジャパンシステムエンジニアリング株式会社	http://www.jase.co.jp/
セントラル情報センター 九州営業所	https://www.cic-kk.co.jp/
柳井電機工業株式会社	http://www.yanaidenki.co.jp/

・学術会員 3団体
・個人会員 8名

JASA新入会員企業紹介

合同会社Keychain

〒107-0062 東京都港区南青山1-2-6 Lattice 青山 Square 2F
https://www.keychain.io/ja/

Keychainは、エンタープライズがブロックチェーン技術を迅速・安価に既存システムやアプリケーションに組込み実装するためのKeychain Coreソフトウェアおよび開発環境（SDK）をライセンス提供する会社です。同SDKを利用することで、組込み開発会社様が独自にIoTデバイスやモバイル、クラウドなどにGatewayを組込み、多数のIoTが認証・セキュア通信を行えるようになります。

株式会社 技研工房

〒060-0051 北海道札幌市中央区南1条東3丁目10-1 北海道日伊文化会館 新館6階
https://www.giken-k.biz/

技研工房はハードウェアの設計から筐体デザイン、クラウド アプリケーションに至る全行程をプロデュース。

回路設計、基板設計、製造、実装、ファームウェア開発のハードウェア サービスからデータベース、Webアプリケーションを含めたクラウド サービスをワンストップで対応します。

株式会社ゼロソフト

〒214-0014 神奈川県川崎市多摩区登戸3398-1 大樹生命ビル７F
https://www.zerosoft.co.jp/

(株)ゼロソフトは 1974年6月に下記経営理念の下 コンピュータの品質を検証する会社として設立しました

一、原点（ゼロ）のソフトウェアを開発し社会に貢献する
一、ハードウェアとソフトウェアの接点のソフトウェアを開発しメーカーとユーザーに対してシステム・コンサルタントの役割を担う
一、蓄積された高度な技術力を社会に還元する

対象は汎用 PC からスパコンの検証、コアＩＰの開発、コア・アーキのソフトシミュレータ開発、検証技術や品質システムを活かした機能安全系の開発などをご依頼頂いております
尚、協会の皆様と新しい何かを発見・ご提案する様な活動に参加出来ましたら幸いに存じます

大旺工業株式会社

〒373-0847 群馬県太田市西新町6番3号
http://taiyo-kg.co.jp/

1984年設立。板金業を主軸とし、筐体開発・試作～量産までを「顧客第一主義」を掲げ、お客様の立場に立った製品を提供いたします。

社会のニーズがより多様化・高品質化していく中で、高度情報化に対応する「モノづくり」の質的向上を、新技術に挑戦「スマートファクトリー化」することで達成します。

明日を見続け、挑戦する努力を惜しまず、自社の可能性を伸張し「創造」を実現していくことで「成長し続ける企業」を目指します。

北都システム株式会社

〒004-0052 札幌市厚別区厚別中央2条3丁目5番11号
https://www.hscnet.co.jp/

弊社は1994年に創業し、通信端末の組込みシステム開発からスタートしました。
以来、常にお客様のニーズや時流の変化に対応しながら業容を拡大し、現在では自動車関連ソリューション、医療系ソリューションをはじめとして、そのほか様々な業種業態のお客様に向けたプロダクトやSIサービスなど、ソフトウェア開発を軸に事業を展開しております。

柳井電機工業株式会社

〒870-0017 大分県大分市弁天二丁目７番１号
http://www.yanaidenki.co.jp/

1947年創業翌年に日立製作所の機電計特約店として業務を開始以来長きにわたり、計画から設計施工及びメンテナンスを提供してまいりました。

2017年より研究開発部門を新たに設立し、システム開発、ソフトウェア開発にも取り組んでおります。

ドローンを利用した太陽光発電の検査システムの開発や、地元に根差した企業（お酒造り）へのIoT提供を地元の大学との共同研究により提供していくなど取り組みなどを行っております。

■編集後記

今号は、IoT機器の利用拡大に伴い重要性を増している、組込み開発におけるセキュリティ設計をテーマに特集を組みました。まさに旬の話題です。執筆は、2019年に新設された組込みシステムセキュリティ委員会にお願いしました。グローバルでの動向をはじめ、セキュリティ設計の勘所、IoTシステムの運用、開発プロセスをサポートするツール類の紹介など、とても濃い内容になっています。ぜひ、ご一読ください。

4月1日にホームページ（https://www.jasa.or.jp/）をリニューアルしました。協会の3本柱である「ビジネスマッチング」「技術高度化」「人材育成」などの活動について積極的に情報発信します。皆さまからの情報もお待ちしています。組込みシステム業界の情報ハブとしてご活用ください。

広報委員長　横田 英史

機関誌　Bulletin JASA Vol.73

令和２年 ４月 13 日
東京都中央区日本橋大伝馬町 6-7
Tel.03-5643-0211　Fax.03-5643-0212
URL　https://www.jasa.or.jp

一般社団法人組込みシステム技術協会
発行人　会　長　竹内 嘉一
編集人　広報委員長　横田 英史

JASAは、組込みシステム技術の普及・高度化、調査研究など業界活動を積極的に展開しています。

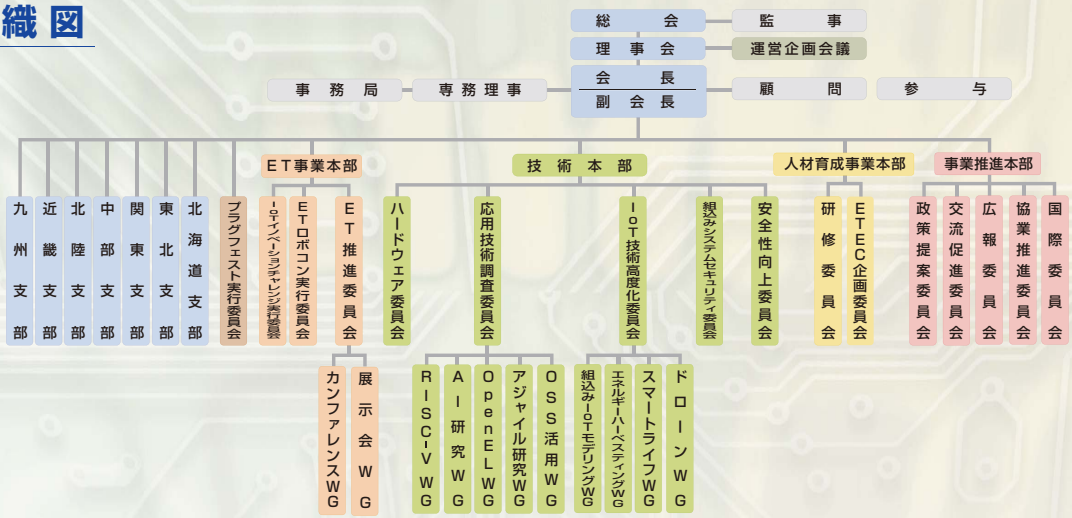
協会概要

名　称　一般社団法人組込みシステム技術協会
Japan Embedded Systems Technology Association（JASA）
会　長　竹内　嘉一
事務所　本部　東京都中央区日本橋大伝馬町 6-7
　　支部　北海道、東北、関東、中部、北陸、近畿、九州
会員数　正会員 144 社　賛助会員 30 社　支部会員 13 社
　　学術会員 3 団体　個人会員 8 名　（2020 年 4 月現在）
設　立　昭和 61 年 8 月 7 日
　　平成 24 年 4 月 1 日 一般社団法人へ移行
組　織　事業推進本部、技術本部、人材育成事業本部、ET 事業本部
産業分類　日本標準産業分類　G-3912　組込みソフトウェア業

目　的

組込みシステム（組込みソフトウエアを含めた組込みシステム技術をいう。以下同じ。）における応用技術に関する調査研究、標準化の推進、普及及び啓発等を行うことにより、組込みシステム技術の高度化及び効率化を図り、もって我が国の産業の健全な発展と国民生活の向上に寄与することを目的とする。

組織図



主な事業活動

1. Embedded Technology（ET展）及び IoT Technology（IoT技術展）の全国展開

Connected Industries実現の先導的役割を担う『エッジテクノロジー総合展』として、関東（横浜）、関西（大阪）、中部（名古屋）等で開催する。

2. ETEC/組込みソフトウェア技術者試験制度の実施、普及拡大

組込み技術者の育成、スキル向上を目的とした組込みソフトウェア技術者向け試験制度「ETEC」の実施、クラス2試験とともに上位のクラス1試験運用

3. 技術高度化のための調査研究活動

①機能安全・情報セキュリティ・生活支援ロボットの安全性に関する技術動向調査及び、組込みセキュリティ対策検討
②OSS普及活動（ロボット用OSS：OpenEL、OpenRTM等）、ライセンスの啓発活動
③IoT・M2Mをエッジ側の観点で、構成／サービス／拡張性／検証性／保守性等を調査研究する。
④センサー活用におけるセンサー基盤開発・評価。XDに着目した組込み技術の共創開発の考察及び人材育成

4. 人材育成・教育事業

①就活・求人支援
②新人研修講座、技術者教育・スキルアップセミナーの実施
③企業が求める新卒人材調査（スキルレベル）の実施と情報提供

5. ETソフトウェアデザインロボットコンテスト（ETロボコン）、IoTイノベーションチャレンジの実施

組込みソフトウェア分野の技術者教育を目的としたソフトウェア開発技術を争うコンテスト。初級者対象のデベロッパー部門2クラス、新しい技術にチャレンジするガレッジニア部門1クラスの2部門3クラス制により、全国地区にて技術教育と競技会を実施。11月開催「ET／組込み総合技術展」にて、各地区優秀チームによるチャンピオンシップ大会を開催。

また、これからの産業界を牽引できる「IoTビジネス人材」の発掘・育成を目的として、教育にフォーカスし、技術を使って学ぶことに主眼を置いたコンテスト「IoTイノベーションチャレンジ」を実施する。

6. 協業支援・ビジネス交流会の運営

①会員内外の協業力を高めるためのマッチングイベント及び交流イベントの実施・運営
②国内外企業との連携支援

7. 国際化の推進、海外機関との連携強化

①国際化・グローバル化に向けた調査研究及び海外視察・会議等への派遣参加
②海外情報を発信する「グローバルフォーラム」等イベントの企画・運営及び機関誌上での「国際だより」による情報発信
③海外機関・団体との連携強化と共同イベント等の企画・運営
④海外人材活用支援

8. 政策提案及び関連機関との連携

関連省庁及び団体等との情報共有と連携を推進し、独立した立場より政策提案するとともに、関連施策等の情報を会員に展開する。

9. 日本プラグフェストの開催

インターフェース規格を持つメーカ同士が相互運用性を検証する技術イベント
年2回（春・秋）開催　HDMI、MHL等

10. 広報活動

①技術・業界動向、協会活動等を掲載した機関誌「Bulletin JASA」の定期発行と活用
②ホームページ活用による委員会活動・研究成果、会員情報、イベント情報等の提供及びメールニュース配信等による情報提供・広報
③キャラクター「クミコ・ミライ」を活用した業界認知度向上と協会活動の周知・PR

一般社団法人
組込みシステム技術協会
Japan Embedded Systems Technology Association

[本部事務局]
〒103 - 0011 東京都中央区日本橋大伝馬町 6-7 住長第 2 ビル
TEL: 03-5643-0211　Email: jasainfo@jasa.or.jp　https://www.jasa.or.jp

アジア最大級の
エッジテクノロジー総合展

出展社募集中! 申込期限 **2020年6月30日(火)**

Embedded Technology 2020

IoT Technology 2020

2020年11月18日(水)▸20日(金)

10:00〜17:00 ※19日(木)は18:00まで

▸会場 パシフィコ横浜

https://www.jasa.or.jp/expo/ ET IoT 検索

2020年4月1日より、本展の企画・推進および事務局が変更になりました。

お申込み・お問合せ

ET・IoT展示会事務局（株）ナノオプト・メディア内
Tel. 03-6258-0589　et-info@f2ff.jp

一般社団法人
組込みシステム技術協会
Japan Embedded Systems Technology Association

[本部事務局]
〒103-0011 東京都中央区日本橋大伝馬町 6-7 住長第 2 ビル
TEL: 03-5643-0211 Email: jasainfo@jasa.or.jp https://www.jasa.or.jp/