技術本部

組込みシステムセキュリティ委員会紹介

組込み開発のセキュリティ対策の体系化と教育を推進
― 国際認証支援プログラムや人材育成カリキュラムを展開 ―

組込みシステムセキュリティ副委員長　牧野進二

組込みシステムセキュリティ委員会は、2019年にサイバーセキュリティについての各省庁やIPAなどからのガイドラインなどを組込み開発で利用できるようにセキュリティの知識体系化と教育を推進するために発足した。

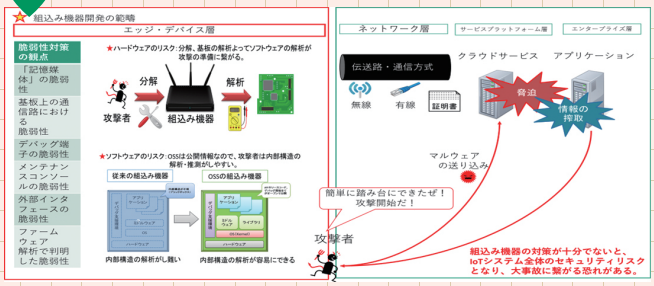
組込み開発のセキュリティ対策は喫緊の課題

組込み開発で利用するセキュリティスキルを体系化する組込みデバイスセキュリティWG、各省庁やIPAなど他団体との情報を取り扱う外部連携WG、広く一般に組込み開発でのセキュリティ対策を啓発する啓発活動WGの活動を通じて、組込み開発でセキュリティの知識体系と教育を広く展開する活動を行っている。

組込み開発におけるセキュリティ対策の必要性は言うまでもない。エンドポイントである組込み機器からデータを収集し、そのデータを分析することで社会問題の解決をめざすSociety5.0においてはIoT機器の重要性は増している。そのセキュリティ対策は喫緊の課題である。

しかしサイバー空間の攻撃者が、エンドポイントとなる組込み機器を悪用し、踏み台にするようになっているのも事実である。踏み台にならないためには、IoT機器のセキュリティ対策が不可欠である。

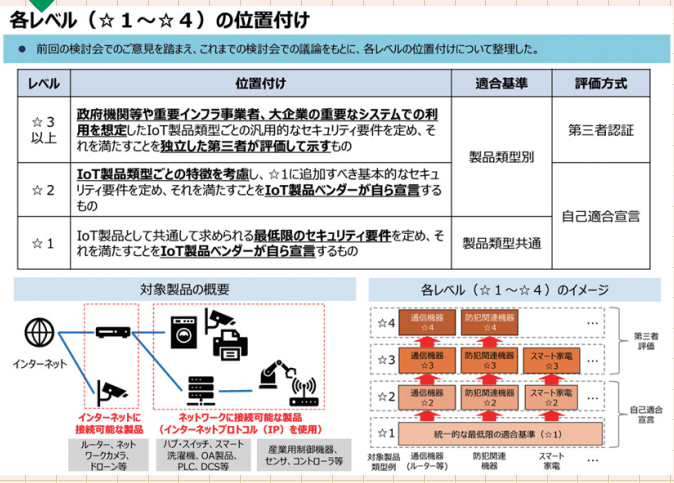
IoT機器のセキュリティ対策イメージ



ISO/IEC 27400シリーズ(概要)

No	規格名	概要	対象者	備考
1	ISO/IEC 27400	IoTソリューションのセキュリティとプライバシーに関するリスク、原則、コントロール(対策)に関するガイドライン	IoTサービスプロバイダ、IoTサービス開発者、IoTユーザ	2017年:総務省・経産省のIoTセキュリティガイドラインv1.0を提案しプライバシー要件が追加され標準化
2	ISO/IEC 27402	IoT機器のセキュリティとプライバシーに関するIoT機器の要求ベースライン要件	IoT機器、製造者	2019年 米国発案 NISTIR 8259がベース。IoTセキュリティ要件を定義後にNISTIR 8425になっている
3	ISO/IEC 27404	消費者向けIoT機器のサイバーセキュリティラベリングフレームワーク	消費者、開発者、サイバーセキュリティラベルの発行団体、試験機関	シンガポール発案。欧米ともラベリング に向けた検討を実施

IoTセキュリティ適合性評価制度



国際認定支援プログラム(概要)

Secure IoT Platform Consortium

IoT機器適合性評価事業「セキュアIoTプログラム」における共同運営

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

IEC62443をはじめとする国際標準やSP800シリーズなどのセキュリティ規格が定められ、調達基準としても採用され始めているが、取得のためには莫大の費用と長期の検証期間がかかるため適合できるのが一部の大手企業に限定されるのが現状である。

「IoTセキュリティ手引書」をベースに「脆弱性検査およびIoTセキュリティ検査」とIoTシステムに求められるセキュリティ要件を以下の点に絞り込み、国際標準(IEC62443)への適合性を確認する「セキュアIoT認定」を組合わせたプログラムを発表。

【検証ポイント】
■ライフサイクル管理
・真正性の担保(鍵管理、ROT: Root Of Trust)
認証と識別 (設計・製造、利用、廃棄、リサイクル)
・セキュアアップデート (OTA: Over The Air)

セキュアIoT認定

コモングラウンド委員会紹介

Society5.0実現のためのデジタルツイン技術を調査・研究
インフラ協調型のJASA版デモ環境を構築中

コモングラウンド委員長　國井 雄介

2015年から活動していた「IoT技術高度化委員会」の研究成果を基に、2023年4月に新たにコモングラウンド委員会を立ち上げた。「コモングラウンド」とは、東京大学の豊田啓介 特任教授が提唱する、現実空間（フィジカル）と情報空間（デジタル）を融合させた次世代の社会基盤であり、人とNHA（Non-Human-Agent：ロボットやアバター等）が共存できる世界を目指す汎用的な空間記述プラットフォームである。委員会は、Society5.0の実現にはコモングラウンドのアプローチが有用であると考え、インフラ協調型のデジタルツインにおけるエッジ側の役割（組込みシステム）の要件定義や技術的課題について議論している。

これまでの活動実績

デジタルツイン技術に関する知見を深めるために、有識者を招いた勉強会や企業のサービス事例を基にした「白熱教室」を実施してきた。委員会参加企業やメンバーは、産学官の専門家から最新の技術動向や実用化に向けた課題を学び、デジタルツイン技術の理解を深めている。また、2023年の委員会立ち上げ時には、新しく立ち上げた委員会の周知と関心のあるメンバーを集めるために、SWEST25や九州ものづくりフェアの展示会などに積極的に参加し、広くメンバーを募集した。

ハイブリッド形式での委員会開催により、全国各地から多様なメンバーや連携団体が参加し、地域に縛られない活動を実施することができた。この結果、多くのメンバーが技術的な交流を深め、知識の共有が進んでいる。そして、得られた知見やメンバー同士で議論した結果などをまとめ、EdgeTech+2023でのセミナーの実施や雑誌Interfaceへの記事掲載を行うことができた。

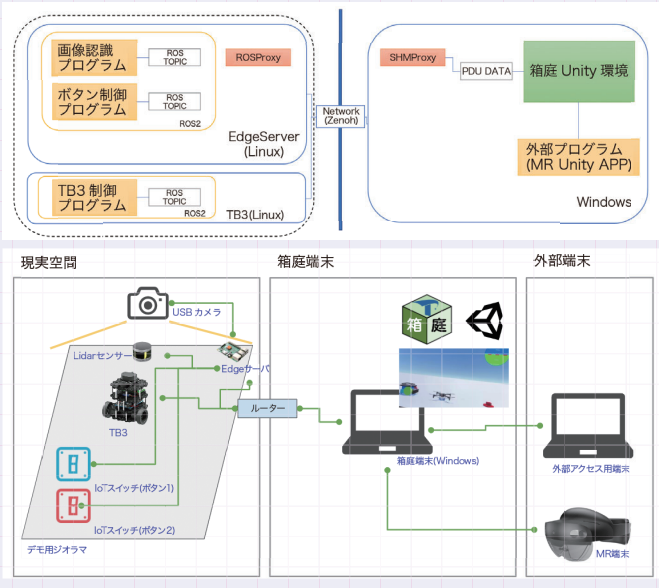
コモングラウンド構想の特徴

- **コモングラウンドは、汎用的な3次元空間記述の体系**
→それを具象化して社会実装しようとしているのが、コモングラウンドリビングラボ。
→コモングラウンドリビングラボでは、UnrealEngineを活用している。
- **データ共有のPF（サービサーに対し、APIとして提供）**
→データは、点群データやBIM、CADのデータの他、センサデータ、人やロボットの位置情報など様々。
- **インフラセンサの活用**
ロボットや人の位置を把握し、物理環境をデジタル環境に再現。
- **動的な空間、時間のスケーリング。**
→精度が必要なところは細かく、不要なところは粗く。
点群データなどは、量が多すぎてリアルタイム処理に向かない。
→Voxelなどの解決策はあるが、コモングラウンドは異なる。
- **神の目、虫の目の視点でのロボット間の協調動作。**
→ロボット単体では、協調動作はできない。
そもそもロボット同士が、連携し動くためには共通の認識（バックグラウンド）が重要。
ロボットの認識精度が異なると連携しづらい。
- **横断的なデータを活用した、最適化。道案内など。**
→System of Systems。デジタルライフライン。
- **双方向の通信。**
リアルからバーチャルにバーチャルからリアルに働きかけできる。
→メタバースでは、物理空間→バーチャル空間は、見えるが、バーチャル空間から物理空間は見えない。

今後のコモングラウンド委員会の活動

今後は、引き続き有識者を招いた勉強会や仲間集めを実施するとともに、インフラ協調型のJASAデモ環境の作成に注力する。このデモでは、プラットフォームとしてTOPPERSプロジェクトのOSSである「箱庭」を活用し、ユースケースとして工場の自律運用を目指したデジタルツイン環境を構築する。具体的にはインフラ側のセンサが取得するデータをリアルタイムでバーチャル空間に反映させ、ロボットの制御や移動経路の最適化をバーチャル空間側で行いリアル側に反映させるシステムである。

このデモは、インフラ協調型ロボット制御を実現するためのエッジ側（センサ、アクチュエータ、ロボット等）の要件定義や課題調査に活用する予定である。デモを実際に作成することで得られた知見を活かし、バーチャル空間からロボットを制御するシステムや、リアルとバーチャルのデータ同期、ロボット同士の協調動作におけるエッジ側の役割などを検討し、課題解決に向けた成果を外部に発信していく。これらの取り組みを通じ、人とロボット、ロボット同士が協調して動作するSociety5.0の実現を目指し、活動を続けていく。



技術本部

応用技術調査委員会AI研究WG紹介

組込みでも活用できるAI研究を継続

AI研究WG主査　中村仁昭

AI研究WGは研究会とセミナーの2本立てで開催していることが特徴に挙げられる。当初セミナーのみで立ち上げ、初学者向けの座学とテーマを各々定めて課題に取り組んでいた。ただしこれは約半年間の取り組みであり、もっと長期的に課題を追い続ける場が欲しくて研究会を追加で設けた。結果として、現在でも研究会は統一したテーマはなく、参加メンバー内でグループを作り個々のテーマを深掘りしている状況である。

また研究会では知見を深めるため、国内の機械学習コンペへの参加を奨励している。実際に賞金を獲得したメンバーも存在する。

今までの研究テーマ
低リソースデバイスでどのようにAIを動作させるかを検証

これまで研究会で扱ったテーマで興味深いものを挙げてみる。

まず組込み業界であることから低リソースデバイスでどのようにAIを動作させるかをテーマに選択することが多い。ESP32などで画像認識を行なったり、重みを二値化しモデルサイズを1/10にするBinarized Neural Network（BNN）に関する検証を行なったり、時系列処理に適したリカレントニューラルネットワークの特殊なモデルを一般化したリザバーコンピューティングに関する検討を行なった。他にもラズパイなどのエッジ端末上で推論だけでなく学習を行うことに挑戦しているメンバーも存在する。

また、もともと知見のある強化学習を継続的に研究しているグループがあったり、業務に近い異常検出をテーマに選んで知見を深めようとするグループがあったりと多彩である。つい最近まで行なっていた競馬AI予測に関する研究も研究本部の成果発表会などで人気があった。

今後の研究テーマ
エッジ端末におけるローカル生成AIの可能性について調査

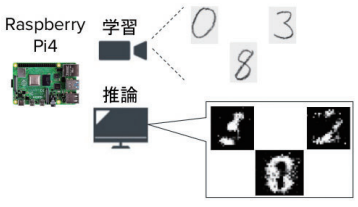
上であげたテーマを継続して研究するグループも多いが、近年生成AIがブームになっていてエッジ端末でローカル生成AIの可能性について調査を行なっている。具体的にRaspberry Pi 4、5、Jetson Xavier NXなどでMetaのLLM、Lllama2を動作させて実用的な速度で動作するかを確認し、組込み端末における将来的な活用方法について考察した。

考察においてマルチモーダルLLMの親和性が高いとの結論を得たが、実際に動作させると通常のLLMに比較して計算量が膨大で現行の機器では実用的でなかった事から、継続検討として一般的なLLMでプロンプトを工夫してZero-shot文章分類器としての活用方法を模索している。

オンデバイス学習

目標・問題設定

- エッジデバイスとUSBカメラを使用して、カメラから得られた実画像データの学習と推論をエッジ上でリアルタイムで行うことを目指す
- タスク
  - 画像生成
- 対象
  - 手書き数字（0と1）
- エッジデバイス
  - Raspberry Pi4（4GB）
- USBカメラ
  - Logicool C270n



競馬予測AI

内容紹介

それぞれの前処理における学習結果は、以下の通り
今回のデータでは、何もしない場合と重み付けを行った場合では、結果に変化はなかった
また、アンダーサンプリングとオーバーサンプリングの場合では、再現率の向上は見られたが、誤判定も多く見られるようになった

	なし	重み付け	アンダーサンプリング	オーバーサンプリング
正答率 (勝ち負け両方の正解率	92%	92%	65%	82%
再現率 (勝った馬の正答率	0%	0%	69%	34%
参加レース全272)	0	0	270	205
勝ったと予想した馬の頭数	0	0	1350	550
収支	0	0	-18200	-12910

組込環境で生成AI_

動作環境

環境	Tokes/sec(tps)
Raspberry Pi 4	0.96
Raspberry Pi 5 without FP16	2.33
Raspberry Pi 5 with FP16	2.97
Jetson Xavier NX	10.97
GeForce RTX 4070Ti(12GB)	12.01

低リソースデバイスでAI

実験　まずは、1桁のフラッシュ暗算を試してみた

プラットフォーム構築委員会 OpenEL活用WG紹介

IoTや制御システム向け統一インタフェースを策定、仕様書、サンプルソースコードをGitHubで公開

OpenEL活用WG主査　中村憲一

OpenEL活用WGは、OpenEL（Open Embedded Library）仕様の策定、サンプルプログラムの実装、国内外における普及、国際標準への提案を目的として毎月活動している。

OpenELとは、制御システムやIoTデバイスなどのソフトウェアの実装仕様（API）を標準化する組込みシステム向けオープンプラットフォームである。デバイスの制御に特化し厳選された19個のAPIを使用することで、モータの制御方法を知らない初心者でも簡単にモータやセンサなどを制御することができるのが特徴である。

少ないAPIで各種のモータやセンサを制御するために、Surface層とDevice層の複数層によるハードウェアの抽象化を実現している。この抽象化により、製品開発時にデバイスが生産中止になったり、次の製品でデバイスを変更してもアプリケーションプログラムを変更する必要がなくなり、開発コストを節約することが可能となる。

OSレスからRTOS、Linux、Windowsのシステムに対応

OpenELの歴史は古く、2011年5月から開発に着手し、2012年5月に当時ETロボコンに採用されていたLEGO Mindstorms NXT（図1）向けのVer.0.1を公開した。その後、経済産業省の事業にも採択され、仕様の強化とともにバージョンアップを重ねた結果、2024年8月現在はVer.3.2（図2、3、4）が最新であり、モータ（位置、速度、トルクの制御と取得）とセンサ（ジャイロ、トルク、加速度、地磁気、距離、力、温度、湿度、気圧、二酸化炭素、色、接触、電流）に対応している。

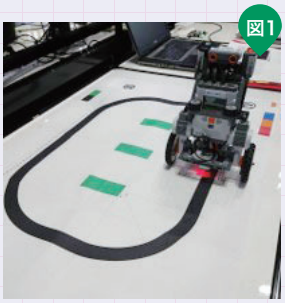


図1

またOSレスの組込みシステムからリアルタイムOS、Linux、Windowsにも対応し、OSの有無や違いを意識することなくモータやセンサを同じAPIで制御できるようになった。開発言語も組込みシステムで使用されるC/C++の他にC#にも対応したため、組込みシステム技術者からエンタープライズシステム技術者まで使用可能な環境が整っている。OpenELはプラットフォームに依存しないモデルで定義されているため、他の言語への展開も可能である。

上流から下流まで一気通貫の開発手法の構築を目指す

今後は、品質と効率を上げる組込み用のモデルベース開発を実現するべく、上流から下流まで一気通貫した開発手法の構築を目指している。具体的には、対応デバイスの追加、デバイスドライバのソースコードの自動生成、テストパターンの自動生成、シミュレーターを使用したテストの検討、国際標準への提案等を進める予定である。

OpenELの仕様書やサンプルプログラムはGitHubで公開している。是非ダウンロードして試していただき、少しでも興味をもった方はWGに参加していただきたい。

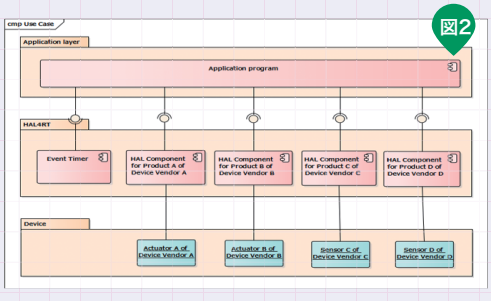


図2

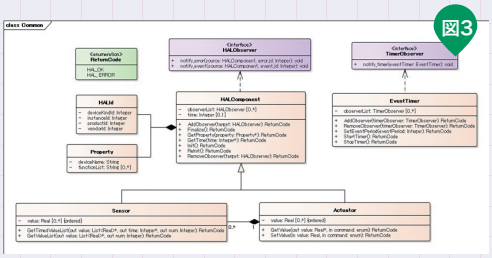


図3

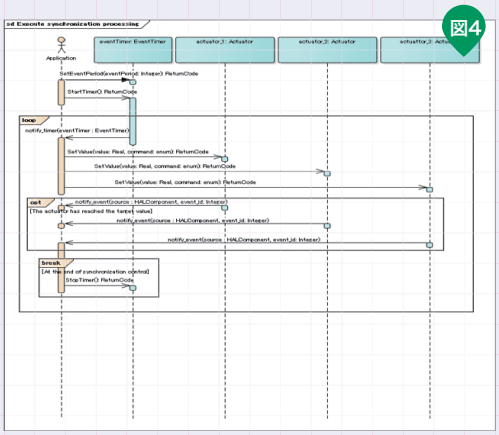


図4

今すぐアクセスを！（GitHub）

OpenEL 3.2 仕様書（PDF）