

# 「つながる世界の開発指針」に関する 実証実験

SEC研究員 丸山 秀史

SEC研究員 小崎 光義

SEC研究員 宮原 真次

## 1 はじめに

IPA/SECでは、IoT時代を踏まえ、安全・安心な製品を開発するための「つながる世界の開発指針」を策定した。開発指針では、つながることによる事故やインシデントを未然に防ぐことを主眼に、指針ごとにポイント、解説、対策例について記載している。開発指針策定において、対策例の中には、既に確立して広く普及している技術と、まだ確立しておらずあまり普及していない技術があることが見えてきた。そのような未確立の技術の一部について、その実現性や有効性に関して実験システムを構築し、検証・評価を行った。

## 2 実証実験の方針

開発指針は分野共通のものであり分野間連携まで適用可能であるが、2015年度では、まずは単一の分野でその実証をする方針とした。また、対策については、なるべく特定の分野や特定の機器には依存せず、様々な分野の機器やソフトウェア製品の開発に参考となるような内容とすることを方針とした。

## 3 実証実験の体制

IoTにおける代表的な活動としてIndustrie 4.0がある。それと親和性の高いFA分野を実証実験の対象とした。実証実験環境には機器を連携させる基盤(ソフトウェア)が必要であり、FA分野における国内の整備状況を調査した結果、一般社団法人日本ロボット工業会ORiN<sup>※1</sup>協議会が開発した基盤製品ORiNがあることが分かった。また、機器や設置する場所について、一般財団法人機械振興協会が保有していることが分かった。体制としては、ORiN協議会、機械振興協会にご協力いただき、IPA/SECを含め3者で実証実験を行うことにした<sup>※2</sup>。

## 4 実験環境

実証実験環境としては、工場内のセル生産環境を想定して整備した。図1に示す通り、SCADA<sup>※3</sup> PC、セルコントロールPC、産業用ロボット(単軸)、産業用ロボット(6軸)、NC装置で構成した。

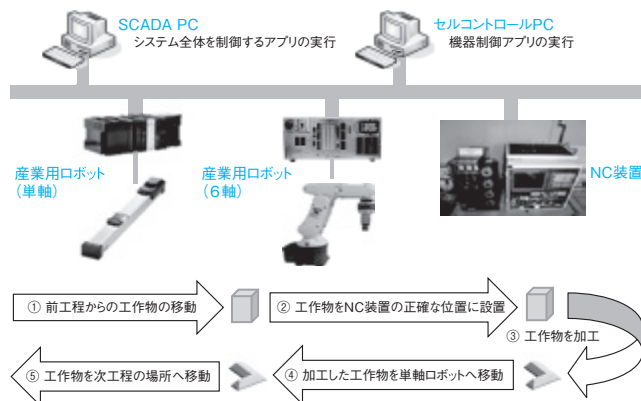


図1 セル生産環境を想定した実証実験環境

## 5 実証実験のテーマ選定

実証実験のテーマは、開発指針の【指針9 つながる相手に迷惑をかけない設計をする】及び【指針11 不特定の相手とつなげられても安全安心を確保できる設計をする】の2つを選定した。

### (1) 障害の波及防止策(製造ライン稼働時の異常検出と対策)【指針9に対応】

工場の生産環境において、ロボットなどに障害が発生すると生産全体に影響を与える。ロボットに渡す制御データの内容や処理が複雑化しており、プログラムミスや運用ミスによる異常発生リスクがある。更に、これらの機器がネットワークにつながるようになるとウイルス感染などにより異常動作を起こすリスクが増加する。障害の波及防止策として、工場内の装置から動作ログなどを収集し、異常を検知した場合に速やかに装置を安全に停止する仕組みについて検証することとした。

### (2) 相互接続時の信用確認(要求品質が異なる装置を接続するときの対策)【指針11に対応】

ORiNなどの基盤製品が普及すると、連携可能な機器が増加する。それにより、実績がなく低品質の機器が接続される可能性が増加すると見込まれるが、そのような機器を接続すると精度の低い動作となったり、ウイルス感染のリスクなどが高まる。工場内に新規に装置を組み込む場合、その装置が信頼できる装置であることを確認するために、「品質情報」をやり取りする仕組みを検証することとした。

## 6 対策技術

### (1) 障害の波及防止策

本セル生産環境ではセルコントロールPCからロボットに動作指示が行われる。ロボットに障害が発生するとセル生産全体に影響を与えるため、ロボットの障害につながる動作指示パラメーター値の異常をいち早く検知し、障害発生前の対応を可能にする方法を検討した。そのための対策としては、ロボットが一定周期で繰り返し動作することに着目し、以下の3つの機能を導入した。

- ① 前準備で各機器の動作指示パラメーター値を採取して正常値として記録する機能。
- ② 動作指示パラメーター値を適切な時間幅で監視し、①で採取したデータと比較する機能。
- ③ 記録した正常値に含まれない場合は異常と判断してロボットを停止する機能。

### (2) 相互接続時の信用確認

相互接続時の問題に対して、以下の機能を組み込んだ。

- ① ロボットの信頼性を示す「品質情報」をアプリケーションから参照可能なロボットの固有情報の中に埋め込む機能。
- ② セルコントロールPC上のアプリケーションからコネクション確立前にその「品質情報」を確認し、接続可否を判定する機能。
- ③ 接続してよい信頼性であることが確認できた場合にコネクションを確立する機能。

## 7 対策技術の評価

### (1) 障害波及防止策の評価

図2は対策未実施の場合であり、図3は対策実施後の場合である。対策の実施により、ロボットの異常が工作物や他の機器に影響を与える前に検知できることを確認した。すなわち、ロボットの移動速度に対して十分に速い速度で異常を検知でき、結果としてロボットの障害による影響の波及抑止につながることを確認できた。また、ロボットとセルコントロールPCに対して制御に影響を与えない程度の負荷で異常を検知可能であることも確認できた。

### (2) 相互接続時の信用確認の評価

今回の実証実験では、ロボットとのコネクション確立前に「品質情報」を確認することで、要求品質の低い機器の接続を防止することが可能であることが確認できた。なお、今回の実証実験での「品質情報」は、実験用の品質識別子を使ったが、実際のシステムにこの対策を適用するに当たっては、「品質情報」の具体化と「品質情報」自体の信頼性を保証するための仕組みが必要である。

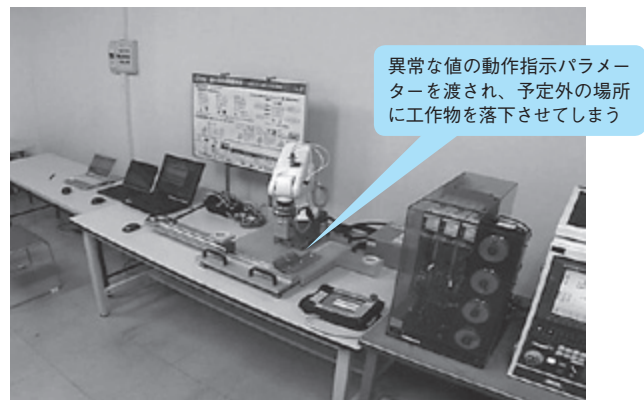


図2 波及防止策未実施の場合



図3 波及防止策を実施している場合

## 8 おわりに

今回は、工場内の製造機器が外部とつながったときに起こり得る異常動作のリスクや新規に機器を増設する場合の導入リスクを想定して実証実験を行った。今回、実証した異常検出及び波及防止手法や「品質情報」による信頼性確認手法は、他のIoTシステムでも参考となる対策技術であると考えている。本実験で得られた結果は、開発指針にも反映している。更に、ORiN協議会におけるORiNの次期バージョン仕様への提案や、FA以外の分野の基盤となるソフトウェアへの実装も提案していく予定である。IPAは、これらの取り組みを通じて、今後、IoT機器の安全・安心を確保する対策技術の普及に貢献していく。

本実証実験の報告書は以下のWebサイトで公開しており、詳細についてはそちらを参照していただきたい。

[http://www.ipa.go.jp/sec/reports/20160511\\_3.html](http://www.ipa.go.jp/sec/reports/20160511_3.html)

### 【脚注】

- ※1 Open Resource interface for the Network
- ※2 <http://www.ipa.go.jp/about/press/20151202.html>
- ※3 Supervisory Control And Data Acquisition : 産業用制御システムの一つ