IoTの高信頼化に向けた分野間連携実証実験
報告書

2017 年 5 月 31 日

独立行政法人情報処理推進機構
Information-technology Promotion Agency, Japan

ORiN協議会

一般社団法人　エコーネットコンソーシアム

学校法人　幾徳学園　神奈川工科大学

目次

0. はじめに

IPA/SEC では、2015 年度の活動として、IoT 時代の安全・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、その中の「[指針 9]つながる相手に迷惑をかけない設計をする」における異常の早期検知の対策、並びに「[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」における接続機器の信頼性確認の対策の有効性を実証実験で確認した[1]。2016 年度は上記の「つながる世界の開発指針」の内容を具体化した「『つながる世界の開発指針』の実践に向けた手引き[IoT 高信頼化機能編]」(以降「実践に向けた手引き」)を策定し、そこでは、IoT の重要な特徴の 1 つである分野間連携におけるリスク分析の例を提示した。今回の実証実験では、その内容を踏まえ、分野間連携システムを対象としたリスクへの対策例を示し、それらの実現性を確認した。

1. 背景

多くの製造工場では、製造活動の省力化を目的として産業ロボット・機器から構成される製造ラインを導入している。工場を稼働するにあたっては、この製造ラインの制御と電力制御が必要であり、またそれらの保守が必要である。したがって、特に中小企業で省力化を進めていくためには、製造ラインを導入するだけでなく、電力系統も含めたそれらの制御と保守を少ない人数で効率的に行うことが求められ、IT の導入によりその要件に対応する企業が増加していると考えられる。

一方、信頼できる研究機関の調査によれば、制御系に関わる脆弱性情報の報告件数が、エネルギー分野、製造分野で 1 位、2 位を占めている、という結果[2]が報告されており、工場のエネルギー管理、製造ラインにおいても、セキュリティ対策の必要性が増していると考えられる。

本実証実験では、これらの状況を考慮して、以下のようなスマート工場を実現する工場管理のシステムを想定した。(図 1)

- 製造ラインの制御とエネルギー管理を一元的に操作できるようになっている。
- 異常時の対応工数を抑えるために、異常監視と異常通知の機能をもつ。

特に、産業ロボットシステムでは、機器やシステムの故障や第三者からの攻撃により異常が発生し、稼働率が低下すると、その影響が損益に直結するため、異常監視の強化が重要となる。

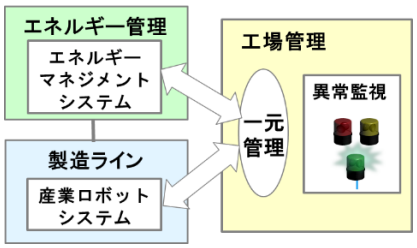

図 1 工場の IT 導入による省力化

1 http://www.ipa.go.jp/sec/reports/20160511_3.html

2 NCCIC/ICS-CERT,FY2015 Annual Vulnerability Coordination Report より
NCCIC(National Cybersecurity and Communications Integration Center) : アメリカサイバーセキュリティ通信統合センター

2. 目的

前述のようなスマート工場システムを構築し、そこで必要となる高信頼化対策を確認する。

異常監視の強化に関して、「実践に向けた手引き」では、次のような要件を提示している。

- 【要件 2　稼働中の異常発生を未然に防止する】
- 【要件 3　稼働中の異常発生を早期に検知できる】

本実証実験は、要件 2、3 を具現化する方式の一例に関して、その実現性を確認することを目的とする。

3. 体制と役割

今回の産業ロボットシステムとエネルギーマネジメントシステムを使った実証実験は、一般社団法人　日本ロボット工業会の ORiN[3]協議会、一般社団法人　エコーネットコンソーシアム、学校法人幾徳学園　神奈川工科大学との産学官連携で実施した。

実証実験の体制と役割を以下に示す。

表 1　体制と役割

団体名	役割
IPA	実証実験の仕様決定、実証実験用プログラムの開発、実証実験の実施、評価と報告書作成
ORiN 協議会	産業ロボットのシミュレーションソフトの提供、実験内容の検討
エコーネットコンソーシアム	エネルギーマネジメントシステム仕様（ECHONET Lite 規格[4]）の技術提供、実験内容の検討
神奈川工科大学	エネルギーマネジメント用 IoT 機器接続ソフト（SDK）の提供と開発技術提供、実験内容の検討

3 http://www.orin.jp/
ORiN（Open Resource interface for the Network）とは、工場内の各種機器に対して、メーカ、機種の違いを超えて統一的なアクセス手段と表現方法を提供する通信インタフェースであり、産業用機器をアプリケーションプログラムから制御するための標準インタフェースの 1 つ。
ORiN 自体はアプリケーションと各機器との間のインタフェースを規定するものであるが、これを実装したミドルウェアが市販されており、実証実験ではそれを利用した。

4 http://www.echonet.gr.jp/
ECHONET Lite とは、家電機器、スマートメーター、太陽光発電システムなどを含む約 80 種類以上の機器の制御を規定した通信規格。

4. 想定モデル

4.1. 想定システム

本書で想定するのは、製造ラインの制御を行う産業ロボットシステムとエネルギー管理を行うエネルギーマネジメントシステムの 2 つを、生産監視システムで一元的に操作できるようになっているシステムである。個々のシステム間の関係は次のとおりである。(図 2)

- 生産監視システムでは、産業ロボットシステムとエネルギーマネジメントシステムの各種監視情報(正常／異常状態、ON／OFF 状態などの運転情報)を得て、それを表示している。特に、前者からは生産稼働情報、後者からは電力情報も取得している。
- 生産監視システムは、産業ロボットシステムの機器やエネルギーマネジメントシステムの機器を操作できる。
- 産業ロボットシステムとエネルギーマネジメントシステムは、直接的につながっており、産業ロボットシステム側からエネルギーマネジメントシステム内の照明や空調等の制御を行うことができる。

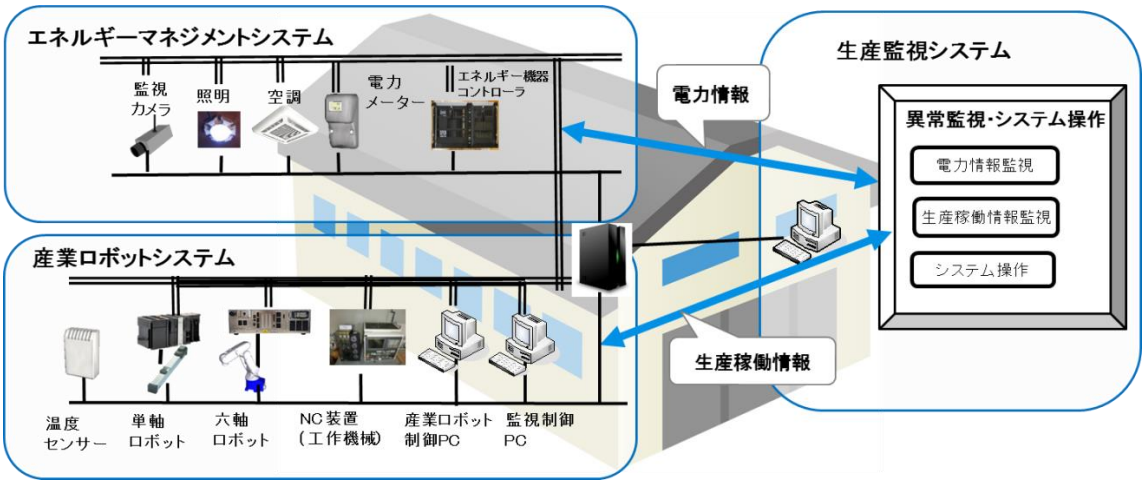

図 2 想定システム

4.2. 想定モデルでの課題

前述のようなシステムを構築するに際しては、種々の脅威の増大が心配されている。特に、産業ロボットシステム側の脅威として、機器の劣化／セキュリティ異常／機器異常の拡散などが考えられる。

- 老朽化した産業用機器の突然の故障、老朽化したインフラ設備の突然の破損
- 産業ロボットシステムの制御系プログラムへのマルウェアによる高度な攻撃[5]

[5] 高度な技術を持ったマルウェアが悪意によりネットワーク上で公開される危険性があり、著名な APT(Advanced Persistent Threat)の 1 つである stuxnet のソースプログラムがネットワーク上で流出している可能性が指摘されている(Forbes)。これにより、重要インフラ施設や大規模企業のシステムに限らず、中小企業の FA システムへの APT による攻撃も懸念されている。

・ オープンな規格により接続可能な機器の範囲が広がり、基本品質や耐久性が低い機器がシステムに接続される可能性が増加

上記に対して、できるだけ早く異常を検知あるいは兆候を予測し、影響を抑止する対策が重要である。 →【課題 1】

次に、異分野のシステム(この場合は、産業ロボットシステムとエネルギーマネジメントシステム)が接続された連携システムを考えると、個々のシステムの制御判断が異なることにより、同一の機器(例えば空調など)への制御の競合が起こり、稼働環境の悪化や機器の故障につながる可能性がある。 →【課題 2】

このように、IoT の特徴である色々な機器やシステムの接続、異分野間でのシステム連携において、早期の異常検知が重要となっている。

4.3. 課題への対応方針

1) 異常検知の能力の向上【課題 1 への対応】

明らかな動作不良等が発生した場合には、現状においても産業ロボットシステム単体でも異常を検知可能だが、経年劣化による故障の予兆は単体では難しい。そこで、今回は産業ロボットシステムとエネルギーマネジメントシステムの 2 つのシステムの監視情報を連携することにより、産業ロボット・機器の異常の兆候の予測、並びに異常の早期検知を可能とする対策を行う。

2) 異なるシステムによる制御の競合の検知【課題 2 への対応】

個々のシステムの制御判断が異なることにより発生する可能性のある同一の機器(例えば空調など)への制御の競合を検知し、運用者の優先度に従ってシステムを制御する対策を行う。

5. 実験環境

5.1. 場所

実証実験は、神奈川工科大学の HEMS 認証支援センターの実験室で行った。

図 3 神奈川工科大学 HEMS 認証支援センター 実験室

5.2. システム構成

実験システムの構成を図 4 に示す。

産業ロボットシステムは、ORiN 協議会の協力を得て作成した。

- 各産業ロボットは、実機相当の動きを表示するシミュレータを利用

  シミュレータによるシステム開発で利用したソフト資産と提供元を以下に示す。

シミュレータ(富士通製 VPS)	:	デジタルプロセス株式会社
産業用ロボットエミュレータ	:	株式会社デンソーウェーブ
6軸ロボット 3D データ	:	同上
単軸ロボット 3D データ	:	ヤマハ発動機株式会社
NC 装置 3D データ	:	一般財団法人 機械振興協会
	:	ファナック株式会社

- 各産業ロボットの一元管理や連携動作は、ORiN2 に準拠したミドルウェア(株式会社デンソーウェーブ社製)を使用して実装

エネルギーマネジメントシステムは、上記神奈川工科大学の実験室の機器、システムを利用して作成した。

- 照明、空調、パトライト等は実験室内の実機を利用
- 上記環境は、ECHONET Lite 規格に準拠

生産監視システムは、ORiN 規格（ORiN2）及び ECHONET Lite 規格に準拠して開発したアプリケーションプログラムを使って独自に作成した。

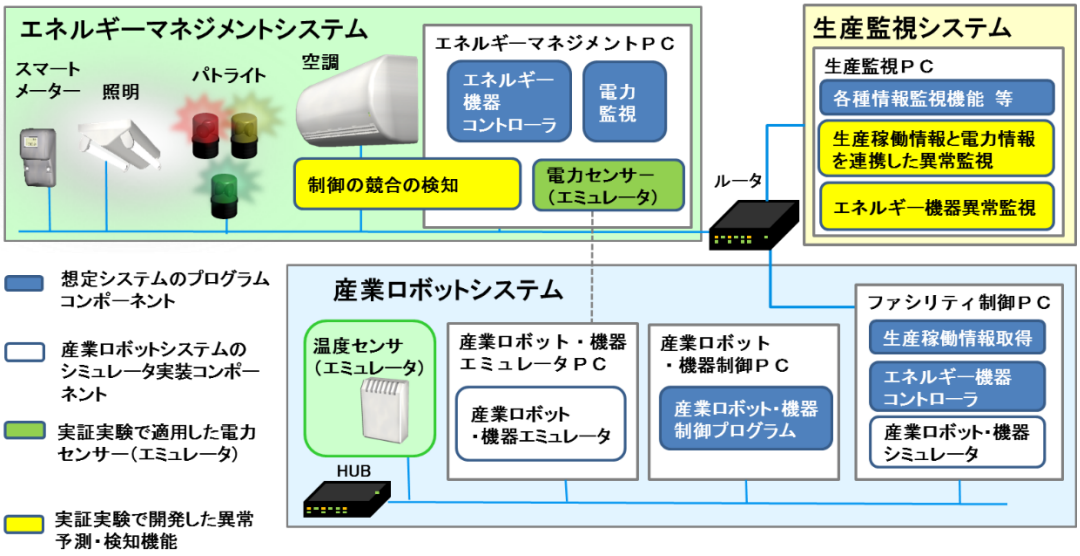

図 4　実験システムの構成

上記実験システムを実験室で動作させたときの様子を図 5 に示す。

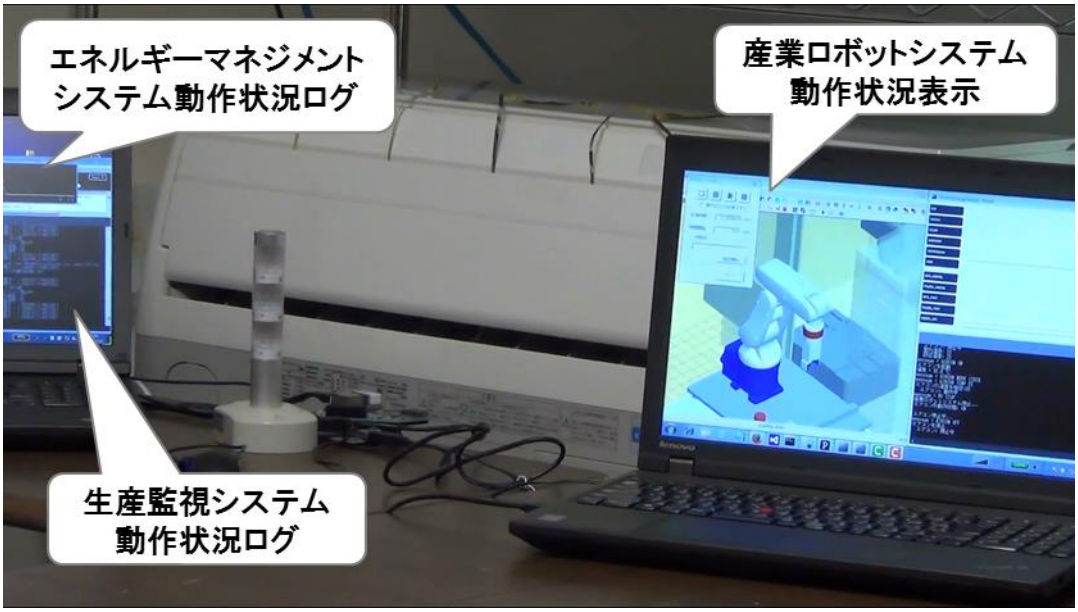

図 5　実験室での実験システム

5.3. 動作概要

想定したシステムでは、産業ロボットシステム、エネルギーマネジメントシステム、生産監視システムがルータに接続され、相互に通信して以下のように動作している。

1） 産業ロボットシステム

- 生産監視システムからの指示により産業ロボットシステムの起動・停止を行う。
- 産業ロボット・機器制御 PC からの指示により各ロボット、NC装置を制御して製造物の運動と加工を行う。前工程から運ばれてきた加工対象の製造物に対して毎回同じ処理を行う。（以降これを「1 加工サイクル」と呼ぶ。）
- 製造物の加工数を一定の時間間隔で取得し、生産監視システムからの要求に応じてそれを通知する。
- 製造環境の適切な温度を保つため、温度センサーから温度情報を取得し、必要に応じて空調に対して温度制御の指示を出す。

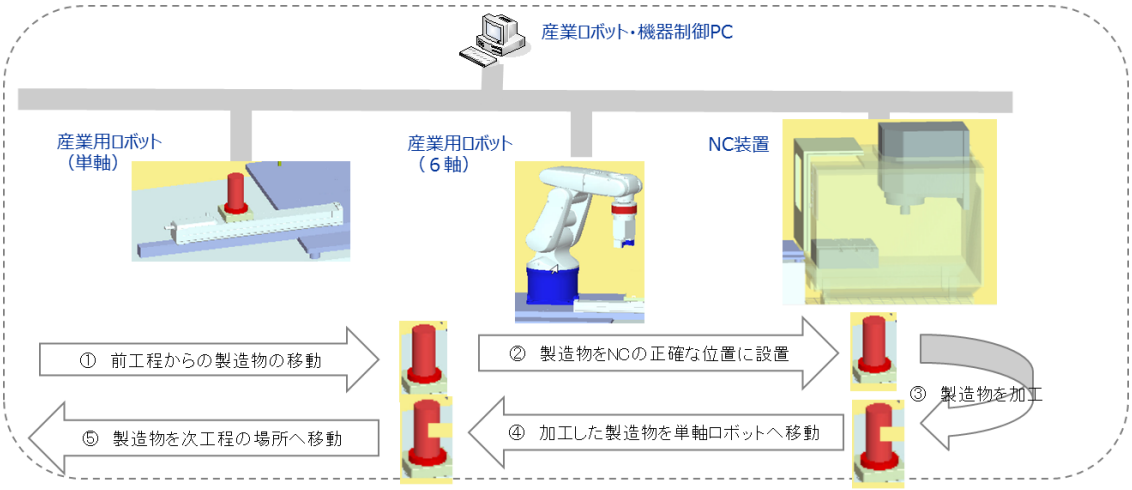

図 6 産業ロボットシステムの 1 加工サイクル

2） エネルギーマネジメントシステム

- 定期的にシステム全体の電力量を取得し、生産監視システムからの要求に応じてその値を通知する。
- システム全体の電力量が想定より速く上限に近づいている場合は、一番電力量の大きい機器（例えば空調）を停止することにより電力量の増加を抑制する。
- 生産監視システムからの指示に応じて、空調、パトライト、照明を制御する。

3） 生産監視システム

- エネルギーマネジメントシステムからの電力情報の取得と表示。
- 管理者によるエネルギーマネジメントシステム内の照明、パトライト、空調への指示。
- 産業ロボットシステムからの生産稼働情報の取得と表示。
- 管理者による産業ロボットシステムの稼働、停止の指示。

6. 実証実験

6.1. [実験 1] 異常検知の能力の向上：【「実践に向けた手引き」の機能要件 3 及び 6】

4.3 で述べたように、産業ロボットシステムの監視情報とエネルギーマネジメントシステムの監視情報を連携することにより、産業ロボット・機器の異常の兆候の予測、並びに異常の早期検知を可能とする方式を考えた。

以下では、その課題の詳細化を行うとともに、対策で適用する方式について述べる。

6.1.1. 一般的な生産稼働情報、電力情報の監視

1） 生産稼働情報の監視

時間、あるいは日単位での生産物数や産業ロボットの稼働時間などを監視しているのが一般的である。システムが意図どおりに稼働しているかを確認し、生産計画と照らし合わせて問題が発生していないかを把握するためのものであり、多くの場合、個々の異常検知を行う目的では利用されていない。

2） 電力情報の監視

産業ロボット及び空調設備などをまとめた工場全体の電力量を監視しているのが一般的である。工場全体の環境状況やコストを確認し、必要に応じて電力量を制御するものであり、多くの場合、個々の異常検知を行う目的では利用されていない。

なお、生産稼働情報と電力情報はそれぞれ独立して参照されていることが多く、それらの関係に関する情報を導出して監視することは、あまり行われていない。

6.1.2. 異常検知を目的とした監視情報

1） 個々の監視情報（生産稼働情報、電力情報）の異常検知への活用

上記のように、多くの場合、生産稼働情報は個々の機器の異常検知を行う目的では利用されていないが、その情報の導出元である産業ロボットシステムの動作の特徴を活用して詳細化を図ることにより、異常検知に役立てることができる可能性がある。しかし、現状のような時間あるいは日単位での生産稼働情報のままだと、以下の理由により、異常検知には利用できない。

- 生産稼働情報の変化が産業ロボットシステムの正常な稼働量の増減によるものなのか、一時的なシステムの停止により発生したものなのか、機器の異常や劣化/操作ミス/データ取得誤りなどによって発生したものなのか、という区別が難しい。

電力情報についても同様に、多くの場合、異常検知を目的としては利用されていないが、電力を使用しているシステムの特徴を活用したり、情報の詳細化を図ることにより、異常検知に役立てることができる可能性がある。しかし、やはり、現状のような工場全体の電力や電力

量の推移を取得しているのみでは、以下の理由により、異常検知には利用できない。

- 最大電力がどの程度か、ある一定期間内の電力量がどの程度か、増加傾向がどの程度か、ということは把握できるが、それらの値が異常なのかどうか、変化の原因はなんであるのか、といったことの推定はできない。

そこで、最初のステップとして、現状の監視情報をシステムの特徴を活用して詳細化することで変化要因の範囲をある程度狭め、異常検知に利用できるようにすることを検討した。

⇒ ステップ 1:監視情報の詳細化による異常検知方式

2) 2 つの監視情報(生産稼働情報、電力情報)を連携して異常検知に活用

複数の監視情報の間に明確な関係が認められる場合、その関係の変化を検知することにより、個々の情報では検知できない異常を検知できる可能性がある。

- 2 つの監視情報の関係の変化を監視した場合、正常な状態では現れることがほとんどなく、異常な状態で現れる変化を検知できるケースがある。
- データ取得誤りやデータ改ざんが発生したとき、個々の監視情報のみではそれらを検知することはできないが、2 つの監視情報の関係を監視した場合、その変化によってそれらの発生の可能性を検出することができる。

そこで、次のステップとして、2 つの監視情報(生産稼働情報、電力情報)を組合せてそれらの関係を示す情報の変化を監視することにより、正常時にはほとんど起きない変化を検知することで異常検知につなげる対策を検討した。

⇒ ステップ 2:生産稼働情報と電力情報の組合せによる異常検知の高度化方式

6.1.3. 異常検知の高度化方式の検討

1） 産業ロボットシステムの特徴

本実証実験で想定している産業ロボットシステムは、産業ロボット・機器が定型的な動作を繰り返すものであり、この一定の加工サイクルに要する時間と消費する電力量は、正常に動作する場合はほぼ一定である。(図 7)

この特徴を用いて、2)、3) で示す対策方式を考えた。

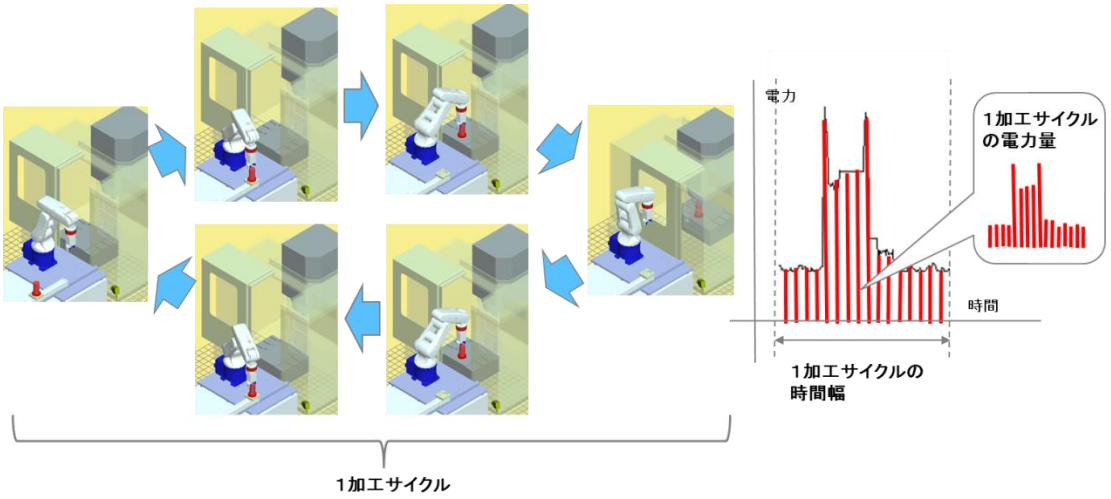

図 7 1 加工サイクルあたりの電力量

2） 異常検知の高度化方式 1⇒ ステップ 1:監視情報の詳細化による異常検知方式

対策前の生産稼働情報の監視では、各産業ロボット・機器の動作情報、並びに製造ライン制御プログラムの動作情報から製造物の加工数を算出して監視していた。それに加えて、上記産業ロボットシステムの特徴を適用し、1 加工サイクルに要する時間を算出し、その値を監視する対策を検討した。その概要を以下に示す。

① 生産稼働情報の正常時の基準値の取得

(基準値 1)生産稼働情報から得られる 1 加工サイクルに要する時間

これまでの生産稼働情報は、時間や日単位のものであったが、1 加工サイクルに要する時間(数秒～数分)を測定し、正常な加工速度との比較を可能にした。

② 基準値との乖離による異常検知

(比較 1) 1 加工サイクルに要する時間を随時監視し、基準値 1 と比較

【検知が可能となる異常】

1 加工サイクルに要する時間が想定どおりでない場合、産業ロボット・機器の動作が異常であることが濃厚である。したがって、この値を動作の異常の検知に活用可能である。

電力情報についても、詳細化により異常検知につなげる対策が考えられる。例えば、産業

ロボット・機器の電力波形について正常時と異常時の違いを明確に判断できれば、それを監視することにより異常を検知することができる。しかし、それらの方式は一般には複雑であり、簡単な実装で効果を期待できそうにない。そのため、今回は電力情報の詳細化は検討からは除外することにした。

3) 異常検知の高度化方式 2⇒ ステップ 2:生産稼働情報と電力情報の組合せによる異常検知方式

上記産業ロボットシステムの特徴で記述したように、生産稼働情報から得られる 1 加工サイクルあたりの時間と電力情報から得られる電力量とは、正常時には以下の関係にある。

＜1 加工サイクルあたりの電力量は常に一定＞

そこで、1 加工サイクルあたりの電力量を算出してそれを監視し、その値の変化から異常を検知する対策を検討した。その概要を以下に示す。

① 生産稼働情報と電力情報を組み合わせた情報の正常時の基準値の取得

(基準値 2)生産稼働情報と電力情報から得られる 1 加工サイクルに要する電力量

生産稼働情報から得られる 1 加工サイクルの開始時刻と時間を電力情報(電力量の時間推移)に適用することにより、1 加工サイクルに要する電力量を算出できる。

② 基準値との乖離による異常検知

(比較 2) 1 加工サイクルに要する電力量を随時監視し、基準値 2 と比較

【検知が可能となる異常】

1 加工サイクルに要する電力量の値が基準値と乖離した場合、何等かの異常が発生したと考えられる。同一の仕事量のために消費した電力量に差異が発生したということは、産業ロボット・機器の動作とそのために消費した電力量との間の相関関係に矛盾が生じたと言えるからである。したがって、個々の情報のみ(生産稼働情報のみ、または電力情報のみ)では判断がつかなかった以下のケースの異常検知が可能となる。

- 内包不良のある、あるいは老朽化した産業ロボット・機器の中での過電流や漏電の発生
- データ取得誤りやデータ改ざん

本方式で検知できる異常の主な原因としては、上記のように、機器の不良、機器の劣化、データ取得誤り、データ改ざんなどが考えられ、その切り分けには更なる詳細情報の取得が必要となる。ここでは、異常を早期に検出してそれを通知することに主眼を置いた。

4) 本方式による異常の検知と考えられる原因

上記対策により検出される各異常のパターンと考えられる原因を表 2 に示す。

表 2 異常検知のケースと考えられる原因

比較 1 の結果（1 加工サイクルあたりの時間）	比較 2 の結果（1 加工サイクルに要する電力量）	考えられる原因
許容範囲内	許容範囲外（大きい）	A. 産業ロボット・機器での過電流または漏電の発生 （内包不良 または 老朽化による）
		B. 産業ロボット・機器以外の箇所での漏電の発生
		C. 攻撃による改ざん ・ 産業ロボット・機器制御プログラムが改ざんされて産業ロボット・機器が速く動作し、更に、生産稼働情報が正常時の値に改ざん
		D. 監視情報の誤り
	許容範囲外（小さい）	E. 攻撃による改ざん
		F. 監視情報の誤り
許容範囲外（短い）	許容範囲外（大きい）	G. 産業ロボット・機器での過電流または漏電の発生 （内包不良 または 老朽化による）
		H. 産業ロボット・機器以外の箇所での漏電の発生
		I. 攻撃による改ざん ・ 産業ロボット・機器制御プログラムが改ざんされて産業ロボット・機器が速く動作
		J. 監視情報の誤り
	許容範囲内	K. 攻撃による改ざん ・ 産業ロボット・機器制御プログラムが改ざんされて産業ロボット・機器が速く動作
		L. 監視情報の誤り
	許容範囲外（小さい）	M. 攻撃による改ざん ・ 産業ロボット・機器制御プログラムが改ざんされて産業ロボット・機器が速く動作し、更に、電力情報が正常時の値に改ざん
		N. 監視情報の誤り

比較 1 の結果 （1 加工サイクルあたりの時間）	比較 2 の結果 （1 加工サイクルに要する電力量）	考えられる原因
許容範囲外（長い）	許容範囲外（大きい）	O. 産業ロボット・機器での過電流または漏電の発生 （内包不良　または　老朽化による）
		P. 産業ロボット・機器以外の箇所での漏電の発生
		Q. 攻撃による改ざん ・ 産業ロボット・機器制御プログラムが改ざんされて産業ロボット・機器が遅く動作し、更に、電力情報が正常時の値に改ざん
		R. 監視情報の誤り
	許容範囲内	S. 攻撃による改ざん ・ 産業ロボット・機器制御プログラムが改ざんされて産業ロボット・機器が遅く動作
		T. 監視情報の誤り
	許容範囲外（小さい）	U. 攻撃による改ざん ・ 産業ロボット・機器制御プログラムが改ざんされて産業ロボット・機器が遅く動作
		V. 監視情報の誤り

6.1.4. 異常検知の高度化方式の実装

本対策の実装方法を以下に示す。

1） 異常検知の高度化方式 1 の実装

本方式による対策の実装の内容を以下に示す。

① 1 加工サイクルあたりの時間の取得

産業ロボットシステム内ファシリティ制御 PC で、生産稼働情報（各産業ロボット・機器の動作情報）を取得し（実証実験では 0.1 秒毎）、各産業ロボット・機器の動作パターンから、1 加工サイクルの開始時刻と終了時刻を取得した。

開始時刻 ： 6 軸ロボットのアームの位置の初期設定動作と単軸ロボットの製造物搬入動作から取得

終了時刻 ： 6 軸ロボットが製造物を単軸ロボットに渡す動作と単軸ロボットが製造物を搬出する動作から終了時刻を取得

上記開始時刻と終了時刻から 1 加工サイクルあたりの時間を算出した。

② 正常時の基準値（基準値 1）の取得

①で記載した機能を使って、正常に動作している時の 1 加工サイクルあたりの時間を測定した。そして 10 回の測定の平均値を基準値として生産監視システム内の生産監視 PC に保存した。

③ 運用時の監視

ファシリティ制御 PC では、①で記載した機能を継続して実行し、随時 1 加工サイクルの開始時刻と終了時刻、1 加工サイクルあたりの時間を取得する。生産監視 PC の「生産稼働情報と電力情報を連携した異常監視」の機能は、1 秒毎にファシリティ制御 PC に対して監視情報の取得要求を送信し、最新の 1 加工サイクルの情報を取得する。そして、取得してきた値を②で保存しておいた基準値と比較し（比較 1）、許容範囲に入っていなければ異常発生を示すメッセージをコンソールに出力すると同時に緑のパトライトを点灯する。1 加工サイクルあたりの時間の許容範囲は以下とした。

1 加工サイクルあたりの時間 ： 基準値の±10%以内

2） 異常検知の高度化方式 2 の実装

本方式による対策の実装の内容を以下に示す。

① 電力センサーの導入

産業ロボットシステムの各機器に電力センサーを取り付けて個々の電力量に関する情報をエネルギーマネジメントシステム内のエネルギーマネジメント PC で取得可能とした。

② 1 加工サイクルあたりの電力量の算出

生産監視 PC の「生産稼働情報と電力情報を連携した監視機能」において、1 加工サイクルあたりの電力量を算出する機能を実装した（図 8）。処理の概要を以下に示す。

- ファシリティ制御 PC に異常検知の高度化方式 1 で算出された監視情報の取得要求を 1 秒間隔で出す。また、エネルギーマネジメント PC（電力監視機能）に電力量情報の取得要求を 1 秒間隔で出す。
- 1 秒毎の電力量情報に対して 1 加工サイクルの開始時刻と 1 加工サイクルあたりの時間を適用し、1 加工サイクルあたりの電力量を算出する。

③ 正常時の基準値（基準値 2）の取得

②の 1 加工サイクルあたりの電力量算出機能を使って、正常に動作している時の 1 加工サイクルあたりの電力量の値を測定した。そして 10 回の測定の平均値を基準値（基準値 2）として生産監視 PC に保存した。

④ 運用時の監視

②の 1 加工サイクルあたりの電力量算出機能により 1 加工サイクルあたりの電力量を随時取得する。この時点で、高度化方式 1 の③の監視処理において、1 加工サイクルあたりの時間が許容範囲内になければ、異常発生を示すメッセージをコンソールに出力すると同時に緑のパトライトを点灯する。1 加工サイクルあたりの時間が許容範囲内であれば、②の機能により 1 加工サイクルあたりの電力量を算出し、その値を③で保存しておいた基準値（基準値 2）と比較する（比較 2）。その結果、許容範囲に入っていなければ異常発生を通知するメッセージをコンソールに出力し、赤パトライトを点灯する。1 加工サイクルあたりの電力量の許容範囲は、基準値の±15%以内とした。実際のシステムで適用する場合は、使用している産業ロボット・機器の仕様と正常に動作しているときの測定値の分散から、許容範囲を決める必要がある。

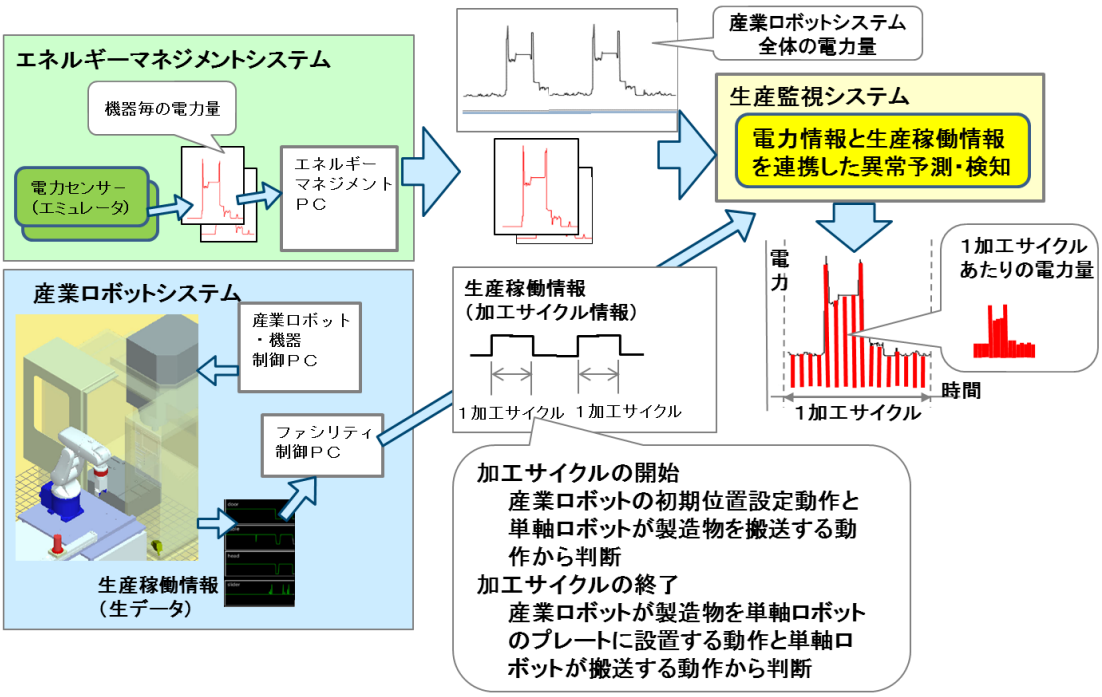

図 8 生産稼働情報と電力情報を連携した監視情報の生成

6.1.5. 実験内容

1）　実験ケース 1(表 2 の K のケース) : 異常検知の高度化方式 1

産業ロボット・機器制御プログラム動作時に各機器の動作速度が格納されているメモリ領域が改ざんされて想定よりも速く動作した場合(1 加工サイクルあたりの時間が許容範囲よりも小さい場合)

【実験内容と結果】(図 9 参照)

1 加工サイクルあたりの時間が許容範囲を超えた場合、それを判断して異常発生通知メッセージが出ることを確認した。

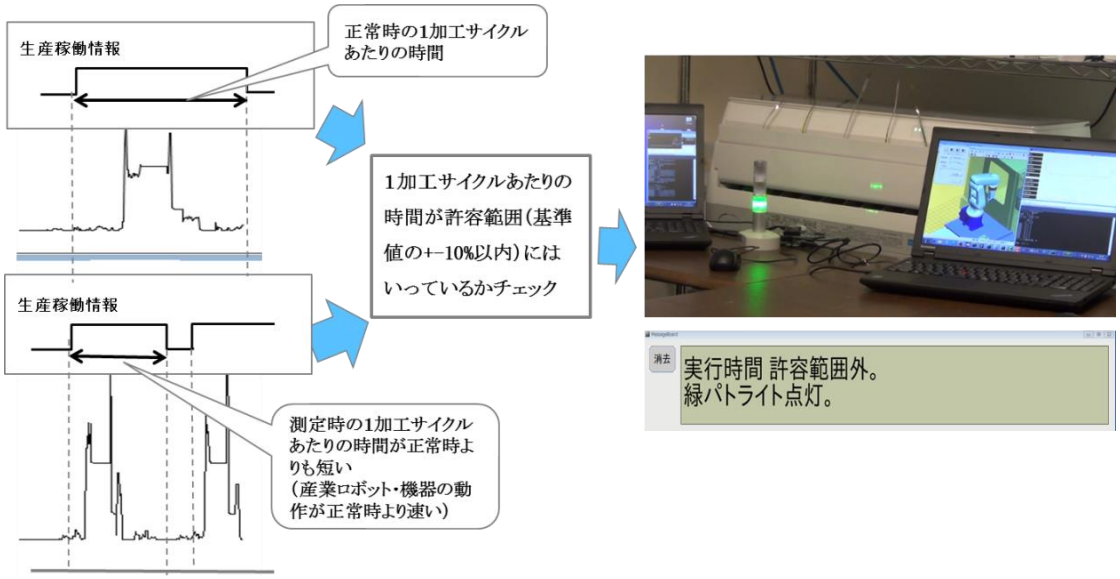

図 9 1 加工サイクルあたりの時間が短いケース

2)　実験ケース 2(表 2 の A、B のケース):異常検知の高度化方式 2

産業ロボット・機器の劣化等により、1 加工サイクル当たりの電力量が許容範囲を超えた場合(1 加工サイクルあたりの時間には大きな変化がないという前提)

【実験内容と結果】(図 10 参照)

上側のグラフは、正常時の 1 加工サイクル当たりの電力量を示したものである。一方、下側のグラフは、1 加工サイクル当たりの電力量が許容範囲を超えた場合である。

電力量が基準値の±15%の閾値を超えたため、それを判断して異常発生通知メッセージが出ることを確認した。

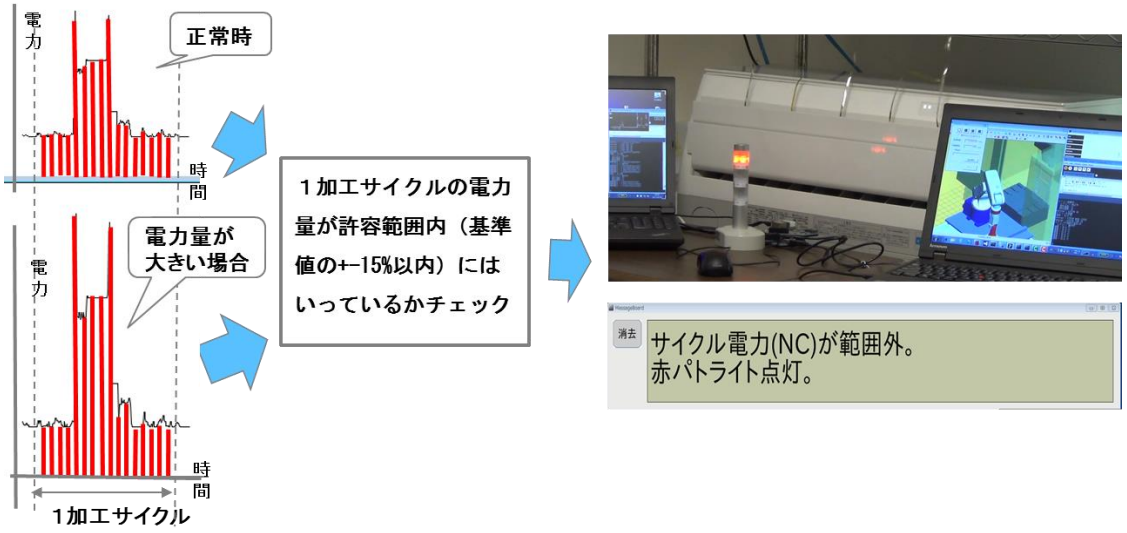

図 10　1 加工サイクルあたり電力量が許容範囲外

3）実験ケース 3(表 2 の C のケース):異常検知の高度化方式 2

産業ロボット・機器制御プログラム動作時に、その制御プログラムがメモリ上に展開していた各機器の動作速度が改ざんされて想定よりも速く動作するが、生産稼働情報が正常な値に改ざんされ、1 加工サイクルあたりの時間が許容範囲内となっている場合(1 加工サイクルの電力量は正常時よりも大きくなる)

【実験内容と結果】(図 11 参照)

1 加工サイクルあたりの時間の異常は検出できないが、その時間での電力量は許容範囲を超え、それを検知して異常発生通知メッセージが出ることを確認した。

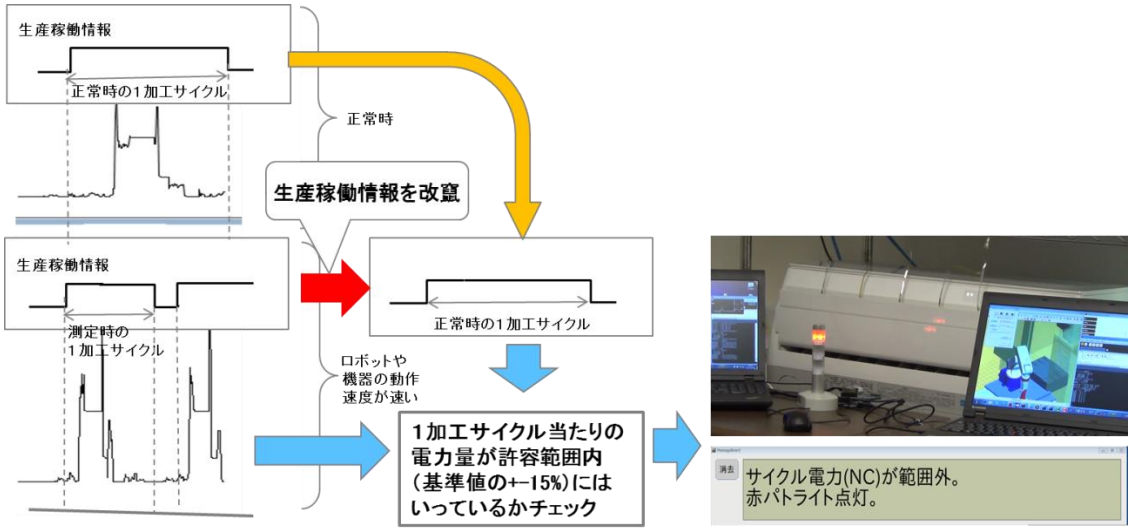

図 11　1 加工サイクルあたりの時間が短いが生産稼働情報が正常時の値に改ざんされたケース

6.1.6. 評価と考察

1） 開発規模と実行時の負荷

本対策を実装したときの開発規模を以下に示す。

- 産業ロボットシステム

  ファシリティ制御 PC での生産稼働情報取得処理　:0.5kstep／機器（C++）

  0.5kstep×3 台（単軸ロボット、六軸ロボット、NC 装置） =1.5kstep
- エネルギーマネジメントシステム

  エネルギーマネジメント PC での電力情報取得処理　:0.6kstep(Java)
- 生産監視システム

  電力情報と生産稼働情報を連携した異常監視機能　:1.1kstep（Java）

本対策で実装した処理を実行したときの負荷については、生産稼働情報と電力情報をともに 0.1 秒毎に取得したケースにおいて、それぞれの PC（ファシリティ制御 PC、エネルギーマネジメント PC）の負荷は CPU 使用率が 1%前後上がったが、それらの PC 上の他の機能の動作が遅くなるといった影響はなかった。また、ネットワーク負荷は、測定ツールでは認識できないほど小さいものであった。

2） 異常検知の高度化方式 1（監視情報の詳細化による異常検知方式）の評価

本方式では、1 加工サイクルあたりの電力量を算出するにあたり、1 加工サイクルあたりの時間を算出し、その値をチェックしている。産業ロボット・機器の動作が正常時より速くなる状態を作り出し、今回実装した機能がそれを異常として検知することを確認した（実験ケース 1）。したがって、産業ロボット・機器の制御プログラムが改ざんされ産業ロボット・機器が想定外の速度で動作した場合、今回の方式によりそれを検知することが可能と言える。

産業ロボット・機器の制御プログラムが改ざんされて想定より速く動作した場合、製造物の破損、産業ロボット・機器の破損を引き起こす可能性がある。逆に想定よりも遅く動作した場合、製造遅延が発生する可能性がある。動作速度が変更されるような改ざん攻撃を受けたときでも、1 加工サイクルあたりの時間が正常時と比べて変化していることを検出することにより、それらの被害を防ぐことができる。

3） 異常検知の高度化方式 2（生産稼働情報と電力情報の組合せによる異常検知方式）の評価（監視情報が改ざんされていないケース）

今回実装した機能を、産業ロボット・機器の電力量が正常時よりも大きくなっている状態を作り出して動作させ、異常として検知することを確認した（実験ケース 2）。したがって、産業ロボット・機器の内包不良や老朽化により、過電流や漏電が発生して電力量が変化した場合、今回の方式によりそれを検知することが可能と言える。

4） 異常検知の高度化方式 2（生産稼働情報と電力情報の組合せによる異常検知方式）の評価（監視情報が改ざんされたケース）

本書 4.2 で記載したように、中小企業の工場であっても高度なマルウェアの攻撃対象となりうる。このようなマルウェアの攻撃により、産業ロボット・機器の動作速度が改ざんされ、かつ、それを検知されないために生産稼働情報が正常時の値に改ざんされるようなケースが考えられる。この状況を想定して、今回実装した機能の動作を以下のように確認した。

- 産業ロボット・機器の制御プログラムを改ざんして産業ロボット・機器が正常よりも速く動作し、その上で生産稼働情報（産業ロボット・機器の動作情報）が正常な値に改ざんされた状態を作り出し、今回実装した機能が異常な状態として検知することを確認した（実験ケース 3）。

前記のように、本方式は、1 加工サイクルあたりの電力量を監視することにより生産稼働情報と電力情報の相関性をチェックしているため、制御プログラムの改ざんを検知させないことを目的として一方の監視情報（生産稼働情報）が正常時の値に改ざんされたとしても、1 加工サイクルあたりの電力量が正常時から変化していることを検知して、それを異常な状態として通知することができた。

異常検知の高度化方式 2 の実証実験では、産業ロボット・機器の刻々と変化する情報を監視して 1 加工サイクルの開始から終了までの時間を検出し、これを時間とともに変化する電力情報にあてはめることにより、1 加工サイクルあたりの電力情報を算出し、その値を監視している。実験ケース 3 では、産業ロボット・機器の動作情報をなんとか正常時の値で更新したが、一方の時間とともに変化する情報をもう一方の時間とともに変化する情報と同期させて改ざんし、正常な状態に見せることは、詳細なシステムの稼働情報を取得しない限り、非常に難しいことを確認した。今回の実験から、時系列で変化する複数の情報の相関性を監視して異常検知につなげる方式は、監視情報の改ざんに対しても非常に有効であると考える。

6.2. [実験2] 異なるシステムによる制御の競合の検知:【「実践に向けた手引き」の機能要件６】

6.2.1. 想定する制御の競合

複数の異なる分野のシステムを使ってシステムを構築した場合、一方の分野のシステムが優先する処理と他方の分野のシステムが優先する処理とが相反する状況が起こることが考えられる。

本実証実験で想定するシステムでは、産業ロボットシステムとエネルギーマネジメントシステムという 2 つの異なる分野のシステムを接続している。産業ロボットシステムでは、適切な温度環境を保つために、温度が一定以上になったとき空調に稼働指示を出すことが想定できる。一方、エネルギーマネジメントシステムの機器を制御するコントローラでは、全体電力量の許容値を超えそうになったら電力消費の大きい機器を停止する、といった機能をもつものも存在する。これらの個々のシステムの判断により、空調に対して稼働指示（パワーオン）と稼働停止（パワーオフ）が交互に指示される可能性がある。このような制御の競合が発生すると、それぞれのシステムの目的が達せられず、またこの状態が続くと空調の故障につながる可能性もある。

6.2.2. 制御の競合への対策の検討

対策の1つの例として、制御の競合自体を発生させないようにする、防止のための対策がある。機器に対して指示をある特定のサーバのみから出すようにし、機器の制御はそのサーバのみが行うようにすれば、制御の競合を防止でき、この対策を実装している例もある。

一方、様々なシステムや機器が動的に接続されていく IoT の世界では、機器の制御をある特定のサーバに集中させる、という防止のための対策は、接続される機器やシステムが増えるたびにそのサーバでの対応が必要になることもあり、すぐには対応できないことも考えられる。そこで、あらかじめ各機器やシステムが単体で制御の競合を検知する機能を実装していれば、なんらかの被害が発生する前に対処することが可能となる。

今回は、被害が発生する前に早期に異常を検知する方式に主眼を置き、空調で制御の競合を検知して監視サーバに通知する機能を設けることを検討した。（導入している機器の中には、仕様上の制限により、制御の競合を検知する機能を実装できないものもある。その場合は、「つながる世界の開発指針」の【[指針 8] 個々でも全体でも守れる設計をする】で提示しているように、監視用のサーバがその機器を監視して実現する方法がある。）

空調で制御の競合を検知する方式として、以下を考えた（図 12）。

- 稼働指示（パワーオン）を受信してかつ実行したとき、稼働指示回数をカウントアップする。空調は、一般に、ある指示を受信したとき、一定時間たたないと次の指示を実行しない制御が実装されている。また、同じ指示が連続してきた場合、後で受信した指示は実行しないようになっている。つまり実行した指示のみをカウントアップの対象とする。
- 稼働停止（パワーオフ）を受信したときも同様で、実行したものについてのみ稼働停止回数をカウントアップする。（稼働停止中に稼働停止の指示がきてもそれは実行で

きないため、稼働停止の回数のカウントアップの対象とはしない。）

- 稼働指示（パワーオン）のカウントと稼働停止（パワーオフ）のカウントを数え、ある時間内にその値が閾値を超えた場合（例えば 5 分間に 4 回以上）は、制御の競合が発生したと認識し、それをログに記録する。
- 生産監視 PC のエネルギー機器異常監視機能から、空調に対してログの取得依頼を例えば 1 秒に 1 回出し、制御の競合を検知したことを示すログが返されてきたら、アラームを上げる。

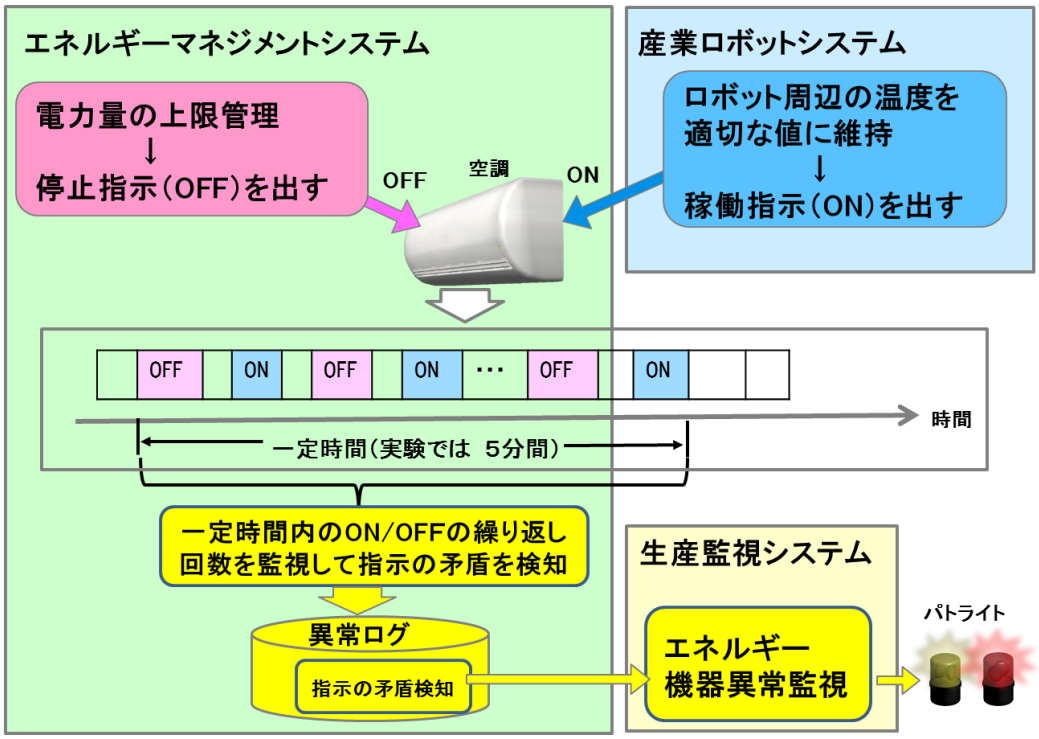

図 12 制御の競合の検知方式

6.2.3. 制御の競合への対策の実装

空調への制御の競合を検知するために実装した方式を図 13 に示す。

本実証実験では、すでに市販されている空調に今回検討して機能を組み込むことは難しいこともあり、エネルギーマネジメントシステム内のエネルギーマネジメント PC で制御の競合を検知するための機能を実装した。そこでは、空調が受信する制御データを通信経路上でキャプチャリングし、パワーオンとパワーオフの制御が一定時間内（実験では 5 分を指定）に一定回数以上（実験では 4 回）連続していることを検知したらそれを一時的なログ領域に保持しておく。生産監視システムは定期的に（実験では 1 秒に 1 回）空調に対して異常ログの取得依頼を出し、制御の競合を示すログが返却されてきたらパトライト（黄）を点灯する。

生産監視システムは、その後も空調から新たな制御の競合を示すログが返却されてきた場合は、警告メッセージを表示し、パトライト（赤）を点灯する。

生産監視システムは、更に空調から新たな制御の競合が返却されてきた場合は、電力量の削減を優先して、空調から返却された制御の競合を示す異常ログの中に記載されている指示の送信元（実証実験では、異常産業ロボットシステム）に停止指示を出す。

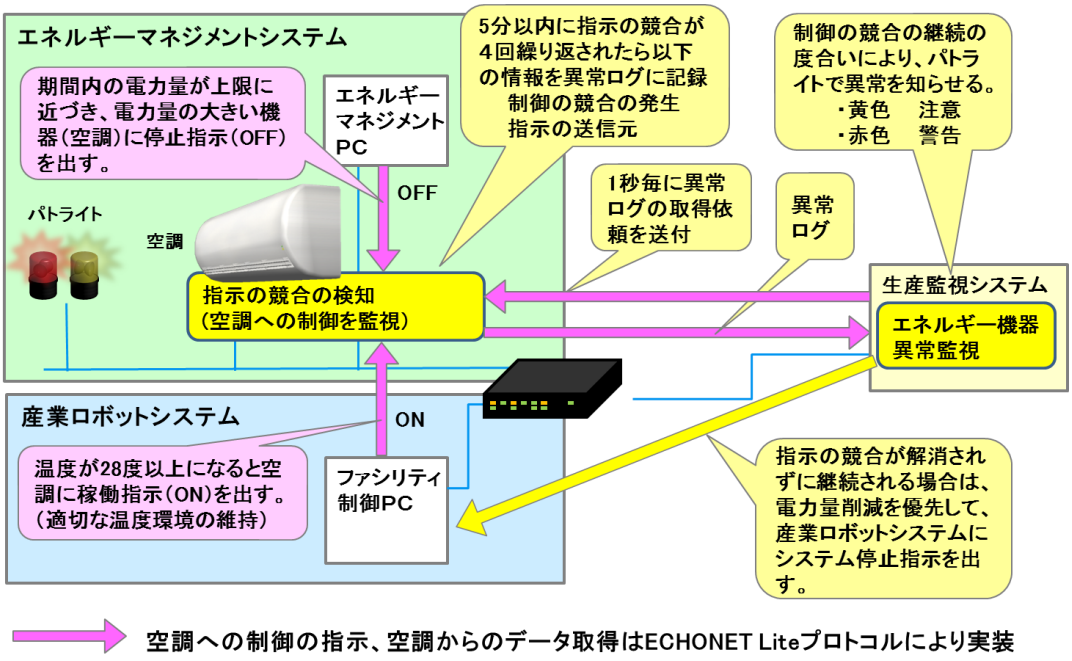

図 13 空調で制御の競合を検知する方式の実装

6.2.4. 実験内容

温度センサーの設定により工場内の温度が高い状況を疑似的に作り、産業ロボットシステムのファシリティ制御 PC は空調が稼働していなければ稼働開始の指示を出す状態にした。また、指定期間（例えば 1 か月）の電力量が上限に近い状態とし、エネルギーマネジメントシステムのエネルギーマネジメント PC は電力量が大きい機器（本システムの場合は空調）が稼働していた場合はその機器に停止指示を出す状態とした。

この状態でシステムを稼働させたとき、以下の順番で状況が推移することを確認した。

① 指示の競合の発生前（図 14）

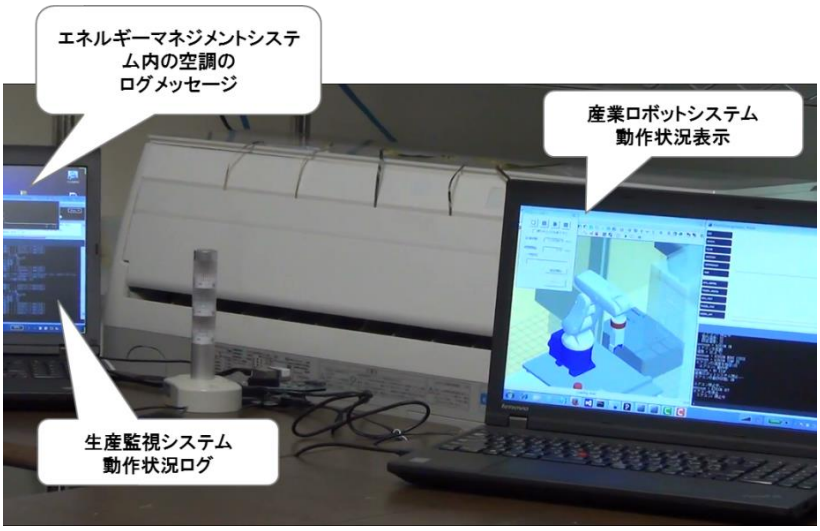

図 14 実験システム（異常発生前）

② 産業ロボットシステムから空調へのパワーオンの指示（図 15）

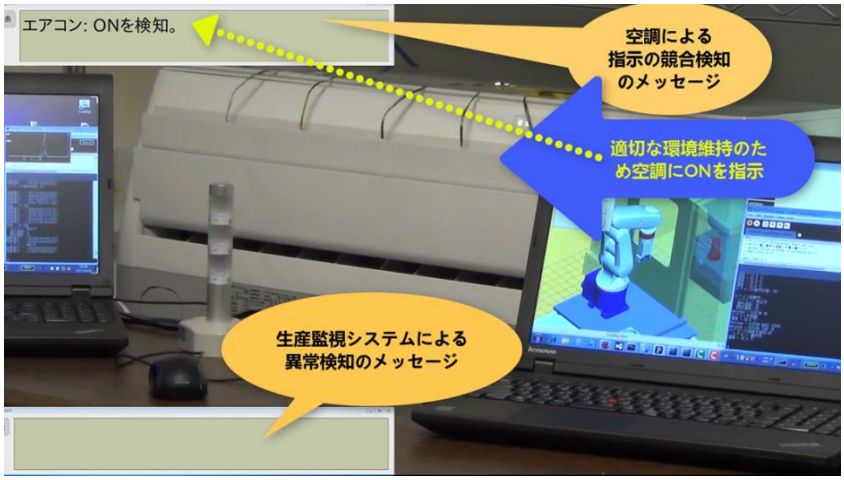

図 15 空調へのパワーオンの指示発生

③ エネルギーマネジメントシステムから空調へパワーオフの指示（図 16）

図 16 空調へのパワーオフの指示発生

④ 制御の競合を検知し、注意発生 → パトライト（黄色）点灯（図 17）

図 17 制御の競合の検知

⑤ 制御の競合が解消されず、警告発生 → パトライト(赤色)点灯(図 18)

図 18 制御の競合の継続発生に対する警告

⑥ 生産監視システムは、電力量制限を優先して産業ロボットシステムを停止(図 19)

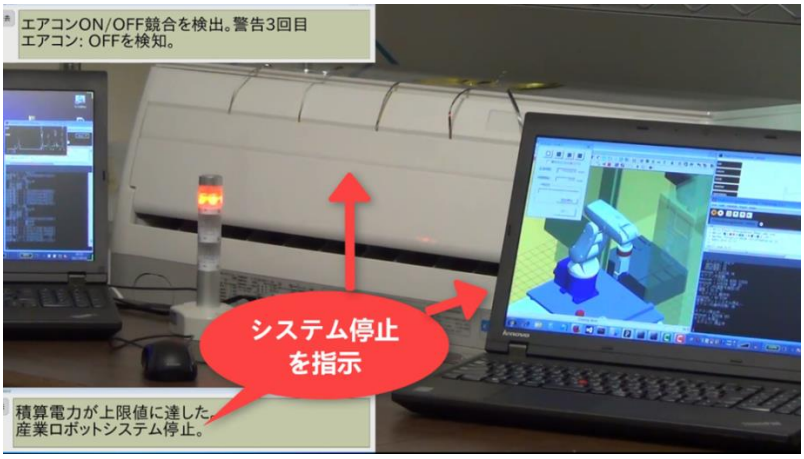

図 19 警告 → 電力量制限を優先して産業ロボットシステム、空調を停止

どの状態を優先するかについては、システム毎の利用者の要件によって決まる。本実証実験では、電力量制限を守ることを優先し、産業ロボットシステムを停止した。

6.2.5. 評価と考察

1) 開発規模と実行時の負荷

開発規模は以下のとおり。

- エネルギーマネジメントシステム

  エネルギーマネジメント PC での空調の制御の競合検出処理 :1.2kstep(Java)

- 生産監視システム

  エネルギー機器異常監視機能 :0.5kstep(Java)

競合制御の検知機能は、1 秒毎に空調が受信する指示を監視している。この場合でエネルギーマネジメント PC の CPU 使用率はほとんど上がっていなかった。ただし、この機能を空調に実装する場合、空調内のファーム実行 CPU の使用率の変化を確認する必要がある。

通信への負荷は、測定ツールで分からないほど小さかった。

2） 制御の競合の発生とその検知

産業ロボットシステムで参照する工場内の温度センサーとして実験環境のエミュレータを利用し、絶えず温度が高い状況を作った。また、電力発生機能を使って期間内の電力量が上限値に近い状態とした。この環境において、産業ロボットシステムからは空調への稼働指示が 10 秒から 30 秒の間隔で送出され、エネルギーマネジメントシステムでは空調への稼働停止の指示がやはり 10 秒から 30 秒の間隔で送出されることを確認した。

この状況において、システムの以下の動作を確認した。

- エネルギーマネジメント PC の制御の競合の検知機能は、空調がパワーオンとパワーオフの指示を連続して受信していることを検知した。
- 生産監視 PC のエネルギー機器異常監視機能が、空調から取得したログ情報から制御の競合の発生を認識してそれをメッセージとパトライト（黄色）により通知した。
- 制御の競合が一定時間以上続いたときは、電力量を制限範囲に抑えることを優先し、産業ロボットシステムが停止した。

今回の実験では、監視制御 PC から空調に異常ログの取得要求を 1 秒毎に出したが、これにより、監視機能が検出した空調の稼働指示（パワーオン）の実行回数と稼働停止（パワーオフ）の実行回数が、実際の空調の動作（パワーオンとパワーオフの繰り返し）と一致していることを視覚的に確認できた。結果として、空調へのパワーオフとパワーオンが交互に発生したとき、それが単発的に発生したのではなく継続して発生している状態を確認し、実装した異常検知機能が、それを確実に制御の競合として検知していることを検証できた。

3） 意図的に機器への指示を改ざんする攻撃への有効性

本実証実験では、産業ロボットシステムとエネルギーマネジメントシステムのそれぞれの空調への指示に矛盾が発生する状況を発生させ、実装した異常検知の機能の効果を確認した。他方、（今回は実験システムで発生させてはいないが、）ある特定の機器（今回は空調）への指示が悪意をもった攻撃により改ざんされて意図的に指示の矛盾が発生させられるケースも考えられる。今回は、異常検知の機能を機器側にもたせることを想定して実装したが、この対策は、機器への指示が機器に届く前に意図的に改ざんされる攻撃を受け、制御の競合が発生させられる場合にも、有効に働くと考える。

7. 関連施策（相互接続時の信用度確認に関する実証実験）

本実証実験で想定したシステムの前提としては、個々の分野のシステム内において、各機器の信頼性の確認が適切に行われていることが望ましい。

IoT 機器・システムの信頼性を確認するには、それらが接続される時に、正しい機器であるかどうかを確認でき、設定された条件に従って利用許可を行う機能が必要である。本章では、HEMS[6]などのエネルギーマネジメントシステムに用いられる ECHONET Lite プロトコルにおいて、機器がお互いの信用度（第三者認証の取得有無など）を確認するための機能である機器認証機能を実装して、効果の検証を行なった実証実験の内容について説明する。

7.1. 背景と課題（機器認証の必要性）

エコーネットコンソーシアムでは、HEMS が対象とする機器[7]について認証制度[8]を開始している。この認証制度では、従来の ECHONET Lite プロトコル実装の認証に加え、アプリケーションの動作を機器毎に詳細に規定した仕様をもとに、第三者機関で認証試験や認証業務を実施することで、マルチベンダ間の相互接続性向上を図る認証プログラムを施行している。

この認証を取得する機器が増加することでマルチベンダ間の相互接続性は高まり、エネルギーマネジメントシステムを容易に構築できるようになってきている。

しかし、その一方で、認証を取得せずに、品質に問題のある機器が市場に出現することが懸念されはじめている[9]。認証を取得していない信頼性の低いエネルギー機器コントローラ（以降「コントローラ」）などがシステムにつながることで、異常な制御や間違った制御が行われ、機器の機能不全につながる恐れがある。

また、従来の ECHONET Lite の通信仕様では平文による通信のみ規定されており、セキュリティ強度は下位層の通信インフラ（Wi-Fi や Ethernet など）の設定に依存している。下位層で十分なセキュリティ設定がなされていないと悪意のある第三者による通信内容の盗聴や改ざん、なりすましなどの攻撃を受ける恐れがある。各機器の情報を不正に取得された場合、個人のプライベート情報の漏洩という脅威に加えて、機器の稼働情報など取得したデータを悪用して不在と分かった場合には、システムが設置されている施設に侵入される恐れがある。さらに、各機器を不正に操作されるとエネルギーの浪費による金銭的被害や、最悪の場合、火災などの物理的な被害を生じる危険性がある。

6 HEMS(Home Energy Management System)とは、エネルギー管理システムの 1 つであり（主に家庭を想定）、エネルギーの「見える化」と一元管理を実現する。

7 スマート電力量メータを含む HEMS 重点 8 機器

8 2016 年春より AIF（Application InterFace）認証制度を開始

9 実際に、認証を取得していないスマートフォン向け ECHONET Lite 操作アプリが公開されている例がある。

7.2. 機器認証の目的

前述した課題に対して、悪意のある(あるいは信頼性の低い)コントローラから不正にエネルギーマネジメントシステム内の機器が操作されることを防ぐことにより、負担やダメージを与える悪意ある攻撃から機器を守りたいという要求がある。また、盗聴や、改ざん(なりすまし)による踏み台攻撃といった間接的な問題を防止することが、機器の利用者、製造者のいずれの観点からも要求されつつある。

こうした状況を鑑みて、 エネルギーマネジメントシステム内の機器およびコントローラがお互いの信用度(正規の機器認証を取得しているか否か)をネットワーク上で確認するための機器仕様の策定が進められている。

7.3. 機器認証による対応方針

今回実装した機器認証仕様のシーケンス概要[10] を図 20 に示す。

以下の 3 つのステップで機器を識別し、機器認証済みの機器間のみに通信を制限することを可能にする。

① 機器認証仕様では、利用者が、グループマネージャ(GM)機能を持つコントローラと、グループへ参加する機器のそれぞれに対して、認証開始トリガをかけて機器認証を開始する。これにより、利用者が意図した通信相手とのみ接続し、誤接続を防止する。(操作画面などを持たない機器では、認証開始トリガはボタン押しなどを想定)

② コントローラと機器がお互いの電子証明書を検証することで機器認証を行い[11]、認証に成功すると、認証済の証としてコントローラが機器に対して以降の暗号通信で使用するグループ鍵(共通鍵)を配布する[12]。

③ グループ鍵を用いてメッセージ認証と暗号通信を行うことにより、機器認証済の機器間のみに通信を制限する。(通信内容や送信元の改ざん、成りすまし、盗聴を防止)

証明書を使った機器認証の処理は負荷が大きいが、今回の実装方式では、その処理は上記①、②で実行される。つまり、機器認証の処理は、新たな機器がシステムに接続されて利用が開始されるとき、並びに証明書の（期限切れや失効後の）更新が行われたときにだけ実行され、通常利用の中で機器やコントローラ間で通信が行われるときは③の処理しか実行されない。これにより、機器認証の処理の負荷による影響を低く抑えることが可能となる。

---

10 ECHONET Lite 規格書第 2 部で規定される ECHONET Lite 通信仕様に機器認証機能を追加した通信仕様に関する規定による

11 PANA/EAP-TLS に準拠
［PANA］ Y. Ohba, et.al. Protocol for Carrying Authentication for Network Access (PANA). : RFC 5191, 2008.
［EAP-TLS］ D. Simon, et al. The EAP-TLS Authentication Protocol. :RFC5216, 2008.

12 IEEE802.21m に準拠
［IEEE802.21m］ IEEE. Draft Standard for Local and metropolitan area networks - Part 21: Media Independent Services Framework.: P802.21/D02

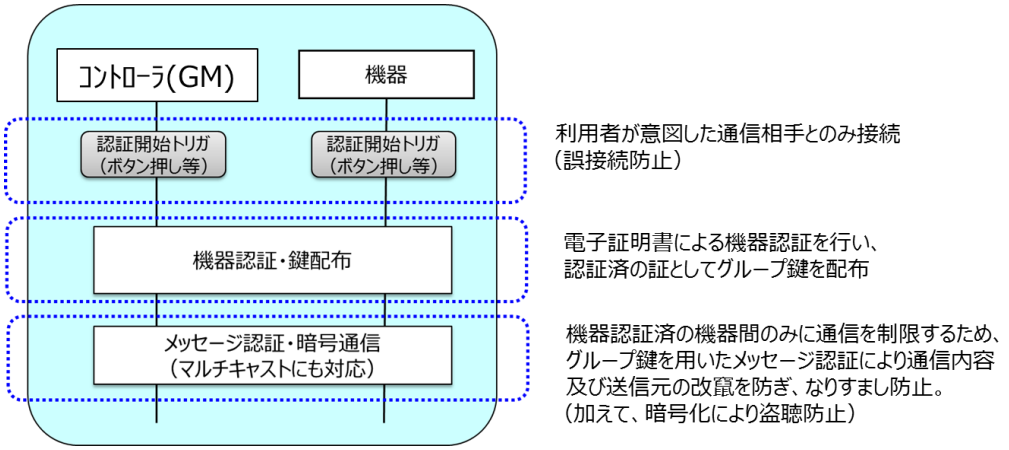

図 20 機器認証仕様のシーケンス概要

7.4. 機器認証の実証実験

7.4.1. 機器接続の制限方法の検討

エネルギーマネジメントシステムにおいて、利用者が意図しない機器が接続されたり、信頼性の低いコントローラが接続されたりする可能性がある。安全・安心にシステムを運用するために、機器認証機能により、信頼性の高い機器のみでシステムを構成したり、信頼性の低い機器やコントローラのアクセスを制限したりすることが可能である。

現在、市場には既に正式な認証を取得した機器が存在しているが、それらの機器は機器認証機能に対応していない。そのため、実際のシステム構成にあたっては、機器認証機能に対応していない従来の機器と機器認証機能に対応した新たな機器とが混在する可能性があり、以下の 4 つの構成パターンが挙げられる。それぞれのパターンでの接続可能な機器を制限する方法を表 3 に示す。

表 3 機器接続の制限の方法

	コントローラ	機器	制限の方法のパターン
システム構成 1	機器認証対応	機器認証対応	機器認証が正常終了した機器は、基本的には接続を許容する
システム構成 2	機器認証対応	機器認証非対応	・コントローラ側は、非対応機器も許容する ・コントローラ側は、ユーザが認めた場合、非対応機器を許容する
システム構成 3	機器認証非対応	機器認証対応	・機器側は、情報取得/通知を受け付けるが、制御は受け付けない ・機器側は、ユーザが許可すれば全ての操作を受け付ける ・機器側は、全ての操作を受け付けない
システム構成 4	機器認証非対応	機器認証非対応	基本的には接続を許容する

7.4.2. 機器認証の実装

コントローラと空調（本章では以降「エアコン」と記載）に実装した機器認証のための処理の動作シーケンスを図 21 に示す。なお、現在想定している実際の運用事例の 1 つである「電子証明書は事前に配布され、工場出荷時に各機器に搭載される」という形態を想定して実装した。

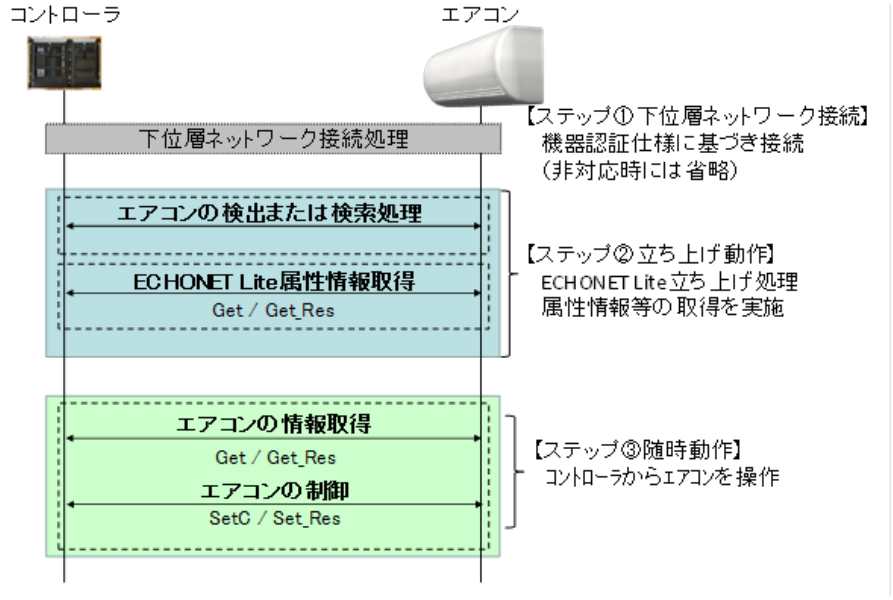

図 21 コントローラとエアコンの標準的な動作シーケンス例

動作シーケンスの各ステップの詳細は以下のとおりである。

ステップ①:

下位層ネットワークとして Ethernet の接続設定を完了させる。続いて、コントローラ、エアコンともに機器認証に対応している場合、認証トリガをかけてグループ鍵の配布を行う。

ステップ②:

下位層ネットワークの接続が完了すると、エアコンから「インスタンスリスト通知」と呼ばれる通知が送信される。インスタンスリスト通知を受けたコントローラは、エアコンを検出し属性情報を取得する。エアコンからインスタンスリスト通知が送信されない場合は、コントローラからエアコンの検索処理を行い、エアコンを見つけると属性情報を取得する。

ステップ③:

コントローラからエアコンに対して、情報取得（動作状態、運転モード設定）した後、制御（運転モード設定：冷房、温度設定値：28℃）を行う。

ここで、コントローラ、エアコンはいずれも PC によるエミュレータである。また、各エミュレータ間は

Ethernet により接続した。

7.4.3. 実験内容

1） 実験ケース 1(表 3 のシステム構成 1 のケース)

本項では、システム構成 1 のケースの検証結果を示す。システム構成 1 では、コントローラ、エアコンともに機器認証対応であるため、検証ステップ①において機器認証によりお互いの接続が許容され、検証ステップ②、③のやり取りが正しく実行されることを図 22 に示すようなパケット解析ツールにより確認した。

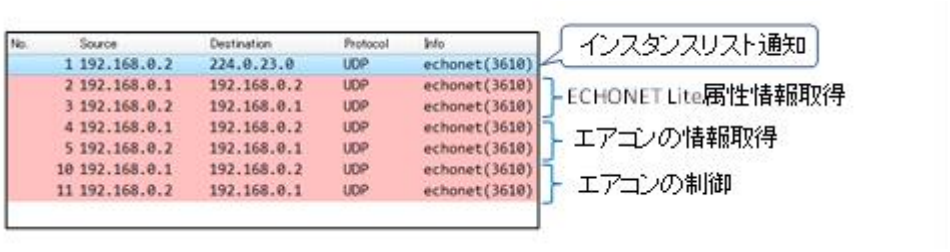

図 22 システム構成 1 のケースにおけるパケット例

また、具体的なパケットの内容は暗号化されているため、図 23 に示すような各エミュレータのログ出力内容により確認した。

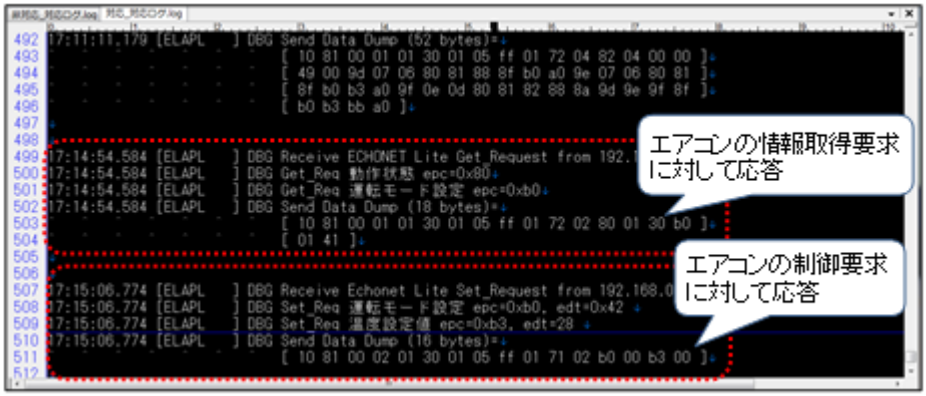

図 23 システム構成のケースにおける通信ログ内容

2） 実験ケース 2(表 3 のシステム構成 2 のケース)

本項では、システム構成 2 のケースの検証結果を示す。システム構成 2 では、コントローラが機器認証対応、エアコンが機器認証非対応であるため、検証ステップ①で下位層ネットワークの接続が完了すると、エアコンから暗号化されていない「インスタンスリスト通知」が送信される。インスタンスリスト通知を受けたコントローラは、機器認証に非対応であることを認識して、図 24 のコンソール画面に示すようにユーザに対して接続可否について問合せが行なわれる。本項の検証では、ユーザが接続を許

可した場合を想定し、検証ステップ②、③のやり取りが正しく実行されることを確認した。

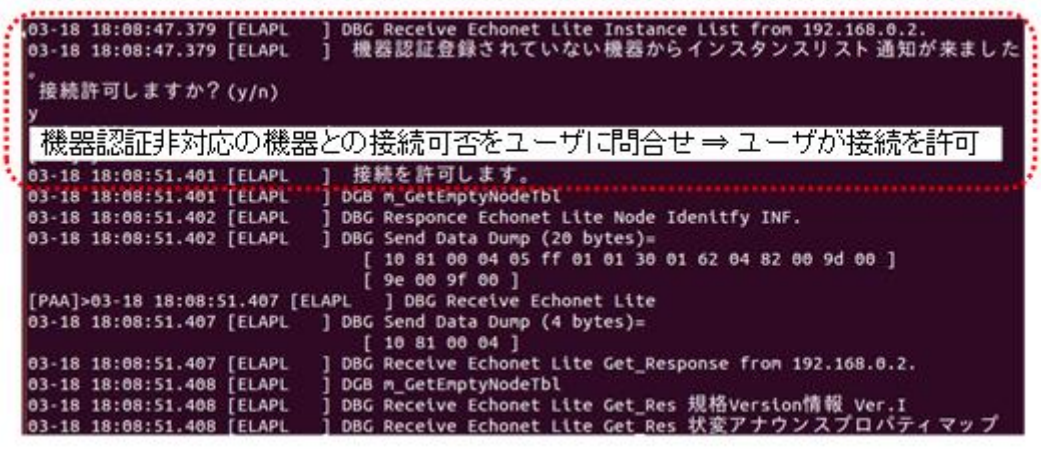

図 24 システム構成 2 のケースにおけるコントローラのコンソール画面

3) 実験ケース 3(表 3 のシステム構成 3 のケース)

本項では、システム構成 3 のケースの検証結果を示す。システム構成 3 では、コントローラが機器認証非対応、エアコンが機器認証対応であり、本検証ではエアコンは情報取得/通知を受け付けるが、制御は受け付けないような実装例を想定した。本検証では、検証ステップ①、②のやり取りが正しく実行されることを確認し、図 25 の通信ログ内容に示すように検証ステップ③においてエアコンは情報取得/通知を受け付けるが、制御は受け付けないことを確認した。

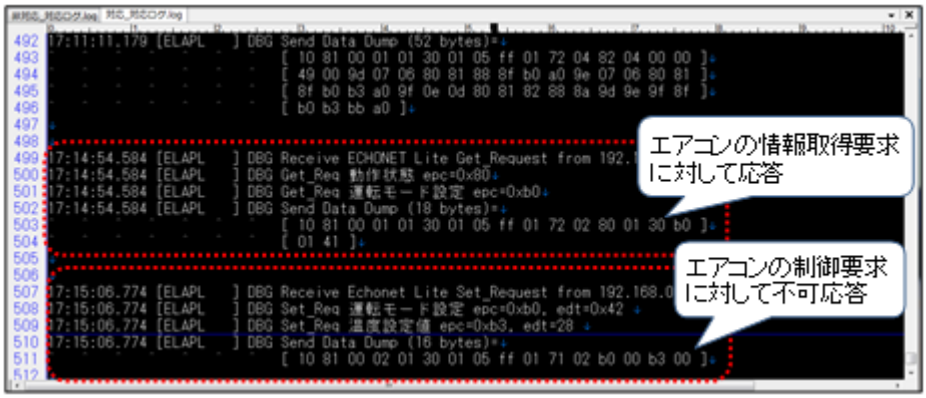

図 25 システム構成 3 のケースにおける通信ログ内容

7.4.4. 評価と考察

本章では、HEMS などのエネルギーマネジメントシステムに用いられる ECHONET Lite プロトコルにおいて、機器がお互いの信用度を確認するための機能である機器認証機能を実装し、機器認証仕様書どおりに動作することを確認した。これにより、仕様策定した機器認証機能の導入により、当初の目的である「第三者認証を取得していない通信信頼性の低い機器やコントローラのアクセスを制限可能であること」を確認できた。

おわりに

「実践に向けた手引き」で記載している IoT 高信頼化の対策のための機能要件について、分野間連携に主眼を置いた異常検知のための機能を検討し、以下の機能についてその実現性と有効性について評価を行った。

１）異常検知の能力の向上

異なる分野の監視情報を連携した異常検知の方式

２）異なるシステムによる制御の競合の検知

分野間の指示の矛盾検出と矛盾により及ぼされる相互の指示への影響の防止

また、関連施策（相互接続時の信用度確認）として機器認証機能の実証実験を行った。

1）では、産業ロボットシステムの監視情報とエネルギーマネジメントシステムの監視情報との間の相関性を示す情報を監視することにより、産業ロボットシステムの異常の兆候（過電流や漏電）を示す状態を検知できることを確認し、また、産業ロボットシステムの制御プログラムだけでなく監視情報も改ざんして監視を妨害するような高度な攻撃に対しても、異常な状態を検知できることを確認した。複数の情報の相関性を異常検知に利用する方式では、近年、複数のシステムの監視情報を蓄積し、機械学習により相関性のある情報の組合せを割り出し、異常検知に利用する方式の例も出ている。個々の異分野連携でどのような相関情報があるか、については、課題として調査・検討が必要である。

2）では、空調に対するパワーオンとパワーオフの矛盾した指示を検知する対策を実装し動作を確認した。その結果、指示の矛盾の発生は人間の感覚では判別しにくいことが分かり、今回のようにソフトウェアにより自動的に検知することの必要性を確認した。一般的には、一見制御の競合が発生していないように見えても、複数の機器やシステムが連携して動作した結果、ある機器やシステムと他の機器やシステムとが互いの効果を打ち消しあうようなケースが起こりうる。また、悪意を持ったものによる攻撃の結果、そのような矛盾した状況が引き起こされる可能性もある。これも本質的には制御の競合であり、早期に検出できることが望ましい。このタイプの制御の競合の実例とその対策を検討していくことが必要であり、今後の課題としたい。

機器認証の実証実験では、HEMS などのエネルギーマネジメントシステムに用いられるプロトコル（ECHONET Lite）において機器認証機能を実装し、第三者認証を取得していない通信信頼性の低い機器やコントローラのアクセスを制限可能であることを確認した。今回作成した機器認証仕様では、ネットワークセキュリティ分野において標準的なプロトコルや暗号アルゴリズムを用いており、オープンソースの活用などにより、ソフトウェアにおいて容易に実装できた。したがって、本章で検証した機器認証の考え方や具体的な方式は他の分野にも応用可能である。

本実証実験報告書が、分野間にまたがる IoT 製品開発時の考慮点を先駆的に示したものとして、「実践に向けた手引き」の活用の一助となり、分野間連携システムの安全安心の向上において産業界への参考になるものと期待する。

謝辞

本実証実験にあたり、ご協力いただいた皆様に心から謝意を表する。

IPA 関係者一同
ORiN 協議会　関係者一同
エコーネットコンソーシアム　関係者一同
神奈川工科大学 HEMS 認証支援センター　関係者一同