産業オートメーションにおける社会的環境変化と対応の現状
～技術革新と求められるセキュリティ～

産業オートメーションと社会的環境変化

橋　本　芳　宏*

＊名古屋工業大学　愛知県名古屋市昭和区御器所町
＊Nagoya Institute of Technology, Gokiso-cho, Showa-ku, Nagoya, Aichi, Japan
＊E-mail: hashimoto.yoshihiro@nitech.ac.jp

キーワード：環境変化 (Environmental Changes)，コロナ禍 (COVID-19)，リモートワーク (Remote work)，産業制御オートメーションシステム (Industrial Control & Automation System)，セキュリティ (Security).
JL 0004/23/6204–0188

1．はじめに

本特集は，COVID-19 の世界的規模での感染により，われわれの生活様式や企業活動などの社会的環境に大きな変化がもたらされていることから，その産業オートメーションへの影響に注目して，今後の計測自動制御のありかたについて考える参考になるようにと 2 年前に企画された．その後，ロシアのウクライナ侵攻が発生し，地政学的リスクも顕在化し，世界的な気候変動に対応するための脱炭素化への取り組みを含む SDGs など，世界的な協調を求められる動きも高まってきている．雇用動向の変化による人手不足，リモートワークの普及による働き方の変革，輸送手段停滞による物流コストの増大，生産縮小による半導体等の素材の不足や価格の高騰，ICT 利用の活性化にともなうサイバーセキュリティリスクの増大などの社会的環境変化が長期化しており，産業オートメーション分野においても新しい事業リスクとして対応を余儀なくされている．

産業オートメーションの分野では，COVID-19 以前から，競争力強化策として IoT，AI，ロボット，ドローンなど新技術の導入がうたわれ，現在は DX としてその活用に取り組んできている．

本特集では，総論にて，近年の社会的環境変化について俯瞰し，解説にて，日本政府が取り組む社会的な変化への展望とその取り組みやデータ流通基盤，サイバーセキュリティの最近の状況，DCS に代わるプロセス制御システムとして期待される Open Process Automation (OPA)，そして感染，防疫対策について紹介いただく．そして，産業オートメーション分野のユーザやベンダから，リモートメンテナンス，リモートエンジニアリング，AI などの技術活用について紹介する．

2．COVID-19 に対する産業オートメーション分野での対応

COVID-19 感染は，ほぼ 3 年経った 2022 年 12 月の時点でも**図 1** に示すように終結しておらず，マスクと手洗い，消毒は習慣化し，入店時等には体温測定をするのは常態化したが，第 8 波の感染拡大とともにインフルエンザの流行が危惧されている．感染者数は 2020 年時点よりも桁違いに多くなっているが，重症化率は低くなり，

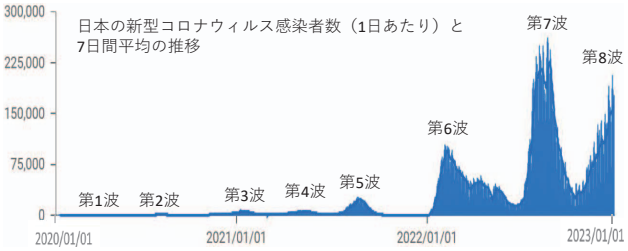

図 1　日本国内の COVID-19 の感染者数の推移

海外からの旅行者の受け入れも行われ，2020 年のように行動制限が発せられることはなくなった．

SICE 安全のための計測・制御・システムを考える会では，第 2 波が収まった 2020 年 11 月から 12 月の期間に，産業オートメーション分野を対象に，COVID-19 への対応に関するアンケート調査を行い，各事業所での感染防止対策，事業継続計画，コロナ禍で進展した or 期待されるリモートなどの技術，さらにサイバーセキュリティへの取り組みを調べた[1]．回答は 45 事業所から得られ，感染対策で工夫している体験など共有すべき情報が多く得られたため，回答者には 2021 年 3 月に集計結果をフィードバックし，6 月に報告書を SICE ホームページに公開した．運転室への他部署の出入りを禁じるなどさまざまな対策が今も継続しており，鉄道や病院などでは，操業現場での感染者の発生によるサービスの停止が発生したが，産業オートメーションの分野では，そのような操業停止は回避されてきている．

スマート保安で取り上げられている AI や IoT などの新技術とともに，従来から取り上げられている自動化などの技術的課題に対する取り組みについては，COVID-19 で特に進んだというより，それまでに取り組んでいたことが，この時期に役立ったという回答が多く寄せられている．リモートによる海外プラントの点検や作業支援も，すでに所有していたモバイル端末やウェアラブルカメラが役立ったという回答があった．

事業継続計画については，すでに国からの要請があった新型インフルエンザに対する対応も未策定であったとの回答が半数以上から寄せられたが，策定していた事業所のすべてからは，マスクの確保など感染防止対策で有効に機能したという回答が得られている．今後も新たな感染症のパンデミックが発生する可能性があり，事業継

続計画策定の浸透が求められる．

サイバーセキュリティに関しては，COVID-19 を機にセキュリティ対策の見直しを行い，サイバー攻撃による安全の破綻を認識したうえで，ホワイトリストなど新たな対策の導入も進んでいるという回答が特に石油，化学を中心とするプロセス産業から多く集まっている．サイバーセキュリティに対する高い意識が認められるアンケート結果であった．

3. COVID-19 による職場環境の変化

COVID-19 の感染対策により，出社や登校が制限され，リモートワーク，オンライン学習を余儀なくされた．産業オートメーションの分野でも，交代勤務の在宅勤務はほとんど検討されていないが，これまで対面が必要と考えられていた検査や作業指示などの業務は，リモートでこなせるように工夫されている．

在宅勤務になれば，出勤，出張の時間も費用も不要になり，オフィスを手放す企業も発生しており，NTT は行動制限が解除されたのちも，全社員，在宅勤務を宣言し，出勤は出張扱いとするとしている．ほかの企業でも在宅が勤務体制として取り入れられ，働き方改革につながっている．さらに，時間基準から成果基準への勤務管理の移行など，労働自体の見直しにもつながり，社会の変革に進展していくことが期待される．

このリモートワークの広がりで，コンピュータシステムにも大きな変化を与えた．社外から社内データへのアクセス量はこれまでとは桁違いに増え，インターネットとのゲートウェイである VPN が対応しきれず，内部で保持していたデータは，一挙にクラウドに移行し，会議も講義も接続先はクラウド，文書の編集も個々の PC 内部ではなく，クラウドを利用するのが一般的になった．

4. データは戦略物資

自然言語処理の AI は高度化し，世界各国の音声の聞き取り，翻訳，音声合成が身近になり，医療画像の診断も人間を上まわる性能を発揮するようになっているのも大量のデータを集められる結果である．

GAFAM というプラントフォーマへのデータ集中が問題にされ，プラットフォーマが管理する Web2.0 からブロックチェーン技術を駆使した分散型インターネット Web3.0 への移行が話題になっているが，その観点での産業オートメーション分野での変化は，まだ見えない．

データを取り扱う上で，プライバシーとセキュリティは重要で，EU の GDRP (General Data Protection Regulation) では，データ主体の権利を侵害する行為や，域外移転の手続に反する行為に対しては，2000 万ユーロ以下か，全世界の年間総売上の 4%以下の，いずれか高いほうの金額の制裁金が科されることになっている．また，個人データの侵害があった場合に 72 時間以内に監督機関に通知しなかった場合や，個人データの取扱活動の記録を残さなかった場合など GDPR の手続違反に関する行為に対しては，1000 万ユーロ以下か，全世界の年間総売上の 2%以下の，いずれか高いほうの金額の制裁金が科される．Google が 5000 万ユーロ（約 60 億円），顧客 50 万人の個人データを流出させた British Airways は 1 億 8300 万ポンド（約 246 億円）など高額な支払いを請求されている．

EU は現在 GAIA-X という分散型データ連携の仕組みを推進しており，各拠点のデバイスと各社のクラウドが，IDS コネクターを介して通信し，法令やデータ利用契約の開示条件に従って，アクセス可否を制御する．特定のデータを特定の相手と特定の期間，安全・確実に共有し活用することをめざしている．航空業界や自動車業界での取り組みが進んでいて，特に電気自動車用のバッテリーは個別番号をもち，原料の採掘から製造・輸送，運用，リユース，リサイクルまで CO_2 排出量が管理されなければならないという EU バッテリー規制（2026 年施行）に対応できるように，リチウムの大量供給国である中国とも組んで，GAIA-X の枠組みでデータを集約できるシステムを構築している．プロセス産業でもセパレータやさまざまな部材を提供しているが，品質が良くても，セキュリティを担保したこのようなシステムでデータを共有することに対応できなければ市場に参加できなくなると考えられる．データの管理がビジネスに大きな影響を及ぼすことを強く意識すべきであろう．

5. セキュリティ管理体制の重要性

サイバーセキュリティに関しては，2021 年 5 月に発令されたゼロトラストと SBOM (Software Bill of Materials) に言及した米国大統領令も重要である．攻撃が巧妙化し，パスワードを搾取され水際防御を突破されるなど，信頼できるゾーンは確保できないという発想のもと多要素認証を導入するなどの対応を要求するのがゼロトラストで，リモートワークの進展とともに，その必要性が高まっている．制御システムネットワークでは，緊急時の対応の阻害になることを危惧し，パスワードすら利用しない体制が一般的であるが，水際で守り切ることは困難になっていることを意識すべきである．

最近のシステムは，できるだけ独自のコーディングを避け，共通のモジュールを組み合わせて開発されるが，システムにどのようなモジュールが利用されているかを示すのが SBOM である．常に新たなサイバー攻撃が生まれ，開発者の配慮不足だけでなく，サイバー攻撃者の発明品ともいうべき脆弱性が 1 年に 18000 件以上報告されていて，その脆弱性をついたマルウェアは年間 1 億種類以上現われている．OpenSSL のようなセキュリティのためのモジュールにも脆弱性が報告されており，セキュア開発をしても，脆弱性を完全に排除することは不可能で

あると考えるべきである．そのため，製品自体がセキュアであるためには，脆弱性の発生を検知し，即座にパッチをあてるという運用が不可欠である．出荷時にセキュアであることも必要ではあるが，運用が伴わなければセキュアな製品とは評価できない．

SBOMは，ライフサイクルにわたって脆弱性を管理する重要な情報になる．産業オートメーション分野のベンダは製品へのサイバー攻撃が安全の破綻にもつながるので，出荷後の脆弱性管理が重要であり，内部モジュールの管理も責任をもたなければならない．組込みシステムでは利用するセンサなどのモジュールについてもSBOMを管理する必要があるが，管理できないモジュールを利用せざるを得ないときには，たとえそのモジュールに危険な脆弱性が発生しても，周りのシステムで安全を確保するなどの対応も検討する必要があると考えられる．SBOMの徹底は，既存のシステムをつなぐことで新たな価値を創造するSoS (System of Systems) の世界では，それぞれの脆弱性管理の責任分担を明確するのに重要なものになるとも考えられる．

6. 産業制御システムの新たな動き

産業制御システムの新たな動きとしてOPA (Open Process Automation) を本特集で解説いただく．これは，1975年からHoneywellとともに，DCSによるコンソールオペレーションを推進してきたExxonMobilがDCSに代わる次世代の制御システムとして提唱しているものであり，技術的には，ネットワーク技術や仮想環境技術など，最新のDCSでも可能なものではあるが，重要なのはOpenであることで，マルチベンダによる高度化の進展が期待されている．しかし，トラブル時の責任の問題は，マルチベンダになるとやっかいになる．これまで，制御ベンダによる「責任をもてません」という発言で，ユーザが手出しできなくなっていた問題もあったが，ExxonMobilという大企業が推進することで，そこにブレークスルーがうまれることを期待している．

7. セキュリティと企業の信頼性

デバイスやシステムは，購入時にセキュアであるだけでなく，その後に発現する脆弱性への対応も要求されるはずである．そのため，購入後もそのような対応をしてくれると信頼できる企業であることが，提供する側のビジネスにとって重要であり，それを明確に示すことが求められるようになると考えられる．デバイスやシステムを開発する立場としては，SBOMへの対応がその1つの組織的対応となる．システムを運用する立場としては，インシデント発生に対する対応が重要な要素であり，セキュリティ対策をしっかり推進できる組織となっていることが求められる．特に産業オートメーション分野においては，サイバー攻撃が安全の破綻にも関係するので，安全を担保するにもセキュリティ対策は不可欠である．このための枠組みとして，オバマ大統領の大統領令で作成されたNIST CSF (Cyber Security Framework) がある．経営トップが日々高度化するサイバーセキュリティの最新の知識をもってトップダウンにセキュリティ対策を実践することは困難であり，セキュリティとセーフティの両面の最先端をキャッチアップする中核人材チームがトップとなり，情報システム，生産システムなど全社のセキュリティ対策を指導するとともに，経営者に適切に提案を行い，予算，権限を受けとるという上下のPDCAを推進する体制を構築することが提案されている[2]．そして，Identify（特定），Protect（防御），Detect（検知），Respond（対応），Recover（復旧）の全社員が理解できるであろう5つの用語を用いてセキュリティ対策を推進する．

世界的にセキュリティ人材は不足していて，外部から導入することも容易ではなく，まず，このような体制を主要企業が確保し，そのサプライチェーンの関連企業のセキュリティ対策も向上させるというアプローチも必要であると考える．中核人材としては，IPAやJPCERT/CCなどの外部組織，業種別ISACなどの業界団体との連携も必要である．

IPAでは2017年から産業サイバーセキュリティセンターを設立し，中核人材育成プログラムを推進している．1年間職場を離れて学習プログラムで，それだけの環境を社員に与えられる企業は多くないが，その企業の中核となるとともに，国のセキュリティを支える人材となってくれることを期待した取り組みになっている．

8. 高圧ガス保安法等の改定

スマート保安のさらなる進展を求めて，経済産業省は，高圧ガス保安法，ガス事業法，電気事業法の一部改正を2022年6月に実施した．認定事業所制度を改定し，従来スーパー認定事業所だけであったスマート化の要件を従来の認定事業所に対応するB認定にも加え，従来のスーパー事業所に相当するA認定とB認定の両方にセキュリティに関する要件を加えた．さらに，従来は事故調査を被災企業の自主的な活動としていたものを，「サイバーセキュリティに関する重大な事態が生じた場合等に，経済産業大臣は独立行政法人情報処理推進機構（以下，「IPA」）に対し，原因究明の調査を要請することができることとする.」という項目を加えた．

第2章で，石油・化学産業からのアンケートの回答には，サイバーセキュリティに関する高い意識が認められると書いたが，実際に企業の担当者に聞いた範囲では，制御システムネットワークに通信監視やシステムログの保存を実施している事業所はほとんどないと把握している．どのような形で，調査が必要な重大な事態と判断されるのか，まだうかがいしれない部分が多いが，いざ調査に

入ると，今のままでは，なにも痕跡が残っていないという事態になるのではないかと危惧している．再発防止ができて，初めて復旧したといえるので，原因究明は必要であり，それをささえる情報を確保する体制の整備が早く進むことを祈念する．

9. 経産，消防，厚労3省連絡会議

Cyber Physical Space や Digital Twin の観点で経済産業省は，新たな社会，新たな産業の創出を企画していて，そこでの取り組みの一部を本特集で紹介いただく．従来の自動化をより進めるものとして，ロボットやドローンの存在も大きい．建設の現場ではすでにロボットでの巡回点検も実用化されていて，防爆のロボットも開発されている．産業オートメーション分野では従来からマニピュレーター型ロボットが多く導入されているが，さらに，人の代替になる高度なロボットも期待される．また，高所の点検や消防時の把握などに有効なドローンについては，経済産業省，総務省消防庁，厚生労働省の3省連絡会議により，防爆管理区域の見直しがなされるなど，活用推進がはかられている．安全のための規制はなかなか見直しが進まず，海外では防爆認定されていても国内では利用できないという状況が続いているが，このドローン活用を発端として，防爆規制も見直しが進むことを期待している．

また，この3省連絡会議では，プラント保安分野 AI 信頼性評価ガイドラインも開発している．このガイドラインの特徴は，AI の信頼性を評価するだけなく，たとえ AI が異常なふるまいをしたとしても，安全を担保する保護を設置して，AI を適用するというアプローチを示していることである．すべてを把握できない場合でも，便利なものを安全に利用するための発想として，世界にも広げたいガイドラインであると考える．

10. COVID-19 による教育環境の変化

筆者が大学教官であり，本原稿が学会誌への寄稿であることから，最後に教育環境についても触れたい．

感染防止のため，学校の講義は，リモートになった．通学をしなくても，なんとか学習がこなせるという世界が否応なく実現された．小学生も各自，PC かタブレットを所有し，e-learning が可能な環境がいっきに広がった．

この環境変化は大きなチャンスであり，感染がおさまったら従来の対面に戻すというのではなく，大学も含め，教師による講義というものを根本的に見直すべきであると考える．せっかく全国で作成されたリモート用の講義は見直されることもなく，なかったことにされるのであろうか．基礎的な内容の講義は優れたオンデマンドに委ね，対面の教師は理解度に合わせた支援に専念するというのも検討できる環境になったのではなかろうか．

高校の学習が大学受験のためのものになっているという問題はこの環境でも変えがたい課題かもしれないが，入学後の大学の変革は検討できるはずである．最先端の仕事をする企業もリモートワークとなっており，新入社員がその仕事をこなせるように，最新のさまざまなツールは便利で利用するだけなら動画検索でマスターできてしまうものになっている．3D プリンタや AI，IoT，データ処理などのツールは，必ずしも高価ではなく，自由にアクセスできる環境を与えれば，教師が細かく教えなくても，学生の興味で最先端の世界を体験できる．創造性は，うまくいかないからなんとかしようと考えて育まれるものであり，こうすればうまくいくということは，できないことを経験することで価値がわかる．3D アニメのゲームでも，その作成ツールに触れることでつくるほうにも興味がわき，学習意欲が刺激されるかもしれない．これを知ってからこれをという積み立て型の教育も必要ではあるが，最先端はさまざまな方向にはるか高いところにあり，めざすまえに歩みを止めたくなるのでは危惧する．若者の創造性を高める教育を志向して，教官自体がこれまでの教育を見直す貴重な機会が今ではなかろうか．

（2022 年 12 月 27 日受付）

参 考 文 献

1） 新型コロナウィルス禍における操業現場の対応に関するアンケート報告書，https://www.sice.jp/info/info_press/press_20210623.html
2） 橋本芳宏：制御技術者にとってのサイバーセキュリティ，計測と制御，**61**–12, 921/922 (2022)

［著 者 紹 介］

橋本芳宏（はしもとよしひろ）君（正会員）

1985 年京都大学大学院化学工学専攻博士課程（単位取得退学）．1985 年名古屋工業大学生産システム工学科助手．学内組織再編を経て，現在にいたる．2010 年～計測自動制御学会プロセス塾講師．2017 年～IPA 産業サイバーセキュリティセンター講師．最近は主に制御システムセキュリティの研究に従事している．