

3.11 CPS/IoT

CPS（サイバーフィジカルシステム、Cyber Physical Systems）とは、ネットワーク化されたコンピューティングによる処理と物理的な要素が統合されたものを指す。実世界や人間から得られるデータを収集・処理・活用し、社会インフラの効率化、新産業の育成、知的生産性の向上などに資すると期待されている。一方、似た概念としてIoT（Internet of Things）がある。これは、パソコンやサーバー、携帯電話などの情報・通信機器だけでなく、家電製品や自動車、機械など、様々なモノに通信機能を持たせ、インターネットに接続し、モノの制御や周囲の状況の計測などを行うことである。人、モノ、コンピューターなどが有機的に結合することによって、社会、経済、産業の効率化と付加価値の向上を実現する。

CPS/IoT が社会に与える影響は、PLC（Programmable Logic Controller）が社会に与えた影響と同じように考えることができる。PLC が登場したことより、製造過程の自動化が進み、生産性の格段の向上につながった。

同じように、CPS/IoT は、すべての産業セグメントの生産性を向上させ、新たな価値を創出する分野であり、成長戦略の一丁目一番地とも言える領域である。Industrial Internet を推進している米国のGE社によると、CPS/IoT は2030年に世界のGDPを約15兆ドル押し上げるとのことである。ドイツが製造業の復活を期して進めているIndustrie 4.0は、製造業に特化したCPS/IoTである。

CPS/IoTにより、生産性が相対的に低いと言われている我が国の多くの産業セグメントにおいても生産性向上につなげることが期待できる。

CPS/IoT はすべての産業セグメントに関わる。適用領域を考慮せずにCPS/IoTの研究開発を進めることはできない。このため、CPS/IoT分野を俯瞰するにあたっては、社会という視点を盛り込みながら、「アーキテクチャー」「M2M」「社会システムデザイン」「IoTセキュリティ」「応用と社会インパクト」「ものづくりとIoT」に分類した。

「CPS/IoTアーキテクチャー」は、クルマの運転支援や高速デマンドレスポンスなどといったリアルタイムかつ低遅延な性能が求められるアプリケーションやサービスが登場してくることを踏まえ、新たに必要となるコンピューティング/ネットワーク/ストレージアーキテクチャーである。

「M2M」は、センサーなどのモノからデータを収集するネットワーク基盤である。センサーネットワーク、膨大な数のノード管理機構、シグナリングトラフィックを削減する仕組みなど、多角的に検討を進めながら、フィールドへの展開を進めていかなければいけない。

「社会システムデザイン」は、CPS/IoTならではの領域であり、CPS/IoTを支える技術を用いて社会をデザインしていくことを目的とする。このためには、社会で何が求められているのかをフィールド指向で把握した上で、技術課題に落とし込んでいく研究アプローチが必要である。

「CPS/IoTセキュリティ」は、膨大な数のモノがネットワークにつながる世界において切り離して考えることのできない重要な領域である。CPS/IoTにおいてネットワークに接続されるノードの資源には制約があることも踏まえた上で、かつアプリケーション/サービスの特性をも踏まえた上で、セキュリティを考えていかなければならない。

「応用と社会インパクト」は、CPS/IoTの具体的な適用領域に軸足を置きながら研究開発を進める「フィールド指向型研究開発」である。CPS/IoTの適用領域は、環境、エネルギー、医療、ヘルスケア、農業、防災などすべての産業セグメントにわたる。IT/ICT研究者がそれぞれの産業セグメントのフィールドに出向いて、課題やニーズを抽出しながら研究開発を行う領域である。

「ものづくりとIoT」は、昨今の製造業に対する期待の高まりに応じて、スマートな製造業を実現するための領域である。ドイツのIndustrie 4.0をはじめとして、米国においても雇用の観点からものづくりの重要性が強烈に意識され始めている。ものづくりに強い我が国の強みを発揮できる領域である。

生産性を高め付加価値を創出できるCPS/IoTは、製造業に強いことからわかるように、我が国に優位性があると考えられることのできる領域である。しかしながら、従来の研究領域と異なり、CPS/IoTを推進していくためには、多様なプレーヤーの参画の促進、基礎技術から実用化につなげるリニアモデルではなく社会課題から技術課題につなげるトップダウン型の研究開発、ビジネスとして成立させることが可能なエコシステムの考案など、従来型の研究開発と異なる推進方策が求められる。

具体的には、多様なプレーヤーが参画するアンブレラプロジェクト、地域それぞれにニーズが存在することから地方大学や高専などをネットワークさせるプロジェクト、ハッカソンやアイデアソンなどといったイベントを介して多様なアイデアを吸い上げるプロジェクト、新たなエコシステムをもあわせて考えるプロジェクト、市場創出ということを前面に押し出したプロジェクトなど、従来とは異なる新たな形態のプロジェクトも必要となる。



図 3.11.1 CPS/IoT の俯瞰図

【重要な研究開発領域】

- ・ 物理世界とサイバー世界をつなぐ M2M と、安全性を担保するセキュリティー
- ・ 社会と IT をつなぐ IoT アーキテクチャーと社会システムデザイン
- ・ 実世界への適用を進める応用開発とそのインパクト評価、特に製造業への影響

3.11.1 CPS/IoTアーキテクチャー

(1) 研究開発領域名

CPS/IoT アーキテクチャー

(2) 研究開発領域の簡潔な説明

CPS/IoT は、自動車、エネルギー（スマートグリッド）、環境、防災、農業、土木、物流などさまざまな分野に適用される。膨大な数のセンサーがネットワークに接続される世界であり、従来のコンピューティング/ネットワーキング/ストレージパラダイムではサポートされない新たな要求が出現される。これらの新たな要求に対処するパラダイムが CPS/IoT アーキテクチャーである。

(3) 研究開発領域の詳細な説明と国内外の動向

Cyber Physical Systems (CPS)、 Internet of Things (IoT)、 M2M (Machine-to-machine)などと呼ばれる言葉は、従来の PC やスマートフォン以外のモノがネットワークに接続される世界を示している。クルマがネットワークに接続される Connected Vehicle、スマートグリッドにおける高速デマンドレスポンス(Fast DR)、橋梁などの社会インフラモニタリングなど、多様なアプリケーション/サービスが出現する世界である。センサーやクルマなどといった新しいモノがネットワークに接続されることで、以下に示すような新たな要件が出現する。

【エッジコンピューティング】

膨大な数のモノがネットワークに接続されるようになると、クラウドコンピューティングでは遅延や性能の観点で対応することが難しくなる。モノがクラウドに接続される形態に加えて、「エッジ」に機能追加することが必要となる。

例えば、スマートグリッドにおける高速デマンドレスポンスでは、数秒オーダーの速度で需要側に設置されたスマートメーターと需給調整を行うことが必要となる。膨大な数のスマートメーターからデータを収集して、需給調整方法を計算し、需給側に対して制御を行うことを考えると、集中管理のクラウドでは遅延の制約を満たすことが難しくなる。「エッジ」と「クラウド」が連携しながら処理を行う仕組みが必要となる。

また、Connected Vehicle においても同様である。安全・安心を実現するためには、クルマと歩行者との間での連携も必要となるが、このためには物理的なネットワーク遅延を極限まで小さくしなければいけない。また、信号機の制御を動的に行うためにも、局所的なクルマの位置を把握した上で、信号機間での自律分散制御が求められる。

現在の CPS/IoT の研究開発は、手元にある技術の延長線上でどのようなアプリケーション/サービスを実現することができるのかを主目的としたものが多く、エッジコンピューティングの研究開発まで踏み込んでいるものはほとんどない。しかしながら、CPS/IoT では、アプリケーションやサービスを見据えながら研究開発を進めていくことが必須であり、現在の研究開発の次のフェーズにおいてはエッジコンピューティング的な視点を考慮する必要がある。

【ストリームコンピューティング】

CPS/IoTの世界では、リアルタイム／オンライン処理が求められる。現在でも、ツイートをリアルタイムに処理・分析することが行われているが、CPS/IoTの世界では多様なセンサーからストリームデータがエッジ／クラウドに流れ込んでくることになり、今まで以上にストリームコンピューティングに頼らざるを得なくなる。

例えば、防災向けでは、人の位置データや雨量、水位、風量、気圧などの環境データに基づいてリアルタイムに避難指示を出さなければいけない。また、渋滞制御においても、クルマの位置データと現在の道路状況を勘案してリアルタイムに信号機などの制御につなげていかなければならない。さらに、公共映像監視にしても、危険人物の素早い検知が求められる。原子力発電所や新生児病棟などでの異常検知も、敷地内や病院内に張り巡らせた多様なセンサーからのデータに基づき迅速に異常を検知しなければならない。

大規模データ蓄積においては Hadoop など、バッチ機械学習においては Mahout など、米国が先陣を切って開発をしてきた。これに対して、ストリームコンピューティングが視野に入ると、ストリーム処理、分散機械学習、オンライン機械学習など新たな軸での研究開発が必要になる。

現在のビッグデータ処理基盤は Google などをはじめとした米国の独壇場と言わざるを得ないものの、ストリームコンピューティングはこれからの研究開発であり、米国以外の国々も同じ土俵で戦うことができる分野である。

【自律分散協調】

CPS/IoT には、膨大なモノが自律分散協調で動作するアプリケーションやサービスもある。信号機制御、高速デマンドレスポンス、車々間通信、複数ドローンでの協調監視、センサーノード協調によるノード省電力化など、自律分散協調が必要となる場面は増加する。

自律分散協調に関しては、理論的には人工知能やエージェント分野などで以前から研究が進められてきた。今後は、既に得られている視点を活用して、具体的な出口に展開することが求められる。現場（フィールド）で何が求められているのかをしっかりと把握した上で、自律分散協調に求められている要件を明らかにしながら研究開発を進めていくことが求められる。

自律分散協調は、人工知能やエージェントの分野に限定されるものではない。CPS/IoT では、ネットワークにおいても自律分散協調が必要となる。例えば、火山監視や山火事監視など人の手が届かないエリアにおいては、センサーノード自身が自律分散協調機能を有し、トラフィック管理や故障管理などを自律的に行わなければならない。今まで、ネットワークはアプリケーションとは個別に議論されてきた。しかしながら、CPS/IoT におけるネットワークは、アプリケーション／サービスとは独立に議論することができない。要件自体が多様になるためである。アプリケーション／サービスで求められる要件を把握しながら、具体的な自律分散協調機能を明らかにし、ネットワーク研究開発を進めていくことが求められる。

（４）科学技術的・政策的課題

- ・ CPS/IoT アーキテクチャーの研究開発において重要なことは、出口となるアプリケーションやサービスをしっかりと把握した上で、どのような要件が求められるのかを明確にする

ことにある。これを経ずして構築したアーキテクチャーは机上の空論になってしまう。そのため、出口となるアプリケーションやサービスに出向く「フィールド指向」を推進することが必須である。

- コンピューティング、ネットワーク、ストレージと、多岐にわたる分野を考えていくことも必要である。そのため、プロジェクト組成においては、アーキテクチャーのレイヤーにとどまらず、「アンブレラプロジェクト」など幅広いレイヤーからの参画を促し、レイヤー間での情報の流れを滑らかにすることが望ましい。
- アーキテクチャーの有用性を明らかにするためには、「データ収集」を避けて考えることはできない。データがなければ、評価さえ何もできないためである。データの収集には膨大な投資が必要となることや、ニーズが明確ではない状態で模索的にデータを収集することが必要となるため、政策的な支援が必須である。
- 地方には生産性の低い産業セグメントが多く、CPS/IoT が果たすべき役割は極めて高い。そのため、研究開発推進においては、地方大学や高専などをも巻き込みながらプロジェクトデザインしていくことも効果的である。

（５）注目動向（新たな知見や新技術の創出、大規模プロジェクトの動向など）

• NSF Cyber-Physical Systems

2006年からNSFはCPSに継続的に財政支援を行っている¹⁾。2015年1月に発出された新しいプログラムでは、「Breakthrough projects」（基礎研究）：\$500,000/3年、「Synergy projects」（学際研究）：\$500,001～\$1,000,000/3～4年、「Frontier projects」（大規模研究）：\$1,000,001～\$7,000,000/4～5年の3つに分けて募集をかけている。分野としては、System design、System verification、real-time control and adaptation、Manufacturing、Smart cities、IoTなどのキーワードが挙げられている²⁾。

• NSF Cyber-Innovation for Sustainability Science and Engineering (CyberSEES)

NSFは2014年に、持続可能性をテーマにしたプログラムを開始した³⁾。「持続可能性」をテーマにしているが、プログラムの実態は「社会課題型のCPS/IoTプログラム」であり、Large-scale Data Analysis and Management、Robust Observation, Sensing, and Inference、Modeling of Complex Systems、Dynamic and Intelligent Decision Making、Control and Management of Infrastructureをテーマとして挙げている。

• NSF Cyber Physical Systems Virtual Organization⁴⁾

CPS研究を推進するための産官学の「集まる場」。CPS/IoTの推進にあたっては、いろいろなバックグラウンドを有する人たちが有機的に連携することが重要であり、このような「場」の提供の仕方は参考になる。

• DARPA Cyber Physical Systems

2014-2014のAdaptive Vehicle Make programや2012-2017のHigh Assurance Cyber Military Systemsなど、CPS/IoT関連のプログラムを継続して推進している。

• Industrie 4.0

ドイツでは製造業の産業競争力強化を目指して、Industrie4.0が推進されている。Industrie4.0は生産から小売りまでのすべてのフェーズから得られるデータを活用して生

産性向上を図ることを目的とした意欲的なプロジェクトである。

- Industrial Internet

米国 GE 社が製造業の将来のあり方を示したビジョンであり、コンソーシアムを構成して、Industrial Internet を推進している。

- EU

EU においても、CPS/IoT は重要テーマとして認識されており、Digital Agenda においても強調されており、さまざまなプロジェクトが進められている⁵⁾。

（6）キーワード

Cyber Physical Systems、モノのインターネット、M2M、ビッグデータ、データ駆動型経済

（7）国際比較

国・地域	フェーズ	現状	トレンド	各国の状況、評価の際に参考にした根拠など
日本	基礎研究	○	→	世界に伍する能力を有するベンチャー企業等のアクティビティが上昇している。
	応用研究・開発	○	↑	産業界を中心に、研究・開発が活発になっている。
	産業化	○	↑	産業界を中心に、研究・開発が活発になっている。ただ、個別企業での取り組みにとどまっており、業界全体としての取り組みはこれから。
米国	基礎研究	◎	→	DARPA、NSFの支援により、大学や公的機関での研究成果が蓄積されつつある。
	応用研究・開発	◎	↑	産業界を中心に、官と学を巻き込んだ動きが活発である。
	産業化	○	↑	GEやシスコなど、大きなビジョンを掲げ、エコシステムを構築し、実ビジネスにつなげる動きが活発になりつつある。
欧州	基礎研究	○	→	EUのプロジェクトが継続的に支援している。ただ、日本、米国と比べ産業界側の動きが弱い（ドイツを除く）
	応用研究・開発	○	↑	EUプロジェクトを中心に、産学でさまざまな動きがなされている。ただ、ビジネスにつながるような動きには結びついていない（ドイツを除く）
	産業化	△	↑	EUプロジェクト以外に大きな動きはみられない（ドイツを除く）
中国	基礎研究	△	→	物連網など、トップダウンのプロジェクトに大きな予算が投下されているものの、大きな成果は見えない
	応用研究・開発	△	→	相対的に近視眼的なテーマが多い
	産業化	△	→	産業界が弱いこともあり、大きな動きは見えない
韓国	基礎研究	△	→	大学は産業界との接点が弱いこともあり、出口を見据えた基礎研究はこれから。
	応用研究・開発	△	→	スマートシティなどの政府主導のプロジェクトはあるものの、研究開発の視点からの大きな成果は見えない
	産業化	△	→	これから一気に動き始めるように思われる

（8）引用資料

- 1) NSF Cyber Physical Systems, http://www.nsf.gov/funding/pgm_summ.jsp?pims_id=503286
- 2) NSF Cyber Physical Systems, Program Solicitation, http://www.nsf.gov/pubs/2015/nsf15541/nsf15541.htm?WT.mc_id=US-NSF_25&WT.mc_ev=click
- 3) NSF Cyber-Innovation for Sustainability Science and Engineering (CyberSEES), <http://www.nsf.gov/pubs/2014/nsf14531/nsf14531.htm>
- 4) NSF Cyber Physical Systems Virtual Organization, <http://cps-vo.org/>
- 5) EU Digital Agenda for Europa, Cyber Physical Systems, <http://ec.europa.eu/digital-agenda/en/cyber-physical-systems>

3.11.2 M2M

(1) 研究開発領域名

M2M

(2) 研究開発領域の簡潔な説明

M2M 研究開発の目的は、環境、都市、農業、流通、土木、医療といった各種産業構造の变革に向けたエコシステムの構築である。センサーや産業設備からのデータを収集・分析することで、各産業ひいては社会基盤の高度化・高効率化が可能になる。

M2M は Machine-to-Machine の短縮語であり、様々な捉え方や定義がなされている。本節では、M2M を Machine-to-Machine Communication (マシン間通信)として、M2M デバイス(ヒトではなくモノ)が通信ネットワークを介してサービスアプリケーションとの間で双方向の情報を交換するための通信技術を研究開発分野として取り扱う。

(3) 研究開発領域の詳細な説明と国内外の動向

・M2M 通信の特徴と要件

M2M が様々なサービスや産業においてビジネスとして機能するには、M2M デバイスが通信ネットワークを介し、クラウド上のサービスアプリケーションとの間で双方向情報をやりとりするための条件を提供することが不可欠となる。その関係を仲介するために通信ネットワークが重要な役割を担っている。

M2M 通信の特徴は、将来予想される膨大な端末数と、多様なサービスアプリケーションの利用形態、そして厳しいコスト環境にある。欧米通信機器ベンダの予測では、2020 年の M2M デバイス数は、500 億端末まで増加するとも見込まれている。従来、M2M の用途としては各種センサーを用いた情報収集系が主体であったが、Cyber Physical Systems (CPS) や拡張現実 (Augmented Reality)の動向にもみられるように、より即時性が求められる制御 (アクチュエーター)系にまでその応用が拡大していく可能性がある。

M2M では、サービスアプリケーションごとに設置場所やモビリティ、消費電力などが多様であり、M2M に適したネットワークの要件も多様である¹⁾。従来の人による通信の場合は、電話、メール、動画視聴などランダムに数 Kbps~数十 Mbps の大容量通信トラヒックが発生するのに対し、モノによる通信、特にセンサーを用いる情報収集系においては数十~数百 Kbps と、必ずしも大容量を必要としないものが多い。一方、機械的に定期間隔で通信を発生させるなど、M2M 特有のトラヒック特性を特徴としている。

・M2M のアーキテクチャー

M2M のアーキテクチャーは、M2M アプリケーション、M2M プラットフォーム、M2M ネットワーク、M2M デバイスの4層構造として考えることができる²⁾。M2M アプリケーションは、個々の M2M サービスに対応して、クラウド上のアプリケーションサーバー上で動作するソフトウェアとして実装される。M2M プラットフォームは、複数アプリケーションが様々なネットワークを介してデバイスと接続するための共通基盤機能を提供する。M2M ネットワークとしては、移動網 (GSM、3G、LTE、WiMAX 等)や固定網 (FTTH、DSL 等)に代表される広域公衆網や、さらにゲートウェイ機器を介して接続される自営系ローカルネットワーク (WiFi、ZigBee、Bluetooth、Z-wave、PLC 等)が利用され、さらにセンサーや

アクチュエーター群に対応する M2M デバイスへと接続される。

・M2M ネットワーク技術

現在の M2M ソリューションでは、固定網よりも移動網を活用したものが多い。これは、M2M サービス構築に移動網の既存機能を、容易に活用できるためである。例えば、SIM カードを組み込んで移動デバイスとして機能させたり、SIM カードを別途用意する必要のない E-SIM (埋め込み型 SIM) を利用した認証やセキュリティーを利用したりと、既存機能を活用した普及や展開が容易である。特に、M2M においては、携帯電話機能の一つである SMS (ショートメッセージ) を用いたサービスが主流である。第 2 世代 (GSM) や第 3 世代携帯電話はほぼ世界中をサービスエリアとしてカバーしており、グローバルなサービス展開が可能である。M2M 通信モジュールの価格も 20US\$ を切る価格帯となっており、今後 LTE モジュールの低価格化も進むと考えられる。

一方で、M2M 端末の移動網への直収は、エンドーエンド間での接続コストに課題があり、移動網の最適化が課題となる。既存の通信ネットワークは無数のデバイスが少量のデータ通信を行うことを想定しておらず、例えば移動しない M2M 端末に対しては、ユーザーデータよりもシグナリングの増大が問題となる。そこで、携帯電話の技術仕様を策定する 3GPP においてマシンタイプ通信 (MTC) の検討が進められており、特に制御プレーンを活用したアーキテクチャーやシグナリングなどの検討が活発である。また、M2M の接続遅延時間要求は VoIP などに比べて一桁以上小さいなど、既存の通信ネットワークとは異なる要求条件に基づく最適化が必要になる。従来とは異なる通信トラフィック特性に柔軟かつ低廉に対応するため、移動パケットコア網 (EPC 等) へのネットワーク仮想化技術 (NFV や SDN) の適用などが検討されている。

M2M デバイスは、その通信や処理に関する能力や消費電力等が限定されるため、M2M デバイスとサービスアプリケーションとをゲートウェイで中継する構成も想定される。ゲートウェイ構成により、近傍の複数デバイスを収容し、さらに広域の移動網・固定網に接続することで、通信モジュールのデバイスコスト増大や通信回線費用の削減が期待できる。ゲートウェイより先の自営系ローカルネットワークを総称して M2M エリアネットワークと呼ぶ。Wi-Fi、ZigBee、Bluetooth、Z-wave、PLC、特定小電力無線等が代表的な M2M エリアネットワークである⁵⁾。これらは、サーバーからの設定変更や監視を行う遠隔管理機能を想定しておらず相互互換性もない。そこで、OMA-DM (主に移動網端末) や TR-069 (主にホームゲートウェイ向け) などの遠隔管理プロトコルを適用し、ゲートウェイでのプロトコル変換を組み合わせ、M2M アプリケーション-M2M デバイス間のエンドーエンド間通信を実現している。

・M2M プラットフォーム技術

従来の M2M サービス (ソリューション) は、サービス事業者が既存の広域通信インフラ等を活用し、個別のサービスアプリケーションに特化したシステム構築を行う垂直統合型の M2M であった。しかし垂直統合型 M2M は、他の産業とは分離された垂直統合型のアプリケーションとして開発され、相互運用性については殆ど考慮されていない。よってシステム構築にコストを要し、複数サービス間での相互連携や複数のアクセスネットワークの切り替え、ソフトウェア共用・再利用が困難である。そこで、様々な M2M サービスを単一プラットフォームに集約するアプリケーションの水平統合と、既に上述した様々な M2M ネットワ

ークを集約するネットワークの水平統合とを実現するため、アプリケーションとネットワークとの間にミドルウェアが必要となる⁴⁾。これを M2M プラットフォームと呼ぶ。各サービスアプリケーションは、M2M プラットフォームが API として提供する共通プラットフォーム機能を利用し、M2M デバイスからの情報収集や制御を容易に行うことができる。かつて ETSI (欧州電気通信標準化機構)にて上位サービスレイヤーの M2M サービスプラットフォーム標準化が先行して行われてきたが、現在は日米欧中韓が参加する oneM2M (3GPP 同様のパートナーシッププロジェクト)において、標準化が引き継がれており、2015 年 1 月に初版仕様がリリースされた。

・M2M セキュリティー技術

M2M サービスアプリケーションでは、例えば eHealth やスマートグリッドのように安全性が重要で、多数のセキュリティーに関する脅威に対して堅牢である必要がある。M2M ネットワークは、時に低消費電力&高パケット損失ネットワーク (LLN: Low Power and Lossy Network)としての特徴を備える。インターネット関連技術の標準化を行う IETF では、DTLS (Datagram Transport Layer Security)の検討が行われている。インターネット上で安全に個人情報やクレジットカード番号などを送受信する技術として TLS が知られるが、TLS は信頼性が確保されたパケットを対象にした技術であり、データグラム(着信確認などを行わず信頼性より転送速度を優先した分割データ)に対しては適用が困難である。そのため、TLS の仕組みを一部変更し、データグラムでも実質的に TLS と同じような安全性確保を目指した技術開発が行われている。

・各国の M2M 技術開発の動向

各国とも、M2M 通信ネットワークが国の将来にとって重要なインフラであり、特に国家産業活性化の観点から、M2M/IoT に関する技術開発の重要性を認知している。米国オバマ政権によるスマートグリッド提唱や NIST(国立標準技術研究所)を中心とした研究開発・標準技術検討、欧州の欧州委員会によるスマートメータや e-Call 義務化に関する欧州指令の発令やフレームワークプログラムの実施、日本でも各省庁の M2M/IoT 関連の様々な研究開発プロジェクトに資金が投入されている。

【米国】国の科学技術推進施策である「ネットワーキング及び情報通信技術開発(NITRD)計画」に基づき、各省庁・機関が連携してプロジェクトを実施している¹⁾。特に M2M アプリケーションの一つであるスマートグリッドを取り組みとして掲げており、NIST(国立標準技術研究所)、NSF(国立科学財団)等の取り組みとして、スマートグリッドのセキュリティーや相互接続・運用に関する研究開発・標準化に取り組んでいる。

【欧州】欧州委員会が、スマートメータや電気自動車の充電、e-Call 等に関する標準化指令を発出している¹⁾。また、2009 年には Internet of Things (IoT)行動計画を発表し、IoT を健康、環境、交通等の社会的課題を解決する手段と位置づけて検討を行っている。また、欧州委員会の研究開発助成プログラムである第 7 次フレームワークプログラム (FP7) では、RFID や IoT に関わる研究開発プロジェクトを多数実施し、スマートシティの高信頼化、スマート化、セキュリティー強化等に関するテーマに取り組んでいる。

【中国】第 12 次 5 年計画(2010~2015 年)の中で、「省エネ、環境保護」「新エネルギー」「次世代情報技術」「新材料」「バイオ」「新エネ自動車」「ハイエンド設備製造」の 7 大産業の高度化を打ち出し、重点政策として物聯網 (IoT) と、スマートシティ、スマートグリ

ッド、スマートコミュニティー等のスマート ICT 推進を掲げている⁶⁾。

【韓国】2009年に政府が「モノの通信基盤構築基本計画」を発表。2011年から「モノのインターネット支援センター」を運営して中小ベンチャー企業の技術開発と試験環境を支援している。2013年6月にはIoTの中長期発展計画を盛り込んだ「インターネット新産業育成方案」を発表し、2017年までにM2M・クラウド・ビッグデータなどの新産業を育成し雇用を創出する方針を打ち出している。

【日本】2012年7月に閣議決定された「日本再生戦略」で、環境変化に対応した新産業・新市場の創出に向け、ビッグデータビジネスの創出に向けたM2M通信等の技術の検討・確立を掲げている。2020年までにビッグデータの利活用等により約10兆円規模の関連市場の創出を目標とする⁵⁾。経済産業省・総務省・農林水産省・国土交通省等々において、ICT技術を活用した産業振興・研究開発プロジェクトが実施されている。

（4）科学技術的・政策的課題

従来のM2Mアプリケーションでは、状態の遠隔監視やセンサー情報の収集自動化など、省力化によるコスト削減を目的としたものが多かった。しかし今後は、遠隔センシングのような通信部分に閉じた局所的なコスト改善ではなく、米国のIndustrial InternetやドイツのIndustrie 4.0に代表されるように、産業全体のモノやカネの流れと結合してエコシステムを変えるコスト構造変革がより一層期待される。そこで、科学技術的な課題として、ネットワークの提供事業者や接続形態が複雑多様化する中でも、要件の厳しい産業応用やCPSの実現のため、エンド・エンド間の全体を通して通信品質（容量や遅延など）を担保する技術や、低能力なM2M端末にも適用できるセキュリティー・プライバシー技術の研究開発の重要性が増してくると考えられる。

一方、政策的課題としては、電波利用料制度や通信料金制度、電波割り当て等が考えられる。ライセンスバンドを用いる移動網では、一端末あたりに課せられる電波利用料はスマートフォンもM2M端末も事実上同じだが、通信頻度や通信時間・容量等の特性が両者で大きく異なることから、例えば、実際の通信量に応じた電波利用料とするなど、より柔軟性の高い制度への転換も考えられる。また、移動網・固定網等の利用料金は、数々の規制緩和が図られてきたが、通信回線のボリューム契約や卸提供、複数事業者間の回線共有、季節的な回線利用など、多様化するM2Mの利用形態に対応可能な柔軟な料金体系導入を可能にする更なる規制緩和等が考えられる。また、電波の割り当てに関して、特にアンライセンスバンドでは、我が国でのM2M活用に支障を来すことのないよう、グローバル共通バンドの確保に引き続き配慮していく必要がある。さらに、ビッグデータ時代を控えて、利用者と事業者の双方が安心して各種サービスを利用するためのプライバシー関連の法規制の整備・充実が期待される。

（5）注目動向（新たな知見や新技術の創出、大規模プロジェクトの動向など）

M2Mデバイス通信・管理プロトコルに関する業界アライアンスが2013年終盤から2014年にかけて続出している。スマートホーム向けプロトコルとしてGoogleのNest Labが推進するThread Group、オープンソースであるAllJoin技術をベースにIoT標準を目指しQualcommが主導するAllSeen、AllSeenとは異なる立ち位置でセキュリティー等を強化し

て Intel などが主導する OIC (Open Interconnect Consortium)、産業界向けに GE などが推進している IIC (Industrial Internet Consortium)、iOS デバイスを軸とした Apple の Homekit など、多種多様な業界アライアンスが乱立している。それらの中でも、特に Google の Thread は実際に利用可能なソリューションを提供しており、国家や複数の参加社の思惑で標準を策定していくスタイルと一線を画し、デファクトスタンダードとして IoT 標準プロトコルの定着を図る動きとして今後が注目される。

(6) キーワード

M2M、IoT、M2M プラットフォーム、水平統合、スマートメーター、スマートグリッド、スマートシティー、スマートホーム、マシンタイプ通信、SIM、E-SIM、仮想化、NFV、SDN、セキュリティー、HEMS、ビッグデータ

（7）国際比較

国・地域	フェーズ	現状	トレンド	各国の状況、評価の際に参考にした根拠など
日本	基礎研究	○	→	・大学等の研究機関で、M2Mエリアネットワーク(Wi-Fi、920MHz帯無線、Bluetooth等)に関する要素技術研究の取り組みあり
	応用研究・開発	○	↑	・日本再生戦略において、新産業・新市場の創出や、ビッグデータビジネスの創出に向けたM2M通信等の技術の検討・確立を掲げる ・経済産業省・総務省・農林水産省・国道交通省等において、ICT技術を活用した各種産業振興・研究開発プロジェクトを実施 ・HEMS向けにEchonet Lite等の国産標準を推進
	産業化	○	→	・HEMS向けをはじめ、国内家電/通信機器ベンダが技術開発に注力。ただしグローバルベンダとしての存在感の向上に努める
米国	基礎研究	○	→	・欧州同様、M2Mに関しては、大学などの場で長く揉まれてきており、基礎研究としては既に成熟段階と想定
	応用研究・開発	◎	↑	・NITRD計画等に基づき、各省庁・機関が連携しプロジェクトを実施 ・NIST、NSF等が、スマートグリッドのセキュリティや相互接続・運用に関する研究開発・標準化を推進
	産業化	◎	↑	・有力な大手通信機器ベンダやM2M/IoTに関するトップベンチャーが存在感を示す ・三大通信キャリアがいずれもM2Mに関する取り組みに意欲を示す ・有力なM2Mプラットフォームベンダを多数擁する
欧州	基礎研究	○	→	・米国同様、M2Mに関しては、大学やETSIなどの場で長く揉まれてきており、基礎研究としては既に成熟段階と想定
	応用研究・開発	◎	↑	・スマートメータや電気自動車、e-Call等に関する標準化指令を发出 ・フレームワークプログラム(FP7等)で、スマートシティの高信頼化、スマート化、セキュリティ強化等に関する研究開発を実施
	産業化	◎	↑	・スウェーデンやフランスなど、有力な大手通信機器ベンダがM2M分野でも存在感を示す ・イギリス・ドイツ・フランス・イタリア・スペイン等のフラッグシップ通信キャリアが、ネットワーク仮想化をはじめ技術開発に熱心 ・SIMカードベンダを多数擁し、セキュリティ技術レベルも高い
中国	基礎研究	△	→	・基礎研究レベルのアクティビティは見えにくい
	応用研究・開発	◎	→	・第12次5カ年計画の中で7大産業の高度化を打ち出し、重点政策として物聯網(IoT)、スマートシティ、スマートグリッド、スマートコミュニティ等のスマートICT推進を掲げる ・標準化等では独自規格路線を貫く
	産業化	○	↑	・Huawei、ZTE等の通信機器ベンダがグローバルに力をつけて存在感を増している
韓国	基礎研究	○	↓	・国策として、センサーネットワークやRF-IDの取り組みに熱心
	応用研究・開発	△	↑	・中小ベンチャー企業の技術開発と試験環境を支援。ただし、財閥系大企業は力があるものの、中小企業は層が薄く底力に欠ける
	産業化	○	→	・M2M・クラウド・ビッグデータ等の新産業育成・雇用創出を標榜

（註1）フェーズ

基礎研究フェーズ：大学・国研などでの基礎研究のレベル

応用研究・開発フェーズ：研究・技術開発（プロトタイプの開発含む）のレベル

産業化フェーズ：量産技術・製品展開力のレベル

（註2）現状

※我が国の現状を基準にした相対評価ではなく、絶対評価である。

◎：他国に比べて顕著な活動・成果が見えている、○：ある程度の活動・成果が見えている、

△：他国に比べて顕著な活動・成果が見えていない、×：特筆すべき活動・成果が見えていない

（註3）トレンド

↑：上昇傾向、→：現状維持、↓：下降傾向

（8）引用資料

- 1) デビッド・ボスワーシック他, 「M2M 基本技術書 ETSI 標準の理論と体系」, リックテレコム, 2013.
- 2) 森川 博之, 鈴木 誠, 「M2M が未来を創る」, 電子情報通信学会会誌, Vol.96, No.5, pp.292-298, May 2013.
- 3) 布施田 英生, 「M2M の国際標準化活動と我が国の取組み」, 電子情報通信学会会誌, Vol.96, No.5, pp.299-304, May 2013.
- 4) 藤田 隆史, 後藤 良則, 小池 新, 「M2M アーキテクチャと技術課題」, 電子情報通信学会会誌, Vol.96, No.5, pp.305-312, May 2013.
- 5) 堀 賢治, 服部 雅晴, 吉原 貴仁, 井戸上 彰, 山崎 徳和, 「M2M エリアネットワーク」, 電子情報通信学会会誌, Vol.96, No.5, pp.299-304, May 2013.
- 6) 平成 23～26 年版 情報通信白書, 総務省, 2011～2014.

3.11.3 社会システムデザイン

(1) 研究開発領域名

社会システムデザイン

(2) 研究開発領域の簡潔な説明

交通・物流、エネルギー、公共サービス、医療・介護、第一次産業といった社会システム全般が対象となる課題である。実世界である社会システムの全ての領域において、インターネットにより形成されるサイバー世界との融合により、我々の日常生活全般におけるスマート化・効率化・高度知的化などが実現されることが期待される。鍵となる技術が CPS/IoT とソーシャルメディアである。CPS/IoT においては、導入が遅れている第一次産業への積極的な展開と、モノから人へのより能動的な働きかけを実現するアンビエント情報基盤技術の進展が課題であり、後者の課題の本質はソーシャルメディアにおける課題と同じく「個人適応」にある。そして、個人適応のための鍵となる情報が CPS/IoT やソーシャルメディアを始めとするインターネットを介して得られる、日常生活における各個人レベルの膨大な活動情報から各個人の行動パターンや行動の意図を抽出・推定するビッグデータマイニング・機械学習技術である。

社会システムを構成する最小単位であると同時に、社会システムの対象であるのが「人」であり、CPS/IoT やソーシャルメディアの浸透と、人工知能技術の高度化、そしてクラウドコンピューティングや並列コンピューティング技術の急速な発展に伴い、個人レベルの振る舞いを考慮した社会システムデザインを可能とする段階に入りつつあると考えられる。

(3) 研究開発領域の詳細な説明と国内外の動向

国内における CPS/IoT への取り組みとしては、2011年に経済産業省にて中間報告としてまとめられた「融合新産業の創出に向けて ～スマート・コンバージェンスの下でのシステム型ビジネス展開～」において、農業や医療、交通などの社会システムと IT との融合による新しいシステム産業創出を目指すとした提言や、それを受けての2012年のNEDOによる「IT 融合による新社会システムの開発・実証プロジェクト」として、都市交通、ヘルスケア、農商工連携を例とした取り組みが現在実施されている。また、環境センシングや、バイタルセンシングやスマホを介したユーザーの様々な行動情報、店舗での POS データや、PASMO を始めとする電子マネーの利用履歴など、我々の日常生活における多種多量な時系列データが容易に収集かつ、利用可能となりつつある。ビッグデータ化する膨大なセンサーデータのためのデータマイニングにおいても、MapReduce を始めとする分散処理技術や Jubatus⁴⁾ といった新しいストリームマイニング技術の台頭などを背景として、大学や企業、国家プロジェクトを始め様々な応用先かつ規模にて研究開発が行われている。

米国における CPS への取り組みは2009年からNSFが研究支援を開始しており、企業においてはIBMが「Smarter Planet」という、環境・エネルギー・食の安全といった地球規模の課題をIT活用により解決することを目的とするビジョンを立ち上げるなど、「smart」をキーワードとした展開を加速させている。また、DARPA ロボットチャレンジを通じたロボット技術の向上を目指す実践的なプロジェクトも開始されている。米国での研究開発速度は速く、Google が買収した Boston Dynamics 社の BigDog ロボットを海兵隊がリムパック

でテストを実施する段階にあり、Amazon と Google が 2015 年開始のドローンによる宅配サービス構想を発表し、これは欧州においては DHL が同様のサービスを 2014 年度中の開始を発表している。また、同じく Google においては、ソーラーエネルギーにて駆動する無人機を開発するタイタンエアロスペース社を買収し、ネット接続サービスや地理情報収集用途に利用することが発表されるなど、欧米では日本に比べて企業による CPS/IoT に関する新規サービスに向けた進化が急加速している。

欧州では、FP7 による ICT への戦略的投資を始め、FP5 における ARTIST プロジェクトによる組み込みシステムに関する研究開発への投資など、CPS/IoT を意識した投資がなされている。また、FP7 においては、Ambient Intelligence 研究プロジェクトも実施されており、大学・企業・公的研究機関が参加するなど精力的な研究開発が行われている。

中国においては、物聯網（ウーレンワン）という名称にて、RFID やセンサーネットワークを利用したセンシングと情報ネットワークを融合により、交通や物流の効率化を目指す活動が広く都市間にて競争的に行われている。

韓国においては、サムソンがけん引役であり、2014 年 7 月に家庭内機器の IoT の標準化に主眼を置く非営利団体 Thread Group ²⁾ に参画するなど、積極的な展開を見せているが、国レベルの活動という点では日米欧に比べて注目度が低いように見受けられる。

（４）科学技術的・政策的課題

- ・ CPS/IoT の導入に向けた活動においては、SUICA や電子マネーなど、主として都市部における日常生活への導入速度は向上しつつあるが、第一次産業への展開が相対的に遅れているように見受けられる ³⁾。農業試験場といった研究拠点では IT 導入に向けたセンシングやロボット活用といった試みが盛んになりつつあるが、それ以外の一般の農家に対しての本格的な展開についてはまだ時期尚早というレベルである。都市部に野菜を安定供給するための野菜工場の駆動に向けた展開は加速しつつあるが、国内における農作業現場の大半は従来通りの屋外にて自然と相対する環境である。屋内と異なり天候の影響を直接受ける環境であることから、センサーなどの設置と管理が容易であることが必須である。また、圃場に電源とネットワークのためのケーブルを敷設することも困難であり、これらの要求に対応したセンシングデバイスの更なる開発が急務である。
加えて問題となるのがセンサー等の価格である。現状では個々の農家がこれらのデバイスを購入するしかなく、抜本的な助成などの政策が必要であろう。そもそも、一般農家がセンサーシステムを導入するだけで生産性や農作物の質が向上することはなく、熟練農家や農業試験場でのノウハウを一般農家に反映させるための「暗黙知抽出」や個々の農家の農作業の仕方に対応してノウハウを伝授する仕組みの確立のための研究・開発も急務である。第一次産業に関する社会システムデザインは国の基盤を成す重要な課題であり、農産物に関しては TPP 問題を鑑みるに「量」に加えて「質の向上」が求められる。
- ・ 社会システムは大規模かつ動的な複雑システムであり、現在の社会システムもすべてが計画通りに設計されたものではない。大規模複雑系では多数の自律的なシステムが複雑に影響し合い、様々な階層が構成されている。社会システムであれば、自律システムの最小単位が人であり、様々な人々の振る舞いの集合として社会や国家が形成される。従来の工学的なシステム構築方法、すなわち大問題を小問題に分化して再構成する還元的手法では大

規模複雑システムを構築することは困難であり、大規模複雑系を理解・制御・構築する理論体系を構築する必要がある。この課題に対して、センサーや RFIDなどを介して様々な実世界の情報が容易かつ大量に収集可能となる CPS/IoT 基盤は極めて重要である。

- CPS/IoT は今後の社会システムデザインにとって基盤となるものであり、CPS/IoT を社会全般に偏在させることが必要であろう。そのためには、センシングデバイス同士での通信プロトコルや収集されるデータの管理方法に対する社会全般レベルでの標準化も必要となる。例えば、現在は、家電ネットワークと ITS における車内 LAN や、上記農作業でのセンシング機器の通信方法などはすべて独立した研究開発となっており、これら全てにまたがる標準化が必要となる。そのための産官学の積極的な連携が必要であろう。
- CPS/IoT とソーシャルメディアとの関係においては、特に情報拡散の観点からのセキュリティ対策が課題であろう。アカウント情報の不法取得やデータの不法入手といったシステムに関連する脆弱性に対する防衛は無論のこと、デマや流言・個人情報の拡散といった、人為的に起こされる問題に対応するための技術開発が急務である。CPS/IoT の浸透により、より詳細な個人情報や環境情報が流出する事態は避けなければならない。難しいのは、デマや流言といった事象が、必ずしも悪意で発生するわけではないということであろう。最初は善意から発信された情報が結果的に間違っただけの情報であるにも関わらず拡散されてしまうというケースも多々存在する。情報が拡散するパターンからのこれらの異常な現象の早期検出と拡散を早期に収拾するための技術開発が急務であろう。

(5) 注目動向（新たな知見や新技術の創出、大規模プロジェクトの動向など）

- 農林業など熟練者の暗黙知の形式知化に向けた取り組みが、様々なバイタルセンサーや環境センサーによる CPS/IoT を基盤として加速しつつある。
- CPS/IoT にて収集されるデータは多様かつ多量であり、時系列性のあるデータも含まれる。まさにビッグデータと呼ぶべきデータであるが、ビッグデータに対するデータマイニング技術・機械学習技術において深層学習といったニューラルネットワーク型手法の進展が見られる。また、様々なデータに対しても対応可能な汎用性を持つ人工知能研究についても注目され始めている⁵⁾。
- 関連予算
 - NEDO 「IT 融合による新社会システムの開発・実証プロジェクト」
 - 文科省 「社会システム・サービスの最適化のための IT 統合システム構築」
 - JST CREST 「共生社会に向けた人間調和型情報技術の構築」
 - JST CREST 「ビッグデータ統合利活用のための次世代基盤技術の創出・体系化」
 - JST CREST 「科学的発見・社会的課題解決に向けた各分野のビッグデータ利活用推進のための次世代アプリケーション技術の創出・高度化」
 - JSPS 課題設定による先導的人文・社会科学推進事業 「リスク社会におけるメディアの発達と公共性の構造転換～ネットワーク・モデルの比較行動学に基づく理論・実証・シミュレーション分析¹⁾」

(6) キーワード

CPS、IoT、センサーネットワーク、社会システム、複雑系、ビッグデータ、RFID、ロボット、インターネット、自律分散システム

(7) 国際比較

国・地域	フェーズ	現状	トレンド	各国の状況、評価の際に参考にした根拠など
日本	基礎研究	◎	↑	NEDO、JST、JSPSなど、基礎研究への予算配分も積極的に行われている。科研費における関連研究も多く採択されている。国内研究会も活性化されている。
	応用研究・開発	○	↑	標準化など、産業化に向けた動きは基礎研究に比べて遅いように見受けられる。主として都市部での展開に比重が置かれている。
	産業化	△	↑	第1次産業への展開が遅れている。国の基盤をなす部分でもあり、積極的な展開が望まれる。CPS/IoT 導入に向けた抜本的な助成なども必要であろう。
米国	基礎研究	◎	↑	NSF, DARPAなど、精力的に研究が展開されている。
	応用研究・開発	◎	↑	軍事への応用という観点からもロボット研究と並び開発に向けたサポートが積極的に展開されている。
	産業化	◎	↑	日本と異なり、農場は大規模であり、ロボットやセンサーといったCPS/IoTの導入の必要性が特に高く、産業化も進んでいる。都市部での導入・産業化については日本と同等のレベルにあると考えている。
欧州	基礎研究	◎	↑	FP5, 7 などにおいて助成も活発であり、従来理論主導である欧州において基礎研究は活性化されている。
	応用研究・開発	○	↑	日本と同等レベルであると思われる。
	産業化	◎	↑	ドイツ、フランスなど、ID管理によるレンタル自転車サービスや、RFIDによるバス・メトロ・トラムの共通利用など利便性を感じることが多い。
中国	基礎研究	○	↑	近年、CPS/IoT関連の国際会議を多く誘致するなど、基礎研究に対しての積極性が見られる。
	応用研究・開発	○	↑	国内において競合が乱立しており標準化がボトルネックとなっている。また知的財産問題も課題。
	産業化	×	↑	都市部と農村部での乖離が激しく産業化はこれから。
韓国	基礎研究	×	↑	基礎研究においては日米欧に遅れていると感じる。際だった論文も少ないと感じられる。
	応用研究・開発	○	↑	韓国におけるIoTのけん引役はサムソンであり、2014年7月に家庭内機器に主眼を置いたIoTの標準化を目指すThread Groupに参画するといった展開を見せている。
	産業化	○	↑	開発に呼応して産業化にも積極的である。

（8）引用資料

- 1) 課題設定による先導的人文・社会科学研究推進事業：
<http://www.jsps.go.jp/ryoiki/saitaku.html>
- 2) Thread Group: <http://threadgroup.org/Home.aspx>
- 3) AI 農業： <http://www.maff.go.jp/j/shokusan/sosyutu/sosyutu/aisystem/aisystem.html>
- 4) Jubatus： <http://jubat.us/ja/>
- 5) 汎用人工知能研究： <http://www.sig-agi.org/>

3.11.4 CPS/IoTセキュリティ

(1) 研究開発領域名

CPS/IoT セキュリティ

(2) 研究開発領域の簡潔な説明

CPS は、交通・エネルギー・製造業・ヘルスケアといった様々なセクターのスマートデバイスやシステムに、今までにない方法でサイバー世界を接続し新たな機会を生む。IoT も同様であり、モノが新たにインターネットに接続することで新たな機会が生まれる。新たな機会が生まれることで、サイバー攻撃（ハッキング）などによるプライバシー・データ保護などセキュリティに関しても新しいリスクや懸念が生まれる。

このような新しいリスクに対してのセキュリティ対策が必須である。今後の CPS/IoT の発展における重要性を考え、CPS/IoT に関するサイバー攻撃からの予防、軽減、対応技術についての研究開発が欠かせない。なお、データ保護・プライバシーについては別の節にゆずる。

(3) 研究開発領域の詳細な説明と国内外の動向

CPS/IoT には多くの利点もあるが、悪意のあるハッカーにもメリットがあり、人々の生活に容易に潜り込めるようになる。ハッカーたちは既に色々なモノを支配できることを証明している。また、セキュリティ研究者たちも特別な知識とツールを入手し新たなハッキング手法を見つけている。セキュリティの動向を事例に基づいて説明する。まずは悪意のあるハッカーが起こした事故事例を紹介し、次に研究者の発表事例を紹介する。

さらに、制御システムの重要な要素である SCADA (Supervisory Control And Data Acquisition) について述べ、分野別動向についても解説する。

悪意のあるハッカーが起こした事故事例

- ・ 冷暖房管理用のセットトップボックスから DDoS 攻撃（韓国）¹⁾
2014 年、韓国インターネット振興院（KISA）によると、ゲーム会社のヨーロッパ支社のゲームサーバーが、DDoS 攻撃の対象となっていた。DDoS の送信元は、韓国内の複数の大学に設置された冷暖房管理用のセットトップボックスであった。
- ・ 胎児モニターがマルウェア感染（米国）²⁾
2013 年、ボストンにおいて、高リスク妊娠の女性向けの胎児モニター装置がマルウェアに感染し、装置のレスポンスが遅くなったことが報告された。患者に直接の被害はなかった。装置は Philips 製とされている。
- ・ アイロンがウイルスをまき散らす（ロシア）³⁾
中国製のアイロンの中に、近隣 200m 以内の無線 LAN にアクセスし、同 LAN 上の PC にマルウェアをまき散らすチップが埋め込まれていることが発見された。
- ・ 核燃料施設の遠心分離器が稼働不能（イラン）⁴⁾
2011 年、イランの核燃料施設のウラン濃縮用遠心分離機を標的としてサイバー攻撃が実施された。遠心分離機を制御する PLC が乗っ取られ、周波数変換装置が攻撃されたことにより、約 8400 台の遠心分離機の全てが稼働不能に陥った。またブーシェフル原子力発

電所においても被害が生じたとされている。

- 病院の冷暖房管理システムや顧客情報管理のコンピューターへ侵入(米国)⁵⁾
2009年、テキサス州の病院の警備員が、同病院の冷暖房管理（HVACシステム）や顧客情報のコンピューターに侵入し、HVACシステムのスクリーンショットをオンラインで公開。公開された画面では、手術室のポンプや冷却装置を含め、病院の様々な機能のメニューが確認できる。さらに、病院内のPCにマルウェアをインストールする様子なども動画で公開された。逮捕により未遂に終わったものの、警備員は、乗っ取った病院のシステムを使って独立記念日に大規模なDDoS攻撃を仕掛ける計画を立てていた。
- 26万4000ガロンの未処理水が近隣の川に流される（オーストラリア）⁶⁾
2000年、制御システムの一つであるSCADAソフトウェアを開発する企業の元従業員が、上下水処理場の運営会社の職に応募した。しかし不採用とされたことに恨みを抱き、2カ月の間46回にわたって同社の下水処理の制御システムに侵入し、下水排水施設のデータを書き換えたりオペレーションを妨害。26万4000ガロンの未処理水が近隣の川に流された。

研究者の発表事例

- ホテル内の任意の部屋の電源、温度管理などが操作される（中国）⁷⁾
2014年、中国・深圳市のホテル St Regis Shenzhen で、各客室に備え付けられた iPad（室内の照明やテレビ、ブラインドの開閉、温度管理などを制御）のプロトコル（KNX/IP）を解析し、任意の部屋のテレビ等の電源を入れるなどのハッキング事例を報告。
- 飛行機の機内システムがハッキングされる（米国）⁸⁾
2014年、IOActive社のサイバーセキュリティ専門コンサルタントが機内システム用の機器を製造する Cobham、Harris、Hughes Network Systems、Iridium Communications、そして JRC 日本無線の機器をリバースエンジニアリングの手法を用いて検証し、脆弱性をあぶり出すことに成功した。
- 信号機がハッキングされる（米国）⁹⁾
2014年、ミシガン大学の研究チームが、無線ネットワークにつながった交通信号をハッキングできないか試みたところ、100カ所ほどの交差点の信号機のハッキングに成功。この自動車の交通量に応じて信号機を自動制御するシステムは、アメリカや日本で導入されている。
- 刑務所のドアが囚人によって開かれる（米国）¹⁰⁾
2011年、刑務所（連邦刑務所施設）をコントロールするために使用されているコンピューターシステムのドアやゲートをリモートで開閉するために使われている SCADA システムの PLC に脆弱性が発見された。この脆弱性を悪用すると、監獄のドアをリモート操作で開閉したり、内部通信システムをシャットダウンできることが明らかになった。
- インスリンポンプがハッキングされる（米国）¹¹⁾
2011年、糖尿病患者にインスリンを持続的に注入するコンピューター制御の携帯型医療機器であるインスリンポンプや、体内に植え込んで使うペースメーカー・ICD（植え込み型除細動器）について、無線機能の脆弱性により、インスリンポンプを停止に追いやり、投与するインスリンの量を外部から操作し致死量まで増やすことができるという研究

が発表された。

- ・スマートメーターがハッキングされる（米国）¹²⁾

2009年、認証の不備を利用し、1つのスマートメーターに悪質なプログラムを仕掛けると、隣接するメーターを次々と感染させ、エリア内のすべてのデバイスをこの悪質なファームウェアに感染させることができると発表された。

SCADA

M2M 製品として、世界で最も使用されているシステムが SCADA (Supervisory Control And Data Acquisition) である。SCADA とは産業制御システムの一つである。用途は幅広く、製造・生産・発電・組み立て・精錬などを含む工業プロセス、水処理・水道・排水・下水処理・石油やガスのパイプライン、送電網・大規模通信システムなどのインフラ、ビルディング・空港・船舶・宇宙ステーションなどの設備に使用される。

2013年にICS-CERTは、ユーザーやパートナー経由にて産業システムの256件の事件に対応したと発表している。共通の初期感染方法は、インターネットからの不正アクセス、USB接続のリムーバブルメディア経由のマルウェアの転送、ソフトウェア/ハードウェアの脆弱性の悪用、および標的型攻撃であった。これらの事件の報告は自主的に行われるため、この報告以上の事件が発生していると考えられる。

最も多く攻撃対象となったシステムはSCADAである。次点ではユーザー・インターフェースをつかさどるHMI。その後PLC、Hardware、Software、Interface/Protocolと続く。割合として50%が一位であるSCADAが占める。SCADAとHMIで75%、PLCを合わせると90%をも占める。¹³⁾

分野別 SCADA 動向

- ・水道分野

オランダ政府とTNO Defence, Security and Safety社が、上水道分野用SCADAのセキュリティ水準向上のために「上水道分野用のSCADAセキュリティ グッド・プラクティス」を2008年3月に公開。ここには39の対策項目がチェックリストとして掲載されており、内11件が企業経営者向け、28件が重要インフラシステムの管理に関する技術者向けとなっている。

- ・石油分野

2004年に米国石油協会が「API Standard 1164」を策定。

SCADAシステムセキュリティのための実践策を提供するとともに、SCADAシステムによるパイプラインオペレーションのセキュリティを向上する手段として「SCADAシステムのインシデント発生可能性の識別と分析のためのプロセス」「コアとなるアーキテクチャーの堅牢化のための実践策」「推奨実践策の提示」を提供。

- ・発電システム分野

2006年にNorth American Electric Reliability Councilが、発電設備と伝送システムに対するセキュリティリスクを低減するためにNERC Cyber Security Standardsを策定。

（４）科学技術的・政策的課題

CPS/IoT システムにおいてセキュリティーを確保するためには、以下のような取り組みやリスクを踏まえたシステム設計が必要である。

- ・技術的問題解決のためにまずはセキュリティーテストを実施する
CPS/IoT にのみ言えることではないが、まずはセキュリティーテストをきちんと実施すべきである。一般的な製品の出荷プロセスと同様に、品質のチェックという意味でのテストのみならずセキュリティーの観点からのテストが必要である。
現在では完成品に対して、脆弱性調査やペネトレーションテストという手法が使われている。この手法の問題点は、表面からテスト（擬似攻撃、解析）を行うことであり、テスト項目が網羅的ではない上に、仮に問題点が検出されてもその部分だけを修正するいわばもぐらたたきの修正アプローチとなり、潜在的な問題点が残り続ける原因となる。また、完成品の入手や検証施設（テストベッド）の準備も技術者の負担となるため、大規模なものでは十分に評価されない可能性がある。製品としての網羅性を考えたテストを実施しなければならない。
- ・サプライチェーンリスクを考慮する
各種製品は世界中の複数のベンダーによって組み立てられて輸送されるが、それが安全だとは限らない。悪意のある当事者が製品の改ざんや妨害行為をしたり、最終的にはシステムインテグリティや信頼性、安全性を危険にさらされるなど、多くの危険性が存在する。ハードウェアやソフトウェアそしてサービスを不正に入手する組織については完全に解明されていないことに加えて、これらの製品やサービスに関係するセキュリティーリスクの適切な管理もできていない。従来、納期や障害時の回復に加えて、製品に脆弱性があった場合のリスクや情報が不正に抜き取られるものを埋め込まれていないかなどのリスクマネジメントが必要である。
- ・リスクはコンテキストウェア（context aware）である
多くの個人がプロセスに関わるほど、プライバシーの考慮やポリシーがコンテキストウェアとなる。プライバシーやデータ保護、セキュリティー保護については、考慮するオブジェクト（ヘルス系なのか、位置情報系なのか等）の目的によって変わる。例えば、スマートホームやスマートグリッドといった電力管理アプリケーションでは、プライバシーとデータ保護をどう確保するのかを考慮しなくてはならない。
- ・データ保護、プライバシーとコンプライアンス教育が必要である
データ保護の権利とデータ保護の基本方針をどのように受け入れるかを教育することが必要である。裏で IoT アプリケーションが動いていても、個人情報処理されていることに気付かない可能性がある。さらには、データを収集するための権限とデータ収集の最適な頻度も慎重に対処すべき問題である。
- ・プライバシーとデータの保護
IoT 環境の特徴は、デバイス、センサー、リーダーそしてアプリケーションが環境内でやり取りする様々なタイプの個人情報を収集することである。このような情報は、ID やセンサーデータそして IoT システムへの接続機能から収集した情報によって、個人の趣味、位置情報が露呈するかもしれない。こういった懸念は、電子認証の欠陥や ID の盗難にも

関連する。この問題に関する最近の事例は、コンタクトレスなクレジットカード（非接触型クレジットカード）に見られる。このクレジットカードは、認証せずに名前やカード番号を読み取ることができるので、カードデータを悪用した攻撃者がカード所有者の ID と銀行口座から買い物ができてしまう。従って、プライバシーの保護と同時にデータの保護にも配慮する必要がある。

（5）注目動向（新たな知見や新技術の創出、大規模プロジェクトの動向など）

国際動向

・欧州 Cyber-Physical Systems of System(CPSoS)

EU が出資するプロジェクト¹⁴⁾。CPSoS は、System of System(SoS)関連のプロジェクトやコミュニティ向けのエクステンジプラットフォームを提供している。これは、大規模で複雑な Physical System に関係するコンピューティングシステムやコミュニケーションシステムのエンジニアリングやオペレーションがもたらす課題に焦点を当てている。CPSoS のアプローチは、異なる SoS 関連のコミュニティから知識を集めると同時に、アプリケーションを動かすという方法である。また、欧州委員会（European Commission）ではセキュリティー分野として、データ保護とプライバシーについて述べている¹⁵⁾。トレーサビリティ（追跡可能性）/プロファイリング/違法な処理、個人向けのデータ保護の権利に関する教育と組織へのコンプライアンス教育、ユーザーコントロールの喪失と決断の困難さなどが検討されている。

・米国 IEEE CPS Testbeds

Smart Grid、CPS のテストベッドについてセキュリティーが述べられている。セキュリティーテストの手法、評価システムについてテストベッドを中心として検討が行われている。この CPS のテストベッドによって、スマートグリッド研究開発におけるセキュリティーや技術転換のペースは加速するという認識である。このようなニーズは NIST Smart America Challenge (SAC) によって国家の優先事項として位置づけられている¹⁶⁾。SAC では、セキュリティーとして、プライバシーの問題と安全な通信について検討する必要があると指摘している。アーキテクチャーとして、セキュリティーセンターを一カ所用意し、既存技術と同じく、認証・証明書サービス、認証局、ID 管理の機能が定義されている。

・サプライヤー関連の情報セキュリティーマネジメント

世界的な適用を目指した国際基準であり、アクワイアー（ベンダー）とサプライヤー両方に対応する情報セキュリティーマネジメントとして ISO/IEC27036 が存在する。対象は商業、公共セクター、非営利やその他すべてのサプライヤー関係に関連する組織である。システムやソフトウェアエンジニアリングや情報セキュリティーに関する ISO 基準と一致させることとしている。現在、パート 1 から 3 は現在の国際基準のドラフトで、パート 4 は作業草案である。基準として ISO/IEC JTC1 SC27 を発展させたものである。

・米国連邦政府の情報システム向け国家サプライチェーンリスクマネジメント

政府機関では NISTIR7622 が存在する。目的は連邦政府関係機関のガイダンスとサプライチェーンリスクマネジメントを調達機関のプロセスに統合させることである。サプライチェーンにおける 3つの役割に対処している。

- Acquirer—政府の部門や機関が製品やサービスを入手する

- Integrator－要員やプロセス、システムをカスタマイズする特別な組織
- Supplier－Acquirer や Integrator との合意や COTS 製品の供給のためのインテグレーターを結ぶための組織や個人

（6）キーワード

セキュリティーテスト、データ保護、プライバシー、データ収集、SCADA、サプライチェーンリスク、セキュリティー運用

(7) 国際比較

国・地域	フェーズ	現状	トレンド	各国の状況、評価の際に参考にした根拠など
日本	基礎研究	△	↑	事例の収集、NEDOにてセキュリティーベンダーとメーカーにて実証実験 JNSAにてIoTセキュリティーWGの発足 サイバーセキュリティー2013
	応用研究・開発	△	→	事例の収集中心であり、特筆すべき事例は存在しない JAISTや東京電機大学にてセキュリティーコース開設予定、今後に期待
	産業化	×	→	CPS/IoTに限らず製品開発においては特筆すべき活動が見当たらない 一部のセキュリティーベンダーにて警鐘が鳴らされている
米国	基礎研究	◎	↑	BlackHatなどのセキュリティーカンファレンスにて研究者が問題と課題について発表 NIST IR 7628, Smart America Challenge
	応用研究・開発	○	→	スマートメーターを中心に、テストベッドを利用して議論を行っている
	産業化	○	↑	CPS/IoT製品専用の攻撃ツールの販売 既存セキュリティーベンダーによる、CPS/IoT向けのマルウェア対策
欧州	基礎研究	○	→	BlackHatなどのセキュリティーカンファレンスにて研究者が問題と課題について発表
	応用研究・開発	○	↑	データプライバシーとデータ保護について活発に議論 IoT Privacy, Data Protection, Information Security
	産業化	◎	↑	SCADA専用のIDSの製品開発
中国	基礎研究	×	→	特筆すべき事例は存在しない
	応用研究・開発	×	→	特筆すべき事例は存在しない
	産業化	×	→	特筆すべき事例は存在しない
韓国	基礎研究	×	→	事例の収集中心であり、特筆すべき事例は存在しない
	応用研究・開発	×	→	事例の収集中心であり、特筆すべき事例は存在しない
	産業化	△	→	IoTデバイス自体にセキュリティー機能を盛り込んだ製品発表

(註1) フェーズ

- 基礎研究フェーズ：大学・国研などでの基礎研究のレベル
- 応用研究・開発フェーズ：研究・技術開発（プロトタイプの開発含む）のレベル
- 産業化フェーズ：量産技術・製品展開力のレベル

(註2) 現状

- ※我が国の現状を基準にした相対評価ではなく、絶対評価である。
- ◎：他国に比べて顕著な活動・成果が見えている、○：ある程度の活動・成果が見えている、△：他国に比べて顕著な活動・成果が見えていない、×：特筆すべき活動・成果が見えていない

(註3) トレンド

- ↑：上昇傾向、→：現状維持、↓：下降傾向

（8）引用資料

- 1) <http://m.etnews.com/20140516000085>
- 2) <http://www.ipa.go.jp/files/000038223.pdf>
Hospital medical devices riddled with malware :
<http://www.fiercehealthit.com/story/hospital-medical-devices-riddled-malware/2012-10-18>
- 3) 英国 BBC サイト（「TV 番組ロシア 24」の放映内容より）：
<http://www.bbc.co.uk/news/blogs-news-from-elsewhere-24707337>
- 4) <http://www.globalresearch.ca/israeli-intelligence-report-us-drone-downed-by-iran-cyber-attack/28114>
- 5) Feds: Hospital hacker's 'massive' DDoS averted :
http://www.theregister.co.uk/2009/07/01/hospital_hacker_arrested/
- 6) http://www.css-center.or.jp/pdf/about_CSSC_20140929.pdf
- 7) Here's How Easy It Could Be for Hackers to Control Your Hotel Room :
<http://www.wired.com/2014/07/hacking-hotel-room-controls/>
- 8) Hacker Says He Can Break Into Airplane Systems Using In-Flight Wi-Fi :
<http://www.npr.org/blogs/alltechconsidered/2014/08/04/337794061/hacker-says-he-can-break-into-airplane-systems-using-in-flight-wi-fi>
- 9) Researchers Demo Hack to Seize Control of Municipal Traffic Signal Systems :
<http://www.eecs.umich.edu/eecs/about/articles/2014/Green-Lights-Forever.html>
- 10) SCADA & PLC VULNERABILITIES IN CORRECTIONAL FACILITIES :
http://www.wired.com/images_blogs/threatlevel/2011/07/PLC-White-Paper_Newman_Rad_Strauchs_July22_2011.pdf
- 11) Black hat hacker can remotely attack insulin pumps and kill people :
<http://www.cbsnews.com/news/black-hat-hacker-can-remotely-attack-insulin-pumps-and-kill-people/>
- 12) IOActive Unveils Smart Grid Security Research :
http://www.ioactive.com/services_grid_research.html
- 13) http://www.ptsecurity.com/download/SCADA_analytics_english.pdf
- 14) A European Roadmap on Cyber-Physical Systems of Systems
<http://ercim-news.ercim.eu/en97/special/a-european-roadmap-on-cyber-physical-systems-of-systems>
- 15) IoT Privacy, Data Protection, Information Security
http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1753
- 16) CPS Testbeds: Energizing a Cybersecure Smart Grid
<http://smartgrid.ieee.org/march-2014/1055-cps-testbeds-energizing-a-cybersecure-smart-grid>

3.11.5 応用と社会インパクト

(1) 研究開発領域名

応用と社会インパクト

(2) 研究開発領域の簡潔な説明

スマートフォンや、Wi-Fi・Bluetooth を搭載した低価格の組み込みデバイスと Web サービスが連携することにより、実空間の情報を巧みに取り込んだリッチなサービスが展開され始めている。ウェアラブル、スマートホーム、ヘルスケア分野における期待が大きい。キラーアプリケーションと呼べるものはいまだ不在ではあるが、プラットフォームや標準のイニシアチブをとることで当該研究分野の主導権を握ろうとする動きが加速している。

(3) 研究開発領域の詳細な説明と国内外の動向

従来ユビキタスコンピューティングであったり、センサーネットワークといったコンセプトで提唱されていた様々なが、CPS/IoT の応用技術として実際の製品に採用され始めた。スマートフォンの普及が果たした役割は大きく、近距離無線で到達する数メートルの範囲を超えなかった実空間に配置されたセンサー情報を、ユーザーのスマートフォンを通じてネットワーク上のクラウドにアップロードすることが低コストで可能になってきた。

CPS/IoT の研究領域は多岐にわたり、両者の専門領域が存在するというよりも、MEMS やセンサーデバイスの素子、回路技術、システムエレクトロニクス技術、通信ネットワーク、ミドルウェア、ユーザーインターフェース技術などの従来から存在する技術分野における新たな潮流として位置づけられている。したがって、CPS/IoT の主要な応用事例はあらゆる業種において見つけることができる。一般的な CPS/IoT のアプリケーションを定義することは難しいが、特に 2014 年から 2015 年にかけて注目の大きかった領域はウェアラブル、自動車、そしてスマートホームである。

ウェアラブル分野で 2013 年にもっとも注目が高かったのはゴーグル型の表示装置である。Google Glass¹⁾のようなスマートフォンなどの情報提示装置のほか、Oculus Rift²⁾のような没入感のある映像を手軽に提示するための表示装置としての商品が多く提案された。日本ではソニーやエプソンが製品を販売している。2014 年にはスマートウォッチの新製品が多く登場した。ソニーやサムスンのほか、Apple が開発する Apple Watch³⁾への期待は大きい。多くのスマートウォッチはスマートフォンと連携して利用するものであり、小さなスクリーンにスマートフォンへの各種通知を表示する機能を備えている。Adidas や Nike、Fitbit⁴⁾、Jawbone⁵⁾などはよりスリムなデザインを導入し活動量計としての機能を前面に打ち出している製品もある。3 軸加速度センサーが小型低消費電力になり、信号処理を行うことで歩数以上の複雑な活動状態や睡眠を推定できることになったことが大きい。必ずしも腕時計型でないものも含めればさらに製品は増える。

スマートホームのコンセプトは数十年前から存在し、現代でも基本的なアイデアに変わりはない。ただ 2011 年 11 月に発表された Nest 社のスマートサーモスタット⁶⁾などスマートホームは IoT 技術を巧みに利用した代表的な商品として紹介されることが多い。セントラルヒーティングが主流の米国では、ユーザーが細かな室温調節などを行うことは習慣に無かった。Nest のサーモスタットは住んでいる人の行動パターンや設置されている家の気象情報、

部屋の室温上昇・低下の傾向を学習して約2割から3割の光熱費を削減することができる。スマートフォンとの連携により、外出先から戻る前にサーモスタットをONにすることもできる。1台249ドルの製品で、平均的な家庭では半年から1年で機器購入コストを償却できることを売りにしている。同社が開発する火災報知器 Protect のほか、サードパーティー製の機器やデバイスともAPIを通じて連携可能である。単なるサーモスタットというよりはIoT時代のスマートホームのハブとなることが期待されており、同社はGoogleによって32億ドルで買収されたことも、同社が話題になった原因の一つである。

スマートロックも主に米国で需要と注目度の高いアプリケーションである。ルームシェアやAirBnB⁷⁾といった個人での部屋の貸し借り、シェアオフィスを対象として既存のドアにデバイスを付加し、スマートフォンを用いて鍵の開け閉めを行うことができる。モバイルアプリによって動的に登録者を細かく制御できるため、友人家族、訪問者のアクセス権を細かく制御できる。Bluetoothを搭載した機種では接近を検知しただけでキーコードなしで解錠されるものもあり、利便性も向上する。また解錠した人の顔写真をとることができる機種もある。Goji⁸⁾, Lokitron⁹⁾, Augst¹⁰⁾といった製品が代表的な物である。

自動車もIoTにより、ユースケースが変わりそうな分野の一つである。LTE技術により、高速移動時でも無線でブロードバンド通信が可能になってきた。カーナビゲーションの地図情報や、交通情報のオンラインからの取得に加え、車内のエンターテインメントコンテンツのダウンロード配信が期待されている。車載インフォテインメント分野では、Windows Embedded Automotive 7、QNX、Tizen、iOS 7 in the car、OAAなど、各自動車会社がソフトウェア企業等を巻き込んでプラットフォームの構築にしのぎを削っている¹¹⁾。IoTにより新たに登場した車関連のサービスとしてはカーシェアを挙げることができる。米国のzipcarや日本のTimesやOrixのカーシェアサービスにおいては、無線通信可能な車載機により、ユーザーが携帯するICカードなどで車の鍵の開け閉めをするのが一般的である。サイクルシェアリングについても同様である。また、自動車分野では自動操縦技術も盛んである。Googleなど自動車産業以外の会社も同技術を積極的に開拓しており、ビジネス展開の方向性について注目度の高い分野である。

（4）科学技術的・政策的課題

前述したように、IoTやCPSの近年の注目の理由は、各種無線通信技術の進展にあらう。4G LTE技術が広範囲で低コストに使えるようになり、広い範囲に展開されたデバイスがクラウドに用意にアクセスできるようになったこと、MVNO (Mobile Virtual Network Operator)が普及することで、通話が無い代わりに通信料が比較的安い通信プランなどが提供されるようになったことが、各種のサービスの実現に貢献している。また、広域の無線のみならず、ユーザーの周り数メートルといった近隣のデバイスとの通信をつかさどる Personal Area Networkの通信仕様も多いに改善した。かざすだけで使えるNFC、ペアリングが容易なBluetooth 4.0 (BLE) は従来のBluetooth 3.0よりもシンプルで低消費電力の通信が可能になっている。iBeaconと呼ばれる位置情報システムではFMP “Find me” profileという無くした端末を別のデバイスから探すためのプロフィールや、PXP (proximity profile)と呼ばれる受信信号強度からだいたい位置を求め対象の物が付近にあるかどうかを調べるためのプロフィールが用意されるなど、3.0以前と比べてもより多様なデバイスのネットワーク化

を意識したプロファイルが用意されている。

IoT や CPS のアプリケーションは膨大に存在し、IoT や CPS を統一的に取り扱うミドルウェア技術や通信標準は存在し得ないと考えるのが妥当である。ただし、ある程度アプリケーションドメインが絞られた業界においてはプラットフォームの標準化に向けての動きがいくつも見られる。前述した車載インフォテイメントの分野以外では、センサーやスマートホームにおけるエンターテインメントやホームセキュリティー等を対象にしたコンソーシアムが林立している。通信会社や ARIB などが関わる oneM2M、サムスン、インテル等がリードする Open Interconnect Consortium¹²⁾、Linux foundation が中心となり Qualcomm や電機系の企業、シスコが関わる AllSeen Alliance¹³⁾、Google 傘下の Nest や Samsung など 7 社が結成した Thread¹⁴⁾ などがある。私的な企業が形成した物では、Apple の Home kit、iControl、ドイツテレコム の QIVICON、AT&T の Digital Life 等も存在する。こうしたプラットフォームの研究開発は今後も激化すると考えられる。

基礎研究で活発なのは、センサーや有機エレクトロニクスの開発である。特にヘルスケア用のセンシング技術は日米欧の高等研究機関で活発に研究が進められている。センシング技術の進展により、これまで離散的にしか測れなかった生体情報（例えば血圧や血糖値）を連続的かつ非侵襲に計測する技術などが多く提案されているほか、医師が不足している発展途上国においてスマートフォンなどを活用することで遠隔診断を行う技術なども盛んに研究されている¹⁵⁾。

（5）注目動向（新たな知見や新技術の創出、大規模プロジェクトの動向など）

魅力的な IoT 製品が数多くの米国のスタートアップ企業から提案、実用化されている。これには、IoT 分野における投資が過熱しているというだけでなく、クラウドファンディングプラットフォームが身近になってきたという影響が大きい。クラウドファンディングとは、Web 上でプロジェクトへの出資者を募るサービスのことを呼ぶ。米 Kickstarter¹⁶⁾などは目標額が集まるとキャンペーンが成功と見なされ企画者へ現金が振り込まれる。昨今では出資者への見返りとしてプロダクトを現物支給するようなキャンペーン形式も定着し、事実上の事前購入サイトとして機能している。通常の EC サイトと異なりキャンペーンには成功しても、プロダクトの開発自体には失敗することもある。はソフトウェア開発と異なり、製品の開発にまとまった金額の現金が必要になるほか、部品の調達の都合から注文台数の正確な読みが求められる。したがって、こうしたクラウドファンディングのサイト上でアイデアを先行公開し、ユーザーに対して需要を正確に評価して生産計画をたてられるようになったことでより少ないリスクで新製品開発野チャレンジが可能になった意義は大きい。製品化に成功した場合には、Google など大手資本に買収されるというケースも見られる。

欧米では私企業やコンソーシアムによる IoT の製品開発が盛んであるが、国からの支援が大きいのが中国と韓国である。中国は 2012 年 8 月に「IoT 発展省庁横断会議」を発足し、国を挙げて標準制定、技術開発、方向付けに力を入れている¹⁷⁾。センサーの開発や無線通信のほか、スマートグリッド分野における送電施設の監視技術やスマートメーターに IoT 技術を用いることに熱心であるという。

一方の韓国は 2014 年に EU と共同宣言を採択し、5G 関連の技術開発、周波数政策などで、緊密な協力体系を構築している。韓国側には 2018 年の平昌冬季オリンピックにおいて

5G 関連技術を披露し、2020 年には世界に先駆けて商用化するもくろみがある模様である。

ドイツ政府が掲げる「Industrie 4.0」では IoT を第四次産業革命を実現しうる技術として期待を集めている。工業製品の生産工場をセンサー技術でスマート化し、適応性が高く、高効率で生産性の高い工場の実現を目指している¹⁸⁾。

Fairchild Semiconductor は Trillion Sensors Universe プロジェクトを立ち上げ米国の大学を巻き込んで 1 兆個のセンサーにより生活を豊かにする新ビジョンを押し進めている¹⁹⁾。

（6）キーワード

センサーネットワーク、スマートホーム、スマートメーター、コネクテッドホーム

(7) 国際比較

国・地域	フェーズ	現状	トレンド	各国の状況、評価の際に参考にした根拠など
日本	基礎研究	○	→	センサーネットワークを用いた実空間情報の取得を行う研究については基礎研究が一通り終了しているという印象がある。デバイス系の研究は強い。
	応用研究・開発	○	→	実際に利用可能なセンサーが多く市販されるようになったことやスマートフォンが普及したことにより研究開発が容易になった。アプリケーションやシステムの研究ではプレゼンスがあるが、センサー自身の研究コミュニティ等は必ずしもIoT、CPSを強調している訳ではない。
	産業化	○	↑	元来、家電などのハードウェアに強いメーカーが、ネットワークサービスと連携する様々なハードウェア製品を積極的に出している。ハードウェア製造を手がけるスタートアップ企業も増加している。
米国	基礎研究	○	→	基礎研究を巡る動向に関しては、日米欧でそれほど大きな違いは見られない。
	応用研究・開発	◎	↑	応用研究についてはセンサーやMEMS、回路系の研究分野からネットワーク、ヒューマンコンピュータインタラクションに至るまであらゆる分野でIoTやCPSを意識した研究が増加している。ヘルスケア分野でのイノベーションの期待が特に大きいのも米国の特徴。
	産業化	◎	↑	デバイスからシステム、アプリケーションに至るまで様々な分野での産業化へのチャレンジが進んでいる。大企業だけでなくベンチャー企業の参入も活発であり、IoT、CPS分野への投資も活発である。
欧州	基礎研究	○	→	基礎研究を巡る動向に関しては、日米欧でそれほど大きな違いは見られない。
	応用研究・開発	○	↑	センサー技術、デバイス技術に関してユニークな技術を有する研究所が欧州には点在する。
	産業化	○	→	電気、自動車関係の企業が産業化をけん引している。スタートアップでは独シーメンスのスピノフであるEnOceanなど、IoT機器向けのエネルギーハーベスティングを手がける会社が存在する。
中国	基礎研究	△	↑	国家としてIoTやCPSを推進する施策を積極的に打ち出している。当該分野の基礎研究についての期待は非常に大きい。標準制定、技術開発に対して非常に積極的である。
	応用研究・開発	◎	↑	応用分野としては、スマートグリッドが大きなアプリケーションの柱の一つである。
	産業化	◎	↑	世界中のIoTやCPS機器の製造に深センの工場群が深く関わっている。
韓国	基礎研究	△	↑	基礎研究を巡る動向に関しては、日米欧同様の状況であるが、大企業が中国同様に標準制定等に熱心である。
	応用研究・開発	◎	↑	特にサムソン電子やLGといった電気系企業がM2M標準規格の制定に熱心に関わっている。大企業はアプリケーションよりも、標準技術の制定に熱心である。
	産業化	◎	→	スマートフォンと連携するサービス等についてサムソン、LGなどが積極的に打ち出している。

(註1) フェーズ

基礎研究フェーズ：大学・国研などでの基礎研究のレベル
 応用研究・開発フェーズ：研究・技術開発（プロトタイプの開発含む）のレベル
 産業化フェーズ：量産技術・製品展開力のレベル

(註2) 現状

※我が国の現状を基準にした相対評価ではなく、絶対評価である。

◎：他国に比べて顕著な活動・成果が見えている、○：ある程度の活動・成果が見えている、
 △：他国に比べて顕著な活動・成果が見えていない、×：特筆すべき活動・成果が見えていない

(註3) トレンド

↑：上昇傾向、→：現状維持、↓：下降傾向

（8）引用資料

- 1) Google Glass, <https://www.google.com/glass/>
- 2) Oculus Rift, <https://www.oculus.com/ja/>
- 3) Watch, <https://www.apple.com/jp/watch/>
- 4) Fitbit, <http://www.fitbit.com/jp>
- 5) Jawbone, <https://jawbone.com/>
- 6) Nest, <https://nest.com/>
- 7) AirBnB, <https://www.airbnb.jp/>
- 8) Goji, <http://www.gojiaccess.com/>
- 9) Lockitron, <https://lockitron.com/>
- 10) Augst, <http://august.com/>
- 11) シリコンバレーにおけるイノベーション Connected Cars と Autonomous Cars 調査報告, NEDO シリコンバレー事務所委託調査
<http://www.nedosv.org/wp-content/uploads/2014/05/Connected-Cars-and-Autonomous-Cars-調査報告書.pdf>
- 12) <http://openinterconnect.org/>
- 13) Allseen Alliance, <https://allseenalliance.org/>
- 14) Thread, <http://www.threadgroup.org/>
- 15) David Robson, Should we diagnose rare diseases with smartphones?, BBC, World-changing ideas, 2014, <http://www.bbc.com/future/story/20141017-the-ebola-detector-in-your-pocket>
- 16) Kickstarter, <https://www.kickstarter.com/>
- 17) 工業情報化部電信研究院、<http://www.catr.cn/>
- 18) 高野敦、Industry 4.0 ドイツが目指す第四次産業革命、日経テクノロジーオンライン、
<http://techon.nikkeibp.co.jp/article/COLUMN/20140107/326061/>
- 19) Janusz Bryzek, Roadmap for the trillion sensor universe, iNEMI Spring member meeting and webinar, 2013.

3.11.6 ものづくりとIoT

(1) 研究開発領域名

ものづくりとIoT

(2) 研究開発領域の簡潔な説明

センサーネットワーク、ウェアラブルデバイス、データ分析などのIoT(Internet-of-Things)関連の技術・サービスを製造業および周辺産業において活用し、製品の品質や機能の向上、製品やビジネスモデルの高付加価値化、あるいは設計や製造プロセスにおけるイノベーションを実現することによって、モノづくりに関わる産業の競争力を強化することを目的とする応用技術領域。

(3) 研究開発領域の詳細な説明と国内外の動向

従来、企業情報システムの役割は、電子化による業務の記録と効率化、ルーティンワークの自動化、大量データの集計や検索、ワークフローなどによるビジネスプロセスの制御・管理などが主であった。現在では、情報システムがビジネスにおいて不可欠なものとなったが、情報システムに対する期待は、データ分析や最適化などの機能による業務上の意思決定の支援や、診断・分析・設計・計画などの高度な知的作業を必要とする業務の支援や自動化など、ビジネスに対する直接的な価値をもたらす領域に移りつつある。また、個々の業務のみならずビジネスモデル全体が情報技術を核としたものに変化していくデジタル化と呼ばれる動きも活発である。

一方で、スマートフォンやタブレットなどのスマートデバイスの普及と進化によって、高性能なセンサーデバイスなどが急速に広まってコモディティ化している。また、ソーシャルネットワーキングサービスやオンラインショッピングの普及によって、ビジネスにおいて有益な情報が抽出できる可能性のある多量のデータがネット上に蓄積されている。それらのデータを扱うために、統計解析・機械学習などのデータを扱う技術、またそれらの処理を効率よく並行化して実行するプラットフォームも発展してきている。これらのビッグデータと呼ばれる動きにおける関連技術は、一般消費者向けのネットビジネスや実店舗の小売業においての活用が進みつつある。

提供される商品やサービスにおいては、モノ（物理的実体のある製品）のサービス化、あるいはサービスのモノ化と呼ばれる、サービスとモノとが一体となる方向性も見られる。従来モノとして売られていた製品がネットワークにつながるようになり、その製品が得るデータをクラウドサービスに吸い上げて処理をすることによって、高い付加価値を持つ情報やサービスを、スマートデバイスなどを通じて提供することが可能になってきた。このように従来は個々の独立したモノとして扱われていた、PC やスマートデバイス以外の様々なモノがネットワークに接続されていく姿としてのIoT (Internet of Things)と呼ばれる方向性が注目されている。現実世界の様々なリアルなモノがネットワーク上の仮想的なサイバー空間に密に接続されていく姿は、サイバーフィジカルシステム (CPS)とも呼ばれる。

これらの一般消費者向けの製品やサービスにおいて使われる要素技術とその利用技術の進化の傍ら、製造業においてもそれらの活用が求められるようになってきた。例えば、米国や欧州においては製造業の再強化が重点政策となっていて、その手段として、いずれにおいて

も IoT 関連技術などの IT の活用あるいは IT との融合が共通して挙げられている。すなわち、「モノづくりと IoT」は政策的なコンセプトとシーズ技術が先行する領域である。

製造業においては、設備そのものの自動化に加えて、生産管理やエネルギー最適化など様々な領域において情報技術の活用が進められてきたが、IoT によって従来より細かい粒度（対象、時間間隔）でのモニタリングや制御が可能になることで、生産性・品質・歩留まり・エネルギー消費などの観点において、設計や製造プロセスの更なるイノベーションを起こすことが期待されている。一方で、長期にわたる設備投資の抑制傾向による設備老朽化への対策として、異常検知や故障の予兆診断の高度化のニーズがあり、センサーネットワークやデータ分析・機械学習技術の適用などが期待される。また、現場技能者の高齢化や若年層の労働力不足に備えて、現場の安全確保や技能伝承を目的としたスマートデバイスやウェアラブルデバイス、あるいは拡張現実 (AR) の適用も進むであろう。

また IoT は、製品そのものの高付加価値化（モノのサービス化、サービスのモノ化）への動きも加速する。産業向けの重機から一般消費者向けの靴に至るまで、様々なものにセンサーが組み込まれてネットワークに接続されつつある。これらの方向性は、モノづくりの際の製品設計の考え方を大きく変えていく。生産ラインの製造装置、工場全体のエネルギー・リソース消費量、運送手段（クレーン、車両など）に加えて、作業員や製造対象物そのものもセンシング対象となり得る。これらの情報が蓄積されて、生産ラインや工場間、あるいは企業間で共有できると、生産・在庫・出荷・物流などのサプライチェーンの効率向上に加えて、個々のプロセス自体の改善やイノベーション、製品設計に対する生産工程や利用者（部品・部材としての利用、最終製品としての利用の双方を含む）からのフィードバックなどが期待できる。

（４）科学技術的・政策的課題

製造現場には、ネットワークや管理の観点から、製造機器などを制御するファクトリオートメーション (FA) あるいはオペレーショナルテクノロジー (OT) と呼ばれる領域（以下 FA/OT 領域）と、生産管理システムなどが稼働する情報システム領域（以下 IT 領域）の階層がある。日本の製造業においては、個別の工場や生産ライン、すなわち FA/OT 領域においては自動化を始めとする高度なオペレーションが実現されていることも多い。IT 領域においては、個別の工場や生産ラインのレベルでは高度なシステム化がされていることも多いが、工場や生産ライン間のシステムの標準化・共通化、サプライチェーン全体の最適化、設計情報のライフサイクル管理や、設計と生産ラインの統合などの観点では、まだシステム化が十分ではない。

製造現場におけるビッグデータや IoT 関連技術の活用はまだ緒に就いたばかりである。

「モノづくりへの IoT」については、基本的にはコンセプトとシーズ技術が先行しているが、個別に見れば先進的な取り組みの事例も少なくはない¹⁾。事例の収集と整理によって、現時点の IoT 関連技術を利用して実現できることが何か、どのような対象領域に適用できるのか、そこでどのようなメリットが享受できるか、そのコストはどの程度か、といった情報を企業間で共有することが有効であろう。

FA-IT 連携と呼ばれる FA/OT 領域と IT 領域のそれぞれのネットワークを、プロトコル変換などの機能を介して連携させる手段は提供されているが、現時点では製造指示と実績デー

タ収集などの必要最小限の接続のみが実現されていることが多い。FA/OT 領域において取得・蓄積されている操業データを IT 領域のシステムで活用するには、この連携機能とネットワークを強化する必要がある。一方で、インターネットとの接続性が比較的高い IT 領域との接続は、外部からの FA/OT 領域への侵入の可能性を高めることになるので、従来よりもなお一層強固なセキュリティー対策が必要となる。

既存設備に対して IoT を適用する場合は、データを収集するセンサーノードに対する電源や電波環境の課題がある。省電力で信頼性の高いセンサーネットワークやノードが安価に提供されることが前提となるだろう。また、センサーからのデータが膨大な量となる場合は、ネットワークの帯域やデータの蓄積が課題になる。また移動体や製品自体にセンサーを仕込む場合には、センサーからの情報に加えて、センサー自体の位置や測定対象などのメタデータの管理が重要になってくる。様々な観点からの分析を可能にするには、センサーデータそのものに対する情報であるメタデータを格納し、柔軟なクエリを受け付けられるデータベースが必要となる。

作業者が身に着けたウェアラブルコンピューターなどによって状況をモニタリングすることで、安全面や作業効率面における効果を狙うことも考えられる。作業効率面では、インダストリアルエンジニアリングやエスノグラフィなどの行動観察的なアプローチとセンサー情報とを組み合わせた進め方も研究開発の対象となるだろう。

FA/OT 領域と IT 領域とでは技術担保やシステム化を主管する組織が異なる場合が多い。例えば FA/OT 領域は生産管理部の管轄、IT は情報システム部の管轄であり、IoT を活用したスマートな工場の実現においては、企画・予算などのオペレーション上の課題も大きい。さらに、経営層の理解度も米国に比べると著しく低いのでトップダウンでのアプローチも難しい。モノづくりと IoT に対する推進体制や経営陣に対する啓蒙活動が必要である。

また、本領域のように、メリットやコストが十分確認できていない新しい対象においては、IT 領域と FA/OT 領域および生産現場の関係者とが協調して漸進的・反復的に試行錯誤を進めていくアイデア共創の仕組みが必要となる。そのような仕組みの確立と共に、異なる領域の橋渡しができる人材の育成も課題であろう。

（5）注目動向（新たな知見や新技術の創出、大規模プロジェクトの動向など）

[注目すべきプロジェクト]

Industrial Internet

米国 GE 社の提唱するコンセプト²³⁾。デジタルな世界と機械の世界との融合によってイノベーションと経済的利益をもたらす。具体的には、ジェットエンジンや発電機などの工業製品や製造設備をセンサーなどからの情報を活用してインテリジェント化し、高度な分析によって予防保全などによる経済的価値を得ると共に、作業者の働き方を変えていくものである。Industrial Internet Consortium には GE の他に AT&T、CISCO、Intel、IBM などが参画し、イノベーション事例の収集・整理、相互接続性を担保するための参照アーキテクチャーの構築、国際標準策定プロセスへの意見反映などを中心に活動している。

Industrie 4.0

Industrie 4.0 はドイツ政府と産業界が推進しているプロジェクトであり、産業界からは SIEMENS、ABB、BMW、ThyssenKrupp、ドイツテレコムなどの企業が、そして多数の大学や研究機関が参加している⁴⁾⁵⁾⁶⁾⁷⁾。Industrie 4.0 は、第一次産業革命としての機械化、第二次の電氣化、第三次の自動化に次ぐ第四次の産業革命を意味していて、その本質はサイバーとリアル融合 (=CPS、Cyber-Physical Systems) であるとされている。具体的には、生産・物流に関わる様々な機械や施設などを個別に自動化・インテリジェント化すると共に、グローバルなネットワークで接続して相互に情報をやり取りできるようにする。これによって、生産プロセスの上流から下流までの垂直方向と、同列の企業や生産ラインを水平方向のネットワーク構造において、リアルタイムで生産ラインおよび製品の管理が可能になる。また、顧客の個別要請へのフレキシブル対応、生産ラインのエネルギー効率の向上、ネットワークを介した遠隔地からのサービスなどによる専門家リソースの有効活用、あるいは冗長なサプライチェーンによるリスク低減などが期待できる。さらに自動化によって人間が創造的な仕事に集中できること、生産計画を動的に調整して柔軟な勤務条件を可能にすることによって、ワークライフバランスの実現にも寄与するとされる。

ワーキンググループによる勧告⁴⁾においては、優先すべき取り組みとして、

- ・参照アーキテクチャーの構築に向けての標準化とオープンスタンダードのアプローチ
- ・複雑なシステムのマネジメント
- ・産業界からの包括的な要求に応えるブロードバンド基盤
- ・Industrie 4.0 の成功に不可欠な安全とセキュリティー
- ・デジタル時代の労働組織とワークデザイン
- ・Industrie 4.0 に必要なトレーニングと継続的なプロフェッショナル養成
- ・規制のフレームワーク
- ・エネルギー・資源の効率性

などが挙げられている。

Industrie 4.0 に着目すべき理由は、新産業創出だけでなく既存産業のリフォームを狙っている点と、標準化への取り組みにみられるトップダウンのアプローチによって関係省庁の壁を越えてドイツ産業界全体のグローバル競争力を強化しようとしている点である。

ドイツにおいては製造装置産業や製造現場がソフトウェア企業や IT 部門に比して強い立場にあるので、IoT などのトレンドに乗り遅れるのではないかとの危機感があったとの見方もある⁵⁾。また、ドイツは伝統的に中小製造企業が強く、グローバル競争力がある中小企業（グローバルニッチトップ）も少なくない。大企業だけでなく、これらの個別に強みを持つ中小製造企業を含めた動的かつ有機的なサプライチェーンが構築可能になれば、あるいは、この巨大な仮想サプライチェーンがグローバルな拠点でのサービスや人材リソース供給などの仕組みと一体化すれば、相当の競争力を有することになるだろう。

(6) キーワード

IoT、CPS、Industrial Internet、Industrie 4.0

（7）国際比較

本領域は領域自体が応用領域であるので、基礎研究についてはIoTの要素技術（センサー、無線通信、データ分析など）の動向を参照のこと。

国・地域	フェーズ	現状	トレンド	各国の状況、評価の際に参考にした根拠など
日本	応用研究・開発	○	↑	個々の要素技術についての応用研究・開発は進んでいる。
	産業化	○	↑	個々の企業での取り組みには先進的なものも散見されるが、業界や産業界全体としての取り組みはこれからの段階。
米国 ²⁾³⁾	応用研究・開発	○	↑	国立標準技術研究所 (NIST)への資金拠出。3DプリンターやITを活用した新しい製造業などを対象とした Institute of Manufacturing Innovation (IMI)の設立。
	産業化	◎	↑	国際競争力強化や米国製造業への投資増加のための地域ハブとしての機能を持つNational Network for Manufacturing Innovation Institutes (NNMII)の創設、Industrial Internet 普及を促進する Industrial Internet Consortium (IIC)の設立など。どちらかと言うとボトムアップ的なアプローチであって、实际的で役立つユースケースを重視しているように感じる。
欧州 ⁴⁾	応用研究・開発	○	↑	ドイツにおいてはIndustrie 4.0の枠組みにおいて要素技術の応用研究・開発が進められていて、通信プロトコルの標準化や異なる製造機器同士の相互接続性の検証などが先行している。他にもEUのHorizon 2020において、「未来の工場」に関する提言 (Vision for Manufacturing2.0)が支援対象選定の議論の材料となっている。
	産業化	◎	↑	ドイツのIndustrie 4.0のコンセプトと、そこで策定が進められている参照アーキテクチャと標準化の動きについては注視する必要がある。
中国 ⁵⁾	応用研究・開発	○	↑	IoTやスマートシティなどを含む物聯網（ウーレンワン）と呼ばれるコンセプトの下、市や省などの地方政府単位で様々なアクションプランの策定やプロジェクトが進んでいる。
	産業化	○	↑	2011年11月に策定された物聯網第12次五カ年計画における重点分野の一つとして工作機械、生産プロセス、サプライチェーンのスマート化が挙げられている。
韓国 ⁶⁾	応用研究・開発	△	↑	様々な産業がITと融合していくとする“IT Convergence”の旗印の下に研究開発が進められている。
	産業化	△	↑	上記以外の目立った取り組みは見られない。

（註1）フェーズ

基礎研究フェーズ：大学・国研などでの基礎研究のレベル

応用研究・開発フェーズ：研究・技術開発（プロトタイプの開発含む）のレベル

産業化フェーズ：量産技術・製品展開力のレベル

（註2）現状

※我が国の現状を基準にした相対評価ではなく、絶対評価である。

◎：他国に比べて顕著な活動・成果が見えている、○：ある程度の活動・成果が見えている、

△：他国に比べて顕著な活動・成果が見えていない、×：特筆すべき活動・成果が見えていない

（註3）トレンド

↑：上昇傾向、→：現状維持、↓：下降傾向

（8）引用資料

- 1) 経済産業省、2014年版ものづくり白書（ものづくり基盤技術振興基本法第8条に基づく年次報告）
<http://www.meti.go.jp/report/whitepaper/mono/2014/index.html>
- 2) GE社ホームページ：Industrial Internet
http://www.ge.com/jp/company/industrial_internet/index.html
- 3) Industrial Internet Consortium ホームページ
<http://www.iiconsortium.org/>
- 4) Communication Promoters Group of the Industry-Science Research Alliance:Securing the future of German manufacturing industry, Recommendations for implementing the strategic initiative INDUSTRIE 4.0, Final report of the Industrie 4.0 Working Group, Apr. 2013
<http://www.plattform-i40.de/finalreport2013>
- 5) 国際社会経済研究所, ドイツの「Industrie4.0」戦略について, Oct. 2014
http://www.i-ise.com/jp/information/report/pdf/industrie40_04.pdf
- 6) 科学技術振興機構 研究開発戦略センター, ドイツ政府の第4次産業革命 Industrie4.0, Sep. 2014
<http://www.jst.go.jp/crds/pdf/2014/FU/DE20140917.pdf>
- 7) 日本貿易振興機構（ジェトロ）, ドイツ「Industrie4.0」とEUにおける先端製造技術の取り組みに関する動向, Jun. 2014
<http://www.jetro.go.jp/world/europe/de/reports/07001735>
- 8) 韓国 IT Convergence :
<http://itce.postech.ac.kr/>