4. IoT 時代の情報処理基盤

4.1 IoT 情報処理基盤

(1) 爆発するデジタルデータへの対応

インターネットの普及、IoT の勃興によりデジタルデータの量は近年急増しており、グローバルなデータ量は、2011 年の約 2 ゼタバイト（2 兆ギガバイト）から 2016 年には約 4 倍の 8 ゼタバイトに拡大すると予想されている。クラウドサービスの普及や IoT の進展等により、データ量は今後大幅に増大すると見込まれ、2020 年には、2000 年のデータ量の約 6,500 倍の 40 ゼタバイトに達するとの予想[61]もある。

IoT 時代には、ネットワークやデバイスの高度化、生活や経済構造に欠かせないインフラとしての ICT 活用の定着、スマートフォンの普及や交通・流通系の IC カード、ウェアラブル機器の普及、センサの小型化・低廉化が、デジタルデータの爆発的増加の要因となる。さらに、SNS などインターネット上のデジタルデータのみならず、自動車や住宅、さらにはものづくりや農業などの産業や社会インフラに係るモノがネットワーク化され、自然現象データ、生体情報等のデータに加え、交通・電力、機械等のデータといったこれまでデジタルデータとして取扱われてこなかったデータがネットワーク化されると見込まれる。米国の大手通信機器ベンダーである Cisco は、モノだけでなく人やプロセスがネットワーク化された世界を IoE(Internet of Everything)と捉えた上で、2000 年には約 2 億であったインターネット・ユーザーが、2013 年には、100 億近くまで増加し、2020 年にはインターネットに接続する機器が、全世界で 500 億台を超えると予測している。また、全世界に 1.5 兆個を推測されるモノのうち、ネットワーク化されているのは僅か数%に過ぎず、潜在的に残りの 9 割を超えるモノが、ネットワーク化される可能性があることを指摘している。実際に IoT 時代に流通するデジタルデータ量を正確に試算することは難しいが、IoT 時代には、これまでにはない膨大なデジタルデータが流通し、そのデータを処理するための仕組みが必要になる。

(2) IoT を実現する情報処理基盤

IoT 時代にデジタルデータが爆発的に増加したとしても、個々のデータのみで生み出せる付加価値は限定される。デジタルデータから付加価値を創出し、経済価値を生み出すためには、データを管理した上で、利用者のニーズに応じて、データ分析、他システムとの連携、リアルタイム処理等を行い、付加価値を生み出すための新たな情報処理基盤が必要となる。そのため、IoT を商機と見込む ICT 企業では、IoT に対応した情報処理向けの製品や情報処理基盤[62]の提供に力を入れている。以下には、ICT 企業による IoT

[61] 総務省「ICT コトづくり検討会議報告書－データの開放・共有・活用による新たな社会・経済構造への転換－」（平成 25 年 6 月）

[62] 各社公表資料、報道資料等を参考としてみずほ情報総研が作成したものである。各製品や具体的な技術に関しては、各社の公表資料等を参照されたい。

に対応した情報処理基盤例[63]の概要を示す。

① IBM

IBM は、同社が提供しているクラウドベースの情報処理基盤に IoT 向けの機能を拡張する形で IoT 向けの情報処理基盤を提供している。2014 年 10 月には、IoT を構成するデバイスの接続を促進するため IoT Foundation[64]と呼ばれるクラウドベースの SaaS の提供を開始した。IoT Foundation は IBM SoftLayer[65]を基盤とする IBM Bluemix[66]環境で稼働する。Bluemix はウェブやモバイル、ビッグデータ、スマートデバイス向けのアプリケーションの開発や管理、運用を行うための同社のクラウドベースのプラットフォームであり、IoT Foundation は Bluemix を IoT 向けに拡張したものである。IoT Foundation を利用することにより、不安定な稼動環境、低帯域 N/W 環境で使用されるセンサや端末向けに開発された IoT や M2M 環境に最適化された通信プロトコルである MQTT[67]（MQ Telemetry Transport）基盤を利用することが可能となる。Bluemix は Cloud Foundry[68]に完全準拠した製品であり、IoT Foundation と IBM Bluemix を組み合わせることで、IoT デバイスやそのデータへのアクセスのセキュリティ、容易性が実現される。

② Microsoft

Microsoft は、2014 年 4 月に、IoT からのデータを収集し、クラウド上で管理する Microsoft Azure Intelligent Systems Service(ISS)[69]を公開している。このサービスを利用することで、Microsoft のデータ分析ツール、例えば Windows Azure 上に構築した Hadoop ベースのサービスである HD Insight や､同社のビジネスインテリジェンスサービス Power BI を利用することが可能となる。ISS は、Microsoft の Azure のクラウドサービスがネット接続型の産業装置やセンサといった IoT デバイスにまで拡大され、装置が生成するデータを OS に依存せず収集、セキュアに接続・管理することが可能となる。Microsoft の IoT 情報処理基盤は、基本的に IoT データを Azure クラウド上に集約する仕組みとなっている。

③ Oracle

Oracle の IoT 向け情報処理基盤は、同社が提供している複数の製品の組み合わせにより実現される。各種センサ情報を識別・集約してサーバーにつなぐセンサ・ゲートウェ

---

[63] IoT に対応した情報処理向けの製品や情報処理基盤は、本レポートで取り上げた例以外にも、日系 ICT 企業を含めて複数の ICT 企業から提供されている。
[64] IBM IoT Foundation（https://internetofthings.ibmcloud.com/）
[65] IBM Cloud SoftLayer（http://www.ibm.com/cloud-computing/jp/ja/softlayer.html）
[66] IBM Bluemix（ https://www.ibm.com/developerworks/jp/cloud/library/cl-bluemixfoundry/）
[67] MQTT は 1999 年に IBM 社と Eurotech 社のメンバーにより考案された M2M や IoT の実現に適したシンプルで軽量なプロトコル。標準化団体である OASIS によって、MQTT の標準化が進められている。
[68] オープンソースの Platform as a Service(PaaS)ソフトウェア群
[69] Microsoft　Microsoft Azure IoT Service
（http://www.microsoft.com/ja-jp/server-cloud/solutions/internet-of-things-health.aspx）

イ機能は Oracle Event Processing for Embedded[70]と呼ばれる。端末側には、データ処理エンジン（Complex Event Processing :CEP）が組み込まれ、フィルタリングやデータ処理機能の一部が実装される。これにより端末側でデータの 1 次処理を行い、ネットワークへの負荷を下げるとともにリアルタイムなフィードバック処理を実現する。長期的なデータ蓄積や高度な分析、フィードバックに関しては、ゲートウェイを経由したサーバーで処理される。サーバー側は、Oracle Linux 上の Oracle WebLogic Server、Oracle Coherence、Oracle Event Processing を活用したインメモリ・プロセッシング基盤、Oracle Database によるビッグデータ管理・蓄積、およびビッグデータアナリティクス製品 Oracle Endeca Information Discovery によるデータ分析基盤から構成される。

④ Cisco

Cisco は、IoE のコンセプトを提唱するとともに、IoE を実現する情報処理基盤として、5 階層モデルを提案している。この階層モデルは、センサや端末等のデバイス層、フィールドエリア～バックホールのネットワークおよびゲートウェアから構成されるネットワーク層、IoE プラットフォーム層（IP ネットワークを管理する IP ネットワークプラットフォームおよびデータ分析を行うためのアナリティクスサービスプラットフォームから構成される）、産業分野でのアプリケーションであるインダストリーアプリケーション・サービス層及びアプリケーションの共通機能となる共通ビジネスサービス層から構成される。

Cisco のデータ処理は、エンドポイント層、マルチサービスエッジ層、コア層、データセンタークラウド層の 4 階層から構成される。Cisco の IoT 情報処理基盤の特徴は、IoE プラットフォームからインダストリアプリケーションサービスをクラウド/フォグコンピューティング上で稼働することが想定されている点である。フォグコンピューティングは、クラウドとデバイスの間にフォグ（霧）と呼ばれる分散処理機能を配し、大量データ処理のクラウドへの集中を防ぐ。これにより、ビッグデータのクラウドコンピュータでのデータ処理負荷を下げると同時に、ネットワークのトラフィック爆発を回避することが企図されている。フォグコンピューティングを実現するためのソフトウェアプラットフォームとして Cisco IOx[71]が発表されている。

(3) IoT 向け情報処理基盤の特徴

各社の IoT 情報処理基盤の基本的な構造や機能は比較的類似し、端末層、ネットワーク層、アプリケーション層とその基盤となるプラットフォーム層から構成される。プラットフォーム層は、データ管理、セキュリティ管理、接続及びデバイス管理の機能から構成される（図 4-1）。

[70] Oracle Oracle Event Processing for Oracle Java Embedded
（http://www.oracle.com/us/technologies/java/embedded/event-processing/overview/index.html）
[71] Cisco、Cisco Fog Computing with IOx（http://www.cisco.com/web/solutions/trends/iot/cisco-fog-computing-with-iox.pdf）

他方、リアルタイムデータの収集や処理の考え方には違いが見られる。IoT において端末のコントロールやリアルタイムな制御が必要な場合には、収集したデータを即時に処理しフィードバックする必要があるが、実際にネットワークに接続される端末の数や処理するデータが膨大な場合、クラウド側のサーバーで一括処理することは、ネットワークのトラフィックと処理速度の観点から問題が生じる可能性がある。そのため、端末やエッジと呼ばれるゲートウェイで一部の処理を行う分散処理方式も採用されている。分散処理による方式は、IoT のネットワーク利用環境が厳しい場合やローカルでリアルタイムなデータ処理が必要なケースでは不可欠なアーキテクチャになる一方、システムの構成や情報処理機能の実装が複雑になる可能性もある。また、膨大なデジタルデータの取扱いが必要な IoT においては、従来の情報処理技術では処理に限界が見込まれ、クラウド側での情報処理に関しては、ビッグデータを活用したビジネスを行う ICT 企業で導入されている超多重分散処理技術[72]等が必要となる。

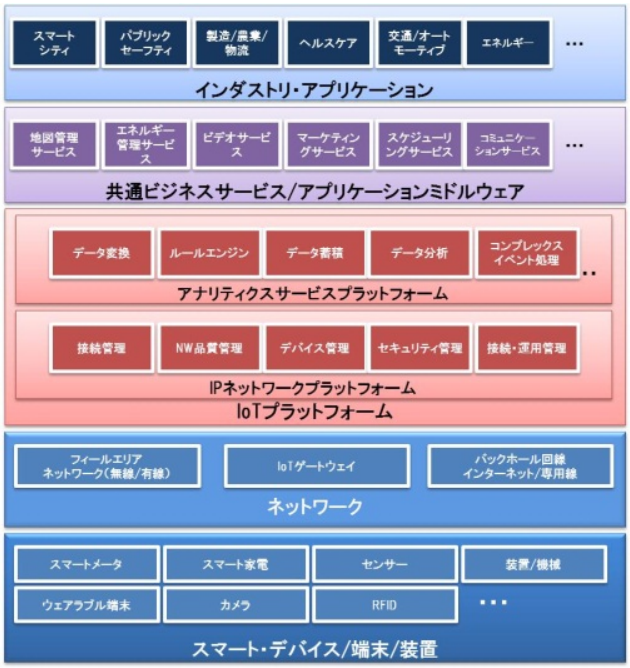
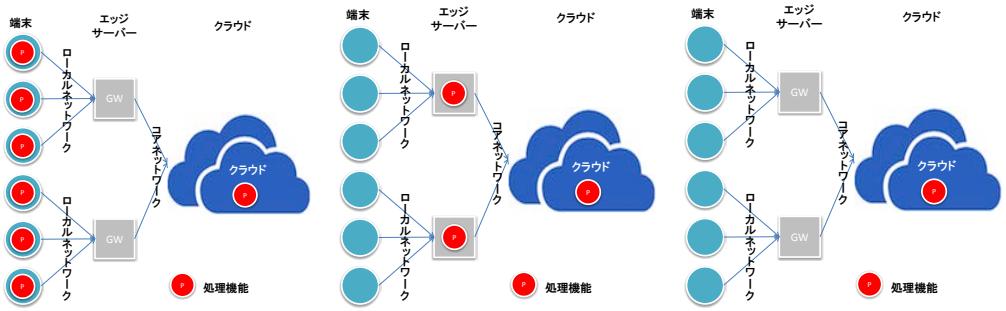


図 4-1　IoT 向け情報処理基盤の階層モデルと機能

出所：各社資料をもとにみずほ情報総研作成

[72] Google により導入された超多重分散処理の手法 MapReduce は、オープンソフトウェア開発団体である Apache Software Foundation が、Hadoop としてオープンソフトウェアとして公開している。また、Facebook 社が開発した大規模データ向けの分散データベース管理システムである Cassandra というソフトウェアも Apache Cassandra という名前で、オープンソフトウェアとして公開されている。こうした超多重分散処理技術は、一定以上のデータ量となるビッグデータの情報処理技術として不可欠になっている。Google 日本法人元社長村上氏は、RDBMS 等、従来の情報処理技術で処理できるビッグデータと区別するためビッグデータ 1.5 と呼んでいる。(出所)村上憲郎、「SNS と IoT（Internet of Things）が切り拓く，ビッグデータ 2.0 の世界」 情報管理 vol.56 no.2（2013）独立行政法人科学技術振興機構



クラウド&エッジ　クラウド&エッジサーバー　クラウド

図 4-2　IoT 情報処理基盤のアーキテクチャの違い

（出所）各社資料をもとにみずほ情報総研作成

(4) 付加価値を生み出すデータ分析機能

センサやデバイス等から収集された膨大なデータを処理したとしても、それだけで、付加価値を生み出すわけではない。膨大なデータから利用者にとって有益な情報を生み出すためには、データを分析して利用者が欲しい情報の獲得や意志決定、機器制御に生かすための情報“分析”技術（アナリティクス）が重要となる。そのため、各社の情報処理基盤には、定型的なデータによる統計的な分析から人工知能による分析まで、様々な技術による情報分析機能が組み込まれている。特に、IoT では、膨大かつ非定型なデータの分析が必要になると見込まれ、従来技術による効果的分析の限界も指摘されている。そのため、膨大かつ多様なデータを効果的に分析するための新たな情報分析技術に注目が集まっている。

4.2　注目される人工知能

IoT データからの情報分析技術として、注目されるのが人工知能の応用である。人工知能は情報分析技術の一つとして旧来から存在していたが、その適用の限界から下火となっていた。しかしながら、新たな理論と人工知能の高度化に不可欠な、計算性能向上と学習のためのデータ環境が現実化することで、第 3 次の人工知能ブームとして脚光を浴びている。以下には、人工知能の歴史と近年の人工知能の発展を牽引している機械学習の進化・ディープラーニングの概要と動向を解説 [73]した上で、今後の展望や課題を示す。

(1) 人工知能の研究領域と研究の変遷

人工知能の定義には、様々なものが存在するが、オペレーションズ・リサーチ学会は、人工知能を「人間や生物の知能を、機械によって実現したもの、あるいはその研究分野」と定義 [74]した上で、具体的なテーマとしてコンピュータを処理の中心とした 各種入出力機器を結合したシステムによるチェス、将棋等のゲームを典型的問題とする問題解決・推論、文字、パターン等の認識、言語の理解、診断等の現象の分析、経験からの学習等を挙げている。

人工知能の関連研究は、生理学、認知心理学、情報工学などの分野で取り組まれている。このうち、情報工学分野では、①知識：知識の獲得と表現とその利用、②推論：推論表現と推論方式、③学習 : 学習理論と学習機能、④アルゴリズム : 有効な解探索戦略、⑤プログラム：人工知能プログラミング言語の開発等が研究対象となっている。

人工知能研究の黎明期には、アルゴリズム、論理、シミュレーションの研究が行われ、現在の人工知能に関する基本的概念が提案されている。1956 年に開催されたダートマス会議において McCarthy により、人工知能の名称が提案された。

その後の研究では、論理型計算や認知心理学的アプローチによる人工知能の研究が行われた他、実用的問題に対するアプローチとして知識工学が提唱され、人工知能の実用化を企図したエキスパートシステム等が開発された。また、我が国においては、人工知能に関連する大型の研究プロジェクトとして第 5 世代コンピュータ計画が通商産業省（現 経済産業省）により行われた。

しかしながら、人間の直感や感性等を論理型計算により実現することが難しく、実用化を目指したエキスパートシステムも知識獲得がボトルネックとなることが判明し、人工知能研究の限界が指摘された。その後、ニューラルネットワークが再び注目され、逆伝播学習アルゴリズムによる学習とパターン認識への応用、遺伝的アルゴリズムによる

---

[73] 人工知能全般に関する動向に関しては、小林雅一、「朝日新書 クラウドから AI」（2013）（朝日新聞出版）などが詳しい。また、人工知能の研究全般に関する書籍としては、馬場口登，山田誠二、「人工知能の基礎（第 2 版）」（2015）（オーム社）などがある。

[74] オペレーションズ・リサーチ学会、OR 事典 Wiki（http://www.orsj.or.jp/~wiki/wiki/index.php）。人工知能の定義や研究の変遷がまとめられている。人工知能学会、What’s AI （http://www.ai-gakkai.or.jp/whatsai/）にも人工知能や研究の変遷等がまとめられている。

人工生命の研究等が活発化した。また、脳科学の立場から脳機能の解明を目指す脳研究も活発化し、その成果の人工知能モデルの高度化への活用も期待されている。

(2) 新たなニューラルネットワーク技術：ディープラーニング

近年人工知能が注目される背景には、ディープラーニング[75]と呼ばれる新たなニューラルネットワーク技術の登場により、従来の人工知能の課題をブレークスルーする可能性が示されたことが大きい。ディープラーニングは、人間の頭脳を構成する無数の神経細胞のメカニズムを模倣した新たなニューラルネットワーク技術である。ニューラルネット自体は、人工知能の研究開発が始まった 1950 年代から存在する技術である。初期のニューラルネットは、米国の Rosenblatt らが開発した「パーセプトロン」である。パーセプトロンは、脳の神経細胞とシナプスの信号伝達メカニズムを単純化させ、工学的に再現したものである。パーセプトロンは、「排他的論理和」という初歩的な論理演算を理解できないという欠陥を持つことが指摘され、一旦は注目されなくなったが、パーセプトロンの構造に「隠れ層」と呼ばれる新たなレイヤーを追加・拡張することで、排他的論理和など初期の問題が解決された。しかしながら、拡張されたニューラルネットも比較的簡単な概念を理解するだけでも、隠れ層の数を増やす必要がある等の課題が指摘され、その期待が後退した。

こうした課題にブレークスルーをもたらした技術が、視覚や聴覚、味覚など人間の様々な認知メカニズムにあるアルゴリズム[76]に基づく「スパース・コーディング（Sparse Coding）」と呼ばれる手法である。スパース・コーディングは、ニューラルネットへの入力情報から、認識に必要な概念形成のための情報（特徴量）を取り出す技術[77]である。スパースコーディングを取り入れた多層化ニューラルネットワークでは、隠れ層の情報が深部にまで伝達されるに伴い、画像であれば、点から線、線から輪郭、輪郭から部分、部分から全体のイメージへと、高次な概念に、学習の深度が段階的に引き上げられる。こうした学習深度が階層化されたニューラルネットワークを総称して「ディープラーニング」と呼んでいる。

---

[75] ディープラーニングに関する書籍には、松尾豊、「角川 EPUB 選書 人工知能は人間を超えられるか ディープラーニングの先にあるもの」（2015）（KADOKAWA）、日経コンピュータ編、「日経 BP ムック The Next Technology 脳に迫る人工知能 最前線」（日経 BP)（2015）、小林雅一著「朝日新書 クラウドから AI」（2013）（朝日新聞出版）などがある。

[76] 脳の視覚野は、網膜から伝達された映像情報を、映像を構成するピクセル情報の中から、物体を認識するための特徴ベクトル（特徴量）を抽出し、これらを段階的に組み合わせ高次の概念を形成する。

[77] 与えられた画像を少数の基底の線形和で表現するため、適切な基底系を統計的・情報論的な基準にもとづき構成する手法である。（出所）村田昇、「スパースコーディングの基礎理論と画像処理への応用」、情報処理学会研究報告 IPSJ SIG Technical Report（2006）一般社団法人情報処理学会

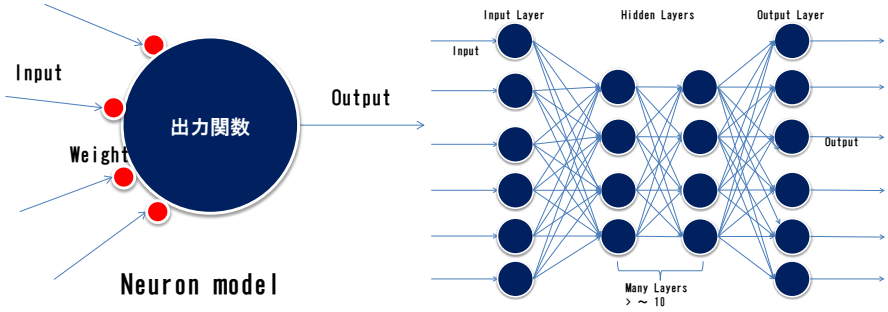


図 4-3　ニューロンモデルと階層型ニューラルネットワーク

（出所）各種資料をもとにみずほ情報総研作成

また、ディープラーニングが逆伝播学習アルゴリズムによる階層型ニューラルネットワークによる機械学習の進化のみならず、入力信号を教師信号として学習することで特徴量を獲得するオートエンコーダの導入やノイズを加えた膨大なデータによる学習を行うことによりロバスト性を高めたことが、ディープラーニングの実用性と可能性を革新的に高めた。

ディープラーニングは、Google をはじめとした ICT 企業が、最優先課題として取り組んでいる人工知能技術である。Google は、米 Stanford 大学との共同研究によりディープラーニング技術を使って YouTube 上にある大量の動画から「猫」を抽出し、そのイメージ（概念）をぼんやりとコンピュータ画面上に表示することに成功した。また、ディープラーニングは実際の製品にも応用され、その成果を上げている。例えば、Google の音声検索や、Apple の音声アシスタント「Siri」などの音声認識技術にはディープラーニングが導入されている。こうした認識技術では、人間の評価を与えない無教師学習モデルが主に利用され、利用の回数が増すにつれて、精度が上がる（賢くなる）仕組みとなっている。

Hawkins らは、人間の認知・学習のメカニズムは、観測された周囲のデータのパターンから予測を行う能力によるとした理論[78]を提唱している。ディープラーニングは、そのメカニズムを再現しているという見解もあり、汎用性と応用の可能性が期待されている。

ディープラーニングの活用の可能性は、一部の特別な ICT 企業に限定されているわけではない。ディープラーニングを実装するための開発フレームワークも複数登場し、代表的なフレームワークには、UC 大学 Berkeley で開発された Caffe[79]や Montreal 大学による Theano/Pylearn2[80]、Facebook、Twitter、Google の技術者により開発された Torch7[81]があ

[78] Jeff Hawkins, Sandra Blakeslee, On Intelligence: How a New Understanding of the Brain will Lead to the Creation of Truly Intelligent Machines, Times Books (2004）.
[79] Berkeley Vision and Learning Center (BVLC)、Caffe（http://caffe.berkeleyvision.org/）
[80] LISA group at the University of Montreal、Pylearn2（http://deeplearning.net/software/pylearn2/）
[81] Torch（http://torch.ch/）

る。ディープラーニングの実装では、GPU の汎用演算機能(GPGPU)との適合性が高いため GPU 専用の開発フレームワークも提供されている。

ディープラーニングの実用性が注目されることで、ディープラーニング専用のプロセッサの開発も始まっている[82]。大脳の神経回路網を模した「ニューロモーフィック・チップ（Neuromorphic Chip）」の開発が進められている。TeraDeep[83]は、ディープラーニング向けのニューロモーフィック・チップを開発し、スマホ内臓のカメラによる映像情報をディープラーニングで解析し、スマホが周囲の環境を認識する。また、大手チップ・メーカーも脳を模倣したチップの開発を進めており、Qualcomm は、「スパイキング・ニューラルネット（Spiking Neural Network）」を実装したニューロモーフィック・チップを開発[84]している。スパイキング・ニューラルネットは、従来のニューラルネットに時間的パルスを付加したものであり、従来のチップ（CPU）が不得意であった物体認識、不完全な情報の処理、雑音の多い環境下での情報抽出等を効果的に行うチップである。米国防高等研究計画局（DARPA）もシナプス（SyNAPSE[85]）プロジェクトを立ち上げ、スパイキング･ニューラルネット型のニューロモーフィック･チップの開発を進めている。同プロジェクトには米 IBM の Almaden 研究所や Watson 研究所、米 Hughes Aircraft 社の HRL 研究所などが参加している。

(3) 企業による人工知能分野への取組

昨今の人工知能の進展の動きを受けて、米国等を中心に情報通信関連企業（ICT 企業）では、人工知能の技術開発と実用化に向けた取組が活発化している。こうした動きは、IoT によるデジタルデータを含め、所謂ビッグデータからユーザーにとって付加価値を生み出す情報分析技術の競争力が ICT 企業の競争力の差別化[86]につながるからである。また、ICT 企業以外でも人工知能の活用に関する研究開発に取り組む動きも見られる。

以下には、最近の ICT 企業等による人工知能に関する取組み[87]を概説する。

① IBM

IBM による人工知能に関する技術開発への取組は、現在の IBM の事業戦略であるコグニティブ（認知）コンピューティング[88]の推進の柱の一つとなっている。ニューヨー

---

[82] 小林雅一「AI（人工知能）にかける米シリコンバレーと Google の野望－危機に晒される日本の産業用ロボット」（株式会社 KDDI 総研）（2014 年 5 月）（http://www.kddi-ri.jp/article/RA2014005）

[83] TERADEEP（http://www.teradeep.com/）

[84] Qualcomm、Qualcomm Zeroth is advancing deep learning in devices（https://www.qualcomm.com/news/onq/2015/03/02/qualcomm-zeroth-advancing-deep-learning-devices-video）

[85] SyNAPSE ：Systems of Neuromorphic Adaptive Plastic Scalable Electronics

[86] 米調査会社は、人工知能市場は世界規模で 2014 年の 62 億ドルから 2019 年までに年率 20%近い成長により 153 億ドル規模まで伸びると予測している。また、2024 年までにはエキスパートシステムが約 124 億ドル、自律型ロボットが 139 億ドルの市場規模になると予測している。（出所）独立行政法人情報処理推進機構「IPA ニューヨークだより　米国における人工知能に関する取り組みの現状」（2015 年 2 月）

[87] 本節では、各社公表資料、報道資料を参考にビッグデータの情報分析に係る人工知能に関する技術開発や実用化動向を記載する。ビッグデータの対象は、必ずしも IoT に限定していない。

[88] IBM、Watson HP（http://www.ibm.com/smarterplanet/jp/ja/ibmwatson/）

ク・マンハッタンにあるシリコンアレーに、人工知能 Watson の開発を手掛ける Watson Group のグローバル本部を開設し、コグニティブコンピューティングの進展に向けて、Watson 事業に 10 億米ドルを投資することを発表している。IBM は、Watson のグローバル本部の建設と並行して、25 カ国以上でコグニティブコンピューティングの事業を展開している。

IBM は、ダブリンとロンドン、メルボルン、サンパウロ、シンガポールの世界 5 都市に Watson Client Experience Center を開設する計画[89]も明らかにしている。同センターでは、アプリケーションの学習アルゴリズムを適用する方法について、Watson に精通した研究・設計チームがアドバイスを提供する予定である。IBM は、Watson を中心としたコグニティブコンピューティング関連事業を加速するため、グローバル本部の開設と合わせ、国内外の研究者やパートナー企業、クライアント、開発者、学者、ベンチャーキャピタリスト等とも世界的なネットワークの構築に取り組んでいる。

Watson[90]は、2011 年のクイズ番組 Jeopardy！で人間のチャンピオンに勝利するなどの取組みを通じて社会的認知が進み、Watson の質疑応答エンジンは、医療や小売業など、様々な分野に採用されはじめている。IBM は、過去には、1997 年には Deep Blue により人間のチェスチャンピオンに勝利するなど、人工知能の研究開発成果を分かりやすくプロモートすることで、人工知能分野における IBM のリーディングカンパニーとしての認知向上に成功している。

IBM は、Watson をベースとした新しいサービスを 3 種類発表している。Watson Analytics は、自然言語処理によるトレンド分析、Watson Discovery Advisor は、医薬品や出版物のリサーチ機能の簡易化と向上の実現、Watson Explorer は、ビッグデータの処理向けにデータ主導型のダッシュボードや開発フレームワークを提供する。こうした機能は、IBM の特定アプリケーション向けビッグデータ処理向けのハードウェア・ソフトウェアシステムである PureData System 等で稼働し、IoT 等、データ量が膨大、非構造データなどの場合、Hadoop による分散処理機能を持つ PureData System for Hadoop が利用されると見られる。

Watson の実用化に向けた取組の事例[91][92]も増えつつある。米オースティンの観光局 Austin Convention ＆ Visitors Bureau は、Watson を活用したトラベルサイト WayBlazer を運用して、Watson の学習機能や、自然言語インタフェースによる映像を交えたアドバイス機能を検証している。オーストラリアの ANZ Global Wealth 銀行は、Watson Engagement Advisor ツールをベースとしたアプリケーション開発に取組み、従来数週間を要していた

[89] IBM、世界規模で加速する IBM Watson の採用（http://www-06.ibm.com/jp/press/2014/10/0801.html）

[90] クイズ番組「Jeopardy！」に勝利した Watson は、ライトウェイト・オントロジーの研究成果や機械学習を組み合わせによるものである。IBM は、ディープラーニングの研究開発や企業買収も進めており、今後、IBM の人工知能に関するシンボル名称（コア・プラットフォーム）である Watson の機能にディープラーニングが取り込まれ、能力強化が図られると見られる。

[91] Watson の活用事例や活用に向けた事例は、各社発表、報道等で公表・報道されている。Watson の活用事例は、特定の技術や製品の活用というよりは、Watson ブランドとして IBM が提供する一連の人工知能関連技術やプラットフォームの活用事例である。

[92] IBM、IBM Watson Accelerates Global Expansion （ https://www-03.ibm.com/press/us/en/pressrelease/45022.wss）

財務アドバイス報告書を、短期間でクライアントに届けることを目指している。南アフリカの医療保険会社 Metropolitan Health は、Watson Engagement Advisor の導入を進め、膨大な非構造化データの中から、300 万人の顧客の個々のニーズに対応した情報を提供することを目指している。また、オーストラリアの Deakin 大学は、学生へのアドバイスの提供に Watson を活用する計画を持ち、5 万人の学生一人一人に対応したアドバイスを Web 上で行う。この他、英国の Red Ant の製品情報やマニュアル、カスタマーレビューのデータをもとにした購買層や購買履歴、ターゲット価格などの分析、米国の Reflexis による顧客サービス向上のための店舗マネジャーに対するリアルタイムな注意等への Watson の活用等が報告されている。また、スペインの CaixaBank と提携し、Watson に第二言語としてスペイン語を学習させるなど、英語圏以外での Watson の活用を進める動きも見られる。日本国内では、みずほ銀行と共同で音声データをテキスト化する音声認識技術、および IBM の保有する Watson テクノロジーや関連技術を組み合わせて、コールセンターや銀行窓口でのお客さま対応等で有益な情報を提示するシステムを共同構築することに合意するなど、様々な産業分野で Watson の活用が始まっている。

IBM は、人工知能による情報分析技術の開発と並行して、専用のチップの研究開発にも取り組んでいる。2008 年から Cornell Tech、iniLabs, Ltd.等と共同で、米国防省国防高等研究計画局(DARPA)による SyNAPSE プログラムにより、ニューロン（脳神経細胞）の働きを模したプロセッサ「ニューロシナプティック・コンピュータ・チップ」の開発に取り組んでいる。2014 年 8 月には、CMOS チップの中でも最大級といえる 54 億個のトランジスタを備え、これらが 100 万個のニューロン、2 億 5600 万個のシナプス（ニューロン間結合）の働きをシミュレートするチップ [93]の開発に成功したことが発表 [94]された。

開発されたチップは、必要な箇所だけニューロンを稼働させるため、通常の汎用マイクロプロセッサより消費電力を抑えられ、生物と同じ時間軸でニューロンやシナプスを動作させた場合、消費電力は 70mW 程度に止まる。さらに、IBM はチップの開発と並行して、アプリケーション開発に必要なシミュレータ、プログラミング言語、サンプルのアルゴリズムやアプリケーション、ライブラリ、教材などを開発している。

IBM は長期的なゴールとして、100 億ニューロン、100 兆シナプスのシステムの開発を目指し、消費電力は 1kW、体積は 2 リットル以下を目標としている。こうした技術は、公衆安全、視覚障害者支援、健康モニタリング、自動運転などへの応用が想定されている。

② Google

Google は、検索エンジンを無料で提供し、オンライン広告で利益を上げるビジネスモデルで成長した ICT 企業である。Google は、1998 年創業の企業であるが、時価総額は

[93] チップは韓国サムスン電子の 28nm プロセスで製造されている。
[94] IBM、新しい IBM SyNAPSE チップを発表（www.ibm.com/jp/press/2014/08/0801.html）

トヨタ自動車の 2 倍の規模の世界第 2 位の巨大企業となっている。

Google は、Google X[95]と呼ばれる次世代技術開発プロジェクトを進め、Google グラス（拡張現実メガネ）、自動運転、音声認識など多数の研究に取り組んでいる。近年は、自動運転や音声認識等、人工知能技術に係るテーマが重点的に取り組まれ、Google は、最高水準の人工知能技術を有する企業となっている。2012 年には、米 Stanford 大学との共同研究で、1,000 台のクラスタ・マシンにより、YouTube の動画からランダムに抽出した 1,000 万枚の画像を用いて 3 日間をかけた教師なし学習により人や猫の顔に強く反応する人工ニューロンの作成に成功した。人間が事前に人や猫の顔の画像をまとめたり、画像にラベルを付けたりすることなく、人工知能が自律的に認識性能の高い機械学習を実現できた例として知られている。また、近年は、人工知能や人工知能を搭載したロボット等、人工知能に関連する多数の企業買収を積極的に進めている。

表 4-1　Google による人工知能・ロボット等の企業買収動向

年月	企業名	所在	概要
2013 年 3 月	DNNresearch	カナダ	ジェフリー・ヒルトン氏のニューラルネットワーク企業
2013 年 10 月	Flutter	米国	ジェスチャー認識アプリケーションの提供
2013 年 12 月	Schaft	日本	作業用の人間ロボットの開発
2013 年 12 月	Industrial Preception	米国	物流など向けロボットアームの開発
2013 年 12 月	Redwood Robotics	米国	物流など向けロボットアームの開発
2013 年 12 月	Meka Robotics	米国	人型コミュニケーション・ロボットの開発
2013 年 12 月	Holomni	米国	物流など向けキャスター（車輪）の開発
2013 年 12 月	Bot & Dolly	米国	映像向けロボットアームの開発
2013 年 12 月	Autofuss	米国	Bot & Dolly の関連会社である映像作成企業
2013 年 12 月	Boston Dynamcs	米国	災害や軍事向け 4 足走行ロボットの開発
2013 年 12 月	Nest Labs	米国	知的な家庭用サーモスタットなどの開発
2014 年 1 月	DeepMind Technologies	英国	ゲームやシミュレーション向けの AI 開発
2014 年 4 月	Titan Aerospace	米国	災害や軍事向けの無人飛行機の開発

（出所）総務省「平成 26 年版情報通信白書」から作成

Google が買収したディープラーニング関連企業の一つは、ディープラーニング研究の第一人者である Toronto 大学の Hinton 教授によるニューラルネットワーク関連の研究開発企業 DNNresearch である。また、2014 年にはイギリスのディープラーニング企業 DeepMind Technology[96]を買収した。DeepMind Technology は優れたディープラーニング研究者を擁していることから、DeepMind Technology の買収競争に Google や Facebook などのインターネット企業が参画し、6 億 5000 万ドルで Google が買収に成功した。DeepMind の技術は、Google の検索エンジンに搭載され、利用者の意図を学習した上での最適な情報提示、YouTube の推奨機能、モバイル音声検索機能などに適用される予定である。

また、Google はロボット企業や IoT 関連企業の買収にも積極的であり、4 脚ロボット

[95] Bloomberg Business Inside Google's Secret Lab(May 22, 2013)
（http://www.bloomberg.com/bw/articles/2013-05-22/inside-googles-secret-lab）
[96] Google DeepMind（http://deepmind.com/）

や軍備輸送用ロボットなどを開発する Boston Dynamics、ヒト型の二足歩行ロボットを開発した日本企業である Schaft を買収するなど、多数のロボット会社を買収している。今後、こうしたロボットに洗練された人工知能が搭載される可能性もある。

Google は、Web サービスやスマートフォンサービスに留まらず、ロボット、家電、自動車等、ネットにつながる全てのモノ（IoT）をビジネスの対象としており、それを支える人工知能の強化を急いでいる。Google の人工知能に関連する研究は、ディープラーニング等のソフトウェアの技術開発に限らない。2014 年には、California 大 Santa Barbara（UCSB）の John Martinis の率いる研究チームが Google の量子コンピュータ研究プロジェクトに参加した他、量子コンピューティングの研究にも積極的であり、NASA や USRA（Universities Space Research Association）の量子人工知能研究所と協力して、推論プロセッサの開発を進めるなど、新たなコンピューティングの研究開発にも取り組んでいる。

③ Microsoft

Microsoft は、既に人工知能を様々な製品機能として市場投入している。2014 年 11 月には、人工知能による重要メール識別機能 Clutter を Office 365 で提供開始することを発表している。Clutter は、Office 365 for Business の利用者向けの機能であり、人工知能により、最重要メールを識別、分類する。重要メールの識別には、Microsoft の Office Graph 技術が利用され、ドキュメント共有、頻繁な利用、オフィス内の様々な人間関係やアクティビティのつながりを機械学習で学習し、メールが振り分けられる。

Microsoft の人工知能活用は、Clutter のようなオフィスツールの利便性を高めるといった機能に止まらず、IoT 向けのサービスにも展開されている。Microsoft は、2014 年 4 月に Microsoft Azure Intelligent Systems Service という新たなクラウドサービスの提供を開始した。このクラウドサービスは、IoT を前提として、センサや端末からマシン生成データを取得し、管理することが可能となる。実際には、Windows Azure 上に構築した Hadoop ベースの HD Insight やビジネスインテリジェンスサービス Power BI 等を利用して、Azure Intelligent Systems Service からデータの取得や分析ができるようになる。この分析機能に Microsoft が 2014 年 6 月に公表した Microsoft Azure Machine Learning を応用することが可能である。これにより、過去のデータ分析だけでなく、過去のデータを学習し、それをベースに将来予測を行うことができる。Microsoft Azure Machine Learning は、Microsoft の機械学習の研究成果をクラウドサービス化したものであり、E コマースの監視や、顧客分析・予測、信用リスク予測、機器の故障予測に応用でき、IoT 分野にも応用できるとしている。Microsoft Azure Machine Learning は、機械学習のモデル作成・モデルの評価～作成した分析モデルの利用、環境（Web サービス）まで、機械学習の開発～サービス提供で必要となるすべてのコンポーネントを PaaS により提供する。

Microsoft Azure Intelligent Systems Service と Microsoft Azure Machine Learning を IoT 分野で応用した事例として、竹中工務店と日本マイクロソフトによるオフィスビルなどの

環境を最適にするサービスがある。このサービスは 2015 年に開始される予定で、空調設備などのデータを蓄積・分析して、自動で対応を指示することにより管理担当者の負荷軽減や制御の最適化を実現する。システムには、データ形式や順番の既定、形式変更やフィルタリングの機能を持つ Azure Intelligent System Services と、機械学習機能を提供する Azure Machine Learning Service が使用され、空調の設定変更の最適化や、高度な自動化が実現する。

④ Facebook

Facebook は、2013 年に、New York 大学の Yann LeCun 教授を所長に招き人工知能研究所を設立した。2014 年には、人工知能のベンチャー企業 Vicarious 社に対し、約 4,000 万ドルの投資を実施した。また、Facebook の人工知能の研究施設には、New York 大学の Fergus 氏、Google が買収した DNNresearch の元メンバーである Ranzato 氏などが所属している。Facebook の人工知能の研究施設はニューヨーク、カリフォルニアのメンローパーク、イギリスのロンドンに所在し、機械学習やコンピュータの視覚情報処理機能に関する研究が行われている。その成果はユーザーがアップロードした画像やテキストの分析等での活用が想定されている。

2014 年 3 月には、97.25%という高い認識率で個人の顔を認識することができる技術 DeepFace[97]を開発したことを公表している。DeepFace は画像をそのまま学習していくのではなく、画像から 3 次元の顔の形状を推定し、1 億を超えるパラメータを持つネットワークに学習させることによって個人を特定する特徴を自ら生成している。DeepFace は、Facebook 等の SNS に自由に投稿される画像全てから個人を特定できる高性能な画像認識の実現を目指している。DeepFace の技術は、カメラ等の画像による個人特定にも応用できるため、様々な IoT 分野の応用も期待できる。

Facebook はディープラーニングを扱うオープンソースのフレームワーク Torch のためのモジュールを公開している。Torch には複数のディープラーニングのアルゴリズムが導入されている。Facebook が、自社の研究成果を公表する背景には、Facebook は成果をオープンにすることで、オープンなコミュニティと人的ネットワーク形成により、企業買収と人材獲得で先行する Google に対抗する方策を選択していると考えられる。

⑤ Amazon

Amazon は、2014 年 11 月に音声アシスタント機能を搭載したスピーカーAmazon Echo[98]を発表している。Amazon Echo はインテリジェントな家電で、音声で操作することができる。利用者が質問すると音声で回答する。Amazon Echo は、家庭内でモノがインターネットに繋がれた IoT の事例であり、ユーザーとのインタフェースとして言語解析技術

[97] Facebook（https://research.facebook.com/）
[98] Amazon（http://www.amazon.com/oc/echo/）

が重要となる。Echo では、2012 年に Amazon が買収した英国企業 Evi の持つ知識ベースとセマンティック検索技術が応用されていると見られる。

Amazon の人工知能活用は、音声認識、自然言語処理に限らない。同社は、米連邦航空局（Federal Aviation Administration : FAA）による許可が出れば、ドローン（無人飛行機）を利用した配送サービス（Amazon Prime Air[99]）を開始すると見られる。FAA は、2015 年 1 月に報道機関である CNN とドローン利用に関する研究協定を結び、ジャーナリズムでのドローン使用の研究に許可を出したことから、将来的に Amazon によるドローン配送の可能性も高まっている。無人飛行するドローンには、飛行制御の正確性と安全性が求められる。そのため、飛行制御に関するソフトウェアの高度化が必要となっている。こうした飛行制御のソフトウェアは、自動操縦や障害物を判断して避けるなどの高度な判断が必要であり、広義な意味で人工知能が応用されると考えられる。

⑥ Baidu

人工知能に関する研究開発に積極的な取組を行う IT 企業は、シリコンバレー企業だけに限らない。中国の検索大手 Baidu は、2013 年にシリコンバレーにディープラーニングの研究所を設立し、2014 年には、Stanford 大学の Andrew Ng 教授を研究所長に迎え入れ、300 億円の研究開発投資と約 200 人の雇用計画を発表した。Ng 氏[100]は Stanford 大の人工知能研究チームのリーダーで、ニューラルネット研究の第一人者の一人である。Baidu は北京にも人工知能の研究所を開設し、検索サービスの向上につながる画像認識や音声認識、自然言語解析、機械翻訳などの研究に取り組んでいる。Baidu の研究は、検索サービスの高機能化に止まらず、自律走行型の自転車の開発等、IoT 分野への人工知能の応用も含まれている。

⑦ 日本電信電話株式会社（NTT）

NTT は、ビッグデータ解析などの技術分野で、NTT グループ内の複数研究所が連携する研究組織「機械学習・データ科学センター」[101]（MLC）を 2014 年 4 月に設立し、人工知能の実用化の取組を本格化した。同センターの規模は、30 名程度で、外部企業や大学機関との連携により技術開発を進める予定である。NTT は、Preferred Infrastructure と共同で、リアルタイムに膨大なデータを高速・分散処理できるオープンソースソフトウェア Jubatus[102]を開発し、ツイッターのリアルタイム分析や映像データ、全地球測位システム（GPS）、交通・流通のデータと関連づけにより震災時の行動パターン分析への応用を検討している。IoT 分野の分析では、リアルタイム性が求められる場合も多く、その効果が注目される。通信サービスを提供する NTT では、音声認識や機械翻訳分野での機械

[99] Amazon、Amazon Prime Air（http://www.amazon.com/b?node=8037720011）
[100] インターネット上で受講できる大規模なオープンな講義である MOOCs （Massive Open Online Courses）の代表的なプラットフォームの一つである Coursera の共同創業者でもある。
[101] NTT コミュニケーション科学基礎研究所、機械学習・データ科学センタ（http://www.kecl.ntt.co.jp/mlc/index-j.html）
[102] 日本電信電話株式会、Jubatus （ユバタス）（http://www.ntt.co.jp/RD/hotkeywords/vol3_jubatus_part1.html）

学習の応用に積極的である。同社では、大学の講義など難しい専門用語を含む音声データでも正確に文字情報として処理することができる音声処理技術に取組み、同分野でもビッグデータ分析や機械学習技術が応用されている。

⑧ ソフトバンク

ソフトバンクは、米 IBM と共同で人工知能型コンピュータ Watson の日本語対応版を開発し、2015 年にも事業展開する方針を打ち出している。Watson の対応言語は英語であるが、今後日本語、スペイン語、ポルトガル語の対応を優先的に進めることが計画されており、日本語版の開発では、ソフトバンクと共同により翻訳やデータ出入力といった日本語にかかわるシステム基盤の構築が行われる予定である。また、IBM は、ソフトバンクとロボット分野で協業することも発表し、ソフトバンクが提供するパーソナルロボット Pepper への人工知能コンピュータ技術の応用が検討されると予想される。

⑨ ヤフージャパン

ヤフージャパンは、IoT 向けの SDK やデータベース、解析、ID といったバックグラウンド環境をサービスとして提供する仮称「Yahoo! IoT プロジェクト」を進めている。同社では、IoT の付加価値を生み出す、IoT のバックエンドの機能を BaaS（Backend as a Service：ユーザーの登録や管理、データ保管といったバックエンド環境のサービス）として提供する予定である。さらに、IFTTT（if this then that）（ウェブサービスを連携して利用できるようにするサービス）を例に挙げ、バックグラウンドで複数のサービスが連携できる仕組みも提供していくことを公表している。同社では、IoT 向け BaaS を当面無料で提供していく予定である。

⑩ 日立製作所

日立製作所は 2016 年度以降の研究開発費を 5,000 億円程度に拡大し、センサや人工知能、ロボット等に集中投資することを発表している。日立はビッグデータ解析など高度 IT と社会インフラ事業を融合したビジネス開拓を進めており、中核技術となる人工知能、センサ、ロボット、セキュリティなどへの開発投資を 3 倍に増やす方針を打ち出している。その内容は、センサ技術や人工知能による鉄道車両や太陽電池モジュールの劣化状況のモニタリングによる設備稼働率向上や抑制技術開発、センサによる店舗内の顧客の行動パターン把握による店舗業績向上が含まれる。

⑪ ドワンゴ

ニコニコ動画などのサービスを提供するドワンゴは 2014 年 11 月にドワンゴ人工知能研究所 [103] を発足し、所長に株式会社富士通研究所の山川宏氏が就任した。同研究所は、

[103] 株式会社ドワンゴ、ドワンゴ人工知能研究所（http://ailab.dwango.co.jp/）

産学官により教育、エネルギー、環境、水資源、食糧、貧困、セキュリティ等の社会課題解決に貢献が期待される人工知能に関する研究を推進する予定である。また、人工知能の若手研究者のレベルアップを企図した NPO 法人全脳アーキテクチャイニシアティブが 2015 年中に設立され、ドワンゴ人工知能研究所が事務局として機能することが発表されている。

⑫ Preferred Networks

自然言語処理技術を利用した研究開発、検索・データ解析製品を提供するベンチャー企業である株式会社 Preferred Infrastructure[104]は、2014 年 10 月に IoT 時代に向けた次世代ビッグデータ技術基盤の確立を目指した株式会社 Preferred Networks を設立[105]した。Preferred Networks では、IoT の課題であるデータ量と種類の爆発に対応するため、エッジヘビーコンピューティング技術、分散インテリジェンス技術、機械学習、ディープラーニング、映像解析技術等の独自技術により、IoT 時代に相応しいコンピュータ、ネットワークアーキテクチャを確立することを目指している。Preferred Networks では、Preferred Infrastructure が NTT の研究所と共同開発したビッグデータ処理基盤 Jubatus を IoT に対応させ、小売、広告、自動車、安全・防犯、ネットワークセキュリティ・帯域制御、製造、公共交通機関、ヘルスケアの分野で外部企業と共同開発・事業提携を進めることを公表している。

⑬ リクルート

リクルートホールディングスは、2015 年 4 月に新規事業開発機関 Recruit Institute of Technology を再編した人工知能研究所の設置を発表[106]した。同研究所では、人工知能分野の世界的権威 Tom M. Mitchell 氏（米 Carnegie Mellon 大学教授）、Oren Etzioni 氏（Allen Institute for Artificial Intelligence CEO 元・米 Washington 大学教授）、 David M. Blei 氏（米 Colmbia 大学教授）をアドバイザーに迎え、人材領域・販促領域を中心としたグローバル規模の人工知能に関する研究を行い、産業界と生活者を結びつけるマッチングサービスの実現を目指している。また、同社では、米 Massachusetts Institute of Technology メディアラボとの共同研究、米 Stanford 大学と自然言語処理に関する共同研究を行う他、人工知能分野の研究人材の採用を積極的に行い、世界各国の有識者の指導のもとでの研究推進に着手している。

---

[104] 第 6 節に Preferred Infrastructure 岡野原氏のインタビューを掲載した。
[105] 株式会社 Preferred Infrastructure 株式会社、Preferred Networks 設立（https://preferred.jp/news/2835/）
[106] 株式会社リクルートホールディングス、ホールディングスプレスリリース
（http://www.recruit.jp/news_data/release/2015/0415_15754.html）

⑭　国立情報学研究所

国立情報学研究所（大学共同利用機関法人情報・システム研究機構）では、細分化された人工知能分野の再統合を企図した研究活動「ロボットは東大に入れるか」プロジェクト[107]を進めている。同プロジェクトでは、2016 年度までに大学入試センター試験で高得点マーク、2021 年度に東京大学入試の突破を目標に置き、2014 年には、全国の私立大学 8 割にあたる 472 大学の合格可能性が 80%以上の A 判定の結果を出すなど人工知能研究の発展と同時にその可能性を広く社会に示している。同プロジェクトには、国立情報学研究所の他、大学、ICT 企業等が参加している。

[107] 国立情報学研究所、ロボットは東大に入れるか（http://21robot.org/）

4.3 IoT 時代の情報処理基盤、人工知能の展望、課題

(1) IoT 情報処理基盤の展望と課題

① 活発化する IoT 情報処理基盤提供の動き

4.1 節で示したように、IoT の進展を見込み、主要な ICT 企業は IoT 向け情報処理基盤をビジネスの主戦場と捉え、その提供に力を入れている。IoT の活用を進める企業では、IoT で処理する情報の量や処理のリアルタイム性、分析技術の深度等に応じて必要となる情報処理基盤の選択・導入を進めていくと見られる。また、IoT の情報処理基盤の導入にあたっては、IoT に係るデータ管理の仕組みも重要となるため、システム的な機能の観点と同時に、データマネージメントの機能が情報処理基盤の選択・導入における差別化要素になると見込まれる。

ICT 企業が IoT 向け情報処理基盤の提供を新たなビジネス機会と捉える一方、IoT 活用を進める企業は、IoT 向け情報処理基盤を自らの競争力強化のための新たな事業基盤と捉えている。そのため、特定分野の IoT 向け情報処理基盤を自ら開発提供する動きも見られる。産業機器の製造を担う GE は、Industrial Internet の実現に向けた取組を進め、産業機器を対象とした IoT 向け情報処理基盤である GE Predix[108] を提供することで製造機器分野における IoT 関連ビジネスの覇権を狙っている。こうした動きの背景には、産業機器や自動車をはじめ、膨大なデバイス（モノ）がネットワークにつながる中、今後、ハードウェア（モノ）単体からソフトウェア・サービスを融合したビジネスが成長すると見込まれ、その事業基盤として IoT 向け情報処理基盤が不可欠であることが挙げられる。今後、産業機器分野以外でも、様々な分野において IoT に関連するビジネスの覇権を狙った IoT 向け情報処理基盤の提供の動きが登場する可能性もある。

また、IoT 向けの情報処理基盤をクラウドサービスにより提供する動きも見られる。例えば、米 Jasper Technologies[109]は、大手企業を含む 2,000 社以上の企業に IoT 向けの情報処理基盤をクラウドサービスとして提供している。また、ベンチャー企業の米 Mode[110] は IoT デバイス用のバックエンドシステムを BaaS（Backend as a Service）として提供し、接続 IoT デバイス数が少ない場合、無償利用できるため、独自の IoT 向けの情報処理基盤を持たない/持てないベンチャー企業等によるトライアル的な活用等が可能である。今後、IoT 向け情報処理基盤は様々な形態で提供されると予想され、IoT の活用を進める企業が導入する IoT 向け情報処理基盤の選択肢が増えると見込まれる。

② 重要となる標準化・相互接続性

IoT に係るビジネスにおいては、多様な機器の IoT 向け情報処理基盤への接続が求められる。そのため、機器と情報処理基盤間のデータの送受信に係る接続の標準化が重要となる。こうした標準化の動きは第 1 部 3.1 節に示したとおりである。また、IoT に係る

[108] GE Predix については、第 1 部 2.2 節の GE「Industrial Internet」参照。
[109] Jasper Technologies（https://www.jasper.com/）
[110] MODE（http://www.tinkermode.com/）、Mode, Inc.の創業者/CEO は上田学氏。

ビジネスでは、業界横断的なデータの接続が新たなビジネスを生み出す可能性もある。そのため、異なる IoT 向け情報処理基盤同士の接続の必要性が生じると考えられる。昨今の急速な IoT に係るビジネスの立ち上がりを踏まえると、こうした標準化や情報処理基盤間の相互接続性確保に関する取組みが遅れると、円滑な機器接続の障害、IoT 向け情報処理基盤の乱立等により、将来的に IoT に係るビジネス発展の阻害要因になる可能性もある。

③ ソフトウェア比重の増大

IoT においては、自動運転車、ウェアラブルデバイス、センサ等の最先端のデバイス等のモノに目が向きがちであるが、それらの最先端デバイスの機能はソフトウェアにより実現されている。また、IoT の活用における付加価値は、ソフトウェアにより実現された機能とネットワークで繋がった IoT 向けの情報処理基盤により生み出される。そのため、モノのインターネットである IoT の時代においては、従来にも増してソフトウェアの重要性と比重が高まると見込まれる。モノの機能がソフトウェアにより実現されると考えれば、ネットワークの構成や制御がソフトウェアにより実現されるソフトウェアディファインドネットワーク（Software Defined Network: SDN）と呼ばれるように IoT 時代のモノはソフトウェアディファインドデバイス（Software Defined Device: SDD）という言い方で呼ばれ、モノの機能がソフトウェアによりダイナミックに制御される時代が来るのかもしれない。

④ セキュリティへの対応

IoT 時代においては、モノや情報が繋がるため、これまでにはない利便性やサービスの高度化、効率化といったメリットが生み出される。その一方、セキュリティリスクやプライバシーリスク等が取り扱う範囲が広がることが予想される。そのため、IoT 向け情報処理基盤においてもセキュリティに係る懸念に対応していくため、仕組みや機能が必要となる。IoT の推進においてもセキュリティの確保が最大の障害であるとの意見もある中、IoT のセキュリティの全ての課題が ICT 技術だけで解決されるわけではないが、IoT 向けの情報処理基盤においては、デバイス、ネットワーク、クラウド、その上で稼働するソフトウェアやアプリケーション、ストレージ・データ管理等において適切なセキュリティ対策とそのための技術開発等の取組みを進めていくことが求められる。IoT 時代のセキュリティについては、第 2 部 5 節を参照されたい。

(2) 人工知能の発展への期待と課題

① 人工知能の応用分野の進展

IoT の時代には、モノの情報がインターネットに繋がり、膨大なデジタルデータが流通する。その膨大なデータから付加価値を生み出すには、新たな情報処理基盤と情報分

析技術が不可欠となる。特に、IoT 分野では、多種多様な膨大なデータの分析が必要となるため、手作業的な情報処理や伝統的な分析技術の適用には限界がある。こうした限界に対し、ディープラーニング等を始めとする人工知能関連の最新技術は、コンピュータ“自ら”（人工知能）が、データの中に存在する「特徴量」や「特徴表現」を学習することに成功し、分析者の知見や経験に依存する従来の分析技術の限界をブレークスルーする可能性を示している。こうした技術が登場した背景には、人間では処理できない多種多様かつ膨大なデジタルデータの分析の必要性が顕在化したことに併せ、インターネットの進展や IoT の登場により人工知能の学習に必要な膨大なデータの収集が可能となり、その学習に必要な情報処理を行うための強力なコンピュータ利用環境が実現されたことが挙げられる（図 4-4 参照）。IoT の拡大・進展やコンピュータ性能向上を考えると、その環境が一層充実すると予想され、人工知能の進化・進展も加速すると予見される。

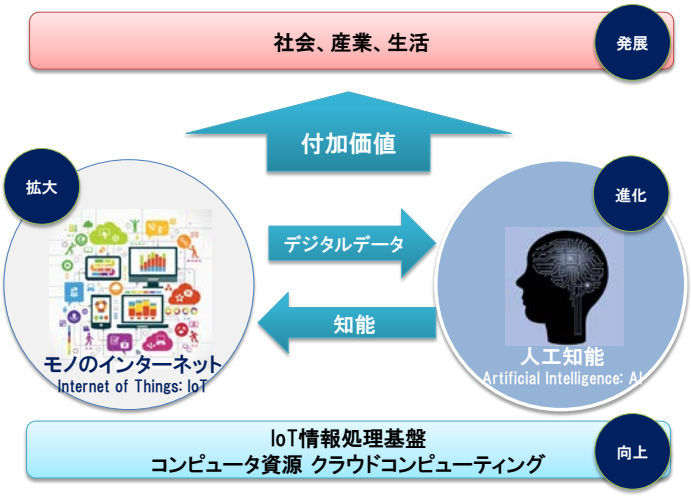


図 4-4　IoT と人工知能の進化・発展 [111]

（出所）みずほ情報総研作成 [112]

人工知能研究者である東京大学の松尾氏は、「特徴表現学習の一つの手法」としてのディープラーニングがすごいというよりも、特徴表現学習ができるようになったその先に広がる人工知能の可能性 [113]の広がりの大きさの重要性を指摘している。同氏は、今後の人工知能の技術発展と応用の可能性について、画像・音声認識や診断に続き、行動予測や環境認識による防犯・監視、自律的な行動計画による自動運転や農業の自動化や物流の高度化等を挙げ、将来的には、家事・介護、教育、秘書、ホワイトカラー支援を人工知能の応用分野に広がる可能性に言及している。

[111] IoT の拡大・発展と人工知能の進化は一つのエコシステムを形成している。
[112] IoT のイメージに関する図の出所は、European Commission, Digital Agenda for Europe The Internet of Things（http://ec.europa.eu/digital-agenda/en/internet-things）
[113] 松尾豊、「角川 EPUB 選書 人工知能は人間を超えられるか　ディープラーニングの先にあるもの」（2015）（KADOKAWA）

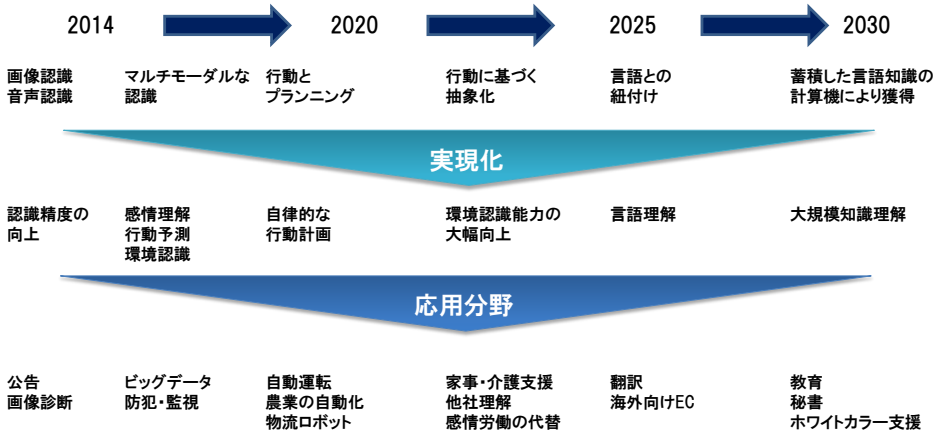


図 4-5　人工知能の技術進展と応用分野の広がり

（出所）総務省情報通信政策研究所「インテリジェント化が加速する ICT の未来像に関する研究会
東京大学松尾豊氏説明資料をもとにみずほ情報総研作成

IoT と人工知能の組み合わせは、デジタル空間の中で進展してきた情報通信技術の活用をモノと人を含めた実世界における情報通信技術の活用へと拡張するものである。こうした発展は、従来の情報通信技術が創りだしてきた情報通信社会の姿を超えて、人、モノ、情報の全体がネットワーク化され、情報通信技術により最適化された新たな情報通信社会を創りだす可能性が高い。

人の行動や生活の利便性を高め、産業活動を効率化してきた情報通信社会から、IoT と人工知能の組み合わせにより、人の行動や生活の利便性を高め、産業活動の効率化を図るだけでなく、その質を本質的に高め、産業活動が新たな付加価値を生み出す情報通信社会の新たな時代の到来が近づいている。

②　人工知能の進展に関する課題

人工知能の技術進展と応用分野の広がりへの期待が高まる一方、人工知能の進展に対するリスクや課題を指摘する意見もある。以下には、人工知能の発展に係る懸念として、下記の 4 点を取り上げる。

1)　シンギュラリティ（技術的特異点）の可能性

第 1 の懸念は、人工知能が人類の知能を超える人工知能に関するシンギュラリティ（技術的特異点）に対する懸念である。

半導体の性能向上が 1 年半ごとにその処理速度と記憶容量を 2 倍ずつ高めるムーアの法則に従うと想定すると、今後、コンピュータは知能水準を上げ、2045 年頃には人間の知能を超える可能性が予見されている。他方、生物進化のスピードは、その速度に比べ相対的に遅いため人類がコンピュータと競うことは難しく、人工知能の進化により、人類の地位がコンピュータに奪われる懸念を指摘する意見がある。こうした懸念は、過去

の産業革命や技術革新が登場した際に、新たな技術や機械が、仕事や活動を脅かす[114]といった懸念に近い。しかしながら、こうした人工知能の進展に対する懸念を主張する見解においては、人工知能の進化が、従来の技術革新と異なる点として、従来の技術革新が、人類が制御可能な技術のイノベーションであったのに対し、人工知能の場合、コンピュータ自体による自律的な知能水準の進化が想定されるため、人類による制御が難しい技術となる可能性がある点を挙げている。他方、こうした懸念に対し、現状の人工知能の能力は人間を脅かす水準になく、過度な危険性を懸念することは人工知能の研究を阻害するとの意見もある。人類は過去も技術的なイノベーションによる社会変革を経験しており、イノベーションを社会として受け入れることで、経済や社会の発展を図ってきた歴史を持つ。そう考えると、ディープラーニングという革新的な人工知能の実用性と新たな発展の可能性が具現化しつつある中、人工知能の活用に関するリスクや課題を整理した上で、人工知能を経済や社会の発展に効果的に生かしていく方策を考えることが必要であろう。

2) 人工知能の産業競争力に対するインパクト

第 2 の懸念は、人工知能の産業競争力に対するインパクトの大きさへの懸念である。

人工知能の技術進展と応用分野の広がりが見込まれ、人工知能の技術水準が産業競争力に直結すると予見される。今後、IoT が本格化する中、膨大なデータから付加価値を生み出す人工知能が、インターネットビジネスのみならず多くの産業の産業競争力の要になることが予見される。

前出の松尾氏は、Google や Facebook が人工知能の学習精度と売上増加が直結するビジネスモデルを構築していることへの危機感を指摘している。また、米 GE が進めるインダストリアル・インターネット構想では、産業機械・装置のモノのデータの獲得の仕組みづくりを進めており、今後、それらのデータから付加価値を生み出す分析技術として人工知能が活用されると予想される。我が国でも近年、様々な産業分野で人工知能に関する研究開発が活発化しつつあるが、諸外国による人工知能の様々な分野での実用化に向けた取組みに出遅れれば、モノを含めたデジタルデータからの付加価値創出という IoT 時代の産業競争で後れを取ることが懸念される。そのため、我が国においても産業競争力強化の観点から、人工知能の技術開発と産業応用等の実用化に対する取組み[115]を急ぐことが求められる。

---

[114] Carl Benedikt Frey、Michael A. Osborne は、「THE FUTURE OF EMPLOYMENT: HOW SUSCEPTIBLE ARE JOBS TO COMPUTERISATION?」（Oxford University）（2013）の中で、人工知能による置き換えを踏まえた上で、将来的なくなる職業と残る職業のリストを提示している。

[115] 経済産業省 産業構造審議会 商務流通情報分科会情報経済小委員会では、2015 年 5 月に「CPS（Cyber Physical System）によるデータ駆動型社会の到来を見据えた改革」と題する中間とりまとめを公表した。同とりまとめでは、IoT の進展や人工知能の高度化・自律化等による産業構造・経済社会全体の変革を踏まえ、産業競争力強化に向けた施策が打ち出されている。

3) 過熱する人工知能に関する研究開発

第 3 の懸念は、最近の人工知能に関する研究開発の過熱への懸念である。

ディープラーニングという新たな技術の登場と画像や音声認識分野での実用化の成功により、人工知能の様々な分野への適用による可能性への期待が高まっている。そのため、世界中の研究機関や情報通信関連企業や研究開発ベンチャー企業等による人工知能に関する研究開発が過熱している。人工知能に関する研究開発を振り返ると、人工知能はコンピュータが人間の知能を実現するという重要かつ夢のあるテーマであるゆえに、新たな技術が登場する度に、その技術に過度ともいえる期待が寄せられ、その実用の限界に落胆し、人工知能に関する研究全般が下火となってきた経緯がある。現在のディープラーニングという新たな技術も、現状、解決できていない課題もあり、今後何かしらの限界が出てくる可能性がないとは言い切ない。そのため、ディープラーニングを含め人工知能の可能性を冷静に受け入れた上で、実用性を検証していくとともに、一過性ではない人工知能に関する着実な研究開発を進めるという姿勢も重要であろう。

4) 人工知能の活用に関する社会的受容

最後に取り上げる懸念は、人工知能活用の社会的受容に対する懸念である。

人工知能は、今後、人による認識や判断の行為の一部を代行する機能となる可能性もある。例えば、IoT 分野の一つである自動運転[116]の運転判断に人工知能が利用されると仮定した場合、人工知能は、運転者に代わり、“意外”な進路変更の判断[117]をするかもしれない。その場合、自動走行車に乗った人は、その判断が信頼できるかに迷うであろう。仮に、人がデータや知見や経験に基づき判断してきたことを人工知能に置き換えた場合、如何に人工知能の性能が高いとしても、判断ミス（学習不足）が生じる可能性やその判断は正しいとしても利用者が納得・理解できない可能性もあり、人工知能による判断に対する漠然とした不安が残存すると考えられる。そのため、人工知能の利用においては、人工知能の技術進展を取込みつつも、その活用の限界を示すとともに、その利用により獲得する利便性や効率性等の便益と利用により発生するかもしれない万が一のリスク（例えば、人的影響や経済リスク）を考慮して、人工知能による判断への依存度を変える等、人工知能の活用方法の使い分けのルールがないと活用が広まらない可能性もある。人工知能の判断ミスは、人のミスと同じように取り扱えるのであろうか。人工知能の進展と広がりに合わせ、人工知能の現実世界の中での活用方法や理解[118]、つまり人と人工知能との上手い付き合い方[119]を、人工知能を利用する人の立場から考える必要

---

[116] 自動運転に関する動向に関しては、第 2 部 1.3 節を参照されたい。

[117] 意外な進路変更は、人が気づきにくいデータも考慮した合理的な判断である場合もあれば、学習として考慮されていない予想外のデータによる判断ミスの場合などが考えられる。何れの場合も、自動運転車に乗った人は、何故人工知能が意外な進路変更するのかが理解できないと、漠然とした不安を感じるであろう。判断ミスを犯す確率が自分より低くても、自分に理解できない判断に不安を感じるのは多分に心理的要因によるのかもしれない。

[118] 人と人工知能の間のコミュニケーションも重要な役割を果たすと期待できる。

[119] 米 Stanford 大は、人工知能による生活、仕事、コミュニケーションの変化を研究する One Hundred Year Study on Artificial Intelligence（AI100）を立ち上げている。米 Stanford 大、AI100（https://ai100.stanford.edu/） また、米

があるのかもしれない。

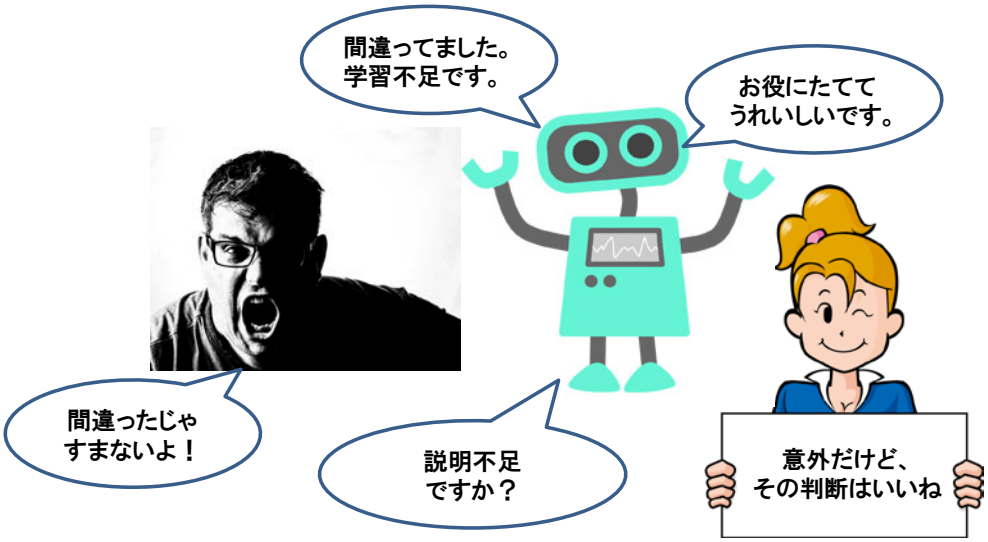


図 4-6　人工知能による判断の理解と受容

Stanford 大のロースクールでは、人工知能と法律の関係についての公開講義も行われ、人工知能に関する研究は技術研究にとどまらない。

5. IoT 時代のセキュリティ

ネットワーク通信の高速化、センサ技術の高度化、技術を組み込んだ製品の低廉化などの様々な要因を背景に、IoT（Internet of Things、モノのインターネット）が注目されている。2015 年の 1 月にアメリカのラスベガスで開催された世界最大級の IT&家電ショー2015 International CES や、3 月にスペインのバルセロナで開催されたモバイル通信機器の国際展示会 Mobile World Congress 2015 において、IoT はテーマとして掲げられており、その勢いは留まるところを知らない。

現在、全世界でインターネットに接続されているデバイスは約 90 億台。この数字は現在の世界人口である約 70 億人よりも多い。そして、自動車や家電に通信端末を組み込こんだ、いわゆる IoT（Internet of Things）にかかわる「モノ」の数は、2015 年で 250 億、2020 年には 500 億に達すると予想されている。

来るべき IoT 時代では、あらゆるモノや情報が繋がり、様々なサービスが提供されていくことが想定されている。「サービス」であるため、利便性に目が行きがちだが、その利便性とトレードオフの関係にあるのが「セキュリティ」である。前述の「Mobile World Congress 2015」において、Vodafone の Chief Executive である Colao 氏は、IoT 時代で重要となるのはセキュリティの課題であると述べている。

すでに車載の組み込み OS がハッキングされたり、防犯カメラの制御システムが乗っ取られて画像が盗まれたりしている。本節では、IoT 時代の「セキュリティ」に注目し、IoT が生む新たな脅威とその対策について考察する。

5.1 IoT におけるセキュリティの必要性

(1) セキュリティの現状

2014 年 7 月に Hewlett-Packard が、テレビ、Web カメラ、家電コントロール、玄関ドアロックなどの既に販売され普及度合いの高い IoT 製品 10 種類のセキュリティに関する調査結果を発表している。調査には同社のセキュリティサービス「HP Fortify on Demand」が利用され、調査対象製品の 70％にセキュリティ問題が見つかり、1 製品あたり 25 件の脆弱性があったと報告している。また、IoT 製品 10 種類の他に、クラウドアプリケーションやモバイルアプリケーションも調査対象となっており、半数の IoT 製品のモバイルアプリケーションが、暗号化せずクラウドやインターネット、ローカルネットワークと通信していると併せて報告している。これらを踏まえると、現状セキュリティについて、十分に検討されているとは言えない。

また、調査では、「Privacy concerns」、「Insufficient authorization」、「Lack of transport encryption」、「Insecure web interface」、「Inadequate software protection」の 5 種類の脆弱性を挙げている。各脆弱性の具体的な内容は以下の通りである。

脆弱性	内容
Privacy concerns	消費者の名前、E メールアドレス、住所、生年月日、クレジットカード情報、医療情報といった個人情報の収集に関するプライバシー問題が 80%の製品に見つかった
Insufficient authorization and authorization	パスワードの長さや複雑さに関する要求がなく、例えば、「1234」や「5678」などの安易なパスワードが利用できてしまう問題が 80%の製品に見つかった。
Lack of transport encryption	インターネットとローカルネットワークとの通信が暗号化されていない製品が 70%、モバイルアプリケーションが暗号化せずクラウドやインターネット、ローカルネットワークと通信している製品が 50%あった。
Insecure web interface	クロスサイトスクリプトの受け付け、非力なセッション管理、脆弱な証明書の標準設定、証明書情報の平文通知といった不備が 60%の製品に見つかった。
Insecure software and firmware	ソフトウェアアップデートをダウンロードする際に暗号化を使っていない製品は 60%あった。いくつかのダウンロードにおいて中断、抽出、変更ができるような状態であった。

（出所）Hewlett-Packard 「Internet of Things Research Study」をもとにみずほ情報総研和訳

Hewlett-Packard は、今後インターネットなど他と接続する IoT 製品は増え続け、比例してセキュリティ上の懸念も指数関数的に増え続けるとの見通しを示している。また、IoT 製品は消費者にとっての利便性の向上をもたらす一方で、DoS 攻撃、パスワードやクロスサイトスクリプティングの脆弱性を突いた攻撃などの危険にさらされる可能性の増加を指摘している。そのため、IoT 製品が繋がることを考慮すると、IoT 製品のセキュリティリスクを理解することが最も重要であると結んでいる。

(2) セキュリティ被害や攻撃などの具体事例

前述の通り、IoT がもたらす利便性に着目した製品やシステムがリリースされているが、セキュリティリスクについて十分に検討されていないのが現状である。セキュリティリスクについて検討されていない製品やシステムを使用した場合、実際にどのような事象、被害が起こるのか。スマート家電、自動車、医療など一例ではあるが、以下にセキュリティ被害や攻撃などの具体事例を示す。

① 自宅ネットワーク

（カスペルスキー・ラボ　デイヴィッド・ジャコビィ氏による発表 [120]）

[120]（出所）株式会社 KADOKAWA、ASCII.jp（http://ascii.jp/elem/000/000/971/971034/）

自身の自宅ネットワークに接続されているデバイスを調査した結果、NAS（ネットワーク接続型ストレージ）2 台、スマートテレビ、衛星放送の受信機、インターネットプロバイダーのルーター、ゲーム機、ネットワークプリンターなど、11 の製品が接続されていた。それらのデバイスの多くは製造中止、ファームウェアの自動更新に非対応あるいは、更新が提供されていないなど課題を抱えていることが判明した。

インターネット対応のデバイスが増加し、攻撃者のターゲットとなり、簡単にハッキングできる可能性がありながら、対策が用意されていないのが実態として、下記の製品の実際の脆弱性を例示している。

- NAS（ネットワーク接続型ストレージ）

リモートからルート権限でコード実行可能な脆弱性を発見した。この脆弱性を利用すれば、たとえ NAS がプライベート IP アドレスからの接続のみを受け付ける状態であったとしても攻撃可能である。攻撃は、たとえば SNS のメッセージやメールなど何かしらの方法でリンクをクリックさせる方法が有効である。ユーザーが何も分からずにクリックすると JavaScript コードが実行され、プライベート IP アドレスをリストアップする。その後 Web サーバーを探し、どのデバイスが接続されているかを調べる。あとは、そのデバイスのプライベート IP アドレスにエクスプロイトコードを送り込み、C&C サーバーとの通信を開始する。

- スマートテレビ

サムネイルやウィジェットの最新版がセキュリティなしでベンダーサイトからダウンロードされていた。NAS と同様の攻撃手法を使ってデバイスのローカルファイルを洗い出し、脆弱な部分を探すことが可能である。

② ウェブカメラ

（朝日新聞による発表 [121]）

朝日新聞は、IP アドレスを無作為にたどる方法による独自調査を行い、インターネットでつながるウェブカメラにパスワードを設定する等のセキュリティ対策がとられていない場合が、調査対象の 3 割以上あり、商業施設や住宅の映像・音声を第三者がネット上で見聞きできることがわかった。

それらのウェブカメラは、防犯や監視用として設置され、レンズが向けられている対象と状況から書店や美容院、飲食店、スーパーなどとみられた。事業所の従業員控室、幼い子どもたちがいる託児所のようなスペースもあった。

ウェブカメラには一般にパスワードの設定機能がついているが、設定されていない購入

[121]（出所）株式会社朝日新聞社、朝日新聞（http://www.asahi.com/articles/ASH3654C1H36PTIL00W.html）

時の状態で使われているケースも少なくないとみられる。

③　インスリンポンプ

（研究者　ジェローム・ラドクリフ氏による発表[122]）

ラドクリフ氏は、糖尿病患者の治療に用いるインスリンポンプの制御システムに脆弱性を突いて侵入し「致死的な攻撃」を仕掛けることができることを発表している。具体的には、インスリンを送り込むポンプの無線機能に脆弱性が存在し、それを突くことでポンプ自身を停止においやったり、投与するインスリンの量を外部から操作したりすることが可能であることを指摘している。

同氏は、ハッキング対策検討のために、インスリンポンプ及び CGM（continuous glucose monitors）センサ[123]について、以下の情報収集を行っている。

・対象デバイスのマニュアルからの情報を収集し、マニュアルの付録部分にデバイスの詳細情報（パケットのサイズや伝送間隔等）や Federal Communication Commission (FCC) ID を取得

・特許庁 Web site より機器製造業者を検索し、デバイスの特許情報からデバイスの機能情報や構成情報の詳細情報を収集

その結果、CGM センサでは容易に通信情報の解読が可能であり、インスリンポンプにおいても機器のシリアル番号を取得できれば無線通信により誤った命令を実行が可能であり、CGM センサ、インスリンポンプにおいて、理論上、以下の攻撃が可能であることを発表している。

- CGM センサ攻撃例

・実際のデータと違う血糖値データを送ることで、インスリン投入量の変化を誘発

・正しい血糖値データ受信を妨害し、別のデータを送信

- インスリンポンプ攻撃例

・ワイヤレス機器を用いて、設定の書き換えを行い、意図しない動作を誘発（インスリン投入のタイミングや一回当たりの投入量の変更等）

[122]（出所）独立行政法人情報処理推進機構（IPA）、「医療機器における情報セキュリティに関する調査～医療機器のセキュリティの現状を整理」（https://www.ipa.go.jp/files/000038223.pdf）

[123] CGM（continuous glucose monitors）：継続的に糖濃度を計測するシステム

④　自動車（事件・事故）[124]

2010 年 3 月、米国テキサス州オースティンで、突然 100 台以上の自動車のエンジンがかからない、警告ホーンが鳴り続け止められなくなる事件が発生した。

これらの自動車は返済が滞ったユーザーに自動車を利用させなくするために遠隔イモビライザーが装着されていた。この遠隔イモビライザーはその自動車販売店の従業員が制御できるようになっており、従業員が操作用のパソコンを使って Web サーバーにアクセスすれば集中的に停止処理を操作できた。警察によれば、解雇された従業員が、別の従業員の ID とパスワードを入手して不正に操作したものだとされている。

この事件では、利用者が自動車のキーを持っていたとしても警告ホーンの鳴動を止められない、エンジンをスタートできないため自動車を移動できず、原因がわからなかったため、自動車から鉛蓄電池をはずしてレッカー車で移動することになった。

⑤　自動車（ワシントン大の Kohno 氏らによる発表 [125]）

Kohno 氏らは、実証実験に基づく論文「Experimental Security Analysis of a Modern Automobile1」において、CAN （Controller Area Network）に関する以下の課題を指摘している。

- CAN 通信は同一バス上に同報する方式のため、盗聴、解析が容易。
- 認証フィールドとソースアドレスがなく、なりすましが容易。また、下記に示した CAN を利用した車載 LAN 機器の実装上の課題も存在。
- 一部の ECU が使うチャレンジ用メッセージ長が 16 ビットと短く、解読が容易
- CAN バス全体の通信を停止させる「通信停止」メッセージは、走行中には無視しなければならないが、車輪が回っていても通信を停止させることが可能。
- 走行中の ECU 上のソフトウェア書換えは禁止されているはずであるが、書換えモードに入ることが可能。
- 追加で装着されていた米国大手のテレマティクス端末は、認証メッセージのなりすましを防ぐためにチャレンジとレスポンスを毎回変更するはずが、固定値を利用。
- OBD-II に接続した実験用の PC から上記のテレマティクス装置にチャレンジとレスポンスによる認証手順なしで、テレマティクス装置の組込みソフトウェアを書換え可能。

[124] 独立行政法人情報処理推進機構（IPA）、「2010 年度自動車の情報セキュリティ動向に関する調査報告書～6 件のセキュリティ上の脅威（問題点）を分析～」（http://www.ipa.go.jp/files/000014119.pdf）
[125] 同上

⑥　スマート家電１（事件・事故）[126]

米 Proofpoint は、2014 年 1 月にテレビや冷蔵庫などのスマート家電から、大量の不正メールが送信されたことを確認し、「モノのインターネット」を利用したサイバー攻撃の最初の事例の 1 つだと述べている。

Proofpoint によると、10 万台以上のスマート家電がハッキングされ、75 万通以上のフィッシングメールやスパムメール送信に使われた。乗っ取られたスマート家電には、家庭内ネットワークのルーター、マルチメディアセンター、インターネットテレビ、そして少なくとも 1 台の冷蔵庫が含まれるという。

攻撃が発生した期間は 2013 年 12 月 23 日から 2014 年 1 月 6 日で、世界中の企業および個人に対して、1 日平均 3 回、大量の不正メールが一斉送信された。全不正メールのうち 25%以上は、デスクトップやノートパソコン、モバイル端末といった従来のデバイスを経由せず、スマート家電から直接送信された。単一の IP アドレスを発信元とする電子メールは 10 件以内であり、位置ベースで防御することは非常に困難であった。

個人情報の窃盗や企業システムへの侵入を意図しているサイバー犯罪者は、セキュリティが不十分なスマート家電の方が、パソコンやタブレット端末よりも手軽に感染して制御を奪える可能性があることに気づき、モノのインターネットを「thingbots（モノのボットネット）」に変える方法に移行し始めていると、Proofpoint は注意を促している。

⑦　スマート家電２（セキュリティ会社 Trustwave による発表 [127]）

セキュリティ会社 Trustwave は、LIXIL が提供する Android 向けトイレ操作アプリ「My SATIS」にハードコード化された Bluetooth PIN の脆弱性が見つかったことを発表した。脆弱性は、販売中のトイレ「SATIS」と連携に利用されている Bluetooth の PIN コードが「0000」固定で設定されているというものである。この脆弱性を利用することにより、攻撃者は「My SATIS」をダウンロードするだけで、任意の「SATIS」トイレを制御可能となる。

攻撃者は、トイレ利用者が予期しないタイミングでトイレのフタを開け閉めすることができるほか、ビデや空気乾燥機能のオン/オフも可能となる。

⑧　制御システム（事件・事故）[128]

2011 年 2 月 6 日、ブラジル製鉄所内発電所における制御システムが「WORM_DOWNAD（ダウンアド、Conficker とも呼ばれる）」に感染した。この感染により発電所のオペレーションが停止した。

[126] 株式会社日本経済新聞社、日本経済新聞（http://www.nikkei.com/article/DGXNASFK2000I_Q4A120C1000000/）
[127] 株式会社マイナビ、マイナビニュース（ http://news.mynavi.jp/news/2013/08/05/015/）
[128] 技術研究組合制御システムセキュリティセンター （http://www.css-center.or.jp/pdf/about_CSSC_20140916.pdf）

ワームはプラントのネットワーク全体に広がり、通信トラフィックも急増したため、PLC と SCADA 間の通信が不安定となり、SCADA の機能は大部分が停止した。

復旧では、感染したマシンのワーム除去作業がされたが、感染マシンの後から出現、外部ネットワークと接続した際に、ワームの再度の起動等の事象が発生した。そのため、復旧には数カ月間を要し、その被害は甚大なものとなった。

プラントの発電能力は 550MW であり、2009 年に運用が開始されたものであった。

⑨　航空機（n.runs ヒューゴ・テソ氏）[129]

テソ氏によりアムステルダムで開催されたセキュリティカンファレンス「Hack-in-the-Box」で、遠隔操作による攻撃により航空機を制御するデモが実施された。

Hack-in-the-Box の Web サイトに掲載された発表によると、この攻撃では標的とする航空機に一切の物理的なアクセスは必要とせず、全て遠隔操作で航空機を制御することが可能である。カンファレンスの発表では、実験環境の仮想航空システムにより実証された。テソ氏は「航空機に搭載されたシステムは、その複雑さゆえに、一般的な脆弱性研究や悪用の手口に対して脆弱」だと解説している。

セキュリティ企業 Kaspersky Lab のニュースサービス「threatpost」によると、テソ氏は民間機で実際に使われているシステムを正確に再現した仮想環境を、全て eBay で入手したというハードウェアとソフトウェアで構築し、航空機と地上局の間でデータをやり取りするシステム「ACARS」の脆弱性を見つけ出し、仮想環境の中で実際の航空機のコードを使って飛行管理システムを乗っ取った。

攻撃の準備には航空機の位置や高度を知らせるシステム「ADS-B」も利用されている。ADS-B にはセキュリティ対策が存在しないも同然で、それなりの知識がある攻撃者なら、このシステムを使って航空管制通信を盗聴して操作し、航空機に不正コードの挿入が可能であるとテソ氏は述べている。

Forbes は、Honeywell など航空機のシステムを手掛ける各社や米連邦航空局（FAA）が、テソ氏の攻撃は実際の航空機には、通用しないとコメントしていることを報じている [130]。

[129] アイティメディア株式会社、ITmedia エンタープライズ
（http://www.itmedia.co.jp/enterprise/articles/1304/12/news037.html）

[130] Forbes Media LLC, Forbes, （http://www.forbes.com/sites/andygreenberg/2013/04/10/researcher-says-hes-found-hackable-flaws-in-airplanes-navigation-systems/）

5.2　求められるセキュリティ対策

(1) IoT のアーキテクチャとセキュリティ対策

IoT 関連の製品やシステムの現状に対し、多くの有識者がセキュリティの課題、必要性について、各所で声高に主張している。しかしながら、IoT が、センサやデバイスといったヒトと距離の近いレイヤーから、クラウドのような得られた情報の処理やデータ分析するレイヤーまで幅広いため、議論の前提となるシステム構成や注目するレイヤーによって、実際のセキュリティ対策も異なる。

IoT においてどのようなモノが繋がる対象となり、どのようなセキュリティ対策がされているか俯瞰的に捉えるために、NPO 日本ネットワークセキュリティ協会（JNSA）では、2014 年に「IoT セキュリティ WG」が立ち上げている。初年度は「IoT のセキュリティ脅威と今後の動向」についてまとめており、セキュリティを考慮する際に以下のアーキテクチャモデルを参考としている。例えば、Cisco が提唱する IoE のアーキテクチャ [131]と比較すると表現の違いはあるものの、センサ、ネットワーク、GW、クラウドといった構成要素は類似している。

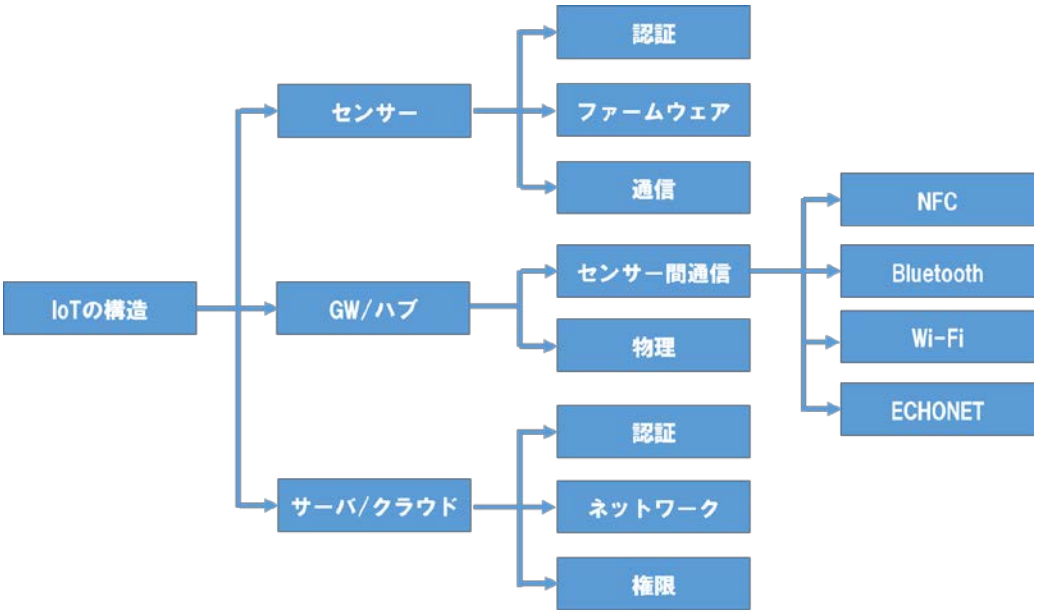


図 5-1　JNSA が発表した IoT のアーキテクチャ

（出所）JNSA「IoT のセキュリティ脅威と今後の動向」をもとにみずほ情報総研作成

脅威に関しては、OWASP（Open Web Application Security Project）の発表をベースに、下記に示す 10 個の脅威について攻撃内容や影響を含め分析している。以下にその脅威の分類を示し、一部の脅威についての詳細を紹介する。

[131] Cisco の IoE アーキテクチャに関しては、第 2 部 4 節 IoT 時代の情報処理基盤を参照されたい。

表 5-1　リストアップされた 10 個の脅威

1.	Insecure Web Interface (不備のある Web インタフェース)
2.	Insufficient Authentication / Authorization (不十分な認証/認可)
3.	Insecure Network Services (不備のあるネットワークサービス)
4.	Lack of Transport Encryption (通信暗号化の欠如)
5.	Privacy Concerns (プライバシー)
6.	Insecure Cloud Interface (不備のあるクラウドインタフェース)
7.	Insecure Mobile Interface (不備のあるモバイルインタフェース)
8.	Insufficient Security Configurability (不十分なセキュリティ設定)
9.	Insecure Software / Firmware (不備のあるソフトウェア/ファームウェア)
10.	Poor Physical Security (脆弱な物理セキュリティ)

（出所）JNSA「IoT のセキュリティ脅威と今後の動向」

表 5-2　各脅威の詳細例　不備のある Web インタフェース

脅威内容	内部及び外部ネットワークからの Web アクセス
攻撃	認証の規定値、認証の平文通信の盗聴、アカウント攻撃、内部および外部からの攻撃
懸念	アカウントリスト、ロックアウト機能無し、安易なパスワード設定。Web インタフェースは、内部からの設定を想定しているが、外部からのアクセスと同様に重要。問題は、Web インタフェースの脆弱性は、XSS のようにツールの利用等で簡単に見つけられること
技術的な影響	データ漏えい、破壊、規約準拠の欠如、サービス停止、機器の乗っ取り
ビジネスへの影響	脆弱な Web インタフェースは、危ないデバイスとなり顧客を危険にさらす。ブランドイメージの失墜となる

（出所）JNSA「IoT のセキュリティ脅威と今後の動向」

これに対し、日本クラウドセキュリティアライアンス（CSA）の代表理事でアルテア・セキュリティ・コンサルティングの二木氏は、Cisco や JNSA とは違うアーキテクチャモデルを提示している。その特徴はネットワークレイヤーが含まれていない点である。同氏へのインタビューによれば、IoT 全体をシステムとし、役割や機能に絞った場合、ネットワークはレイヤーとして存在するものの、ネットワークは言わば土管であり、下記の図に示す各レイヤーもしくはレイヤー間の接続手段として含まれると捉えている。

図 5-2　二木氏が示す IoT のアーキテクチャ

（出所）二木氏発表資料「IoT におけるクラウドの役割とセキュリティ上の課題」より抜粋

(2) IoT のセキュリティで考慮すべき項目

ユーザー視点に立つとセキュリティに加えてプライバシーも確保して欲しいと考えるのではないか、IoT 時代の脅威や守るべき資産は何なのか、IoT 製品のライフサイクルはどのようなものなのかなど、セキュリティ対策を検討する上で、考慮すべき項目は数多い。このような状況の中、国の機関やセキュリティベンダーなどが、IoT が持つリスクについて言及し､様々な観点からセキュリティで考慮すべき項目を挙げている｡しかし、これら項目に対し、現実的ではないだとか、費用対効果の分析がない、ビッグデータに関するリポートに似た内容で目新しいものではないといった見方もある。さらには、IoT 企業の技術進歩やイノベーションが阻害されるという意見もある｡このような状況の下、セキュリティで考慮すべき項目、その内容について概観する。

①　Symantec

技術戦略パシフィック地域情報セキュリティ担当の Mark Shaw 氏は「IoT のセキュリティ対策は、デバイス（センサ）からネットワーク、データ管理に至るまで、既存のセキュリティ対策を拡張して講じる必要がある」と主張し、IoT のセキュリティで考慮すべき項目として、以下の 4 つを挙げている [132]。

[132] 朝日インタラクティブ株式会社、ZDNet Japan（http://japan.zdnet.com/article/35057835/）

- デバイスの保護と収集されるデータのプライバシーを守ること
- デバイスの多様性と性能面での制限を考慮すること
- ソフトウェアのアップデート手段を確保すること
- 収集されるビッグデータの所有権を明確にすること

同氏は、特に「デバイスの多様性と性能面での制限」に注目している。「PC やスマートフォンであれば､デバイス自体にセキュリティソフトウェアをインストールできるが、IoT デバイスの場合、すべてのデバイスにセキュリティ機能を組み込めるとは限らない。また、デバイスの CPU やメモリ性能によっては、セキュリティ機能に制限が生じる可能性がある｡このような状況においては､デバイスとサーバーとの間でやり取りする際の、データと相手先が“本物”であるかどうかを確認する対策が重要になってくる」と主張しており、暗号や署名などの重要性を説いている。

また､セキュリティに配慮した設計（Secure by Design）は、一定のコストがかかる中、テクノロジー シニアディレクターを務める SeanKopelke 氏は、「Secure by Design だからといって、100 ドルのデバイスが 200 ドルになることはない。むしろ（Secure by Design は）付加価値となるはずだ」と主張している。フィットネス系の IoT を管理するソフトウェアの 20%が、（セキュリティが十分に担保されていない）パブリッククラウドで管理されているとの報告もある中、同氏は「仮に生体情報などの個人情報がサイバー攻撃で漏えいした場合、その対策にかかる費用は莫大なものになる。このリスクを正しく認識することができれば、IoT 製品を提供するメーカーは、セキュリティに欠陥のある製品は販売しなくなるかもしれない」と主張している。

② FTC（米国連邦取引委員会）

2015 年 1 月に FTC（米国連邦取引委員会）は「Internet of Things －Privacy & Security in a Connected World－」[133]と題するレポートを公表している。その中で、IoT が人々の生活にさまざまな恩恵をもたらす可能性を認めつつも、IoT に潜むプライバシーとセキュリティのリスクについて指摘し、これらの問題に企業が真剣かつ具体的に取り組むよう強く促した。このうち、1）セキュリティリスク、2)プライバシーリスク、3）リスクへの対応について概観する。

1) セキュリティリスク

３つのセキュリティリスクに関して指摘している。１つ目は、「enabling unauthorized access and misuse of personal information（権限のないアクセスと個人情報の悪用)」である。従来のコンピュータと同様、セキュリティの欠陥によって集積および通信されてい

[133] Federal Trade Commission, “Internet of Things －Privacy & Security in a Connected World－”（https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf）

る個人情報にアクセスされ悪用される。例えば、スマートテレビのセキュリティの脆弱性によって、アカウント情報、パスワードなどの個人情報が他者に盗まれる危険性がある。

２つ目は、「facilitating attacks on other systems（他のシステムへの攻撃可能性）」である。IoT デバイスは他のシステムへの DoS 攻撃を容易にする。今後 IoT デバイスの数が増えていくと、このような攻撃にさらされる危険性が高まる。これは前述のレイヤーをイメージすると理解しやすく、クラウドレイヤーのセキュリティ対策が十分だったとしても、デバイスレイヤーのセキュリティが不十分であると、IoT の系として脆弱であるということになる。

３つ目は、「creating safety risks（安全リスクの発生）」である。権限のない人物がセキュリティの脆弱性を悪用し、リモート操作によって機器をハッキングできたり、通信データを搾取できたりできる可能性がある。例えば、車の組み込みテレマティックスユニットに侵入し、車両を制御する、リモートにスマートメーターからエネルギーの使用状況に関するデータにアクセスし、住宅所有者が家から離れているかどうかを判断するということも起こりえる。

2)　プライバシーリスク

プライバシーリスクとして、位置情報、口座番号、健康情報などの機密性の高い個人情報をインターネットやモバイル取引を通して直接収集されてしまう可能性、また時間をかけて週間や場所や物理的な状況といった個人情報をも収集される可能性がある。それによって、(1)大量かつ正確な個人情報の蓄積、分析が悪用されるというリスク、(2)企業によって個人情報を目的外利用されるというリスク（例えば、個人情報を、信用評価、保険会社の保険料の計算、企業の採用選考に用いる）、(3) 脆弱性を突いた攻撃の発生リスクを挙げている。

3)　リスクへの対応

IoT が今後活用されていくためには、消費者の信用が不可欠であるとして、そのための対応を企業に求めている。具体的には、以下の 10 の対応を挙げている。

1. セキュリティを後付するのではなく、最初から機器に実装する。
2. 企業はユーザーに対し消費者データの取り扱い方を保証する。
3. セキュリティを維持できるサービスプロバイダの確保とセキュリティを維持していることの監視を行う。
4. セキュリティ対策がいくつかのレベルで検討され、多層防御を実装する。

5. 権限のないユーザーがデバイスやネットワークに保管されている消費者の個人情報にアクセスできないようアクセス制御を行う。
6. 製品ライフサイクルの間、機器の監視と修正パッチの適用を続ける。
7. データ収集、保存を最小化する。
8. 消費者は収集を拒否する機会が与えられるべきである。
9. 企業に収集するデータを制限し、一定の時間が経過した後にそれを廃棄する。
10. 消費者は企業がどの情報を収集するか、また何のために収集するかを知らされるべきである。

（出所）FTC「Internet of Things －Privacy & Security in a Connected World－」の内容をもとにみずほ情報総研作成

③ クラウドセキュリティアライアンス（CSA）の場合

2015 年の 4 月に、非営利法人である日本クラウドセキュリティアライアンス（CSA）が、「Security Guidance for Early Adopters of the Internet of Things (IoT)」[134]と題し、IoT において推奨されるセキュリティ対策や将来的に取り組むべき項目などを体系的にまとめたガイドを公表している。

本ガイドでは、大きく分けて以下の 7 つのセキュリティ対策が取り上げられている。

1. Analyze privacy impacts to stakeholders and adopt a Privacy-by-Design approach to IoT development and deployment（プライバシーに関する影響を分析し、プライバシーに配慮した設計を IoT の開発や方針へ適応）
2. Apply a Secure Systems Engineering approach to architecting and deploying a new IoT System.（セキュアな設計開発）
3. Implement layered security protections to defend IoT assets（段階及びレイヤー毎のセキュリティ保護の実装）
4. Implement data protection best-practices to protect sensitive information（機密情報保護）
5. Define lifecycle controls for IoT devices（IoT デバイスのライフサイクルの定義）
6. Define and implement an authentication/authorization framework for the organization’s IoT Deployments（認証/認可の枠組み）
7. Define and implement a logging/audit framework for the organization’s IoT ecosystem（ログ/監査の枠組み）

（出所）Security Guidance for Early Adopters of the Internet of Things (IoT)

[134]（出所）一般社団法人日本クラウドセキュリティアライアンス, “Mobile Working Group Peer Reviewed Document”（https://downloads.cloudsecurityalliance.org/whitepapers/Security_Guidance_for_Early_Adopters_of_the_Internet_of_Things.pdf）

特に注目されるのが「3. Implement layered security protections to defend IoT assets（段階及びレイヤー毎のセキュリティ保護の実装）」で、段階及びレイヤーには、「Network Layer」「Application Layer」「Device Level」「Physical Layer」の他に、「Human Layer」が定義されている。「Human Layer」は、IoT におけるリスクを軽減する上で最も安全にすることが難しく、グレーな領域だとされている。従来はシステムとヒトには境界があり、仮にシステムに問題があってもヒトが対処することができた。しかし、IoT 時代では、ヒトはシステムを使う側というより、IoT システムの一部として組み込まれるものとして、考え方を改める必要がある。

(3) IoT のセキュリティで考慮すべき項目

2015 年の 3 月に興味深い集団訴訟がアメリカで起きている。ハッキングされてドライバーの安全が脅かされる可能性のある車両を、安全だと保証して販売したなどの理由により、トヨタ、GM、Ford の自動車メーカー３社が提訴[135]された。欠陥があるプログラムを組み込んだハードウェアの使用により損害を被った場合に、製造者の責任が追求される可能性があるのは理解できる。しかし、訴状からは事故などの直接的な損害は発生しておらず、直接的な損害が出ていなくても、人命に関わるような脆弱性があるものを販売すれば提訴される可能性がある。

また、訴状には「In particular, wireless technologies create vulnerabilities to hacking attacks that could be used to invade a user’s privacy or modify the operation of a vehicle.（とりわけ、無線技術は利用者のプライバシー侵害や車両の操作変更にも利用可能なハッキング攻撃への脆弱性を生み出す）」という記載があり、通信による遠隔操作でエンジン始動を禁止するような機能・サービスの悪用が指摘されている。これは、あらゆるモノと通信しながら走行する自動運転車、コネクテッド・カーは、このような通信機能の悪用に関連した訴訟のリスクと常に隣り合わせであるということを暗に示しているといえるだろう。

ハッキングされるリスク対策自体が製造者責任の範疇になるのか、ソフトウェアには何らかの欠陥が含まれると理解されている状況における法的責任とは何なのか、IoT 時代における製造者の法的責任を占う意味で、今後の訴訟の展開が注目される。

[135] STANLEY LAW GROUP, “COMPLAINT FOR BREACH OF WARRANTY, BREACH OF CONTRACT,AND VIOLATION OF CONSUMER PROTECTION LAWS”
（http://www.stanleyiola.com/files/2015/03/20150310_Complaint.pdf）

5.3 IoT 時代のセキュリティに関する展望、課題

IoT に関する議論はまだ途上である。現在では、IoT がもたらす利便性やサービスの高度化、効率化といったメリットや IoT が作り出す社会像が議論の中心となっている。勿論、利便性や未来像も非常に重要だが、我々に深刻な危害や損害を与える可能性がある IoT のセキュリティリスクやプライバシーリスク、倫理等について、さらなる議論が必要ではないか。前述の Hewlett-Packard による調査結果の通り、調査対象製品の 70%にセキュリティ問題が見つかっており、これらについて、十分に議論されているとは言えない。

これまでセキュリティは、後回しにされることが多かった。この背景には、セキュリティが利便性やコストとのトレードオフの関係にあり、利便性を追求する際の足枷になったり、セキュリティ対策の費用対効果が見えづらかったりといった理由があったように思われる。また、何かセキュリティ上の問題が起こったとしても、これまではインターネットの世界に閉じており、ある意味影響は限定されていたのかもしれない。しかし、前述の CSA のガイドが示すように、もはや人間は IoT システムの一部として組み込まれており、有事の際は実社会や人命にまで多大な影響が及ぶ可能性が少なくない状況なのである。そう考えると、IoT が私達の生活に組み込まれるほど、セキュリティやプライバシー、倫理を考える必要性は、否応無しに高まってくる。

セキュリティリスク等が十分に考慮されていない IoT 関連のサービス、製品、システムが世の中に展開され、その後何らかの事故が発生した際に、想定外という言葉で済ませてはならない。考慮不足は、結果的に危険を招く可能性を増大させる。したがって、IoT 時代に求められるセキュリティは、利便性などのメリットの次ではなく、同じレベルでの優先事項として検討される必要がある[136]。利便性とセキュリティ対策といった両面のバランスをいかに取っていくか。それを見極めることこそが、IoT が作り出す確かな未来の原動力になるのではないか。

[136] 政府は 2015 年 5 月に、サイバーセキュリティ戦略本部の第 2 回会合を開催し、「サイバーセキュリティ戦略（案）」を決定・公表した。その中では、「安全な IoT（Internet of Things）システムの創出」「セキュリティマインドを持った企業経営の推進」などの施策が盛り込まれている。今後、IoT に関するセキュリティ確保の具体的な議論が本格化すると見られる。（出所）内閣サイバーセキュリティセンター、「サイバーセキュリティ戦略（案）」（http://www.nisc.go.jp/active/kihon/pdf/cybersecurity-senryaku.pdf）

みずほ産業調査 ／51　2015 No.3　　平成 27 年 8 月 28 日発行

編集／発行　みずほ銀行産業調査部　　東京都千代田区大手町 1-5-5　Tel. (03) 5222-5075