技術戦略研究センターレポート

TSC Foresight Vol.18

IoTソフトウェア分野の技術戦略策定に向けて

2017年7月

1章 IoTソフトウェア分野の概要 …… 2

2章 IoTソフトウェア分野の置かれた状況 …… 4

2-1 組込みソフトウェア …… 4

2-2 情報セキュリティ …… 11

3章 IoTソフトウェア分野の技術課題 …… 18

3-1 スマート・コネクティッドを実現するIoTソフトウェア …… 18

3-2 IoTソフトウェアのディペンダビリティ …… 19

4章 おわりに …… 20

TSCとはTechnology Strategy Center（技術戦略研究センター）の略称です。

国立研究開発法人 新エネルギー・産業技術総合開発機構
技術戦略研究センター（TSC）

1章 IoT ソフトウェア分野の概要

IoT（Internet of Things）は、1999年頃にRFID（Radio Frequency Identifier）の普及を指して呼んだ言葉とされるが、その後のユビキタスコンピューティングやM2M（Machine-to-Machine）通信の概念と、スマートフォンなどのモバイルデバイスの普及によって、2012年頃から、様々な機器がインターネットに接続される状況を指す言葉として広まった。

現在、インターネットにつながるデバイスの多くは、PCあるいはスマートフォンなどの情報家電製品と呼ばれる機器である。しかし、これからは自動車、家電、自動ドア、自動販売機、健康器具、ウェアラブルデバイス、鍵といった、ありとあらゆる機器がネットワークにつながる。そして、デバイス自体がインテリジェントになるとともに、情報を収集してクラウドに送るセンサーにもなる。こうして形成されたビッグデータは、未来予測やAI学習に使われ、より高い価値を生み出すためのビジネス資産となる。また、デバイスの処理能力が増すことにより、ディープラーニングに基づくAIを組み込むことが可能となり、デバイスの一層の高度化につながる。

これを実現する技術がIoTソフトウェアであり、デバイスの進化により、「情報系と制御系の統合」、「ビッグデータの利活用」、「ビッグデータの相互接続」などが促進され、プリエンプティブ・サービス※1が新たな価値創造手段として拡大する。プリエンプティブ・サービスを構成するIoTソフトウェア技術群を図1に示す。

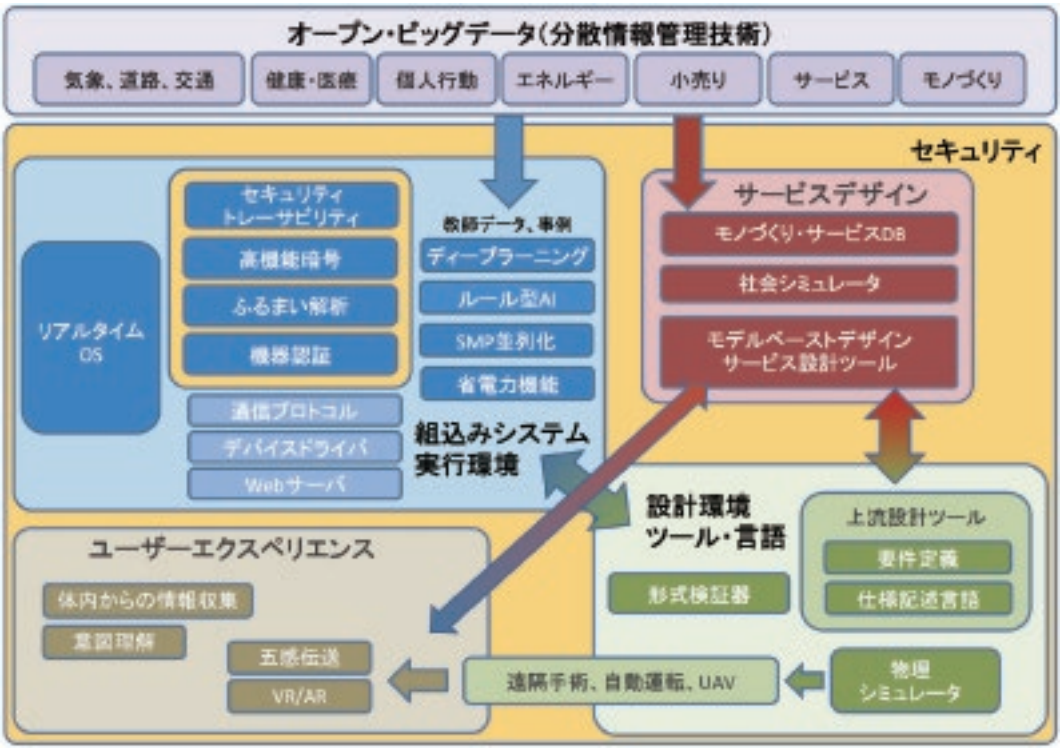

図1　プリエンプティブ・サービスを構成するソフトウェア技術群
出所：NEDO技術戦略研究センター作成（2017）

※1　製品自体の販売をビジネスの主たる目的とするのではなく、その製品を使ってサービスを提供することを目的とする。製品はサービスを構成するための一つの要素と位置付けられる。代表的なものとして、「Power by the hour」などがある。

IoT ソフトウェア分野の技術戦略策定に向けて

機器が様々なデータにアクセスし、自律分散的に機能制御を行うためには、機器に搭載された組込みシステムが重要な機能を担う。電気・機械装置に特定の機能を発現させる組込みシステムは、主にマイクロコントローラとそれを制御するソフトウェアで構成され、マイクロコントローラは一般的に汎用的なものが用いられることから、機器が発現する機能は、組込みソフトウェアが決めることになる。したがって、組込みソフトウェアをいかに正確に効率よく開発できるかが、製品やサービスに大きく影響する。

また、プリエンプティブ・サービスを構成するIoTデバイスに搭載される組込みシステムは、様々なものとインテリジェントにつながる機能（スマート・コネクティッド）が必要である。ハーバード大学経営大学院のマイケル・ポーター教授※2は、IoT社会におけるスマート・コネクティッド機能を、「他の製品やシステムとアドホックに連携することによって、新しいサービスを実現するとともに、自己診断や自己修理といったことも自律的に行う機能」と定義しており、IoT社会において、製品がスマート・コネクティッド機能を持つことの重要性を指摘している。

スマート・コネクティッド機能を備えることによって、新たな価値創造を実現する一方で、新たなセキュリティリスクが生じることが懸念される。例えば、情報系と制御系の統合により、様々な機器を最適制御できるようになるが、サイバー攻撃による不正侵入により、より直接的に生命や財産を侵食するリスクにつながる。しかし、サイバー攻撃を受けたからといって、直ちに機器や装置を止めればよいというものではない。例えば、発電プラントのような重要インフラは、社会基盤を維持するという観点から、すぐ止めることはできない。すなわち、こうしたシステムには、「攻撃下でも必要最小限の動作を続けること」が求められる。

また、制御系システムは、常時稼働していることが前提となっているものも多く、セキュリティ上の対策を含めたソフトウェア／ファームウェア等のアップデートのためにシステムを停止させることができない。つまり、制御系のシステムが運用される数十年に渡って、システムを止めることなく、発見された脆弱性に対する対策を施すことができることが必要である。さらに、こうした対策を施すことによって、システムの稼働に影響がないことを事前に検証しなければならないが、IoT化の進行により、検証対象が、より広域かつ複雑になる。すなわち、IoTソフトウェアには、図2に示すように、製品に要求される機能を継続的に提供するための品質を維持する機能が必要であり、この機能をディペンダビリティという。

以上のように、IoTに対応した製品に組み込まれるIoTソフトウェアは、従来の組込みソフトウェアの機能に加え、スマート・コネクティッドとディペンダビリティという機能を基本特性として兼ね備えなければならない。

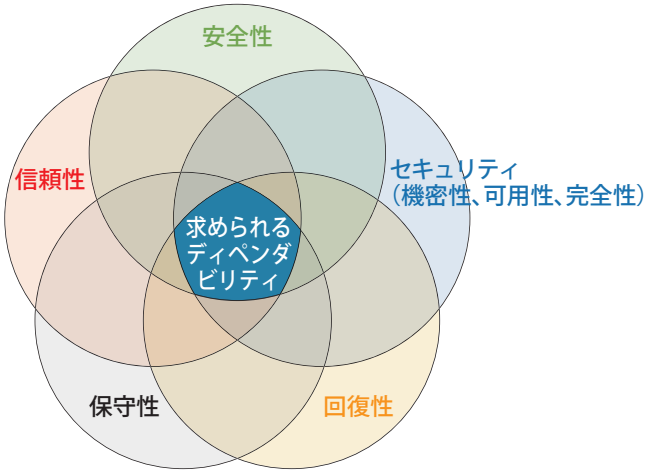

図2　ディペンダビリティの概念図
出所：NEDO技術戦略研究センター作成（2017）

※2 Porter, Michael E., Heppelman, James E. "How smart, connected products are transforming competition", *Harvard Business Review*, November 2014.

2章 IoT ソフトウェア分野の置かれた状況

2章では、組込みシステムの中で特に重要な技術である、組込みソフトウェア及びセキュリティの置かれた状況について、分析した結果を示す。

2-1 組込みソフトウェア

(1) 市場

組込みソフトウェアに関係する製品（OS・ミドルウェア・開発環境・ツール）の市場規模は表1のとおり、2014年現在で国内はおよそ800億円程度である。参考資料を基に、GDPの伸びなどから外挿すると、2030年の世界市場規模はおよそ2兆円規模と類推できる。

また、組込みソフトウェアは、外販のみならず組込みシステムを製造するメーカーにおいて内製されることも少なくないため、正確に市場規模を算定することは難しい。参考として、図3に独立行政法人情報処理推進機構（IPA:Information-technologyPromotionAgency）が算出したデータを示す。国内では組込みソフトウェアの開発に年間およそ3兆円が投じられており、組込みシステムの開発費全体の過半数を占めている。この割合は年々増加傾向にある。

表1　組込みソフトウェア関連製品の市場規模

分野	2014年国内市場規模（百万円）	2014年世界市場規模（百万円）	2030年世界市場規模（百万円）	（参考）分野市場規模
車載	32,370	461,289	808,754	輸送用機器：21.2兆円（2030年国内GDP）
産業機械	18,705	266,556	467,338	一般機械：15.0兆円（2030年国内GDP）
家電	26,467	377,168	661,269	白物家電：2.0兆円（2030年国内GDP）
医療・福祉	2,118	30,183	52,918	ヘルスケア機器：37.0兆円（2030年国内GDP）
計	79,660	1,135,196	1,990,278	

出所：各種資料を基にNEDO技術戦略研究センター作成（2017）

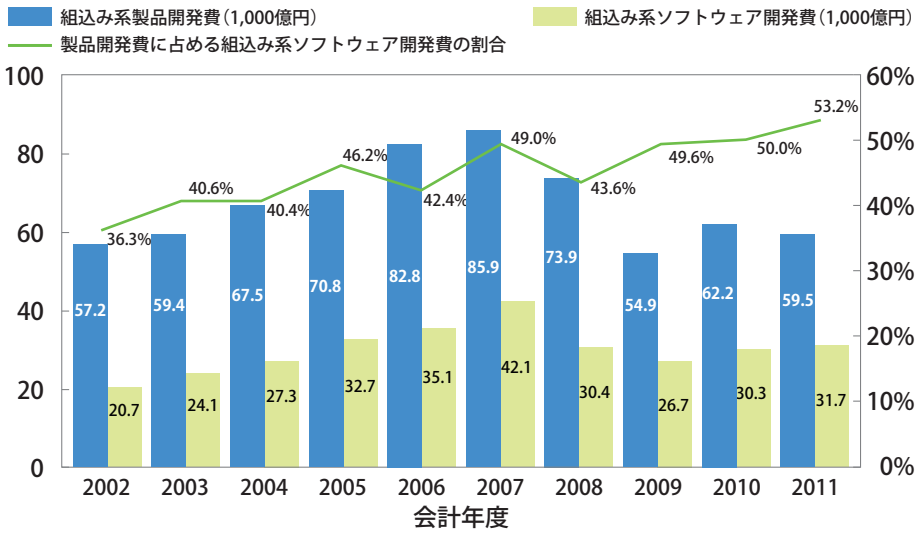

図3　製品開発費と組込みソフトウェア開発費の推移
出所：「ソフトウェア産業の実態把握に関する調査」にみる組込み産業の現状（情報処理推進機構（IPA），2013）を基にNEDO技術戦略研究センター作成（2017）

IoT ソフトウェア分野の技術戦略策定に向けて

(2) 技術分野の動向

①論文

組込みソフトウェアについて、「embedded software」「embedded middleware」をキーワードに、2007年から2016年に発表された論文数の推移を図4に示す。2007年以降、ほぼ右肩上がりに発表論文数は増加している。

表2に示す国／地域別の発表論文数では、米国が全論文数の約25%を占めており、中国、ドイツがそれに続く。日本は14位に位置しており、論文数は127本（2.8%）にとどまっている。

上位3か国と日本の発表論文数の経年変化を図5に示す。米国、中国、ドイツの3か国はいずれも、この10年間でほぼ右肩上がりに増加している。特に、中国は過去10年間でほぼ4倍と、最も増加している。一方、日本は10年間ほぼ横ばいの状態である。

図4　「embedded software」「embedded middleware」に関する発表論文数の経年変化（2007～2016年）

出所：Web of Science™での検索結果を基にNEDO技術戦略研究センター作成（2017）

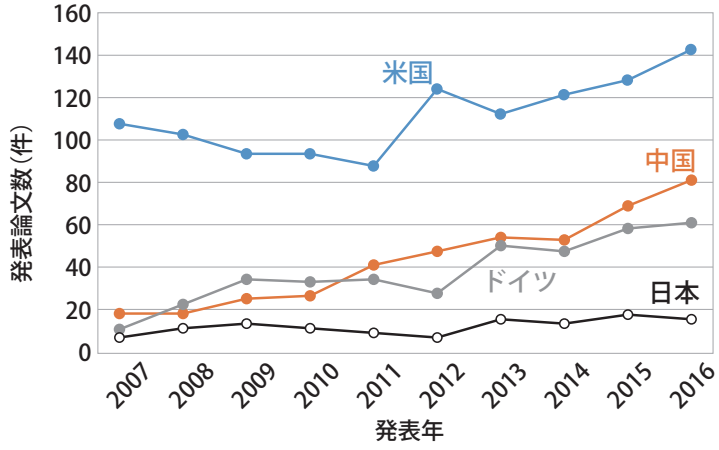

図5　上位3か国及び日本の発表論文数の経年変化（2007～2016年）

出所：Web of Science™での検索結果を基にNEDO技術戦略研究センター作成（2017）

表2　「embedded software」「embedded middleware」関連の国／地域別発表論文数（2007～2016年）

順位	国 / 地域	発表論文数（割合）
1	米国	1134（25.0%）
2	中国	443（9.8%）
3	ドイツ	384（8.5%）
4	イタリア	297（6.6%）
5	イギリス	282（6.2%）
6	フランス	267（5.9%）
7	スペイン	260（5.7%）
8	韓国	242（5.3%）
9	カナダ	188（4.2%）
10	台湾	174（3.8%）
11	オランダ	148（3.3%）
12	ブラジル	137（3.0%）
13	オーストラリア	135（3.0%）
14	日本	127（2.8%）

出所：Web of Science™での検索結果を基にNEDO技術戦略研究センター作成（2017）

世界の研究機関別の発表論文数を表3に示す。世界の研究機関の中では、中国科学院（中国）が最も多くの論文を発表しているが、他の研究機関に比べて突出しているわけではない。

日本の研究機関別の発表論文数を表4に示す。10位までを大学及び国立研究開発法人で占めているが、他国の研究機関と比べて論文数が少ない。いずれの研究機関も平均すると年間1本以下の論文数にとどまっている。

表3　世界の研究機関別発表論文数（2007～2016年）

順位	研究機関	国	発表論文数
1	中国科学院	中国	42
2	カリフォルニア大学バークレー校	米国	35
3	トリノ大学	イタリア	32
	ソウル大学	韓国	32
5	ミラノ工科大学	イタリア	31
	ミュンヘン工科大学	ドイツ	31
7	メリーランド大学	米国	30
8	清華大学	中国	27
	マドリード・カルロス３世大学	スペイン	27
	ヴァンダービルト大学	米国	27

出所：Web of Science™での検索結果を基にNEDO技術戦略研究センター作成（2017）

表4　日本の研究機関別発表論文数（2007～2016年）

順位	研究機関	発表論文数
1	九州大学	8
2	慶應義塾大学	7
	東京大学	7
4	早稲田大学	6
5	京都大学	5
	大阪大学	5
7	情報通信研究機構	4
	東北大学	4
	豊橋工科大学	4
	筑波大学	4

出所：Web of Science™での検索結果を基にNEDO技術戦略研究センター作成（2017）

②特許

組込みソフトウェアに関わる特許に関しては、用途が多岐にわたり、出願件数も数十万件以上におよぶことから、全てを調査対象とすることは困難である。そこで、組込みソフトウェアの主要なアプリケーションのひとつであり、規模の拡大が著しい自動車制御用の調査結果を示す。

自動車用制御システムにかかる組込みソフトウェアのうち、重要機能であるパワートレイン制御・ボディ制御・シャーシ制御・情報通信の4項目について、2000 ～ 2014年に日米欧中4か国で出願された特許件数（累計44,631件）の推移を図6に、国／地域別の出願件数の推移を図7に示す。

2000年以降、右肩上がりに出願件数は増加しており、2012年以降は特に増加のペースが上がっている。国／地域別にみると、自動車産業の競争力が特許出願件数に関係しており、日本からは継続的に多数の特許出願が行われている。しかし、2004年以降中国の出願件数の増加が著しく、2012年以降は中国が出願数でトップとなっている。

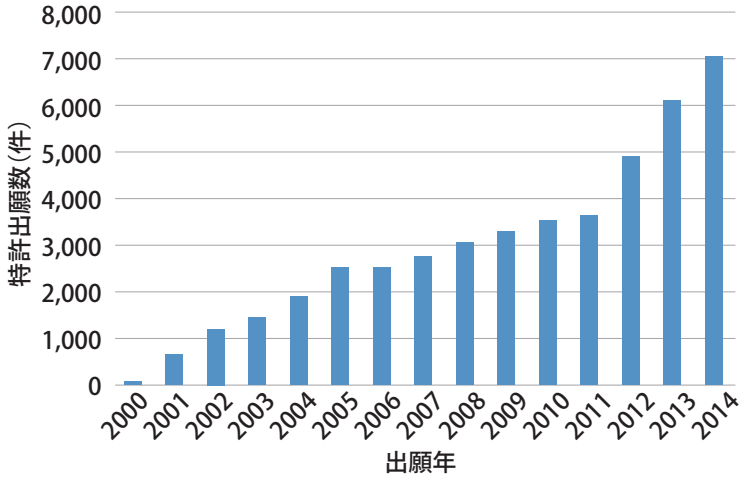

図6 「自動車用制御システム」組込みソフトウェアに関する日米欧中の特許出願件数推移
出所：NEDO技術戦略研究センター委託調査（2015）

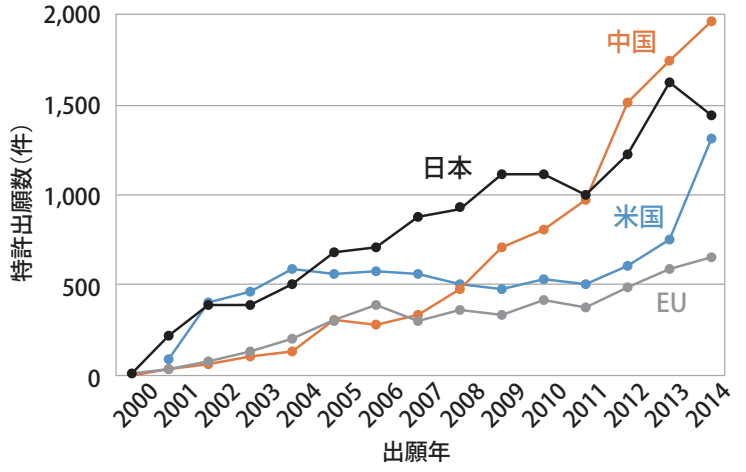

図7 「自動車用制御システム」組込みソフトウェアに関する国／地域別特許出願件数推移
出所：NEDO技術戦略研究センター委託調査（2015）

(3) 海外の取組

①米国

米国では、CPS(Cyber-Physical System)の考え方を実現、高度化して活用すべく、政府機関や企業等により取組が進められている。

アメリカ国立科学財団(NSF:National Science Foundation)等により2006年からCPSに関するワークショップが開催されている。また、大学と産業界とをつなぐ研究拠点整備としてIndustry/University Cooperative Research Centers(I/UCRC)プログラムが実施され、その中にアリゾナ州立大学と南イリノイ大学を拠点とするCES(Center for Embedded Systems)がある。同センターには、産業界からIntelやQualcomm、Marvell、UTC Aerospace Systems、Rockwell collins、Bosch、Ford、トヨタ自動車などが参画している。

研究分野としては、組込みソフトウェアシステム、組込みマルチコアアーキテクチャ・プログラミング、CPS、エネルギー消費効率化などが含まれている。CESにおける主な研究テーマを表5に示す。

表5　CESにおける主要な研究テーマ

サイバー・フィジカル・システム	モデリング及びシミュレーション
	モデルベースの形式検証
	モデルベースの合成
エレクトロニクス・システムレベル(ESL)の設計と技術	モデリング及びシミュレーション
	ハードウェアとソフトウェアの共創及び最適化
	信頼性及びセキュア設計
組込みマルチコアアーキテクチャとプログラミング	ネットワーク・オン・チップ設計及び最適化
	マルチコアプロセッサ上でのストリームアプリケーションのコンパイル
	高電力効率プログラマブル・アクセラレータ
	ソフトエラー耐性システム設計
	低消費電力組込みシステムの設計及びプログラミング
	組込み GPU コンピューティング
	温度変化を考慮したアーキテクチャ及びプログラミング
組込みソフトウェア・システム	リアルタイムスケジューリング
	スマートグリッドのための組込みシステム
	組込みシステムのためのミドルウェア及びバーチャルマシン
	組込みソフトウェアの計測及びツール
集積回路技術、設計、及びテスト	悪環境下の使用に耐える半導体チップ
	デバイス物理学及びモデリング
	マイクロエレクトロニクスデバイスとセンサーの設計及び製造
	アナログ / RF 混合信号回路の設計とテスト
	デジタル回線のテスト及びシリコンデバック
電力、エネルギー、熱に観応性が高い設計	低消費電力回路アーキテクチャと設計ツール
	マルチコア組込みシステムの動的性能、電力、エネルギー及び熱管理
	デジタルシステムの統計的変動を考慮した設計
	組込みシステム向けのエネルギー効率の良いアーキテクチャとコード最適化

出所:「Center for Embedded Systems (CES)」(NSF, 2016) を基にNEDO技術戦略研究センター翻訳 (2017)

また、IT研究開発を促進する連邦省庁横断のプログラム「ネットワーキング及び情報技術研究開発プログラム」（NITRD：Networking and Information Technology Research and Development）という取組も行われている。NITRDはホワイトハウスの下部組織OSTP（Office of Science and Technology Policy）傘下のNSTC（National Science and Technology Council）の小委員会の1つとして位置づけられており、2014年時点で17の省庁が参画しており、2015年に約38億ドルの予算が割り当てられた。

このNITRDのプログラムの1つが「高信頼性ソフトウェアとシステム（HCSS：High Confidence Software and Systems）」であり、同プログラムにおいて、組込みシステムに関する研究開発が進められている。

HCSSに関しては、表6に示すとおり、大統領府と参加省庁から要求された研究テーマについて、年度展開して取組が進められている。

表6　HCSSが取り組んでいる研究テーマ（2011～2015年）

	研究テーマ	2011	2012	2013	2014	2015
大統領府リクエスト	サイバーフィジカルシステムのためのテクノロジーと技術開発	←	—	—	—	→
	サイバーフィジカルシステム・イノベーションチャレンジ	←	→			
	保証技術	←	—	—	—	→
	高信頼リアルタイムソフトウェアとシステム	←	—	—	—	→
	複合システムの管理と理解を促進させる研究	←	→			
	研究と教育の統合	←	→			
	複合システムと自律システムのマネジメント			←	—	→
	政策課題対応型研究開発への転換			←	—	→
	サイバーフィジカルシステムの教育			←	—	→
HCSS参加省庁リクエスト	サイバーフィジカルシステム	←	—	—	—	→
	サイバー空間への接続を可能とする研究とイノベーション	←	→			
	高信頼システムと保証コンピューター技術の構築	←	—	—	—	→
	情報保証の必須要件	←	—	—	—	→
	自律式工業制御システムにおけるセキュリティとネットワークのための標準化とテスト手法	←	→			
	大規模複合システム		←	→		
	航空安全		←	—	—	→
	コンピューター技術の調査		←	→		
	複合システム			←	—	→
	エネルギー分野における高信頼システム				←	→
	航空基幹システムの保証				←	→

出所：ニューヨークだより「米国におけるソフトウェア信頼性に関する取り組みの現状」（JETRO/IPA New York, 2014）を基にNEDO技術戦略研究センター作成（2017）

②欧州

2004年、欧州委員会は、組込みシステムの共同研究開発と標準化に向けて、ARTEMIS（Advanced Research & Technology for Embedded Intelligence in Systems）を設立した。ARTEMISは、欧州研究エリア構想を受けて開始された欧州技術プラットフォームのひとつである。組込みシステムやサイバー・フィジカル・システム（CPS：Cyber-Physical System）に関する幅広い技術課題や応用分野で共通して利用できる、1.リファレンス設計&アーキテクチャ、2.シームレス接続&相互運用性、3.システム設計手法&ツールの3つの研究領域を定めている。また、2030年の組込みシステムやCPSを実現するうえで、7つの技術課題が挙げられている（表7）。

2014年には、ARTEMISのFP（Framework Programme）のもとで作られたJTI（Joint Technology Initiatives）のテーマであったENIAC（European Nanoelectronics Initiative Advisory Council）とARTEMISがECSEL（Electronic Components and Systems for European Leadership）として統合され、研究開発を継続して進めている。

表7　ARTEMISが挙げる技術課題

1	新しい機能と高性能化を可能にするアーキテクチャモデルと原則
2	システム設計ツールの総合運用標準に基づく設計段階からのセーフティ＆セキュリティ
3	分散リアルタイムシステム、高度認証運用のための状況認識
4	新しいスマートアプリケーションの開発を可能とし、大きく変化する分野のソリューション構築のためのインターコネクション
5	自律、ダイナミック、適応的、自己組織化システム
6	組込み・CPSとのシームレスなインタラクション
7	最適化された統一的なプロセスとツール

出所：NEDO電子・材料・ナノテクノロジー部「組込みシステム及び関連ソフトウェアに関する技術課題の検討」（NEDO, 2015）

2-2 情報セキュリティ

(1) 市場の動向

①経済損失

サイバー犯罪による経済損失を正確に見積もることは困難であるが、グローバルで50兆円以上と見積もられており、2013年には日本でも920億円の経済損失が発生しているとされる※3。

②市場規模

NPO日本ネットワークセキュリティ協会の報告書によると、国内情報セキュリティ市場は、情報セキュリティツール市場及び情報セキュリティサービス市場に分類され、それぞれ、2017年度には5,099億円、4,697億円、合計9,795億円に成長すると見込まれている（図8）。

また、2014年から2015年にかけて、国内情報セキュリティ市場は年率5%で成長すると予想され※4、この成長率が継続する仮定のもと、NEDOでは国内情報セキュリティ市場は2020年に1兆1,300億円、2030年に1兆8,400億円に拡大すると予測している。

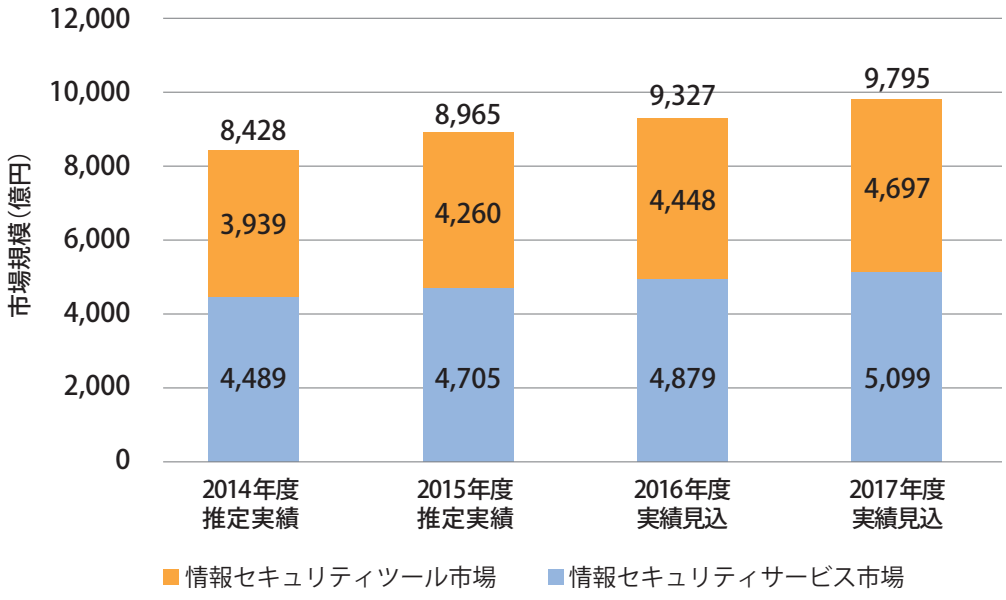

図8　国内情報セキュリティ市場規模の推移
出所：2016年度国内情報セキュリティ市場調査速報（2017年1月23日時点）
（日本ネットワークセキュリティ協会，2017）を基にNEDO技術戦略研究センター作成（2017）

※3 出所：Center for Strategic and International Studies, 2014
※4 経済産業省、ガートナージャパン株式会社（2014）のレポート

(2) 技術分野の動向

①セキュリティ技術のマッピング

セキュリティ技術について、外部からの攻撃対象となるノードと、その攻撃に対する対策技術で整理した結果を、表8に示す。このうち、IoT 組込みソフトウェアに関する部分は、主に「エッジ端末、組込み機器（制御機器、IC カード、車載等）」の列である。

表8　攻撃対象ノードと対策技術の分類

対象ノード		汎用クライアント（PC、スマートフォン）	エッジ端末、組込み機器（制御機器、ICカード、車載等）	インフラサーバー（データセンター、ネットワーク）
攻撃法		マルウェア、ソーシャルエンジニアリング、バッファオーバフロー、バックドア、ルートキット、パスワードクラック、証明書偽造		
		広告アプリ 標的型 Email ランサムウェア 水飲み場攻撃 ドライブ・バイ・ダウンロード	キルシグナチャ サイドチャネル LSI 偽造	DoS、SQL インジェクション フィッシング クロスサイト・スクリプティング ハードウェアトロイ木馬
対策	脆弱性を作らない	セキュアプログラミング、レビュー、暗号化情報処理、アップデート、システム検証 ペネトレーションテスト、Fail-safe-C、脆弱性データベース（CWE、CVE）		
		NX（スタック実行不能化）	————	NX（スタック実行不能化）
	侵入防止、侵入検知	アンチウィルス、暗号通信、証明書、電子署名、パスワード認証 スタックのカナリア（オーバフロー検出）		
		アプリ権限の限定 ワンタイムパスワード バイオメトリクス TPM 検閲	デバイスの使用制限 ホワイトリスト制御 振る舞い解析 軽量暗号 SE-Linux	IDS、WAF、VPN セキュリティトークン DNS、SMTP などの暗号化 仮想化 鍵管理、ルート権限管理 認証基盤 システム監査、SDN
	操作制限 操作無効化	ファイアウォール		
		アプリ権限の限定 メモリ保護	ホワイトリスト SE-Linux	SE-Linux 仮想化 DoS 対策（十分な処理能力）
	感染防止	ファイアウォール、ログ監視		
		リモートワイプ	ゾーニング	ゾーニング
	早期回復	バックアップ、ログ監視		
		————	冗長化	冗長化
	評価認証 標準・規格	IEC61508（機能安全）、CC 認証（IEC15408）		
		スマートフォン・タブレット 業務利用セキュリティ 無線 LAN セキュリティ （総務省ガイドライン） プライバシーマーク	EDSA、IEC62443（CSMS） ISO26262（自動車） IEC62304（医療機器）	EAL ISO/IEC-27001（ISMS） 情報セキュリティ対策基準（NISC）

出所：NEDO 技術戦略研究センター作成（2017）

②論文

「security」をキーワードとして、IT、IoTとの関連が深いCOMPUTER SCIENCE、INFORMATION SYSTEMS、COMPUTER SCIENCE SOFTWARE ENGINEERINGの3つの研究分野において、2007年から2016年に発表された論文数の推移を図9に示す。

2007年以降、右肩上がりに発表論文数は増加している。表9に示す国／地域別の発表論文数では、米国と中国で全論文数の約半数を占め、韓国、台湾などのアジア圏の国がそれに続く。日本は8位に位置しており、論文数は710本（4.3%）であった。

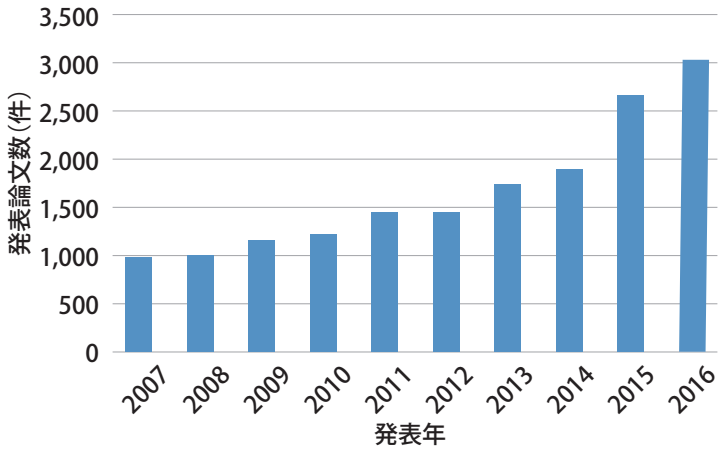

図9 「security」に関する発表論文数の経年変化（2007～2016年）
出所：Web of Science™での検索結果を基にNEDO技術戦略研究センター作成（2017）

表9 「security」関連の国／地域別発表論文数（2007～2016年）

順位	国 / 地域	発表論文数（割合）
1	米国	4221（25.3%）
2	中国	4024（24.1%）
3	韓国	1354（8.1%）
4	台湾	1036（6.2%）
5	インド	846（5.1%）
6	カナダ	829（5.0%）
7	イギリス	824（4.9%）
8	日本	710（4.3%）
9	オーストラリア	706（4.2%）
10	スペイン	646（3.9%）

出所：Web of Science™での検索結果を基にNEDO技術戦略研究センター作成（2017）

上位3か国と日本の論文発表数の経年変化を図10に示す。2007年には米国が多数の論文を発表しており、その後も発表論文数は年々増加している。しかし、2008年以降は中国からの発表論文数が急激に増加しており、2013年には米国を抜いて国別の発表論文数の首位となっている。現在に至るまで、中国とその他の国との発表論文数の差はさらに拡大している。韓国も2007年以降、徐々に発表論文数は増加しているが、日本は2007年以降の10年間でほぼ横ばいの状態である。

世界の研究機関別の発表論文数を表10に示す。上位10の研究機関のうち、中国の大学・研究機関が過半を占めている。

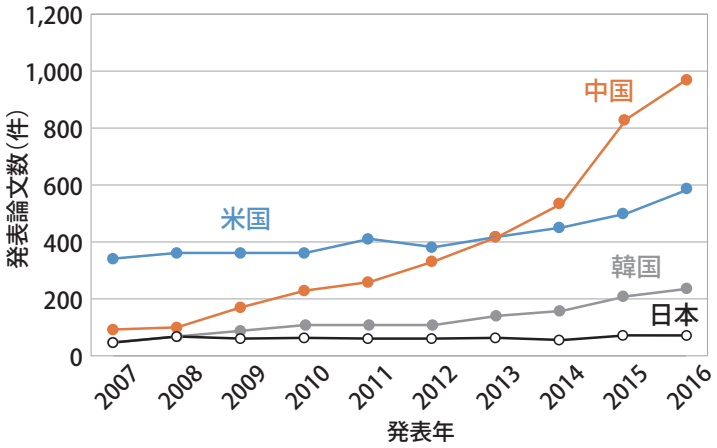

図10　上位3か国及び日本の発表論文数の経年変化（2007～2016年）
出所：Web of Science™での検索結果を基にNEDO技術戦略研究センター作成（2017）

表10　世界の研究機関別発表論文数（2007～2016年）

順位	研究機関	国	発表論文数
1	西安電子科技大学	中国	322
2	中国科学院	中国	310
3	北京郵電大学	中国	252
4	上海交通大学	中国	237
5	高麗大学	韓国	207
6	パデュー大学	米国	170
7	電子科技大学	中国	165
8	清華大学	中国	155
	ウォータールー大学	カナダ	155
10	南洋理工大学	シンガポール	147

出所：Web of Science™での検索結果を基にNEDO技術戦略研究センター作成（2017）

日本の研究機関別の発表論文数を表11に示す。上位10のうち6機関を大学が占めている。

表11　日本の研究機関別発表論文数（2007～2016年）

順位	研究機関	発表論文数
1	九州大学	70
2	日本電信電話株式会社	67
3	産業技術総合研究所	53
4	情報通信研究機構	45
5	早稲田大学	34
6	東北大学	33
7	東京工業大学	32
8	東京大学	30
9	大阪大学	28
10	日本電気株式会社	26

出所：Web of Science™ での検索結果を基に NEDO 技術戦略研究センター作成（2017）

③特許

情報セキュリティ技術に関しては、特許庁が2015年に「情報セキュリティ技術特許出願動向調査」を実施している。同調査から、出願人国籍別の出願件数を図11に示す。日本国籍の出願人による出願については、暗号技術の出願件数が他の技術よりも多く、同様の傾向は欧州国籍の出願人による出願にも見られる。

他方、米中韓国籍の出願人による出願では、暗号技術以外の侵入検知、ウイルス・マルウェア検知や認証技術の出願件数についても同程度に出願されている。

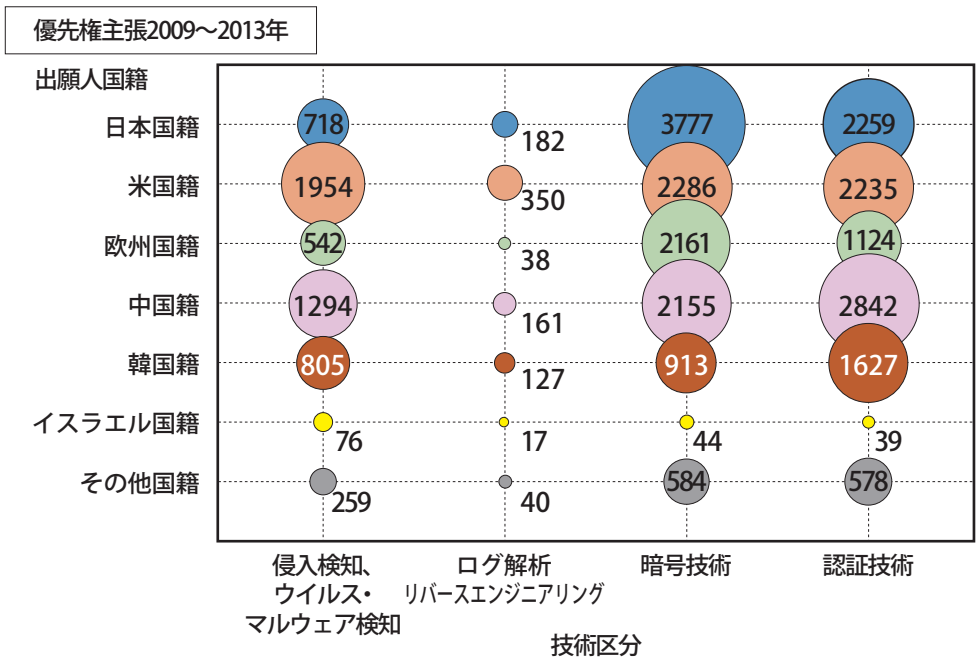

図11　技術区分別 - 出願人国籍別出願件数
出所：平成27年度特許出願動向調査 - 情報セキュリティ技術 -（特許庁）

④規格・標準化

情報セキュリティ分野の標準化は、図12に示すように、分野ごとの標準化機関が連携する体制によって管理されている。社会インフラシステムは長期間運用するため、サイバー攻撃の進歩も踏まえた対策を強化できるようにすることが重要とされている。

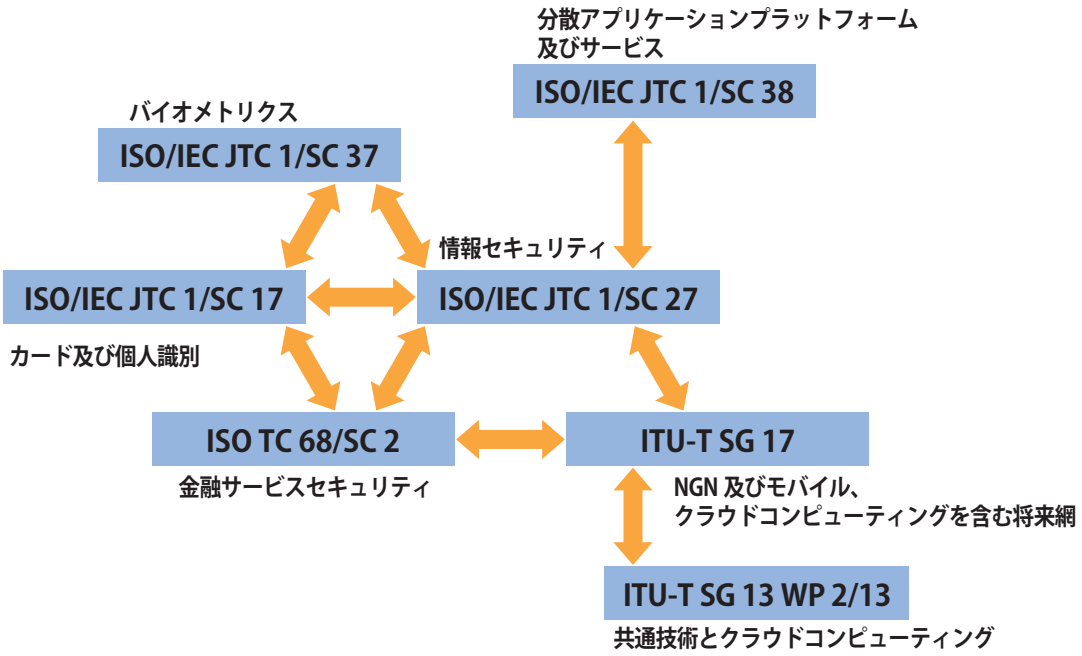

図12　情報セキュリティ関連の標準化機関の相関図
出所：情報処理推進機構「情報セキュリティ白書 2015」を基に NEDO 技術戦略研究センター作成（2017）

⑤国内外の技術動向及びベンチマーク

IoT セキュリティに関連する技術分野について、表12に日米欧中韓の技術水準の比較を示す。全ての技術分野について、米国が高い技術水準を持っており、欧州がそれに続く。暗号や認証基盤、量子情報セキュリティなど、日本が高い技術水準を持つ分野もあるが、IoT 社会における基盤技術として必要なネットワークセキュリティの分野では、欧米に比べて技術水準は劣位にある。

表12　IoT セキュリティ関連技術水準の国際比較

フェーズ	日本	米国	欧州	中国	韓国
基礎研究	○(↗)	◎(↗)	○(→)	△(→)	△(→)
応用研究・開発	○(↗)	◎(↗)	◎(↗)	○(→)	△(→)

【フェーズ】
基本研究　　：大学・国立研究開発法人などでの基本研究のレベル
応用研究・開発：研究・技術開発（プロトタイプの開発含む）のレベル
【評価】
◎：特に顕著な活動・成果が見えている
○：顕著な活動・成果が見えている
△：顕著な活動・成果が見えていない
【トレンド】
↗：上昇傾向
→：現状維持

出所：「研究開発の俯瞰報告書 システム・情報科学技術分野（2017年）」（科学技術振興機構 研究開発戦略センター、2017）を基に NEDO 技術戦略研究センター作成（2017）

3章 IoT ソフトウェア分野の技術課題

前述したように、IoT ソフトウェアにはスマート・コネクティッドが必須であり、同時に、ディペンダビリティの確保も必要である。

IoT ソフトウェアを設計・開発するにあたっては、この2つの機能を効率よく、正しく確実に実装できるかどうかが、IoT 対応機器の製品競争力を左右し、それらの機器によって構成されるサービス・エコシステムの価値を決定する。そこで、この2点の技術課題を取り上げる。

3-1 スマート・コネクティッドを実現する IoT ソフトウェア

(1) 機能

多くの製品は組込みシステムとして、マイクロコントローラと組込みソフトウェアを備えるが、スマート・コネクティッド機能を実装することによって、以下の機能を実現する。

- 製品の稼働状況や性能のモニタリング
- 製品が外部に干渉する機能の制御
- 環境変化に対応した製品機能のアジャストメント
- 他の機器と自律的に連携して全体最適化を図る機能

(2) 課題

①機能要件の定義

スマート・コネクティッド機能を備えることによって、製品は従来のビジネスの枠を超えて、様々な機器とつながる。それは、ビジネス領域の拡大をもたらし、新たなビジネスの機会を創出する。一方で、ビジネス領域の拡大は、製品に組み込まれるソフトウェアが実現すべき機能を複雑にする。その結果、ソフトウェアが実現すべき機能要件を正確に定義することが難しくなる。

②開発環境とメソドロジー（方法論）

あらゆる製品において、IoT 化によって高機能化が進行し、そこに搭載される組込みソフトウェアは肥大化が加速的に進行する。ソフトウェア技術者の能力や経験にのみ頼っていては、高品質の組込みソフトウェアを効率的に開発していくことが、今後ますます困難となることが容易に予想できる。

これらに対応した開発環境と、開発のためのメソドロジーがなければ、非線形な開発コスト増の要因となり、組み込まれる製品の競争力が失われることになる。

③検証プロセス

機能とともに規模が肥大化するソフトウェアを検証するために、実機を使ったテストを行うことによるコストや工数の増加が問題となる。当然ながら、多機能な製品に搭載されるソフトウェアほど多くのテストを必要としている。実機を用いたテストのみを行うとすれば、製品開発期間が非常に長期化してしまう。そのため、近年では積極的に物理シミュレーションを利用する動きが活発になっている。しかし、物理シミュレーションツールの多くはオープンソースであるため、十分なサポートが受けられないなどの問題がある。また、必要な検証項目すべてについて、物理シミュレーションツールが用意されているわけではない。

3-2 IoT ソフトウェアのディペンダビリティ

(1) 機能

ディペンダビリティとは、システムの信頼性、安全性、保守性、回復性にセキュリティ（機密性、可用性、完全性）を含んだ広い概念であり、品質の一部をなす。1章の図2でディペンダビリティの概念図が示すように、信頼性、安全性、保守性、回復性、セキュリティといった要素は、それぞれに独立しているのではなく、お互いに関係し、影響し合っており、ディペンダビリティはこれらが高度に連携して成立しているのである。

どんなシステムでもディペンダビリティは重要であるが、医療機器、航空機、車載エレクトロニクスなどに組み込まれるソフトウェアは、人命に関わることもあり、PCのソフトウェアのように頻繁にダウンすることは許されない。

(2) 課題

①ディペンダビリティ・エコシステム

ディペンダビリティについては、ソフトウェア設計時のみならず、これを組み込んだ製品が市場投入された後もメンテナンスしなければならない。設計時に注意深く検証を重ねたとしても、市場投入後に、ソフトウェアに起因する脆弱性が発見されることは珍しいことではない。製品ライフサイクル全般でディペンダビリティを担保できるようなシステムがなければ、ディペンダビリティを維持し続けることは難しい。

②多様性の拡大と相互干渉

製品に詰め込まれた、多種多様なソフトウェアは、IoT社会の進展によってしだいに関係を深めつつあり、相互に干渉する事例が増えつつある。例えば、ある種のソフトウェアをインストールするときは、アンチウィルスソフトを停止させる必要があるなどがその例である。その他にもライブラリやバージョンのミスマッチが不具合を引き起こす例は多数ある。同様のミスマッチが、システムやアプリケーションごとのセキュリティポリシーの違いで引き起こされ、それが強い脆弱性に至ることも考えられる。

③暗号化技術

ビッグデータ解析などが産業競争力に大きく影響を及ぼすようになってきたことによって、データを安全に、かつ確実に処理する研究が世界中で進められている。特に、秘匿検索やプライバシー保護の観点から、秘密の情報を使用する権限を階層的に付与するために、IDベース暗号や関数暗号など、高機能暗号の研究が盛んである。

日本における高機能暗号に関する研究機関は、欧米と比べて数は少ないものの、研究レベルは比較的高いレベルを維持している。しかし、高機能暗号を用いて実現しようとする具体的なビジネスモデルや用途が明確ではない。この結果、開発目標が定まらず、汎用的に利用可能な高機能暗号を目指した研究開発が先行しており、実用化のためには長期間に亘る究開発が必要な状況となっている。

4章 おわりに

組込みシステムに関連する日本の産業分野の総額は100兆円を超えており、3兆円が組込みソフトウェア開発に投じられている。その一方で、精密機械をアナログ電子回路で制御するメカトロニクス産業が、マイクロコントローラとソフトウェアによる組込みシステムに変貌し、容易に設計製造できるようになったことから、日本の組込みシステム産業は競争力を失いつつある。

また、すべてのモノにソフトウェアが組み込まれるIoT社会では、スマート・コネクティッドを実現するIoTソフトウェアの品質が競争力を左右し、信頼性や安全性、保守性、回復性とセキュリティを保つディペンダビリティがなければ、健全かつ安全な社会を実現することは難しい。

マサチューセッツ工科大学スローン経営大学院のマイケル・A・クスマノ教授の研究※5によれば、日本のソフトウェア設計開発能力は、欧米に比べて決して劣るものではなく、むしろ高品質のソフトウェアを開発する能力は優れているとされている。今後、日本のみならず、世界の市場で日本の産業界が競争に勝ち抜いていくために、高品質なIoTソフトウェアを効率よく開発していくことが重要である。

※5 Cusumano, M.A.(2010) *Staying Power: Six Enduring Principles for Managing Strategy and Innovation in an Uncertain World,* Oxford University Press(鬼澤忍訳, 2012『君臨する企業の「6つの法則」ー戦略のベストプラクティスを求めて』日本経済新聞社)

〈 Memo 〉

技術戦略研究センターレポート

TSC Foresight Vol. 18

IoTソフトウェア分野の技術戦略策定に向けて

2017年7月14日発行

TSC Foresight Vol.18　IoTソフトウェア分野作成メンバー

国立研究開発法人 新エネルギー・産業技術総合開発機構
技術戦略研究センター（TSC）

■ センター長　川合　知二

■ センター次長　矢島　秀浩

■ 電子・情報・機械システムユニット

・ユニット長　伊藤　智

・研究員　砂口　洋毅
有馬　宏和
大窪　宏明
松尾　直之

・フェロー　松井　俊浩　情報セキュリティ大学院大学教授
林　秀樹　元住友電工フェロー、IEEE Life Fellow、応用物理学会フェロー
遠藤　直樹　株式会社東芝インダストリアル ICTソリューション社技監
中屋　雅夫　元株式会社半導体理工学研究センター代表取締役社長
山口　佳樹　筑波大学准教授

● 本書に関する問い合わせ先
電話 044-520-5150（技術戦略研究センター）

● 本書は以下URL よりダウンロードできます。
http://www.nedo.go.jp/library/foresight.html