

戦略プロポーザル

Society 5.0 時代の
安心・安全・信頼を支える
基盤ソフトウェア技術

STRATEGIC PROPOSAL

System Software to Support Safety, Security,
and Trust in the Era of Society 5.0

研究開発戦略センター（CRDS）は、国の科学技術イノベーション政策に関する調査、分析、提案を中立的な立場に立つて行う公的シンクタンクの一つで、文部科学省を主務省とする国立研究開発法人科学技術振興機構（JST）に属しています。

CRDSは、科学技術分野全体像の把握（俯瞰）、社会的期待の分析、国内外の動向調査や国際比較を踏まえて、さまざまな分野の専門家や政策立案者との対話を通じて、「戦略プロポーザル」を作成します。「戦略プロポーザル」は、今後国として重点的に取り組むべき研究開発の戦略や、科学技術イノベーション政策上の重要課題についての提案をまとめたものとして、政策立案者や関連研究者へ配布し、広く公表します。

公的な科学技術研究は、個々の研究領域の振興だけでなく、それらの統合によって社会的な期待に応えることが重要です。「戦略プロポーザル」が国の政策立案に活用され、科学技術イノベーションの実現や社会的な課題の解決に寄与することを期待しています。

さらに詳細は、下記ウェブサイトをご覧ください

<https://www.jst.go.jp/crds/>

エグゼクティブサマリー

わが国が提唱する Society 5.0時代の安心・安全・信頼を支える基盤ソフトウェアの研究開発として、本提案は、特に緊急性の高いセキュリティ、プライバシー、プラットフォームに関わる課題を解決するための研究開発戦略を提言する。

Society 5.0が目指す社会は、人とモノがつながり、さまざまな知識や情報が共有され、今までにない新たな価値を生み出すデータ駆動社会である。データ駆動社会では、デジタル時代の競争力の源泉である「データ」は、特定の国や企業が抱え込むのではなく、プライバシーやセキュリティ、知的財産などの安全を確保した上で、自由に流通することが必要である。しかし、現状では、わが国のデータの大部分はGAFAに代表される米国の巨大IT企業に握られている。そのデータ覇権に対抗し自由なデータ流通と個人情報保護を両立する枠組みを実装することが求められている。

わが国はハードウェアやOSを海外に依存している。1990年代以降の情報システムのオープン化、コモディティ化により、情報科学技術の基盤に関わる研究開発の機会を喪失し、産学ともに国際的な競争力を失ってしまった。GAFAの競争力の源泉はビジネスモデルとそれを支える情報科学技術の基盤である。情報科学技術の基盤をおろそかにしては、Society 5.0が目指す社会を実現することはおぼつかない。さらに、情報通信産業においても、情報科学技術基盤の強化なくしては、わが国がIoTやロボット活用などの強みを生かして国際競争力を強化することは難しい。

新型コロナの災禍は、働き方、学び方、医療のあり方など、これまで当たり前と感じていたものを問い直す貴重な契機となった。再認識された価値も含む新たな常態（ニュー・ノーマル）に向けて、ITにより社会を変革するDX（デジタルトランスフォーメーション）の取り組みの徹底が求められている。これは、2016年にわが国が目指すべき経済発展と社会的課題の解決を両立する、人間中心の社会として提唱された Society 5.0の実現であり、その実現に向けたこれからの時代を「Society 5.0時代」と呼ぶ。本提案では、Society 5.0時代の社会システムにおいて優先的に解決すべき共通課題として、情報科学技術の基盤技術のうち、セキュリティ、プライバシー、プラットフォームに関わる課題を解決するための研究開発を取り上げた。

セキュリティに関しては、これまでインターネットを経由した攻撃が主たる脅威だったものが、近年はそれに加えて、ハードウェアやOSなど計算環境のコアに関わる新たなぜい弱性を狙った脅威が現れ始めた。これまでより一歩進んだ、信頼できない計算環境でも安全に正しく動くソフトウェアを動作させる技術が必要となる。具体的な研究開発課題としては、安全性指向コンピューターアーキテクチャー技術、信頼できる隔離実行環境の構築技術、および、エッジからクラウドまでの総合的なセキュリティを実現するセキュアOS技術などが挙げられる。

プライバシーに関しては、データ駆動社会においてデータは重要な資産であり、個人情報や企業の機密情報、研究データなどは安全に管理しつつ活用することが求められる。しかし現実には、システムのぜい弱性を悪用した漏えいや改ざんなどの事象にはとどまる兆しが見えない。プライバシー確保に関しても、これまでより一歩進んだ、オープンなネットワーク上のデータは見られるという前提のもとで、データの秘匿性を確保する技術が求められる。技術的には、秘密計算によるトラスト確保技術、相互に信頼できる範囲や開示レベルを動的に制御可能な分散認証技術、秘密計算に基づく分散データ収集・解析技術などの研究開発課題が考えられる。一方でCOVID-19の接触追跡に見られるように、公益とプライバシーの交錯する領域でもあるため人文・社会科学の知見を交えた研究も必要である。

プラットフォームに関しては、研究成果は Society 5.0時代の安心・安全・信頼を支える基盤ソフトウェア技術として Society 5.0プラットフォームに適用することを最終的な目標とする。研究成果は実社会に貢献することで社会的な意義を持つからである。プラットフォーム技術においては、従来のような後追いの対処では

ない、システム全体をby-Designの観点で捉え、きめ細かいセキュリティ要件とプライバシー確保を担保した上で、データの流通と情報処理を可能とすることが求められる。ただし、現時点で巨大IT企業のもつプラットフォームを置き換えることは現実的でないため、本提案では既存のさまざまな実行環境からなるハイブリッドなハードウェアやOS上で動作させることを前提に置く。具体的な研究開発課題として、多様な実行環境からなる分散データ処理環境の管理・制御技術、セキュリティ・プライバシー処理の高性能実装技術、データの真正性証明や来歴保証技術などがある。

研究開発の推進においては、基礎研究（理論）と応用研究（システム基盤）を同時に進める。理論では計算機科学が依って立つ数学領域の研究者との連携が必要である。一方、システム基盤においては、研究成果を実証する際のターゲットシステム環境が重要である。人材育成の観点から、研究者が経験と自信と達成感を感じるためには、現実に使われて社会に貢献するシステムであることが望ましい。わが国の大学・国研のもつ研究開発プラットフォームはその有力な候補である。プロジェクトの遂行では、異分野の研究者や産と学がアンダーワンルーフに集う研究体制を構築し、将来に向けた人材育成の礎とする。

提案による研究開発を実施することで得られる科学技術上の効果として以下の3点があげられる。第1は、理論およびシステム基盤の研究者が連携して同じ課題に取り組むことで、Society 5.0時代のシステム基盤に資する基礎理論を構築することができる。第2は、高度化・複雑化し続けるセキュリティ・プライバシー課題の解決に向けて、アーキテクチャーからOS、データベース、セキュリティ、言語の研究者が一丸となって取り組むことで、後追いでない根本的な解決方式を確立できる。第3は、国際連携強化である。今回のような課題の解決は一国の力だけでは難しい。海外の一流の研究者を招くこと、海外の研究機関との共同プロジェクトを運営すること、研究成果は論文だけでなくオープンソースソフトウェアとして発信することなど、国際連携の機会を多面的に設けることが、国際貢献そのものになり、ひいてはわが国の研究者の実力を向上させるものと考ええる。

社会経済的効果としては、短期的には、プライバシー侵害やセキュリティ不安の軽減と、セキュリティ事象による直接的・間接的被害を減少させる。中長期的には、国内に向けては、デジタル革新・データ駆動によりさまざまな社会課題を解決し、より人間的で幸福な社会であるSociety 5.0の実現に繋がる。また、国際的には、ICT技術領域における新規ビジネスや社会的イノベーションの創出、標準化案の策定、人材育成等が推進され、SDGs達成に向けた科学技術イノベーション推進に貢献する。

Executive Summary

As research and development of system software to support security, safety, and trust in the Society 5.0 era proposed by Japan, this proposal proposes a research and development strategy on system software to solve issues related to security, privacy, and platforms.

The goal of Society 5.0 is to create a data-driven society where people and things are connected, various knowledge and information are shared, and new values are created that have never been seen before. In a data-driven society, data, which is the source of competitiveness in the digital age, should not be held by a specific country or company but should be freely distributed while ensuring privacy, security, intellectual property, and other safety features. At present, however, most of Japan's data is under the control of the US IT giants represented by GAFA. To counter this data hegemony, it is necessary to implement a framework that balances free data distribution and personal information protection.

Japan is depending on foreign countries for hardware and operating systems. The trend toward openness and commoditization of information systems since the 1990s has resulted in the loss of its R&D opportunities related to the foundation of information science and technology, and the loss of its international competitiveness in both industrial and academic areas. The source of GAFA's competitiveness is their business models and the foundation of information science and technology. If Japan neglects the foundation of information science and technology, it will not be able to realize the society that Society 5.0 aims for. Furthermore, in the information and communication industry, without strengthening the foundation of information science and technology, it will be difficult for Japan to strengthen its international competitiveness by leveraging its strengths in IoT and robotics.

Meanwhile, the new coronavirus pandemic has provided an inevitable opportunity to reexamine what people had taken for granted in terms of how they work, how they learn, and how they receive medical care. Toward the reaffirmed value with the new normal, Japanese society is required to thoroughly implement DX (Digital Transformation) initiatives to transform itself through IT. This is the realization of Society 5.0, which was proposed in 2016 as a human-centered society that balances economic development and the resolution of social issues, and the coming era toward the realization of this society is called the "Society 5.0 era. This proposal focuses on research and development to solve issues related to security, privacy, and platforms among the fundamental technologies of information science and technology because this proposal believes that these are the common, as well as urgent, issues that need to be solved in the social system of the Society 5.0 era.

Firstly, concerning security issues, attacks via the Internet used to be the main security threat, but in recent years, new threats have emerged that target new vulnerabilities in the core of the computing environment, such as microprocessors and operating systems. It is necessary

to go one step further to develop technologies that enable the software to run safely and correctly even in untrustworthy computing environments. Concrete research and development issues include safety-oriented computer architecture technology, technology to build a trusted execution environment, and secure OS technology to realize comprehensive security from edge to cloud.

Besides, as for issues on privacy in a data-driven society, data serves as a critical asset, and personal information, confidential corporate information, and research data must be safely managed and utilized. However, there is no sign of an end to leaks and tampering that exploit the vulnerability of the system. To ensure privacy, it needs to go one step further to develop technologies that ensure data confidentiality based on the premise that data on open networks can be seen. In terms of technology, possible R&D issues include trust assurance technology based on secret computation, distributed authentication technology that can dynamically control the range of mutual trust and disclosure level, and distributed data collection and analysis technology based on secret computation. On the other hand, as seen in the contact tracing of COVID-19, it is also an area where national interests and privacy intersect, so it is necessary to conduct research that includes knowledge from the humanities and social sciences.

The final challenge is to establish a platform technology that supports security, safety, and trust in the Society 5.0 era. This is because research results have social significance only when it contributes to the real world. The platform technology must enable data distribution and information processing while ensuring detailed security requirements and privacy assurance, by considering the entire system from the perspective of by-Design, rather than the conventional follow-up measures. However, since it is not realistic to replace the platforms IT giants provide at this time, this proposal assumes that the proposing system will run on various existing platforms. Concrete research and development issues include management and control technologies for distributed data processing environments consisting of various execution environments, high-performance implementation technologies for security and privacy processing, and technologies for proving the authenticity and provenance of data.

In the promotion of research and development, basic research (theory) and applied research (system foundation) will be conducted simultaneously. In theory, it is necessary to collaborate with researchers in the field of mathematics, on which computer science depends. On the other hand, in the system foundation, the target system environment is important for demonstrating the research results. From the viewpoint of researchers' human resource development, the system should be used in real systems and contribute to society to give them experience, confidence, and a sense of accomplishment. The research and development platforms of Japanese universities and national laboratories are strong candidates for this purpose. In the execution of the project, it is essential to build a research system that brings together researchers from different fields and industry and academia under one roof and use this as a foundation for human resource development for the future.

By implementing this proposal, three scientific and technological benefits are predicted to

be achieved. First, by having researchers in theory and system infrastructure work together in the same project, it will be possible to build a basic theory that will contribute to the system infrastructure of the Society 5.0 era. Second, researchers in the areas of architecture, operating systems, databases, security, and languages can work together to solve the security and privacy issues that continue to become more sophisticated and complex, thereby establishing a fundamental solution method that does not follow suit. The third is to strengthen the international research and development community. It is difficult for a single country to solve a problem like this one. Inviting top-notch researchers from overseas, managing joint projects with overseas funding agencies, and disseminating research results not only in the form of papers but also as open-source software are all opportunities for international collaboration. This strategic proposal believes that this will contribute to the international community and improve the capabilities of Japanese researchers.

Finally, as a socioeconomic effect, in the short term, it will reduce privacy violations and security concerns, and decrease direct and indirect damages caused by security events. In the medium to long term, the results of this proposal will help solve various social issues through digital innovation and data-driven solutions, leading to the realization of Society 5.0, a more humane and happy society. Internationally, the project will promote the creation of new businesses and social innovations in the ICT technology field, the formulation of standardization proposals, and human resource development, and will contribute to the promotion of science and technology innovation toward the achievement of the SDGs.

目次

1	研究開発の内容	1
2	研究開発を実施する意義	5
2.1	現状認識と問題点	5
2.2	社会・経済的効果	11
2.3	科学技術上の効果	13
3	具体的な研究開発課題	15
3.1	セキュリティに関する研究開発課題	15
3.2	プライバシーに関する研究開発課題	17
3.3	プラットフォームに関する研究開発課題	19
4	研究開発の推進方法および時間軸	21
4.1	研究開発推進の全体構想	21
4.2	研究開発の戦略とロードマップ	22
付録 1	検討の経緯	24
付録 2	国内外の状況	30
付録 3	専門用語説明	34

1 | 研究開発の内容

わが国が提唱する Society 5.0 時代¹の安心・安全・信頼を支える基盤ソフトウェアの研究開発として、本提案では、特に、緊急性の高いセキュリティ²、プライバシー²、プラットフォーム³に関わる課題を解決するための研究開発を提言する（図 1-1）。

Society 5.0 が目指す社会は、人とモノがつながり、さまざまな知識や情報が共有され、今までにない新たな価値を生み出すデータ駆動社会である。データ駆動社会では、デジタル時代の競争力の源泉である「データ」は、特定の国や企業が抱え込むのではなく、プライバシーやセキュリティ・知的財産などの安全を確保した上で、自由に流通することが必要である。しかし、現状では、わが国のデータの大部分は GAFA⁴に代表される米国の巨大 IT 企業に握られている。そのデータ覇権に対抗し自由なデータ流通と個人情報保護を両立する枠組みを実装することが求められている。

わが国はハードウェアや OS（Operating System）を海外に依存している。1990 年代以降の情報システムのオープン化、コモディティ化により、情報科学技術の基盤に関わる研究開発の機会を喪失し、産学ともに国際的な競争力を失ってしまった。GAFA の競争力の源泉はビジネスモデルとそれを支える情報科学技術の基盤である。情報科学技術の基盤をおろそかにしては、Society 5.0 が目指す社会を実現することはおぼつかない。さらに、情報通信産業においても、情報科学技術基盤の強化なくしては、わが国が IoT やロボット活用などの強みを生かして国際競争力を強化することは難しい。



図 1-1 Society5.0時代の安心・安全・信頼を支える基盤ソフトウェア技術

- 1 新型コロナの災禍は、働き方、学び方、医療のあり方など、これまで当たり前と感じていたものを問い直す貴重な契機となった。再認識された価値も含む新たな常態（ニュー・ノーマル）に向けて、ITにより社会を変革する DX（デジタルトランスフォーメーション）の取り組みの徹底が求められている。これは、2016年にわが国が目指すべき経済発展と社会的課題の解決を両立する、人間中心の社会として提唱された Society 5.0 の実現であり、本提案ではその実現に向けたこれからの時代を「Society 5.0 時代」と呼ぶ。
- 2 ここでいうセキュリティとは情報セキュリティのことであり、情報システムに対するさまざまな脅威から情報を守ることである。一方、プライバシーとは人に知られたくないこと（個人情報）を適切に扱うことである。基本的人権の一つであり、欧州データ保護規則やわが国の改正個人情報保護法などの法制度により守られる。
- 3 ここで言うプラットフォームとはアプリケーションを動作させるために必要となる共通的な機能をまとめたシステムソフトウェアを指す。仮想化ソフトウェア、オペレーティングシステム（OS）およびミドルウェアから構成される。
- 4 GAFAは米国の IT 企業 4 社（Google、Amazon、Facebook、Apple）頭文字を並べた造語で世界のサイバービジネスを支配する。これに Microsoft を加えて GAFAM と称することもある。

(1) Society 5.0システムソフトウェアとは

Society 5.0を実現するさまざまなアプリケーションシステムはSociety 5.0プラットフォームと呼ばれる実行環境で動作する。Society 5.0プラットフォームは、システム群、データベースおよび基盤技術から成る（図1-2）。ここで、基盤技術と書かれた部分こそが、冒頭に述べた競争力の源泉たる情報科学技術の基盤である。基盤技術は、ハードウェアとソフトウェアから成る。ソフトウェアは、機械学習やスパコン、データ処理など技術分野に特化したソフトウェアと、分野によらず必要となる共通ソフトウェアに分けられ、本提案ではこの共通部分をSociety 5.0システムソフトウェアと呼ぶ。Society 5.0システムソフトウェアは、セキュリティー技術（プライバシー技術も含む）以外に、広域分散処理や人工知能用の新たな計算原理の実現に向けた機能を有することが求められる。

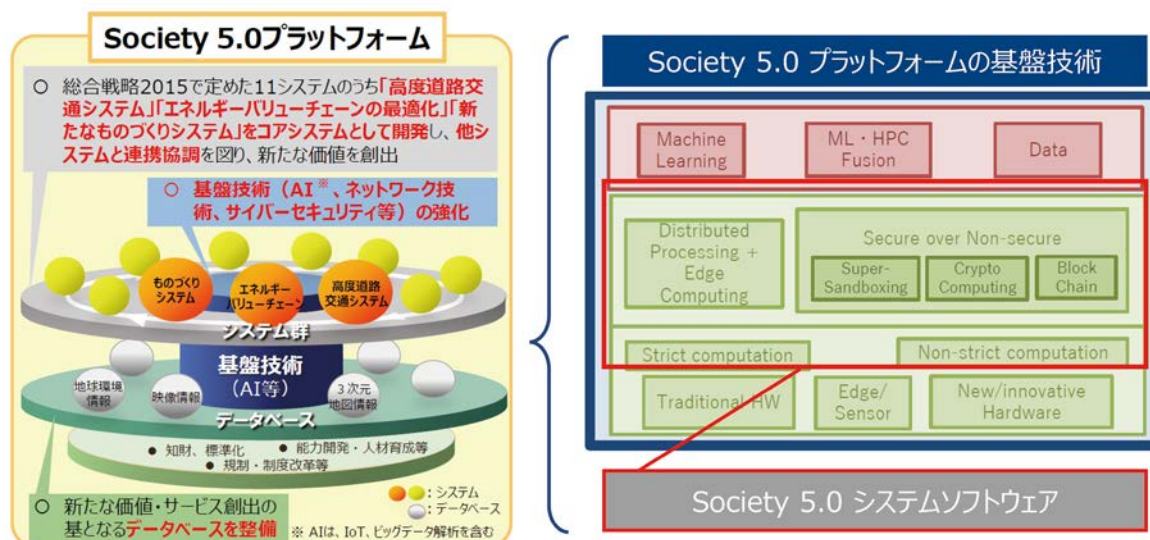


図 1-2 Society 5.0プラットフォームとSociety 5.0システムソフトウェア
(内閣府公開資料と文部科学省情報委員会資料をもとに作成)

(2)「理論×システム基盤技術」による安心安全なSociety 5.0情報処理基盤の構築

本提案で、情報科学技術の基盤技術のうち、セキュリティー、プライバシー、プラットフォームに関わる課題を解決するための研究開発を取り上げたのは、それらがSociety 5.0時代の社会システムにおいて優先的に解決すべき共通課題と考えるからである。以下、個別の研究開発課題の説明に入る前にこれらの課題に共通する基本的な考え方を述べる。

2020年6月に実施したワークショップ「Society 5.0システムソフトウェア」⁵にて、情報処理学会の五つの研究会（アーキテクチャー、OS、セキュリティー、データ保護、プログラミング言語）から約40名の研究者が、システムソフトウェアに関わる技術の俯瞰と、研究動向の現状・課題や今後の取り組みの方向性を議論した。その結果、分野間の連携や交流の強化と合わせて、「理論×システム基盤技術」で安心安全なSociety 5.0情報処理基盤を構築するという考え方が導出された。

5 科学技術振興機構, 科学技術未来戦略ワークショップ報告書「Society 5.0システムソフトウェア」, CRDS-FY2020-WR-04

特に強調されたのは理論の研究者⁶と組むことの重要性である。情報科学技術の分野では、計算機科学の創成期から、常に基礎（理論）と基盤（システム基盤）は連動しながら発展してきた。アルゴリズム理論の導入による新しい実用手法が、一方で現在の情報社会を先導し、他方でGAFAに代表されるIT企業を育ててきたと言える。例えば、検索エンジン（PAGERANK）、暗号（RSA 暗号）、プライバシー（差分プライバシー）など社会・経済的意義は計り知れない。ムーアの法則の限界からハードウェア単独での性能向上の達成が難しい場合でも、理論研究（アルゴリズムや最適化など）でブレイクスルーする可能性がある。

（3）信頼できないハードウェアやOSを含む計算環境で安全なシステムを構築可能とするセキュリティ技術の創出

セキュリティに関しては、これまでインターネットを経由した攻撃が主たる脅威だったものが、近年はそれに加えて、ハードウェアやOSなど計算環境のコアに関わる新たなぜい弱性を狙った脅威が現れ始めた。そのため、これまでより一歩進んだ、信頼できない計算環境でも安全に正しく動くソフトウェアを動作させる技術が必要となる。具体的な研究開発課題としては、安全性指向コンピューターアーキテクチャー技術、信頼できる隔離実行環境の構築技術およびエッジからクラウドまでの総合的なセキュリティを実現するセキュアOS技術などが挙げられる。

ネットワークセキュリティに関しては、ゼロトラストセキュリティという考え方が主流になりつつある。これまで外部のネットワークは信用できないのでファイヤーウォールや侵入検知ソフトウェアなどで外部からの攻撃を防ごうという考え方であったものが、外部だけではなく内部も含めてすべてのネットワークは信用できないので、エンドツーエンドでセキュリティを確保しようという考え方である。しかしながら、2018年に発見されたMELTDOWNやSPECTREというCPUのぜい弱性をついた攻撃が現実のものになることを考えると、アプリケーションが動くCPUやOSすら信頼できないと考えなければならないことになる。

（4）オープンな環境でもプライバシーを確保するデータ収集・解析技術の創出

データ駆動社会においてデータは重要な資産であり、個人情報や企業の機密情報、研究データは安全に管理しつつ活用することが求められる。データの統合利活用を促す動きとして、ここ数年、わが国でも、改正個人情報保護法をはじめ法制度が着々と整ってきた（2章表2-2参照）。これらを支える安心・安全なデータ利活用のためのプライバシー技術がますます重要になっている。

しかし現実には、システムのぜい弱性を悪用した漏えいや改ざんなどの事象にはとどまる兆しが見えない。プライバシー確保に関しても、これまでより一歩進んだ、オープンなネットワーク上のデータは見られるという前提のもとで、データの秘匿性を確保する技術が求められる。具体的には、秘密計算によるトラスト確保技術、相互に信頼できる範囲や開示レベルを動的に制御可能な分散認証技術、秘密計算に基づく分散データ収集・解析技術などの研究開発課題が考えられる。また、準同型暗号やマルチパーティーなど従来の代表的なプライバシー技術は、計算量が多い等の問題があり、理論的なブレイクスルーによる高速化が期待される。

（5）データの自由な流通と個人情報の安全性確保を両立するデータ駆動プラットフォーム研究

研究成果は実社会に貢献することで社会的な意義を持つ。本提案においては、研究成果は、Society 5.0時代の安心・安全・信頼を支える基盤ソフトウェア技術として、プラットフォームに適用することを最終的な目標と考える。プラットフォーム技術においては、従来のような後追いの対処ではない、システム全体をby-

6 計算機科学は数学の応用分野の一つなので、基礎理論の研究者には、計算機科学の研究者と数学の研究者の両方を含む

Design⁷の観点で捉え、きめ細かいセキュリティ要件とプライバシー確保を担保した上で、データの流通と情報処理を可能とすることが求められる。ただし、現時点で巨大IT企業のもつプラットフォームを置き換えることは現実的でないため、本提案では既存のさまざまな実行環境（CPU、OS、仮想化等）からなるハイブリッドなハードウェアやOS上で動作させることを前提に置く。具体的な研究開発課題として、多様な実行環境からなる分散データ処理環境の管理・制御技術、セキュリティ・プライバシー処理の高性能実装技術、データの真正性証明や来歴保証技術などがある。

（6）理論的な考察・検証からプロトタイプソフトウェアの開発・検証まで

高度化・複雑化するICT環境を想定した本提言におけるセキュリティ・プライバシー研究は、基礎研究による理論的な考察・検証に加え、応用研究としてのプロトタイプソフトウェアの開発や実社会での利活用を想定した動作や効果の検証・評価を、並列して進める事が重要である。さらに、短期と中長期の研究開発を有機的に連携させ、基盤ソフトウェア領域のシームレスな研究開発戦略の実施が、来たるデジタル社会の安心・安全・信頼の実現に必須である。

特にシームレスな研究開発の推進においては、研究成果を要素技術ごとに、又はパッケージ化して、例えばGitHub⁸等でOSS（オープンソースソフトウェア）として公開し、利活用と社会実装を促進する運営が重要と考える。また、研究開発プロジェクトを多彩な人材が集い切磋琢磨する人材育成の礎の場とし、文部科学省主導のもと産官学が一体となり戦略目標達成型の研究開発を行うことが適切である。2030年以降、最終的にGAFAと国産の基盤技術が相互利用されたプラットフォームの実現を目指し、国内においては、デジタル革新・データ駆動によりさまざまな社会課題を解決し、より人間的で幸福な社会であるSociety 5.0の実現（Society 5.0サービスシステムの構築）に本提案成果を繋げていきたい。

7 バイデザイン（by-Design）とは、情報システムの企画・設計段階から、セキュリティやプライバシーを確保するための方策を考慮し、設計・構築・運用することをいう。事象が発生後の後追いの対応に比べ、迅速かつ低コストに対応できると言われる。

8 GitHub（ギットハブ）は、版管理ソフトGitの仕組みを利用して、プログラマーがソフトウェアの公開と共有ができるウェブサービスである。特にOSSの開発において世界中で使われている。

2 | 研究を実施する意義

2.1 現状認識と問題点

(1) Society 5.0におけるシステム基盤ソフトウェアの必要性

2020年に世界を襲った新型コロナウイルスは人類の経済活動、社会活動に大きな打撃を与え、人々の生活や労働、教育などに多大なる影響を与えた。世界が先の読めない不確実な時代にあることを痛感させたが、ITの有効性を示すこともできた。在宅勤務や在宅学習が広く行われ、多くの人々がインターネットを介したサービスを利用し、昼間の時間帯の通信量は3割程度増加した。幸い、わが国においてはネットワークの輻輳やサービスシャットダウンなどの事態には至らなかったが⁹、今後も想定されるさまざまな状況においても、持続的かつ強靱な社会・経済構造を支える、強靱かつ柔軟なシステム基盤が必要である。しかるに、わが国はITプラットフォームを海外に依存している。米中の技術競争も激化している中、わが国の競争力は低下している。今のままでは、デジタル革新によりさまざまな社会課題を解決し、より人間的で幸福な社会を実現することは困難である。

2016年1月に閣議決定された第5期科学技術基本計画¹⁰において、わが国が目指すべき未来社会の姿としてSociety 5.0が示された。これは、サイバー空間（仮想空間）とフィジカル空間（現実空間）を高度に融合させたシステムにより、人とモノがつながり、さまざまな知識や情報が共有され、今までにない新たな価値を生み出す経済発展と社会的課題の解決を両立する人間中心の社会である。現在検討中である第6期科学技術・イノベーション基本計画においても、わが国が目指すべき社会として、「国民の安全と安心を確保する持続可能で強靱な社会」と「一人ひとりの多様な幸せ（Well-being）が実現できる社会」が具体的に挙げられている¹¹。

Society 5.0を実現するためには、システム基盤ソフトウェアがまさに重要な役割を果たす。まず、安全と安心を確保するためには、信頼できないハードウェアやOSを含んだ計算環境でも安全なシステムを構築できなければならない。さらに、多様な幸せを実現するためには、さまざまなサービスやソフトウェア、プラットフォームが混在するようなオープンな環境でもプライバシーを保護したままデータの収集、解析ができるようなデータ駆動プラットフォームが必要となる。

(2) サービスプラットフォームの現状

現実にはGAFAMが席巻

現状のインターネット上のサービスを見ると、検索エンジンやメール、SNS、あるいは音楽配信、通信販売など、多くのサービスにおいていわゆるGAFAM（Google、Amazon、Facebook、Apple、Microsoft）と呼ばれる米国のプラットフォーム事業者が市場を席巻している。検索エンジンにおいてはGoogleが全世界の検索のうち、91.38%という圧倒的な占有率である¹²。SNSにおいても、Facebookが

9 総務省総合通信基盤局データ通信課、「新型コロナウイルス感染症の影響下におけるインターネットトラフィックの推移について」、https://www.soumu.go.jp/main_content/000692609.pdf

10 第5期科学技術基本計画、<https://www8.cao.go.jp/cstp/kihonkeikaku/5honbun.pdf>

11 第6期科学技術基本計画答申素案、https://www8.cao.go.jp/cstp/stmain/6ki_tosinsoan.pdf

12 Statcounter, "Search Engine Market Share Worldwide – December 2020", <https://gs.statcounter.com/search-engine-market-share>

68.39%を占めており¹³、ユーザ数においても2020年時点での月間アクティブ利用者数は27億4,000万人にのぼる¹⁴。これは消費者向けサービスだけではなく、ビジネスを対象としたクラウドコンピューティング事業においても、Amazon、Microsoft、Googleの3社で全世界のクラウドインフラサービスの58%のシェアを有している¹⁵。

GAFAMの強みはビジネスモデルだけではなく、基本ソフト、技術が強みの源泉

Googleは検索サービスを利用したインターネット広告、FacebookもSNSをベースとした広告事業が中心である。Amazonはネットショップの運営に加えてクラウドコンピューティング事業に強みがある。それぞれに巧みなビジネスモデルを持ち、強い事業を展開しているが、ビジネスを支える強力な基本技術を持っている。表2-1にその特徴をまとめる。

表 2-1 GAFAM プラットフォームの特徴¹⁶

企業名	概要	エネルギー	セキュリティ	プラットフォーム
Google	自社のビジネスである広告、検索などの業務と、Cloud事業としてのデータセンター	2018年から再生可能エネルギー率100% データセンターの効率を2倍にし、PUEを1.11に AIを使って再生可能エネルギー利用を推進	サイバー攻撃からの防御だけでなく、物理的なセキュリティ、通信の保護にも注力	コンテナを活用し、運用を管理 独自サーバーを活用
Amazon	主にCloud事業	パリ協定を10年前倒しで実現、2040年に炭素排出量をゼロに 物流などのリアルビジネスも2024年までに再生可能エネルギー率を80%に、2030年には100%	顧客システムの構成管理 データセンター内/間データの暗号 顧客IDとアクセスコントロール API監視、ロギングなど	仮想化されたサーバー、ストレージの上に、AIやIoTなど豊富な機能をセキュアに提供
Facebook	自社のSNSサービス事業	2020年に再生可能エネルギー率を100%に 水利用率を80%以上向上 高温で動作可能なハードウェアにより、外気冷却で消費エネルギーを低減 AIを利用したデータセンター効率化	プロフィール、投稿の共有範囲の設定、ブロックなどのプライバシー保護 ログインアラート、二段階認証などのアカウント管理	Open Compute Projectにより、製品とデータセンター運用のベストプラクティス収集 OSSに熱心
Apple	iCloudはAmazon、Googleを利用 自社製品に注力	製品を中心に省電力化 新しい本社の屋根にソーラーパネル	バイオメトリクスなどで端末を保護 端末内データは暗号化 アプリケーション認証	製品はプロプライエタリ データセンターはアウトソース
Microsoft	自社製品とCloud事業としてのデータセンター	製品を中心に省電力化	シングルサインオン、多要素認証などのIDとアクセス管理 エンドポイントセキュリティ、ふるまい検知などの脅威対策	自社製品で端末からデータセンターまで強力な連携

¹³ Statcounter, "Social Media Stats Worldwide - December 2020", <https://gs.statcounter.com/social-media-stats>

¹⁴ Facebook 社 2020 年第 3 四半期（7 月～9 月）業績ハイライト, <https://about.fb.com/ja/news/2020/10/2020-third-quarter-results/>

¹⁵ Canalys, « Global cloud infrastructure market Q3 2020 », <https://www.canalys.com/newsroom/worldwide-cloud-market-q320>

¹⁶ https://services.google.com/fh/files/misc/google_2019-environmental-report.pdf
<https://sustainability.aboutamazon.com/sustainable-operations/amazon-co-founds-the-climate-pledge-setting-goal-to-meet-the-paris-agreement-10-years-early>
<https://sustainability.fb.com/>
https://www.apple.com/euro/environment/pdf/a/generic/Apple_Environmental_Responsibility_Report_2019.pdf
<https://www.microsoft.com/en-us/devices/sustainability-report>
<https://cloud.google.com/security/overview/whitepaper?hl=ja>
https://d1.awsstatic.com/whitepapers/Security/Intro_to_AWS_Security.pdf?did=wp_card&trk=wp_card
<https://support.apple.com/ja-jp/guide/security/secdd5016d31/web>
<https://www.microsoft.com/ja-jp/security/business/solutions>
<https://clonos.jp/knowledge/detail11/>
<https://japan.cnet.com/article/20390984/>

(3) わが国のIT基盤技術の現状

ハードウェア、基本ソフトはほとんど海外

1980年代、わが国の情報処理産業においては今のような寡占化が進んでいなかったため、各社がプロプライエタリーなハードやOSを開発し、製造・販売を行っていた。企業にも大学にも研究者や開発者が多くおり、OSやコンパイラなどの開発が研究開発として成立していた。1990年代以降の情報システムのオープン化、コモディティ化により、国産のプラットフォームが淘汰されたために、ハードウェアや基本ソフトのなどの基盤構築に関わる研究開発が廃れてしまった。マーケットの変化もあり、アプリケーションやサービス開発が研究の主たる対象となった。これは経済合理性を考えると企業としては正しい判断ではあったが、ハードウェアや基本ソフトウェアの分野の研究者は産学とも応用領域や別の研究領域に移ってしまった。

研究開発でもプレゼンスが低い

海外製品への依存に伴い、産学での研究開発も基盤から応用領域へシフトし、基盤領域での研究開発プレゼンスも低下した。関連分野の論文発表数を調査してみると、図2-1に見るように、全体傾向としては1980年代から全期間を通じて当分野の論文および知財は堅調な伸びを示しており研究開発活動は活発であった。国別では米国が圧倒的だが過去20年で中国が猛追、独英仏および日本がその次に位置するが、近年インドが躍進している。著者所属機関は10位以内に米国5、中国4、フランス1、日本は18位に日本IBM、38位に東大が入るだけである。

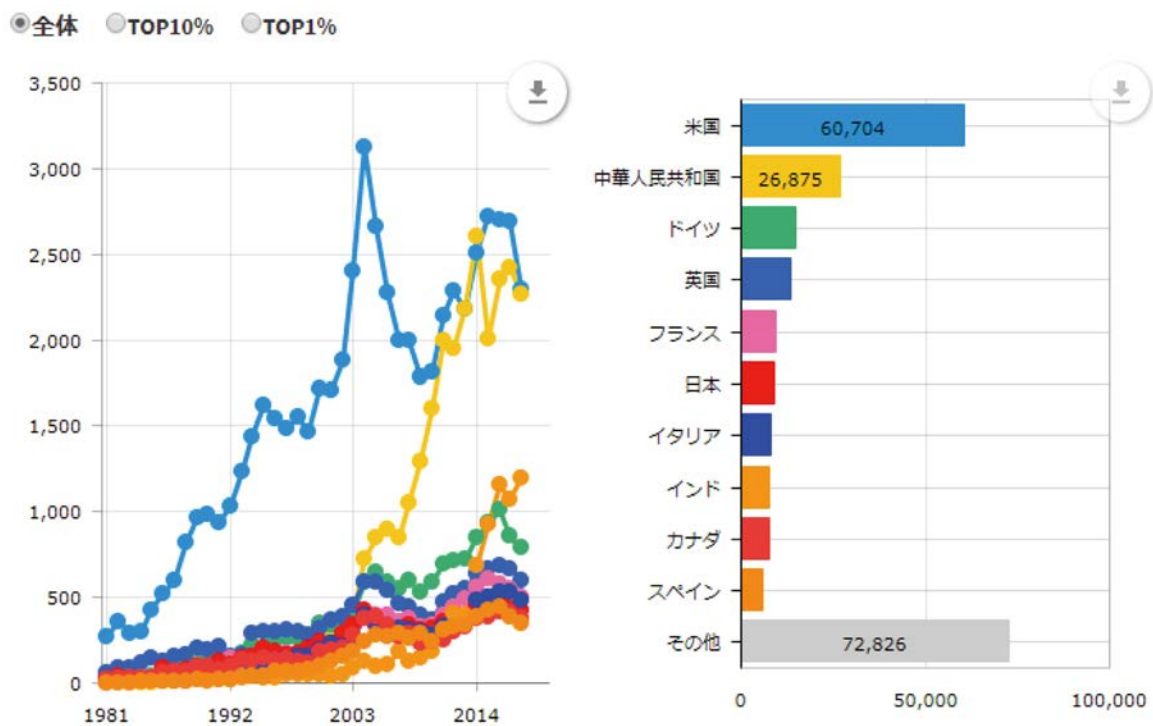


図 2-1 計算機基盤領域の論文動向¹⁷

¹⁷ ソース：論文（Scopus、FMDDB）、特許（PATSTAT）
 検索キーワード：“Operating System” OR “Programming Language” OR “Virtual Machine”
 文献数：224,971、被引用数：2,707,237、著者数：約392,000

海外製品やサービスに依存することの危険性

このように我が国はハードウェアやOS、サービスプラットフォームまで海外に依存しており、巨大IT企業に対抗することは困難であるが、そのデータ覇権に支配されることなく、自由なデータ流通と個人情報保護を両立する枠組みを実装することが求められている。例えば、下記のように、海外の製品やサービスに依存してしまうことは危険である。

●プラットフォームは信頼できない

Googleではショッピング情報提供等のサービスにサインアップした何百万ものGmail利用者の受信箱を何百人ものサービス開発者がスキャンしていたと言われている¹⁸。Facebookはユーザーの情報をCambridge Analytica社が利用するのを黙認していた¹⁹。このようにわが国の法律や規制の届かないプラットフォームに依存しきってしまうことには危険がつきまとう。海外のクラウドに企業や政府の機密情報を預けるというのは危険である。

●システムも信頼できない

2019年の1年間で公開サーバーが攻撃を受けた被害の公表事例86件のうち約52%が公開サーバーにおけるシステムのぜい弱性を悪用されており、AWS（Amazon Web Service）上で公開されるミドルウェアやOSのぜい弱性が深刻である²⁰。AWSといえども安心して運用できるとは限らない。

●ネットワークも信頼できない

2019年4月のブルームバーグによる、中国政府に情報が流れていることを報告する記事を発端に、欧州や米国ではHuawei製品導入を控える（締め出し）という社会問題が起きている²¹。通信事業者が運用する公衆通信ネットワークは安全であると思われていた神話が崩壊している。5Gに関しても、特定のメーカーの機器に依存することが問題となり、米英と協調して調達先の多様化を目指すという動きが出ている。

●ハードウェアすら信頼できない

2018年にマイクロプロセッサのぜい弱性問題としてMELTDOWNとSPECTREが発表された²²。これは投機的実行を実装したCPUで本来アクセスできないメモリ領域を読み出してしまうぜい弱性でIntelやAMDなど多くのマイクロプロセッサにて発生する可能性がある²³。本来はプロセッサメーカーで対処すべきであるが、任せきりにせず、上位のソフトウェアやサービスとして対抗策を考えるべきである。

(4) 政府の取り組み

このような状況の中、わが国政府においてもデータの保護と流通に向けた取り組みが活発に行われている。

●データ・フリーフロー・ウィズ・トラスト（DFFT）

デジタル時代の競争力の源泉である「データ」は、特定の国が抱え込むのではなく、プライバシーやセキュ

18 Google Blog, "As G Suite gains traction in the enterprise, G Suite's Gmail and consumer Gmail to more closely align", <https://blog.google/products/gmail/g-suite-gains-traction-in-the-enterprise-g-suites-gmail-and-consumer-gmail-to-more-closely-align/>

19 BBC Japan, "フェイスブックのデータ不正共有疑惑「8700万人に影響」", <https://www.bbc.com/japanese/43650517>

20 TRENDMICRO, "AWS環境の公開サーバに対するセキュリティ検討ガイド", <https://resources.trendmicro.com/jp-docdownload-form-t294-sem-aws2.html>, P9

21 Bloomberg, "華為の問題は製品の不具合、予想以上に脆弱か", <https://www.bloomberg.co.jp/news/articles/2019-04-01/PP9I7V6JTSE801>

22 Google Project Zero, "Reading privileged memory with a side-channel", <https://googleprojectzero.blogspot.com/2018/01/reading-privileged-memory-with-side.html>

23 TRENDMICRO, 投機的実行に関するぜい弱性「Meltdown」と「Spectre」について解説, <https://blog.trendmicro.co.jp/archives/16735>

リティー・知的財産などの安全を確保した上で、自由に流通することが必要である²⁴。

●デジタル革新（デジタルトランスフォーメーション）

新型コロナウイルス感染症対策において、デジタル革新が極めて有効であることが世界各国で実証されている。医療、教育、行政、金融、製造業等の各分野において徹底した規制改革とデジタル化・データの共有等を進め、データ駆動社会を構築する²⁵。

●Trusted Web 推進協議会

2020年6月16日デジタル市場競争会議において公表された「デジタル市場競争に係る中期展望レポート」²⁶に基づき、将来の競争構造の変化を睨み、データ・ガバナンスのあり方をテクノロジーで変える分散型の“Trusted Web”の構築を進めるための官民の連携体制として設立した²⁷。

●データの統合利活用を促す法制度

データ駆動社会においてはデータは重要な資産であり、個人情報や企業の機密情報、研究データは安全に管理されつつ活用することが求められる。データの統合利活用を促す動きとして、ここ数年、法制度が着々と整ってきた（表2-2）。

表 2-2 データ統合利活用を促す動き²⁸

改正個人情報保護法（2017） －データ利活用とプライバシー保護の両立
次世代医療基盤法（2018） －匿名加工医療情報等の取扱いに関する規制を定める
「情報銀行」認定事業（2018） －民間事業者が個人データを収集・管理し、第三者の事業者提供
IoT 投資減税（2018） －セキュリティ対策が講じられたデータ連携・利活用への投資を支援

多くの取り組みが進められており、わが国のデジタル化がいっそう進展することが期待される。しかし、これらは上位のサービス層やアプリケーション、あるいはビジネスや政策に関連する内容であり、最も基本的な競争力として、Society 5.0を実現するためのシステムソフトウェアの研究開発も必要であろう。

24 首相官邸、“世界経済フォーラム年次総会 安倍総理スピーチ”，
https://www.kantei.go.jp/jp/98_abe/statement/2019/0123wef.html

25 首相官邸，“デジタル改革関係閣僚会議”，https://www.kantei.go.jp/jp/99_suga/actions/202009/23digital.html

26 デジタル市場競争会議，“デジタル市場競争に係る中期展望レポート（案） ～ Society 5.0 におけるデジタル市場のあり方～”，
<https://www.kantei.go.jp/jp/singi/digitalmarket/kyosokaigi/dai4/siryou3.pdf>

27 首相官邸，“Trusted Web 推進協議会”，https://www.kantei.go.jp/jp/singi/digitalmarket/trusted_web/index.html

28 盛合志帆，“安心・安全な Society 5.0の実現にむけて ～プライバシー保護データ解析技術の現在～”，CRDS-FY2020-WR-04, p10

コラム

Society 5.0 と DX（デジタルトランスフォーメーション）

Society 5.0は、2016年に策定された第5期科学技術基本計画に基づき、わが国が目指すべき未来社会の姿として提唱されたものであり、SDGs（Sustainable Development Goals）のJapan Modelという位置づけである。Society 5.0で実現する社会は、IoT（Internet of Things）で全ての人とモノがつながり、さまざまな知識や情報が共有され、今までにない新たな価値を生み出し、また、人工知能（AI）により、必要な情報が必要な時に提供され、ロボットや自動走行車などの技術で、少子高齢化、地方の過疎化、貧富の格差などの課題が克服される社会である。社会の変革（イノベーション）を通じて、これまでの閉塞感を打破し、希望の持てる社会、世代を超えて互いに尊重し合あえる社会、一人一人が快適で活躍できる社会である。2021年度より実施される第6期科学技術・イノベーション基本計画においてもSociety 5.0はわが国が志向すべき未来社会像として位置づけられており、実現に必要なものとしてサイバー空間とフィジカル空間の融合と社会全体の再設計（リデザイン）が記載されている。

このコンセプトは、情報通信技術の浸透が人々の生活をあらゆる面でより良い方向に変化させる、「DX（デジタルトランスフォーメーション）」により導かれる未来像である。

Society 5.0の前提となるDXについて振り返ると、あらゆる分野でIT化を進めていたものの、既存業務の効率性の向上を目指す取組が中心となり、諸外国のようなデータ連携・活用によるいわゆるプラットフォーム型の新たなビジネスモデルの創出などは十分に行えず、情報通信技術の持つ本来の力を十分に生かし切れていなかった。また、各組織が異なるシステムでネットワークを閉鎖的に利用している現在の状況では、分野を跨いだリアルタイムでのデータ収集・分析・活用を行う環境が整っていないなど、Society 5.0の実現に向けたDXのための基盤整備は道半ばであった。

この度のコロナ禍により、基盤が整備されない中で半ば強制的に我々に新しい生活様式への移行が強いられ、社会全体のDXが十分に進んでいないことが露呈した。行政のデジタル化の遅れや企業等におけるテレワーク、大学等におけるオンライン教育など、DXに対応した環境整備は、組織・機関によって進捗状況に差があり、しかも社会全体としては、印章文化に象徴される旧来の慣習や、国民の情報セキュリティ・プライバシーに関する強い不安など、今なお技術的課題を超えた多様な社会的課題が残っている。

わが国では、OSやハードウェアの多くを海外に依存しているが、米中対立の先鋭化など地政学的リスクの高まりにより、新たなぜい弱性や情報漏洩等の危険性も指摘されている。また、欧州で一般データ保護規則（GDPR）が施行され、わが国でも個人情報保護法の見直しが行われる等、プライバシー意識が向上している。さらに、今回のコロナ禍で問われた国難級の災害に対するレジリエンス向上の観点からも、安心・安全・信頼を支える国産の基盤ソフトウェア技術の研究開発が急務である。具体的には、信頼できないハードウェアやOSを含む計算環境で安全なシステムを構築可能とするセキュリティ技術、オープンな環境でもプライバシーを確保するデータ収集・解析技術、データの自由な流通と個人情報の安全性確保を両立するプラットフォーム技術を創出・確立し、それによってわが国のDXを支える社会システムの信頼性を高め、さらに質の高い社会データの存在と結び付け、わが国の未来社会像として国民一人ひとりに幸せ（well-being）をもたらすSociety 5.0を世界に示していかなければならない。

2.2 社会・経済的効果

(1) 社会的効果

Society 5.0という、サイバー空間とフィジカル空間が密接に連動する社会において、プライバシーの侵害やセキュリティの不安なくデータを活用しさまざまな社会課題を解決し、より人間的で幸福な社会や大規模災害や、感染症により物理的な行動が制限されても生活や経済を速やかに復旧できる持続的で強靱な社会を実現することができる。

計算機は、小型化、高性能化、省電力化、ネットワーク化と進化するなかで、計算をするだけの機械ではなく、メディアを含むさまざまな情報処理を行うようになり、人と人とのコミュニケーションを支えるシステムとなった。利用の場も企業から、社会へと広がってきた。それが、第5期科学技術基本計画で提唱されたSociety 5.0へとつながっている。Society 5.0はサイバー空間とフィジカル空間を高度に融合させたシステムにより、経済発展と社会的課題の解決を両立する人間中心の社会である。Society 5.0のサイバー空間はAIといった大規模で複雑な処理を高速、効率的に実行することが求められるが、社会を支えるインフラストラクチャーであることから物理的な社会インフラと同様、いかなる処理であっても安全に実行できて、人が安心して処理を任せられることが必要である。本提案で提案する研究開発は、サイバー空間を安全にかつ安心して利用できるものとするために、本質的な個々の要素技術からプラットフォームの構築までをカバーするものである。

また、Society 5.0は大規模災害や新型コロナウイルスの流行に対して社会の機能を維持し、元の状態にできるだけ素早く戻れるようなレジリエンスを備えることが求められている。2020年に世界中で蔓延した新型コロナウイルスのような感染症は、感染対策として人と人との物理的な接触を制限する。物理的な接触を制限した状態でも社会活動を継続するためには、サイバー空間を上手に利用することが有効であることが新型コロナウイルスの経験からわかった。大規模災害や新型コロナウイルスが流行した場合、サイバー空間はライフラインとなるので、その安全性・安定性は大変重要である。

2019年度の日本における情報セキュリティインシデント458件のうち、最大件数を占めたのは175件の不正アクセスで、2位が129件の情報流出であった²⁹。本提案はこれらのインシデントの発生件数削減に寄与する。

日立製作所と博報堂が2013年度から継続的に実施しているビッグデータを取り扱う生活者情報に関する意識調査³⁰によると、企業や公的機関がパーソナルデータを活用することに対してリスクに対する不安が活用への期待より大きい（利用に対して不安の方が勝る）という割合は50%前後で推移しており、20%前後で推移している期待の方が大きいという層の2倍以上の割合を占めている。不安を覚える理由として、最も多いのは、利用されたくない場合に拒否権がない、が50%前後（重複回答を許す）、企業のプライバシー保護対策が積極的でない、あるいはプライバシー保護のための加工処理を十分におこなっていない、という項目を挙げる割合がそれぞれ20%程度存在している。

また、みずほ情報総研が発表した、令和元年度データの流通環境等に関する消費者の意識に関する調査研究の請負報告書³¹によると、一般国民に対するアンケート調査の結果、パーソナルデータを提供することに対して、日本、アメリカ、ドイツ、中国のいずれも6～8割の人が不安を感じており、特に日本は78.2%と、この4カ国の中で一番高い。

29 情報処理推進機構、情報セキュリティ白書 2020

30 日立製作所、ニュースリリース「第五回 ビッグデータで取り扱う生活者情報に関する意識調査」を実施、<https://www.hitachi.co.jp/New/cnews/month/2020/12/1222a.html>

31 総務省、令和元年度 データの流通環境に関する消費者の意識に関する調査研究の請負 ー 報告書ー、https://www.soumu.go.jp/johotsusintokei/linkdata/r02_04_houkoku.pdf

さらに、平成29年版情報通信白書³²でも、パーソナルデータの利活用は他国と比較して活用度がやや低く、利活用における課題・障壁として、個人データの管理に伴うインシデントリスク・社会的責任の大きさを挙げる企業が多いためとしている。

このように、パーソナルデータの活用に対しては漠然とした不安をいだく人が多いが、どのようなプラットフォームでも安全に処理が行われ、常に暗号化した状態で処理することで、仮に情報流出しても悪用される危険性が少なく、さらに自分のデータを自分でコントロールできるデータ主権が設定できるような技術が開発されれば、こういった不安が減少し、個人データの活用がさらに進むと考えられる。また、今のところ企業は自身が持っているデータを他社に利用させることに消極的だが、安全にデータを集めて処理できれば、各社が保有するパーソナルデータを持ち寄ることでより精度の高い機械学習を実行するといった、協業のメリットを享受することができるため、データ提供のハードルが下がる可能性がある。

なお、2020年10月に実施された日立製作所と博報堂のアンケート調査結果によると、新型コロナウイルス感染拡大防止対策として個人データを活用することは、利用目的が明確であれば、より踏み込んだデータ活用を容認する傾向がみられるとのことである。安全性を担保できる技術が普及すれば、こういった非常時に限定的に個人データを平時よりも踏み込んで利用することへの理解も得やすいのではないだろうか。

このように、プライバシーの侵害やセキュリティの不安なくデータを活用しさまざまな社会課題を解決し、より人間的で幸福な社会や大規模災害や感染症により物理的な行動が制限されても生活や経済を速やかに復旧できる持続的で強靱な社会を実現することができる。

(2) 経済的効果

コンピューターセキュリティは、マルウェアやスパイウェアといったコンピューターウイルスによる秘密情報の漏えい、あるいはランサムウェアによる金銭やビットコインの要求など、直接的な経済被害だけでなく、企業の社会的信用の失墜という間接的被害も生じさせる。つまり、コンピューターセキュリティ技術はマイナスの経済的効果を減少させる効果がある。一方、個人データを適切に管理し、活用することができれば、ユーザーにとっての利便性が増し企業の収益拡大や新たな市場の創出につながるというメリットがあるため、プライバシー保護技術はプラスの経済的効果を生む。

日本ネットワークセキュリティ協会の2018年情報セキュリティインシデントに関する調査報告書【速報版】³³によると、2018年の個人情報漏えいのインシデント数は443件で、想定損害賠償額は2684億5743万円にもなるとのことである。インシデントの原因としてはPCの紛失・置き忘れが最多で116件であるが、不正アクセスによるものも90件（全体の約20%）あり、近年は増加傾向にある。個人情報がすべて暗号化されて、プラットフォーム上に置かれ、復号化されことなく処理がなされるようになると、不正アクセスによって暗号化されたデータが流出しても、悪用されることがないため、想定損害賠償額の20%、約500億円を減らすことに貢献できる。

また、日本サイバーセキュリティ・イノベーション委員会の調査³⁴によると、日本国内で情報流出等の適時開示を行った企業の株価は平均10%下落し、純利益は平均21%減少していたという。セキュリティ事故はこのように、間接的な被害も及ぼすため、個人情報の安全性を確保することで、間接的被害額も減らすことが可能である。

32 総務省、平成29年度 情報通信白書、
<https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h29/pdf/index.html>

33 日本ネットワークセキュリティ協会、2018年 情報セキュリティインシデントに関する調査報告書【速報版】、
<https://www.jnsa.org/result/incident/2018.html>

34 日本サイバーセキュリティ・イノベーション委員会、取締役会で議論するためのサイバーリスクの数値化モデル、
[https://www.j-cic.com/pdf/report/QuantifyingCyberRiskSurvey-20180919\(JP\).pdf](https://www.j-cic.com/pdf/report/QuantifyingCyberRiskSurvey-20180919(JP).pdf)

一方、データを活用することはあらゆる産業分野で、デジタル革新として推進されている。特に個人データを活用することで売り上げの向上や品質向上に寄与するのは、個人相手のビジネスを展開しているサービス産業である。統計局のサービス産業動向調査³⁵によれば2019年のサービス産業売上高は約380兆円である。2020年は新型コロナウイルス感染症の影響でサービス産業の売上が減少すると思われるが、個人データを活用することでこの市場の拡大を支援することができる。情報通信総合研究所が2020年3月に発表した、デジタルデータの経済的価値の計測と活用の現状に関する調査研究の請負報告書³⁶によると、公共データの利用が日本の経済全体に与える波及効果は2.4～4.7兆円と見積もる先行研究があり、個人データの活用も同様な波及効果が期待できる。

2.3 科学技術上の効果

(1) 社会の安心・安全・信頼に資する基礎理論の構築

基礎（理論）と基盤（システム基盤）の研究者が連携して同じ課題に取り組むことで、Society 5.0時代のシステム基盤に資する基礎理論を構築する。理論に関しては数学分野の研究者をプロジェクトに参画させることが重要である。いうまでもなく、数学は自然科学・工学、社会科学や医療の基礎力を高める要である。数学の持つ抽象性は思考の整理や課題の本質の洗い出しに役立ち、技術の汎用性の確保にもつながる。特に、情報科学技術の分野では、計算機科学の創成期から、常に理論とシステム基盤は連動しながら発展してきた。アルゴリズム理論の導入による新しい実用手法が、一方で現在の情報社会を先導し、他方でGAFA等のIT企業を育ててきたと言える。例えば、検索エンジン（PAGERANK）、暗号（RSA暗号）、プライバシー（差分プライバシー）など社会・経済的意義は計り知れない。ムーアの法則の限界からハードウェア単独での性能向上の達成が難しい場合でも、理論研究（アルゴリズムや最適化など）でブレークスルーする可能性がある。

また、技術と密接な関係にあるのが、情報システムや情報サービスにおける安心・信頼の背景にある「トラスト」の研究である。技術的な信用の担保だけではなく、人間の心理的な要素や、制度による保証などもあわせて、多面的に考慮することが重要になってきている。心理学や社会学（法律、政治学）、経済学などの人文・社会科学の研究者との連携や、一歩進んでデータ駆動社会を支える融合分野の人材育成が従来以上に必要な分野である。

以上述べたような取組みを行うことで、社会の安心・安全・信頼に資する基礎理論を構築することができる。

(2) 高度化・複雑化し続けるセキュリティ・プライバシー課題の根本的な解決方式の確立

高度化・複雑化し続けるセキュリティ・プライバシーの課題に対し、アーキテクチャーからOS、データベース、セキュリティ、言語の研究者が一丸となって取り組むことで、後追いでない解決方式を確立することが期待できる。情報セキュリティの脅威は、個人の情報端末や企業の情報システムのネットワーク化に従って拡大してきた。不正アクセス、ウイルスなどのマルウェア、標的型アタックなど、情報システムのぜい弱性をついた攻撃は高度化・複雑化し続けている。情報システムのぜい弱性とは、本来、プログラムやシステムの不具合や設計上のミスが原因となって発生した情報セキュリティ上の欠陥のことをいうが、近年、CPUの実行速度向上のために搭載される投機実行機能とキャッシュの実装そのものを狙った攻撃方法（Meltdownと

35 総務省統計局、サービス産業動向調査、<https://www.stat.go.jp/data/mssi/>

36 総務省、デジタルデータの経済的価値の計測と活用の現状に関する調査研究の請負報告書、https://www.soumu.go.jp/johotsusintokei/linkdata/r02_05_houkoku.pdf

Spectre) が報告され、これまでCPUは安全だと信じていた人々を驚かせた。

攻撃者はシステムが一番弱い（ぜい弱な）部分を狙うため、システム全体をby-Designの観点で、きめ細かいセキュリティ要件とプライバシー確保を担保できるような方式をシステム全体の設計に盛り込んでおく必要がある。ぜい弱性の特定や対策方策の考案に関しては、アーキテクチャーからOS、データベース、セキュリティ、言語の研究者が一丸となって、システムエンジニアのシステム構築に参画する。ただし、システムの脅威はユースケースごとに異なるため、4章に記載するように、具体的なターゲットシステムを定めることで、根本的な解決方法を段階的に確立してゆくことができる。

（3）情報科学の基盤分野のコミュニティの再構築と国際連携の強化

海外と積極的に交流してわが国の研究力を高揚させるとともに、研究成果を論文だけでなくOSSとして発信することで国際社会に貢献する。1966年から1972年にかけて通商産業省が実施した超高性能電子計算機プロジェクト³⁷の結果、わが国の情報科学の分野の競争力は世界に伍する位置まで向上した。しかし、1990年代以降の情報システムのオープン化、コモディティ化により、わが国は基盤構築に関わる研究開発の機会を喪失し国際的な競争力を失った。一方、学術界においても基盤研究への研究投資を怠ったために、スーパーコンピュータ³⁸を除いて研究力は大幅に低下した（図2-2）。

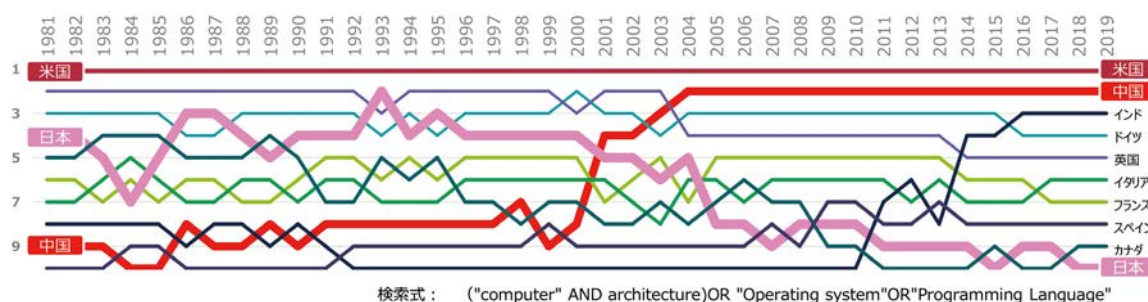


図 2-2 基盤ソフトウェア関連の論文数ランキング（1981～2019）

すでに述べた通りGAFAの競争力の源泉はビジネスモデルとそれを支える情報科学技術の基盤である。情報科学技術の基盤をおろそかにしては、Society 5.0が目指す社会を実現することはおぼつかない。さらに、国際的にも、情報科学技術の基盤なしに、わが国がIoT（Internet of Things）やロボット活用などの強みを生かして競争力を強化することは難しい。

失った研究力を取り戻すのは簡単ではないが、歴史に学べることは、基盤分野への研究開発投資を継続して、人材育成と研究コミュニティの再構築を促進することが有力な手段であるということである。システム基盤の研究開発は机上や実験室で完了するものではないため、実システムへの適用・評価が不可欠であることは言うまでもない。

また、国際連携も重要である。今回のような課題の解決は一つの国の力だけでは難しい。海外の一流の研究者を招くこと、海外のファンディングエージェンシーとの共同プロジェクトを運営することなど、国際連携の機会を設けることが、国際貢献そのものであり、ひいてはわが国の研究者の実力を向上させる。

37 情報処理学会コンピュータ博物館, 大型プロジェクト超高性能電子計算機開発スタート, <https://museum.ipsj.or.jp/computer/main/0109.html>

38 文部科学省「次世代IT基盤構築のための研究開発」や後継の数々の開発投資により国際競争力が向上した

3 | 具体的な研究開発課題

Society 5.0 プラットフォームに求められる、柔軟かつ堅固なシステム基盤を実現するために、理論とシステム基盤が高度に連携した研究開発を推進する（図3-1）。これにより、Secure & Safe & Trustworthyな（安心、安全、信頼できる）システムソフトウェアの実現を目指す。

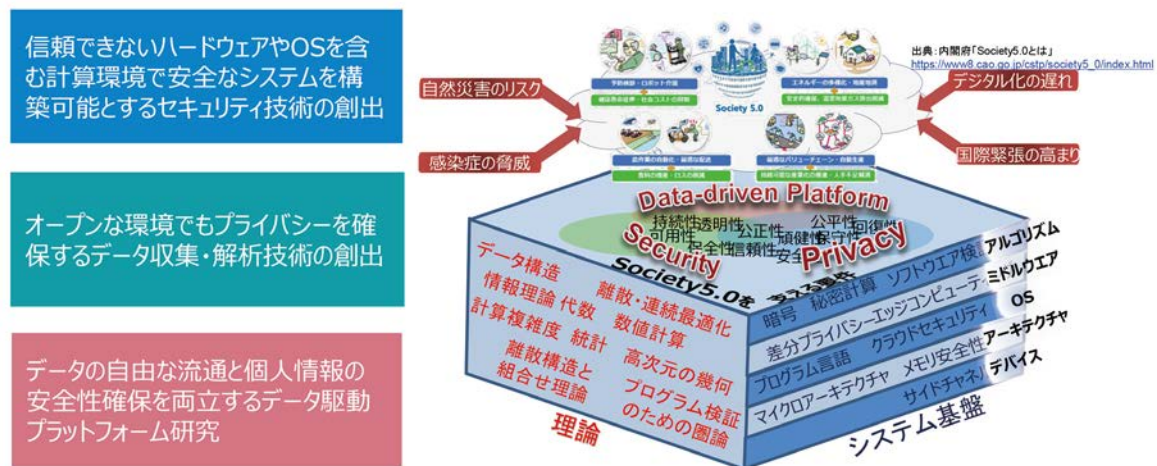


図 3-1 「理論×システム基盤」で安心・安全・信頼を支える

3.1 セキュリティーに関する研究開発課題

セキュリティーに関しては、これまでインターネットを経由した攻撃が主たる脅威だったものが、近年はそれに加えて、ハードウェアやOSなど計算環境のコアに関わる新たなぜい弱性を狙った脅威が現れ始めた（詳細は2章）。そのため、これまでより一歩進んだ、信頼できない計算環境でもソフトウェアを安全に正しく動作させる技術が必要となる。具体的な研究開発課題としては、安全性指向コンピューターアーキテクチャ技術、信頼できる隔離実行環境の構築技術およびエッジからクラウドまでの総合的なセキュリティーを実現するセキュアOS技術などが挙げられる。

ネットワークセキュリティーに関しては、ゼロトラストセキュリティーという考え方が主流になりつつある。これまで外部のネットワークは信用できないのでファイヤーウォールや侵入検知ソフトウェアなどで外部からの攻撃を防ごうという考え方であったものが、外部だけではなく内部も含めてすべてのネットワークは信用できないので、エンドツーエンドでセキュリティーを確保しようという考え方である。しかしながら、2018年に発見されたMELTDOWNやSPECTREというCPUのぜい弱性をついた攻撃が現実のものになることを考えると、アプリケーションが動くCPUやOSすら信頼できないと考えなければならないことになる（図3-2におけるゼロトラストコンピューティング）。

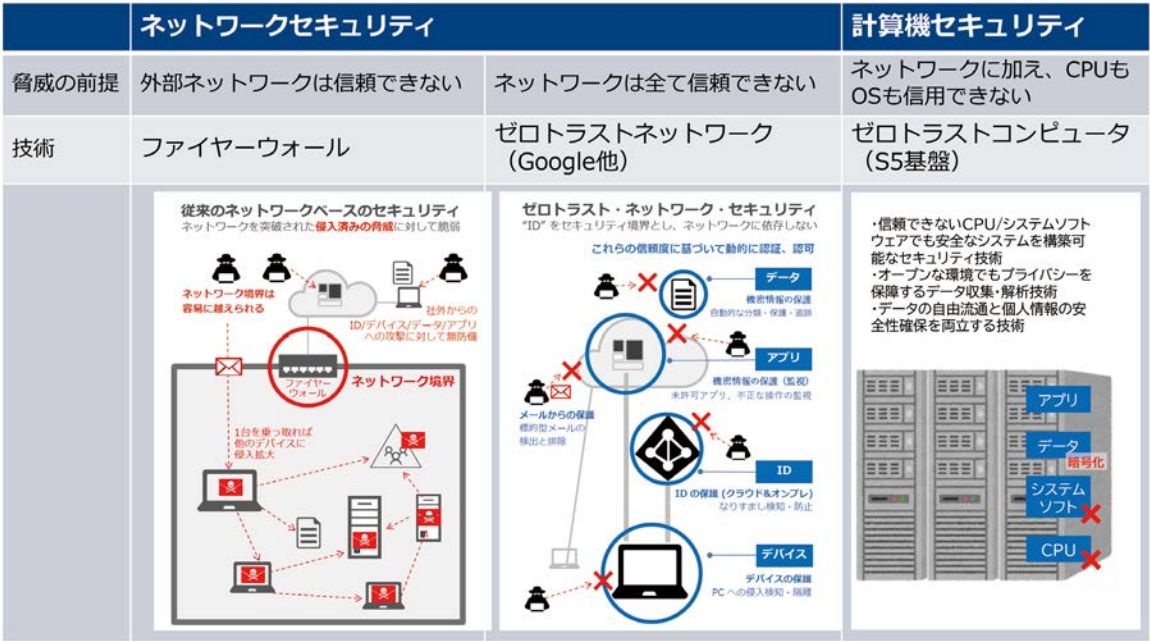


図 3-2 ゼロトラストコンピューティング

(1) OSの権限分散・階層化等による安全性指向コンピューターアーキテクチャー技術

「理論×システム基盤技術」による次世代セキュア・コンピューティング技術を確立する。現状では、システム階層ごとの研究開発が主流だが、一箇所でもセキュリティーホールがあれば攻撃可能となり、一番弱いところが狙われる。このため、システム階層横断（理論×システム基盤技術）による新しい分野融合研究が必要である。具体的には、「安心・安全・高信頼」の極めて低いオーバーヘッド(性能や消費電力)での実現、ハードウェアからソフトウェア、アルゴリズムまでのシステム階層横断型研究および理論的アプローチとエンジニアリング・アプローチの相乗効果によるさまざまな対策の探索などが考えられる。ワークショップ³⁹では表 3-1 に示す連携研究の例が議論された。

表 3-1 想定される連携研究例

連携研究名	研究内容	連携分野
高性能・低消費電力秘密計算基盤	秘密計算アクセラレーター	理論＋コンパイラー＋アーキテクチャー
Open-TEE	信頼できるプロセッサシステム	プログラミング＋OS＋コンパイラ＋アーキテクチャー
権限分割OSによる相互監視システム	権限定のためのアーキテクチャーサポート	OS＋アーキテクチャー
アーキテクチャを考慮した脆弱性検証	アーキテクチャーレベルでのセキュリティ検証技術	理論＋プログラミング＋アーキテクチャー
Dynamic Information Flow Tracking (DIFT)	アーキテクチャーサポート ヘテロな環境対応	理論＋プログラミング＋OS＋コンパイラー＋アーキテクチャー

39 科学技術未来戦略ワークショップ報告書「Society 5.0システムソフトウェア」総合討議より、CRDS-FY2020-WR-04

(2) 信頼できる隔離実行環境の構築技術

OSとは別に信頼できる隔離実行環境（TEE: Trusted Execution Environment）をハードウェアとソフトウェアを協調設計することでプログラムやデータ資産を守る。考え方自身はそれほど新しいものではなく、現在のCPUでも、IntelのSoftware Guard Extensions（SGX）やAMDのSecure Memory Encryption（SME）、ArmのTrustZoneなどで実装されている他、オープンアーキテクチャーであるRISC-VでもTEE開発が進められている。しかし、これらのTEEは、ハードウェア実装が非公開だったり、ベンダー固有の認証方式を採用していたりするため、ユーザーや第三者機関からの監査・検証ができない。また、クラウドとエッジの両側で信頼の基点のハードが壊れるとそれまでの隔離実行で守ってきた資産が無効になるなどの問題がある。そこで、本研究課題では、これらの課題を解決し、ソフトウェア・データの不正コピーがなく、ハードの故障からの重要ソフト・データ移動が容易で、第三者機関からのハードウェア・ソフトウェア安全性検証が可能な次世代のTEE技術を開発する必要がある。

(3) エッジからクラウドまでの総合的なセキュリティを実現するセキュアOS技術

Society 5.0向けに設計されたシステム全体で首尾一貫した統合セキュリティを実現するOS環境の研究開発である。現状は世界各国が独自にエッジやクラウド向け最先端OS環境の研究開発を積極的に行っており、システム全体として一貫性のあるセキュリティを担保することが困難になりつつある。具体的には、OSを含むシステムソフトウェアが巨大かつ複雑になり過ぎて、セキュリティ上の問題が発生しないようにすることが専門家でも困難になっていることや、エッジやクラウド等でつぎはぎ的にセキュリティ機能が拡張されており、システム全体を俯瞰した総合的なセキュリティ機能が実現されていないことや、システムソフトウェア技術をブラックボックス化して自前で持たないと安全保障上の障害になる可能性があることなどである。このため、Society 5.0システム向けに設計された、システム全体で首尾一貫した統合セキュリティを実現するOS周辺環境のセキュア技術の研究開発が必要である。

3.2 プライバシーに関する研究開発課題

オープンな環境でもプライバシーを確保するデータ収集・解析技術を創出するための研究開発課題である。データ駆動社会においてデータは重要な資産であり、個人情報や企業の機密情報、研究データなどは安全管理されつつ活用することが求められる。データの統合利活用を促す動きとして、ここ数年、わが国でも、改正個人情報保護法をはじめ法制度が着々と整ってきた（2章表2-2参照）。これらを支える安心・安全なデータ利活用のためのプライバシー技術がますます重要になっている。

しかし、現実には、システムのぜい弱性を悪用した漏えいや改ざんなどの事象にはとどまる兆しが見えない。プライバシー確保に関しても、これまでより一歩進んだ、オープンなネットワーク上のデータは見られるという前提のもとで、データの秘匿性を確保する技術が求められる。技術的には、秘密計算によるトラスト確保技術、相互に信頼できる範囲や開示レベルを動的に制御可能な分散認証技術、秘密計算に基づく分散データ収集・解析技術などの研究開発課題が考えられる。

また、プライバシーに関しては、日本人のパーソナルデータ提供に対する許容度は、諸外国と比較して平時

のみならず緊急時においても、低いという報告がある⁴⁰。COVID-19の接触追跡アプリ⁴¹においてもわが国の場合、個人を特定する情報はもとより接触日時、位置情報さえもサーバーには送られない。技術的な安全が人々に安心を与え信頼されるようになるためには何が必要か、人文・社会科学の知見を交えた検討や研究が必要となる。

(1) 準同型暗号やマルチパーティー計算等の秘密計算によるトラスト確保技術

データを秘匿（暗号化）したまま計算や解析する技術である。準同型暗号は、暗号化したまま加法や乗法といった演算が可能な暗号技術である（図3-3）。加法乗法どちらも可能な完全準同型暗号が2009年に

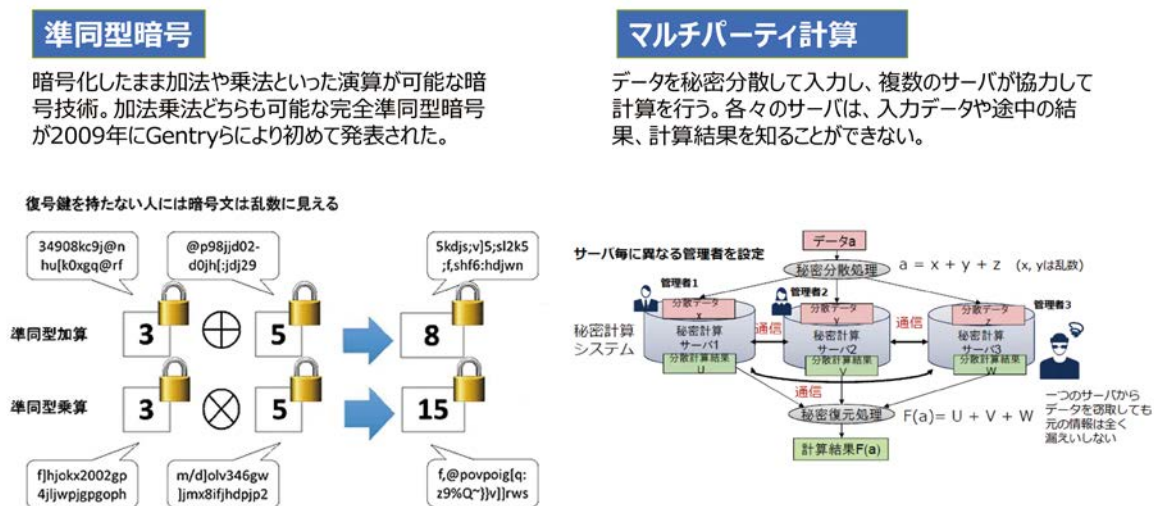


図 3-3 プライバシーを守る技術の例

Gentryらにより初めて発表された。また、マルチパーティー計算は、データを秘密分散して入力し、複数のサーバーが協力して計算を行う。各々のサーバーは、入力データや途中の結果、計算結果を知ることができないという利点がある。どちらの技術もこれまでに性能上の課題が指摘されてきた。Society 5.0社会においては、IoTで多くのモノと人や情報システムとがつながるためさらに大量なデータを処理する必要がある。特に、機械学習との組合せにおいては、使えそうな分野のユースケースを特定し、社会実装への足掛かりを見つけていくことが重要である。

(2) 差分プライバシーなどの秘密計算に基づく分散データ収集・解析技術

差分プライバシー（DP: Differential Privacy）とは、大量のデータがあったときに、統計解析の結果を一般に公開する際に用いるプライバシー基準であって、結果を乱数でランダム化をすることにより、データ解析者に個人のデータの推定できないようにすることでプライバシーを守ろうとする技術である。また、局所差分プライバシー（LDP: Local Differential Privacy）とは、データを収集する際のプライバシー基準であって、解析者だけでなく収集者にも個人データを推定できないようにする技術である。AppleがiOSデバイスのユー

40 野村総合研究所，個人情報保護法改正における論点およびニューノーマルにおけるパーソナルデータ活用のあり方，<https://www.nri.com/jp/knowledge/report/lst/2020/cc/mediaforum/forum290>

41 厚生労働省，接触確認アプリケーションプライバシーポリシー，https://www.mhlw.go.jp/stf/seisakunitsuite/japanese_pp_00027.html

ザー統計情報の収集解析でLDPを使用していると発表したことで有名になった。

局所差分プライバシー下での統計的推定は、どのようなタイプの統計的推定をやりたいのか、どのような対話モデルでユーザーとインタラクションしようとしているのかで、問題が定義される。統計的推定としては、最も単純なものではヒストグラムや平均値の推定に始まり、メジアンとか線形回帰のような統計もあり、最も複雑になると深層学習のようなものが含まれてくる。対話モデルとは、どのぐらいの複雑さをもってユーザーと対話をしていくのかのモデルであり、ユーザーが1回だけ情報提供をして終わりというモデルから、過去の処理に依存した複数回情報を提供する複雑なモデルもある。現状、非対話モデルにおける単純な統計的推定の理論はかなりできているが、より複雑な対話型モデルへの対応は課題である。IoTデバイスやSNSデータなどの大量のデータを取得し機械学習により解析し続けるような場合が今後増えてくると想定されるが、そのような場合にも対応可能なプライバシー技術の研究開発が必要である。本研究においても理論研究とシステム基盤の研究者の協調作業が求められる（図3-4⁴²）。

差分プライバシーとシステムソフトウェア

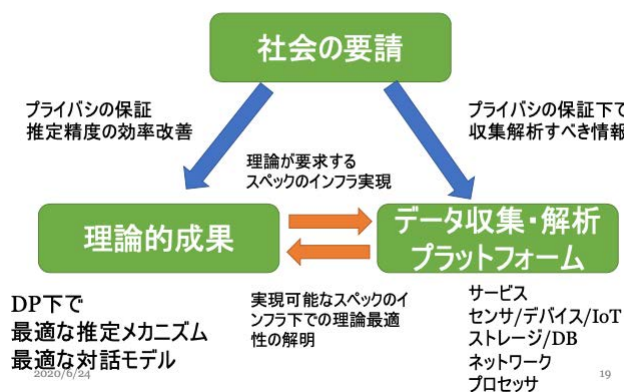


図 3-4 差分プライバシー

3.3 プラットフォームに関する研究開発課題

データの自由な流通と個人情報の安全性確保を両立するデータ駆動プラットフォーム研究に関する研究開発課題は以下の通り。

(1) セキュリティー・プライバシー処理の高性能実装技術

異分野連携によるセキュリティー検証技術

異分野の研究者の連携により、基盤ソフトウェアの脆弱性発見とセキュリティー検証のための技術を開発する。セキュリティーを厳密に検証するための技術としては、プログラミング言語分野で発展してきた形式検証技術があるが、Society 5.0アプリケーションでは、セキュリティーの問題がシステムの複数の階層や構成要素にまたがって生じ得るため、個々の階層や構成要素だけでなく、システム全体のセキュリティーを検証する技術へと範囲を拡大する必要がある。対象となる基盤ソフトウェアの例としては、センサーからのデータ収集、大

42 佐久間淳, プライバシー保護分野 Overview & 最先端研究, CRDS-FY2020-WR-04, p40

規模データの解析や管理、アクチュエータの制御、機器の間の通信などのソフトウェアが考えられる。具体的な研究内容の例としては、

- ・ ソフトウェアサイドチャネルに関するぜい弱性発見・検証技術
- ・ 複数の階層にまたがるセキュリティのモデル化・ぜい弱性発見・検証技術
- ・ システム実装のセキュリティの検証技術

などが考えられる。形式検証技術の研究者と、アーキテクチャーやOS、暗号理論などの多様な分野の研究者の密接な連携が必要である。

(2) データの真正性証明や来歴保証技術

権限や信頼の範囲が動的に変化する中でセキュリティー確保とプライバシー保護を行いながらデータを管理する技術には、現状さまざまな問題がある。組み込みデバイスなどを対象とした動的分散認証技術の開発は進められているが、それを前提としたデータ管理手法開発はまだ開発されていない。また、動的分散認証の下ではデータの来歴や操作履歴の管理を行う必要があるが、そのようなメタデータとデータの統一的な管理手法は確立していない。さらに、パーソナルデータの利活用については個人によりその選好が異なるにもかかわらず、それを考慮したプライバシー保護に基づく報酬配分法などが開発されていない。具体的な研究例としては、頑健で永続的なデータ来歴および操作履歴管理システム、履歴参照型プライバシー保護計算機構、問合せ系列に対するプライバシー漏洩増加の防止、参加者集合および各参加者のアクセス権が動的に変更される場合のプライバシー保護型連合学習、データ提供および効用に対する貢献に基づく報酬配分などが考えられる。

4 | 研究開発の推進方法および時間軸

Society 5.0時代のデジタル社会情報基盤は、多種多様なIoTセンサーデバイスや通信事業者、サービス事業者の提供するパブリッククラウド、政府・自治体・企業等が利活用するプライベートクラウド等の複合的なシステム形態に実装される。このように高度化・複雑化するICT環境を想定したセキュリティ・プライバシー研究は、基礎研究による理論的な考察・検証に加え、応用研究としてのプロトタイプソフトウェアの開発や実社会での利活用を想定した動作や効果の検証・評価が重要である。さらには、短期と中長期の研究開発施策を有機的に連携させ、基盤ソフトウェア領域のシームレスな研究開発投資戦略の実施が、来たるデジタル社会の安心・安全・信頼の実現に必須である。

4.1 研究開発推進の全体構想

(1) 研究開発は、基礎研究と応用研究を並行して進める

本提案における「理論とシステム基盤が高度に連携した研究開発の推進」の視点から、理論に基づく解決すべき課題の定式化、安全性の保証、計算複雑度の抑制、局所および全体的な最適化等の研究開発に加え、その成果を実社会での利活用が可能な規模・品質で実証実験や評価検証を行うことが重要である。

このように基礎研究と応用研究を並行して進めるにあたり、利活用可能なテストベッドシステムの候補を図4-1に示している。左図は、令和元年度より文部科学省にて研究開発を進めている「Society 5.0を実現するためのデータ活用による知識集約型社会の創成ーデータ活用社会創成プラットフォームの構築ー」である。さらに右図は令和4年度より運用開始計画である、学術におけるデータ駆動型研究を促進することを目的とする「次世代学術研究プラットフォーム」である。これらのプラットフォームをテストベッドとして活用することを検討するとともに、本動向で研究開発するシステムソフトウェアをこれらの上に構築することで、わが国の研究分野まで含めた広範な分野に利するものとなる。

事業の推進に当たっては、大学や国立研究所のテストベッド等の利活用を含む情報研究エコシステムを構築し、若手研究者や学生、民間企業等を巻き込んで先導的な取り組みに挑戦できる環境を整備し、社会実装を進めることも検討する。



図4-1 安心・安全・信頼を支える基盤ソフトウェアで利活用可能な国内テストベッドの候補

(2) 成果はモジュール化し、OSSとして世界に発信する

本提案で研究開発するSociety 5.0時代に必要なアプリケーションを支える基盤技術（セキュリティーやプライバシー保護の技術を含む）については、要素技術ごとに、又はパッケージ化して、例えばGitHub等でOSSとして公開し、利活用と社会実装を促進する。OSSの公開・利活用促進は、技術成果の国際展開・発信力向上のみならず、プログラムコード開発を通じた研究コミュニティの構築・拡充や、開発ソフトウェアの効率的な品質やユーザビリティの向上、他の機能コンポーネントとの連携・統合の促進等のソフトウェア開発の効率向上・コスト削減の視点からも重要な施策である。

(3) プロジェクトの遂行では、多彩な人材が集う研究体制を構築し人材育成の礎とする

基盤ソフトウェア領域の基礎研究は、設計段階からby-Designでセキュリティーやプライバシーを組み込むという観点から科学的にも挑戦的な課題であり、その要素技術であるセキュリティー・プライバシー・トラストは国際的にもデジタル社会における長期的な協調領域であることから、文部科学省主導のもと産官学が一体となり研究開発を行うことが適切である。

アカデミアの基礎研究者と産業界等の実用化研究者の総力を結集して、戦略目標達成型の研究開発を実施することで、幅広いシステム基盤技術を俯瞰しイノベーション創発を可能とする人材育成を進めつつ、革新技術創出と技術競争力強化が可能となる。

4.2 研究開発の戦略とロードマップ

(1) 短期と中長期の研究開発を有機的に統合・連携させる

情報通信インフラにおけるセキュリティー・プライバシー問題は、現状においても顕在化・深刻化しつつある課題である。図4-2は既に現状課題の短中期的な解決に向けた研究開発施策を直近の社会実装（2020～）と5～10年後の実用化を目指す応用研究に分けて示し、中長期の研究開発施策の1つとして今回提案の基礎研究（2030～実用化）の位置づけを明確にしている。

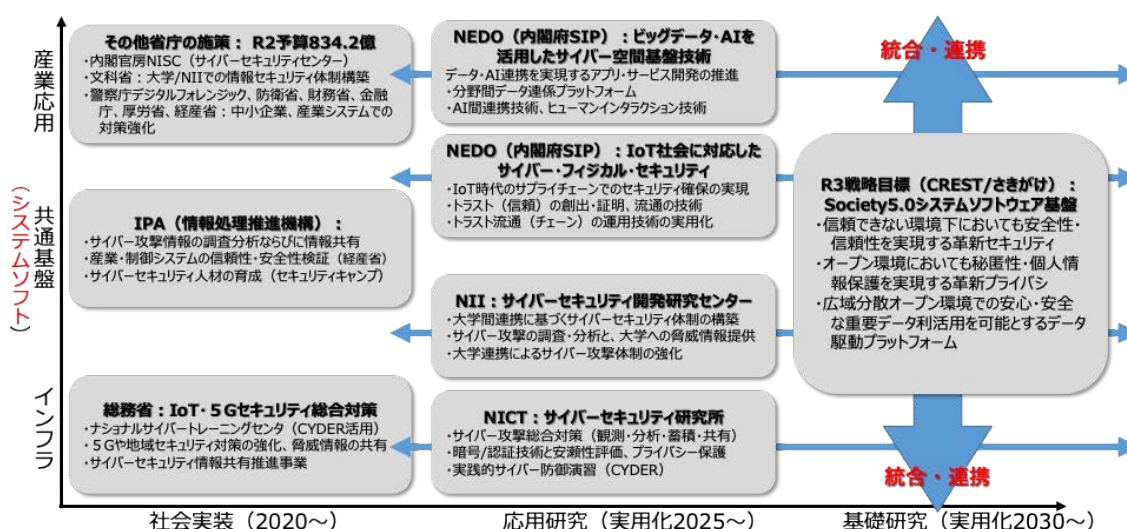


図4-2 国内におけるセキュリティー研究開発の全体像

今回提案の基盤ソフトウェア技術の研究開発においては、これまでの対症療法的な問題解決アプローチで

はなく、将来にわたる Society 5.0時代のデジタル社会におけるセキュリティ・プライバシー課題を予見し、本質的な課題解決を可能とする革新技術の創出に挑戦する。短中期の研究開発施策の成果および今後の研究開発施策の成果との連携・統合を視野におき、高度化・多様化するデータ駆動型社会システムのぜい弱性と脅威を根本から解決することを目指す。

また、研究の評価に関しては、第6期科学技術・イノベーション基本計画で検討されているように、従来の論文数や被引用度といったものに加えて、イノベーションの創出、新領域開拓、多様性への貢献等、新たな指標にしたがった評価を実施する。

(2) 段階的な成果発展に向けたプロジェクト運営を推進する

2030年以降、最終的にGAFAと国産の基盤技術が相互利用されたプラットフォームの実現を目指すことを目標とし、図4-3に示すとおり、段階的な成果発展を達成するプロジェクト運営を推進すべきである。第1段階では、本提案である「Society 5.0システムソフトウェア」の研究開発を遂行し、著名な学術論文誌や国際学会での発表やOSS公開等により、セキュリティ&プライバシー分野の国際的存在感を向上させるとともに、研究成果をOSS等の使える形での他事業への利活用展開を推進する。次に第2段階では、研究開発の対象分野を、データ活用基盤やネットワーク基盤を含むシステムソフトウェア全体に拡大した研究開発を推進し、システムソフトウェア全般にまたがる横断的な研究コミュニティの醸成を推進する。

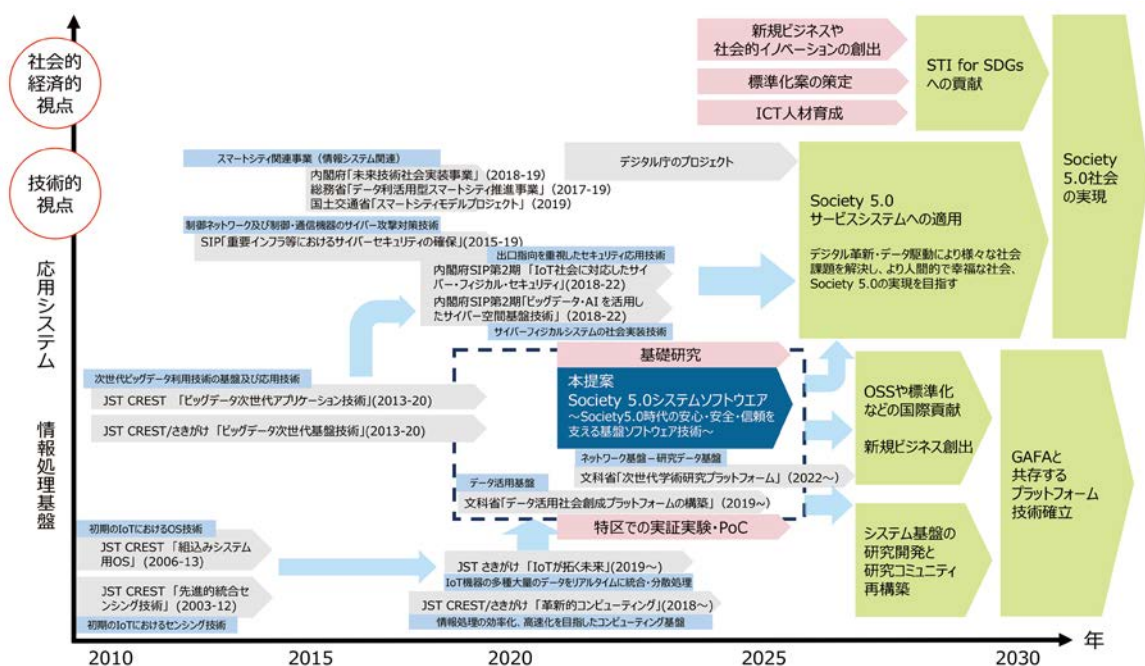


図4-3 安心・安全・信頼を支える基盤ソフトウェア技術の研究開発ロードマップ

科学技術振興機構、STI for SDGsの具現化に向けて - 国連決議から4年、新しいステージへ、2019、(https://www.jst.go.jp/sdgs/pdf/sti_for_sdgs_report_nov_2019.pdf) を参考にSDGsへの適用を明示した

本提案の成果となる基盤技術の企業への成果展開等により、国際社会のデジタルインフラを支えるプラットフォーム構築の実現が最終目標であるが、国内に向けては、デジタル革新・データ駆動によりさまざまな社会課題を解決し、より人間的で幸福な社会である Society 5.0の実現（Society 5.0サービスシステムの構築）に本提案成果を繋げていきたい。また、社会的・経済的視点からは、ICT技術領域における新規ビジネスや社会的イノベーションの創出、標準化案の策定、人材育成等を推進し、SDGs達成に向けた科学技術イノベーション推進に貢献する。

付録1 検討の経緯

(1) 情報学の次世代検討会（2019年度）

令和元年度に「情報学の次世代検討会（主催：国立情報学研究所および情報処理学会；共催：文部科学省）」にて、情報分野の今後の潮流について、情報処理学会の各研究会よりの講演と議論を実施し、情報学のビッグサイエンス化、OSやミドルウェアといった基盤ソフトウェアの重要性に関する議論を深めた¹。

付表 1-1 情報学の次世代検討会の開催概要

	情報学の次世代検討会Ⅰ	情報学の次世代検討会Ⅱ	情報学の次世代検討会Ⅲ
日時	令和元年8月13日（火） 13：00～18：00	令和元年8月20日（火） 13：00～18：00	令和元年9月6日（金） 13：00～18：00
場所	国立情報学研究所 12階会議室	国立情報学研究所 12階会議室	国立情報学研究所 19階会議室
参加者 （敬称略）	国立情報学研究所： 喜連川、河原林 情報処理学会： 江村、岡部、中川、倉本、西垣 講演者： 12名 文部科学省研究振興局： 橋爪、丸山、坂下、齊藤、加藤 科学技術振興機構： 青木、福島、高島、井上（CRDS） 山田（プログラム戦略推進部） 横井、岡山、尾崎（戦略研究推進部）	国立情報学研究所： 喜連川、河原林、中島、山岸 情報処理学会： 江村、岡部 講演者： 11名 文部科学省研究振興局： 村田、橋爪、坂下、出口、柴田、 福野、荒井、伊賀、三宅 科学技術振興機構： 青木、福島、井上（CRDS） 山田（プログラム戦略推進部） 横井、坂本、庄司、尾崎（戦略研究推進部）	国立情報学研究所： 喜連川、河原林、宇野、計 情報処理学会： 江村、岡部、木村、西垣 講演者： 12名 文部科学省研究振興局： 増子、橋爪、丸山、齊藤、伊賀 科学技術振興機構： 木村、青木、福島、井上（CRDS） 林部（プログラム戦略推進部） 宮田、庄司、尾崎（戦略研究推進部）

(2) 文部科学省情報委員会（2019年度）

情報委員会が令和元年11月にとりまとめた「今後の情報分野の研究の進め方について」²では以下の提言がなされた。

我が国が世界に先駆けて Society 5.0 が描く社会を実現していくためには、次世代の人工知能（AI）技術やさまざまな分野での革新的な情報化を支える基盤的分野（OS、プログラミング、セキュリティ、データベース、通信、高性能コンピューティング、分散コンピューティング、アーキテクチャ、ハードウェア等）の研究や人材育成を強化し、情報分野が先導する日本発のイノベーション創出を活性化させていくことが重要である。

このため、基盤的分野をベースとし、Society 5.0 が目指す知識を基盤とする人間中心の社会の構築に向けて、自然科学や工学だけでなく人文・社会科学や教育等も含む多様な研究分野との連携や産学官

1 文部科学省情報委員会（令和元年度第3回）配付資料，第6期の情報学を検討する IPSJ-NII-MEXT ラウンドテーブル，
https://www.mext.go.jp/content/20200116-mext_jyohoka01-000004146_3.pdf
2 文部科学省，科学技術・学術審議会情報委員会、今後の情報分野の研究の進め方について，
https://www.mext.go.jp/content/20200313-mxt_jyohoka01-100015685_2.pdf

での連携、あらゆる分野の知識・情報の共有が有機的に行われる「スマート研究プラットフォーム」の構築を進めることが重要である。その際、エネルギー効率とセキュリティを実現するデザイン等を重視すべきである。

(3) 科学技術未来戦略ワークショップ（2020年6月）³

令和2年度には「Society 5.0システムソフトウェアに関わるワークショップ（主催：JST/CRDS；共催：国立情報学研究所、情報処理学会、文部科学省）」にて、システムソフトウェアに関わる研究内容に関する議論と研究成果の応用に関する議論を2日間にわたり実施した（各回約60名参加）。本ワークショップは、上記（1）および（2）にて検討していたものを、関連分野の幅広い研究者層を交えて議論することで、新たな研究領域を作り出してゆく、いわゆるサミット形式のワークショップで開催された。その結果、「理論×システム基盤技術」で安心安全なSociety 5.0情報処理基盤を構築するという考え方が導出された。

ワークショップ（第1回）プログラム

【テーマ】研究内容に関する議論

【日 時】2020年6月24日（水）15:00～20:20（休憩1時間あり）

【場 所】ZOOM会議

【プログラム】（敬称略）

挨拶と趣旨説明	JST/CRDS 文部科学省研究振興局 NEC 国立情報学研究所 国立情報学研究所 京都大学	木村 康則 橋爪 淳 江村 克己 喜連川 優 河原林 健一 岡部 寿男
研究分野発表（1）	セキュリティ分野 OVERVIEW セキュリティ分野最先端研究	松浦 幹太 盛合 志帆
研究分野発表（2）	プログラム言語分野 OVERVIEW プログラム言語分野最先端研究	田浦 健次郎 小林 直樹
研究分野発表（3）	アーキテクチャ分野 OVERVIEW アーキテクチャー分野最先端研究	井上 弘士 佐々木 広
研究分野発表（4）	プライバシー分野 OVERVIEW&最先端研究	佐久間 淳
研究分野発表（5）	OS分野 OVERVIEW &最先端研究	河野 健二
パネルディスカッション ラップアップ		

ワークショップ（第2回）プログラム

【テーマ】研究成果の応用に関する議論

【日 時】2020年6月29日（月）13:00～17:40

【場 所】ZOOM会議+オンサイト（科学技術振興機構東京本部）

3 CRDS-FY2020-WR-04、科学技術未来戦略ワークショップ報告書「Society 5.0システムソフトウェア」、2020/6/24と2020/6/29に開催。

【プログラム】(敬称略)

挨拶と趣旨説明	主催者 (JST/CRDS)	木村 康則
研究成果の活用 (1)	三井住友フィナンシャルグループ	谷崎 勝教
研究成果の活用 (2)	NTT セキュアプラットフォーム研究所	高橋 克巳
研究成果の活用 (3)	NTT セキュアプラットフォーム研究所	千田 浩司
研究成果の活用 (4)	日本アイ・ビー・エム東京基礎研究所	福田 剛志
CRDSの取組み		CRDS
パネルディスカッション		
ラップアップ		文部科学省、CRDS

参加者一覧 (順不同敬称略)

【ステアリングメンバー】

喜連川 優	国立情報学研究所 所長
江村 克己	NEC フェロー
河原林 健一	国立情報学研究所 教授/副所長 (コーディネーター)
岡部 寿男	京都大学 教授/センター長 (コーディネーター)
橋爪 淳	文部科学省研究振興局 参事官 (情報担当)
木村 康則	科学技術振興機構 上席フェロー

【第1回ワークショップの発表者】

井上 弘士	九州大学 教授
佐々木 広	東京工業大学 准教授
河野 健二	慶應義塾大学 教授
松浦 幹太	東京大学 教授
盛合 志帆	情報通信研究機構 企画戦略室長 兼 上席研究員
佐久間 淳	筑波大学 教授
田浦 健次郎	東京大学 教授/センター長
小林 直樹	東京大学 教授

【第2回ワークショップの発表者】

谷崎 勝教	日本総合研究所 代表取締役社長/三井住友フィナンシャルグループ CDIO
高橋 克巳	NTT セキュアプラットフォーム研究所 主席研究員
千田 浩司	NTT セキュアプラットフォーム研究所 主幹研究員
福田 剛志	日本アイ・ビー・エム 東京基礎研究所 所長

【ディスカッサント (コメンテーター)】

吉川 正俊	京都大学 教授
小野 貴継	九州大学 准教授
塩谷 亮太	東京大学 准教授
品川 高廣	東京大学 准教授
光来 健一	九州工業大学 教授
須崎 有康	産業技術総合研究所 主任研究員
稲山 空道	東京大学 助教
花岡 悟一郎	産業技術総合研究所 研究チーム長
縫田 光司	東京大学 准教授
矢内 直人	大阪大学 助教

川本 裕輔	産業技術総合研究所 主任研究員
曹 洋	京都大学 特定助教
宮地 充子	大阪大学 教授
五十嵐 淳	京都大学 教授
住井 英二郎	東北大学 教授
姜 仁河	東京大学 助教
鈴木 豊太郎	IBM Thomas Jr. Watson Research Center Research Scientist
井上 拓	日本アイ・ビー・エム東京基礎研究所 博士

【文部科学省】

橋爪 淳	参事官（情報担当）
出口 夏子	参事官（情報担当）付 参事官補佐
齊藤 修啓	参事官（情報担当）付 情報科学技術推進官
犬塚 恵美	参事官（情報担当）付 情報処理推進係
福野 達也	計算科学技術推進室 企画推進係長
太田 洋一郎	計算科学技術推進室 専門職
宇賀神 昌利	計算科学技術推進室 調査員

【JST】

木村 康則	CRDSシステム情報ユニット 上席フェロー
茂木 強	CRDSシステム情報ユニット フェロー
若山 正人	CRDSシステム情報ユニット 上席フェロー
青木 孝	CRDSシステム情報ユニット フェロー
高島 洋典	CRDSシステム情報ユニット フェロー
辻 真博	CRDSライフユニット フェロー
松村 郷史	CRDS環エネユニットフェロー
村川 克二	CRDS政策ユニット フェロー
桐葉 佳明	戦略研究推進部 ICT グループ 主任調査員

ワークショップで問題意識と方向性を共有した参加者に提案を募ったところ10件の回答があった。発表内容と合わせて本提案の具体的な研究内容を検討する際の参考にした。

付表 1-2 提案書一覧

#	分野	タイトル	提案者（敬称略）
1	アーキテクチャー	全体像とコンピュータ・アーキテクチャ	井上 弘士（九州大学）、 佐々木 広（東京工業大学）、 入江 英嗣（東京大学）、 塩谷 亮太（東京大学）、 小野 貴継（九州大学）
2	OS	IoTからクラウドまで総合的なセキュリティを実現するモダンなセキュアOS	品川 高廣（東京大学）
3	OS	信頼できる隔離実行 ---TEEからCertifiedTEEへ---	須崎 有康（産業技術総合研究所）
4	OS	メモリ省電力化とセキュリティを両立する基盤技術の研究	穂山 空道（東京大学）
5	セキュリティ	システムソフトウェアレベルのトラスト基盤技術	松浦 幹太（東京大学）

6	セキュリティ	数理とソフトウェア科学を融合した機械学習のセキュリティ研究	矢内 直人（大阪大学）
7	プライバシー	データ管理に関するS5Kernel提案書	吉川 正俊（京都大学）
8	プライバシー	異分野連携によるSociety5.0セキュリティ検証技術の研究	川本 裕輔（産業技術総合研究所）
9	言語	広義の「プログラミング言語」にもとづくSociety5.0時代のシステム検証研究	住井 英二郎（東北大学）、 小林 直樹（東京大学）、 田浦 健次朗（東京大学）、 五十嵐 淳（京都大学）
10	セキュリティ	SECURITY PLATFORM FORWARD TO POSTQUANTUM CYPHER, TEE AND IOT	宮地 充子（大阪大学）

（4）有識者インタビュー

（3）のワークショップは、戦略プロポーザルの策定プロセスにおいては、有識者インタビューも兼ねて実施した。従って、招へいた研究者（延60名）は、本来ここにも記載すべきであるが重複を避けるため割愛する。以下では、ワークショップ以外で個別にインタビューを実施した有識者を挙げる。

No.	氏名（敬称略）	所属・タイトル
1	井上 弘士	九州大学 教授
2	江村 克己	NEC フェロー
3	岡部 寿男	京都大学 教授/センター長
4	河原林 健一	国立情報学研究所 教授/副所長
5	喜連川 優	国立情報学研究所 所長
6	河野 健二	慶應義塾大学 教授
7	後藤 厚宏	情報セキュリティ大学院大学 学長
8	佐古 和恵	早稲田大学 教授
9	須崎 有康	産業技術総合研究所 主任研究員
10	徳田 英幸	情報通信研究機構 理事長
11	松井 充	三菱電機株式会社 役員技監
12	松浦 幹太	東京大学 教授
13	盛合 志帆	情報通信研究機構 企画戦略室長 兼 上席研究員
14	森 達哉	早稲田大学 教授
15	安浦 寛人	九州大学 理事・副学長

（5）CRDSワークショップ（2021年1月）

以下の仮説を検証するためにワークショップを開催し、将来にわたる戦略的な取り組みについて議論した。

仮 説：長期視野に基づく、理論の構築およびシステム基盤との高度な連携により、基盤ソフトウェアと応用分野のIT研究者の総力を結集した研究開発戦略を実行する。これによりこの分野の研究力を強化し、わが国の科学技術・イノベーション力を向上させることは可能か。

日時：2021年1月12日（火）15:00～16:00（特任フェロー会議の中で実施）

参加者：システム情報科学技術ユニット特任フェロー

（合原一幸、喜連川優、國吉康夫、田中健一、徳田英幸、森川博之、山口高平）、
文科省参事官（情報担当）付（参事官 橋爪淳、他）、
戦略スコープ作成チーム

仮説を3つの論点で議論し目標を達成するために取り入れるべき助言を抽出した。

①文部科学省としての役割について

- ・文部科学省の意義はポストムーアのアーキテクチャーを学術的に研究することである
- ・ポストムーアは前提が変わる新しいパラダイム、半導体だけでなくハードウェアやクラウドもポストムーアに向かって動き出しているeg. Computational National Security
- ・現代数学、例えばトポロジー、が基盤に果たす役割は大きい

②分野の広がりおよび日本の勝ち筋について（情報分野全体の戦略と位置付けも含めて）

- ・コロナで分かったように、勝ち負けではなく国として持つべきものは持つ必要がある
- ・基盤は地味だが押さえるべき。日米の差は軍があるかどうかの差、それを考慮すること
- ・ニューロモーフィックなどAIでもデバイスの開発でセキュリティを考える必要がある
- ・全体アーキテクチャーを描ける人が必要、それに合わせた基盤をすることが必須である

③この分野の人材育成に向けた中長期的な戦略について

- ・基礎理論、学術的に活躍できる研究者の育成が必要である
- ・セキュリティの現場データを共有できる基盤をNIIに構築しているので活用してほしい

付録2 国内外の状況

(1) プラットフォームに関する国際動向

【日本】

わが国で使われているサービスプラットフォームは現状ほぼ米国に席卷されているが、研究用の計算環境（ビッグデータ処理基盤、スパコン）は着々と強化拡充されている。産業技術総合研究所はわが国における産学共同のAI研究開発を加速するプラットフォームであるAI橋渡しクラウド（AI Bridging Cloud Infrastructure, ABCI）を運用している。ABCIは世界トップレベルの計算処理能力とデータ処理能力を持ち、AIとビッグデータのアルゴリズム、ソフトウェア、応用開発に用いられている。2020年11月には理化学研究所の「富岳」とともに、大規模機械学習処理のベンチマークであるMLPerfHPCにおいて世界最高レベルの性能を達成した。また、光や5Gインフラに関しては強みがある。

「Society5.0を実現するためのデータ活用による知識集約型社会の創成ーデータ活用社会創成プラットフォームの構築ー」の研究開発を開始した。また、2022年度からは、現行のSINETを拡充して「次世代学術研究プラットフォーム」の運用を開始する。

戦略的イノベーション創造プログラム（SIP）第2期において、「ビッグデータ・AIを活用したサイバー空間基盤技術」では、ビッグデータ・AIを活用したサイバー・フィジカル・システムの社会実装を目指し、分野を越えたデータ共有と利活用のための分野間データ連携基盤技術とこれらデータをワンストップで供給する分散型分野間データ連携の促進に係る研究開発を実施している。

また、「IoT社会に対応したサイバー・フィジカル・セキュリティ」では、セキュアな Society 5.0 の実現に向けた社会全体の安全・安心の確立を目指し、IoT機器やサプライチェーンの各要素について、セキュリティ確保とその確認を繰り返し行い信頼のチェーンを構築することで、IoTシステム・サービス及びサプライチェーン全体のセキュリティを実現するための研究開発を実施している。

【米国】

米国においては、The National Strategic Computing Initiative (NSCI) が2015年の大統領令によって発足し、ハイ・パフォーマンス・コンピューティングでの米国のリーダーシップを実現しようとしている。NSCIは複数の省庁にまたがる統一的な戦略であり、産業、アカデミアの連携のもとに活動を進めている。National Science Foundation (NSF) においても、NSCI@NSFと題して、HPCの研究開発と配備に対してファンディングを行っている。Energy-Efficient Computing: from Devices to Architectures (E2CDA) というプログラムでは、材料からデバイス、コンピューティングアーキテクチャーなどの研究に対して、2016年から18年に合計で2千2百万ドル、Scalable Parallelism in the Extreme (SPX) においても2千万ドルの研究資金を提供している。また、Petascale Computing Resource Allocations (PRAC) においては、実際にスーパーコンピューティング環境を構築するために、2013年から2018年までに3億3千万ドルが投資されている。ほかにも、サイエンスのためのコンピューティング、教育、量子コンピューター、産学連携など多彩なプログラムが用意されている。

これまでコンピューティングの性能向上を支えてきたムーアの法則の終焉を迎え、コンピューティングを根底からすべて考え直そうという動きがIEEEのRebooting Computing Initiativeである。材料、デバイス、システム、アーキテクチャー、言語など多くの領域の専門家が集い、コンピューティングの将来を模索している。

GAFAM（Google、Amazon、Facebook、Apple、Microsoft）にみる競争力の源泉はビジネスモデルだけでなく情報科学技術の基盤である。Googleは、高速検索のアルゴリズムやビッグデータ処理基盤、Linuxベースのカスタムサーバー、カスタムOSによる最先端のデータセンターにてサービスのスケラビリティ

ティと可用性を強化している。また独自のセキュリティ対策により、外部の攻撃から転送中のデータを保護する。Amazonは、AWS（Amazon Web Service）上に、高度な仮想化基盤とインフラセキュリティを実現している。

【欧州】

欧州においてはHORIZON2020において、Advanced Computingというトピックを設定し、2014年から研究提案を募集し、現在30以上のプログラムが実行されている。低電力プロセッサ、フォグコンピューティング、ディープラーニングの学習アルゴリズムなど多岐にわたる研究が推進されている。2015年から2017年の間に開始されたプロジェクトへの投資金額は総額1億5千万ユーロに達する。2021年から開始されるHorizon Europeにおいても、Digital and Industryというクラスタの中にAdvanced Computing and Big Dataという領域を設け、ハイ・パフォーマンス・コンピューティング、ビッグデータおよびICTにおける低炭素化などに関する研究開発が予定されている。

欧州には米中のような巨大IT企業が不在のため、OSSによる標準化とGDPR（一般データ保護規則）等の国際ルールによりGAFA支配に対抗している。OSSとしてはFP7にてFIWAREを開発しているが、2019年にGAIA-X（A Federated Data Infrastructure for Europe）というクラウドプロジェクトを発表した。GAIA-Xは、セキュリティとデータ主権を守りつつデータの流通を支援する、ネットワーク相互接続、クラウドソリューション、ハイパフォーマンスコンピューティング等の機能を提供するフェデレーション型のプラットフォームを目指している。

【中国】

米国の技術導入と内製化の結果、BAT（Baidu、Alibaba、Tencent）に代表される中国IT企業のプラットフォーム技術は、そのユーザー数やトランザクション数で圧倒的な規模を処理してきた結果、米国を凌駕するレベルにまで成長しつつある。

HUAWAIを始めとする中国企業の5Gインフラ技術は脅威であり、米中の技術覇権争いの象徴となっている。

新型コロナウイルス対応では、感染者に関する個人情報をぎりぎりまで公開することで感染拡大を防いでいるが、日米欧とのプライバシーに関する考え方の違いが浮き彫りになった。

（2）研究動向

【コンピューターアーキテクチャー】

IEEEの国際学会MicroにおけるTop Pick（最重要トピック）では、Security、Safety、Privacyがここ数年毎年選ばれ、重要性が高まっている。また、マルチテナント、マルチクラウド環境では悪意のある特権ソフトウェアやハードウェアからアプリケーションを守る仕組みとして、アーキテクチャーレベルでTrusted Execution Environment（TEE）を実現する動きが出てきている。

【コンピューターセキュリティ】

情報処理学会コンピュータセキュリティ研究会では、プライバシー、ユーザブルセキュリティ（Security By Design）、オープンソースソフトウェアセキュリティ技術が近年のトレンドになっている。また、データを秘匿したまま解析を行うプライバシー保護データ解析（準同型暗号）や、複数の参加者がデータを隔離したまま計算することで秘匿性を担保するマルチパーティー計算の研究が盛んになっている。

【ネットワークセキュリティ】

従来は社内ネットワークと社外ネットワークとの間にファイヤーウォールと呼ばれる、ネットワークトラフィック監視機構を設けることで、社内のネットワークのセキュリティを担保するやり方が行われてきた。しかし、

“社内（ネットワーク内）は安全である”ということを前提に、境界を守るやり方では守れなくなってきた現状を踏まえ、「すべてのトラフィックを信頼しないことを前提とし、検査、ログ取得を行う」というアプローチである、ゼロトラストセキュリティの必要性が言われるようになってきている。Googleはゼロトラストセキュリティネットワーク（Beyond Corp Remote Access）でエンドポイントセキュリティを実装している。

以下に、セキュリティに関する研究レベルの国際比較を示す。

研究領域	日本				米国				欧州			
	基礎		応用		基礎		応用		基礎		応用	
データ・コンテンツセキュリティ	○	→	○	→	◎	↗	◎	↗	○	→	◎	↗
サイバーセキュリティ	○	↗	○	→	◎	→	◎	→	○	→	○	↗
IoT・制御セキュリティ	○	→	○	↗	◎	↗	◎	↗	○	↗	◎	↗

JST CRDS「研究開発の俯瞰報告書 システム・情報科学技術分野（2021）」より

（3）わが国の関連施策

【データプラットフォーム】

2019年度文部科学省予算にて、「Society5.0を実現するためのデータ活用による知識集約型社会の創成一データ活用社会創成プラットフォームの構築」の研究開発を行っている。また、2022年度より、学術におけるデータ駆動型研究を促進するために「次世代学術研究プラットフォーム」の運用が始まる計画である。本動向で研究開発するシステムソフトウェアは、これらのデータ活用基盤、ネットワーク基盤および研究データ基盤上に構築することで、わが国の研究からSociety 5.0のアプリケーションまで広範な分野に関わるすべての研究開発者に利するものである。

【文部科学省の戦略目標】

2018年の戦略目標「Society5.0を支える革新的コンピューティング技術の創出」に関連するCRESTおよびさがけにおいて、ハードウェア部分に関わる、情報処理を質的に大転換させる新たなコンピューティング技術の創出、半導体微細化に頼らない革新的コンピューティング技術の開拓等、次世代コンピューターシステムの研究が行われている。

また、2019年の戦略目標「次世代IoTの戦略的活用を支える基盤技術」に関連するさがけにおいて、エッジコンピューティング部分に関わる、IoT機器から得られる多種大量のデータをリアルタイムに統合・分散処理する技術等の研究が行われている。

【未来投資戦略】

2018年の『未来投資戦略』において、「サイバーセキュリティ対策に万全を期しながらそのデータ利活用基盤を世界に先駆けて整備」することが謳われている。

【統合イノベーション政策2020】（令和2年7月17日閣議決定）

第III部第1章（2）②目標達成に向けた施策・対応策＜信頼性のある自由なデータ流通の実現及びデータ駆動型社会の社会実装＞に以下の記載がある。

個人情報を含む取扱データの複雑化、高度なセキュリティ、信頼性、エネルギー効率向上等に対応可能な

基盤技術を構築するため、Society 5.0時代の大規模社会システムをターゲットとしたソフトウェアシステムの研究開発を進めるとともに、情報学分野と応用分野との密な連携の下、各種データを基盤とするイノベーション創出を加速する大規模研究プラットフォームの構築を進める。

【デジタル社会の実現に向けた基本方針】(令和2年12月25日閣議決定)

III. 3. (3) ⑤安心して参加できるデジタル社会の形成に以下の記載がある。

国民一人ひとりが安心して参加できるデジタル社会を形成するためには、デジタル技術の悪用への対応や、災害時も機能するネットワーク環境が重要である。

このため、サイバーセキュリティ、個人情報の保護、信頼性のある情報の自由かつ安全な流通の確保や、災害対策の促進を図る。

なお、プライバシーやセキュリティの確保を通じて、国民の重要な情報資産を保護し、人々や企業間の信頼を醸成することで、信頼性のある情報の自由かつ安全な流通を確保し、データの国際的な流通を促すことが期待される。

「第6期科学技術・イノベーション戦略 答申素案」(令和3年1月20日意見募集開始)

第2章1.(1)(b) あるべき姿とその実現に向けた方向性に以下の記載がある。

信頼性のあるデータ流通環境の整備、セキュリティやプライバシーの確保、公正なルール等の整備を図ることで、企業によるデータの相互提供・活用、様々な分野で開発・提供される国民の利便性と安全な暮らしを支える利便性の高いサービスを活性化するとともに、多様な人々の社会参画が促され、国内外の社会の発展が加速する。

付録3 専門用語説明

エッジ、エッジコンピューティング：ネットワークの末端にあるIoTデバイスやそれらを集約するコンピューターをエッジと呼ぶ。一般に、パソコンやスマートフォンなど人間が使うコンピューターは含まない。また、エッジコンピューティングは、エッジにおいて処理を行うコンピューティングのこと。大量に発生するデータの集約や個人情報などの匿名化などの処理を行う。

クラウド、クラウドコンピューティング：クラウドとはインターネット上の計算環境のことであり、クラウドコンピューティングはそれをサービスとして利用する処理形態である。GAFAなどのIT企業は、独自の事業を営む一方で、自社のもつ計算環境の一部をクラウドサービスとして提供するサービスプロバイダーでもある。

セキュリティとプライバシー：セキュリティとは情報セキュリティのことであり、情報システムに対するさまざまな脅威から情報を守ることである。一方、プライバシーとは人に知られたくないこと（個人情報）を適切に扱うことである。

ゼロトラストセキュリティ：利用者（ID、パスワード）、デバイス、ネットワーク、アプリケーションに至るまであらゆるものを信頼せず、攻撃されることを前提とするセキュリティアプローチ。従来、組織の内部と外部の境界をファイアウォールによって区切ることで不正侵入やデータ流出を防ぐのが一般的であったが、それでは対応できないセキュリティリスクが生じるため、別アプローチの重要性が増した。

バイデザイン（by-Design）：特にセキュリティやプライバシーに関して情報システムの企画・設計段階から、システムとして満たすべき要件を確保するための方策を考慮し、設計・構築・運用することをいう。事象発生後の後追い対応に比べ、迅速かつ低コストに対応できると言われる。

トラスト：情報システムや情報サービスにおける安心や信頼の概念の総称。情報セキュリティやディペンダビリティのみならず、心理学や社会学の概念を含む。

システムソフトウェア：アプリケーションを動作させるために必要となる共通的な機能をまとめたソフトウェアである。仮想化ソフトウェア、オペレーティングシステム（OS）およびミドルウェアから構成される。

DX（デジタルトランスフォーメーション）：エリック・ストルターマン（ウメオ大学）が提唱した2004年には「ITの浸透により人々の生活をあらゆる面で良い方向に変化させる」ことを意味していたが、現在ではビジネス用語として「企業・組織がITを利用して事業や業務プロセスを根本的に変化させる」というような意味で使われている。

ELSI（Ethical, Legal and Social Issues）：科学の進歩に伴って生じる倫理的、法的、社会的課題のこと。米国のヒトゲノム計画にて研究で必要性が表明されたが、近年は、情報科学を含む全ての研究者が当事者意識を持って取り組むことが求められている。

GAFA：米国のIT企業4社（Google、Amazon、Facebook、Apple）頭文字を並べた造語で世界のサイバービジネスを支配する。これにMicrosoftを加えてGAFAMと称することもある。

GDPR（一般データ保護規則）：欧州連合（EU）が規定した、個人情報の保護という基本的人権の確保を目的とした規則。2018年5月25日からEU域内のすべての国での適用が開始された。

IoT（Internet of Things）：パソコンや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、機械などさまざま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。ヒト、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。

OSS（オープンソースソフトウェア）：ソースコードが公開されているソフトウェアで、著作権者が利用者にソフトウェアの使用、研究、変更、配布の権利を許諾しているもの。

SDGs（Sustainable Development Goals）：2015年9月25日の「持続可能な開発サミット」で国連が採択した「持続可能な開発のための2030アジェンダ」に含まれる目標。貧困や飢餓を終わらせる、公平性を保ち不平等をなくす、環境への配慮など17の目標と、さらにそれらをブレイクダウンした169の達成基準からなる。開発途上国の目標だけでなく、先進国での取り組みにも触れている。解決策の提供、合理的な政策立案などに向けたエビデンスの提供など、科学技術の貢献が期待されている。

Society 5.0：2016年に閣議決定された第5期科学技術基本計画の中に盛り込まれた未来社会。狩猟社会（Society 1.0）、農耕社会（同2.0）、工業社会（同3.0）、情報社会（同4.0）に続く、新たな社会。サイバー空間（仮想空間）とフィジカル空間（現実空間）を高度に融合させたシステムにより、経済発展と社会的課題の解決を両立する、人間中心の社会と定義されている。現在検討中の第6期科学技術イノベーション基本計画に向けては、Society 5.0は、SDGsを目指すに当たり、デジタル化・データ連携・活用を核とし、日本の価値観（共益）を盛り込むことで実現される知識集約型社会としての戦略・方向性が示されている。

作成メンバー

総括責任者	木村 康則	上席フェロー	(システム・情報科学技術ユニット)
リーダー	茂木 強	フェロー	(システム・情報科学技術ユニット)
メンバー	若山 正人	上席フェロー	(システム・情報科学技術ユニット)
	青木 孝	フェロー	(システム・情報科学技術ユニット)
	高島 洋典	フェロー	(システム・情報科学技術ユニット)
	辻 真博	フェロー	(ライフサイエンス・臨床医学ユニット)
	松村 郷史	フェロー	(環境・エネルギーユニット)
	村川 克二	フェロー	(科学技術イノベーション政策ユニット)
	桐葉 佳明	主任調査員	(戦略研究推進部)
	吉田 健司	副調査役	(未来創造研究開発推進部部)

戦略プロポーザル

CRDS-FY2020-SP-06

Society 5.0時代の安心・安全・信頼を支える 基盤ソフトウェア技術

STRATEGIC PROPOSAL

System Software to Support Safety, Security, and Trust in the Era of Society 5.0

令和 3 年 3 月 March 2021

ISBN 978-4-88890-730-9

国立研究開発法人科学技術振興機構 研究開発戦略センター

Center for Research and Development Strategy, Japan Science and Technology Agency

〒102-0076 東京都千代田区五番町 7 K's 五番町

電話 03-5214-7481

E-mail crds@jst.go.jp

<https://www.jst.go.jp/crds/>

本書は著作権法等によって著作権が保護された著作物です。

著作権法で認められた場合を除き、本書の全部又は一部を許可無く複写・複製することを禁じます。

引用を行う際は、必ず出典を記述願います。

This publication is protected by copyright law and international treaties.

No part of this publication may be copied or reproduced in any form or by any means without permission of JST, except to the extent permitted by applicable law.

Any quotations must be appropriately acknowledged.

If you wish to copy, reproduce, display or otherwise use this publication, please contact crds@jst.go.jp.

FOR THE FUTURE OF
SCIENCE AND
SOCIETY



<https://www.jst.go.jp/crds/>