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

多様な情報システムや大量のデータを使いこなして、質の高い豊かで安心な生活を実現するSociety 5.0時代には、“データの漏えい・流出”や“なりすまし”、“プライバシーの侵害”等の多くの危険が存在

⇒ 情報基盤分野の研究者の力を結集し、日本発の基盤ソフトウェア技術で安心・安全・信頼を確保

なぜ、基盤ソフトウェア技術？

デジタル化への急速な流れ
- デジタル庁の創設
- コロナ新時代の新たなライフスタイルへの移行
- Society 5.0の早期実現

しかし、我が国は・・・

デジタル化のためのハードウェア、OS、クラウド等の大部分を海外に依存

→ リスク管理も海外依存となってしまってよいのか？？

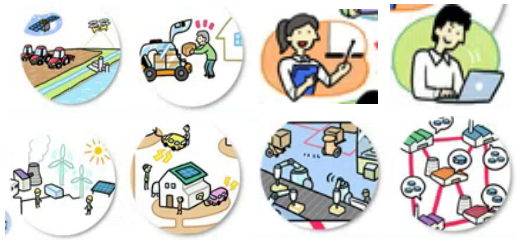
そこで、

情報基盤分野の研究力を再強化
- 研究コミュニティの再構築
- 理論とシステムの研究者の連携

＋

日本発の基盤ソフトウェア※で課題解決
- クラウド等の対策のみに頼らず、データや情報システムの安心・安全・信頼を確保

※基盤ソフトウェア＝アプリとクラウド等を繋ぐソフトウェア



Society 5.0

＝ **人々の多様な幸せの追求**

誰もが、安全・安心にデータを活用
多様な情報システムを信頼して利用

将来像

日本発次世代情報技術が世界で活用

次世代AI、高性能コンピューティング　等

データ

基盤ソフトウェア

安全	信頼できないハードウェアやOSを含む計算環境でも安全なシステムを構築できるセキュリティ技術
安心	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
信頼	データの自由な流通と個人情報の安全確保を両立するシステム実装技術

データ

基盤ソフトウェア技術の蓄積

情報基盤分野の研究者・研究力を結集
理論とシステムの融合

ハードウェア（センサ・デバイス等）・OS・クラウド等の対策のみでは、継続的な安全性・信頼性の確保は困難

令和３年度戦略目標

１．目標名

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

２．概要

我が国が提唱する Society 5.0 が目指す社会は、人とモノがつながり、様々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る。これを実現するため、我が国においては、デジタル庁設置に向けた基本的考え方等を示した「デジタル社会の実現に向けた改革の基本方針（令和２年 12 月 25 日閣議決定)」において、日本が抱えてきた多くの課題の解決と今後の経済成長のため、社会経済活動全般のデジタル化、言わば社会全体のデジタル・トランスフォーメーションを推進することが謳われている。

一方で、新型コロナウイルス感染症拡大を踏まえ、Society 5.0 の実現に向けては社会のデジタル化が一層飛躍的に進み、機密情報やプライバシーを侵害する可能性のある様々なデータがパブリッククラウド等の上に置かれることが想定される。そのため、きめ細かいセキュリティ要件とプライバシー保護を担保したデータの流通、情報処理が可能となる「Security-by-Design」かつ「Privacy-by-Design」な基盤ソフトウェアを、様々な実行環境からなるハイブリッドなハードウェアや OS 上で安心・安全にかつ信頼をもって動作させることができる環境を構築することが急務である。

また、近年報告されているハードウェアや OS の新たな脆弱性は、これを海外技術に依存している我が国においては深刻な課題になっている。計算環境は変化し続けているため、従来のような個別の対応では対処しきれない。システム全体を by-Design の観点で捉えた研究開発や安心・安全で信頼できる国産システムソフトウェアの整備が必須である。

そのため本戦略目標では、理論（数学や計算機科学の基礎）とシステム基盤技術（アルゴリズム・デバイス・アーキテクチャ・OS・ミドルウェア等）の研究者の連携により、科学技術・イノベーションの源泉である研究力を質・量ともに向上させ国際競争力を高める。さらに、これらを通して、by-Design に資する人材を育成する。

３．達成目標

本戦略目標では、基礎理論分野とシステム基盤技術分野を横断的に融合・統合する研究開発の推進により、Society 5.0 時代の安心・安全・信頼を支える革新的な基盤ソフトウェアの創出を目指す。具体的には、以下の３つの達成を目指す。

（１）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

（２）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

（３）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システム実装技術の確立

４．研究推進の際に見据えるべき将来の社会像

３.「達成目標」の実現を通じ、強靭かつ柔軟な基盤ソフトウェアによって持続的な社会・経済構造を支え、以下に挙げるような社会の実現に貢献する。

・データ駆動により様々な社会課題を解決し、より人間的で幸福な社会（Society 5.0）
・人々の行動が制限されても、国民の生活や経済活動に大きな影響なく、速やかに復旧できる社会
・プライバシーの侵害やセキュリティの不安なくデータの活用があらゆる場面で享受できる安心・安全で信頼できる社会

５．具体的な研究例

（１）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

・OS の権限分散・階層化等による安全性指向コンピュータ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（次世代 TEE 等）
・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
・安全な実行環境を実現するための形式検証技術

（２）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

・準同型暗号やマルチパーティ計算等の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
・差分プライバシーやローカル差分プライバシーを用いた分散データ収集・解析技術

（３）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システム実装技術の確立

・様々な実行環境（CPU、OS、仮想化）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
・ハードウェアの直接監視によるソフトウェア実行時の異常・攻撃検知

６．国内外の研究動向

（国内動向）

情報処理学会では、ユーザブルセキュリティ、オープンソースソフトウェアセキュリティ技術等が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計算の研究が盛んになっている。

戦略的イノベーション創造プログラム（SIP）第 2 期「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行っている。

また、同「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行っている。

（国外動向）

IEEE（米国電気電子学会） Micro Top Pick（毎年の最重要トピック）では、Security、Safety、Privacy に関する技術が近年毎年選ばれ、重要性が高まっている。また、複数企業で１つのクラウドを共有するマルチテナントや複数のクラウドを組み合わせて用いるマルチクラウド環境で悪意のある特権ソフトウェアやハードウェアへの攻撃からアプリケーションを守る仕組みとして、アーキテクチャレベルで信頼できる隔離実行環境を実現する動きが出てきた。

Google は、高速検索のアルゴリズムやビッグデータ処理基盤、カスタムサーバーやカスタム OS による最先端のデータセンターにてサービスのスケーラビリティと可用性を強化しているほか、独自のセキュリティ対策により外部からの攻撃や転送中のデータを保護している。Amazon は、自らが提供するウェブサービス上に、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。

欧州においては、令和２年、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す GAIA-X というクラウドプロジェクトを正式に発表した。

７．検討の経緯

「戦略目標の策定の指針」（令和元年７月科学技術・学術審議会基礎研究振興部会決定）に基づき、以下のとおり検討を行った。

（１）科学研究費助成事業データベース等を用いた国内の研究動向に関する分析及び研究論文データベースの分析資料を基に、科学技術・学術政策研究所科学技術予測センターの専門家ネットワークに参画している専門家や科学技術振興機構（JST）研究開発戦略センター（CRDS）の各分野ユニット、日本医療研究開発機構（AMED）のプログラムディレクター等を対象として、注目すべき研究動向に関するアンケートを実施した。

（２）上記アンケートの結果及び有識者ヒアリング並びに JST-CRDS で行われた「科学技術未来戦略ワークショップ『Society 5.0 システムソフトウェア』」等を参考にして分析を進めた結

果、Society 5.0 時代の人々の安心・安全・信頼のためにセキュリティとプライバシーの確保が重要であるとの認識を得て、注目すべき研究動向「Society 5.0 システムソフトウェア」を特定した。

（３）令和２年 12 月に、文部科学省と JST は共催で、当該研究動向に関係する産学官の有識者が一堂に会するワークショップを開催し、情報科学の基礎分野を振興することの重要性や産業界、他省庁との連携等について議論を行い、当該議論等を踏まえ、本戦略目標を作成した。

８．閣議決定文書等における関係記載

「統合イノベーション戦略 2020」（令和２年７月 17 日閣議決定）

第Ⅲ部第１章（２）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

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＞

〇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

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。

「科学技術・イノベーション基本計画について（答申素案）」（総合科学技術・イノベーション会議、令和３年１月 20 日）

第２章１．（１）（ｂ）あるべき姿とその実現に向けた方向性

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。

第２章１.（１）（Ｃ）⑥ デジタル社会の在り方に関する国際社会への貢献

データ流通に関するグローバルな枠組みを構築するため、データ品質、プライバシー、セキュリティ、インフラ等の相互信頼やルール、標準等、国際的なデータ流通を促進する上での課題について、2021 年度までに方向性を示し、解決に向けた方策を実行する。

第２章１.（５）（ａ）現状認識

スマートシティを支える都市データや都市 OS は、限られた者に独占されることなく、セキュリティの確保や個人情報の適切な扱いを前提とした上で、地域住民や新規ビジネス等に対して広く開かれることが必要である。

「サイバーセキュリティ研究・産学官連携戦略ワーキンググループ中間報告」（令和２年 11 月 25 日サイバーセキュリティ戦略本部研究開発戦略専門調査会研究・産学官連携戦略 WG）

第３章 3.2　重点的な研究領域

[安全・安心な社会基盤]

経済社会の安全・安心な社会基盤を支える研究領域

・デジタルインフラ（IoT、5G、クラウド、都市 OS 等）セキュリティに係る研究領域
・サプライチェーンセキュリティ研究領域
・データセキュリティ及びプライバシー保護研究領域
・実装セキュリティ（ハードウェアセキュリティ含む）研究領域

第３章 3.3　取り組むべき研究構想の具体例

（取り組むべき研究構想の具体例）

・信頼ある分散型データの活用を実現するセキュリティ基盤技術（DFFT 関連技術）
プライバシー等を保護しつつ分散型データを活用するためのセキュリティに関する基盤技術の確立を目指す研究構想

９．その他

令和２年度「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、アカデミアや産業界からの参加を得て、システムソフトウェアに関する議論と研究成果の応用に関する議論を実施し、「理論×システム基盤技術」で安心・安全な Society 5.0 情報基盤を構築するという考え方が導出された。

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組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。

本事業で構築した Society5.0 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、またはパッケージ化して、

例えばGitHub等でオープンソースとして公開・活用促進する社会実装も視野に入れる。

システムソフトウェア領域の基礎研究は、設計段階からバイデザインでセキュリティやプライバシーを組み込むという挑戦的な課題があり、その要素技術であるセキュリティ・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、他府省や民間独自ではなく文部科学省で行うことが適当である。アカデミックな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を創出しうる人材の育成を進めつつ、革新技術創出と技術競争力強化を目指す。