○戦略目標「次世代 IoT の戦略的活用を支える基盤技術」の下の研究領域

IoT が拓く未来

研究総括：徳田 英幸　（情報通信研究機構　理事長）

研究領域の概要

Society5.0 が実現された超スマート社会においては、IoT(Internet of Things)でつながった人や機器から生み出される大量かつ多様なデータを、サイバーフィジカルシステム(CPS)において、AI やビッグデータ処理などの情報科学技術により分析・活用し、インテリジェントな機器等をニーズに合わせて制御することで、機器単体では決して得られない新しい価値やサービスを創発することが期待されています。一方、IoT 機器に潜む脆弱性をつく外部からの攻撃等も危ぶまれ、高度な攻撃にも耐える IoT セキュリティやプライバシーに配慮した高度なデータ収集・流通・蓄積・解析基盤等の開発も急務です。

この超スマート社会の CPS を支えるには、カーボンニュートラルなシステム、セキュリティやプライバシー保護をデザイン時点から組み込んだデータエコシステムの実現などが重要です。特に、日本が世界をリードするためには、この急速に進展する IoT 環境の戦略的活用を支援する基盤技術の研究開発を加速することが必須です。

本研究領域は、超スマート社会の実現を見据え、従来技術の単純な延長では得られない、質的にも量的にも進化した次世代 IoT 技術の基盤構築を目指します。例えば、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、IoT 環境における機能・性能・実装の課題を飛躍的に解決する要素技術、IoT 機器の脆弱性、データ保全性等の課題を根本的に解決するセキュリティ技術やプライバシー強化技術等を対象として、大胆な発想に基づいた挑戦的な研究を推進します。

なお、本研究領域は文部科学省の人工知能／ビッグデータ／IoT／サイバーセキュリティ統合プロジェクト（AIP プロジェクト）の一環として運営します。

募集・選考・領域運営にあたっての研究総括の方針

１．背景

将来の超スマート社会では、膨大な数のセンサーがフィジカル空間の情報をリアルタイムに知的センシングし、自動的により広範囲、多頻度にサイバー空間へデータを吸い上げ、フィジカル空間の人間、機械等に様々な形で最適な動作・行動を起こさせるための情報をフィードバックすることを可能にします。また、生成された高付加価値のデータを蓄積し、匿

名化や暗号化等のプライバシー保護を施したうえでセキュアに社会へ提供することが可能となります。これら新しい社会システムを支えるシステムは、無数のハード／ソフトセンサー群、エッジデバイス群、巨大なクラウド群、そしてこれらをつなぐ多種多様なネットワークによって構成されます。これらの中で、世界をリードしていく上では、革新的なデータ収集、流通、蓄積、解析、制御を支える基盤技術が重要です。特に、センサーやアクチュエータをリアルタイムに制御し、多様で大量なデータから新たな価値を見出す次世代 IoT に必要とされる技術は、全く新しい原理に基づくスマートセンサー、デバイス、アクチュエータ、ソフトウェアなどのスマートイネーブラーによって創出される可能性があり、システム全体性能の飛躍的向上、時空間的制約やエネルギー的制約の克服などが期待できます。

２．提案募集する研究について

このような背景のもと、本研究領域では、IoT 機器から得られる大量のデータの連携・統合を高精度高性能に実現する技術や IoT 機器に対するサイバー攻撃やその防御に関する技術等、以下のような次世代 IoT に関わる広範囲な情報科学技術を主な対象とします。ただし、必ずしもこれに限定するものではありません。

- リアルタイムデータ統合技術(Real-Time Data Integration)
- リアルタイムセンサー統合技術(Real-Time Sensor Fusion)
- リアルタイム認識技術(Real-Time Cognition)
- エネルギーハーベスティング(Energy Harvesting)
- 知的ハード／ソフト／バーチャルセンサー
  (Intelligent Hard/Soft/Virtual Sensor)
- 高度なデータ収集・流通・蓄積・解析基盤プラットフォーム
- IoT を活用し新しいコネクテッド・サービスを導出する実現化技術　等
- IoT 認証技術(IoT Authentication)
- IoT セキュア通信プロトコルおよびその検証技術
  (IoT Secure Communication Protocol and its verification)
- データの保証性技術(Data Provenance)
- データの信頼性技術(Digital Forensic)
- プライバシー強化技術 (Privacy Enhancing)
- サイバー攻撃検知・防御技術(Cyber Attack Detection and Protection)
- 動的なセキュリティ制御(Dynamic Security Control)　等

提案にあたり、さきがけを通じて日本の存在感を示し、積極的に世界と協働する若手研究者の参画を強く期待します。次世代 IoT 技術は多くの省庁や企業等で様々な開発がしのぎを削って行われていますが、本研究領域ではさらなる先を目指した基礎研究を大胆な発想

をもって取り組むことを期待しています。

昨年度の選考では、本領域の戦略目標を着実に達成するために、特に、新しい原理に基づく革新的 IoT 技術の創出、IoT システム全体性能の飛躍的向上やセキュリティの強化、あるいは時空間的制約やエネルギー制約といった根本課題の克服等に対する研究提案における充足度を重視して評価を行いました。今年度も同様に、科学技術イノベーションの源泉となる先駆的な成果が期待できる提案を重視したいと思います。次世代 IoT に関わる広範囲な情報科学技術を主な対象とし、数多くの革新的、挑戦的な提案が応募されることを期待します。未来に対するビジョンを持ち、世界にインパクトを与え、科学技術イノベーションや未来社会の実現につながる研究に熱意をもって取り組む研究者を支援します。このさきがけで是非挑戦してください。

３．研究期間と研究費

研究期間は、2021 年 10 月から 2025 年 3 月までの約 3 年半以内(第 4 年次の年度末まで実施可能)です。１課題あたり予算規模は、原則として 3～4 千万円(通期；研究期間 3 年半以内)です。

４．さきがけ研究の進め方について

本研究領域では、要素技術の高度化だけでなく、次世代 IoT 技術をどのように社会に役立て利用するのか、社会にどのように受容されるか等を考慮し研究を進める姿勢を求めます。そのため、研究の進行においては、人文社会科学、システム工学、デザイン工学等の学問分野や、企業等の多様なステークホルダーとの連携を推奨します。

後者の企業等との連携においては、さきがけプロジェクトにおいて、JST の「さきがけコンバージェンスキャンプ」等の活動もあり、領域として活動することも推進して行きます。最後に、研究進行においては、研究成果の検証等に利用するデータの収集や利用基盤等に役立てられるように、以下のような機関との提携を推奨します。

・情報通信研究機構(NICT)における総合テストベッド(https://testbed.nict.go.jp/)
・国立情報学研究所(NII)における IoT 向けデータ収集基盤 SINET5
(https://www.sinet.ad.jp/)

なお、本研究領域は文部科学省の人工知能/ビッグデータ/IoT/サイバーセキュリティ統合プロジェクト（AIP プロジェクト）を構成する「AIP ネットワークラボ」の一研究領域として、理化学研究所革新知能統合研究センターをはじめとした関係研究機関等と連携しつつ研究課題に取り組むなど、AIP プロジェクトの一体的な運営にも貢献していきます。