〇戦略目標「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」の下の研究領域

基礎理論とシステム基盤技術の融合による Society 5.0 のための基盤ソフトウェアの創出

研究総括：岡部 寿男　（京都大学 学術情報メディアセンター　教授）

研究領域の概要

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す。新型コロナウイルス感染症の拡大を契機として、社会のデジタル化、さらには社会全体のデジタル・トランスフォーメションが一層進展すると考えられます。その結果、機密情報やプライバシーの侵害につながる可能性のある様々なデータがパブリッククラウドに置かれインターネットを介してやり取りされるようになることで、セキュリティリスクやプライバシーリスクの増大が懸念されています。

安心・安全で信頼できるデータ駆動型社会の実現には、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必要になります。しかも、高度化・複雑化する社会システムの構築においては、「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 上で動作させることが求められています。とりわけ、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、これらを海外技術に依存している我が国において深刻な課題であり、従来のような個別の対応では根本的な課題解決が困難となっています。社会システム全体を by-Design の観点で捉え、分散協調並列処理や AI 等の理論との融合も視野においた革新的な技術の研究開発と、原理的に安心・安全で信頼できる、ブラックボックスを排除し他国に依存しないオープンな基盤ソフトウェアの創出が必須です。

本研究領域では、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します。具体的には、以下の３つの達成目標に取り組みます。

(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

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

Society 5.0 時代の社会では、道路交通、エネルギー、ものづくり等、社会の様々なシステムから得られる多種多様なデータが互いに連携し、社会に新たな価値を創出していくことが期待されます。加えて、新型コロナウイルスの感染拡大を機に、社会のデジタル化やポストコロナを見据えた社会変革の必要性が意識されています。しかし、そのような社会を実現するためには、セキュリティとプライバシーを守るプラットフォームにおいて想定される様々な課題に対処しなければなりません。ハードウェアや OS など計算環境のコアに関わるぜい弱性を狙った脅威への対処、個人情報や企業の機密情報・研究データを安全に管理しつつ活用する方法、システム全体を by-Design で捉えたデータ流通と情報処理の実現など、様々な研究の推進が求められます。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、アーキテクチャから OS、ソフトウェア、データベース、セキュリティ、プライバシーの研究者が協力し、基礎研究（理論）と応用研究（システム基盤）を進めることで、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を実現することが期待されています。

２．達成目標に沿った研究課題の例

上記の背景を踏まえ、本研究領域では、基礎理論分野とシステム基盤技術分野を横断的に融合・統合する研究開発を推進し、社会インフラ全体を俯瞰した上でセキュリティ・プライバシーの課題を根本的に解決することを目指します。具体的には以下のような研究に取組みますが、必ずしもこれらに限定するものではなく、より自由で挑戦的な提案を期待します。

（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

・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

－ トラスト空間を跨った分散協調アーキテクチャ技術

－ アーキテクチャレベルでのセキュリティ検証等

・信頼できる隔離実行環境構築技術

－ ゼロトラストアーキテクチャに基づくセキュリティポリシーの AI 自動化

－ 現在の課題を解決する次世代 TEE（Trusted Execution Environment)の創出

－ ソフトウェア由来の形式検証や安全な実行環境を保証するデータの真正性確認等

・ヘテロ環境での脅威検出・データ保護を可能とする次世代データ流通基盤技術

－ 脆弱性自動評価技術、脅威検出技術

－ ヘテロ環境でのデータ保護、動的情報フロー追跡技術（DIFT）

－ 次世代高機能暗号やブロックチェーン等を用いた次世代認証･認可基盤(次世代 PKI

技術、分散型アイデンディティ、分散/統合アクセス制御等）

（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

・高機能暗号を用いたプライバシー保護技術

－ 完全/準同型暗号等によるプライバシー保護データマイニングの高速化技術

・国際的な個人情報保護法に対応可能なプライバシーポリシー管理技術

・プライバシー保護の安全性を網羅的に定義するための評価指標技術

（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

・上記（１）と（２）を融合した基盤技術

・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

・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

３．想定する研究の進め方

本研究領域では、将来を見据えた要素技術の高度化だけでなく、実社会を意識し、理論研究をどのように社会実装できるかを具体的に想定する姿勢や、セキュリティ・プライバシーに関わる真の課題を解決する技術を確立する姿勢を求めます。基礎理論のみあるいはシステム基盤技術のみの提案に留まらず、システム全体としてセキュリティ・プライバシーの要件を満たしていることが理論によって保証できるような融合・統合型の提案を期待します。

また、研究成果のユースケースの想定や国際的な競合技術とのベンチマークを自己評価することにより国際競争力の向上を図ります。中間報告時点でのステアリング（予算の見直し、研究テーマの軌道修正等）を強化します。研究成果物は、OSS（オープンソースソフトウェア）化や、オープンな API の提供等により、多種多様な環境に成果が広く普及するよう取り組んで頂きます。本研究領域の他のチームや同じ戦略目標下で設定されたさきがけ「ICT 基盤強化」の研究者との連携・協調、研究成果物の相互利用も期待しています。

研究開発においては、高性能仮想化環境として 2023 年度より正式運用が開始されるデータ活用社会創成プラットフォーム mdx の利用も積極的に検討下さい。

４．研究期間と研究費

研究期間は 5.5 年間（2023 年 10 月から 2029 年 3 月末まで)、予算規模は、総額 1.5 億円～3.5 億円（間接経費を除く）の範囲とします。基礎理論分野とシステム基盤技術分野を横断的に融合・統合する研究開発を推進しますので 1 件当たりの予算規模の大型化を図ります。また、必要に応じた研究加速等の支援や、複数のチームがそれぞれの成果を相互に利用する形での連携を推進するための予算措置も考えています。

５．応募にあたっての留意点

本研究領域では、チーム型研究の「CREST」として運営します。要素技術に留まらない、

基礎理論分野とシステム基盤技術分野を横断的に融合・統合を図った研究開発提案を評価します。融合・統合の結果として体制人数や予算規模が大型化しても構いません。セキュリティやプライバシーに関わる研究者だけでなく、システム・コンピュータアーキテクチャや基盤ソフトウェアの開発者、社会科学の専門家などを体制に取り込むことも必要に応じて検討してください。本領域の研究課題を２．で例示しましたが、研究代表者は、１つの達成目標に対してのチーム構成でも良く、複数の達成目標に跨がる目標を立てたチーム構成でも構いません。また、本領域では、人材育成の観点も重要と考えています。そのため、チーム内での若手研究者の育成はもちろんのこと、若手研究者からのチャレンジングな研究提案も期待します。

また、本研究領域の応募にあたっては5.5年間でのゴールの成果イメージ、および、3年後のマイルストーンについてできるだけ具体的に記載してください。特に、研究成果を実社会にどのように適用していくつもりかがわかるユースケースを必ず記載してください。大型化を希望している提案につきましては、研究成果の実社会での適用を想定した技術検証（Proof of Concept）の実施を研究計画に含めてください。

今年度は本領域の募集最終年度となります。

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）を構成する「AIP ネットワークラボ」の 1 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。