CREST

「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」研究総括説明

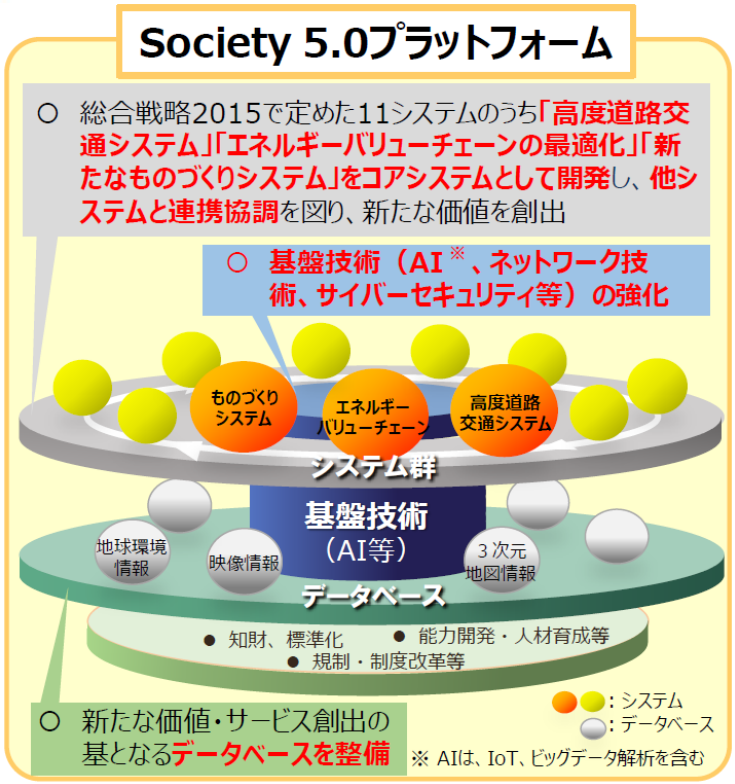
2023年4月

研究総括　岡部　寿男

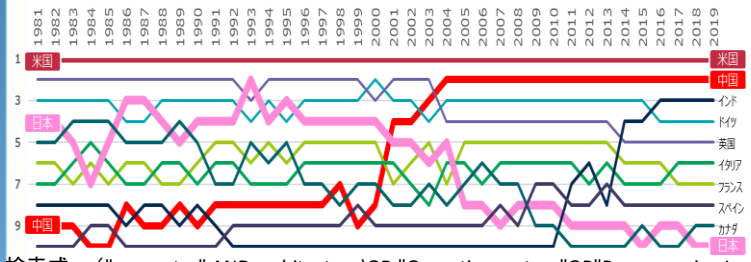
（京都大学 学術情報メディアセンター・センター長／教授）

科学技術振興機構

現状認識：Society 5.0の実現に向けて



（内閣府公開資料より抜粋）



検索式：（"computer" AND architecture)OR "Operating system"OR"Programming Language"

- **Society 5.0 コンセプトはいいが・・・**

  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。Wishに加えて、WhatとHowが必要

- **ハードウェアやOSを海外に依存する日本**

  巨大IT企業に対抗することは困難だが、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

- **情報分野は研究開発でも米国に席巻されている**

  わが国は、情報システムのオープン化、コモディティ化により、基盤構築に関わる研究開発をする機会を喪失し、こ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

- **GAFAの競争力の源泉は情報科学技術の基盤**

  わが国がIoTやロボット活用で強みを伸ばしてゆくためには、そのための情報技術基盤が重要である

現状認識：顕在化する脅威

- **プラットフォーマーは信頼できない**

  Google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にスキャンさせつづけている。Facebookはユーザの情報をCambridge Analytica社が利用するのを黙認していた

- **システムも信頼できない**

  2019年の1年間で公開サーバが攻撃を受けた被害の公表事例が 86件のうち約52% が公開サーバにおけるシステムの脆弱性を悪用されており、AWS上で公開されるミドルウェアやOSの脆弱性が深刻である

- **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、欧州や米国でのHuawei製品導入を控える（締め出し）社会問題になっている。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

- **ハードウエアすら信頼できない**

  2018年にマイクロプロセッサ（CPU）の脆弱性問題としてメルトダウンとスペクターが発表された。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せてしまう脆弱性で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

現状認識：デジタル化の推進

- **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［平成31年1月のダボス会議］

- **デジタル革新（DX）、デジタル庁の創設に向けた緊急提言**

  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、産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［経団連の提言］

- **Trusted Web推進協議会、ブロックチェーン官民推進協議会**

  デジタル市場競争に係る中期展望レポート」（令和2年6月16日デジタル市場競争会議）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する［内閣官房］

文部科学省R3年度戦略目標（概要）

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

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？？

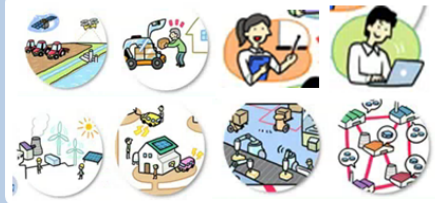
そこで、

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

CREST【S5基盤ソフト】研究領域（概要）

領域名：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（略称：S5基盤ソフト）

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。

CREST【S5基盤ソフト】の達成目標

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

安全

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

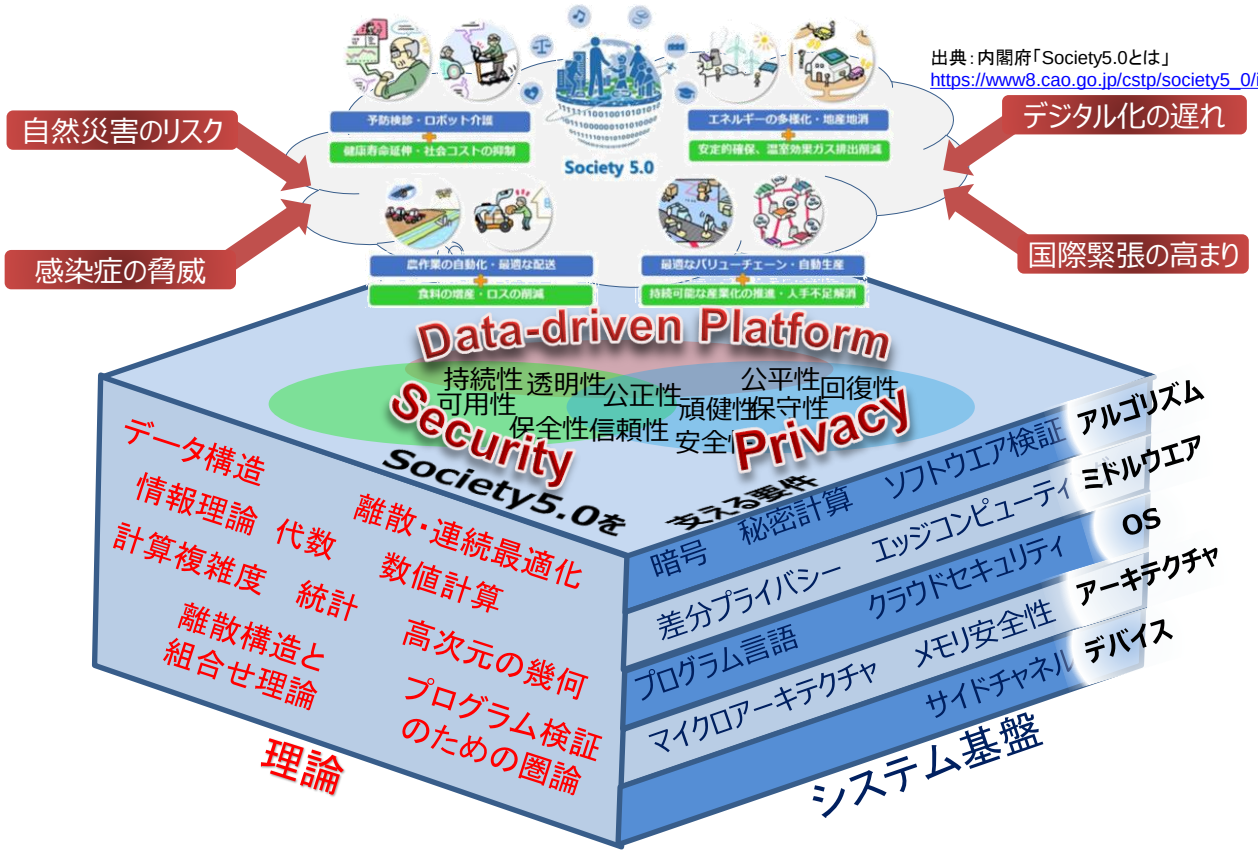
安心

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性確保を両立するシステム実装技術

直面する難局への対応と持続的かつ強靭な社会・経済構造の構築



出典：内閣府「Society5.0とは」
https://www8.cao.go.jp/cstp/society5_0/index.html

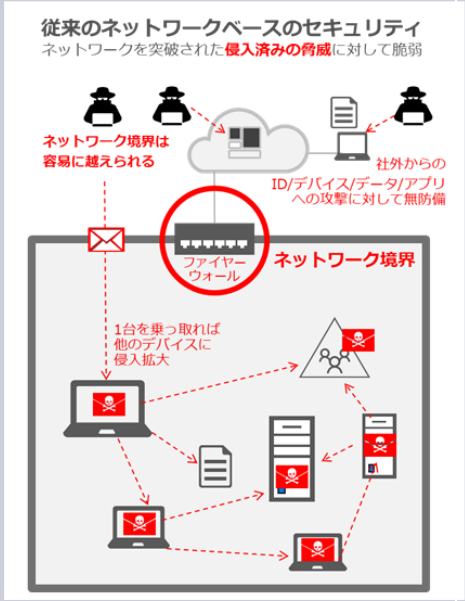
「理論×システム基盤」で安全安心なシステムソフトウエアの実現

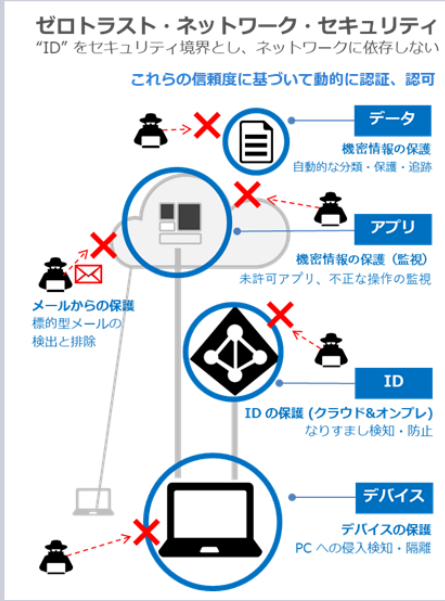
（戦略プロポーザル「Society 5.0時代の安心・安全・信頼を支える基盤ソフトウエア技術」CRDS-FY2020-SP-06より抜粋・一部修正）

CREST【S5基盤ソフト】研究領域の全体像

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

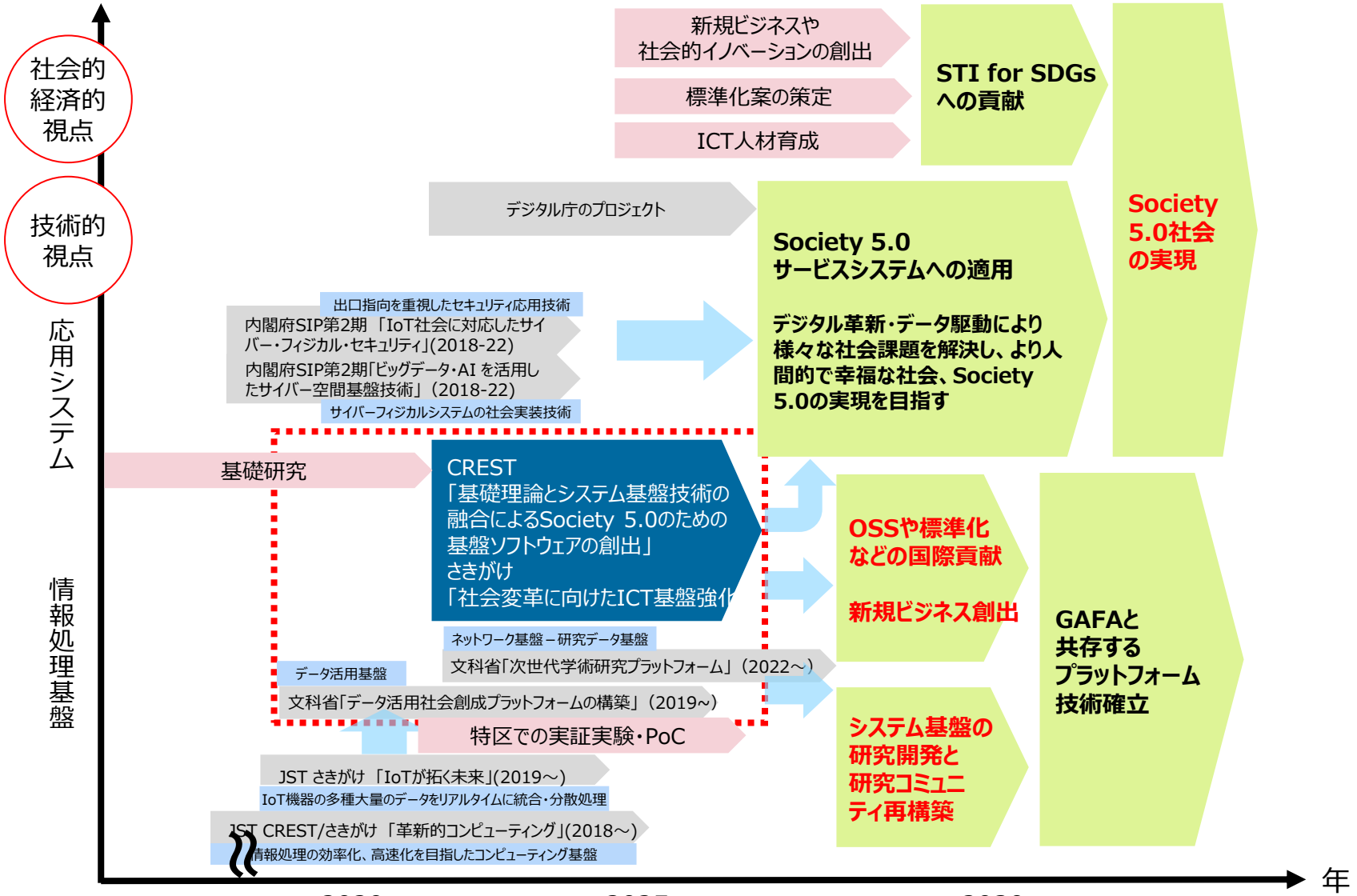
	既存システム・ネットワークセキュリティ		次世代セキュリティ
脅威の前提	外部ネットワークは信頼できない	ネットワークは全て信頼できない	ネットワークに加え、CPUもOSも信用できない
技術	ファイヤーウォール	ゼロトラストネットワーク（Google他）	ゼロトラストコンピューティング（S5基盤ソフト）





（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エア技術」CRDS-FY2020-SP-06より抜粋・一部修正）

CREST【S5基盤ソフト】の想定ロードマップ



（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エア技術」CRDS-FY2020-SP-06より抜粋・一部修正）

募集する技術領域詳細(1/2)

(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
  - ✓ 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、分散型アイデンティティ、分散/統合アクセス制御等)

募集する技術領域詳細(2/2)

(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

CREST【S5基盤ソフト】領域アドバイザー

【アドバイザー一覧（青：企業関係者； 赤：女性研究者）】

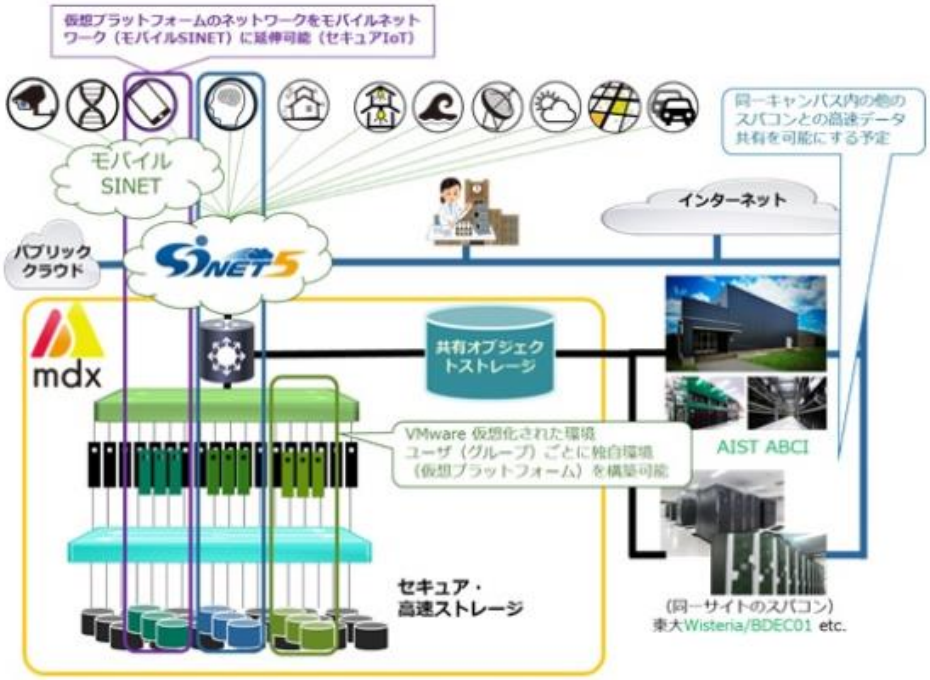
氏　名	所　属	役　職
河野　健二	慶應義塾大学　理工学部	教授
五島　正裕	国立情報学研究所　アーキテクチャ科学研究系	教授
高橋　克巳	日本電信電話(株)　社会情報研究所	主席研究員
寺田　雅之	(株)NTTドコモ　クロステック開発部	担当部長
中野　美由紀	津田塾大学　学芸学部	教授
西垣　正勝	静岡大学　情報学部	教授
松井　充	三菱電機(株)　開発本部	役員技監
盛合　志帆	情報通信研究機構　サイバーセキュリティ研究所	研究所長

CREST【S5基盤ソフト】領域の運営方針

- 研究成果のユースケース想定や競合技術との国際的なベンチマークの自己評価による国際競争力の向上、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
- OSS（オープンソースソフトウェア）化やオープンなAPIの提供等による、多種多様な環境での研究成果普及を推進、本研究領域の他チームや同一戦略目標下のさきがけ「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の推進
- 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等の利活用の推進（次スライド参照）
- 研究ビジョンの構築や研究方向性をブラッシュアップに向けたAIPラボ活動への参画、海外ショートビジットや国際連携ワークショップ等の国際連携推進
- 本年度は、更に日仏共同提案を募集します（詳細は後述）

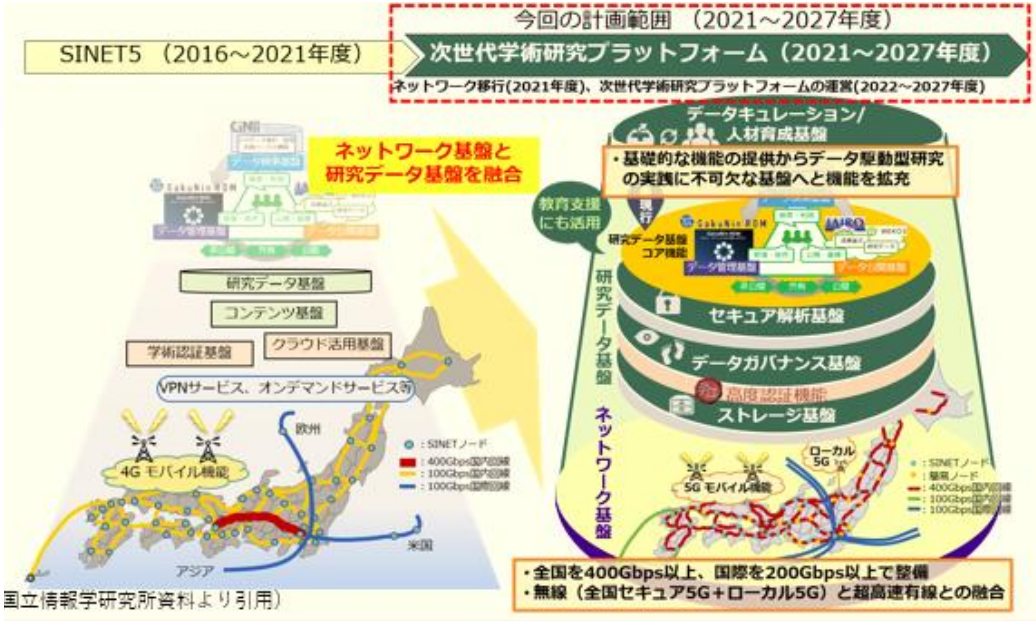
プラットフォーム利活用の例

データ活用社会創成プラットフォーム



（東京大学プレスリリース2021/3/21より抜粋
https://www.u-tokyo.ac.jp/focus/ja/press/z0310_00027.html ）

次世代学術研究プラットフォーム



国立情報学研究所資料より引用）

（第11期情報委員会の資料より抜粋
https://www.mext.go.jp/content/20210412-mxt_jyohoka01-000014099_06.pdf ）

フランスANR(国立研究機構)との日仏共同提案について

1. 日仏の科学研究における協力促進を目的に、2023年度のCRESTの提案募集では、当研究領域において通常の研究提案に加えて、日仏共同研究グループによる共同研究提案を募集します
2. 日仏の研究代表者で1つの共同研究提案書(英語、CREST-ANR共通書式)を作成し、JST(日本)とANR(フランス)にそれぞれ申請していただきます

- JST、ANR両機関に申請されることが審査の要件となります。必ず両機関に申請をしてください(ANR申請受付期間:2023年3月7日(火)～6月5日(月)10:00 CEST)
- ANRとJSTが各々提案の審査を行った後、両機関で協議の上採択を決定します
- CRESTにおける選考では、日仏共同研究提案と通常の研究提案とを分けずに審査します。どちらか一方が有利になることはありません。採択後も通常のCREST課題と同様に研究を推進します
- 研究代表者は日仏共同提案と通常のCRESTの提案の両方を申請することはできません
- CRESTへの応募の際に、ANRに提出した日仏共同研究提案の内容を変更することはできません
- 詳細やその他の留意事項は、WEBをご確認ください

CREST【S5基盤ソフト】研究期間と研究費

- 研究期間：5.5年間（2023年10月から2029年3月末まで）
- 予算規模：総額 1.5億円～3.5億円（間接経費を除く）
- 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のため1件当たりの予算規模を大型化
- 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に向けた予算措置

今年度は本領域の募集最終年度となります。

CREST【S5基盤ソフト】採択評価の基準

- 研究課題例で示した**1つの達成目標**に対してのチーム構成でも、**複数の達成目標に跨がる目標**を立てたチーム構成でも応募可能
- **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より高く評価
- **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を推奨
- **5.5年間でのゴールの成果イメージ、3年後のマイルストーン、研究成果を実社会適用するユースケース、人材育成への取組み**を具体的に記載すること
- **大型化を希望している提案については、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ること**

CREST【S5基盤ソフト】2021年度採択課題

※2021年度採択時

研究代表者（所属機関）	研究課題名	主たる共同研究者
菊池 浩明（明治大学 ）	安全性と有用性の保証のあるヘルスケア匿名コホート基盤	荒井 ひろみ（理化学研究所） 野島 良（情報通信研究機構） 森 由希子（京都大学）
田浦 健次朗（東京大学）	実応用に即したプライバシー保護解析とセキュアデータ基盤	花岡 昇平（東京大学） 塙 敏博（東京大学） 吉川 正俊（京都大学）
竹房 あつ子（国立情報学研究所）	形式検証とシステムソフトウェアの協働によるゼロトラスト IoT	五十嵐 淳（京都大学） 関山 太朗（国立情報学研究所） 松井 俊浩（情報セキュリティ大学院大学）
廣津 登志夫（法政大学）	プライバシセントリック情報処理基盤	光来 健一（九州工業大学）
山口 弘純（大阪大学）	地域を支える知のデジタライゼーションと共有基盤	新井 圭太（近畿大学） 稲場 圭信（大阪大学） 矢内 直人（大阪大学） 矢野 健太郎（讀賣テレビ放送(株)）

CREST【S5基盤ソフト】2022年度採択課題

※2022年度採択時

研究代表者 （所属機関）	研究課題名	主たる共同研究者
アッタラパドゥン ナッタポン （産業技術総合 研究所）	サステナブルな分散型秘密計算 基盤	川村 信一（産業技術総合研究所） 松浦 幹太（東京大学） 松田 隆宏（産業技術総合研究所） 米山 一樹（茨城大学）
天笠 俊之 （筑波大学）	検証可能なデータエコシステム	石川 佳治（名古屋大学） 小口 正人（お茶の水女子大学） 鬼塚 真（大阪大学） 宮崎 純（東京工業大学） 森嶋 厚行（筑波大学）
品川 高廣 （東京大学）	隔離実行と形式検証による 総合的セキュリティ基盤システム	住井 英二郎（東北大学） 広渕 崇宏（産業技術総合研究所）
米澤 拓郎 （名古屋大学）	多様な形態の現実を安心・安全に 創り・繋ぐTrusted Inter-Reality 基盤	青木 崇行（カディンチェ（株）） 金岡 晃（東邦大学）

CREST【S5基盤ソフト】2022年度採択評価の論点

①Society 5.0のスコープ・世界観にマッチしていること
（単なる現状の研究の延長ではないこと）

②基礎理論分野とシステム基盤技術分野を横断的に融合・統合する基盤ソフトを対象とする本領域の趣旨にマッチしていること（しっかりとした理論がない実装のみの提案ではないこと）

③個々のセキュリティやプライバシー技術の組み合わせに留まらないセキュアな基盤やプラットフォームなど全体システムの構築であること

④PoC実施を想定した提案であること。さらに、成果（アウトプット）として、広く利用されるシステムソフトが期待できること

CREST【S5基盤ソフト】採択評価の論点等

・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した提案となっているか

・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・統合型の提案となっているか

・本年度は本領域の募集最終年度となります。戦略目標ならびに本領域の趣旨、目標を踏まえた、自由な発想に基づく挑戦的な提案を多数いただくことを期待いたします

ご清聴ありがとうございました！

多数の研究提案をお待ちしてます

Q&A