「セキュアなデータ流通を支える暗号関連技術（高機能暗号）」に関する研究開発構想（個別研究型）

令和 5 年 12 月
内閣府
文部科学省

目次

1　構想の背景、目的、内容

1.1　構想の目的

1.1.1　政策的な重要性

情報通信技術の発展や社会情勢の変化により、サイバー空間の「公共空間化」が進展し、あらゆるデータがサイバー空間に集積されるようになっている。このような、サイバー空間でのデータ流通が基盤となる時代で、データ流通のセキュリティを自国で確保することは、経済安全保障の観点から不可欠である。サイバー空間におけるセキュリティを確保する手段としては、データを管理する者の能力や対応などの人的アプローチ、データ流通の媒体であるクラウドの外部からの安全性などの技術的アプローチ、クラウドのサーバが所在する場所の法令などの制度的アプローチがある。しかしながら、グローバルなデータ共有や多様な事業者が関与するデータ流通の過程において、機密情報の漏洩やデータの目的外利用、改ざん、不当なモニタリングなどのリスクが高まってきている。したがって、人的・制度的アプローチでは制御しきれないこれらのリスクに対応するため、新たな技術的アプローチが求められている。これは、人工知能や機械学習による大量なデータ消費が一般的となってきた近年、秘匿性の高いデータ処理の実現が要請されていることからも、重要となる。

データ流通のセキュリティを確保する技術的アプローチとしては、データの暗号化が有効であり、単なるデータや通信路の暗号化のみならず、暗号化した状態で解析等のデータ処理ができる高機能暗号が、世界的に注目されている。この高機能暗号の特質は、暗号処理を安全に実行する環境技術や、データのプライバシーを保護する技術を用いることで、最大限に引き出されると考えられる。高機能暗号に、これら技術を補完することで、データ流通のライフサイクル全体でデータ保護を達成することが可能となる。

また、我が国は従前より暗号理論等の研究開発に強みを有しており、安全かつ多様な利用ケースで実装できる次世代技術を、他国を先導して戦略的に獲得できれば、経済社会の発展と経済安全保障の確保・強化に通じるものとして、極めて意義が大きい。

本構想は、個別研究型として、こうした背景の下、領域をまたがるサイバー空間と現実空間の融合システムによる安全・安心を確保する基盤の構

築に資する支援対象とする技術として研究開発ビジョン（第二次）において定められた「セキュアなデータ流通を支える暗号関連技術」[1]において、我が国技術の優位性獲得も念頭に自律性確保を目指すものである。

1.1.2 我が国の状況

近年、様々な分野で、個人情報や企業が持つ機密情報を活用したサービス等を展開する動きが進む一方、他社へのデータ提供時における情報漏洩や不正利用等への懸念も高まっている。また、技術の進歩や社会情勢の変化に伴い、既存の暗号技術よりも効率的で高機能な方式の暗号技術が求められている。データの暗号化及び復号という基本的な機能に加えて様々な特徴をもつ高機能暗号は、機密性の高い金融や医療等の分野のみならず、広範な分野で、データを保護しながら組織内・組織間でのデータ利活用を促進することが期待されている。

そのため、近年 CRYPTREC[2]において、高機能暗号及び耐量子計算機暗号について研究動向等の調査を行っており、2023 年 3 月に技術の概要や活用方法等をまとめたガイドラインを策定している。

国内の研究開発プロジェクトでは、JST AIP 加速課題「秘匿計算による安全な組織間データ連携技術の社会実装」（2022 年度～2024 年度）にて、秘匿計算の実利用を積極的に検討する外部企業・機関と連携し、社会実装に向けた具体的な要望に応える実用的秘匿計算システムの研究開発が行われている。また、戦略的イノベーション創造プログラム（SIP）第 3 期「先進的量子技術基盤の社会課題への応用促進」（2023 年度～）では、秘密計算技術の高性能化・省リソース化に取り組むこととされている。

データ処理を安全に行う補完技術としては、NEDO プロジェクト「高効

---

[1] データ流通の一連の過程（生成～通信～蓄積～解析など）において、データを可能な限り暗号化状態のままで処理し、利用時においてもデータを保護しながら処理するための技術。

[2] Cryptography Research and Evaluation Committees の略であり、電子政府推奨暗号の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討するプロジェクト。デジタル庁、総務省及び経済産業省が共同で運営する「暗号技術検討会」と、国立研究開発法人情報通信研究機構（NICT）及び独立行政法人情報処理推進機構（IPA） が共同で運営する「暗号技術評価委員会」及び「暗号技術活用委員会」で構成される。

率・高速処理を可能とするAIチップ・次世代コンピューティングの技術開発」（2018～2022年度）において、既存のTrusted Execution Environment（TEE）技術に信頼の基点（Root of Trust）をハードウェアとして新規開発し、IoT 機器の信頼性を外部から確認する等のソフトウェア開発が実施されている。また、JST 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」(2021 年度～)では、基盤ソフトウェア研究と理論研究を融合してデータを安全に処理する技術に関する研究開発が、実施されている。

研究機関の取組としては、国立研究開発法人が高機能暗号・耐量子計算機暗号等の暗号・認証技術やプライバシー保護技術の研究開発を実施しており、格子暗号・多変数公開鍵暗号の解読コンテストで世界記録を達成するなど成果を挙げているほか、大手情報通信関係企業が符号暗号の解読コンテストで世界初の成果を創出するなど、大学だけでなく官民での研究開発も盛んに行われている。

1.1.3 世界の取組状況

高機能暗号の研究開発は、従来より暗号の基本的な課題であるが、現在は耐量子計算機暗号の文脈でも行われている。2015 年 8 月に NSA（米国家安全保障局）が暗号方式を耐量子計算機暗号に移行させることを表明し、2016 年 2 月に NIST（米国立標準技術研究所）が標準化計画を発表した。同標準化計画の中で、2022 年 7 月 5 日に公開鍵暗号方式と電子署名方式の標準化方式が発表されたほか、引き続き選定・再公募が行われている。加えて、ISO/IEC（国際標準化機構/国際電気標準会議）や欧州の ETSI（European Telecommunications Standards Institute） においても 耐量子計算機暗号の調査活動や標準化に向けた議論がなされている。

さらに、高機能暗号技術はプライバシー保護の観点でも注目されている。OECD が 2023 年 3 月に PETs[3]に関する報告書をまとめており、暗号技術の近年の進歩や関連技術の整理を行い、高機能暗号、TEE、統計的開示抑制技術（Statistical Disclosure Control, SDC）を活用したプライバシー保護の重要性を提案している。また、米ホワイトハウスも同様に、2023 年 3

[3] PETs: Privacy Enhancing Technologies

月に発表したプライバシー保護データ共有分析（PPDSA[4]）戦略の中で、高機能暗号、TEE、SDC を活用したプライバシー保護を提案しており、データ利活用時におけるプライバシー保護の重要性は国際的にも認識されている。

1.1.4 構想のねらい

本構想では、データ流通の一連の過程（生成～通信～蓄積～解析など）において、データを可能な限り暗号化した状態のままで処理し、利用時においてもデータを保護しながら処理するための技術、すなわち、「セキュアなデータ流通を支える暗号関連技術」の実現を目指す。

データ流通の重要性が増すにつれ、近年、暗号技術への期待が高まってきている。データは流通時に、複雑な経路や雑多な設備下に置かれたとしても確実に保護される必要性があるが、環境に依存せずにデータ保護を実現する手段の一つが、暗号技術である。現状のデータ流通においても通信路の暗号化や、蓄積するデータの暗号化等はなされている。しかしながらデータ流通の全体で見てみると、データの生成から解析までを一貫して暗号化した状態のまま処理する技術は、未だ実現されておらず、元の平文に復号されての処理が随所で行われている。これは、機密情報の漏洩やデータの目的外利用、改ざんなどといった、セキュリティの信頼を低下させる原因となり得る。したがって、データ流通の各過程において有効な高機能暗号技術の獲得を進めていくことが不可欠であり、さらにはこれに加えて、暗号化データ処理の機能性・効率性に限界がある場合への対応方策も、補助的に講じられるべきである。このため、データを隔離して安全に処理し、暗号情報の不正読み出しを防ぐ TEE や、データが平文の状態でもプライバシー等を保護できる統計的開示抑制技術（SDC）等の補完技術を、併せて獲得する。これらの技術を併用して活用することで、データ利用時というデータ流通サイクルの終着点においても、データ保護の達成が可能となる。このような暗号技術と補完技術の両輪をもって、データが安全に保護された、セキュアなデータ流通の実現をねらう。併せて、我が国のデータ流通を長期的に支えてゆくための人材の育成・確保やコミュニティの醸成も目

[4] PPDSA: Privacy-Preserving Data Sharing and Analytics

PETs と PPDSA のいずれも高機能暗号をキーテクノロジーに位置付けている。

指す。

以上により、安全保障に関する情報や個人情報などの機密性が高い情報が含まれるデータのあらゆる処理を、安全を確保して実施することを実現し、また、医療データをはじめとした個人情報や知財との関係性が強い情報など、ニーズが高いが共有・利活用が難しい領域のサービスを活性化させ、経済や研究、自治体サービスなど、様々な場面でのデータ利活用の促進に繋げることを期待する。

1.2 構想の目標

1.2.1 アウトプット目標

＜暗号技術＞

セキュアなデータ流通の実現に必要な高機能暗号に関して、耐量子セキュリティを見据えた高セキュリティ理論の獲得を目指す。また、データ流通に役立つ新しい暗号機能[5]を設計し、その処理における効率も併せて評価することで、機能性・効率性の獲得とその実装（ライブラリ化またはプロトタイプ化）を目指す。

＜補完技術＞

暗号処理を安全に実行する環境技術（TEE 等）：

データを隔離して安全に処理し、暗号情報の不正読み出しを防ぐための技術において、利用ケースに応じて、通常実行環境（アプリケーション、OS、ハイパーバイザ等）から選択的にデータ処理を隔離実行可能とするなど、従来では実現されていない、柔軟性と安全性を有するハードウェア・ソフトウェア技術の獲得を目指す。なお、ハードウェア技術としては、CPU アーキテクチャレベル（計算機方式）における、柔軟な TEE 環境支援技術及びチップとメモリ、チップと IO デバイスの間に流れるデータの耐

[5] CRYPTREC 暗号技術ガイドライン（高機能暗号）では、高機能暗号の有用性は従来の暗号技術と比べ、「暗号化したまま論理演算や算術演算ができる」、「属性、例えば課長以上の役職の職員を指定した、ファイル、ドキュメントへのアクセス制御ができる」、「復号鍵の漏洩対策として、複数人の復号情報が集まらなければ、もとのデータに復号できない設定にできる」、「個人が実際に所有する秘密情報を公開することなく、その秘密を持っていることを他者に証明することができる」等が挙げられている。

タンパ技術の獲得を目指す。

統計的開示抑制技術（SDC）：

暗号化データ処理の出力後（データ復号後）等におけるデータ保護を実現するための、データ利用時のプライバシー保護モデルの研究とセキュリティの検証を目指す。

1.2.2 アウトカム目標

本構想で研究開発する技術で、国内事業者のセキュリティサービスの高度化やエンドユーザーによる安全なデータ処理を実現し、これにより、国内の様々なデータのセキュリティを向上するとともに、データ流通の更なる促進を目指す。また、暗号技術・補完技術の両方において、外国諸組織とも連携しつつ、国際的な新しい技術仕様の検討や、国際標準化に向けたアプローチに貢献することを目指す。加えて、本研究開発を通じ、我が国における暗号技術に関する産学官の連携促進や将来を担う人材の育成、派生的なコミュニティの醸成にも資することを目標とする。

1.3 研究開発の内容

1.3.1 研究開発の必要性

データ流通のセキュリティを確保する技術的アプローチとして、データの暗号化が有効であり、さらに暗号技術をデータ流通の一連の流れにおいて活用することで、更なるセキュリティを獲得できる。例えば、データ漏洩のリスクに対しセキュリティを確保するために、データの目的外利用や意図しない第三者利用を制御するなど、用途に応じて様々な要件を達成していなければならない。こうした種々の需要に応え、媒体や制度に依存しない技術的アプローチとして、高機能暗号の研究開発を行い、セキュリティと利便性を確保することが必要である。また、データ流通のセキュリティと利便性を流通ライフサイクル全般で確保するためには、安全に暗号処理を行うための環境技術及び利用データのプライバシーを保護する統計的開示抑制技術の研究開発に取り組むことが必要である。

1.3.2 研究開発の具体的内容例

＜暗号技術＞

- 高機能暗号の基礎数理モデル等の研究
  - データ処理に活用可能な高機能暗号に関し、量子計算機でも解読されない耐性を持つ基礎数理モデルの検討と、そのセキュリティ評価の研究
  - 高機能暗号に対するサイドチャネル攻撃等の脅威を見積もり、セキュアに実装する研究
- 高機能暗号の機能・効率の開拓の研究
  - データ処理に活用可能な高機能暗号に関し、これまでにない機能や効率の獲得とそのセキュリティ評価の研究
  - 高機能暗号のデータ流通における適用方法を検討し、暗号を用いたデータ処理を高度化する暗号もしくは暗号プロトコルのライブラリ化またはプロトタイプ化を行う研究

＜補完技術＞

- 暗号処理を安全に実行する環境技術
  - TEE に関して、既存の TEE のセキュリティ機構では実現されていない柔軟性、安全性、信頼性を向上させるハードウェア及びソフトウェア技術の研究開発
  - 上記セキュリティ機構を実現するハードウェア及びソフトウェアの安全性等を理論的に検証する技術の研究
- 統計的開示抑制技術（SDC）
  - データ利用時のデータ保護を実現するための、SDC の基礎技術の整備と、そのプライバシー保護モデルの研究
  - 高機能暗号によるデータ処理の出口に SDC を実装し、高機能暗号と SDC の組み合わせの評価を行い、データ利用時のプライバシー保護モデルとそのセキュリティを検証する研究

1.3.3 研究開発の達成目標

セキュアなデータ流通の実現のため、暗号の利用を最大化し、データのセキュリティやプライバシーが確実に守られることを共通の目標として、各研究を行う。暗号技術においては、耐量子セキュリティや、新たな機能性・効率性を有する高機能暗号の理論を獲得する。耐量子セキュリティについては論文出版を、機能性・効率性についてはライブラリ化またはプロ

トタイプ化を、目標とする。

また、従来技術にはない柔軟性と安全性を兼ね備えた、暗号処理を最適な環境で安全に実行可能とする環境技術の開発や、データ流通の様々な局面におけるプライバシー保護に資する新たな統計的開示抑制技術の開発を推進し、高機能暗号との最適な組み合わせを導出する。環境技術については柔軟性と安全性を有する新しい TEE 技術の実現性を検証するプロトタイプシステムの開発を、統計的開示抑制技術についてはプロトタイプ化と実証を目標とする。

これらの研究開発を通じて、個人や組織によってなされるセキュアなデータ流通において、人的・制度的アプローチに依存することなく、まさに技術的アプローチのみによって、実行されるための技術を獲得する。

より具体的には、提案者の設定した個別の達成目標を基本としつつ、文部科学省及び JST のサポートの下、採択後、研究開発を開始するにあたって行う研究計画の調整にて定めると共に、研究開発開始後においては、協議会における意見交換の結果も踏まえ、必要な場合、見直しを行う。

2　研究開発の実施方法、実施期間、評価

2.1　研究開発の実施・体制

公募により研究開発の実施主体をそれぞれ決定する。なお、採択にあたっては、複数の研究開発課題の採択も検討する。また、研究開発成果を社会実装につなげていく視点から、オープンな形での民間企業への技術情報の提供等の民間企業との連携を行うことを推奨する。

プログラム・オフィサー（PO）の指揮・監督の下、研究代表者（研究開発課題の実施責任を法人が担う場合は当該法人を含む。以下同じ。）が研究開発構想の実現に向け責任を持って研究開発を推進する。JST 等の助言に基づき、研究代表者は、適切な技術流出対策を行うよう体制を整備するとともに、研究インテグリティの確保に努め、適切な安全保障貿易管理を行うよう、これらを推進するとともに、研究開発に必要な事項を行う。

研究開発成果を民生利用のみならず公的利用につなげていくことを指向し、社会実装や市場の誘導につなげていく視点を重視するという本プログラムの趣旨に則り、研究代表者は PO 及び研究分担者との協議の上、知的財産権の利活用方針を定めることとする。その際には、研究開発途中及び

終了後を含め、知的財産権の利活用を円滑に進めることができるように努めることとする。

なお、研究開発成果の利活用にあたりその成果にバックグラウンド知的財産権が含まれる場合には、その利活用についても同様に努めることとする。

また、当該分野における民間企業等における処遇水準を踏まえ、研究開発に従事するリサーチ・アシスタント（RA）等大学から人件費の支弁を受ける者には、その報酬等について、海外の事例[6]なども考慮し、これに相応しい水準を支弁する。具体的には、担当する PO が研究計画を踏まえ調整した上で、JST が決定するものとする。

2.2 研究開発の実施期間

研究開発開始から 5 年以内とする。構想全体で最大 50 億円程度の予算を措置する。

2.3 評価に関する事項

自己評価は毎年実施する。外部評価の実施時期は原則、研究開発の開始から 3 年目を中間評価とし、研究開発終了年に事後評価を実施する。具体的な時期については、担当する PO が採択時点でマイルストーンを含む研究計画とともに調整した上で、JST が決定するものとする。

2.4 社会実装に向けた取組

本構想は、高機能暗号技術及び補完技術の研究開発を通じて、データ処理のための暗号技術を公的利用・民生利用が可能な形でライブラリ化・プロトタイプ化し、セキュアなデータ流通の実現を目指すものである。このためには、研究代表者と潜在的な社会実装の担い手として想定される関係行政機関や民間企業等との間で、暗号技術及び補完技術の研究開発成果等

---

[6]「米国高等教育における博士課程学生への経済支援に関する研究」（令和 3 年度学生支援の推進に資する調査研究事業（JASSO リサーチ）研究成果報告書）
https://www.jasso.go.jp/statistics/jasso-research/__icsFiles/afieldfile/2022/03/25/r3jasso-research_report2.pdf

の情報共有や、社会実装イメージ、研究開発の進め方を議論・共有する取組等の伴走支援が有効である。

したがって、今後設置される協議会を活用し、参加者間で機微な情報も含め、社会実装に向けて研究開発を進める上で有用な情報の交換や協議を安心して円滑に行うことのできるパートナーシップを確立することが重要であり、関係者において十分にこの仕組みの運用を検討する必要がある。

なお、協議会の詳細は別に示す。また、PO は研究マネジメントを実施する際には、協議会における意見交換の結果も踏まえるものとする。