2.【研究計画】※適宜概念図を用いるなどして、わかりやすく記入してください。なお、本項目は１頁に収めてください。様式の変更・追加は不可。

(1) 研究の位置づけ

特別研究員として取り組む研究の位置づけについて、当該分野の状況や課題等の背景、並びに本研究計画の着想に至った経緯も含めて記入してください。

[研究計画の背景]

近年、クラウドコンピューティングが普及している。これはクラウドベンダから計算資源をオンデマンドに借りる仕組みである。しかしこの仕組みは、**クラウドベンダが攻撃者にならないという信用**の元でのみ成り立つ。個人情報や営業秘密を含むプログラムなどを扱う場合、このような**信用は前提とするべきでない**。ベンダを信用せずに済むならば、任意のデータ・プログラム・ベンダを用いても**安全に計算資源をシェア**できるプラットフォームが作れるはずである。しかし、いきなり一般の場合を扱うのは困難なため、本研究ではベンダの他にデータ提供者とデータ提供者が１パーティずつ存在する３パーティの場合を扱う。ベンダを信用しない場合、(i)**データとプログラムがベンダに見える**ことがまず問題になる。これは準同型暗号により解決可能 [1] だが、暗号特有の制約によりオンプレミスのサーバと同様に扱える (ii)**利便性が損なわれる**。また、ベンダはコストを抑えるために偽の実行結果を返す可能性があり、(iii) 結果がプログラムの出力だと保証できないことも問題になる。図 1 にこれらの問題をまとめた。

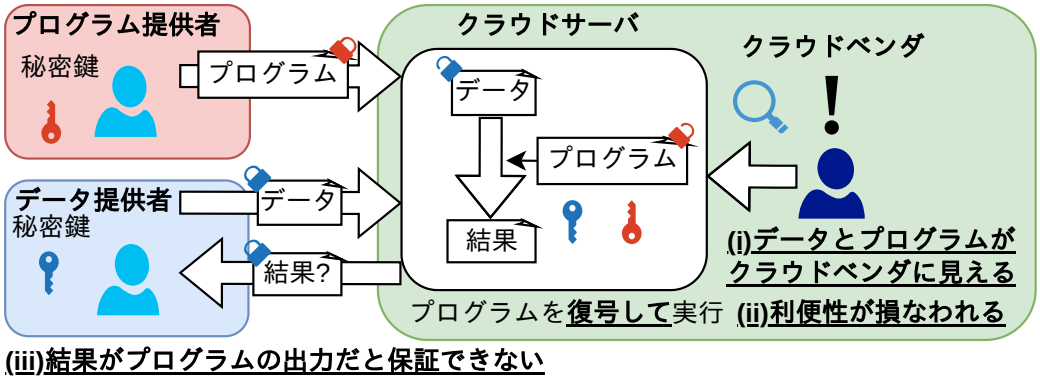

図 1: 既存のクラウドコンピューティングの問題点

[課題・分野の状況]

(i) **データとプログラムがクラウドベンダに見える**: 図１に示すように、クラウドコンピューティングではサーバ上でデータとプログラムは復号される。準同型暗号を用いれば暗号化したまま計算を行えるが、web サービスのようにプログラム提供者とデータ提供者が分かれる場合、計算量が鍵の本数の２乗に比例する [1] ため、計算量が多く現実的でないという問題がある。

(ii) **利便性が損なわれる**: 申請者の過去の研究 [4] では暗号化したまま C 言語を実行可能にした。しかし、2 パーティまでしか対応できず、結果の検証もできない。それに加え、利便性の面でも独自 ISA を採用したためにコンパイラも独自で、他の言語のサポートに多大な労力を要する。

(iii) **結果がプログラムの出力だと保証できない**: **Verifiable Computation(VC)** を用いれば結果がプログラムの実行結果であるかを検証できる。しかし、適用された準同型暗号が限られている [2] か、実装が存在しない [3]。

[着想に至った経緯]

申請者が過去に行った研究 [4] では、データ提供者とプログラム提供者が同一である２パーティの場合にプログラムとデータの同時に保護することを可能にした。しかし、２パーティとして扱えるアプリケーションは限られている。また、過去の研究のセキュリティの評価を行ううちに、偽の結果を返せることが秘密鍵の流出につながるという脆弱性がある。そのため、３パーティへの拡張と結果の検証を同時に達成しつつ、過去の研究で重要視していた利便性を維持するものとして本研究計画を着想した。

【研究計画】（続き）※適宜概念図を用いるなどして、わかりやすく記入してください。なお、各事項の字数制限はありませんが、全体で２頁に収めてください。様式の変更・追加は不可。

(2) 研究目的・内容等

① 特別研究員として取り組む研究計画における研究目的、研究方法、研究内容について記入してください。
② どのような計画で、何を、どこまで明らかにしようとするのか、具体的に記入してください。
③ 研究の特色・独創的な点（先行研究等との比較、本研究の完成時に予想されるインパクト、将来の見通し等）にも触れて記入してください。
④ 研究計画が所属研究室としての研究活動の一部と位置づけられる場合は申請者が担当する部分を明らかにしてください。
⑤ 研究計画の期間中に受入研究機関と異なる研究機関（外国の研究機関等を含む。）において研究に従事することも計画している場合は、具体的に記入してください。

[①研究目的]

本研究の理想は**「クラウドベンダ」への信用を「クラウドコンピューティング」から取り除く**ことである。そのための一歩として本研究では、(I) 線形計算量３パーティ拡張を (II) 暗号上プログラム実行基盤として利便性を保ちながら行い、(III) 計算結果の検証も可能とし、AWS などのパブリッククラウドで動作するプロトタイプ実装も開発する。図 2 にこれらを統合した本研究で提案するプロトコルを示す。

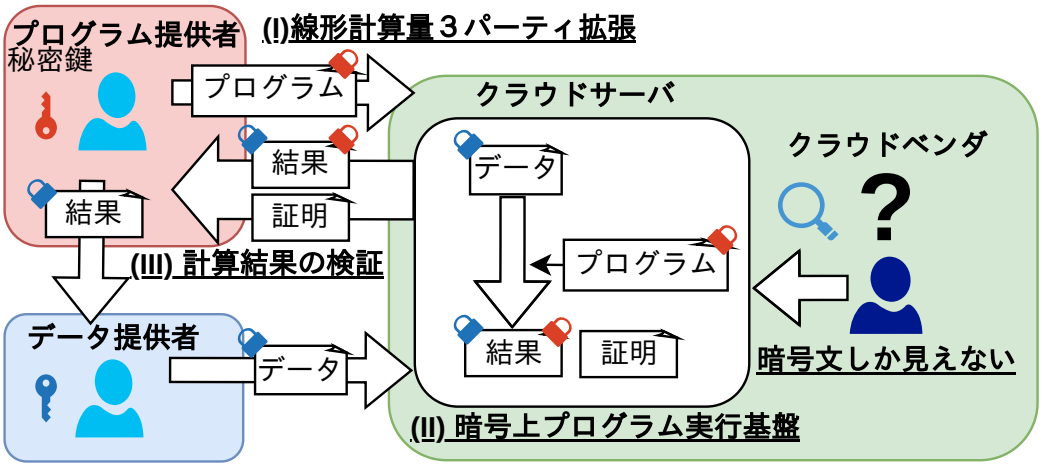

図 2: 本研究の提案するプロトコル

[①②研究内容・研究方法・どこまで明らかにするか]

(I) **線形計算量 3 パーティ拡張**: MK-TFHE(Multi Key TFHE) [1] は３パーティ環境において、(i) データとプログラムがクラウドベンダに見えることを防げる。しかし、計算量が鍵の本数の２乗に比例する欠点がある。本項目では全パーティの鍵の総和を鍵として利用するアイデア [5] を MK-TFHE に適用することで、**計算量を鍵の本数に線形に比例**させる方法を明らかにする。

(II) **暗号上プログラム実行基盤**: 準同型暗号上の計算は特有の表現を使う必要があり、通常のプログラムそのままでは実行できない。(ii) 利便性が損なわれることを防ぐため、本項目では RISC-V CPU の**論理回路を暗号上で実行**することで、プログラムをそのまま実行する方法を明らかにする。さらに、(I) による速度低下を並列化で補う手法、(III) が行いやすくなる CPU の設計法も明らかにする。

(III) **計算結果の検証**: (iii) 実行結果がプログラムの出力だと保証できないことは**準同型暗号に VC を統合**することで解決できる。そのような手法には、(a) 準同型暗号の実行自体を検証する方法 [2] と、(b) 準同型暗号上の計算を検証する方法 [3] の２種類がある。本項目では (I) と (II) と統合する上で (a),(b) のどちらがセキュリティ的・性能的に優れているかを明らかにする。

[②研究計画]

(申請時点から採用までの準備)

採用までの間には (II) 暗号上プログラム実行基盤の実装に向け、CPU・GPU 向け準同型暗号ライブラリの高速化と、準同型暗号の並列実行のためのジョブディスパッチャの複数マシンへの拡張を行う。この成果は論理回路の準同型暗号上での高速な実行基盤として国際会議に投稿予定である。

(研究目的・内容等の続き)
(1 年目: (I) 形計算量 3 パーティ拡張)
採用前から改善する準同型暗号ライブラリにマルチパーティ拡張の知見 [5] を統合し、理論・実装的に高速化する。この成果はマルチパーティでの論理回路向け準同型暗号の理論・実装的改善として国際会議に投稿する。
(2 年目: (II) 暗号上プログラム実行基盤の実装)
採用前と 1 年目の成果に加え、準同型暗号特有の制約を考慮した最適な CPU の設計法を開発することで、既存プログラムの暗号上での高速な実行を実現し、国際会議に投稿する。
(3 年目:(II) 及び (III) 計算結果の検証)
ここまでの成果に VC の知見を統合し、準同型暗号上でのプログラム実行を検証可能にする。この成果は検証可能かつ 3 パーティでの既存プログラムの暗号上実行手法として国際会議に投稿する。

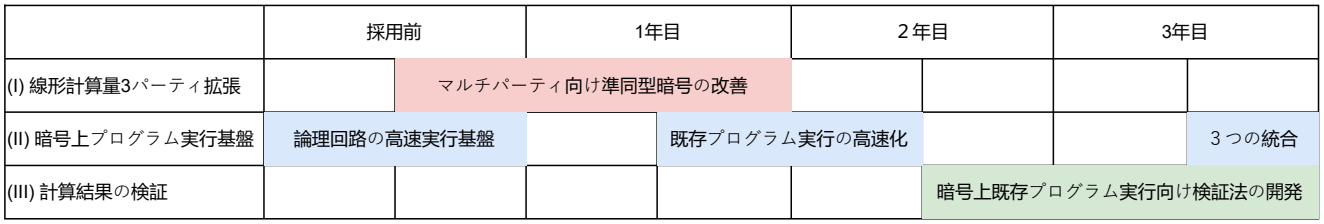

図 3: 研究計画のタイムライン

[③ **特色・独創的な点**]
本研究は準同型暗号上で RISC-V CPU の論理回路を評価することで、既存プログラムの暗号上での実行を可能としつつ、 3 パーティかつ計算結果が検証可能という高いセキュリティを達成することが独創的な点である。特色ある点は本研究では準同型暗号ライブラリ、計算の検証、準同型暗号並列実行のためのジョブディスパッチャ、準同型暗号上で実行する RISC-V CPU をプラットフォームとして実装する点である。
[③先行研究との比較]

(I) 3 パーティに対応した論理回路実行に適した既存の暗号が MK-TFHE[1] であるが、計算量が鍵の本数の 2 乗に比例する欠点がある。本研究では論理回路実行に適した計算量が鍵の本数に線形に比例する準同型暗号を開発する。
(II) 我々の過去の研究 [4] では 2 パーティに限られ、計算の検証は行えていなかった。また、独自 ISA のため、C 言語のみのサポートにとどまっていた。本研究では RISC-V ISA を採用することでより多くの言語を容易にサポートできるようにする。また、(I) と (III) による影響も考慮に入れた最適な CPU の設計法を明らかにする最初の研究である。
(III) 準同型暗号と計算の検証を同時に行う研究は、MK-TFHE [1] に適応できていないか、実装がない [2]。本研究は既存プログラムの暗号上での実行に適した検証法を検討し、実装を与える最初の研究である。

[③ **本研究が完成したとき予想されるインパクト及び将来の見通し**]
本研究完成の暁には、クラウドベンダへの信用を要しない選択肢が用意されることで、社会活動における特定の大企業への依存が低減されると考えている。将来の見通しとしてはクラウドコンピューティングから信用を取り除くことで、個人情報のような機微な情報を扱う場合でも **安全に計算資源をシェア** できるプラットフォームの構築につながると考えている。
[④ **申請者が担当する部分**]
本研究計画の内容はすべて申請者が担当する。

[**参考文献**] [1] “Multi Key Homomorphic Encryption from TFHE”, H. Chen, *et al.* , IACR ASIACRYPT , (2019). [2] “Boosting Verifiable Computation on Encrypted Data”, D Fiore, *et al.* , IACR Cryptology ePrint Archive , (2020). [3] “Non interactive verifiable computing: Outsourcing computation to untrusted workers”, R. Gennaro, *et al.* , IACR CRYPTO , (2010). [4] “Virtual Secure Platform: A Five-Stage Pipeline Processor over TFHE”, Kotaro Matsuoka, *et al.* , 30th USENIX Security Symposium (USENIX Security 21) , pp.4007–4024 (2021). [5] “Key lifting : Multi-key Fully Homomorphic Encryption in plain model”, X. Dai, *et al.* , IACR Cryptology ePrint Archive , (2022).

３．人権の保護及び法令等の遵守への対応 ※本項目は１頁に収めてください。様式の変更・追加は不可。

本欄には、「２.研究計画」を遂行するにあたって、相手方の同意・協力を必要とする研究、個人情報の取り扱いの配慮を必要とする研究、生命倫理・安全対策に対する取組を必要とする研究など指針・法令等（国際共同研究を行う国・地域の指針・法令等を含む）に基づく手続が必要な研究が含まれている場合、講じる対策と措置を記入してください。

例えば、個人情報を伴うアンケート調査・インタビュー調査、行動調査（個人履歴・映像を含む）、国内外の文化遺産の調査等、提供を受けた試料の使用、侵襲性を伴う研究、ヒト遺伝子解析研究、遺伝子組換え実験、動物実験など、研究機関内外の情報委員会や倫理委員会等における承認手続が必要となる調査・研究・実験などが対象となりますので手続の状況も具体的に記入してください。

なお、該当しない場合には、その旨記入してください。

該当しない。

4．【研究遂行力の自己分析】※各事項の字数制限はありませんが、全体で２頁に収めてください。様式の変更・追加は不可。
本申請書記載の研究計画を含め、当該分野における⑴「研究に関する自身の強み」及び⑵「今後研究者として更なる発展のため必要と考えている要素」のそれぞれについて、これまで携わった研究活動における経験などを踏まえ、具体的に記入してください。

(1) 研究に関する自身の強み

・知識の幅・深さ、技量

応募者の最大の強みと言えるのは、研究で使用する**ソフトウェアの多くを自分で開発・保守**を行ってきていることである。中核となる準同型暗号ライブラリは CPU・GPU・FPGA 用の 3 種類を開発しており、それらを用い論理回路を評価する実行エンジン、暗号上で動かすプロセッサまで研究に必要な幅広いソフトウェアをカバーしている [12]。特に準同型暗号ライブラリの実装については情報処理推進機構のセキュリティキャンプにて講師として招聘された他 [13]、企業でのパートタイムジョブとしても行いその成果を査読付き国際ワークショップで発表する [4] など、高い水準にある。学部２, ３年の時には NHK 学生ロボコンにて優勝 [9]、専門分野を超えたハード・ソフトを問わない技量を養った。

・研究における主体性

申請者は**高校生で最初の論文** [1] を出版しており、このときから研究との向き合い方を学んできた。特に本申請の研究計画の核となる準同型暗号に関するテーマは、申請者は学部 3 年生の時点から継続して 3 年以上取り組んできた。学部３年生のときに発案したテーマは、情報処理推進機構の**未踏事業**に採択、スーパクリエータとして認定され [8]、京都大学総長賞も受賞 [10]、成果は査読付き国際学会 (**採択率約 19%**) に採択 [2] された。研究室の継続的指導のない状態で研究を行えたことは主体性の証左であると考える。

・発想力・問題解決能力

学部２回生で準同型暗号を知り、もし準同型暗号が論理関数（NAND）を計算できるのであれば、暗号上でプロセッサが評価できると考えた。最初に発案した準同型暗号のテーマ [2] から始まり本申請に至るまで、このアイデアに基づいており、プログラムとデータの両方を暗号で保護する**セキュリティ**と通常の CPU のような使い勝手という**利便性をより広い条件で達成する**べく進めている。暗号上でのメモリ評価の高速化 [2] や、より複雑な論理ゲートの実現 [4] など、暗号上での CPU の評価における問題をこれまで解決してきている。また、準同型暗号の応用という面では、プロセッサの評価以外にもオートマトン [3] や機械学習 [5] なども試みており、**分野をまたいだアイデア**の実現に取り組んできた。長期的な研究につながるアイデアと分野をまたいだ応用のアイデアの両方に取り組み、その実現のために様々な問題を解決してきたことは申請者の高い発想力と問題解決能力の証と考える。

・コミュニケーション力

未踏 [8] に採択されたチームは異なる背景を持った所属研究室も異なる人間であり、技術的意見の相違から衝突することもままあるが、申請時点まで共同研究を維持できている。また、セキュリティキャンプでは毎年異なる受講者に少人数ゼミを行ってきた。これらは申請者のコミュニケーション力の傍証と考える。

・プレゼンテーション力

申請者は招待講演を含む国内外の会議で発表実績があり [2,4,6]、対外的な発表能力も身につけている。

・成果-レター誌・査読あり

[1] “An RFID tag identification protocol via Boolean compressed sensing,”, **Kotaro Matsuoka** *et al.* , IEICE Communications Express, Volume 5, Issue 5 , 118-123 (2016).

・成果-国際学会またはワークショップでの発表・口頭・査読あり (発表は ○ 筆頭著者)

[2] “Virtual Secure Platform: A Five-Stage Pipeline Processor over TFHE”, ○**Kotaro Matsuoka**, *et al.* , 30th USENIX Security Symposium (**USENIX Security** 21), **採択率約 19%** , pp.4007–4024 (Online, 2021 年 8 月).

[3] “Oblivious Online Monitoring for Safety LTL Specification via Fully Homomorphic Encryption”, ○Ryotaro Banno, **Kotaro Matsuoka** *et al.* , Computer Aided Verification (**CAV**), **採択率約 26%** , (2022 年 8 月).

(研究遂行力の自己分析の続き)

[4] “Towards Better Standard Cell Library: Optimizing Compound Logic Gates for TFHE Association for Computing Machinery”, ○**Kotaro Matsuoka**, *et al.* , In Proceedings of the 9th on Workshop on Encrypted Computing & Applied Homomorphic Cryptography (WAHC ’21), Association for Computing Machinery (ACM) , pp.63–68 (Online, 2021 年 11 月).

・成果-国内学会またはシンポジウムでの発表・口頭・査読なし (発表は ○ 筆頭著者)

[5] 完全準同型暗号における BNN を用いた高速な秘匿推論手法の実装と評価. 情報処理学会全国大会 ○ 橋詰陽太, 古川修平, 松本直樹, 伴野良太郎,**松岡航太郎**, 佐藤高史. (オンライン, 2022 年 3 月)

[6] Virtual Secure Platform: A Five-Stage Pipeline Processor over TFHE (from Usenix Security 2021). 暗号と情報セキュリティワークショップ (WCIS 2021) **招待講演** , ○**松岡航太郎** *et al.* , (オンライン, 2021 年 9 月)

[7] Virtual Secure Platform: A Five-Stage Pipeline Processor over TFHE. FIT2022 **招待講演** , ○**松岡航太郎** *et al.* , (オンライン, 2022 年 9 月)

・成果-受賞

[8] “2019 年度 IPA 未踏 IT 人材発掘・育成事業　スーパクリエータ「準同型暗号によるバーチャルセキュアプラットフォームの開発」”, **松岡航太郎**, https://www.ipa.go.jp/files/000082597.pdf , (2019).

[9] “令和元年度 京都大学総長賞 (NHK 学生ロボコン 2019〜ABU アジア・太平洋ロボコン代表選考会〜 優勝、チェコ杯・NOK 賞受賞、 ABU アジア・太平洋ロボコン選考会ベスト 8、ナガセ賞、ベストデザイン賞受賞)”, 京大機械研究会, https://www.kyoto-u.ac.jp/sites/default/files/embed/jaeducation-campusRecognitionpresidentsdocuments2019zyusyousyalist.pdf , (2020).

[10] “令和 2 年度 京都大学総長賞”, **松岡航太郎** *et al.* , https://www.kyoto-u.ac.jp/sites/default/files/inline-files/r2-sochosho-jyusho-168da1573b39e3ca3fa2c6c362417307.pdf , (2021).

[11] CSS2021 優秀論文賞 https://www.iwsec.org/css/2021/award.html

・成果-公開ソフトウェア

[12] Virtual Secure Platform, https://github.com/virtualsecureplatform

・成果-顕著な学外活動

[13] セキュリティキャンプ 全国大会 2020-2022 L-2 暗号のまま計算しようゼミ 講師 及び 2022 L トラックプロデューサ, https://www.ipa.go.jp/jinzai/camp/2022/zenkoku2022_program_profile.html

(2) 今後研究者として更なる発展のため必要と考えている要素

要素 1: 研究成果を論文としてまとめる能力

これまでの論文執筆では、指導教員等からの指導が不可欠であったと感じている。より高い執筆能力を獲得することは論文投稿にかかるコストを下げより多くの研究に取り組むことを可能にすると同時に、広く成果を発信することでより多くのフィードバックを得られることも意味する。よって、成果を論文としてまとめる能力は研究者としてさらなる発展のため必要と考えている。

要素 2: 暗号学の基礎的知識

ここでいう暗号学の基礎的知識は、2 つの意味合いを持つ。一つには **どういうものならば安全であるか** 、という安全性の前提に関する知識である。準同型暗号は安全性よりその機能に重点が置かれやすく、機能の改善のために既存の安全性証明とは異なる仮定を課すことがある。そのような仮定が安全かを、拡張の提案と同時に議論できる能力の獲得は、より広範な研究テーマに取り組むことを可能にすると考えている。もう一つの意味合いは、ブロックチェーンなどの **準同型暗号以外の暗号技術** への一定程度の理解である。本申請で Verifiable Computation の統合を目指すように、準同型暗号単体では達成できないセキュリティが存在する。よって、どのような技術を組み合わせればより高度なセキュリティが達成できるかの指針が得られる程度の知識を持つことは、より広範な研究テーマの発案につながるものと考える。

５．【目指す研究者像等】※各事項の字数制限はありませんが、全体で１頁に収めてください。様式の変更・追加は不可

日本学術振興会特別研究員制度は、我が国の学術研究の将来を担う創造性に富んだ研究者の養成・確保に資することを目的としています。この目的に鑑み、(1)「目指す研究者像」、(2)「目指す研究者像に向けて特別研究員の採用期間中に行う研究活動の位置づけ」を記入してください。

(1) 目指す研究者像 ※目指す研究者像に向けて身に付けるべき資質も含め記入してください。

①高校時代の自分の助けになるような情報発信

私が人生で初めて読んだ論文は後保範先生の博士論文であり、この論文で学んだ高速乗算法が準同型暗号の高速化に生きている。この経験から、オープンアクセスの論文は誰もが入手できる専門的かつ信頼性の高い情報源であり、高校生が大学院レベルの知識を得ることも可能にする公益性の高いものだと信じている。勿論、前提知識なしに論文を読み解くことは難しく、書籍やブログなど、それ以外の補助的な情報発信も必要である。この自身の経験を次の世代も得られるよう、**最先端の知見をオープンに発信**していくことが目指すべき姿であると考えている。具体的には、自らの論文はすべてオープンアクセスまたはプレプリントを公開し、セキュリティキャンプのような教育的な情報発信の機会には積極的に参加、SNS やブログなどでも補助的な情報を発信する。また、論文はその時の最新の知識を提供するものであるが、自分の知識を体系化し後世に伝える**書籍を執筆することが人生の目標の一つ**である。

②幅広い専門性の獲得

私の座右の銘の一つは「**アイデアは自分の子供**」である。アイデアを実現できるかできないかというのは発案した者の双肩にかかるものであり、最終的に諦めるのだとしても最大限の努力を払ってからにすべきであると考える。この座右の銘を研究者としてのあり方に適用するならば、自分の能力の及ぶ限り研究アイデアの実施を試みるということであり、できる限り**独力で実施するための幅広い専門性を獲得**することが目指すべき研究者像であると考える。幅広い専門性が必要と考えるのは、研究アイデアは自分の専門分野にとどまるものとは限らないと認識しているためである。実際、私が最初の準同型暗号に関連する研究テーマを思いついたのは、準同型暗号という名前と「暗号のまま計算できる」という性質だけを知ったときで、準同型暗号に関する知識はまったくなかった。研究アイデアの実現に自分の専門分野の外の知識が必要なとき、その**学習コストを支払うことをためらわない**ことが目指すべき研究者像であると考える。

③オープンソース実装による再現性の確保

良い研究の必須要件の一つは、再現性が十分に確保されていることだと考えている。実験や評価の結果が再現できなければ、ハードウェアの進歩などで環境が変わった場合に公正な比較ができない。そのため、研究で作成したソフトウェア・ハードウェアは**オープンソースにし後世の研究で自由に使えるように**することが望ましい研究者像だと考えている。

(2) 上記の「目指す研究者像」に向けて、特別研究員の採用期間中に行う研究活動の位置づけ

① 高校時代の自分の助けになるような情報発信

採用中に執筆する**論文はすべてオープンアクセスにするか、プレプリント**を公開する。また、研究内容を Twitter で発信したり、Qiita で基礎的な知識の解説を研究活動の一環として行いたいと考えている。

② 幅広い専門性の獲得

本申請の研究計画の範囲は Verifiable Computation やプロセッサ設計など幅のあるものではあるが、ある程度基礎的な知識を得ている範囲で計画している。これらに加え、エフォートの一部をブロックチェーンや疑似乱数などの暗号学の中の他分野や、機械学習などの応用としての他分野を学習することに当てたいと考えている。

③ オープンソース実装による再現性の確保

採用中に開発するハードウェア・ソフトウェアは Apache または GPL 系のライセンスの元でオープンソースとして公開する。実行環境もパブリッククラウドを利用するなど可能な範囲で再現性に配慮する。