# 令和6年度研究開発成果概要図（目標・成果と今後の成果展開）



## 1．研究課題・受託者・研究開発期間・研究開発予算

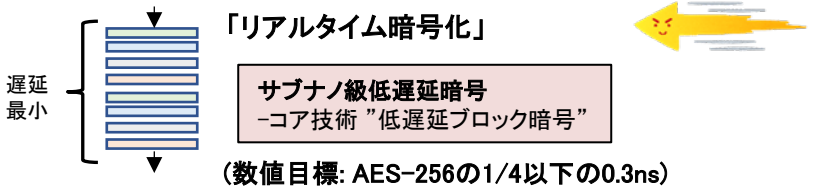
◆研究開発課題名：リアルタイム暗号技術とプライバシー保護への拡張
◆受託者　　：兵庫県公立大学法人　兵庫県立大学、GMOサイバーセキュリティbyイエラエ株式会社
◆研究開発期間　：令和4年度～令和6年度（3年間）
◆研究開発予算（契約額）　：令和4年度から令和6年度まで総額218百万円（令和6年度85百万円）

## 2．研究開発の目標

令和6年度までに「256-bitセキュリティを持つサブナノ級低遅延暗号アルゴリズム」とその拡張であるプライバシー保護技術フレンドリ暗号を開発する。また、開発された各暗号アルゴリズムに対して世界中で利用できる環境の準備として標準化およびOSS化を行う。

## 3．研究開発の成果

研究開発項目1 超低遅延暗号の研究開発




■研究開発項目1　超低遅延暗号の研究開発
・ソフトウェア用低遅延暗号Areionの開発（トップ会議CHES2023採録）
・ハードウェア用低遅延暗号Gleeokの開発（トップ会議CHES2024採録）
**→AES-256の1/4以下の0.3n達成@Nangate 15nm cel library**
・厳密な自動安全性評価技術の確立(トップ会議ASIACRYPT2025採録)
・低遅延技術を拡張し、超高速・低消費電力暗号AETHER開発（トップ会議CHES2025採録）

→研究論文10件採録、特許1件申請

研究開発項目2 プライバシー保護技術への拡張


「プライバシー保護技術」

**プライバシー保護技術フレンドリ共通鍵暗号**
-暗号化したままで演算可能・複数で秘匿計算
-プライバシー保護エッジコンピューティング）

**（数値目標: AES-256の1.5倍以上の速度）**

**研究開発成果：プライバシー保護技術フレンドリ暗号の安全性評価技術確立**
NIST耐量子暗号標準プロジェクトの候補暗号AIMer/Biscuitの脆弱性を発見
- プライバシー保護向けの暗号LowMC/AIM/Rain/Chaghri/Tip5/Monolithの解析
- 技術を開発
- FHE向けの高速暗号PASTAv2を提案(SAC 2024)
- トップ国際会議EUROCRYPT, CRYPTO, ASIACRYPT, FSEに採録

研究開発項目3 研究成果展開

**研究成果展開：標準化団体に関する調査**
- IETFにおける新規暗号アルゴリズムの提案可能性および低遅延/プライバシー保護技術が必要とされるユースケース

**研究成果展開：OSSコミュニティに関する調査**
- 利用実績の多いOSS選定および本研究開発の成果を入れ込むための既存OSSのI/F調査等を実施

研究開発成果: 超低遅延暗号 Areionに関するInternet DraftおよびOSS公開

標準化活動
・IETFにおけるRFC化に向けて、標準化提案としてAreionのInternet Draftを執筆/公開(2件: Areionに関する暗号学的置換、Areion for IPsec)
・IETF Hackathonでの活動報告（3件(見込み)）、セキュリティイベントでの登壇（6件）

OSS活動
・低遅延性が必要とされるQUICプロトコルへの実装に向けて、リファレンス実装、Areion対応TLSライブラリ（quictls）や様々な動作環境・言語対応の4件(見込み)を公開

## 4. 特許出願、論文発表等、及びトピックス

| 国内出願 | 外国出願 | 研究論文 | その他研究発表 | 標準化提案 | プレスリリース<br>報道 | 展示会 | 受賞・表彰 |
|---|---|---|---|---|---|---|---|
| 0<br>(0) | 1<br>(1) | 16<br>(5) | 19<br>(8) | 2<br>(1) | 0<br>(0) | 0<br>(0) | 1<br>(1) |

※成果数は累計件数、( )内は当該年度の件数です。

研究開発項目

- Areionの提案論文が暗号実装分野のトップ会議TCHESに採録
- ßGleeokの提案論文が暗号実装分野のトップ会議TCHESに採録
- 暗号の評価ツールの論文が、暗号分野の難関国際会議CT-RSA, SAC、ASIACRYPT, CICに採録
- 拡張技術(高速艇消費電力暗号AETHER)が暗号実装分野のトップ会議TCHESに採録
- 上記成果により船井学術賞を受賞

研究開発項目2

- FHE向けの高速暗号PASTAv2の提案論文が暗号分野の難関会議SACに採録
- 大きな有限体での解析技術の論文が、トップ国際会議CRYPTO/EUROCRYPT/ASIACRYPT/FSEに採録

研究開発項目3

＜標準化活動＞

- IETFにおけるRFC化に向けて、標準化提案としてAreionのInternet Draftを執筆/公開(2件)
- IETF Hackathonでの活動報告(3件(見込み))、セキュリティイベントでの登壇(6件(見込み))

＜OSS活動＞

- 低遅延性が必要とされるQUICプロトコルへの実装に向けて、リファレンス実装、Areion対応TLSライブラリ(quictls)の2件を公開
- 低遅延性が必要となるアプリケーション向けに様々な環境で利用できるリファレンス実装 4件(見込み)を公開

## 5. 研究開発成果の展開・普及等に向けた計画・展望

- 2025年4月以降における現在公開中のInternet DraftやOSSに対しては適宜更新を行い、利用しようとする方に向けて情報発信を行う。 IETFに投稿しているAreionに関するInternet Draftを中心に、低遅延性を必要としているアプリケーション（e-Sports）や日本国産暗号であることが重要となるユースケース（IPsec）での採用に向けて議論が進展している状況を前向きに捉えて、社会実装に向けて活動を行うための活動費用などの模索を行う。定期的にステークホルダとのやり取りを継続して、実社会で低遅延暗号が利用されるような世界を実現に向けて邁進している。

- 学術的には、本プロジェクトで低遅延性能としてはソフトウェアとハードウェア用で世界最高性能の暗号の開発のために、新しい暗号の設計理論の構築をした。実際この論文発表の後に、いくつかのfollow up workが論文発表されており、学術的な新しい方向性を切り拓いた。具体的には、同様の構造を用いた新しい暗号の設計や、これらの構造に対する安全性評価である。特に後者の安全性評価に関してはまだ未知な部分が多く、今後数年でも厳密な安全性を評価する研究が活発に行われることが予想される。そのため、5年後にはAreionやGleeokの厳密な安全性評価が第三者を中心に実施され、その安全性の信頼がより高まっていることも予想される。また、技術の拡張の観点では、本プロジェクトで実施した高速・低消費電力暗号など新しい実装要求や機能に対する暗号技術への応用も期待される。