# 令和5年度研究開発成果概要図（目標・成果と今後の研究計画）



## 1．研究課題・受託者・研究開発期間・研究開発予算

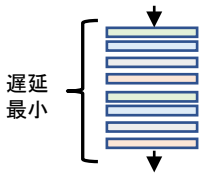
◆研究開発課題名 ：リアルタイム暗号技術とプライバシー保護への拡張
◆受託者 ：兵庫県公立大学法人、GMOサイバーセキュリティ byイエラエ株式会社
◆研究開発期間 ：令和4年度～令和6年度（3年間）
◆研究開発予算（契約額）：令和4年度から令和5年度までの総額134百万円（令和5年度85百万円）

## 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




**「リアルタイム暗号化」**

**サブナノ級低遅延暗号**
-コア技術 ”低遅延ブロック暗号”

**（数値目標: AES-256の1/4以下の0.3ns）**

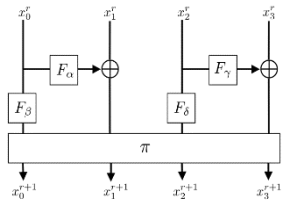
### 研究開発成果A：超低遅延暗号の安全性評価

- **S/W用の低遅延暗号Areion**を設計し、安全性評価完了
  - ✓ 既存のハッシュ関数、認証暗号として世界一の性能達成
- 数理ソルバーを用い安全性評価ツール作成
  - ✓ 既存暗号の未知の特性を発見

### 研究開発成果B：超低遅延暗号の設計

- H/W用の低遅延暗号Gleeokの設計完了
  - ✓ サブナノ級の性能を達成可能

→研究論文6件採録、国際会議1本採択



### 研究開発項目2 プライバシー保護技術への拡張

**「プライバシ保護技術」**

**プライバシ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

- F_(2^n )に定義されるSPN構造に対する厳密な代数度評価技術を開発
- 新しい代数度評価技術の理論を構築
- NIST耐量子暗号標準プロジェクトの候補暗号AIMerの脆弱性を発見
- トップ国際会議EUROCRYPT 2023とCRYPTO 2023とFSE2024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(1件)
・IETF Hackathonでの活動報告（3件）、セキュリティイベントでの登壇（7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）の2件を公開

## 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 | プレスリリース報道 | 展示会 | 受賞・表彰 |
|---|---|---|---|---|---|---|---|
| 0<br>(0) | 0<br>(0) | 10<br>(9) | 11<br>(9) | 1<br>(1) | 0<br>(0) | 0<br>(0) | 12<br>(12) |

※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
- 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に採録
- Gleeokの提案論文が暗号実装分野のトップ会議TCHESに採録

研究開発項目2
- F_(2^n)に定義されるブロック暗号Chaghriに対する解析技術がトップ国際会議EUROCRYPT2023に採録
- F_(2^n)に定義される汎用的なSPN構造に対する代数度評価技術がCRYPTO2023に採録
- NIST耐量子暗号標準プロジェクトの候補暗号AIMerの解析の論文が暗号分野のトップ会議FSE2024に採録

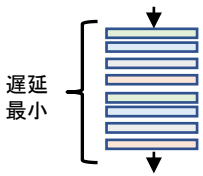
研究開発項目3
＜標準化活動＞
- IETFにおけるRFC化に向けて、標準化提案としてAreionのInternet Draftを執筆/公開(1件)
- IETF Hackathonでの活動報告(3件)、セキュリティイベントでの登壇(7件)

＜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)の2件を公開

## 5. 今後の研究開発計画

| 研究開発目標 | 研究開発計画 |
|---|---|

### 研究開発項目1 超低遅延暗号の研究開発




「リアルタイム暗号化」

**サブナノ級低遅延暗号**
–コア技術 ”低遅延ブロック暗号”

**（数値目標: AES-256の1/4以下の0.3ns）**

| | |
|---|---|
| 2023年度の成果 | 研究開発成果A：初期設計アルゴリズムの安全性評価<br>研究開発成果B：初期設計アルゴリズムの性能評価 |
| 2024年度の計画 | • 超低遅延暗号の最終仕様決定<br>✓ 連携研究員を交えた第三者評価<br>• 連携研究員とハードウェア実装評価<br>最終的なアルゴリズム開発と詳細な安全性、実装評価結果の公開 |

### 研究開発項目2 プライバシー保護技術への拡張

「プライバシ保護技術」


**プライバシ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）**

| | |
|---|---|
| 2023年度の成果 | 研究開発成果：FHEフレンドリー共通鍵暗号に対する新しい解析技術の開発 |
| 2024年度の計画 | • FHEフレンドリー共通鍵暗号の最終仕様決定<br>• 安全性評価<br>• ソフトウェアの実装評価<br>最終的なアルゴリズム開発と詳細な安全性、実装評価結果の公開 |

### 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

| | |
|---|---|
| 2023年度の成果 | IETF会合への参加および低遅延が必要とされる適用先を調査、主要なOSSの調査・実装検討 |
| 2024年度の計画 | 標準化活動<br>・IETFへの標準化提案として、Areion適用のセキュリティプロトコルのInternet Draftを執筆/公開（1件）<br>・IETF Hackathonでの継続活動（1件）、セキュリティイベントでの登壇（2件）<br>OSS活動<br>・リファレンス実装や低遅延性が必要とされるQUICプロトコルやWebRTCの強化（2件） |