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）

プログラム・オフィサー（PO）

プログラム・オフィサー
盛合　志帆
情報通信研究機構 執行役／経営企画部長

サイバー空間におけるデータ流通が国民生活や経済活動の維持・発展の基盤となる中、データ流通をライフサイクル全体で保護する技術的アプローチが求められています。本構想では、高い安全性に加え、新たな機能を備えた機能性や、実装時の性能を高めた効率性を有する高機能暗号技術の確立を目指します。この中で、将来的な量子コンピュータへの耐性をもつ新たな暗号技術や、データ処理を安全に実行するための環境技術、データ利用時のプライバシー保護技術といった補完技術の研究開発にも取り組みます。さらに、本研究開発を通じて、暗号技術に関する産学官の連携強化、人材育成、コミュニティの醸成を促進し、我が国のデータ流通を支えるセキュリティ技術の持続的な発展に貢献したいと考えています。

副プログラム・オフィサー
高橋　克巳
NTT株式会社 社会情報研究所 主席研究員

研究開発構想概要

❶ 暗号技術

暗号の解読を困難にさせるセキュリティに加え、基本的な暗号機能に特別な機能を付加する機能性および、暗号化・復号における計算処理を速める効率性を追求し、高機能暗号技術の獲得を目指す。

❷ 補完技術

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、Trusted Execution Environment（TEE）等の環境技術、および、データ利用時におけるプライバシー保護を実現する、差分プライバシー等の統計的開示抑制技術（SDC：Statistical Disclosure Control）の獲得を目指す。

セキュアなデータ流通を支える技術のイメージ

支援対象となる技術　▶ セキュアなデータ流通を支える暗号関連技術

予算額　最大50億円程度

研究開発構想の詳細はこちらから
https://www8.cao.go.jp/cstp/anzen_anshin/4_20231225_mext.pdf

■ 分科会委員（アドバイザー）

清本 晋作　株式会社KDDI総合研究所 取締役執行役員 副所長
後藤 厚宏　情報セキュリティ大学院大学 情報セキュリティ研究科 教授
佐古 和恵　早稲田大学 理工学術院 教授
曽根 秀昭　東北大学 データシナジー創生機構 特任教授
藤野 毅　立命館大学 理工学部 教授
藤吉 靖浩　株式会社東芝 研究開発センター 上席研究員
森井 昌克　神戸大学 名誉教授

■ 研究開発課題

公募枠 (1)暗号技術

グラント番号 JPMJKP24U1

高機能暗号を活用した連合学習技術の高度化と医療データへの応用

研究代表者

篠原 直行

情報通信研究機構 サイバーセキュリティ研究所 上席研究員

グラント番号 JPMJKP24U2

効率的で安全に利用可能な高機能暗号の数理基盤の構築と展開

研究代表者

高木 剛

東京大学 大学院情報理工学系研究科 教授

グラント番号 JPMJKP24U3

医療ICTの高度化を促進する高機能暗号の開発とその汎用化

研究代表者

花岡 悟一郎

産業技術総合研究所 サイバーフィジカルセキュリティ研究部門 首席研究員

公募枠 (2-1)補完技術(TEE等)

グラント番号 JPMJKP24U4

ハードウェア・ソフトウェア・理論の連携によるユニバーサルTEEアーキテクチャの実現

研究代表者

石川 裕

情報・システム研究機構 データサイエンス共同利用基盤施設 特任教授

公募枠 (2-2)補完技術(SDC)

グラント番号 JPMJKP24U5

高機能暗号と連携するSDC技術の体系化と効率的な実装による大規模分散データの統合

研究代表者

南 和宏

情報・システム研究機構 データサイエンス共同利用基盤施設 教授