■ 公募情報

公募No.	2027R-80
職種	有期研究員
部署	サイバーセキュリティ研究所セキュリティ基盤研究室
研究テーマ	制約のある計算・通信環境における暗号技術・プロトコルの設計・安全性評価に関する研究
研究テーマ要旨	ICT技術の活用においてデータの安全性を確保するためには、暗号アルゴリズム単体の安全性だけでなく、実装、暗号プロトコル、運用を含めたシステム全体の安全性を確保することが重要である。特に、計算能力、メモリ、消費電力、通信量等に制約のある環境では、限られた資源の下で高い安全性と実装効率を両立する暗号技術が求められる。 採用された者は、制約のある計算・通信環境における暗号技術・プロトコルについて、以下の研究開発を行う。 1. 共通鍵暗号や認証暗号等の暗号アルゴリズムの設計および安全性評価に関する研究開発 2. 組込みプロセッサや専用ハードウェア等の多様な実行環境を考慮した暗号技術の設計および実装評価に関する研究開発 3. 実際の通信システムで利用される暗号プロトコルの安全性解析および攻撃手法・対策技術に関する研究開発 4. 形式検証や計算機実験等を用いた、暗号アルゴリズム、実装、プロトコルおよび運用を横断する安全性評価に関する研究開発 5. CRYPTREC事務局運営活動に必要な暗号技術の安全性評価および関連する研究開発
自発的な研究活動等の実施に関して	機構内外の競争性を有する研究資金（科研費等）への申請資格があります。
科学技術・イノベーション創出の活性化に関する法律第15条の2の対象業務該当の有無	【有】
応募要件	1. 暗号技術、情報セキュリティ又は関連する分野における博士課程修了（学位取得）以上、あるいは相当レベルを有すること。 2. 暗号アルゴリズムの設計・解析、暗号プロトコルの安全性評価、形式検証等のいずれかに関する高い知見と研究実績を有すること。 3. 研究開発に必要な計算機実験やソフトウェア又はハードウェア実装に関する高い知見と技術を有していること。 4. 研究成果を論文、技術報告書等として取りまとめ、国内外に発信した経験を有すること。 5. CRYPTREC事務局運営に必要な資料（技術報告書を含む）を執筆できること。
募集人員	1 人
本年度契約期間	採用日　～　令和10年3月31日（更新の可能性：有り）
更新した場合の雇用期間（又は期日）	一定の条件を満たした場合に、採用日より最長5年
給与(本給)	516,000円/月 本給は学歴や職務経験等を考慮し決定します。ただし、本給については、国家公務員の給与に準拠していることから国家公務員の給与に改正があり、当機構労働組合等の合意後に本給の改定が生じた場合は変更する。
勤務地名称	本部 (東京都小金井市)
勤務頻度	週5日（週37時間30分勤務）　※時間外労働有

※従事する業務及び勤務地の変更の範囲：原則として変更無し
※部署の名称、勤務地の名称、及び研究テーマや研究テーマ要旨内の表現に関しては、組織改編等により変更となる場合があります。

NICT有期雇用職員公募情報：https://www.nict.go.jp/employment/apply.html