■ 公募情報

公募No.	2027R-79
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	次世代計算機による暗号の安全性評価
研究テーマ要旨	いかのいずれかの項目（複数項目の場合あり）を実施していただく ・現代暗号に対する次世代計算機の影響調査を理論的および実験的な側面から調査する。 ・素因数分解問題や離散対数問題等の現代暗号の安全性の基礎となる計算問題に対して、量子計算機等の次世代計算機による実験およびシミュレーションを用いた評価を行い、暗号の危殆化時期の予測に役立てる。 ・計算問題を解くための量子回路の設計、実機による実験及び結果の解釈、暗号が危殆化する年代の予測等。
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	・博士の学位を有する者（取得予定を含む）又はこれと同等と認められる研究能力を有する者。以下に示す研究についての知識を有すること。 ・公開鍵暗号に関する知識を有すること。 ・量子計算に関する知識を有すること。特に、電子計算機におけるShorのアルゴリズム等についての知識を有すること。 ・（必須の応募条件ではないが、望ましい応募条件として）：量子計算機によるShorのアルゴリズムの実装など、次世代計算機による暗号の解読実験の実機またはシミュレーターによる経験があること。
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)	541,000円　～　558,000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