■ 公募情報

公募No.	2026R-104
職種	リサーチアシスタント
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	実世界で広く利用されている暗号プロトコルおよびセキュリティプロトコルの安全性評価に関する研究
研究テーマ要旨	当研究室では、実社会で広く利用されている暗号プロトコルおよびセキュリティプロトコルの安全性評価に関する研究を行っている。この補助業務として、主にセキュアメッセージングやエンドツーエンド暗号化プロトコルを対象として、安全性評価に取り組む。具体的には、安全性要件や攻撃者モデルの整理、プロトコル仕様の特定と手動解析に加え、ProVerifやTamarin Proverなどの形式検証ツールを用いた評価を実施する。その過程で、標準化文書や広く利用されている製品の調査を行い、標準化動向や既存製品の設計技術を体系的に整理することが求められる。最終的には、これらの調査・評価結果を担当研究員の下で学術的・科学的観点からまとめ、学会での論文発表に繋げる。
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	以下のすべての要件を満たす者。 1. 基本的な共通鍵暗号および公開鍵暗号の各種プリミティブによって実現可能な、プロトコル設計上の主要な安全性要件について説明できること。 2. セキュアメッセージングおよびエンドツーエンド暗号化において要求される安全性要件（Confidentiality, Integrity, Authenticity, Perfect Forward Secrecy, Post-compromise Security, Deniability 等）を理解し、適切に説明できること。 3. エンドツーエンド暗号化およびクライアント・サーバー間暗号化における攻撃者モデルの相違点を明確に説明できること。 4. 暗号プロトコルおよびセキュリティプロトコルを形式手法により解析するための基礎的な知識を有すること。 5. 実際の製品に組み込まれた暗号プロトコルまたはセキュリティプロトコルに対して、手動での解析に加え、ProVerifやTamarin Proverなどのツールを使用して形式的な安全性検証を実施した経験を有すること。 6. 実際の製品を解析するに当たって重要となる研究倫理とResponsible Disclosureについて理解し、適切に説明できること。 7. 英語による標準化文書（例：RFC、ISO）を読むことに抵抗がないこと。 8. 学会における論文発表経験を有すること、または論文発表を予定していること。 9. 配属研究室内外の人員と協力して研究を遂行できるコミュニケーション能力を有すること。 10. 博士前期課程または博士後期課程に所属している学生であること。 ※ 応募に際して事前に所属大学・研究室の指導教官から了承を得ること。 ※ ※ 日本学術振興会の特別研究員などの専念義務がある学生は、本業務に従事可能であることを示す承諾書を指導教官名で提出すること。また、本業務に支障がある場合は応募者及び指導教官がその責務を負うこと。
募集人員	1 人
契約期間	採用日　～　令和9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)	11,920円～16,920円/日 学部在籍者は日給11,920円、大学院博士課程前期在籍者は日給14,770円、大学院博士課程後期在籍者は日給16,920円。 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2日/1日7時間30分　※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/koubo.html