

■ 公募情報

公募No.	2026R-117
職種	有期研究員
部署	サイバーセキュリティ研究所A Iセキュリティ研究センター
研究テーマ	AIセキュリティおよびAIを活用したサイバーセキュリティに関する研究
研究テーマ要旨	我々は、人工知能（AI）のセキュリティ・安全性確保およびAIを活用したサイバーセキュリティ技術の研究（Studies on AI Security and AI-Powered Cybersecurity）に取り組んでいる。具体的には、AIモデルや機械学習システムの脆弱性分析、敵対的攻撃（adversarial attacks）やデータ汚染攻撃（data poisoning）への対策、AIを用いた異常検知や侵入検知など、多岐にわたる研究を推進している。直近では、特に生成AI（Generative AI）のセキュリティ・安全性評価および生成AIを活用したサイバーセキュリティ応用に注力している。応募者は、これらの研究テーマのうちの一部を担当し、AIセキュリティおよびサイバー防御技術の発展に寄与することが期待される。
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	AIセキュリティに関する研究経験と、その分野での質の高い論文発表実績 英語での技術コミュニケーション能力 博士もしくは修士の学位（取得予定を含む）
募集人員	2 人
本年度契約期間	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)	515,000円 ～ 534,000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	イノベーションセンター (東京都中央区)
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。