■ 公募情報

公募No.	2024T-103
職種	有期研究技術員
部署	サイバーセキュリティ研究所　サイバーセキュリティ研究室
業務名	NICTER解析チームにおけるセキュリティオペレーション業務
業務内容	サイバーセキュリティ研究室では、研究開発した独自のサイバー攻撃観測システムや、セキュリティアプライアンス群、脅威インテリジェンス情報等を用いてNICTER解析チームによるサイバー攻撃の観測・分析を行っている。 本業務では、NICTER解析チームにおいてセキュリティアナリストとして解析業務を行う。主にNICT内のネットワーク（ライブネット）において観測された脅威の解析業務に従事し、脅威の検知から検知された脅威の分析、インシデント対応といったセキュリティオペレーションを実施する。 （主な業務内容） ・SIEMを使った脅威の分析と対応 ・上記オペレーションの高度化・自動化に必要なツール開発 ・脅威インテリジェンス情報を活用したスレットハンティング ・インシデントレスポンス、フォレンジック調査
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	(必須スキル) ・情報セキュリティ、ネットワークセキュリティ、IT技術全般に関する基本的な知識を持ち、さらに専門的な知識や経験を有する特定の得意分野を持つ ・ソフトウェア開発、ネットワーク構築、セキュリティ関連業務の実務経験 ・プログラミング経験（言語は問わない） ・技術文書を読解、作成することができる ・英語の技術文書（RFC、サイバーセキュリティに関する分析レポート、海外ベンダが公表する脆弱性レポート等）を読める ・チームメンバと円滑なコミュニケーションと業務連携をとることができる （あると望ましいスキルや経験） ・課題解決のために既存ツールの活用やプログラムの実装ができる ・どんなに長大なログでも解析し、インシデントの痕跡を発見できる ・SIEMを使ったセキュリティオペレーションの業務最適化や自動化による業務効率化をリードした経験がある ・新しい技術や分析アプローチに対する強い好奇心 （求める人材像） ・言われたことを受け身でやることよりも、主体的に問題解決に取り組むほうが面白いと感じる ・手を動かしてやってみることが苦でない ・「Caring is sharing」の精神に共感し、自分もそうありたいと思ってチームプレイができる
募集人員	1 人
本年度契約期間	採用日　～　令和7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(基本給)	419,000円　～　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

※ 部署名および勤務地名称（業務名、業務内容の記載を含む）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。
※ 従事する業務及び勤務地の変更範囲：原則として変更無し