

■ 公募情報

公募No.	2025T-40
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	セキュリティ脅威情報の分析及びインテリジェンス生成業務
業務内容	<p>サイバーセキュリティ研究室のNICTER解析チームでは、公開された脆弱性情報やサイバー攻撃被害情報、セキュリティベンダーの分析結果など、さまざまな公開情報を収集し、脅威検知および防御力の強化を目的とした独自の分析と脅威インテリジェンス生成を行っている。</p> <p>本業務では、NICTER解析チームでこれらのセキュリティ脅威情報の収集・分析およびインテリジェンス生成を担当する。</p> <p><b>【業務内容の一例】</b></p> <ul style="list-style-type: none"> <li>・脅威情報の収集・整理・分析業務</li> <li>・脆弱性情報の分析（深粒度、被害情報など）業務</li> <li>・インシデント公表された情報の整理と独自評価</li> <li>・脅威アクターの分析（TTPsの把握、攻撃グループの特定）</li> <li>・OSINTの手法やフレームワークの開発、改善、効率化やカバレッジの向上の実現</li> </ul>
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	<p><b>【求める経験・スキル】</b></p> <ul style="list-style-type: none"> <li>・コンピュータサイエンスに関する知識（情報系の4年生大学卒業と同程度）</li> <li>・脆弱性情報の取扱やサイバー攻撃情報の分析に関する業務経験</li> <li>・OSINTに関する専門知識と業務経験</li> <li>・技術文書を読解・作成する能力</li> <li>・英語の技術文書（RFC、海外ベンダが公表する脆弱性レポート等）を読むための英語運用能力</li> <li>・研究室内外の協力者と協調して業務に取り組めるコミュニケーション能力</li> </ul> <p><b>【歓迎する経験・スキル】</b></p> <ul style="list-style-type: none"> <li>・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</li> <li>・Dark Web上の脅威情報を収集・分析する業務経験</li> <li>・Python等のスクリプト言語を用いたプログラム開発経験</li> <li>・中国語やロシア語など英語以外の脅威情報を分析可能な語学力</li> <li>・新しい技術や分析アプローチに対する強い好奇心</li> </ul> <p><b>【求める人物像】</b></p> <ul style="list-style-type: none"> <li>・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方</li> <li>・未知の領域にも好奇心を持ち、積極的に取り組むことができる方</li> <li>・セキュリティ関連のニュースや情報を集めて整理・分析することが好きな方</li> <li>・自分で手を動かして試行錯誤することが苦ではない方</li> <li>・「Sharing is Caring」の精神に共感し、チームプレイを大切にしながら協力できる方</li> </ul>
募集人員	1人
本年度契約期間	採用日～令和8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～611,000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	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（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