■ 公募情報

公募No.	2027T-24
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ネクサスCYNEX研究開発運用室
業務名	サイバーセキュリティ情報収集・分析実証事業支援業務
業務内容	サイバーセキュリティネクサスでは、独自のエンドポイントセキュリティ技術と大規模データ横断分析技術を用いて国内のサイバー攻撃の観測・分析を行っている。 本業務では、CYNEX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。具体的にはエンドポイントセキュリティエージェントが収集する端末の振る舞い情報または、端末で検知されたマルウェア検体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。 加えて、解析結果のレポート作成作業、エンドポイントセキュリティエージェントの性能検証・評価の業務も実施する。 （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 ・マルウェア分析業務 ・解析レポート作成 ・エンドポイントセキュリティエージェントの性能検証・評価
自発的な研究活動等の実施に関して	職務への専念義務があります。
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 ・マルウェア解析またはログ分析業務経験 ・技術文書を読解、作成することができる ・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 ・WIndowsのイベントログを使ったセキュリティ分析することができる ［あると望ましいスキルや経験］ ・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 ・統計学や機械学習、AIに関する専門知識を擁したビッグデータ解析スキル ・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 ・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 ・ARM版Windowsのアプリ開発経験 ［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
募集人員	5 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(基本給)	485,000円　～　738,000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	東京23区内
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、及び業務名や業務内容の表現に関しては、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