■ 公募情報

公募No.	2027T-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脅威分析室
業務名	ライブネット観測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	サイバー脅威分析室ライブネット観測チームにおいて、研究開発した独自のサイバー攻撃観測システムや各種セキュリティ製品、脅威インテリジェンス等を活用し、NICT内の実ネットワーク（ライブネット）を対象としたサイバー攻撃の観測・分析を行う。脅威の検知・分析、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等の一連のセキュリティオペレーションに従事するとともに、得られた知見を活用した検知・分析手法の高度化や自動化、それらに必要となるツールの開発を行う。 【業務内容の一例】 ・SIEMや各種セキュリティ製品を活用した脅威の検知・分析 ・脅威インテリジェンス等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およびフォレンジック調査 ・検知・分析手法の高度化・自動化 ・セキュリティオペレーションに必要となるツールの開発
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	【必須条件】 ・コンピュータサイエンスに関する基礎知識（情報系の4年制大学卒業と同程度） ・TCP/IPをはじめとするコンピュータネットワーク、およびOS等のコンピュータシステムに関する基礎知識 ・インシデントレスポンス、ネットワーク・システム運用、ソフトウェア開発、サイバーセキュリティ等の情報技術分野における実務経験または専門的な知識・経験 ・プログラミングおよびUNIX/Linuxシステムの基本的な使用経験 ・英語の技術文書を読解し、論理的かつ正確な技術文書を作成できること ・研究室内外の関係者と協調して業務に取り組めること ※SOCやインシデントレスポンスの実務経験は必須ではありません。 【歓迎する経験・スキル】 ・SOC、CSIRT等におけるセキュリティ監視・分析やインシデント対応の経験 ・SIEM、EDR等のセキュリティ製品を活用した脅威の検知・分析の経験 ・スレットハンティング、デジタルフォレンジック、マルウェア解析等の経験 ・脅威インテリジェンスを活用したサイバー攻撃の調査・分析の経験 ・課題解決やセキュリティオペレーションの高度化・自動化のために、既存ツールの活用やプログラムの実装を行った経験 【求める人物像】 ・与えられた業務をこなすだけでなく、自ら課題を見つけ、主体的に問題解決に取り組むことを楽しめる方 ・未知の脅威や新しい技術・分析アプローチに好奇心を持ち、積極的に学び、試すことができる方 ・アラートや検知結果を鵜呑みにせず、その背景や原因を自ら調査し、考えることが好きな方 ・自ら手を動かし、試行錯誤しながら検知・分析手法やオペレーションを改善していくことが好きな方 ・「Sharing is Caring」の精神に共感し、自ら得た知識や経験をチームと共有しながら協働できる方
募集人員	1 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　～　558,000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

※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/apply.html