



## サイバーセキュリティエンジニア（公共機関常駐型）

トレンドマイクロ株式会社での募集です。ITコンサルタントのご経験のある方は歓...

### Job Information

**Recruiter**

JAC Recruitment Co., Ltd.

**Hiring Company**

トレンドマイクロ株式会社

**Job ID**

1485334

**Industry**

Software

**Job Type**

Permanent Full-time

**Location**

Tokyo - 23 Wards

**Salary**

6 million yen ~ 10 million yen

**Work Hours**

09:00 ~ 17:30

**Holidays**

【有給休暇】有給休暇は入社後3ヶ月目から付与されます 10~20日。【休日】完全週休二日制 土日 祝日 夏季休暇 年末年始...

**Refreshed**

July 4th, 2024 17:22

### General Requirements

**Career Level**

Mid Career

**Minimum English Level**

Business Level

**Minimum Japanese Level**

Native

**Minimum Education Level**

High-School or Below

**Visa Status**

Permission to work in Japan required

### Job Description

【求人No NJB2236389】

**■業務内容：**

当社お客様先に常駐（23区内）し、各種サポートを頂くポジションです。弊社製品のサポートに留まらず、運用、構築、提案、脅威解析、サイバーセキュリティアドバイザー等、幅広く重要な役割を担い、お客様と密な連携をはかり、サポートおよび各種提案を行って頂きます。

確かな知識と経験を有すサイバーセキュリティのプロフェッショナルとして、トレンドマイクロの価値を直接お客様に届けたいです。（常駐チームは候補者様を含む、当社無期雇用社員、複数人で構成されています。）

<具体的には>

サイバーセキュリティの専門家として、お客様先に常駐し以下の業務を行っていただきます。

- ・様々なログや製品を利用したThreat Hunting業務
- ・セキュリティ全般に関するアドバイザリー業務
- ・マルウェア解析、フォレンジック業務などのインシデントレスポンス業務
- ・当社製品に対する製品サポート業務  
(当社のL3プロダクトチームと連携を実施していただきます。)
- ・当社製品を利用した防御システムの要件定義・基本設計・構築業務・運用業務  
(通常はお客様にて実施いたしますが、インシデントレスポンスの状況や、一部製品に関しては当社にて対応する場合があります。)
- ・最新の脅威動向や国内外のサイバー攻撃等に関するリサーチ業務
- ・上記業務の効率化、自動化

#### ■職務の魅力：

以下の経験を通じて、単なる机上のセキュリティ専門家ではなく、最先端のサイバーセキュリティの知見をもった専門家としてキャリアを築くことができます。

- ・最新のサイバー攻撃手法に対して、予防、検知、防御、調査など様々な観点でアプローチしご自身の力でお客様を守ることができます。
- ・最新のサイバー攻撃手法を解析し、解析結果を元に対策まで一貫してアドバイス、実施しお客様を守っていただきます。そのため、チームや自身の力でお客様を守っているということを実感することができます。
- ・Threat Huntingから対策まで一貫して実施いただきますので、机上の空論ではなく、現実にそった本当にお客様を守るための知識、経験を積むことができます。
- ・サイバーセキュリティの専門家として常駐し、チームで協力しながらお客様との強い信頼関係を構築していくやりがいがあります。

★当社では、従業員の”キャリア自律”を支援するための人事制度を設けております。ぜひご覧ください。

[https://www.trendmicro.com/ja\\_jp/about/careers/mission\\_and\\_culture.html](https://www.trendmicro.com/ja_jp/about/careers/mission_and_culture.html)

社員インタビュー

<https://appweb.trendmicro.com/trendmicro/jobs/interview.html>

## Required Skills

【必須】 ・NWまたはサーバー、インフラ基盤の保守運用、構築経験（5年以上）またはサイバーセキュリティ関連業務（5年以上） ・運用系資格、セキュリティ系資格をそれぞれ1つ以上保持していること ー運用系資格：CCNA、MCP、PMPなど、セキュリティ資格：CISSP、情報処理安全確保支援士などのうち1つ以上（入社時に保持されていない場合は入社後に取得いただきます） 【歓迎】 ・クラウドコンピューティングや仮想化技術に対するセキュリティについての業務経験 ・テクニカルサポート経験（製品の障害が発生した場合は、その対応も含まれるため） ・プログラミング能力【英語力】 入社時は不問ですが入社後学習する意欲がある方 ※グローバルの最先端の脅威動向収集のために、海外のエンジニアとの知識の共有が必要となります。顧客は国内企業であるため実業務における英語の使用はほとんどございません)

## Company Description

コンピュータ及びインターネット用セキュリティ関連製品・サービスの開発・販売