



社内SE／情報セキュリティに関する推進者／週3日以上リモート可

社内SE（インフラ）のご経験のある方は歓迎です。

## 募集職種

### 人材紹介会社

株式会社ジェイ エイ シー リクルートメント

### 採用企業名

非公開

### 求人ID

1481174

### 業種

機械

### 雇用形態

正社員

### 勤務地

東京都 23区

### 給与

550万円～1200万円

### 勤務時間

09:00～18:00

### 休日・休暇

【有給休暇】有給休暇は入社時から付与されます 初年度 22日 1か月目から 【休日】週休二日制 土日 祝日 GW 夏季休暇  
...

### 更新日

2024年06月20日 09:01

## 応募必要条件

### キャリアレベル

中途経験者レベル

### 英語レベル

日常会話レベル

### 日本語レベル

ネイティブ

### 最終学歴

専門学校卒

### 現在のビザ

日本での就労許可が必要です

## 募集要項

【求人No NJB2155233】

### ■配属部門のミッション

グループ全社のセキュリティ活動全体を管理、推進し、OA、OT（工場）、製品の3領域と役割に応じたセキュリティ体制を構築する

### ■職務内容

#### ■入社後に任せる業務

グループ共通のセキュリティに関する企画、展開、運用業務

情報セキュリティ推進はセキュリティ全体活動及び主にOA、ITセキュリティを対象としたセキュリティ推進活動です。

#### <入社後>

現在実施中のセキュリティ活動・課題への参加例)

- ・グループ全体におけるセキュリティ活動の推進（当社ポリシーに則ったIT利用の推進、是正）
- ・セキュリティ関連のシステム運用
- ・SOC（Security Operation Center）の体制整備、運用改善
- ・ガイドライン、チェックリスト整備、展開
- ・資産管理システムの改善、次期システム構想
- ・メールセキュリティ強化
- ・既存運用の見直し、手順整備

#### <将来的に任せたい業務（例）な活動、都度活動>

- ・セキュリティシステムの企画立案・新規導入・展開
- ・セキュリティガバナンス、セキュリティポリシー策定
- ・グループ共通のITインフラ構築PJ
- ・当社グループのセキュリティ委員会の管理・運営
- ・OAセキュリティ組織のとりまとめ

#### ■テレワーク

リモートメイン：週にリモート3日以上

※出社は業務の必要性に応じて個人判断に委ねる（月に数回は対面ミーティングあり）

#### ■フレックス：有

#### ■当業務の面白み・魅力

- ・2022年度から再構築したチームですので、初期チームメンバーとしての参画や組織構築の過程に関わる事ができます。
- ・当社グループ全体のセキュリティを担うことになるので、その面でのやりがいを感じることができます。
- ・主にOA領域において幅広い分野に携わることで関連するスキルを身に付けることができます。
- ・プロジェクトの最上流から下流まで幅広く関わることができます
- ・新技術の調査やPOCによるシステム評価を主導できます
- ・業務に関連する様々な研修やセミナーなどへの参加が認められていますので、スキルアップに繋げることができます

#### ■キャリアステップイメージ

入社直後：グループ内のセキュリティシステムの基本的な運用業務を経て、プロジェクトへ参画

- ・セキュリティに関する課題、運用業務・管理業務を担当
- ・重点課題や構築業務のメンバーとして参加 ※PJ内容、経験に応じて

5年後以降：

- ・セキュリティに関する重点課題のPL・PMを担当
- ・セキュリティに関する課題提案、解決策の企画立案
- ・各種システム導入におけるセキュリティ支援
- ・OAセキュリティのリーダーとしてセキュリティ組織の拡大、他分野取り込み
- ・セキュリティ人材育成及びチームメンバーの拡充・レベルアップ

## スキル・資格

■必須要件【経験】 ・システム設計・構築・運用のいずれか5年以上の業務経験。 ・パソコン・ネットワーク・サーバに対するセキュリティシステムの企画、提案もしくは新規導入 ・セキュリティシステムの運用経験 ・社内ユーザーまたは顧客との直接交渉・調整経験 ・ユーザーへのセキュリティ活動の展開業務経験 ・プロジェクトへの参画経験【知識・専門性】 ・パソコン、ネットワーク、サーバ等のITに関する基本的な知識 ・セキュリティ全般の基本的な知識 ・セキュリティシステム導入時の運用に関する知識【使用ツール、資格】セキュリティあるいはITに関する資格のいずれか【英語】TOEIC500点以上 ■尚可要件【経験】 ・セキュリティ体制の構築もしくは支援経験 ・セキュリティポリシー・ガイドラインの策定、展開経験 ・ペネトレーションテストから課題発見〜対策まで実装した経験 ・実際に発生したセキュリティインシデントへの対応経験 ・プロジェクトマネージャーの経験 ・セキュリティ人材の育成 ・製造業のセキュリティ運用経験【知識・専門性】 ・ITセキュリティ監査の知識 ・セキュリティインシデント対応業務知識 ・セキュリティに関する法律知識 ・クラウドに関する知識【使用ツール、資格】情報処理安全確保支援士、CISSP、SSCP等の高度セキュリティ資格【英語】TOEIC700点以上、メール・マニュアル読解：中級レベル、電話・商談：中級レベル

## 会社説明

ご紹介時にご案内いたします