



## 株式会社日立製作所

### 日立の事業や製品におけるセキュリティ強化のためのセキュリティ人財【課長クラス】

---

日立の事業や製品におけるセキュリティ強化のためのセキュリティ人財【課長クラス】

#### 職務内容:

【配属組織名】

デジタルシステム&サービス統括本部 セキュリティリスクマネジメント本部 セキュリティポリシー&テクノロジーセンター

#### 【配属組織について（概要・ミッション等）】

日立における事業のデジタルシフトによって、すべての製品・サービスでセキュリティ確保の重要性が増しています。日立の中核事業である日立のデジタルシステム&サービスセクターに位置するセキュリティ技術部門となります。デジタルシステム&サービス部門の製品・サービスをサイバー攻撃から護るPSIRT(Product Security Incident Response)活動を始めとし、日立グループ全体の製品・サービスをサイバー攻撃から護るための技術支援活動もおこなうセキュリティ専門家集団です。

#### 【携わる事業・ビジネス・サービス・製品など】

日立グループの製品・サービスのセキュリティを確保するための活動に従事いただきます。日立グループ全体のセキュリティ活動は、情報セキュリティ報告書として発行しています。  
<https://www.hitachi.co.jp/sustainability/download/pdf/securityreport.pdf>

#### 【募集背景】

製品やサービスのセキュリティを確保して、お客様に安心・安全を提供することは、日立における最優先課題の一つです。そのために日立はセキュリティ体制の強化を実施しています。社内でのセキュリティ人財育成に加えて、社外からも人財を募集します。日立の製品・サービスのセキュリティを牽引していく方の応募をお待ちします。

## 【職務概要】

---

製品・サービスのセキュリティを確保するための活動

---

### 1. セキュリティ・インシデント・レスポンス

---

### 2. ホワイトハッカー

---

### 3. セキュリティエンジニアリングデザイン

---

### 4. セキュリティ脅威情報、脆弱性対策業務

## 【職務詳細】

---

### ■セキュリティインシデントレスポンス業務

---

・セキュリティ技術支援[サイバーセキュリティの高度な知見と経験をもとに、脆弱性対策(セキュリティ設計レビュー等)やインシデント対応など]

### ■ホワイトハッカー

---

・サイバー攻撃を行う犯罪者の脅威から、自社のシステムを守るITスペシャリスト

・攻撃者視点で対象を調査分析し、弱点(脆弱性やその悪用方法など)を把握、対応方法についても指示やアドバイス

### ■セキュリティエンジニアリングデザイン業務

---

・システムや製品・サービスへのセキュリティ実装やセキュリティ脅威への対応の仕組み構築

・外部環境変化(モダンな開発手法・技術・規制等)に対応したセキュリティ施策や規則の再構築[DevSecOps, SBOM対応等]

・セキュリティ強化施策支援の立案、推進 など

### ■セキュリティ脅威情報、脆弱性対策業務

・セキュリティ脅威情報、脆弱性情報の発信/分析

・ASM(Attack Surface Management)や脅威インテリジェンスを活用した分析

など

---

※主として製品やサービスのセキュリティに関わる業務となります。上記以外にセキュリティアセスメント業務や脆弱性対策のためのプラットフォームの構築・運用業務などもあり、応募者の経験やスキルに合わせて、具体的な担当業務は決めさせていただきます。

## 【ポジションの魅力・やりがい・キャリアパス】

---

- ・日立においてセキュリティを確保するための技術的な中核を担います。
- ・大きな企業体である日立グループで日立のセキュリティを牽引し、セキュリティに対する課題に取り組みます。セキュリティに意欲のある方にはセキュリティ資格の取得や社内外のセキュリティに関わる研修の受講を支援します。
- ・セキュリティスペシャリストとしてスキル・経験を深めていただけるとともに、ご志向性や評価などによってはマネジメントとしてのキャリアパスもございます。

## 【働く環境】

---

### ■配属組織/チームについて

---

配属組織は、セキュリティの専門組織となり、DPTセンタには約30名程度の社員が在籍しております。関連部門とのコミュニケーションや現場とのコミュニケーションも多くあります。また、経験者採用入社者もあり、ご活躍されていらっしゃいます。

### ■働き方について

---

出社は週1回程度を想定しています。[2025年7月時点での出社頻度。将来を保証するものではない] (グループ単位で出社日をあわせ、会議やグループでのコミュニケーションをはかっています)

※上記内容は、募集開始時点の内容であり、入社後必要に応じて変更となる場合がございます。予めご了承ください。

## 応募資格

### 【必須条件】

- ・セキュリティに関する高度な知識・知見・スキルをお持ちで、セキュリティ分野に更に積極的に関わりたいという意識をお持ちの方。
- ・英語で読み書きが可能な方(英語で書かれたセキュリティ関連の文書が読める)
- ・IT製品あるいはITサービスの開発に関する基本的な知識がある。

### 【歓迎条件】

---

- ・企業のCSIRT/PSIRT業務の従事経験者。
- ・ネットワーク設計・構築、アプリケーションの設計・開発、ITシステムの設計・構築の従事経験者。
- ・セキュリティに関する資格をお持ちの方(CISSPや情報処理安全確保支援士など)

## 【求める人物像】※期待行動・コンピテンシー等

---

### 【全職種共通（日立グループ コア・コンピテンシー）】

---

- ・ People Champion（一人ひとりを活かす）： 多様な人財を活かすために、お互いを信頼しパフォーマンスを最大限に発揮できる安心安全な職場(インクルーシブな職場)をつくり、積極的な発言と成長を支援する。
- ・ Customer & Society Focus（顧客・社会起点で考える）： 社会を起点に課題を捉え、常に誠実に行動することを忘れずに、社内外の関係者と協創で成果に責任を持って社会に貢献する。
- ・ Innovation（イノベーションを起こす）： 新しい価値を生み出すために、情熱を持って学び、現状に挑戦し、素早く応えて、イノベーションを加速する。

### 【最終学歴】

---

高専卒以上

---

待遇:

【想定ポジション】

課長クラス

---

※募集開始時の想定であり、選考を通じて決定の上、オファー時にご説明いたします。

### 【給与】

---

■想定月給：640,000円～730,000円

---

■想定年収：11,600,000円～13,300,000円

---

### 【勤務時間】

---

8:50～17:20（実働7時間45分、休憩45分）

※事業所によって時間帯が異なる場合あり。

その他採用条件についてはこちら

---

### 【更新日】

---

2025年08月04日

---

勤務地:

日立システムプラザ新川崎（神奈川県川崎市）

備考:

【対象年齢】 30才～45才程度

---

