【日系Fintech】サイバーセキュリティ（シニア）｜開発・インフラ経験を活かす

業界経験不問；アプリケーション開発、インフラエンジニア、システム運用経験者も歓迎

Job Information

Recruiter
Morgan McKinley

Job ID
1618670

Industry
Bank, Trust Bank

Job Type
Permanent Full-time

Location
Tokyo - 23 Wards

Salary
Negotiable, based on experience

Refreshed
October 20th, 2026 12:05

General Requirements

Minimum Experience Level
Over 6 years

Career Level
Mid Career

Minimum English Level
Fluent Level

Minimum Japanese Level
Native Level

Minimum Education Level
Bachelor's Degree

Visa Status
Permission to work in Japan required

Job Description

フィンテック大手にて、サイバーセキュリティ・シニアスペシャリストを募集しています。

フィンテック業界未経験でも応募可能。アプリケーション開発、インフラエンジニア、システム運用の経験を活かし、サイバーセキュリティ領域に挑戦できるポジションです。

顧客基盤の拡大とデジタルサービスの進化を背景に、クラウドセキュリティ、システムリスク評価、セキュリティ監視、インシデント対応など、幅広い領域を担当していただきます。

技術部門や事業部門と連携しながら、金融サービスの安全性と事業継続性を支え、専門性を広げられる環境です。

コアタイムなしの柔軟な勤務制度やハイブリッドワーク、スキルアップ支援も魅力です。

主な職務内容

- 顧客向けサービス、クラウド環境、社内システムにおけるサイバーセキュリティ施策の企画・推進、セキュリティ強化プロジェクトの実施
- クラウドサービス、新規システム要件、既存アプリケーションのリスク評価と、実効性のある対策の提案
- ログ分析、セキュリティ設定のレビュー、セキュリティ監視ツールの運用・改善
- 脆弱性診断、ペネトレーションテスト、インシデント対応訓練などの調整・推進
- CSIRT活動の支援、ログ調査、インシデント対応、セキュリティポリシーの改善
- エンジニアリング部門・事業部門・外部セキュリティベンダーとの連携

An established **digital financial services company in Japan** is seeking an experienced **Senior Cybersecurity Specialist** to strengthen its cybersecurity capabilities, protect critical financial systems, and enhance security risk management across its growing digital business.

In this role, you will plan and execute **cybersecurity initiatives, security risk assessments, cloud security improvements, and incident response activities** to safeguard customer-facing financial services, internal business systems, and cloud environments.

Working closely with **IT infrastructure, software engineering, business stakeholders, and external security vendors**, you will identify security vulnerabilities, assess technical risks, and implement practical measures to improve the organization's security posture.

You will also contribute to **Computer Security Incident Response Team (CSIRT) operations**, security monitoring, vulnerability assessments, penetration testing coordination, and incident response readiness.

This opportunity is ideal for professionals with experience in **Cybersecurity Engineering, IT Security, Cloud Security, Information Security Risk Management, Security Operations, or Infrastructure Engineering** who want to make a meaningful impact within Japan's digital financial services industry.

The position offers a **flexible hybrid working environment, core-hours-free flextime, and professional development opportunities**.

Key Responsibilities

- Plan, manage, and execute **cybersecurity initiatives, security improvement programs, and IT security projects** across digital financial services.
- Strengthen security controls for **customer-facing applications, cloud infrastructure, and internal enterprise systems**.
- Conduct **security risk assessments** for cloud services, new system requirements, and existing applications.
- Identify technical vulnerabilities, evaluate potential threats, and recommend effective **risk mitigation measures**.
- Operate and enhance **security monitoring tools, log analysis processes, and security operations procedures**.
- Perform security configuration reviews to identify control weaknesses and improve system protection.
- Coordinate **vulnerability assessments and penetration testing** with internal teams and external cybersecurity vendors.
- Support **cybersecurity incident response exercises, security readiness reviews, and incident handling procedures**.
- Contribute to **CSIRT activities**, including security event investigations, log analysis, incident escalation, and response coordination.
- Collaborate with software engineering and infrastructure teams to improve **application security, cloud security, and system resilience**.
- Review and enhance **information security policies, security procedures, and cybersecurity governance practices**.
- Translate security assessment findings into actionable recommendations for technical and non-technical stakeholders.
- Manage cybersecurity projects and improvement initiatives from planning through implementation.
- Work with business teams to balance **security requirements, operational efficiency, and customer experience**.
- Support the continuous improvement of the organization's **cybersecurity readiness, operational resilience, and enterprise risk management capabilities**.

Required Skills

必須条件 経験・資格：

- サイバーセキュリティ対策の企画・導入・運用経験
- または、アプリケーション開発、インフラエンジニアリング、システム運用の経験 + セキュリティ領域への強い関心
- IT・サイバーセキュリティ領域におけるプロジェクト、施策、業務プロセス改善の主導または推進経験
- ITシステム、インフラ、クラウド環境、情報セキュリティリスクに関する基礎知識
- 技術的なリスクを評価し、改善点を特定して具体的なセキュリティ対策に落とし込む能力
- 大学卒以上

ソフトスキル：

- 複雑な問題を整理し、リスクを分析して実践的な解決策を導く論理的思考力

- 課題を自ら発見し、施策を完了まで主体的に推進する力
- 新しい技術や変化するセキュリティ課題に柔軟に対応する適応力
- 技術・非技術部門と協力し、業務を推進するステークホルダーマネジメント能力

語学力：
- **日本語：**ネイティブレベル
- **英語：**流暢

歓迎条件
- 金融業界におけるサイバーセキュリティ、ITリスク管理、またはシステムリスク評価の経験
- 脆弱性診断、ペネトレーションテスト、CSIRTなどのセキュリティ関連業務の経験

採用企業について
日系フィンテック大手。

手軽に利用できる金融サービスを提供し、確かな事業基盤を持つ日本発のフィンテック企業です。

現在、顧客基盤の拡大とデジタルサービスの進化に伴い、サイバーセキュリティ、オペレーショナル・レジリエンス、全社的なリスク管理への投資を進めています。

技術部門と事業部門が連携する環境で、重要な金融サービスの安全性と信頼性の向上に貢献できます。

この求人がおすすめの理由
- フィンテック業界未経験でも応募可能
- アプリケーション開発、インフラエンジニア、システム運用の経験を活かしてセキュリティ領域に挑戦できる
- クラウドセキュリティ、リスク評価、セキュリティ監視、インシデント対応、セキュリティガバナンスまで幅広く携われる
- ハイブリッド勤務可、コアタイムなしの柔軟な勤務制度
- 専門能力の開発支援あり
- 年収1,400万円〜応相談

Required Skills and Qualifications**Experience:**
- **Over 6 years of professional experience** in IT, cybersecurity, application development, infrastructure engineering, or system operations.
- Experience planning, implementing, or operating **cybersecurity measures**, or a strong technical background in application development, infrastructure engineering, or system operations with a demonstrated interest in security.
- Experience leading or coordinating **IT projects, cybersecurity initiatives, or process improvement activities** .
- Fundamental understanding of **IT systems, network infrastructure, cloud environments, and information security risks**.
- Ability to conduct **technical security risk assessments** and identify potential system vulnerabilities.
- Experience translating technical findings into practical **security improvement plans and risk mitigation measures** .
- Ability to collaborate with technical teams to implement and maintain effective security controls.
- Bachelor's degree.

Soft Skills:
- Strong **logical thinking, analytical problem-solving, and risk assessment capabilities** .
- Ability to break down complex technical challenges and develop practical security solutions.
- Proactive **ownership mindset**, with the ability to identify security gaps and drive improvement initiatives independently.
- Excellent **communication, stakeholder management, and cross-functional collaboration skills** .
- Ability to work effectively with **engineering teams, infrastructure specialists, business stakeholders, and external vendors**.
- Adaptability and willingness to learn new technologies and respond to evolving cybersecurity threats.
- Strong organizational skills with the ability to manage multiple security initiatives and priorities.
- Ability to communicate technical security risks clearly to non-technical stakeholders.
- Strong sense of responsibility, attention to detail, and commitment to continuous security improvement.

Language Requirements:
- Japanese: Native
- English: Fluent

Preferred Skills & Qualifications
- Experience in **Cybersecurity, Information Security, or IT Security within financial services, FinTech, or digital banking organizations**.
- Hands-on experience with **cloud security assessments, security monitoring tools, and log analysis** .
- Familiarity with **Computer Security Incident Response Team (CSIRT) operations and security incident handling**.
- Experience coordinating **vulnerability assessments, penetration testing, and security remediation activities** .
- Knowledge of **cloud security controls, infrastructure security, and application security** .
- Experience with **security configuration reviews, threat detection, or security operations improvement** .
- Familiarity with **cybersecurity governance, information security policies, and operational risk management** .
- Experience working with **software development, infrastructure engineering, and security operations teams** .
- Interest in strengthening **cybersecurity resilience, incident response readiness, and enterprise security governance**.

About the Company
Morgan McKinley is partnering with an **established digital financial services organization in Japan** that combines a strong business foundation with a technology-driven approach to delivering convenient and accessible financial products.

With a rapidly expanding customer base and evolving digital services, the company is investing in **cybersecurity, operational resilience, information security risk management, and enterprise-wide security capabilities**.

The organization focuses on protecting customer information, maintaining the reliability of its digital financial platforms, and

strengthening the security of its technology infrastructure.

Its technology teams work collaboratively across **software engineering, IT infrastructure, business operations, and information security functions**, providing opportunities for cybersecurity professionals to contribute directly to the safety and reliability of critical financial services.

This position offers broad exposure to **cloud security, cybersecurity risk assessment, security operations, incident response, and security governance** within a growing technology-driven financial services environment.

Why You'll Love Working Here

- Join an **established digital financial services company** investing in cybersecurity and technology innovation.
- Work across a broad range of **cybersecurity disciplines**, including cloud security, risk assessments, security monitoring, incident response, and governance.
- Contribute directly to protecting **customer-facing digital financial services and critical business systems** .
- Help strengthen **customer trust, information security, and operational resilience**.
- Enjoy a **flexible hybrid working model with remote work opportunities** .
- Benefit from **flextime without core hours**, supporting greater flexibility in managing your work schedule.
- Work in a **casual dress environment with minimal overtime** .
- Receive **professional development support** to expand your cybersecurity expertise.
- Collaborate with **software engineers, infrastructure specialists, business teams, and external security vendors** .
- Gain experience in **CSIRT operations, vulnerability assessments, penetration testing, and security incident response**.
- Take ownership of meaningful **security improvement projects and cybersecurity initiatives** .
- Develop expertise across **IT Security, Cloud Security, Cybersecurity Engineering, and Information Security Risk Management**.
- Build a long-term career in cybersecurity within Japan's evolving digital financial services industry.

Company Description

Morgan McKinleyは国際的な人材コンサルティング会社として、さまざまな業界・分野をリードする採用企業様と、スペシャリストとしてのスキルを有する人材とを結びつけるお手伝いをしています。1988年の創立以来、Morgan McKinleyの名は、「卓越した質のサービス」「市場知識の豊富さ」「No.1企業であり続けようとする強い意志」、そして何よりも「実績」を体現する会社として知られています。

リクルーティング スペシャリストである弊社コンサルタントまでお気軽にお問い合わせください。