【外資系金融テクノロジー】シニアIAMエンジニア｜クラウドセキュリティ

IAMの専門性を活かす金融テック。基本給1,400万円〜！

Job Information

Recruiter
Morgan McKinley

Job ID
1619166

Industry
Bank, Trust Bank

Job Type
Permanent Full-time

Location
Tokyo - 23 Wards

Salary
Negotiable, based on experience

Refreshed
October 26th, 2026 18:48

General Requirements

Minimum Experience Level
Over 6 years

Career Level
Mid Career

Minimum English Level
Fluent Level

Minimum Japanese Level
Fluent Level

Minimum Education Level
Bachelor's Degree

Visa Status
Permission to work in Japan required

Job Description

金融テクノロジーやデジタル資産分野でグローバルに事業を展開する企業で、ID管理・アクセス制御を担うシニアIAMエンジニアの募集です。

IAMの設計・実装からクラウドセキュリティ、自動化まで幅広く携わることができます。

IAMの専門性を活かして技術的な課題解決に取り組み、グローバルな環境でキャリアをさらに発展させたい方におすすめです。

基本給1,400万円〜（経験・スキルにより応相談）、フレックスタイム制あり。

主な職務内容

- **IAMソリューションの設計・運用：** シングルサインオン（SSO）、多要素認証（MFA）、ユーザー登録・権限付

与、アクセスガバナンスなどの仕組みを設計・管理する。
- **特権アクセス管理（PAM）：** 管理者アカウントや機密性の高いシステムへのアクセスを保護し、適切な権限管理を推進する。
- **クラウドセキュリティ：** AWSを中心に、各種クラウド環境におけるID管理とアクセス制御を強化する。
- **IAM業務の自動化：** スクリプトやInfrastructure as Code（IaC）を活用し、IAM運用の効率化とセキュリティ向上を図る。
- **セキュリティ統制・コンプライアンス：** 最小権限の原則に基づくアクセス管理、セキュリティポリシー、監査対応などの統制を強化する。
- **関連チームとの技術連携：** インフラ、エンジニアリング、サイバーセキュリティの各チームと協力し、複雑なIAMの技術課題を解決する。

Are you an experienced **Senior IAM Engineer or Identity and Access Management (IAM) Lead** looking to advance your career in cybersecurity within the financial technology industry?

Join a global financial technology company operating at the intersection of **investment banking, trading technology, and digital asset infrastructure**.

As a Senior IAM Engineer / IAM Lead, you will play a critical role in strengthening enterprise identity security, privileged access controls, cloud security, and identity governance across the organization.

You will design, implement, and manage **Identity and Access Management (IAM) solutions**, including **Single Sign-On (SSO), Multi-Factor Authentication (MFA), Privileged Access Management (PAM), and Identity Governance and Administration (IGA)**.

The role combines hands-on security engineering with technical leadership, automation, and cross-functional collaboration. You will work closely with cybersecurity, infrastructure, engineering, and global technology teams to improve security controls, reduce identity-related risks, and build scalable access management solutions.

You will also leverage **cloud technologies, scripting, and Infrastructure as Code (IaC)** to automate IAM processes and enhance operational efficiency.

Based in **Tokyo**, this is an excellent opportunity for an experienced cybersecurity professional with strong **Japanese and English communication skills** to contribute to a fast-growing international financial technology organization.

Key Responsibilities

- **Identity and Access Management (IAM) Engineering:** Design, implement, maintain, and optimize enterprise IAM solutions to ensure secure and efficient user authentication, authorization, and access management.
- **Single Sign-On (SSO) & Multi-Factor Authentication (MFA):** Develop and manage secure authentication solutions using technologies such as **Okta, Microsoft Entra ID, SailPoint**, and related identity platforms.
- **Identity Federation & Authentication Protocols:** Implement and support identity integration using **SAML, OAuth 2.0, and OpenID Connect (OIDC)**.
- **User Provisioning & Access Governance:** Manage identity lifecycle processes, user provisioning and deprovisioning, access permissions, and identity governance controls.
- **Privileged Access Management (PAM):** Implement and maintain PAM solutions to secure administrator accounts, sensitive systems, and privileged access.
- **Cloud Identity Security:** Manage and strengthen identity and access controls across **AWS and other cloud platforms**, including Azure and Google Cloud where applicable.
- **IAM Automation & Infrastructure as Code:** Automate identity management processes using **Python, PowerShell, Bash, Terraform**, and other scripting or infrastructure automation technologies.
- **Least-Privilege Access & Security Controls:** Implement and enforce access control policies based on least-privilege principles to reduce unauthorized access and security risks.
- **Security Compliance & Audit Support:** Strengthen IAM governance, maintain appropriate access controls, and support security audits and compliance requirements.
- **Technical Troubleshooting:** Investigate and resolve complex IAM, authentication, authorization, and privileged access issues.
- **Cross-Functional Security Collaboration:** Work with cybersecurity, infrastructure, cloud engineering, and application development teams to improve identity security across enterprise systems.
- **IAM Process Improvement:** Identify opportunities to enhance IAM architecture, automate repetitive tasks, strengthen controls, and improve overall security operations.
- **Technical Ownership:** Take ownership of IAM engineering initiatives and drive security improvements from design through implementation and ongoing operations.

Required Skills

必須条件経験・資格：

- IAMエンジニアリング領域で実務経験 5〜7年以上
- Okta、Microsoft Entra ID、SailPointなどのIAMプラットフォームに関する実務経験
- 企業向けIAMソリューションの設計・導入・運用経験
- SSO、MFA、SAML、OAuth 2.0、OIDCなどの認証技術に関する知識・経験
- 特権アクセス管理（PAM）、アクセス権限管理、最小権限の原則に基づくセキュリティ制御の実務経験
- AWS、Azure、GCPなどのクラウド環境に関する知識・経験、およびPython、PowerShell、Bashなどによるスクリプト作成やTerraformなどを用いた自動化の経験
- アクセスガバナンス、セキュリティ統制、監査要件、技術的なトラブルシューティングに関する知識・経験
- 大学卒業以上、または同等の学歴・資格

ソフトスキル：
- 関連チームや海外チームと円滑に連携できるコミュニケーション能力
- 複雑な技術課題を分析・解決し、セキュリティや業務プロセスの改善につなげる問題解決力
- 変化の速い環境でも自律的かつ柔軟に業務を進め、プロジェクトを主体的に推進する実行力

語学力：
- **日本語：**上級ビジネスレベル（読み書き・会話）
- **英語：**上級ビジネスレベル（読み書き・会話）

歓迎条件
- 金融、フィンテックなど、規制要件の厳しい業界におけるセキュリティ・IAM関連業務の経験
- グローバル企業や複数の海外拠点と連携し、IAM基盤やセキュリティ統制の導入・改善を推進した経験

採用企業について
外資系フィンテック。

伝統的な金融サービスと新興デジタル市場の接点で事業を展開するグローバル企業です。

革新的な投資ソリューションやトレーディング技術、デジタル資産インフラに取り組み、国際的な環境で金融サービスの発展を支えています。

この求人がおすすめの理由
- シニアIAMエンジニアとして、ID管理・アクセス制御に関する重要なプロジェクトを主体的に推進できる
- IAMの設計・実装からクラウドセキュリティ、自動化まで、幅広い技術領域で専門性を発揮できる
- 最先端の金融テクノロジーやデジタル資産関連の技術に携われる
- グローバルなチームと協働し、国際的な環境で経験を積める
- フレックスタイム制があり、柔軟な働き方が可能
- 基本給1,400万円〜（経験・スキルにより応相談）

Required Skills and Qualifications **Experience:**
- **5-7+ years of hands-on experience in Identity and Access Management (IAM) engineering** , including the design, implementation, and management of enterprise IAM solutions.
- **5-7+ years of practical experience with IAM platforms** such as **Okta, Microsoft Entra ID, SailPoint**, or comparable enterprise identity management technologies.
- Strong technical knowledge of **Single Sign-On (SSO), Multi-Factor Authentication (MFA), SAML, OAuth 2.0, and OpenID Connect (OIDC)**.
- Hands-on experience implementing and managing **Privileged Access Management (PAM)** solutions, including privileged account protection, access permissions, and least-privilege controls.
- Experience with **cloud identity and access security**, particularly **AWS**, with exposure to Azure or Google Cloud also relevant.
- Practical scripting and automation experience using **Python, PowerShell, or Bash** .
- Experience using **Infrastructure as Code (IaC)** or automation tools such as **Terraform** to improve IAM security and operational efficiency.
- Strong understanding of **identity governance, security controls, access management policies, audit requirements, and IAM troubleshooting**.
- Experience working with complex enterprise infrastructure and collaborating with cybersecurity and engineering teams.
- **Must currently be based in Japan** .
- Bachelor's degree or equivalent educational qualification.

Soft Skills:
- **Excellent communication and stakeholder management skills**, with the ability to collaborate effectively with cybersecurity, infrastructure, engineering, and international technology teams.
- Strong analytical thinking and problem-solving abilities, particularly when troubleshooting complex identity and access security issues.
- **Proactive and security-focused mindset**, with the ability to identify vulnerabilities, improve controls, and recommend practical solutions.
- Strong sense of ownership and accountability for IAM engineering projects, operational reliability, and security improvements.
- Ability to work independently while contributing effectively to cross-functional security initiatives.
- Adaptability and resilience in a fast-paced, technology-driven international environment.
- Strong organizational skills and the ability to prioritize multiple technical projects and security requirements.
- Commitment to continuous improvement, automation, and maintaining high cybersecurity standards.

Language Requirements:
- **Japanese: Fluent level** - required for communication with Japan-based technology teams, internal stakeholders, and security-related business functions.
- **English: Fluent level** - essential for collaboration with global engineering teams, international cybersecurity stakeholders, and cross-border technical projects.
- **Fluent written and verbal communication skills in both Japanese and English are mandatory.**

Preferred Skills & Qualifications
- **6+ years of experience** in cybersecurity, IAM engineering, identity security, or enterprise access management.
- Previous experience as a **Senior IAM Engineer, IAM Lead, Identity Security Engineer, PAM Engineer, or Cybersecurity Engineer**.
- Professional experience within **investment banking, financial services, fintech, trading technology, or another highly regulated industry**.
- Advanced expertise in **Okta, Microsoft Entra ID, SailPoint**, or other enterprise IAM and identity governance platforms.
- Experience designing or improving enterprise-wide **Privileged Access Management (PAM)** frameworks.
- Strong understanding of **AWS IAM**, cloud identity security architecture, and access governance across hybrid or multi-cloud environments.
- Experience automating security workflows using **Terraform, Python, PowerShell, or Bash** .

- Familiarity with **Identity Governance and Administration (IGA)**, access certification, identity lifecycle management, and compliance-related access controls.
- Experience supporting security audits, regulatory requirements, and identity-related risk management in complex organizations.
- Track record of improving IAM architecture, authentication security, privileged access controls, or identity automation.
- Experience collaborating with global cybersecurity teams and supporting security initiatives across multiple regions.

About the Company
Our client is a **global financial technology company** operating at the intersection of traditional financial services and emerging digital markets.

The organization focuses on innovative **investment solutions, trading technology, and digital asset infrastructure**, combining financial expertise with advanced technology to support its international business operations.

Operating in a rapidly evolving financial technology environment, the company emphasizes secure, scalable, and resilient technology infrastructure.

With a global workforce and an international business model, the organization provides opportunities for technology and cybersecurity professionals to work on complex security challenges involving financial systems, cloud environments, and enterprise identity management.

Joining this company offers the opportunity to strengthen critical security capabilities while contributing to the continued development of sophisticated financial technology solutions.

Why You'll Love Working Here
- **Highly Competitive Compensation:** Annual salary of **¥14M-¥17M**, reflecting the technical expertise and responsibility required for this senior IAM position.
- **Cutting-Edge Cybersecurity Technology:** Work with **enterprise IAM platforms, cloud identity security, PAM solutions, and automation technologies**.
- **Senior-Level Technical Ownership:** Take responsibility for important identity security initiatives and contribute directly to enterprise cybersecurity improvements.
- **Global Financial Technology Environment:** Gain exposure to **investment banking technology, trading platforms, and digital asset infrastructure**.
- **International Collaboration:** Work closely with cybersecurity, infrastructure, and engineering teams across global markets.
- **Advanced IAM Engineering Opportunities:** Strengthen your expertise in **SSO, MFA, IAM, PAM, IGA, cloud security, and identity automation**.
- **Challenging Technical Projects:** Solve complex identity and access security problems while improving authentication, access governance, and operational resilience.
- **Automation & Innovation:** Apply scripting and Infrastructure as Code to improve security processes and develop scalable IAM solutions.
- **Career Growth in Cybersecurity:** Build your technical leadership capabilities within a fast-growing international financial technology company.
- **Flexible Working Culture:** Benefit from workplace arrangements that may include **flexible working hours and limited overtime**, depending on business and operational requirements.

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。