Chief Information Security Officer (CISO) / 最高情報セキュリティ責任者

国際的な環境です。服装自由。住宅手当あり。

Job Information

Hiring Company
Okinawa Institute of Science and Technology Graduate University

Subsidiary
沖縄科学技術大学院大学（OIST）

Job ID
1553551

Industry
Other (Education)

Company Type
Large Company (more than 300 employees)

Non-Japanese Ratio
Majority Non-Japanese

Job Type
Contract

Location
Okinawa Prefecture

Salary
Negotiable, based on experience

Work Hours
09:00~17:30（管理監督者につき、勤務日・勤務時間・休憩時間について一般従業員の所定労働時間等の適用はありません。）

Holidays
年次有給休暇、夏季休暇

Refreshed
February 5th, 2026 04:00

General Requirements

Minimum Experience Level
Over 10 years

Career Level
Executive

Minimum English Level
Fluent (Amount Used: English usage about 75%)

Minimum Japanese Level
Fluent

Minimum Education Level
Bachelor's Degree

Visa Status
Permission to work in Japan required

Job Description

1. Cybersecurity Strategy & Leadership

- Partner with the CIO and executive leadership to develop and execute an information security strategy, embedding cybersecurity into institutional planning and governance.
- Define and track performance metrics (KPIs, SLAs, SLOs) to measure effectiveness and maturity.
- Lead maturity assessments and benchmark against global best practices.
- Lead and develop the information security team, fostering a high-performance and inclusive culture.

2. Governance, Compliance & Risk

- Establish and maintain security policies and standards aligned with institutional and regulatory requirements (e.g., NIST, ISO 27001, Japanese frameworks).
- Oversee compliance across vendors, research partners, and IT contracts (IaaS, PaaS, SaaS, SWAS).
- Collaborate with the Risk Manager and institutional committees to align cybersecurity with enterprise risk management.

3. Security Operations

- Oversee daily security operations and ensure protection of IT assets and data.
- Lead incident response, containment, and remediation efforts, reporting outcomes to the CIO and relevant committees.
- Implement monitoring systems and track threat detection KPIs.
- Guide secure architecture design and adoption of advanced technologies (e.g., IAM, DLP, encryption).
- Strengthen identity governance through RBAC, PAM, and MFA.

---

1. サイバーセキュリティ戦略とリーダーシップ

- CIOおよび経営陣と連携し、情報セキュリティ戦略の策定と実行を主導し、サイバーセキュリティを機関全体の計画およびガバナンスに組み込む。
- 戦略の有効性と成熟度を測定するためのパフォーマンス指標（KPI、SLA、SLO）を定義、追跡する。
- 成熟度評価を主導し、グローバルなベストプラクティスとの比較を行う。
- 情報セキュリティチームの育成と指導を行い、高いパフォーマンスと多様性を重視した職場文化の醸成に努める。

2. ガバナンス、コンプライアンス、リスク

- 機関および規制要件（NIST、ISO 27001、日本のフレームワークなど）に準拠したセキュリティポリシーおよび基準の策定と維持。
- ベンダー、研究パートナー、IT契約（IaaS、PaaS、SaaS、SWAS）におけるコンプライアンスの監督。
- リスクマネージャーおよび機関内委員会と連携し、サイバーセキュリティと機関全体のリスク管理との整合性を確保する。

3. セキュリティ運用

- 日々のセキュリティ運用を監督し、IT資産およびデータの保護を確実にする。
- インシデント対応、封じ込め、復旧をリードし、その結果をCIOおよび関係委員会に報告する。
- 脅威検知に関するKPIを追跡するためのモニタリングシステムを導入。
- セキュアなアーキテクチャ設計を指導し、IAM（アイデンティティ・アクセス管理）、DLP（データ損失防止）、暗号化など先進技術の採用を推進。
- RBAC（ロールベースアクセス制御）、PAM（特権アクセス管理）、MFA（多要素認証）を活用し、アイデンティティ・ガバナンスの強化を図る。

Required Skills

(Required)

1. Bachelor’s degree in Computer Science, Information Security, IT, or a related field.
2. 10+ years of progressive leadership in information security, IT risk management, or related domains.
3. 3+ years in a senior role—ideally as CISO or equivalent—with strategic oversight of enterprise security programs.
4. Demonstrated success in leading institution-wide security initiatives, including governance, risk, compliance, and incident response.
5. Experience in complex, regulated environments such as higher education, research institutions, non-profits, international organizations, or industries like finance, healthcare, and technology.
6. CISSP (Certified Information Systems Security Professional) or Chartered Cyber Security Professional.
7. Deep knowledge of industry frameworks (ISO 27001, NIST CSF, CIS Controls), Japanese data protection laws (APPI), and global compliance standards (GDPR, HIPAA).
8. Strong grasp of enterprise risk management, security architecture, and incident response planning.
9. Familiarity with academic environments, research data protection, and open-access systems.
10. Skilled in solving complex security challenges with a forward-looking, data-informed approach.
11. Excellent communicator in English; Japanese proficiency highly desirable for stakeholder engagement and regulatory alignment.

(Preferred)

1. Master’s or Ph.D. in Cybersecurity, Information Assurance, Business Administration, or a closely related discipline.
2. CISM (Certified Information Security Manager)
3. CISA (Certified Information Systems Auditor)
4. CCSP (Certified Cloud Security Professional)

5. CRISC, CEH, ISO 27001 Lead Implementer/Auditor

（必須）

1. コンピュータサイエンス、情報セキュリティ、ITまたは関連分野の学士号を有する。
2. 情報セキュリティ、ITリスク管理、または関連分野において10年以上の継続的かつ発展的なリーダーシップ経験を有する。
3. CISOまたは同等の役職での3年以上の職務経験があり、企業全体のセキュリティプログラムを戦略的に統括した実績を有する。
4. ガバナンス、リスク、コンプライアンス、インシデント対応などを含む、機関全体にわたるセキュリティ施策の主導に成功した経験を有する。
5. 高等教育機関、研究機関、非営利団体、国際機関、または金融・医療・テクノロジーなどの複雑かつ規制の厳しい業界での業務経験を有する。
6. CISSPまたはChartered Cyber Security Professionalの資格を保有する。
7. 業界標準のフレームワーク（ISO 27001、NIST CSF、CIS Controls）、日本の個人情報保護法（APPI）、および国際的なコンプライアンス基準（GDPR、HIPAA）に関する深い知識を有する。
8. 企業リスク管理、セキュリティアーキテクチャ、インシデント対応計画に関する強い理解を有する。
9. 学術機関の環境、研究データの保護、オープンアクセスシステムに関する知識や理解を有する。
10. 将来を見据えたデータ主導のアプローチで、複雑なセキュリティ課題を解決する優れた能力。
11. 英語での優れたコミュニケーション能力を有しており、ステークホルダーとの連携や規制対応のため、優れた日本語力を有する。

（尚可）

1. サイバーセキュリティ、情報保証、経営学、または関連分野の修士号または博士号を有する。
2. CISM (公認情報セキュリティマネージャー)
3. CISA (公認情報システム監査人)
4. CCSP (Certified Cloud Security Professional)
5. CRISC, CEH, ISO 27001 Lead Implementer/Auditor

Company Description