<table>
<thead>
<tr>
<th>Job Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subject No.</td>
</tr>
<tr>
<td>Job Title</td>
</tr>
<tr>
<td>Department</td>
</tr>
<tr>
<td>Work Contents (Research theme)</td>
</tr>
</tbody>
</table>

**Detail of Work Contents**

- In the face of rapidly evolving and increasingly sophisticated cyber threats that pose a growing risk to society, our research focuses on the development of the following cybersecurity technologies to protect critical social systems and support societal maintenance and growth:
  - Technology for the timely detection, visualization, and analysis of various cyber attacks to stay ahead of the latest cyber threat trends and facilitate effective responses.
  - Techniques for observing, aggregating, and analyzing a wide range of cybersecurity-related information, leveraging AI and other technologies to enhance effective countermeasures and strengthen organizational cybersecurity.
  - Security verification techniques for new network environments, such as those associated with emerging technologies like Connected Cars and IoT devices.
  - Efforts aimed at information fusion with CURE, including DRDoS alerts within CYNEX, and activities related to external information sharing and collaboration.

Please note that this translation is a general interpretation of the provided text, and the specific terminology used may vary depending on the context and target audience.

The Article 15(2) of the Act on the activation of Science, Technology and Innovation will be applied to this work content.

Employees to be hired through this recruitment may apply for external competitive research fundings such as Grant-in-Aid for Scientific Research (KAKENHI) and NICT’s internal research fundings.

**Application requirement**

1. It is preferable that the applicant satisfies at least one of the following two conditions:
   - Research experience and accepted journal papers in cybersecurity area.
   - Practical experience in such as aggregating and analyzing cyber threat intelligence or analyzing malware.
2. Enough knowledge of advanced technology for cybersecurity, especially cyber threat intelligence.
3. Doctoral degree or equivalent experiences in the following research areas: cybersecurity, information retrieval and data mining.
4. Detailed research proposal on future research plan and the contribution to the cyber security R&D activities in NICT is required upon application (any format is acceptable).

**Recruiting (Number of people)**

1

**Contract period**

Hiring date ~ March 31, 2025

N.B. Contract could be renewed.

**The employment period in case of fully renewing**

Up to 5 years if certain conditions are fulfilled

**Salary**

Basic salary shall be determined by taking into account each employee’s experience and task to be engaged in. However, as a basic salary is compliant with government employees’ wages, it shall be changed when a basic salary is changed after labor union and the like of NICT agreed under a revision to the government employees’ wages.

**Work Place**

Headquarters, or Cybersecurity Recurrent Evolution Center (Koganei-shi, Tokyo or Musashino-shi, Tokyo)

**Working frequency**

5 days/week (7.5 hours/day)