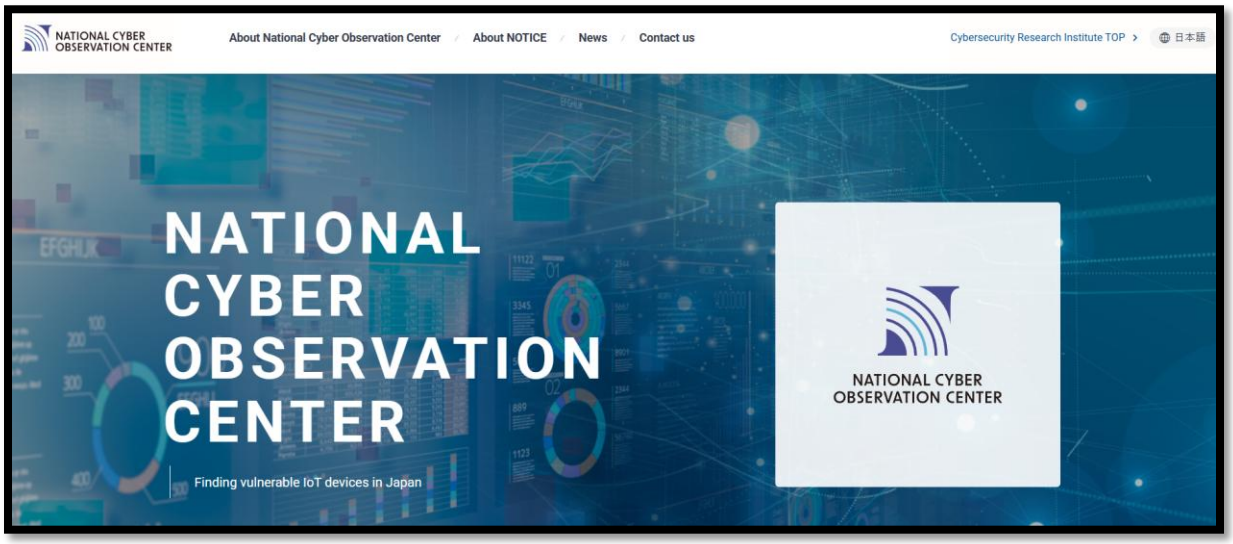
Japan: Cyber Research

Table of Contents

Portal 1: National Institute of Information and Communications Technology (NICT) – Cybersecurity Nexus & National Cyber Observation Centre (https://nco.nict.go.jp/en)

Purpose:



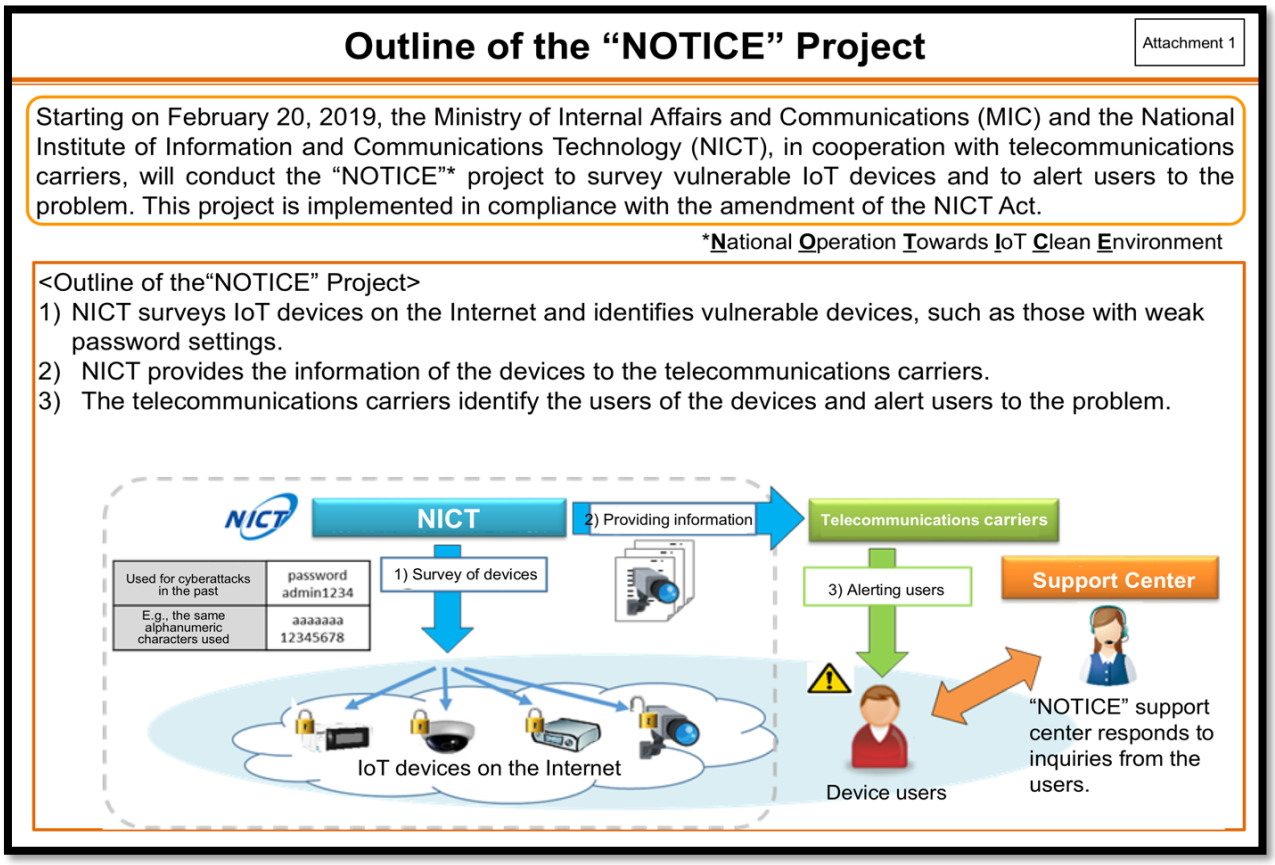
1. The National Cyber Observation Centre (NCO), operated by the National Institute of Information and Communications Technology (NICT), functions as Japan's central framework for monitoring and securing Internet of Things (IoT) devices. It identifies devices vulnerable to weak authentication and other exploitable configurations, aiming to mitigate their misuse in cyberattacks.

2. NCO leads the NOTICE initiative (National Operation Towards IoT Clean Environment) in collaboration with the Ministry of Internal Affairs and Communications (MIC) and various Internet Service Providers (ISPs). The project's core objective is to detect, notify, and remediate insecure IoT devices across Japan.

3. The centre also contributes to Japan's national cybersecurity resilience by collecting and analysing large-scale threat intelligence, which supports both strategic policymaking and operational defines.

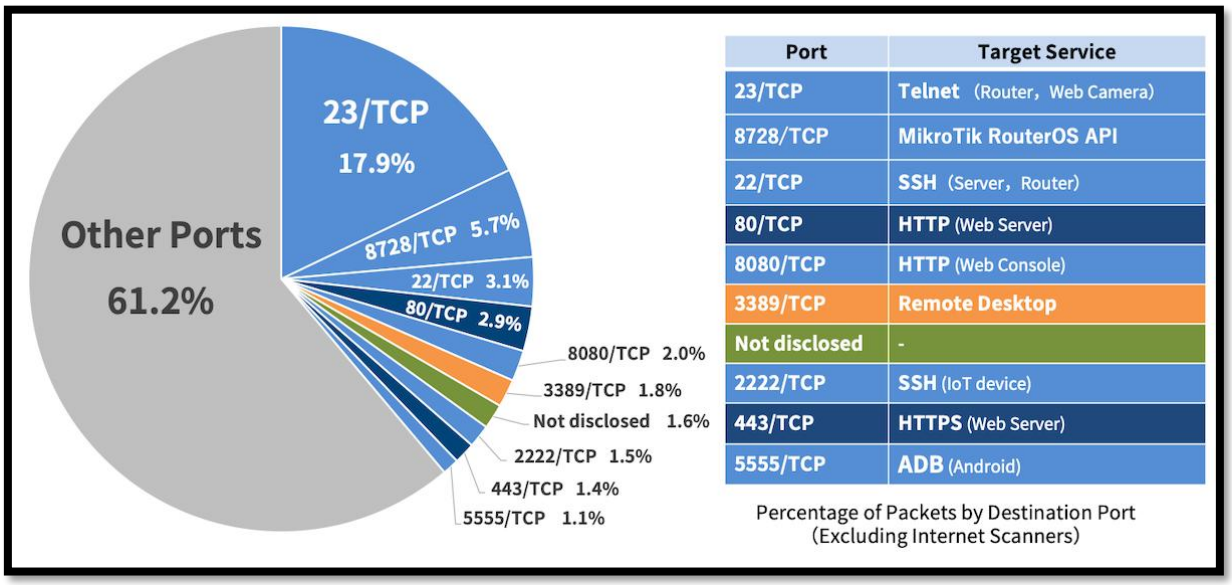
Features:

1. **Internet-wide IoT Device Scanning and Vulnerability Detection**



NCO conducts systematic scans across Japan's IPv4 address space to identify IoT devices that permit access via weak or default credentials. Detected vulnerabilities are reported to corresponding ISPs, who in turn **notify end users** to implement security updates, change passwords, or disable insecure services. This large-scale scanning mechanism forms the backbone of the **NOTICE program**, enhancing the overall hygiene of Japan's IoT ecosystem.

2. Data Collection and Cyber-Attack Trend Analysis



Port	Target Service
23/TCP	**Telnet** (Router, Web Camera)
8728/TCP	**MikroTik RouterOS API**
22/TCP	**SSH** (Server, Router)
80/TCP	**HTTP** (Web Server)
8080/TCP	**HTTP** (Web Console)
3389/TCP	**Remote Desktop**
Not disclosed	-
2222/TCP	**SSH** (IoT device)
443/TCP	**HTTPS** (Web Server)
5555/TCP	**ADB** (Android)

Percentage of Packets by Destination Port
(Excluding Internet Scanners)

The NCO's infrastructure integrates with NICT's **NICTER (Network Incident analysis Centre for Tactical Emergency Response)** platform to aggregate data from honeypot networks and darknet sensors. These datasets are utilized to analyse patterns of cyberattacks targeting IoT devices, including **frequency, geographic origin, and vector characteristics**. Insights derived from these analyses are instrumental in shaping Japan's proactive cybersecurity strategies and defence capabilities.

3. Collaboration through the Cybersecurity Nexus (CYNEX) Platform

CYNEX
CYBERSECURITY NEXUS

As part of the broader **Cybersecurity Research Institute**, the NCO operates within the CYNEX framework, fostering **industry-academia-government collaboration**. This platform enables the sharing of cybersecurity infrastructure, joint research, and talent development initiatives. Through CYNEX, NICT promotes knowledge exchange and capacity-building, ensuring that innovations and countermeasures are effectively implemented across sectors.

4. **Support for Domestic Cybersecurity Technology Development**

NCO supports the evaluation and deployment of domestically developed security technologies. By facilitating testing in real operational environments, NICT encourages the **commercial adoption of Japanese cybersecurity solutions**, reducing dependence on foreign technologies. This initiative aligns with Japan's long-term goal of achieving technological sovereignty in the cybersecurity domain.

Chatbot: No

Additional Pointers:

- The NCO's approach represents a **nationwide cyber-hygiene model**, where vulnerabilities are detected centrally but remediated locally through coordinated communication between ISPs and users.

- While primarily designed for research and national security applications, the outcomes of NCO's activities indirectly enhance **consumer safety** and **IoT ecosystem reliability** by minimizing the risk of device exploitation.

- The NCO's data and analytical reports provide valuable empirical evidence for research in **cyber threat intelligence, IoT vulnerability assessment, and national cyber policy development**.