Outline of the “NOTICE” Project

- Starting on February 2019, the Ministry of Internal Affairs and Communications (MIC) and the National Institute of Information and Communications Technology (NICT), in cooperation with Internet Service Providers (ISPs), have been carrying out the “**NOTICE**”* project to **survey vulnerable IoT devices**, and to **alert users** to any problems found. This project has been implemented in compliance with the amendment of the NICT Act.

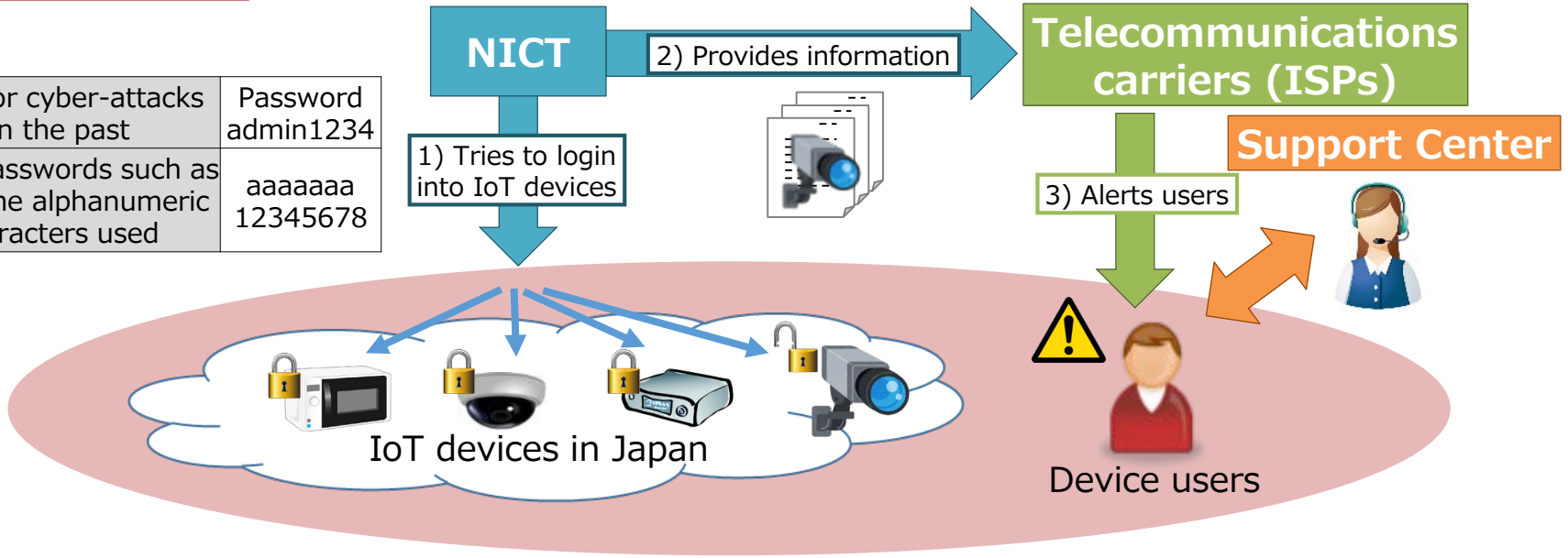
*National Operation Towards IoT Clean Environment

Overview of the “NOTICE” Project

Target
IoT devices which may have vulnerability and be used for cyberattacks

1) **NICT** surveys IoT devices on the Internet and **identifies vulnerable devices**, which are those with weak ID/password settings.
2) **NICT provides information** about the identified vulnerable devices to **ISPs**.
3) The **ISPs identify the users** of the devices **and alert them**.

Used for cyber-attacks in the past	Password admin1234
Weak passwords such as the same alphanumeric characters used	aaaaaaa 12345678



Outline of the NICTER-Alert Project

- Along with NOTICE, MIC and the NICT, in cooperation with ISPs, have been carrying out a project from June 2019 to **identify devices infected with malware** by using **NICTER***, and to notify the ISPs so that they can **alert users** of the infected devices.

*As the NICTER project, NICT conducts a large-scale cyberattack observation by the darknet and various types of honeypot and an analysis of causes of cyberattacks (i.e., malware), using a cyberattack observation, analysis, and countermeasure system which aims at quick response to large-scale attacks on the Internet.

Overview of the NICTER-Alert Project*

*** Project to alert users of IoT devices infected with malware**

Target
IoT devices that are already infected with malware such as "Mirai"

1) **NICT identifies devices that are generating malware-infected traffic** by using NICTER.
2) **NICT provides information** about the malware-infected devices to **ISPs**.
3) The **ISPs identify the users** of the devices **and alert them**.