Progress on the Projects (FY2019)

- ➢ By **March 2020, 50 ISPs** have participated in the projects.
- ➢ Surveys on about **110 million IP addresses** of the ISPs were conducted.
- ➢ **NOTICE**: In FY2019, **total 2,249** devices were detected and ISPs have been notified.
- ➢ **NICTER**: In FY2019, **avg. 162/day** devices were detected and ISPs have been notified.

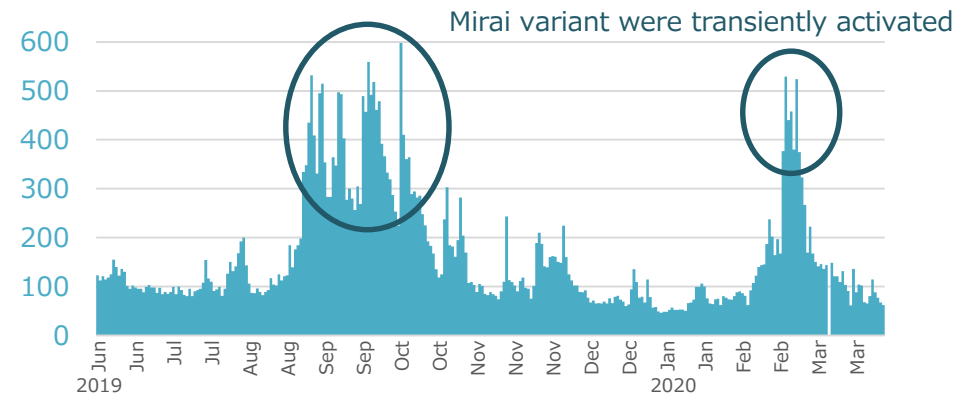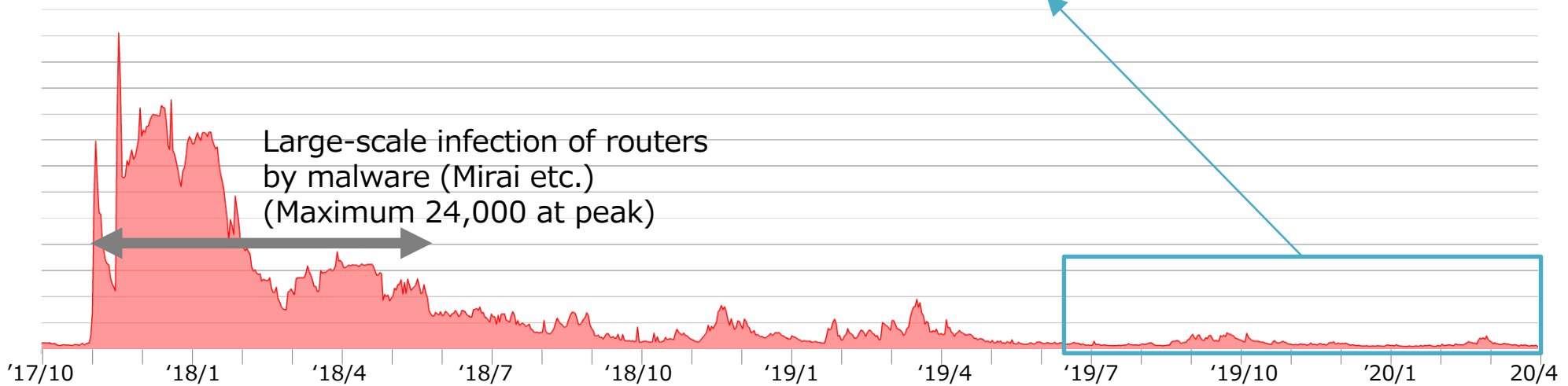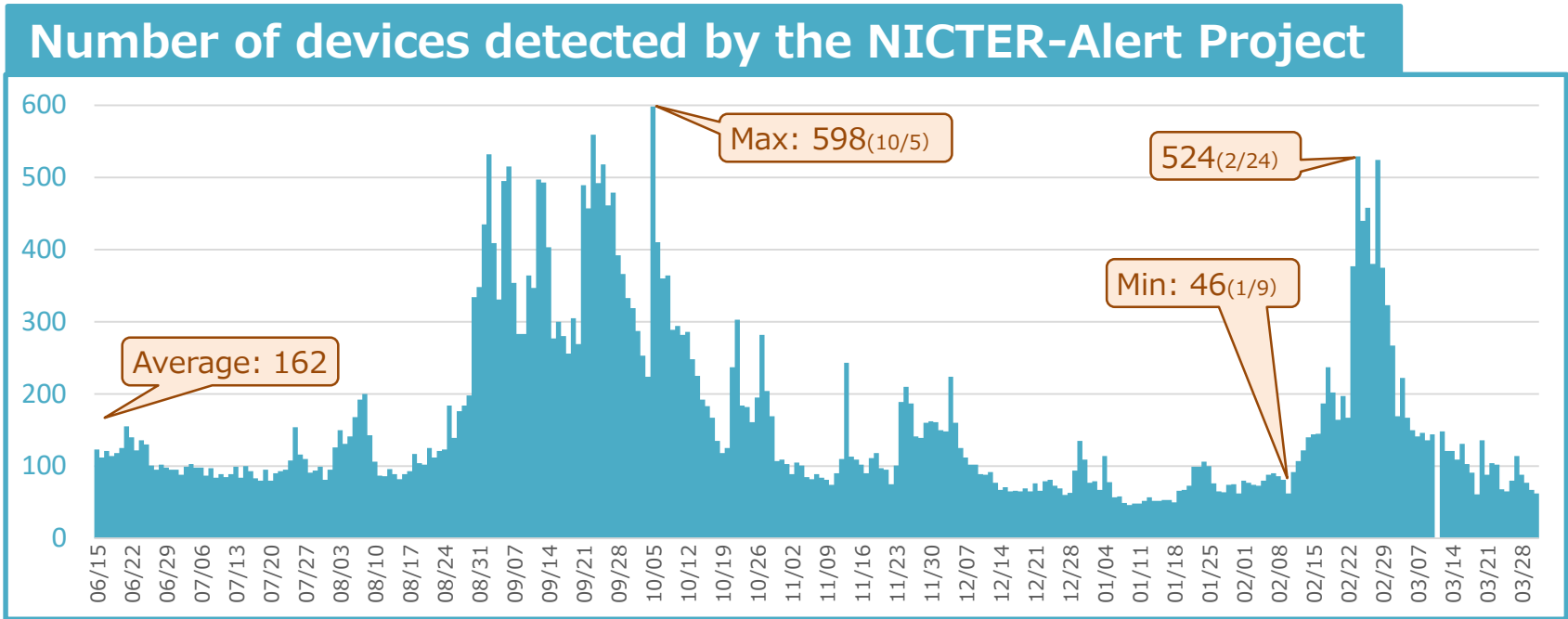| Results of the **"NOTICE"** Project	Results of the **NICTER**-Alert Project* * **Project to alert users of IoT devices infected with malware**
Number of IP addresses in which **ID and password could be entered** ➡ Approx. 100,000 (Recent survey) Out of the above, the number of those which were **successfully logged-in to** with **weak password settings** and were **subject to user alert** ➡ Total 2,249	Number of IP addresses which seem to be **infected with malware** and were **subject to user alert** ➡ Average 162 (per day)

Increasing factors: Enhancement of survey programs and expansion of survey target addresses

Decreasing factor: User takes measures in response to alert by ISP

Bar chart values: Apr 2019: 38, May: 54, Jun: 55, Jul: 55, Aug: 82, Sep: 221, Oct: 282, Nov: 275, Dec: 266, Jan 2020: 304, Feb: 307, Mar: 310

Mirai variant were transiently activated

Detection status of IoT devices infected with malware

Number of devices detected by the NICTER-Alert Project

Max: 598 (10/5)

524 (2/24)

Min: 46 (1/9)

Average: 162

Large-scale infection of routers by malware (Mirai etc.)
(Maximum 24,000 at peak)

Long-term observation trends in the NICTER project (2017/10/1 or later)