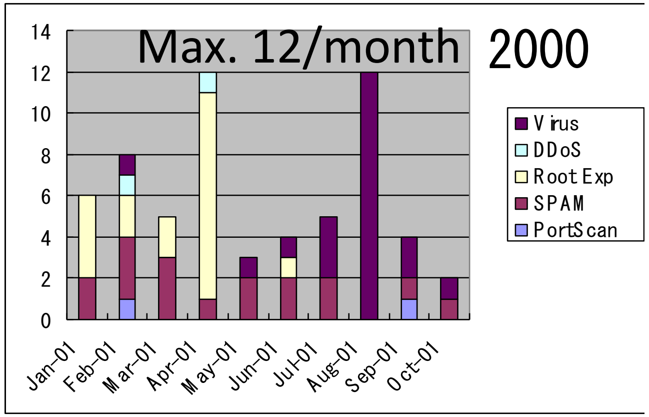
Current Status and Future Directions of KEK Computer Security

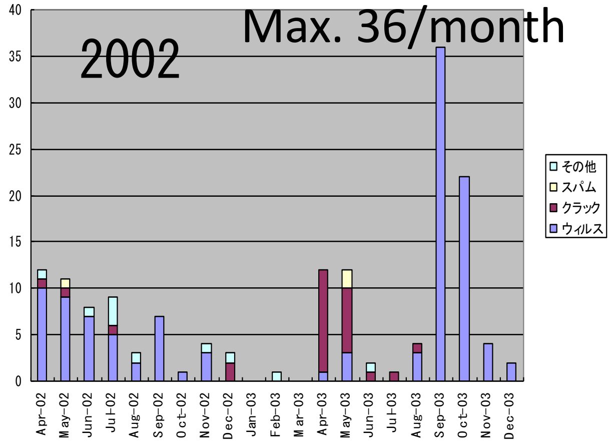
Fukuko YUASA

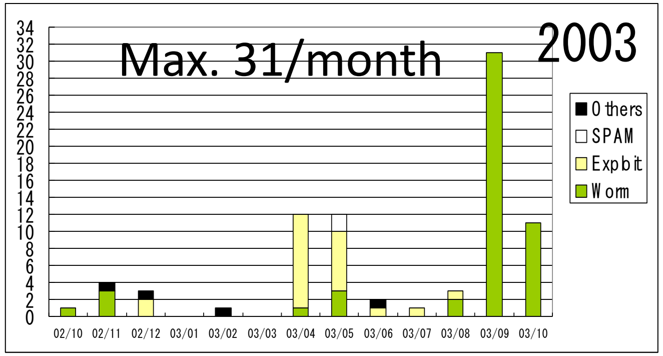
On behalf of security group

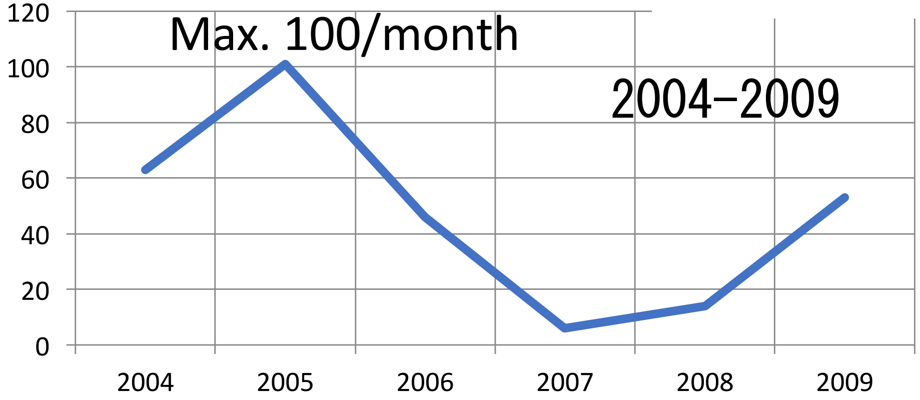
of KEK Computing Research Center

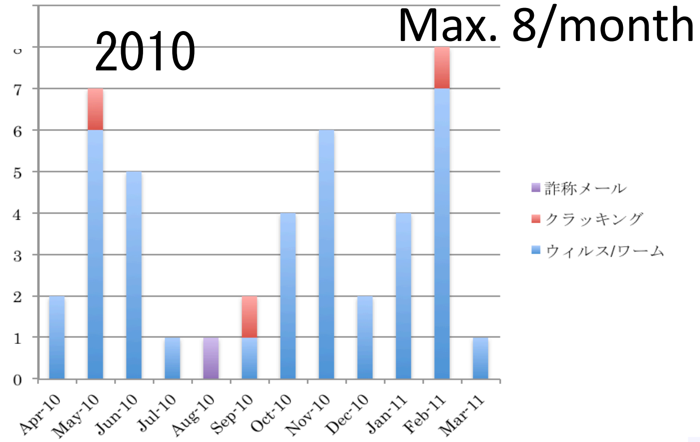
Incidents at KEK year by year

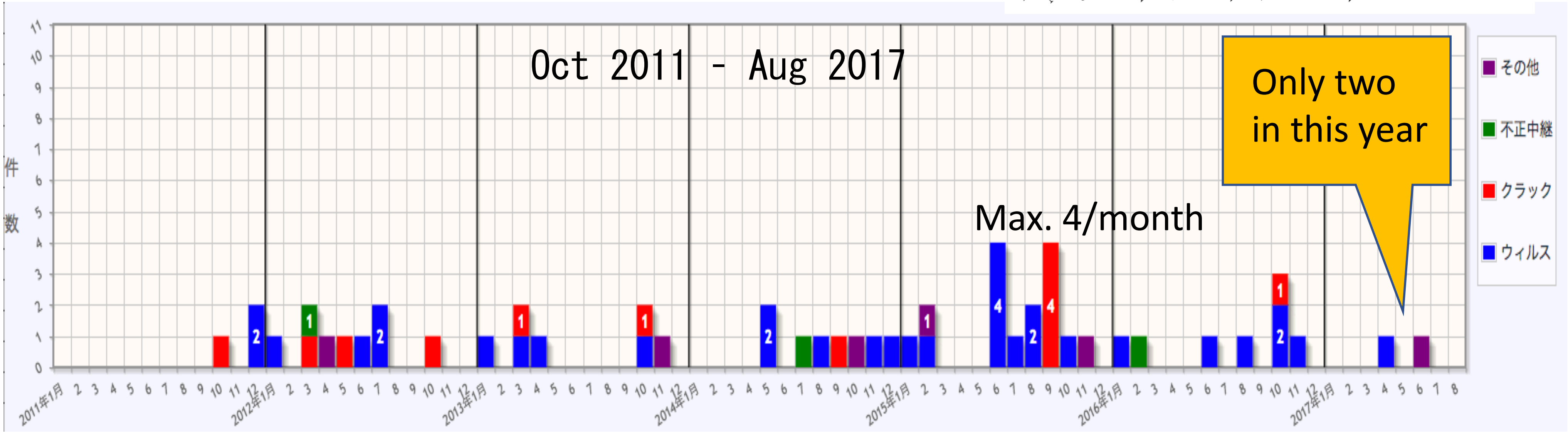












Only two in this year

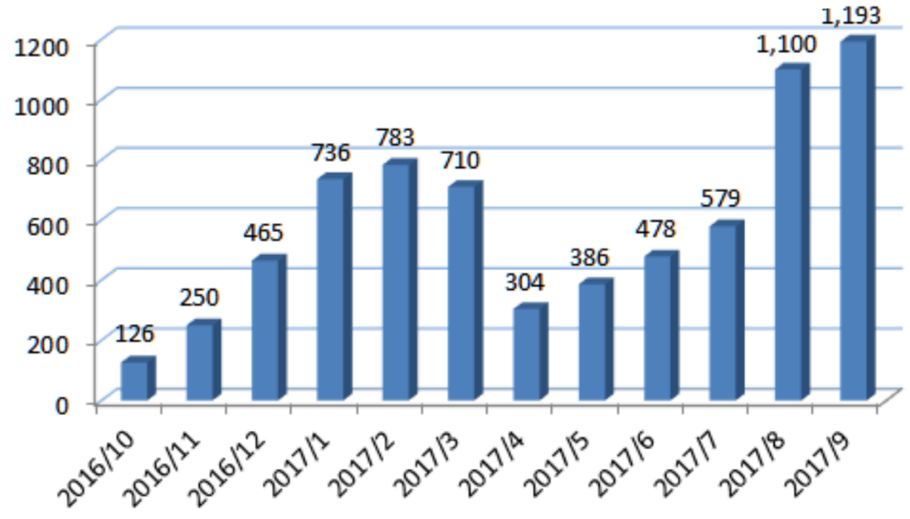
The number of incidents found at KEK is decreasing.
But is it the silence before a storm?

Growing targeted-mail attack in Japan

- Academia becomes a target
  - Jan 2017: Notice mail about carried over grant funding from JSPS with malicious zip file to researchers

  (JSPS : Japan Society for the Promotion of Science)
- KEK users are targeted
  - Password reset scam mails from someone masquerading KEK's mail administrator
  - Suspicious mails from famous companies as Apple, Amazon, NTT-X (Japanese online shop), credit-card company, ...

Number of reports on phishing mails to Council of Anti-Phishing Japan

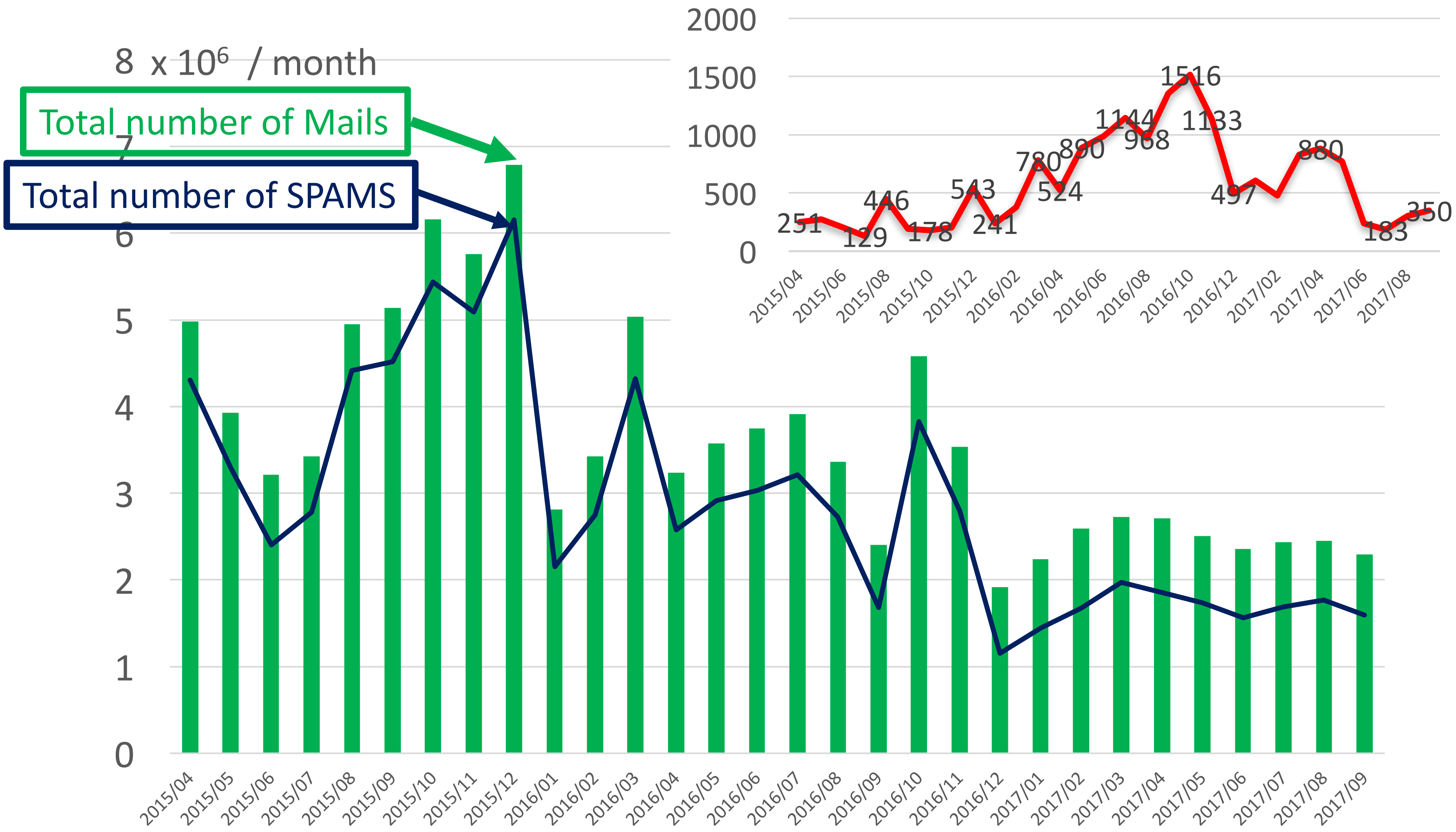


https://www.antiphishing.jp/report/monthly/201709.html

It is difficult to protect against such attacks by a mail security appliance and endpoint anti-virus software.

Monthly mail traffic
Since Apr. 2014 to Sep. 2017

Virus detected in KEK Mail system per month



The situation surrounding us has changed.

- Japanese Government enacted a law on cybersecurity in 2014.

The Basic Act on Cybersecurity
Law Number: Act No. 104 of 2014

(Responsibility of Educational and Research Organizations)

Article 8　In accordance with the basic principles, universities and other educational and research organizations are to make an effort to ensure Cybersecurity voluntarily and proactively, develop human resources specialized for Cybersecurity, disseminate research and the results of research on Cybersecurity, and cooperate with measures taken by the national government or local governments.

(http://www.japaneselawtranslation.go.jp)

in Japanese

（教育研究機関の責務）

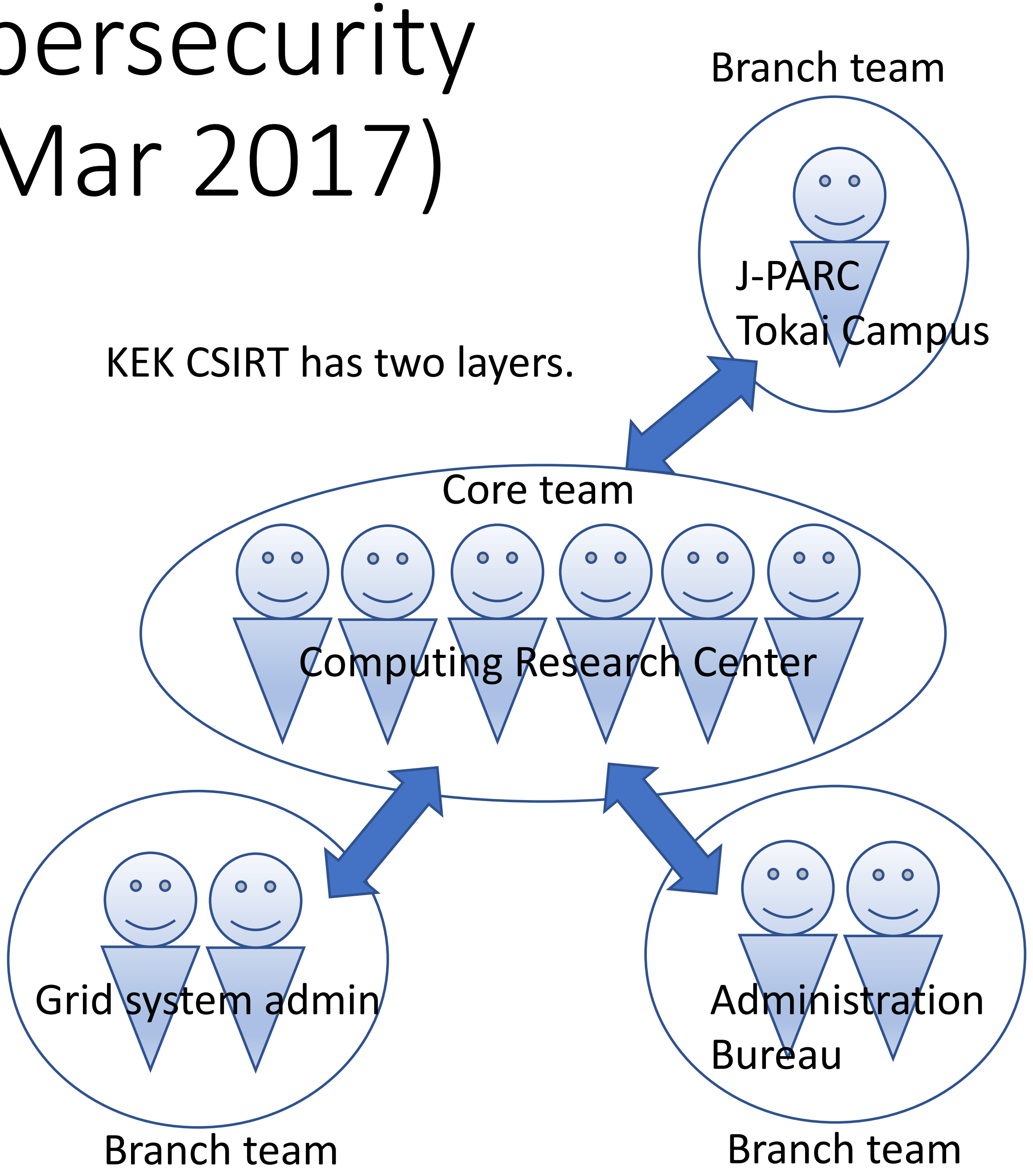
第八条　大学その他の教育研究機関は、基本理念にのっとり、自主的かつ積極的にサイバーセキュリティの確保、サイバーセキュリティに係る人材の育成並びにサイバーセキュリティに関する研究及びその成果の普及に努めるとともに、国又は地方公共団体が実施するサイバーセキュリティに関する施策に協力するよう努めるものとする。

Concerns

- KEK does not want severe security incidents which should be reported to MEXT (Ministry of Education, Culture, Sports, Science and Technology).
- KEK fears “Damage to reputation”.

Basic plan on cybersecurity practices (since Mar 2017)

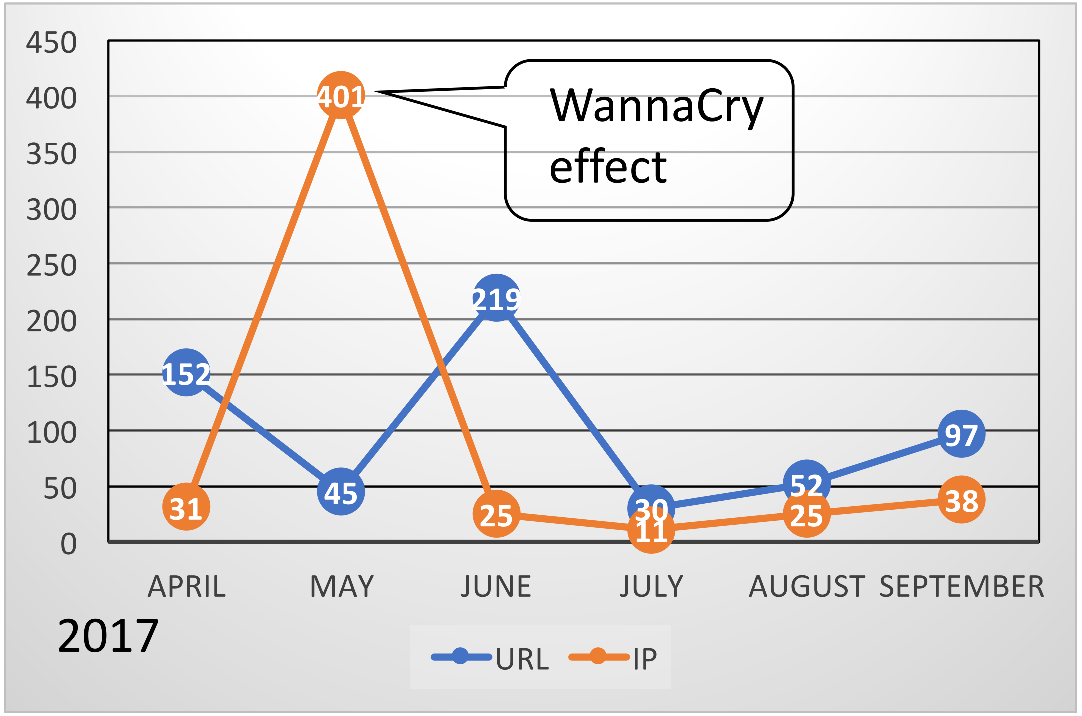
- A new regime for information security started since April 2017 to carry out the plan.
  - Core KEK CISRT becomes a part of Computing Research Center to focus its efforts on the technical things
    - Incident handling
    - Prevention
    - Monitoring and logging



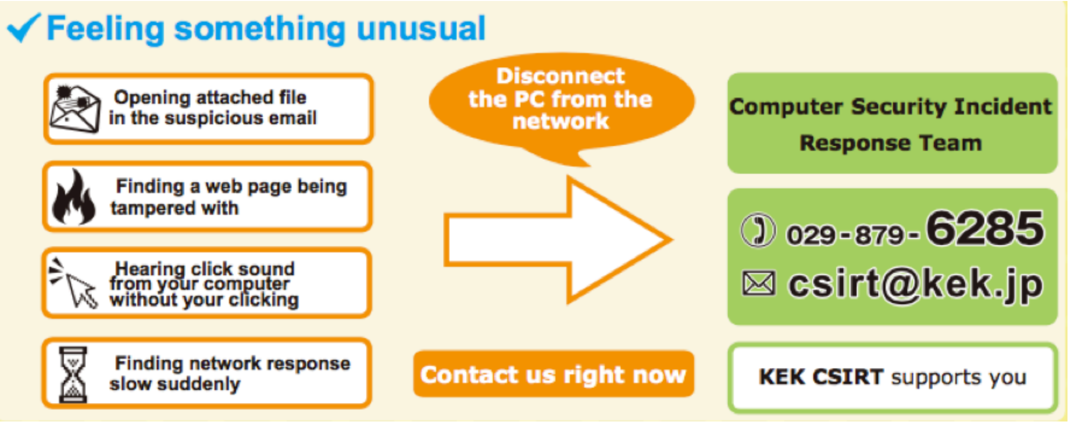
Prevention

- FW blocking of malicious URLs and IP addresses by CSIRT
    - information from JPCERT/CC, IPA, Police, NII-SOCS, MEXT and so on.
- Awareness of mail attacks
    - a Web notification system in an administrative division has been working. About 1 notification per 2 days.
- Education through regular security course (face to face) by CSIRT member

Number of manual blockings since 2017 April



WannaCry effect



✓ Feeling something unusual

Opening attached file in the suspicious email

Finding a web page being tampered with

Hearing click sound from your computer without your clicking

Finding network response slow suddenly

Disconnect the PC from the network

Contact us right now

Computer Security Incident Response Team

☎ 029-879-6285

✉ csirt@kek.jp

KEK CSIRT supports you

Extract from security leaflet “KEK computer security 11 Best Practices” issued in 2017 for foreign researcher

Alert from FW on eduroam network

WildFire Analysis Report

File Name: fetch.php
Uploaded by: XXXXX (S/N 001801008003) at 2017-10-16 09:02:02 JST
SHA256:
082a3011c4f0536468e8fd9ebd9fc14c5c0e6d191b262d527627a1629390dca2
MD5: 4e8b6bf934bd218daac531c89035097a
File URL:
w3.hepix.org/afs/hepix.org/project/benchmarks/lib/exe/fetch.php?media=hep-spec06-cease-and-desist.doc
User: unknown
Application: web-browsing
Source IP/Port: XX.YY.ZZ.UU:80
Destination IP/Port: xx.yy.zz.uu:32099

Verdict: This sample was determined to be malware.

Summary of behaviors observed during analysis:

- Created or modified a file in the Windows system folder
- Created or modified a file
- Started a process
- Modified the Windows Registry
- Executed a DLL with rundll32.exe
- Used SSL
- Opened a Command Prompt window
- Opened a Windows PowerShell window
- Document contains an embedded OLE object
- Document contains a macro
- Opened another process permission to duplicate handle
- Enumerated running processes
- Sample has no signer
- VBA started a program

Alert from ISP we contracted on guestnet

IIJセキュアWebゲートウェイサービス ウイルス検知について

拝啓 時下益々ご清祥のこととお慶び申し上げます。平素はIIJセキュアWebゲートウェイサービスをご利用いただきまして、誠にありがとうございます。さて、下記の通りウイルスを検出し、遮断いたしましたので報告いたします。

敬具

記

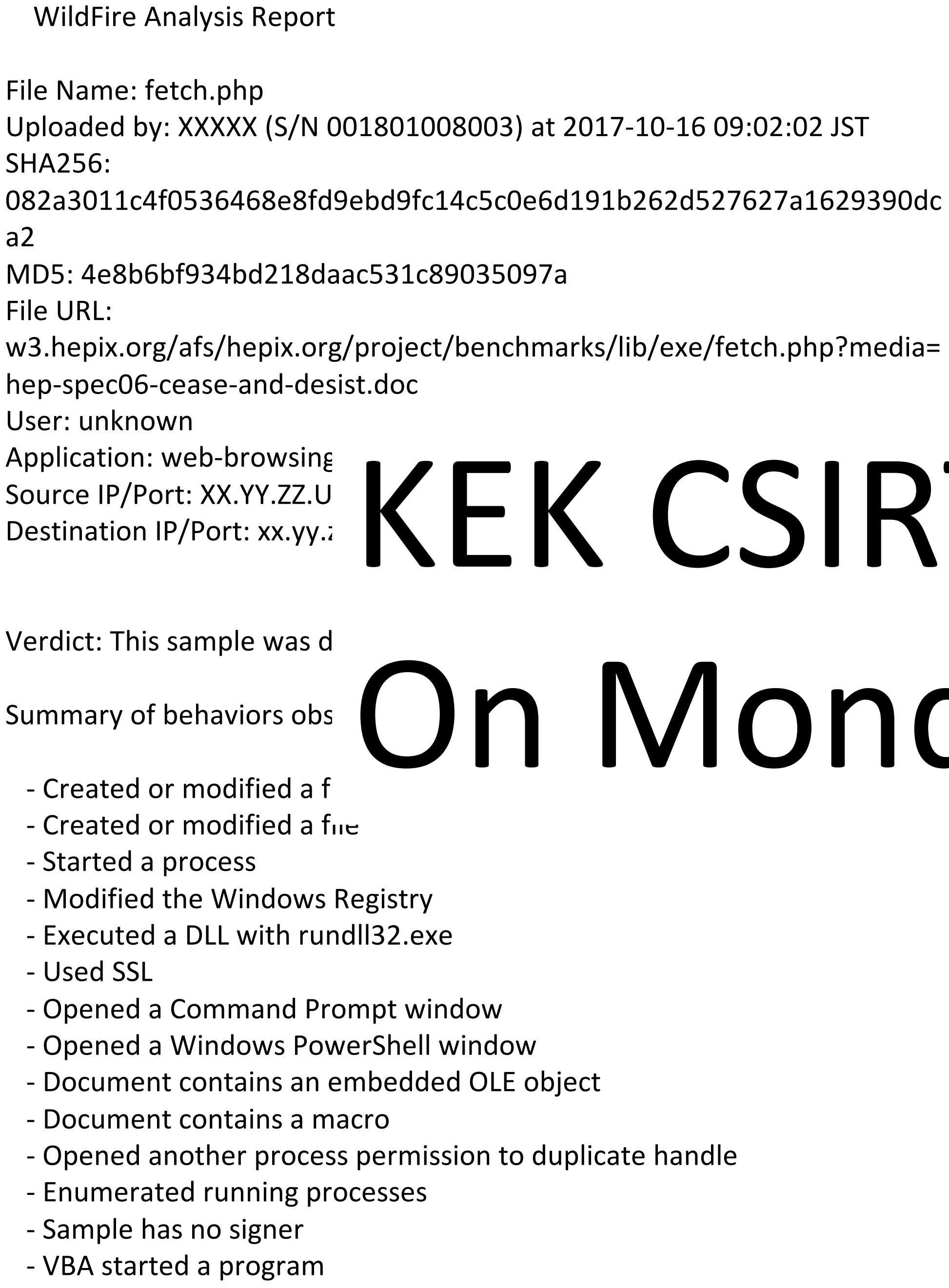
- サービスコード : XXYYZZUU
- お客様名 : 大学共同利用機関法人 高エネルギー加速器研究機構
- 障害情報 No. : 000000000

- 発生時刻 : 2017-10-16 09:33:15
- ウイルス名 : HEUR:Trojan-Downloader.Script.Generic
  : HEUR:Trojan-Downloader.Script.Generic
- 接続元 : xx.yy.zz.uu
- ユーザ名 : -

- 発生時刻 : 2017-10-16 09:34:03
- ウイルス名 : HEUR:Trojan-Downloader.Script.Generic
  : HEUR:Trojan-Downloader.Script.Generic
- 接続元 : xx.yy.zz.uu
- ユーザ名 : -

- 発生時刻 : 2017-10-16 09:34:49
- ウイルス名 : HEUR:Trojan-Downloader.Script.Generic
  : HEUR:Trojan-Downloader.Script.Generic
- 接続元 : xx.yy.zz.uu
- ユーザ名 : -

Alert from FW : eduroam



WildFire Analysis Report

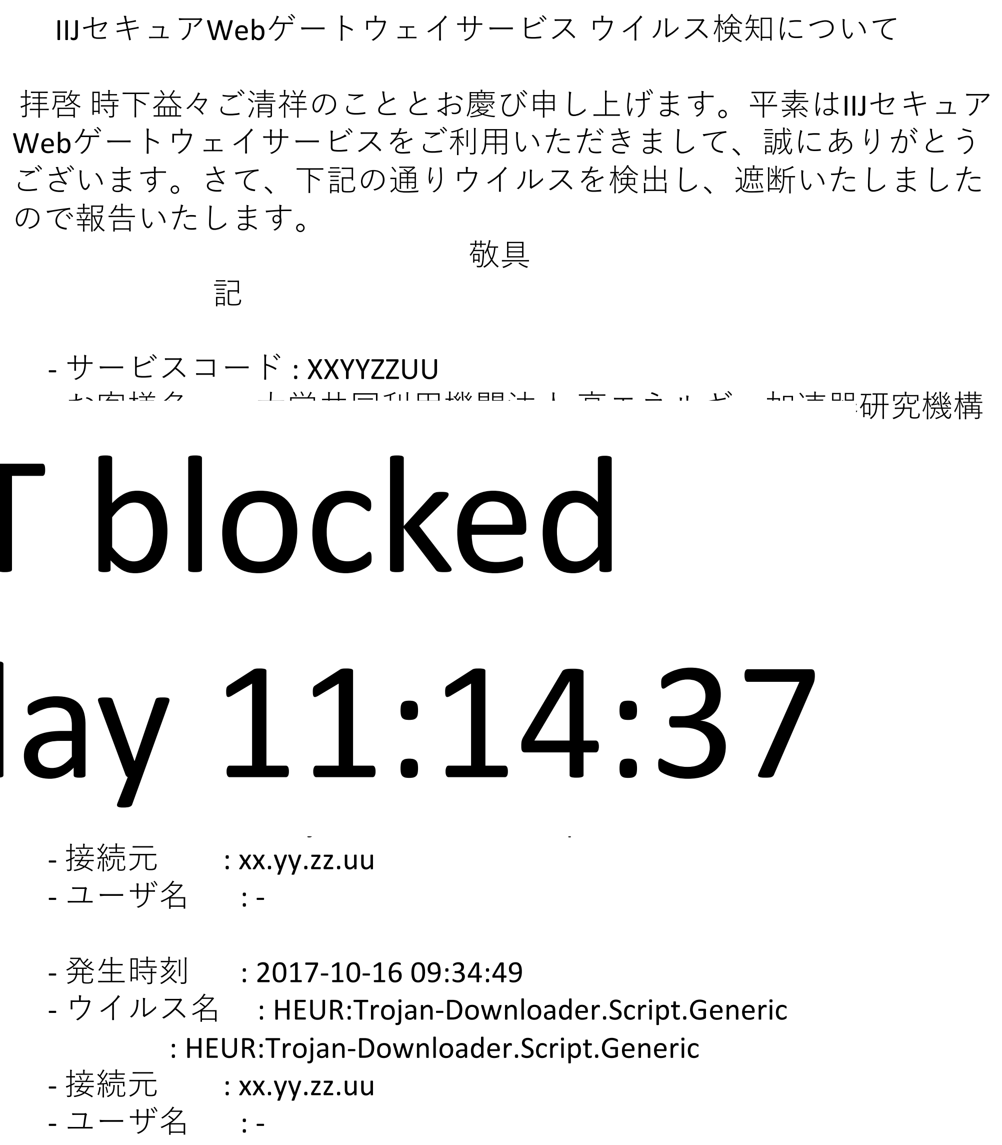
File Name: fetch.php
Uploaded by: XXXXX (S/N 001801008003) at 2017-10-16 09:02:02 JST
SHA256:
082a3011c4f0536468e8fd9ebd9fc14c5c0e6d191b262d527627a1629390dc
a2
MD5: 4e8b6bf934bd218daac531c89035097a
File URL:
w3.hepix.org/afs/hepix.org/project/benchmarks/lib/exe/fetch.php?media=
hep-spec06-cease-and-desist.doc
User: unknown
Application: web-browsing
Source IP/Port: XX.YY.ZZ.U
Destination IP/Port: xx.yy.z

Verdict: This sample was d

Summary of behaviors obs

- Created or modified a f
- Created or modified a file
- Started a process
- Modified the Windows Registry
- Executed a DLL with rundll32.exe
- Used SSL
- Opened a Command Prompt window
- Opened a Windows PowerShell window
- Document contains an embedded OLE object
- Document contains a macro
- Opened another process permission to duplicate handle
- Enumerated running processes
- Sample has no signer
- VBA started a program

Alert from ISP: guestnet



IIJセキュアWebゲートウェイサービス ウイルス検知について

拝啓 時下益々ご清祥のこととお慶び申し上げます。平素はIIJセキュアWebゲートウェイサービスをご利用いただきまして、誠にありがとうございます。さて、下記の通りウイルスを検出し、遮断いたしましたので報告いたします。

敬具

記

- サービスコード : XXYYZZUU
- お客様名 : 大学共同利用機関法人 高エネルギー加速器研究機構

- 接続元 : xx.yy.zz.uu
- ユーザ名 : -

- 発生時刻 : 2017-10-16 09:34:49
- ウイルス名 : HEUR:Trojan-Downloader.Script.Generic
  : HEUR:Trojan-Downloader.Script.Generic
- 接続元 : xx.yy.zz.uu
- ユーザ名 : -

KEK CSIRT blocked

On Monday 11:14:37

Not only us but also NREN is pressured by the law.

NREN In Japan: SINET

The Science Information Network (SINET) is a Japanese academic backbone network for about 850 research institutes and universities operate by NII (National Institute of Informatics).

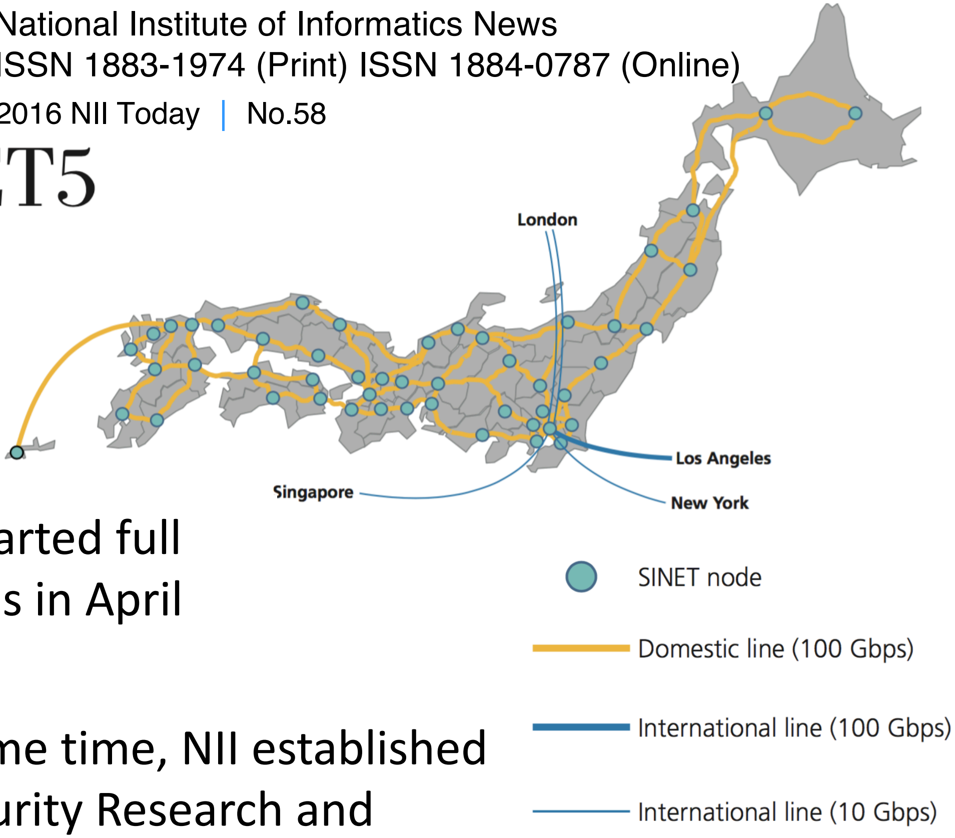
Commentary

National Institute of Informatics News

ISSN 1883-1974 (Print) ISSN 1884-0787 (Online)

2016 NII Today | No.58

SINET5



SINET5 started full operations in April 2016.

At the same time, NII established Cybersecurity Research and Development Center.

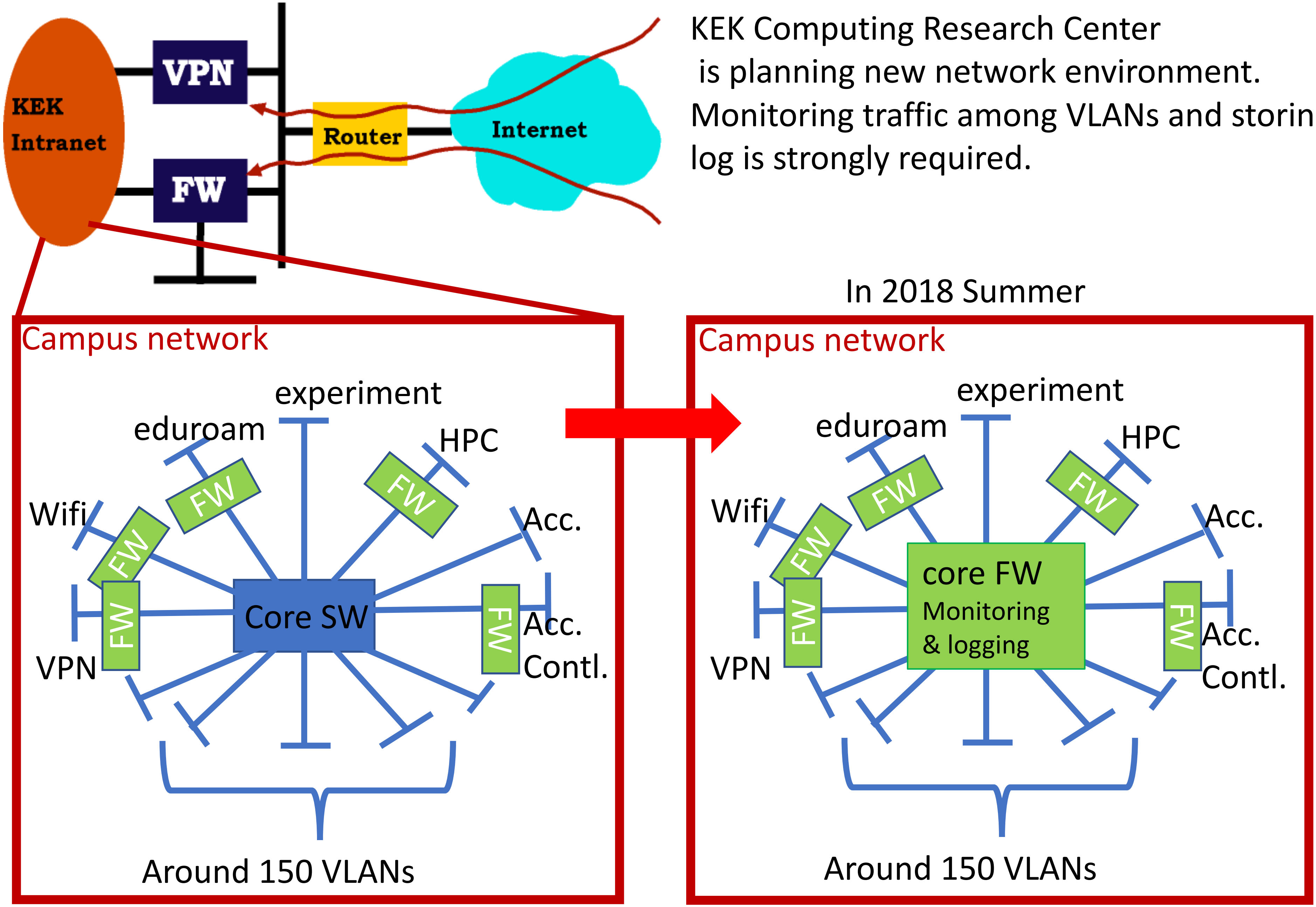
In September 2017, NII started NII-SOCS officially. The SOCS monitors packets in a sampling method and notices when suspicious packets are found.

Concerns

- We have to protect intra network segments where important systems such as an accelerator control system, a detector control system and systems for the administration.
- Though campus wifi VLANs are separated and monitored by FW, there is no FW/IPS among the campus wired VLANs currently.
- So it is difficult to catch the symptom of mal— behavior even if virus tries to spread over a wide area of campus wired VLANs.

We have to consider the future direction of KEK computer security

KEK Computing Research Center is planning new network environment. Monitoring traffic among VLANs and storing log is strongly required.


KEK Intranet
VPN
FW
Router
Internet
Campus network
experiment
eduroam
HPC
Wifi
FW
FW
FW
FW
FW
Acc.
Core SW
Acc. Contl.
VPN
Around 150 VLANs
In 2018 Summer
Campus network
experiment
eduroam
HPC
Wifi
FW
FW
FW
FW
FW
Acc.
core FW
Monitoring & logging
Acc. Contl.
VPN
Around 150 VLANs