Long-term experiences in keeping balance between safety and usability in research activities in KEK

Tadashi Murakami, Fukuko Yuasa, Ryouichi Baba,
Teiji Nakamura, Kiyoharu Hashimoto, Soh Y Suzuki,
Mitsuo Nishiguchi, and Toshiaki Kaneko

High Energy Accelerator Research Organization (KEK)
Computing Research Center, Security Group

Speaker: Tadashi Murakami,
on behalf of Security Group

Background

- We provide KEK general purpose network to support various kinds of research activities
  - in the field of high-energy physics, material physics, and accelerator physics
- Since the end of 20th century,
  - cyber attacks become daily occurrence
  - Rapid and drastic evolution of attacking techniques

We are constantly facing difficult tradeoffs --- safety and usability

Safety includes:

Preventive protection
- monitor / block
- assessment
- (end point security)

- reactive protection

Usability includes:

- throughput
- accessibility
- privacy
- labor-saving

We are constantly facing difficult tradeoffs --- safety and usability

Safety includes:

Preventive protection

- monitor / block
  - FW, IDS/SOC
  - blocking IP/URL
  - logging
- assessment
  - vulnerability mgmt
- (end point security)
  - (Antivirus software)
- reactive protection
  - CSIRT

Usability includes:

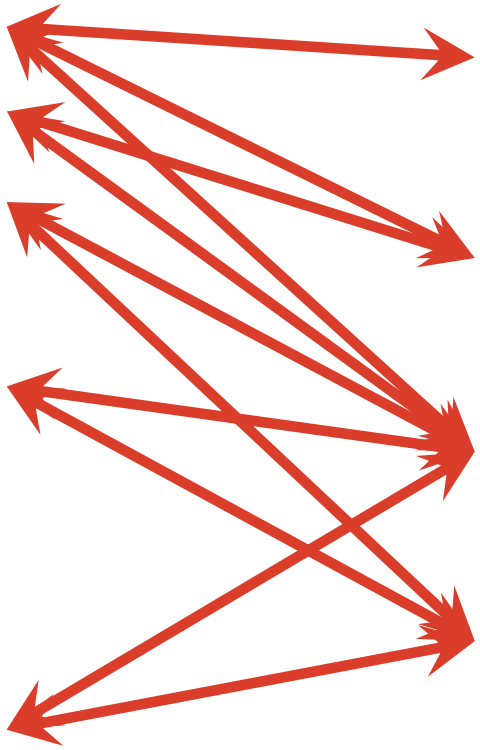
- throughput
- accessibility
- privacy
- labor-saving

We are constantly facing difficult tradeoffs --- safety and usability

Safety includes:

Preventive protection

- monitor / block
  - FW, IDS/SOC
  - blocking IP/URL
  - logging
- assessment
  - vulnerability mgmt
- (end point security)
  - (Antivirus software)
- reactive protection
  - CSIRT



Usability includes:

- throughput
- accessibility
- privacy
- labor-saving

We are constantly facing difficult tradeoffs --- safety and usability

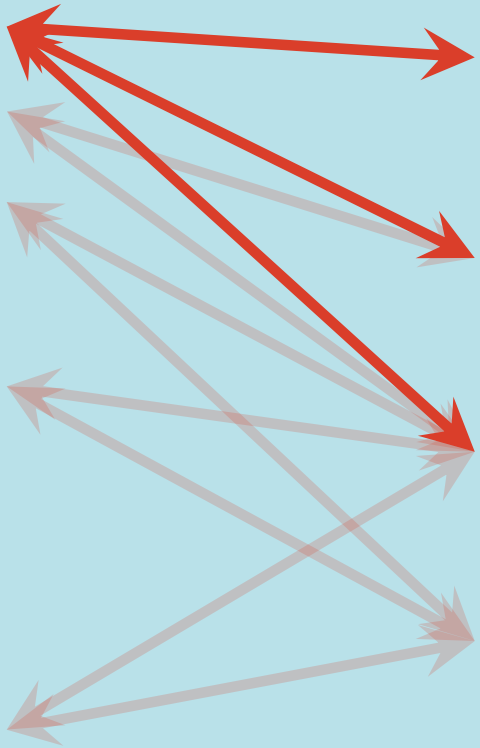
Safety includes:

Preventive protection

- monitor / block
  - FW, IDS/SOC
  - blocking IP/URL
  - logging
- assessment
  - vulnerability mgmt
- (end point security)
  - (Antivirus software)
- reactive protection
  - CSIRT

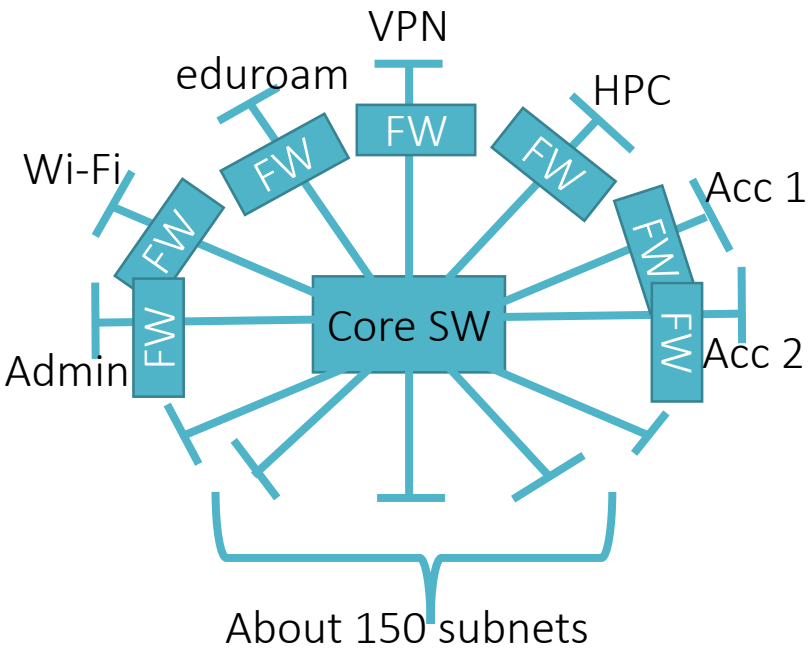
Usability includes:

- throughput
- accessibility
- privacy
- labor-saving



For monitor / block : Firewalls in KEK

- We introduced common FW in zone boundary, since 2002
  - in internet, DMZ, intranet, etc.
- Several research groups manage their own internal FWs
  - for their specific demands
  - e.g., permit only specific segments

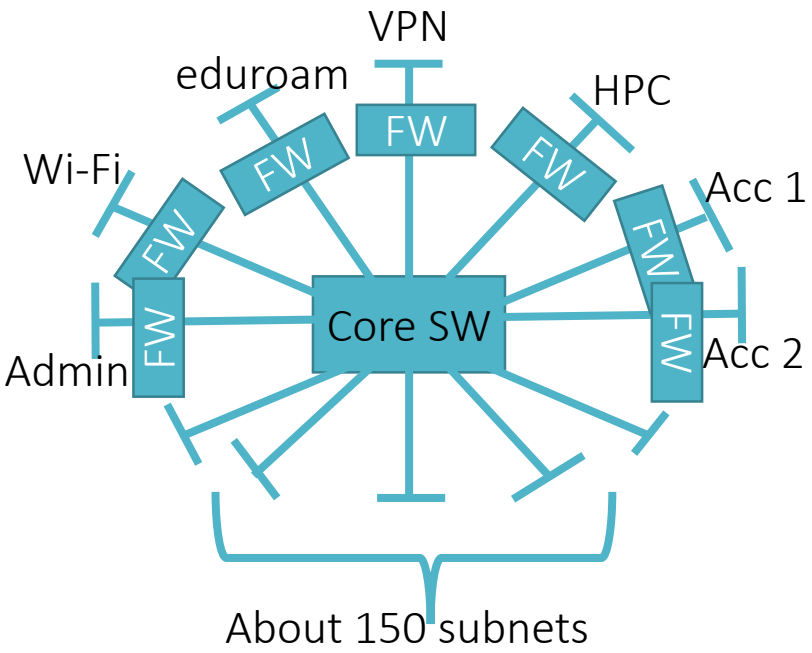


For monitor / block : Firewalls in KEK

Tradeoffs

- FW can be a bottleneck for a network
- Fine segmentation <=> Speedy operation
  - Fine segmentation needs higher operation cost for management of filter rules and packet monitoring

  → slow operation, error-prone
- Privacy
  - FW can monitor users' behavior

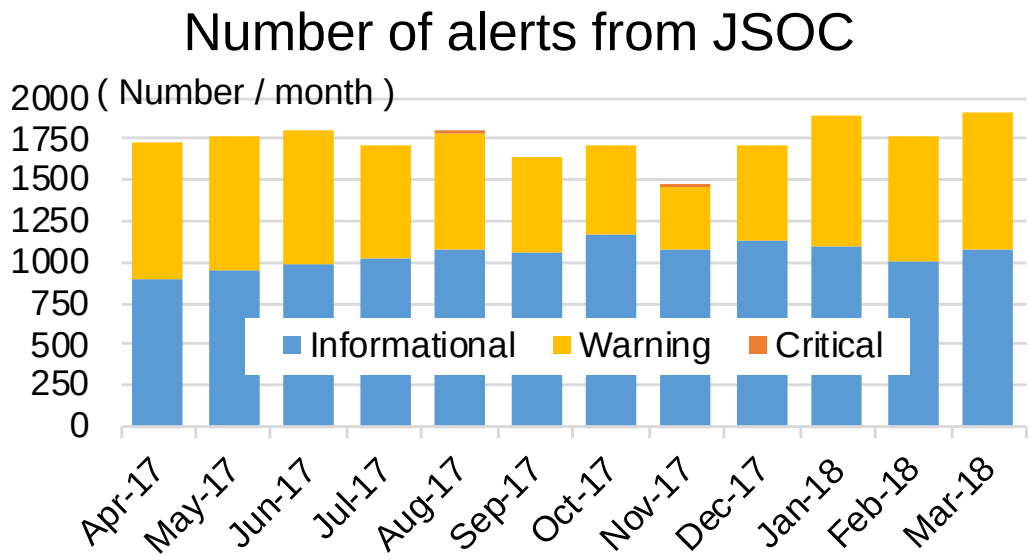


Step-by-step – for cares of throughput, accessibility, privacy

- Since 2004, we added FWs to separate wired network
  - from wireless and VPN in 2004
  - from IPv6, J-PARC, eduroam, ...
- We are preparing a new FW including a virtual FW in 2018
  - That can separate wired network segments themselves

For monitor packets : IDS, SOC

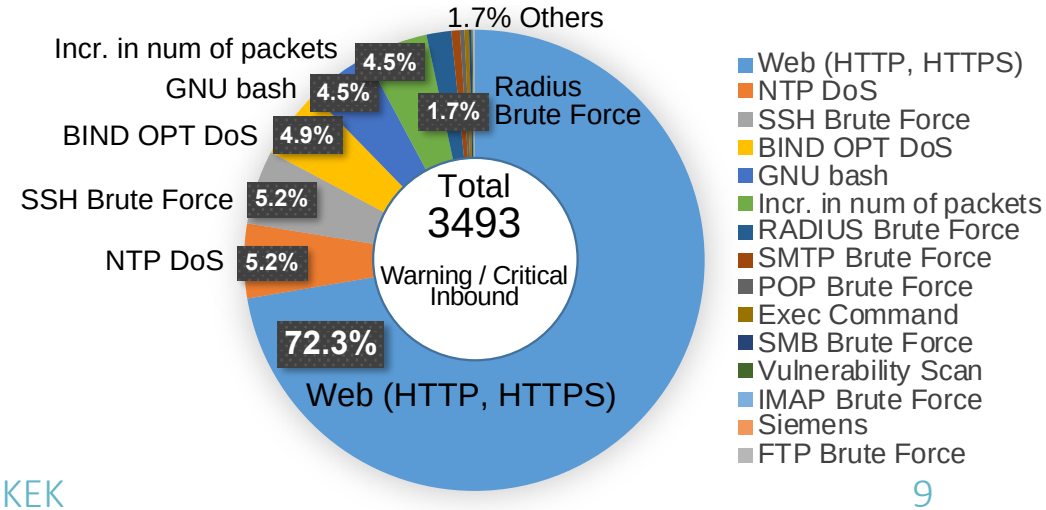
- We mirror every packet from/to internet, and monitor with IDS
  - not IPS, for care of throughput, accessibility, privacy
- Too many alerts
  - total 2.0×10^6 alerts in Apr. 2017
- We outsource SOC provider in 24hours-365 days service, JSOC
  - human-based analysis
  - pick-up important alerts
- Upper graph: Number of alerts from JSOC
  - reduction to about 1800/month
  - 4 of 'Critical' alerts from JSOC in FY2017
- Lower graph: the breakdown (various attacks)
  - Attack to web is dominant



(month from Apr 2017 to Mar 2018)

Breakdown of above

(later half of FY2017: from Oct 2017 to Mar 2018)



We are constantly facing difficult tradeoffs --- safety and usability

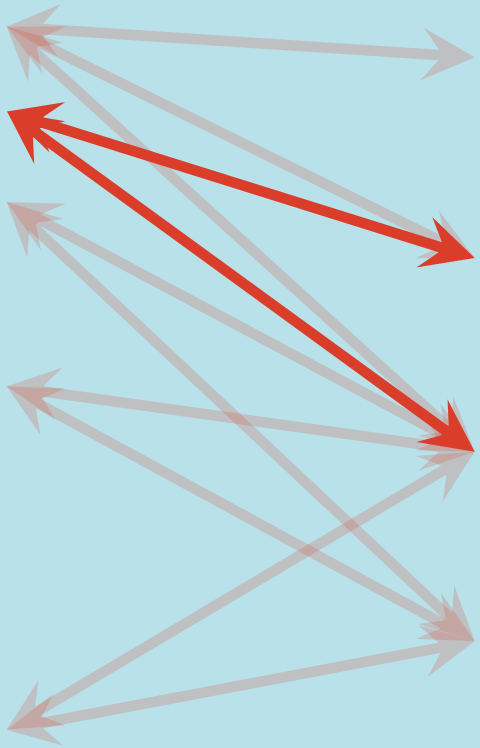
Safety includes:

Preventive protection

- monitor / block
  - FW, IDS/SOC
  - blocking IP/URL
  - logging
- assessment
  - vulnerability mgmt
- (end point security)
  - (Antivirus software)
- reactive protection
  - CSIRT

Usability includes:

- throughput
- accessibility
- privacy
- labor-saving

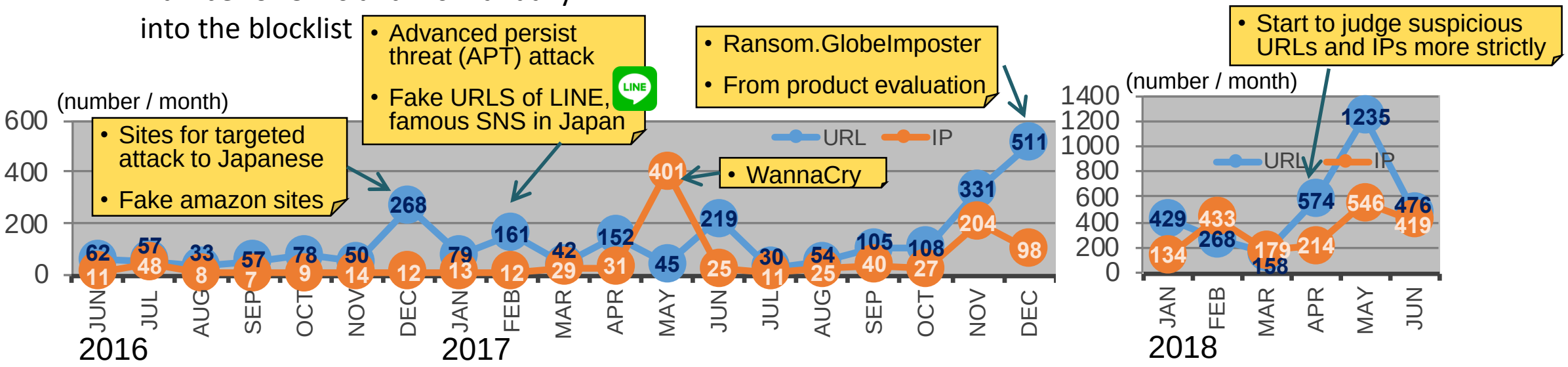


For proactive protection : URL filtering (FW)

- FW can block malicious URLs
  - Blocklist daily supplied by the FW vender
  - Malware / gambling / phishing ...
- We cannot use the whole list
  - false-positives: academic sites are filtered
  - false-negatives: Japanese malicious sites are not filtered

- We add over 8000 of URLs and IPs manually into the blocklist
  - source: JPCERT/CC, IPA, Police, commercial SOC, etc.
- Usability -- only 4 cases of inquiry in URL filtering (from June 2016)
  - All of them are related to false-positives in vender blocklist
- The manual addition works effectively

■ Number of URLs and IPs manually into the blocklist

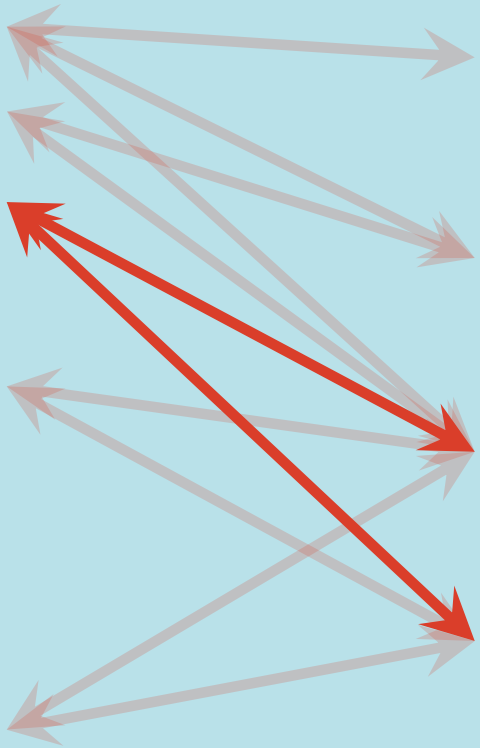


We are constantly facing difficult tradeoffs --- safety and usability

Safety includes:

Preventive protection

- monitor / block
  - FW, IDS/SOC
  - blocking IP/URL
  - logging
- assessment
  - vulnerability mgmt
- (end point security)
  - (Antivirus software)
- reactive protection
  - CSIRT

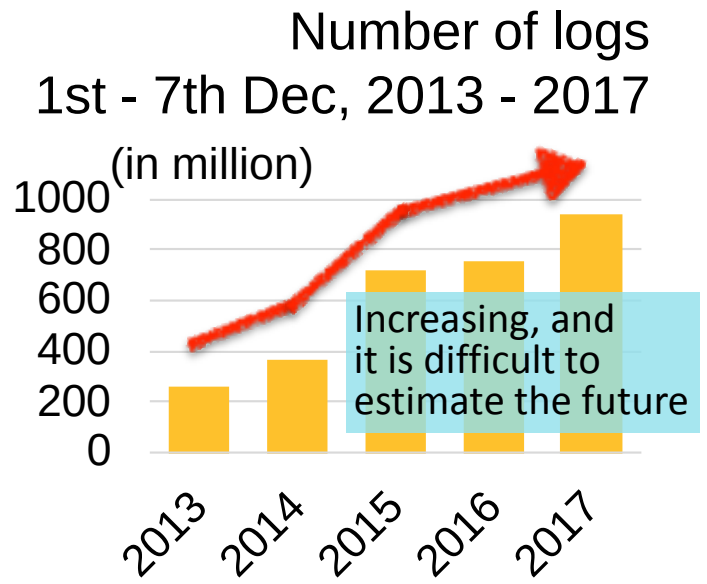


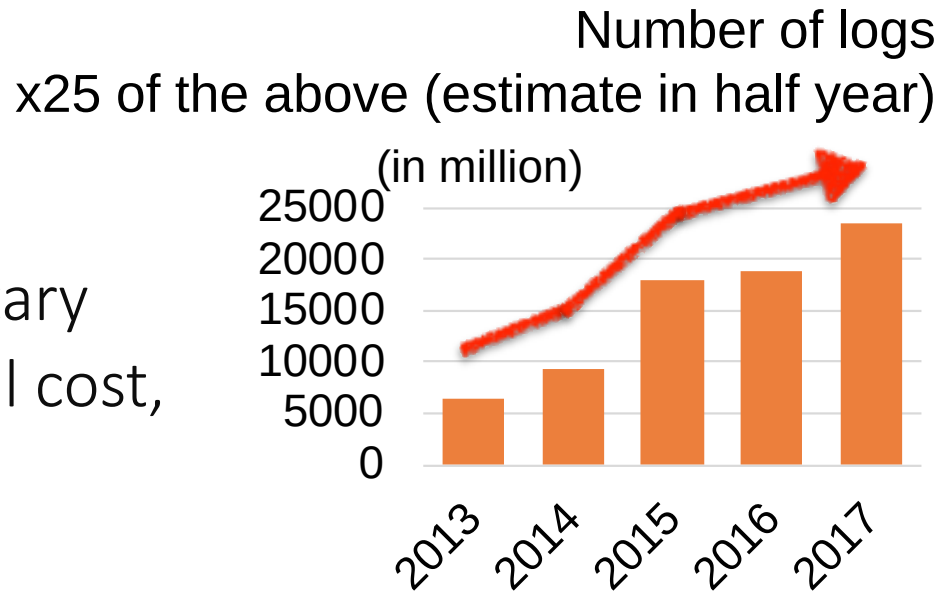
Usability includes:

- throughput
- accessibility
- privacy
- labor-saving

Logging IP traffic

- 940 million records, 315GB in 1 week (Dec 2017)
- multiple copies
  1. syslog server managed by operating staff (not me)
  2. syslog server managed by me
  3. log replication using Gfarm
     - with compression by gzip (under 10% size)
  4. Splunk and some proprietary tools
- Every 15 minutes log-check by cron
- Log analysis is important, but most of proprietary tool does not fit in performance and/or annual cost, in KEK
  - too expensive and/or too slow





We are constantly facing difficult tradeoffs --- safety and usability

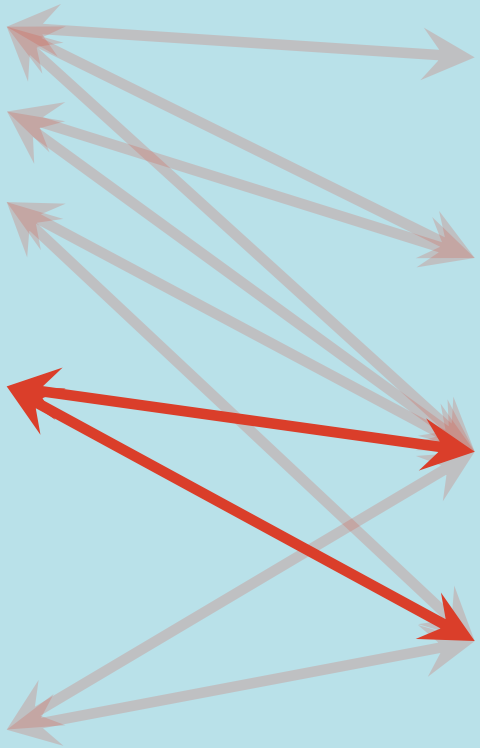
Safety includes:

Preventive protection

- monitor / block
  - FW, IDS/SOC
  - blocking IP/URL
  - logging
- assessment
  - vulnerability mgmt
- (end point security)
  - (Antivirus software)
- reactive protection
  - CSIRT

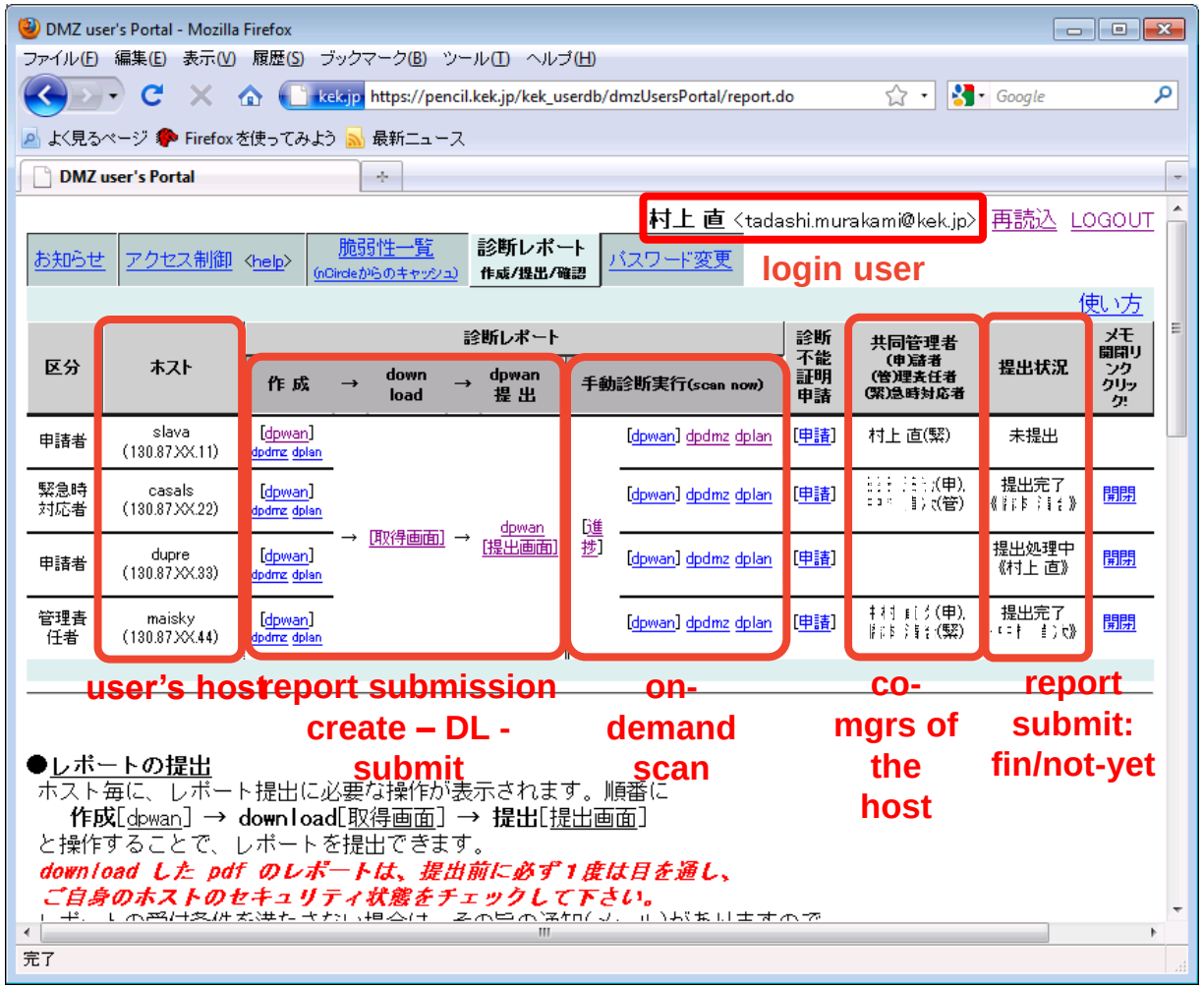
Usability includes:

- throughput
- accessibility
- privacy
- labor-saving



For assessment : Vulnerability Management (1/2)

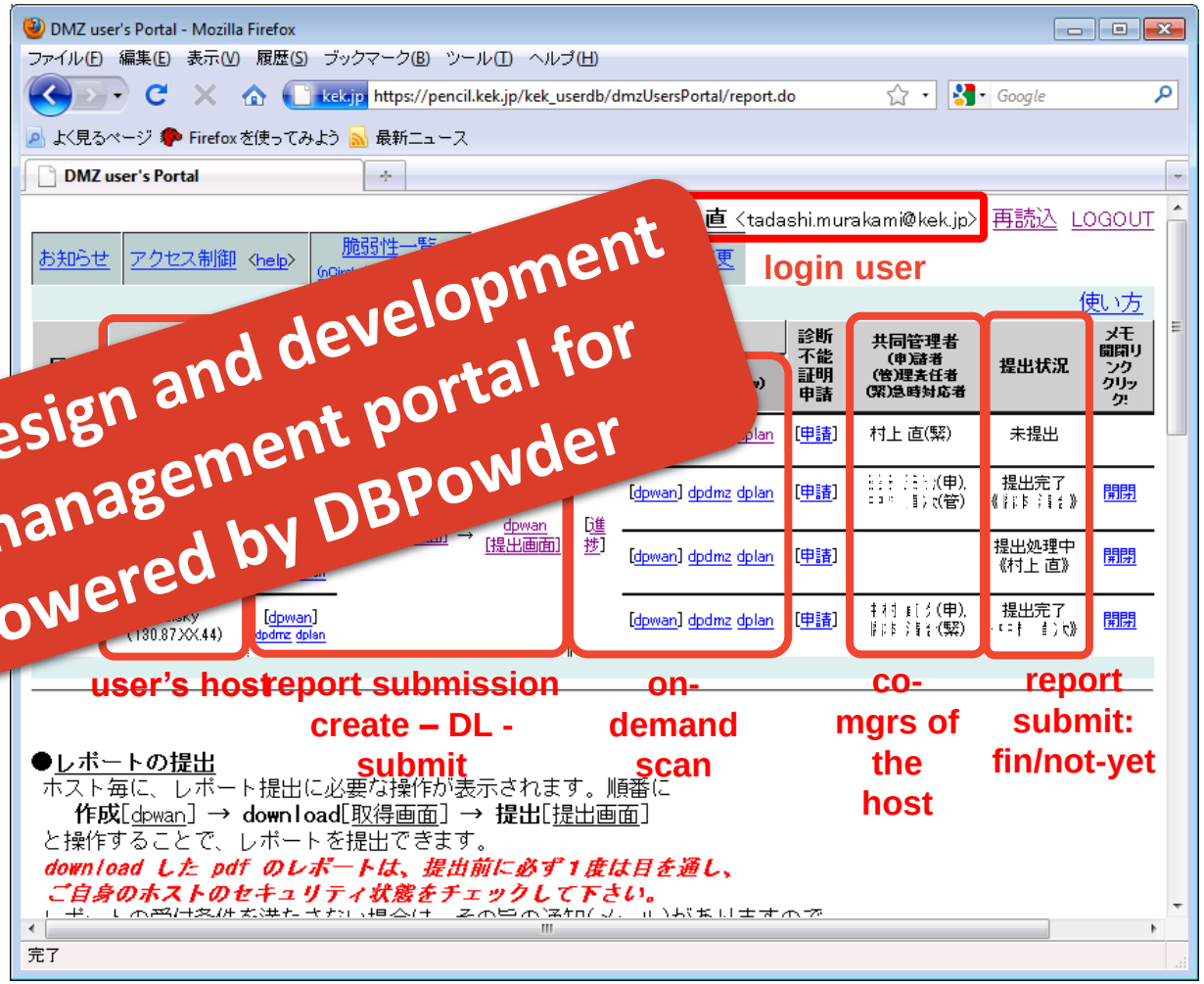
- In our DMZ networks
  - over 350 hosts, total 100 admins, in historical reason ...
- We provide quality management service with Tripwire IP360
  - Vulnerability management device
  - scan DMZ hosts weekly (auto)
  - find vulnerabilities and score them
  - send out a message alert depending on the score
  - We utilize IP360 by in-house development
- We develop DMZ User's Portal site since 2007
  - easy use of IP360 by host admins
    - 1-click based operation
  - extended in our related networks
    - J-PARC (2011), HEPnet-J (2017)



- T.Murakami, et al. DBPowder: A Flexible Object-RelationalMapping Framework based on a Conceptual Model. the 37th IEEE COMPSAC 2013, Kyoto, Japan, pp.589–598, Jul. 2013. (acceptance rate 23%)
- T.Murakami, et al. Vulnerability Management by the Integration of Security Resources and Devices with DBPowder. Grid Camp and HEPiX Fall 2008, Oct. 2008.

For assessment : Vulnerability Management (1/2)

- In our DMZ networks
  - over 350 hosts, total 100 admins, in historical reason ...
- We provide quality management service with Tripwire IP360
  - Vulnerability management device
  - scan DMZ hosts weekly (aut
  - find vulnerabilities
  - send out a messa
    score
  - We utilize IP360 by
- We develop DMZ User's Portal site since 2007
  - easy use of IP360 by host admins
    - 1-click based operation
  - extended in our related networks
    - J-PARC (2011), HEPnet-J (2017)



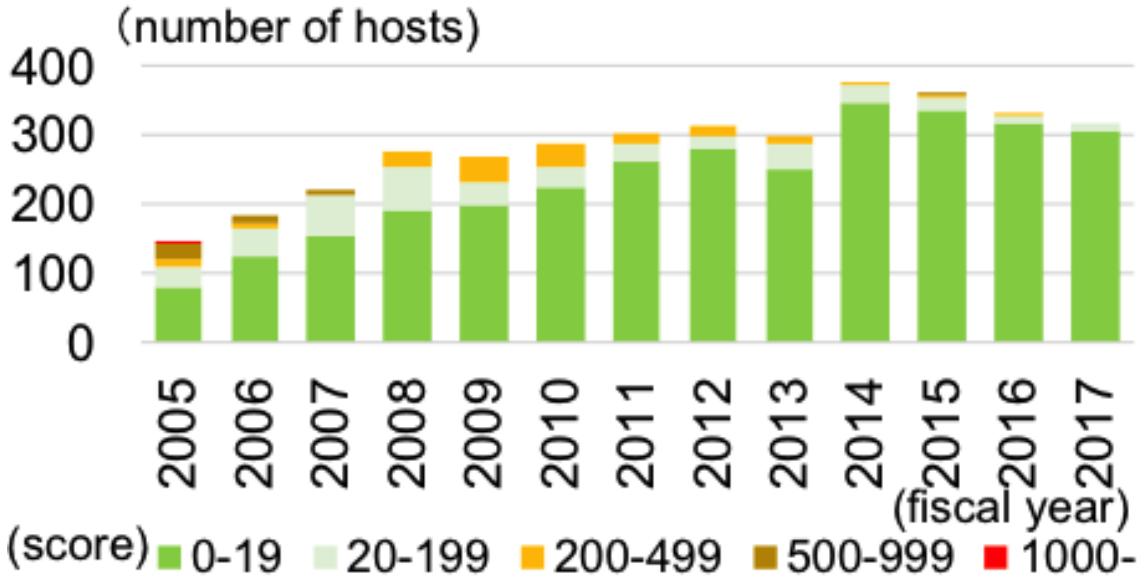
In poster session: Design and development of vulnerability management portal for DMZ admins powered by DBPowder

- T.Murakami, et al. DBPowder: A Flexible Object-RelationalMapping Framework based on a Conceptual Model. the 37th IEEE COMPSAC 2013, Kyoto, Japan, pp.589–598, Jul. 2013. (acceptance rate 23%)
- T.Murakami, et al. Vulnerability Management by the Integration of Security Resources and Devices with DBPowder. Grid Camp and HEPiX Fall 2008, Oct. 2008.

For assessment : Vulnerability Management (2/2)

- The portal helps annual self security inspection performed by KEK mgmt
  - Host admins use DMZ User's Portal themselves
  - to check their hosts, and submit reports
  - The reports are checked by KEK security management committee
- The distribution of score from 2005 to 2017 shows
  - In 2005, not a few hosts with high score (over 25% over 200pt)
  - High score decreases Step-by-step
  - Low score (green) becomes major, over 90%
- User-based quality management remains successful
  - with the help of DMZ User's Portal

Transition of vulnerability score, in max points (DMZ)



We are constantly facing difficult tradeoffs --- safety and usability

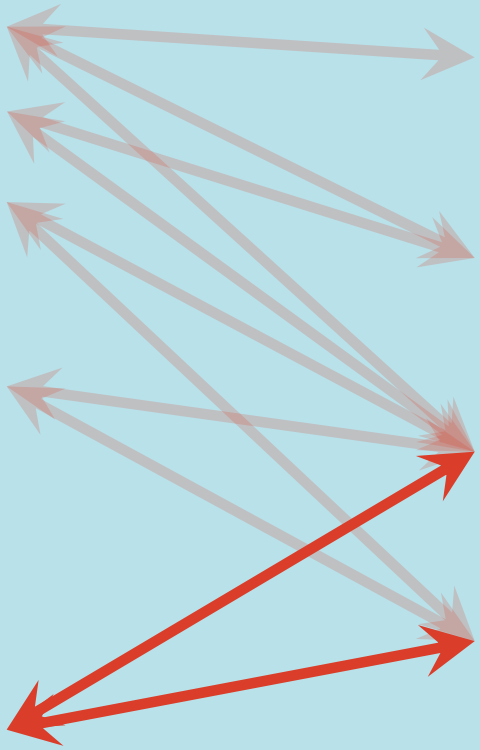
Safety includes:

Preventive protection

- monitor / block
  - FW, IDS/SOC
  - blocking IP/URL
  - logging
- assessment
  - vulnerability mgmt
- (end point security)
  - (Antivirus software)
- reactive protection
  - CSIRT

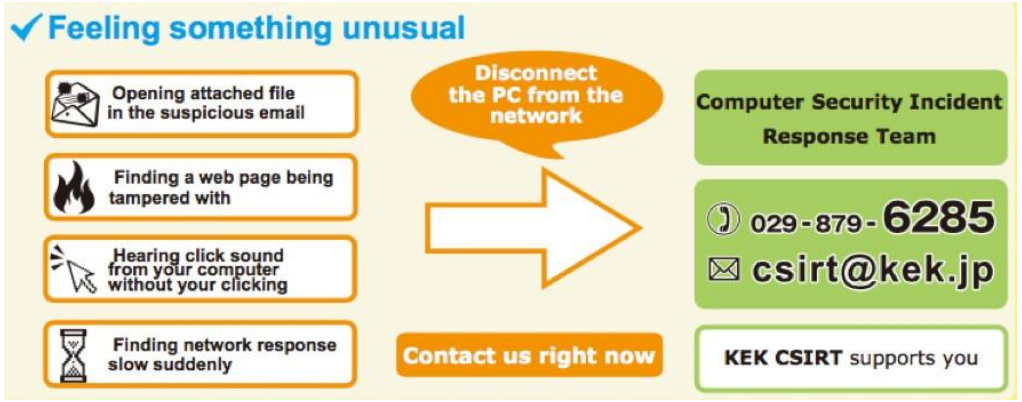
Usability includes:

- throughput
- accessibility
- privacy
- labor-saving



CSIRT: Reactive protection

- When a security incident occurs, we make responses as follows:
  - investigate, analyze, prevent damage from spreading
  - After then, create recurrence prevention measures, make a recovery plan
  - Then, implement the measures and plan
  - We started KEK-CSIRT in 2012 and act explicitly as CSIRT team
- KEK-CSIRT always faces with the trade-offs
  - It is crucially important to keep a network environment safe
  - Too much measure may improve the safety, however, such a network is not suitable for a research institute
- Our activity is based on a trust relationship with network users
  - We respect users' privacy
  - We always interact with users, not in a command-hierarchical manner
  - Without trust from users, we cannot proceed appropriate incident-response



Incidents statistics

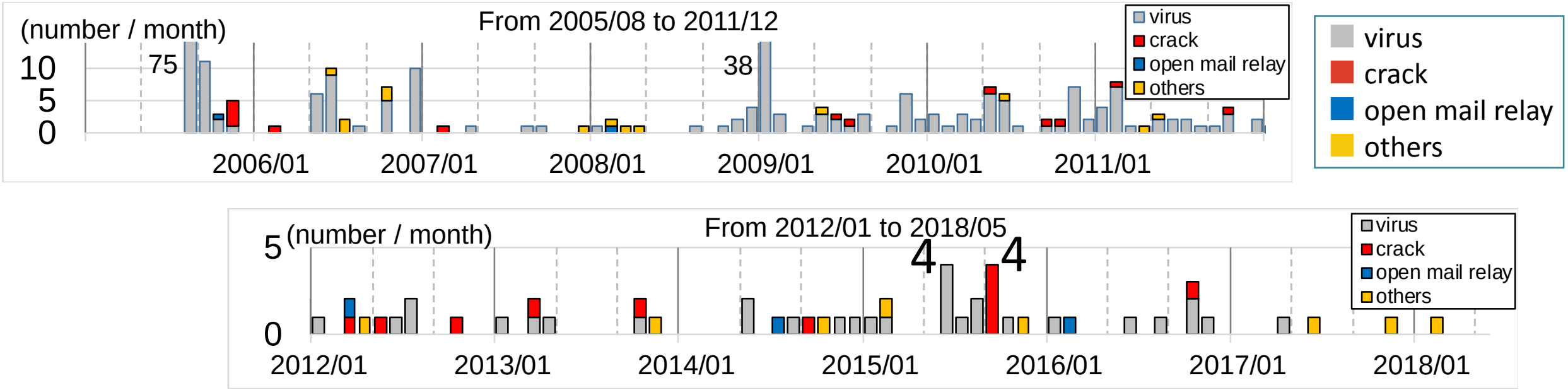


Figure: number of security incidents from Aug. 2005 to May. 2018

- The number is kept relatively small
  - Cyber-attack frequency is obviously increasing in these years
  - We can decrease the num of incidents in recent 10 years
  - Hopefully our strategy goes to the right direction, with users' improvement for security-consciousness
- But sometimes Japanese general opinion demands 'zero risk'
  - '*the goal*' zero incident is still far beyond
- Some serious incidents occur

Conclusions

- Safety and usability: we are facing difficult tradeoffs
  - In monitor/block --- FW, IDS, manual-block, logging
    - tradeoffs: safety <-> throughput, accessibility, privacy
  - In vulnerability management --- vuln. scanner
    - tradeoffs: safety <-> privacy, labor-saving
- Our long-term experiences in keeping a balance b/w safety and usability
  - In monitor/block
    - introduce measures Step-by-step
    - especially, introduce auto-block with care and care
  - In vulnerability assessment
    - provide portal site with easy use of vulnerability scanner
    - Annual self security check
- CSIRT activity is important for reactive protection
  - in cooperation with proactive protections