Cyber Clean Center Project
- A five year retrospective -

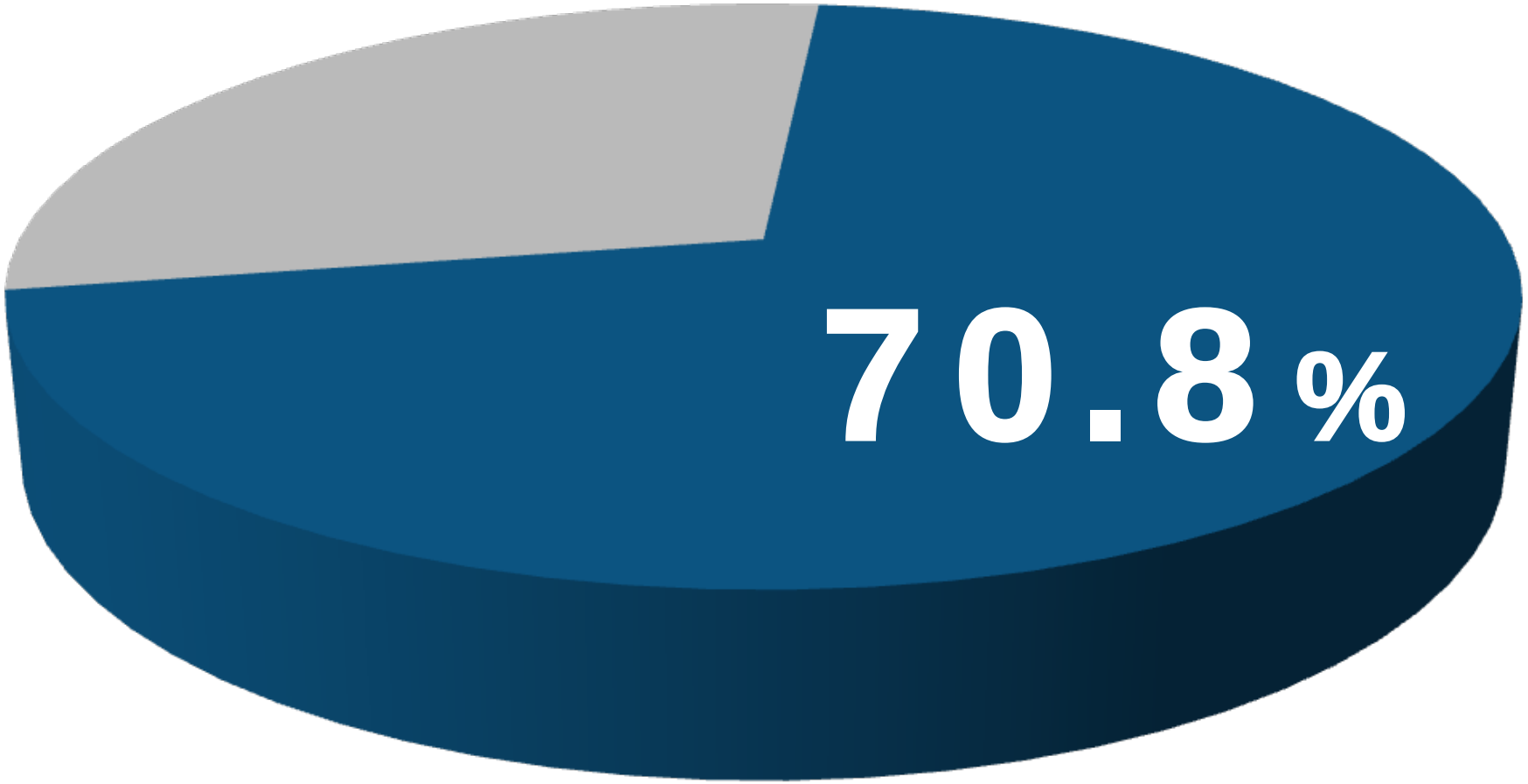
You NAKATSURU
JPCERT Coordination Center
Analysis Center

Agenda

- Background - Japanese situation -
- The Cyber Clean Center
- Seeing the Effect
- Achievement
- Existing Issues
- Current Status

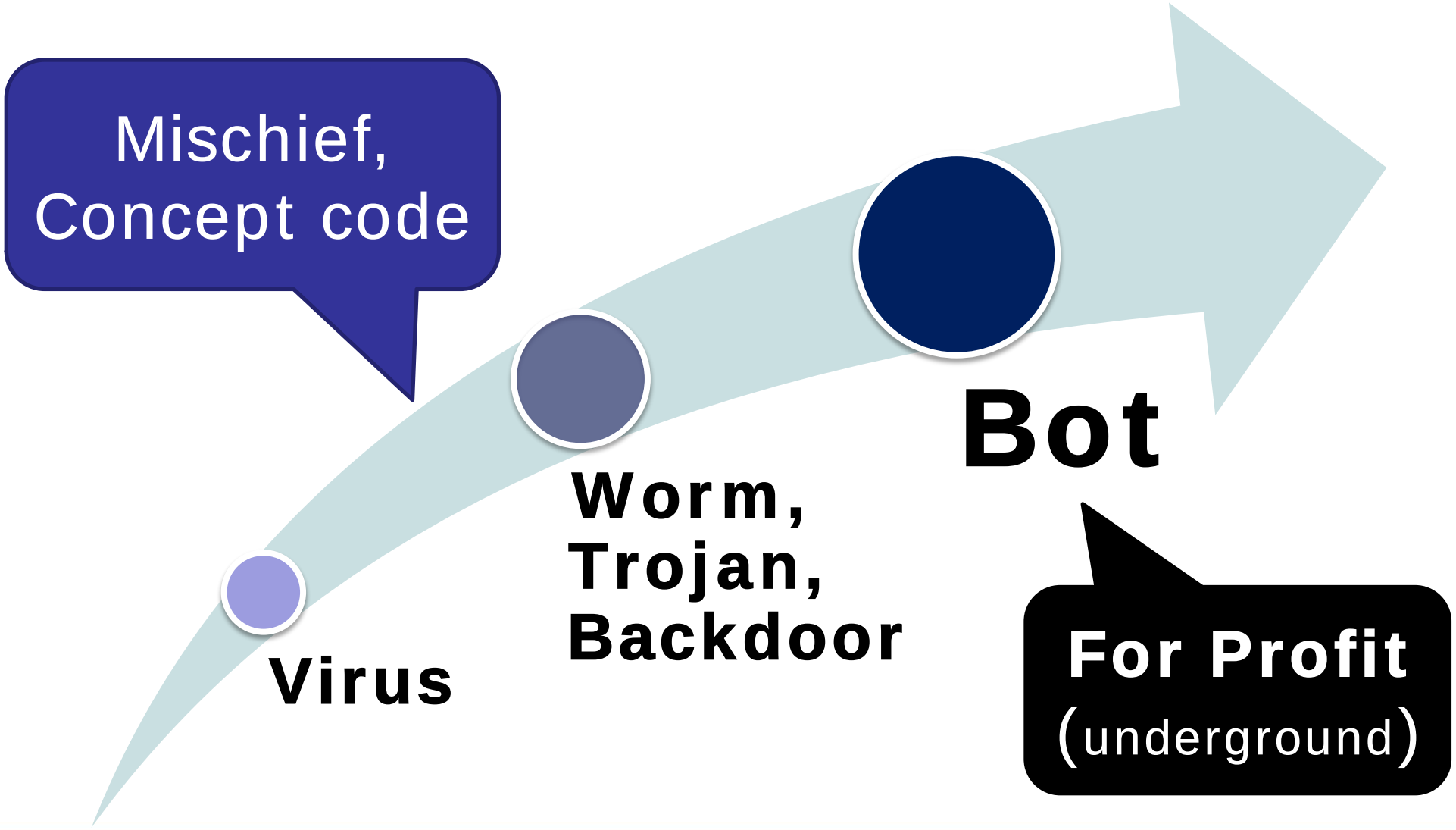
BACKGROUND
- JAPANESE SITUATION -

Internet users in 2005



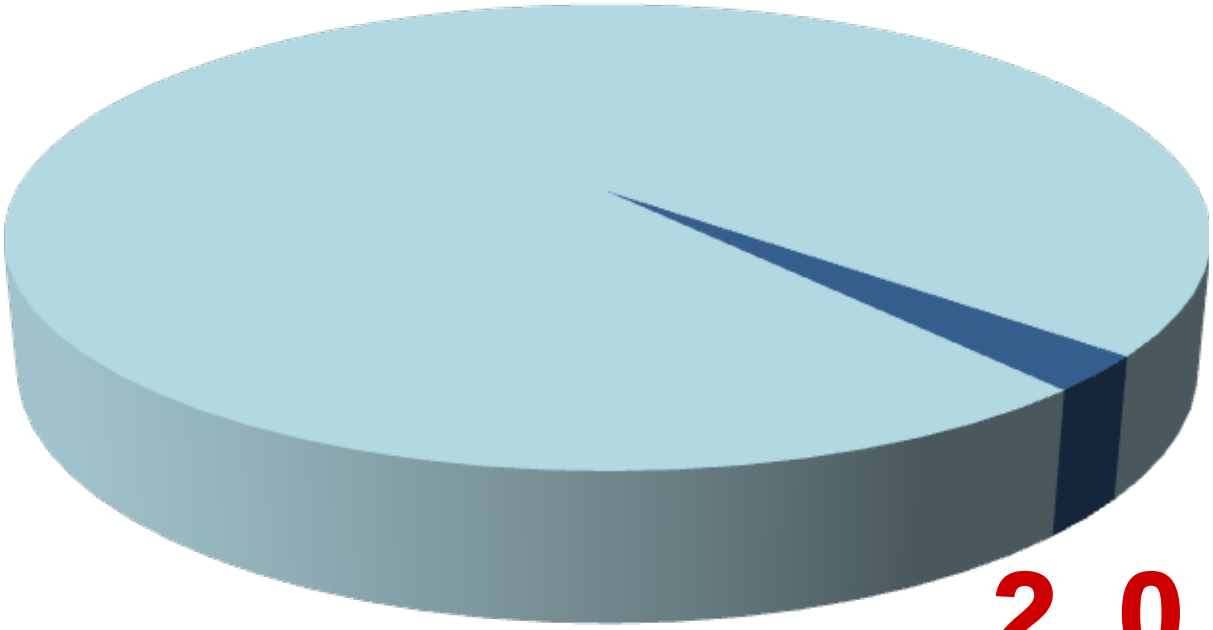
source: MIC "Internet users as a proportion of the population"
http://www.soumu.go.jp/johotsusintokei/english/

Growth of malware until 2005



Infected PCs in 2005

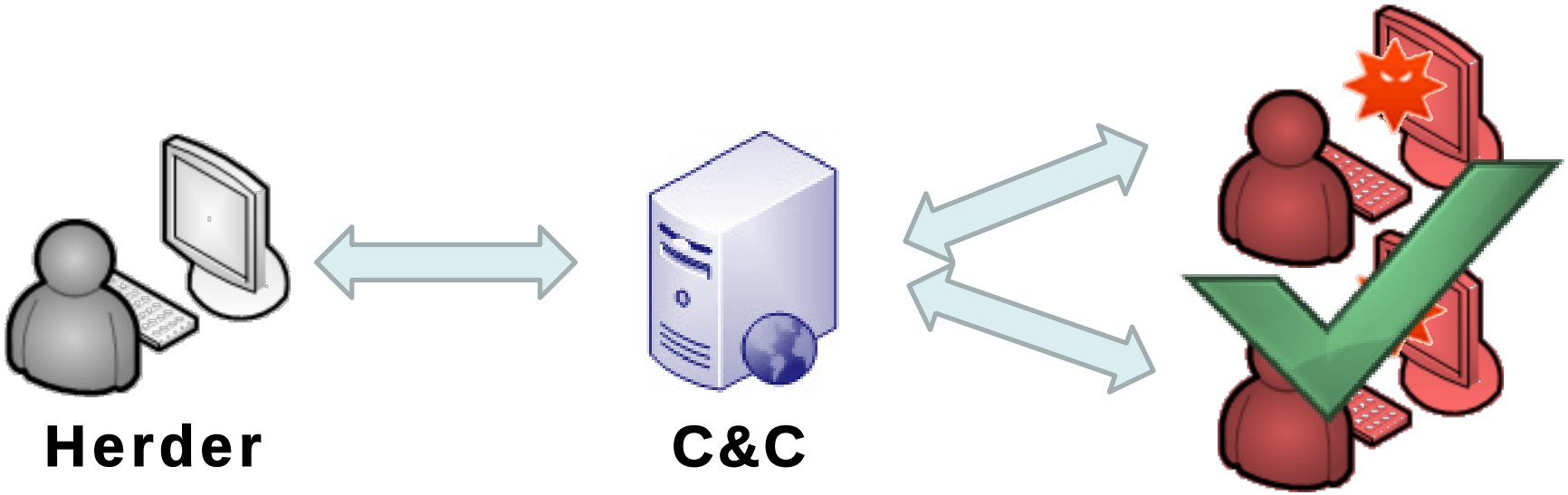
- Targeted "broad-band users"



2.0 ~ 2.5 %

400,000 users

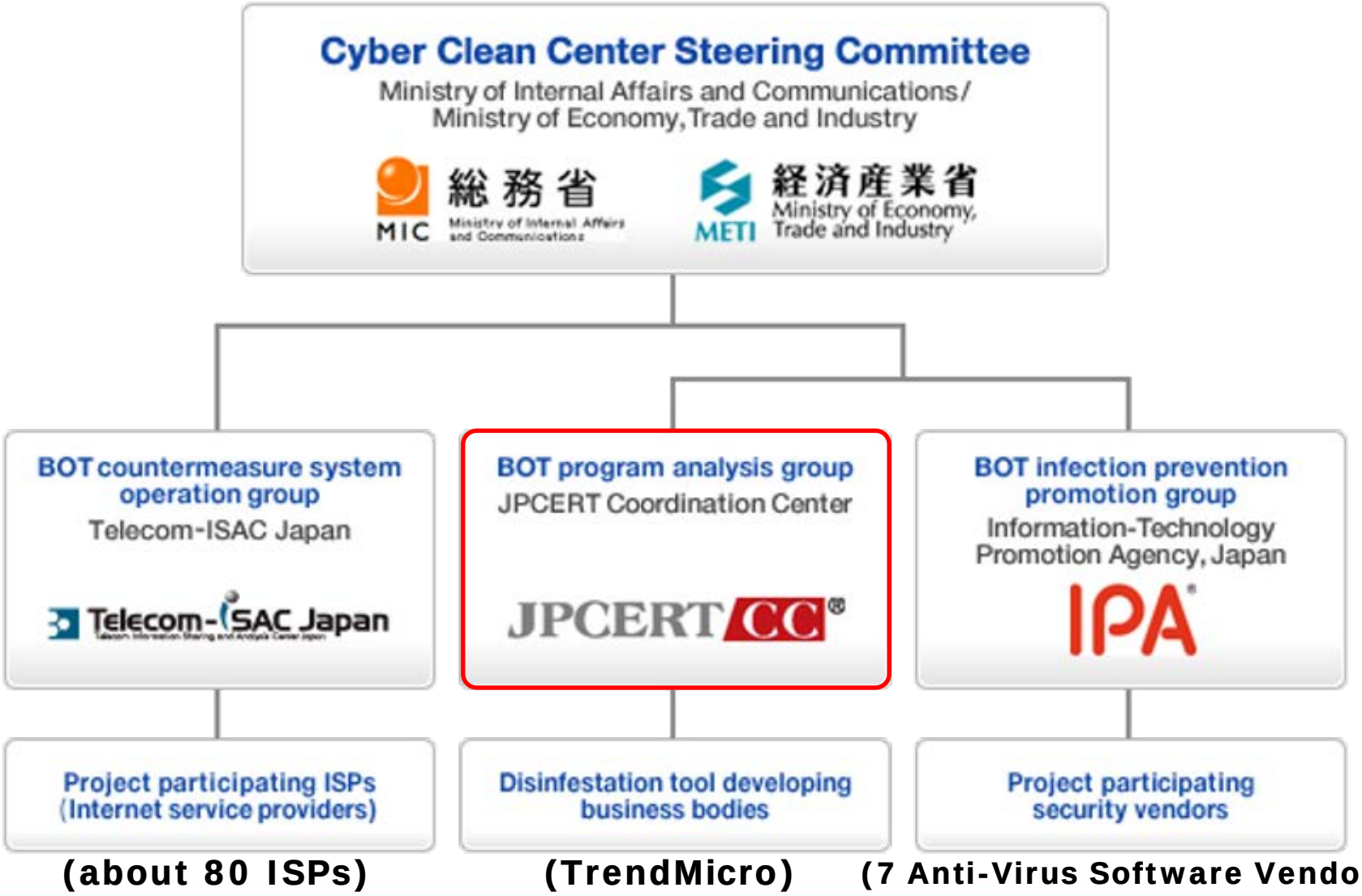
Our Decision



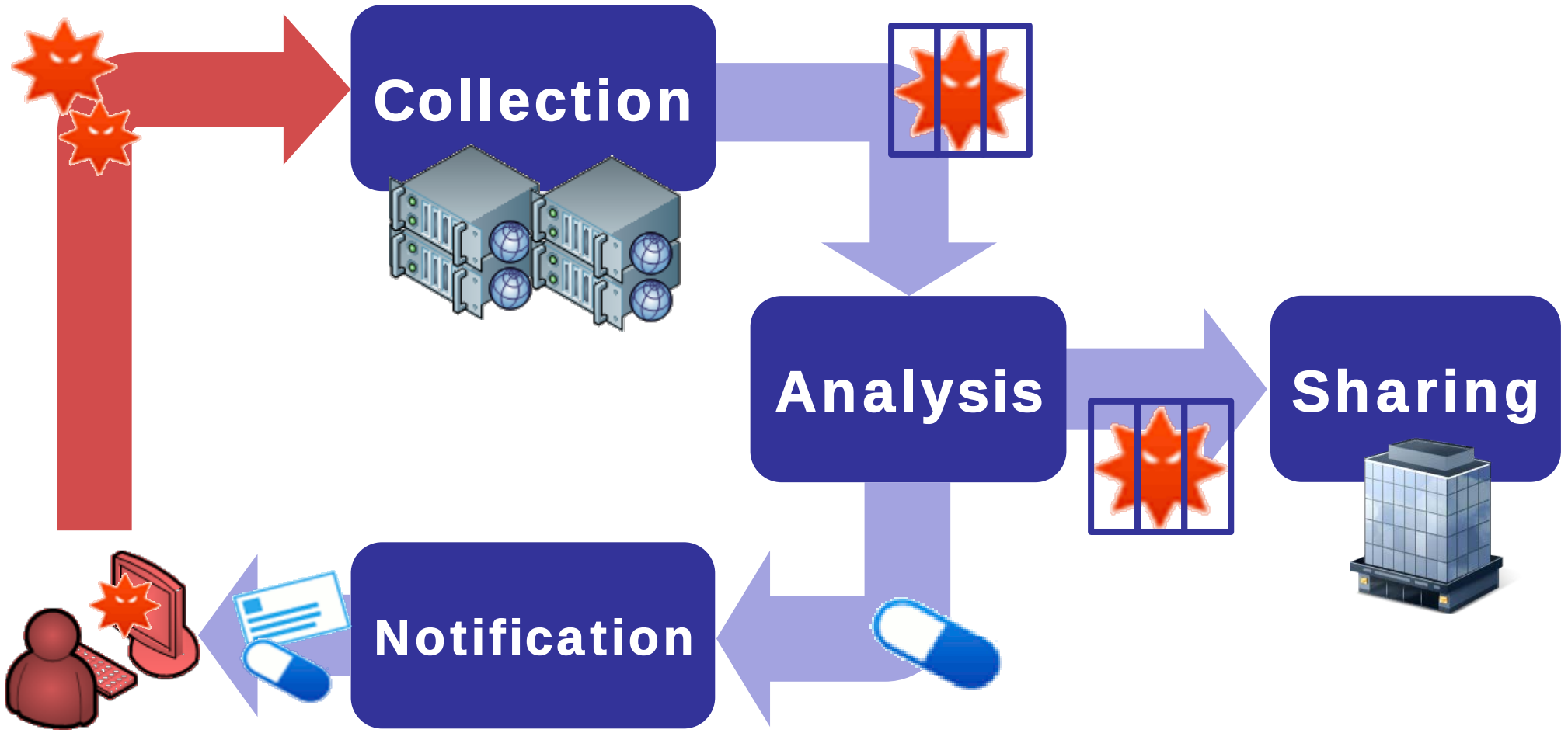
- It's easy to reach infected users.
- It's a good idea to develop user literacy.

THE CYBER CLEAN CENTER

Organization Chart

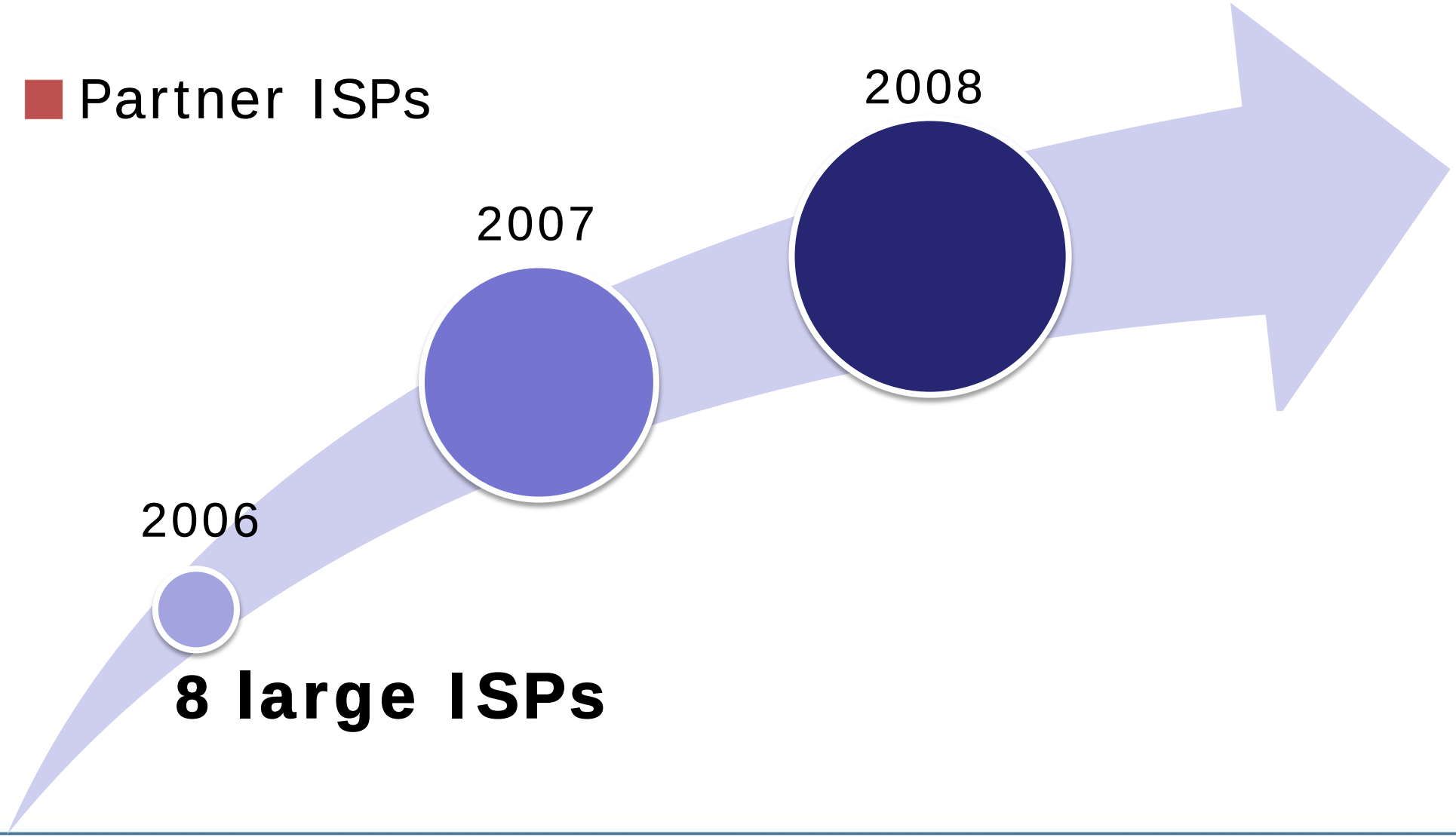


Operational Framework



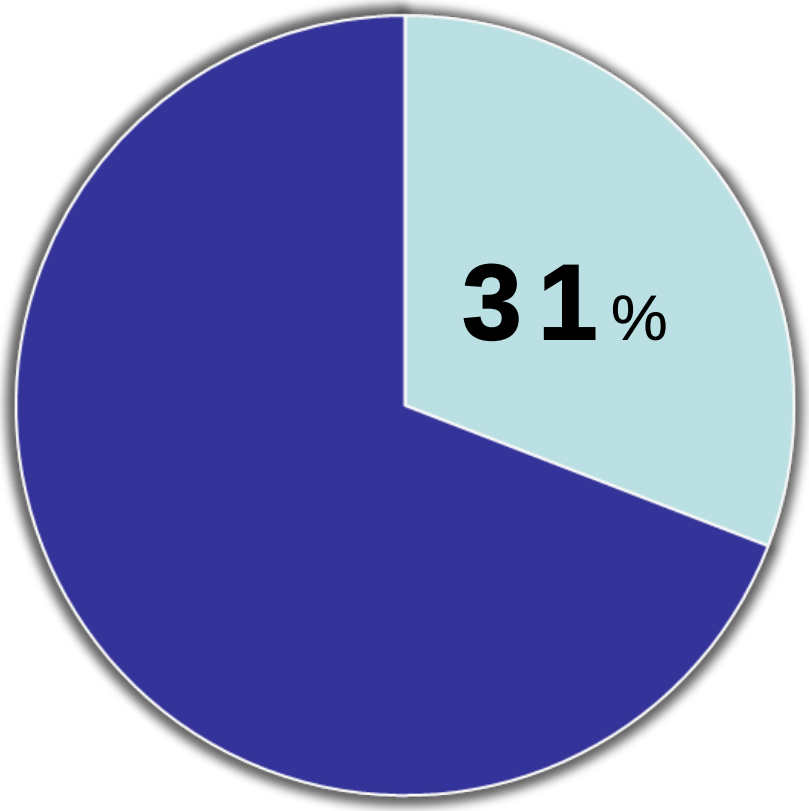
SEEING THE EFFECT

User coverage

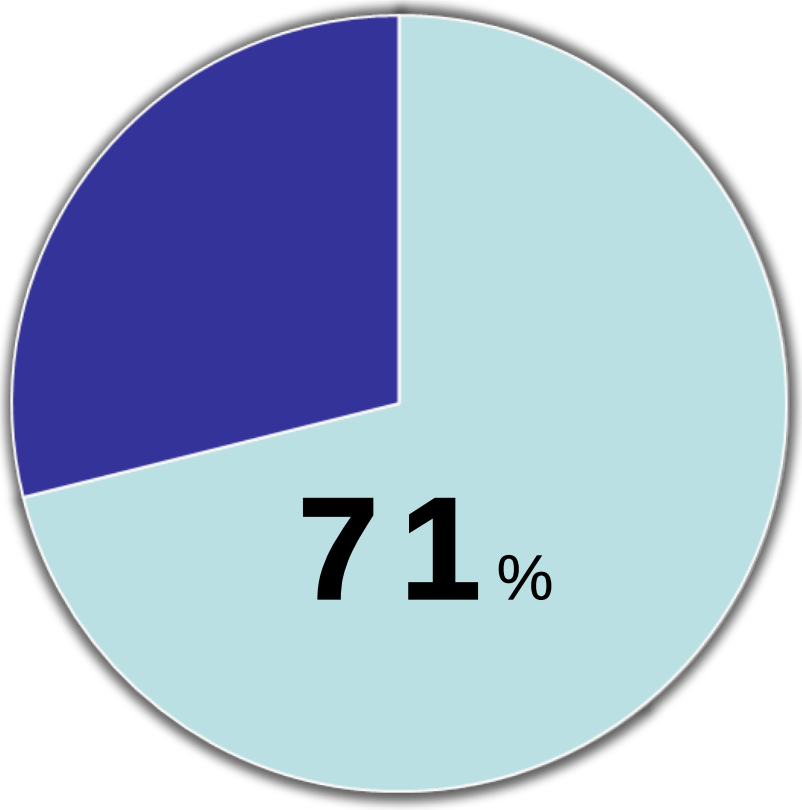


Honeypot coverage

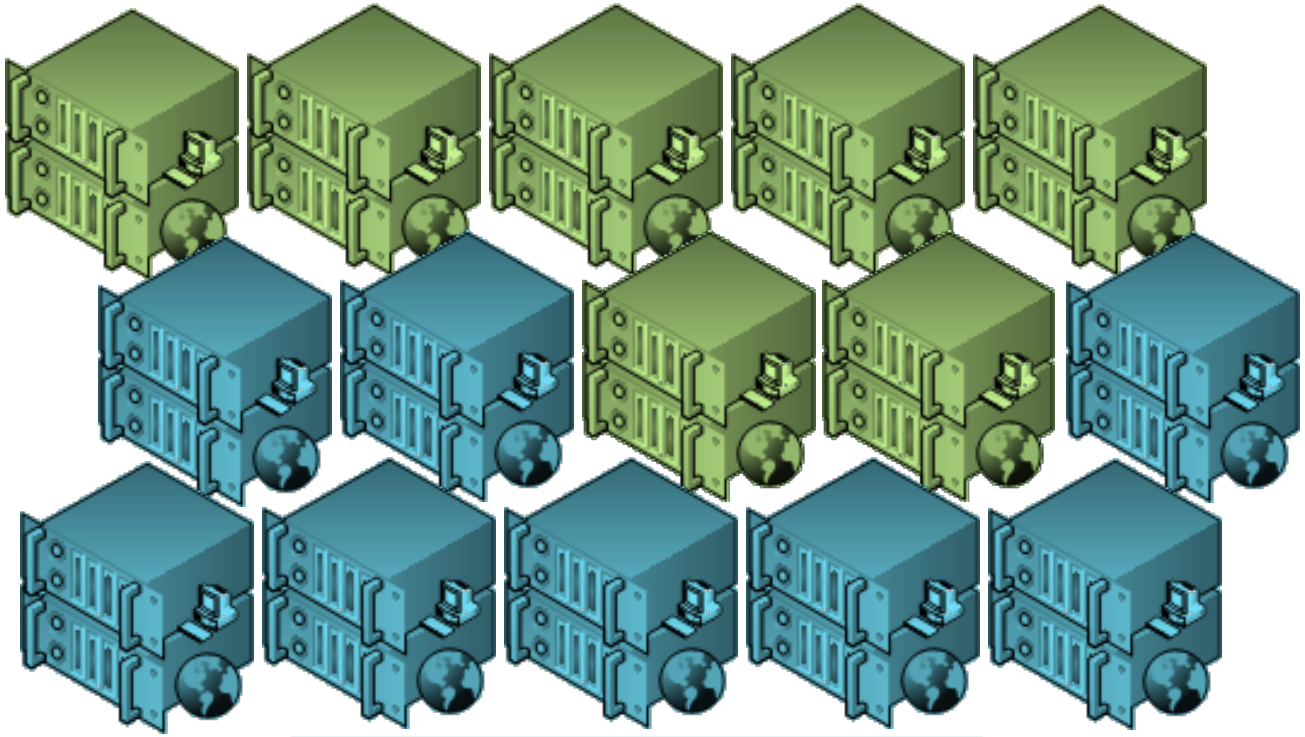
/16 block count
(Honeypot)



/16 block count
(Attack source)

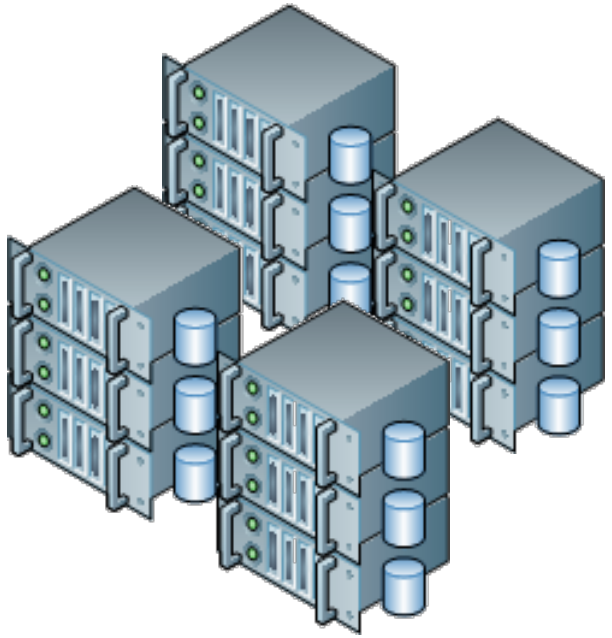


Honeypot improvement



Windows client type
(XP + 2000)

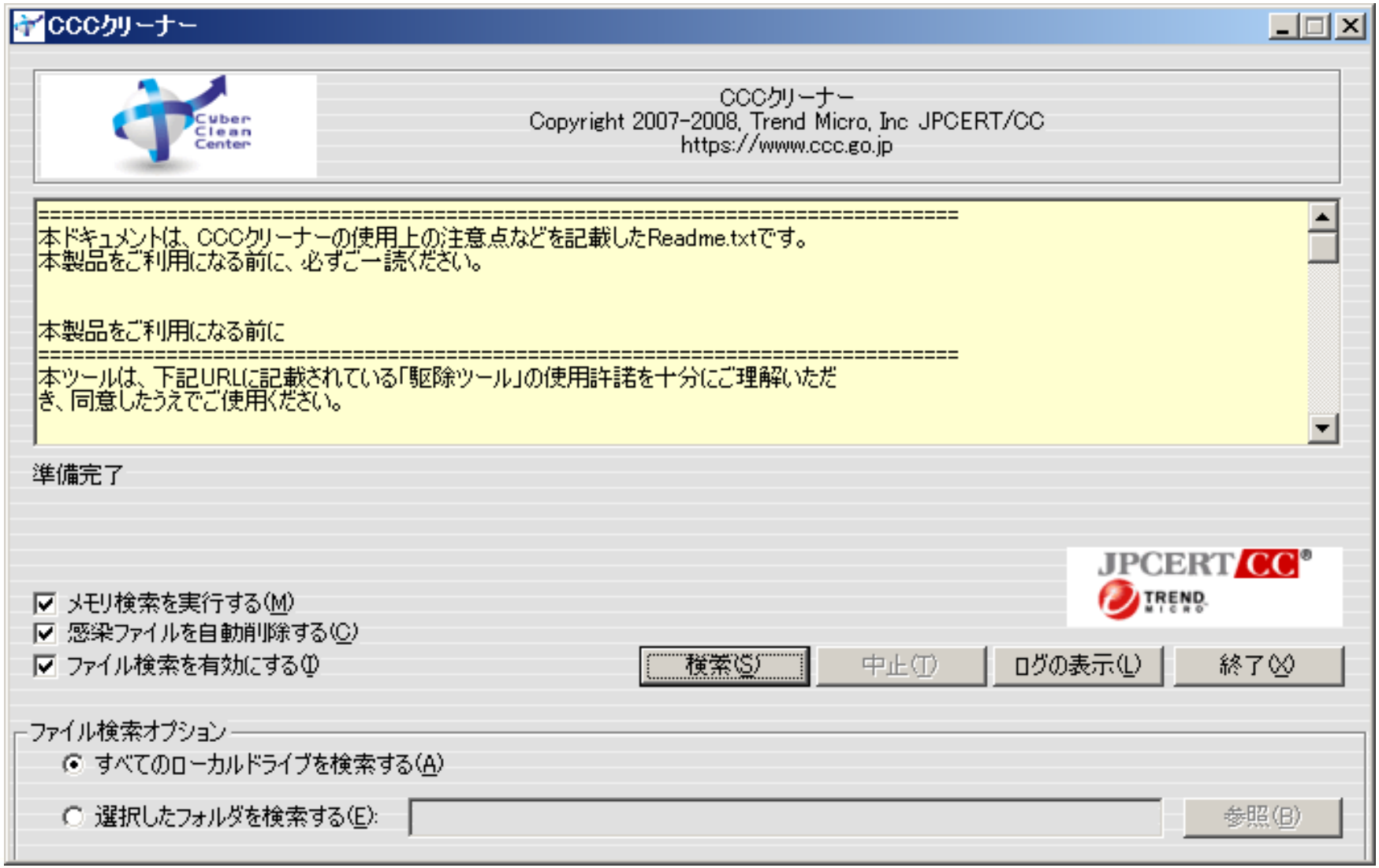
[redacted] + [redacted]



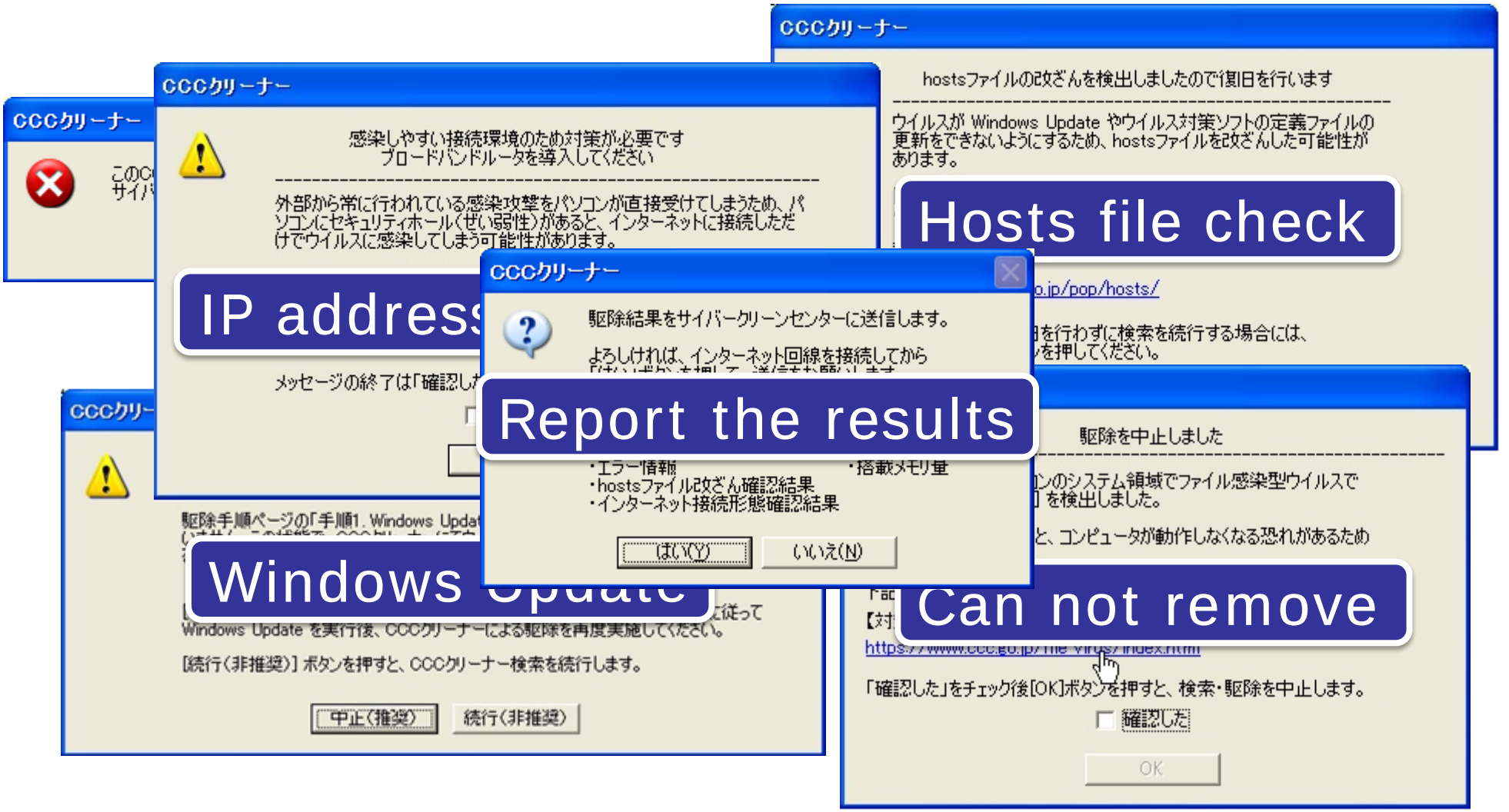
Exploit emulation

[redacted]

CCC Cleaner enhancement

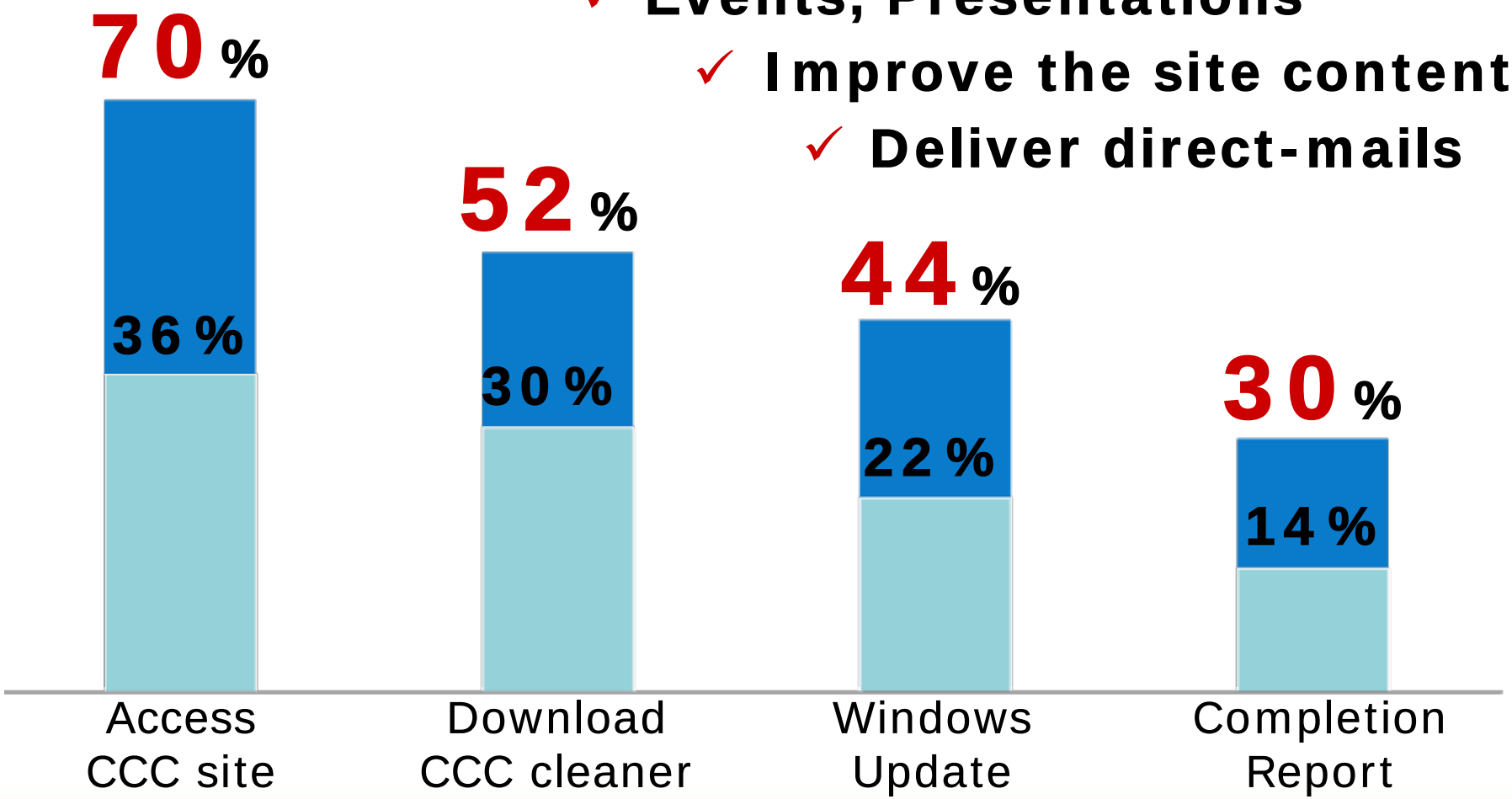


CCC Cleaner enhancement



Activities of infected users

- ✓ TV shows, Newspapers, Magazines
- ✓ Events, Presentations
- ✓ Improve the site contents
- ✓ Deliver direct-mails

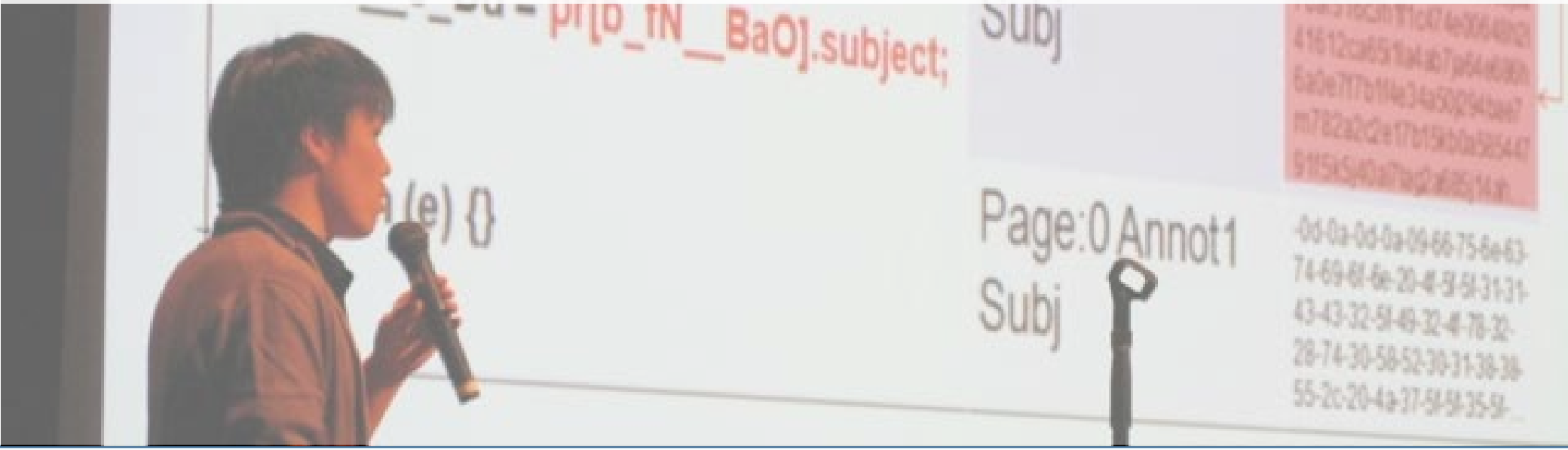


International cooperation

- **Information sharing**
- **Incident response**

Human resource development

- **anti-Malware engineering WorkShop (MWS)**
  - —Using "CCC's data" as shared dataset
  - —http://www.iwsec.org/mws/2010/en.html



Human resource development

- **IT specialist program to promote Key Engineers as securitY Specialists (IT Keys)**
  - —http://www.iwsec.org/mws/2010/en.html

ACHIEVEMENTS

Statistics

17,426,320 samples

(**1,992,928** unique samples)

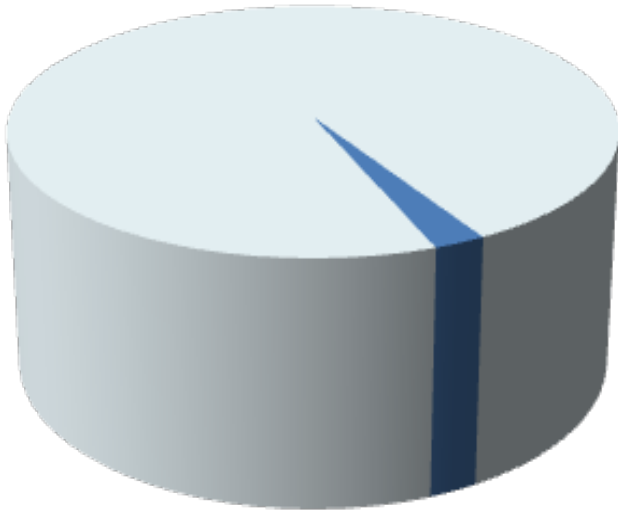
30,217 hash-unique unknown samples

206 updates

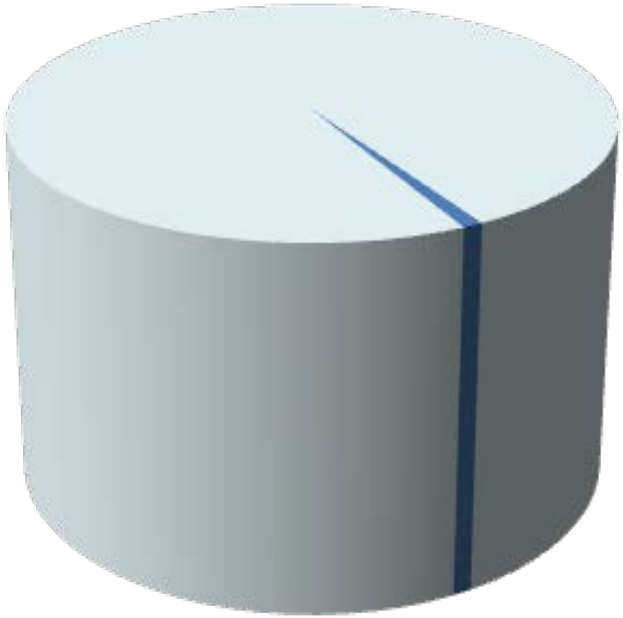
536,628 emails for **108,726** users

Infected PCs

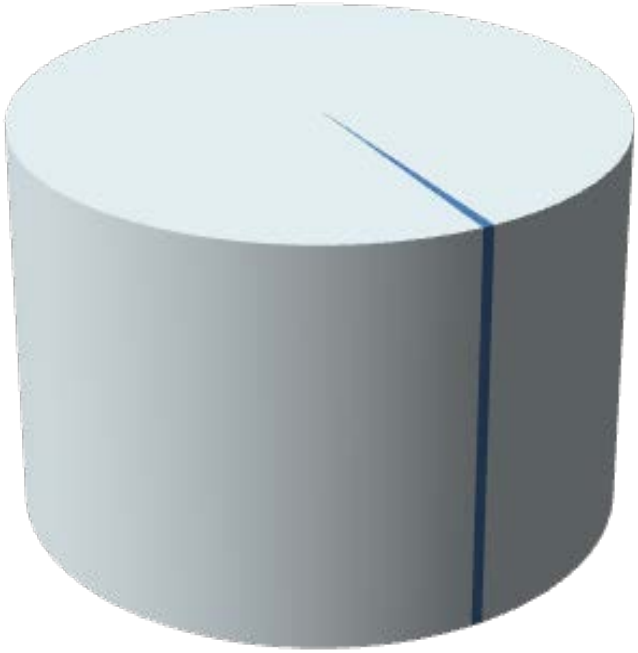
In **2005**
2.0~2.5%
450,000users



In **2008**
1.0%
300,000users



In **2010**
0.6%
190,000users



CCC as a best practice

- ITU-T Study Group 17

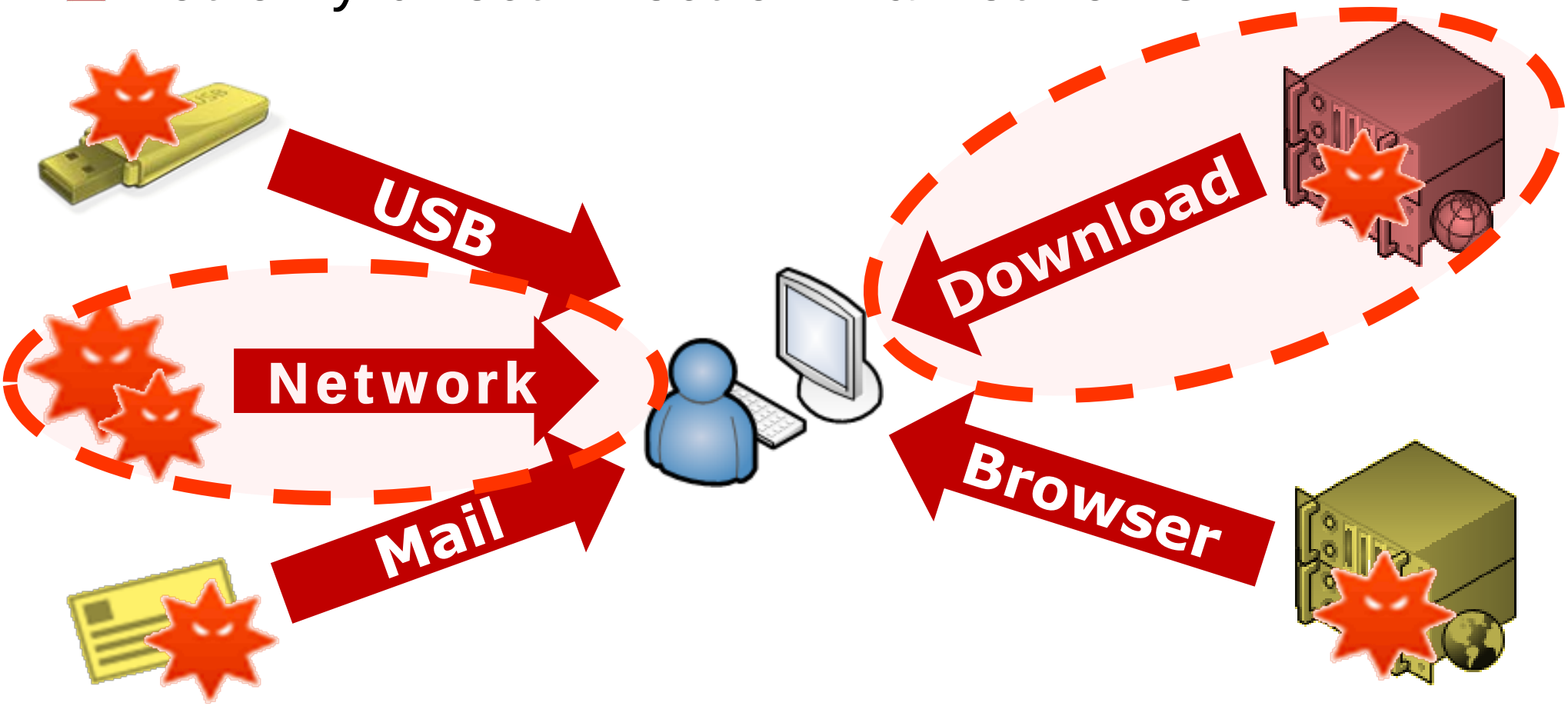
ITU-T X.1205
Overview of cybersecurity
(Approved on 2008-04-18)

ITU-T X.1205
Supplement on best practices against botnet threats
(Approved on 2010-12-17)

EXISTING ISSUES

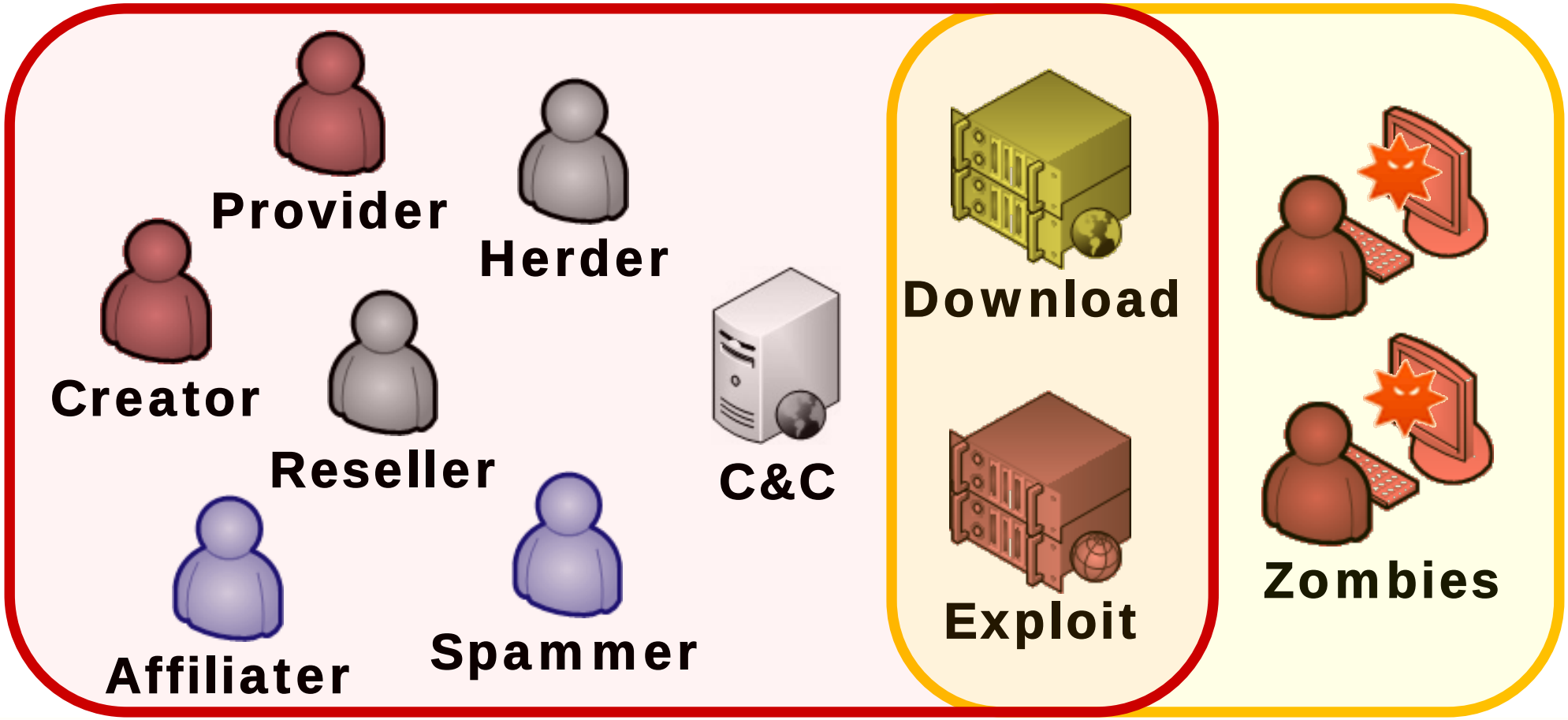
Attack vector

- Not only direct infection via networks



Countermeasure approach

- Considering other ways to reduce malwares



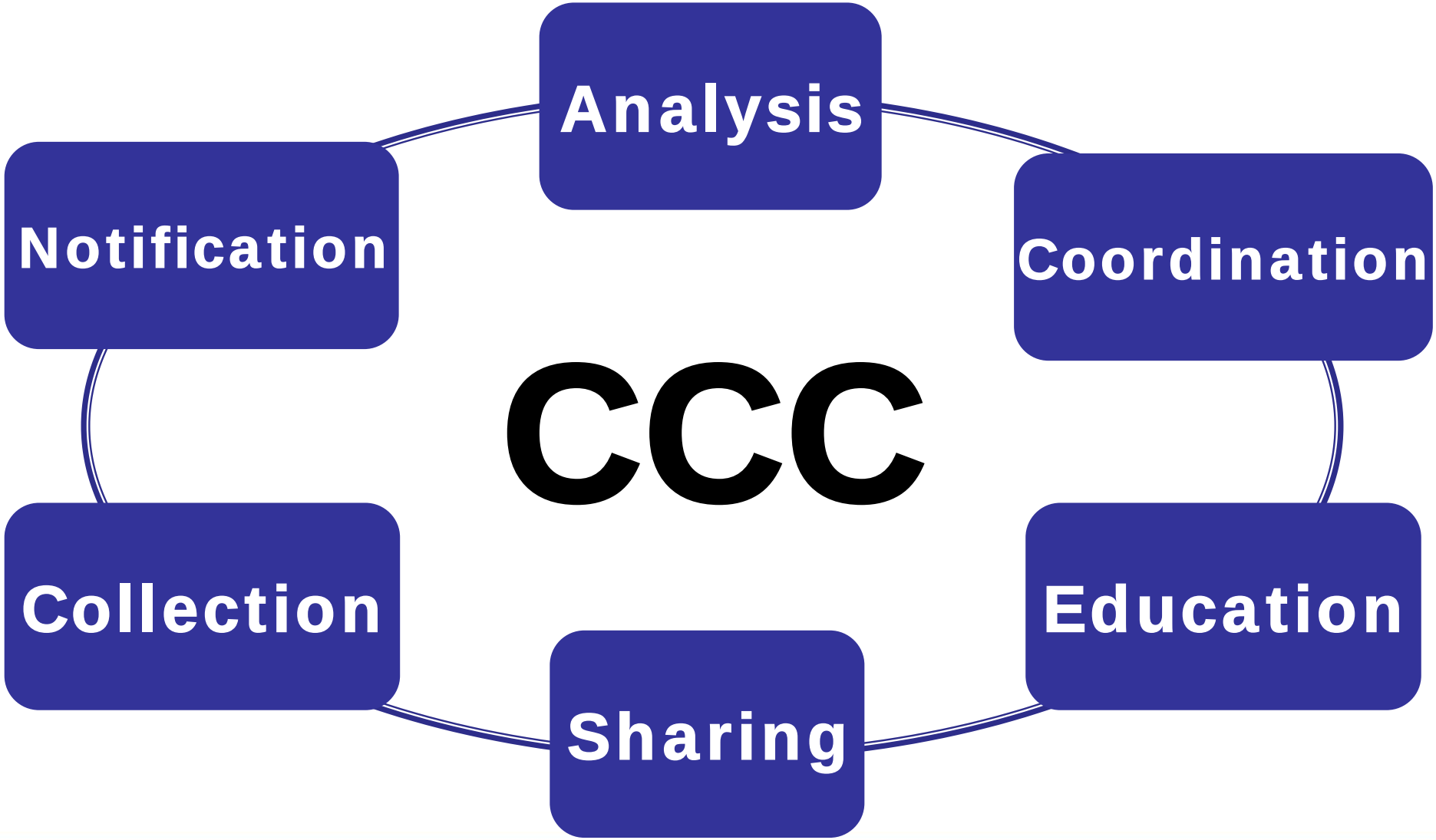
CCC as a national project

- a 5 year project

http://www.flickr.com/photos/chaojikazu/531004191/

CURRENT STATUS

Cyber Clean Center Council?



Thank You!

Web: https://www.ccc.go.jp/en_index.html
https://www.jpcert.or.jp/

Email: aa-info@jpcert.or.jp