

Cyber Clean Center Project

- A five year retrospective -

You NAKATSURU
JPCERT Coordination Center
Analysis Center

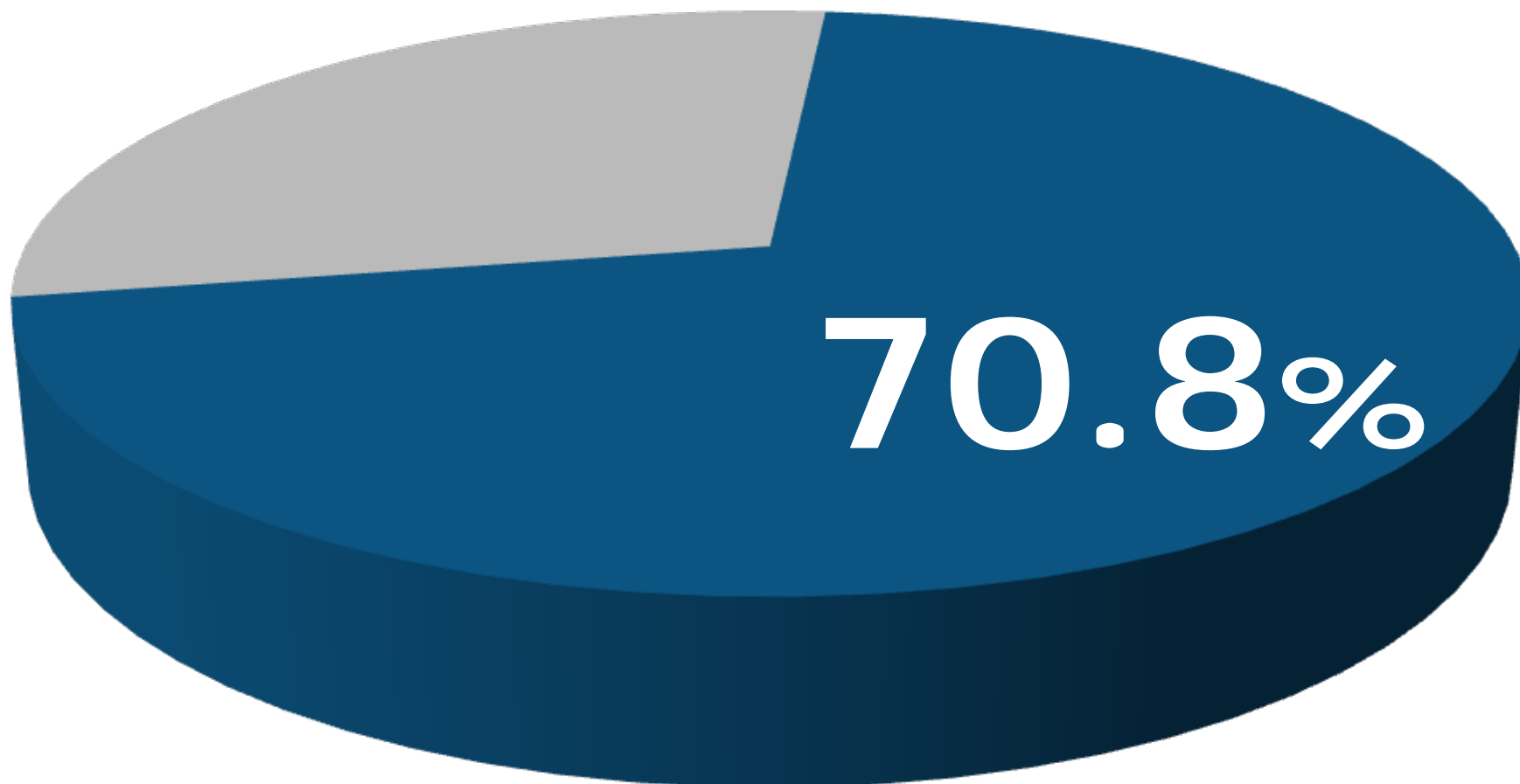
Agenda

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

BACKGROUND

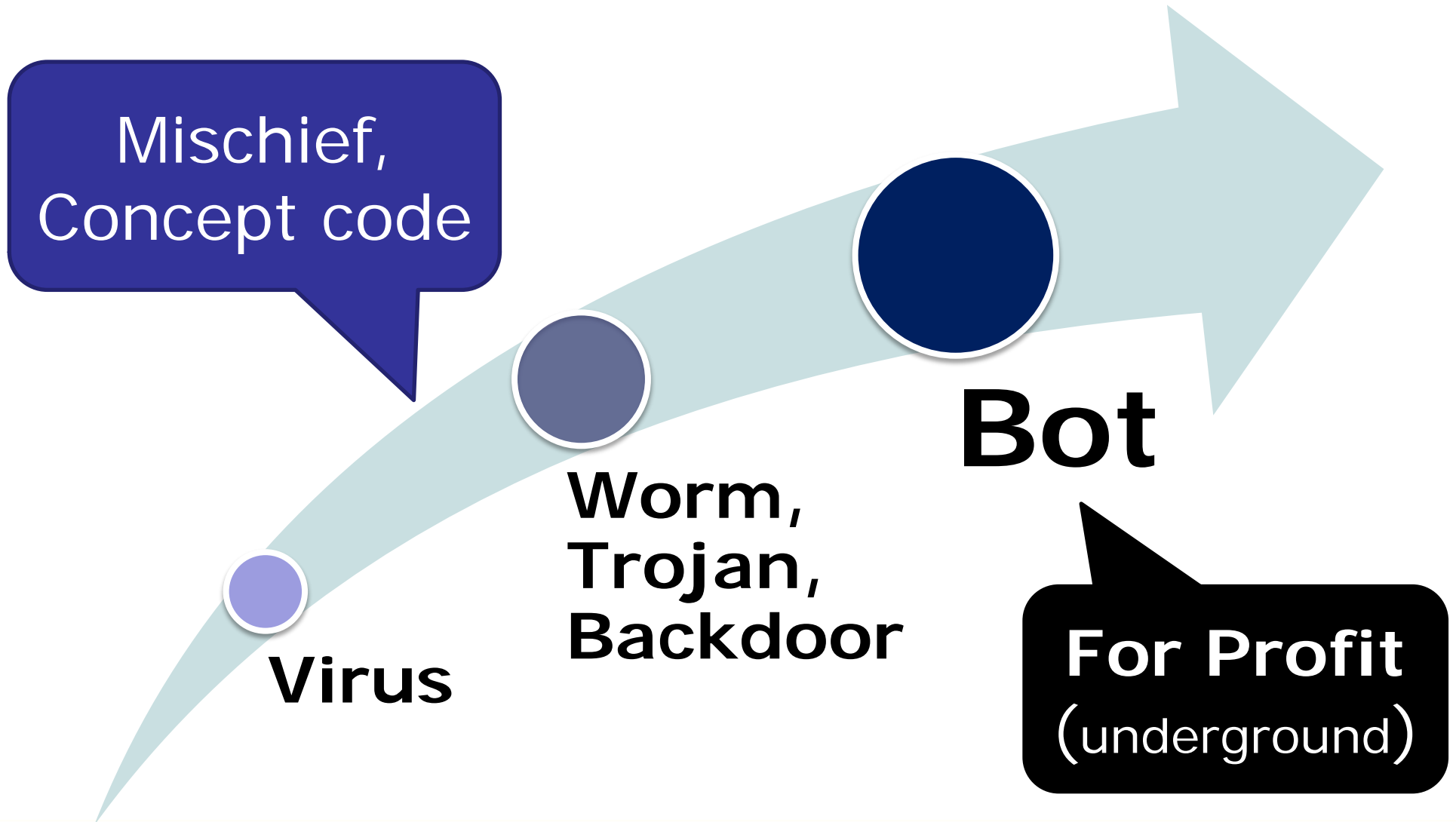
- JAPANESE SITUATION -

Internet users in 2005



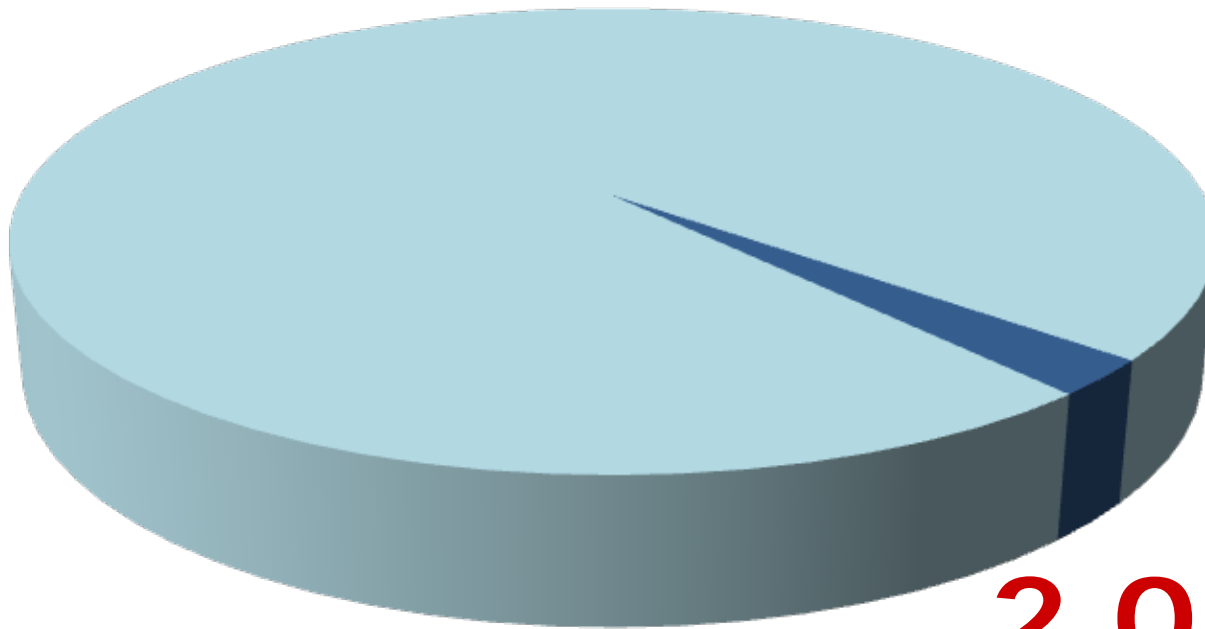
source: MIC "Internet users as a proportion of the population"
<http://www.soumu.go.jp/johotsusintokei/english/>

Growth of malware until 2005



Infected PCs in 2005

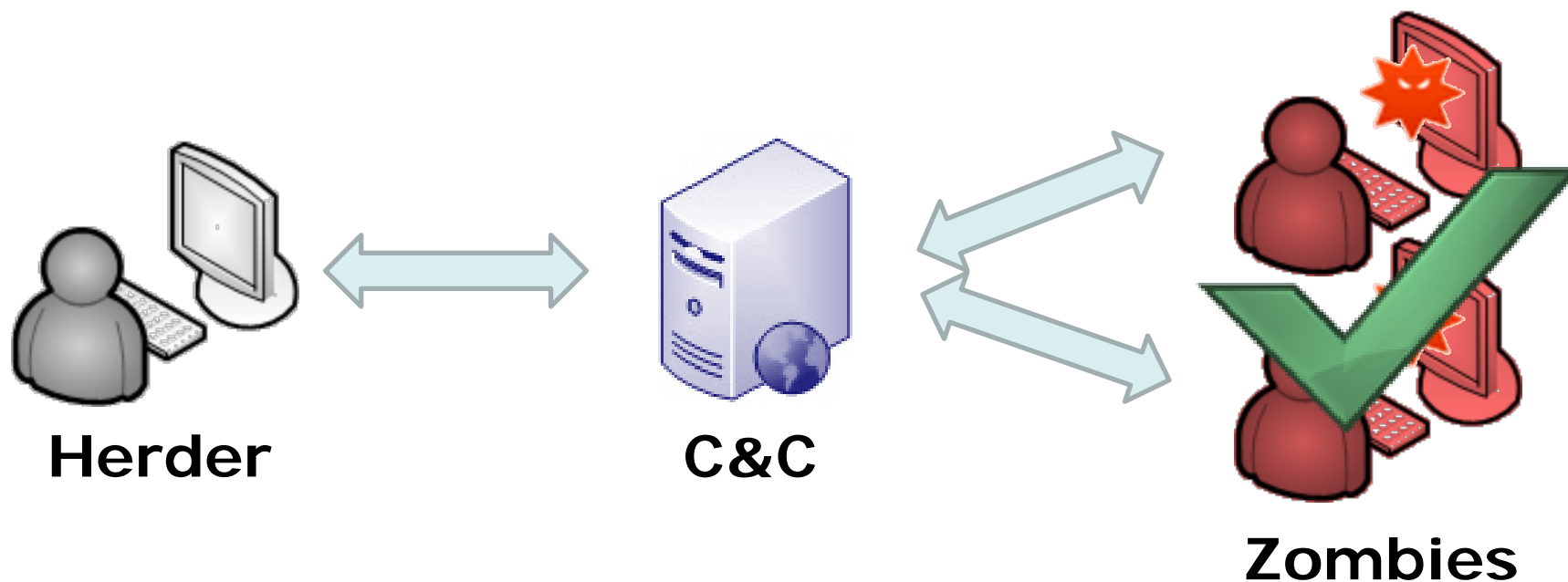
■ Targeted "broad-band users"



2.0 ~ 2.5%

400,000 users

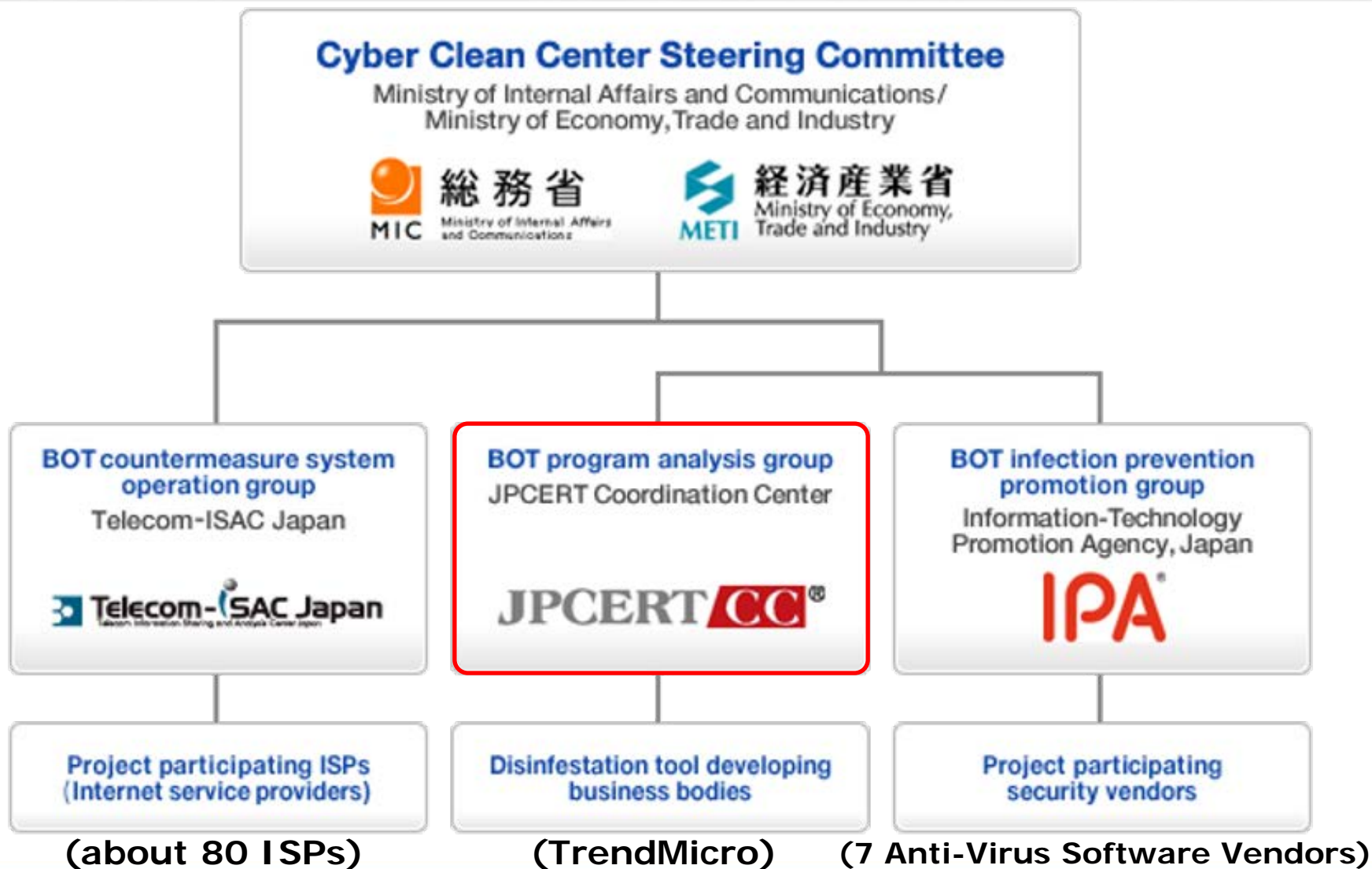
Our Decision



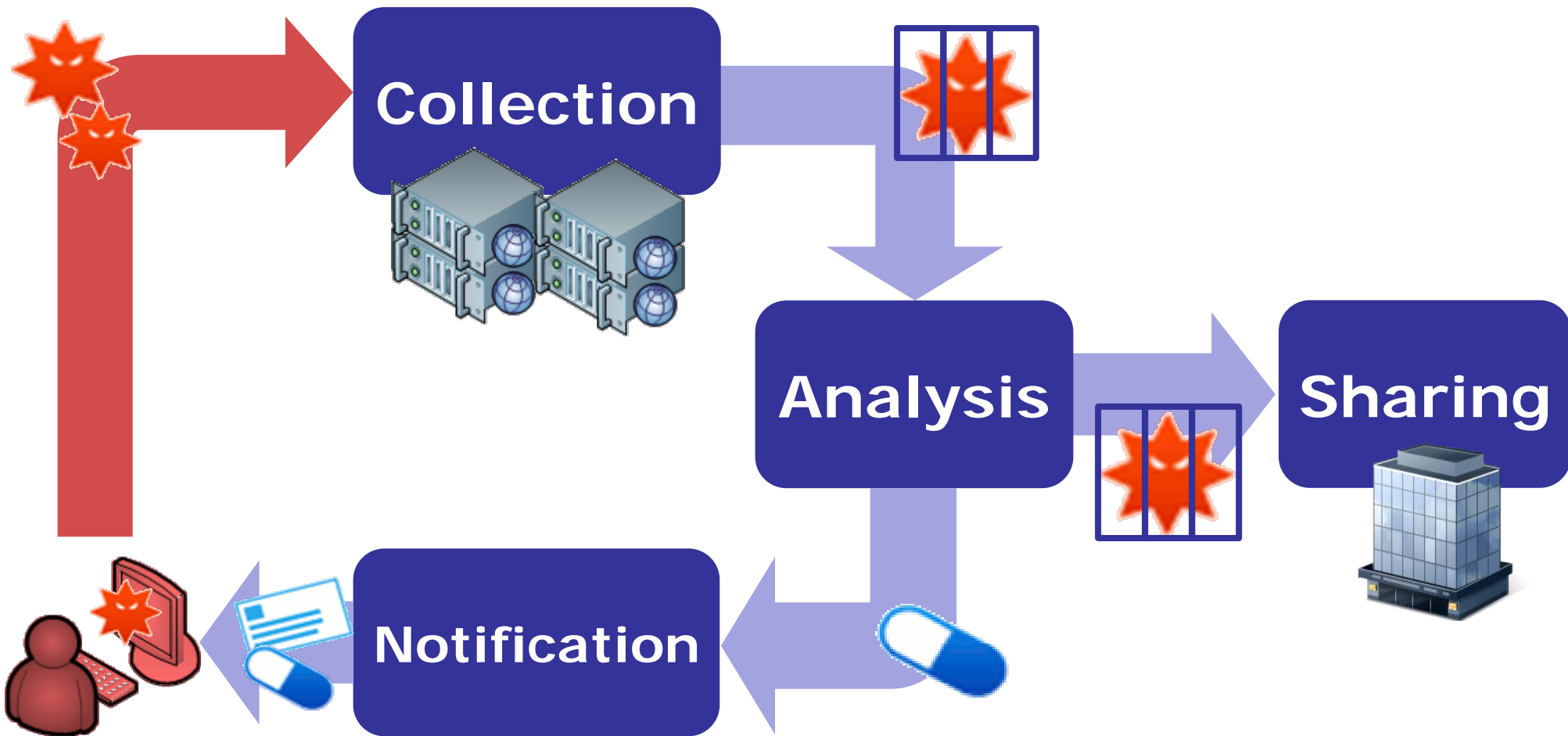
- It's easy to reach infected users.
- It's a good idea to develop user literacy.

THE CYBER CLEAN CENTER

Organization Chart



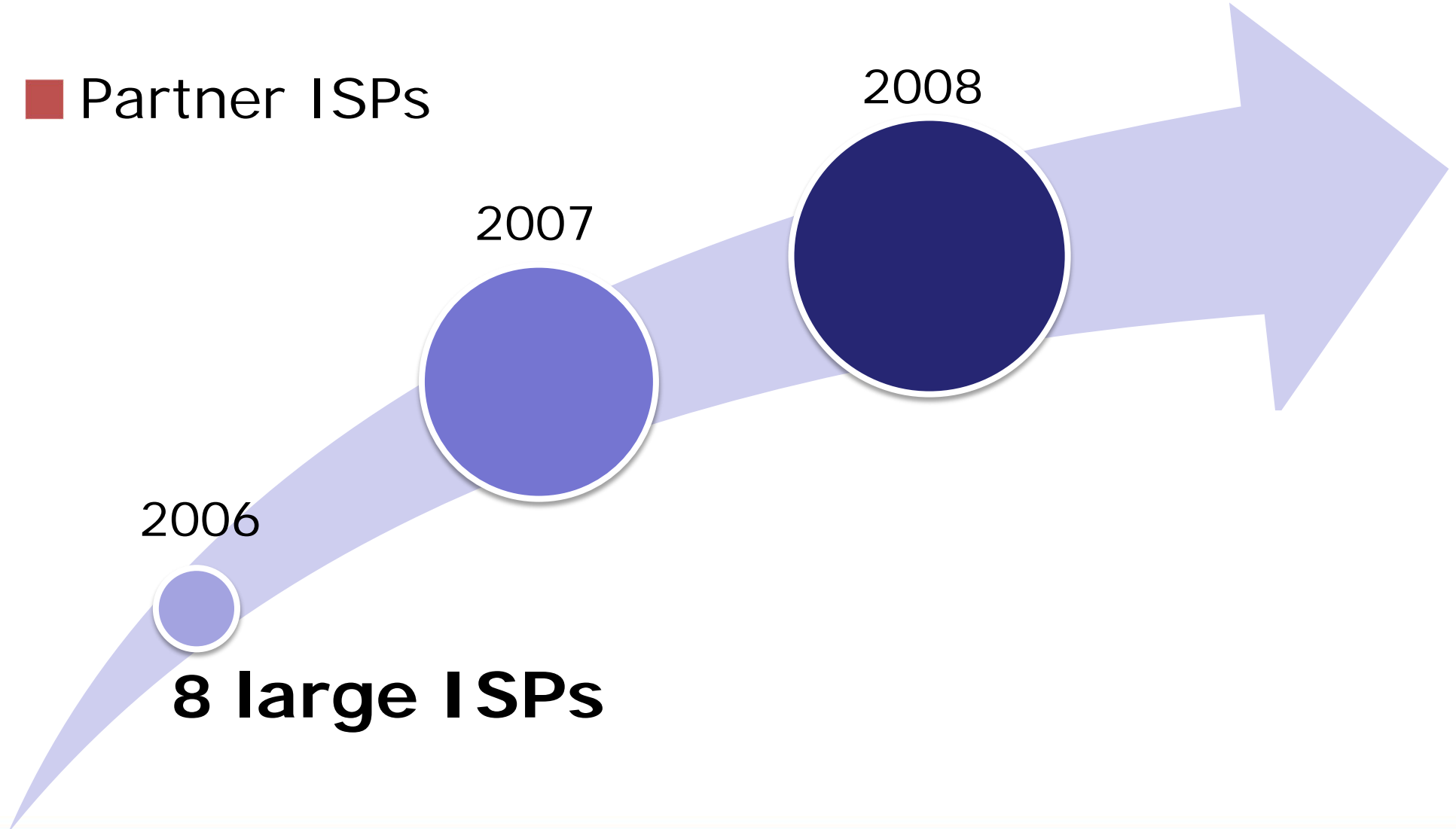
Operational Framework



SEEING THE EFFECT

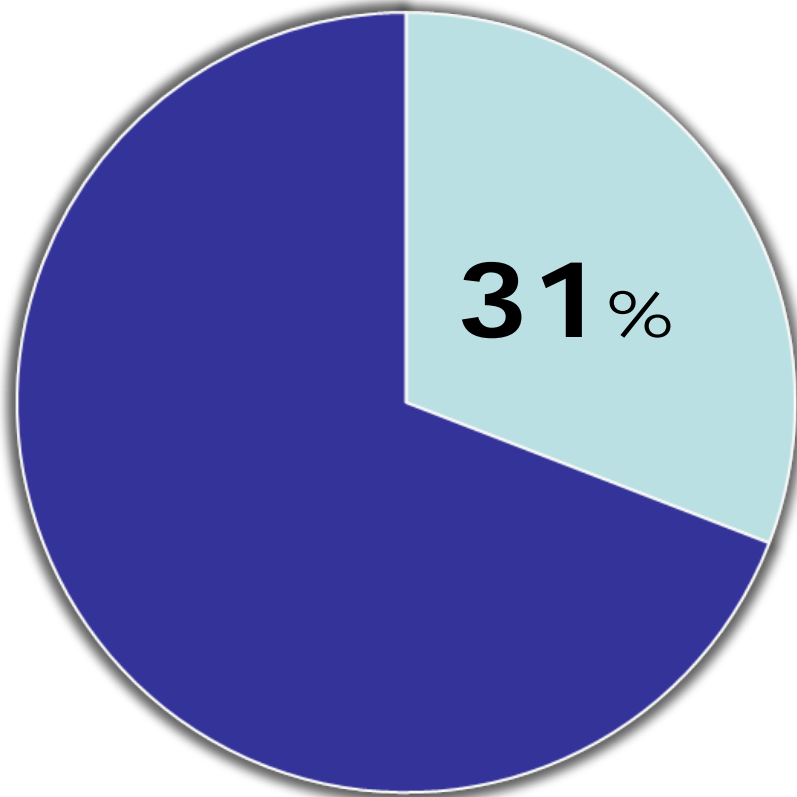
User coverage

■ Partner ISPs

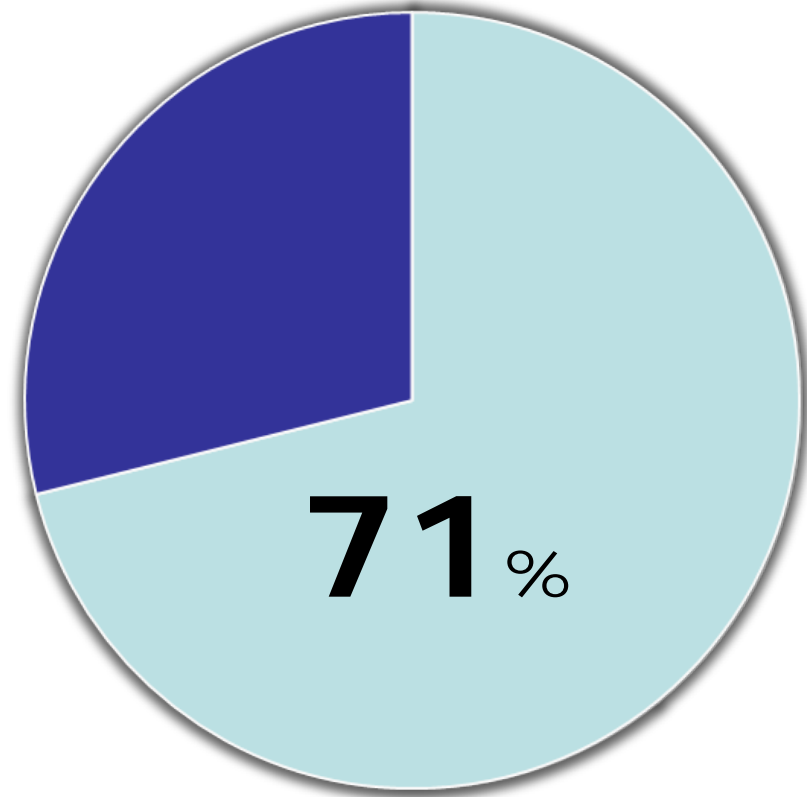


Honeypot coverage

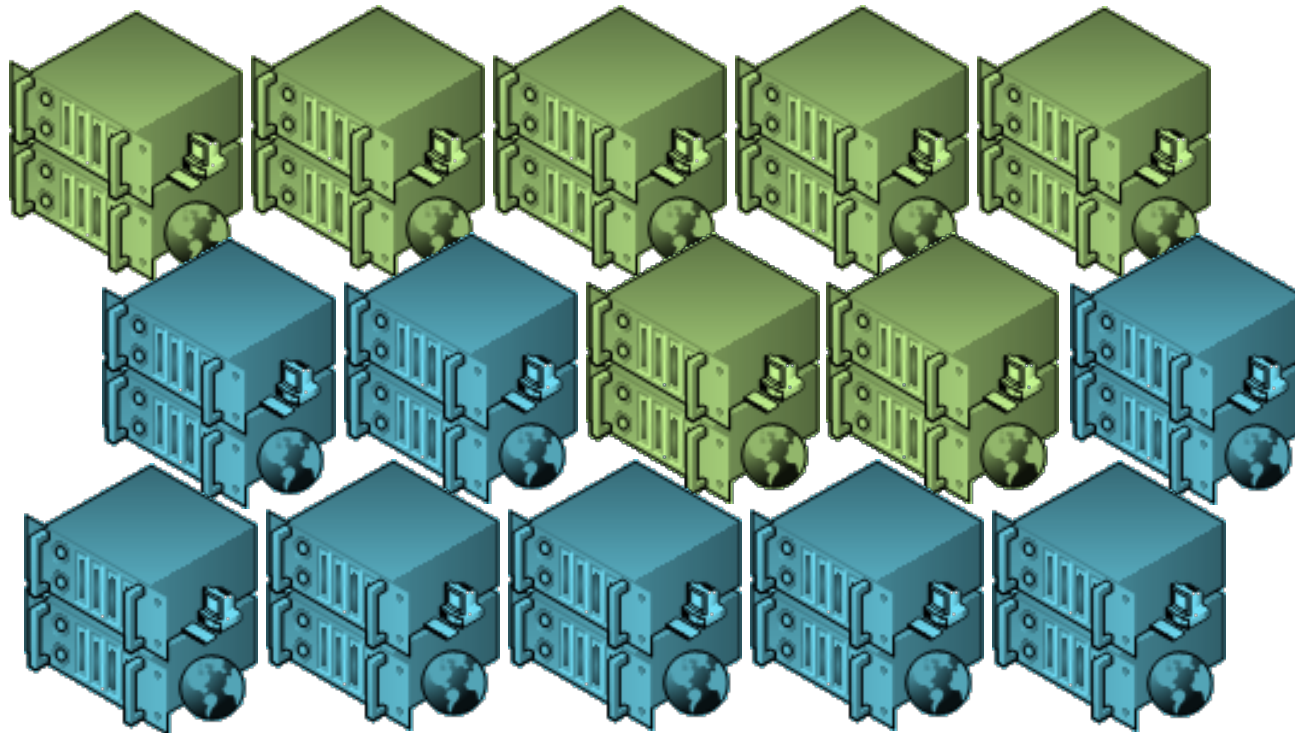
/16 block count
(Honeypot)



/16 block count
(Attack source)

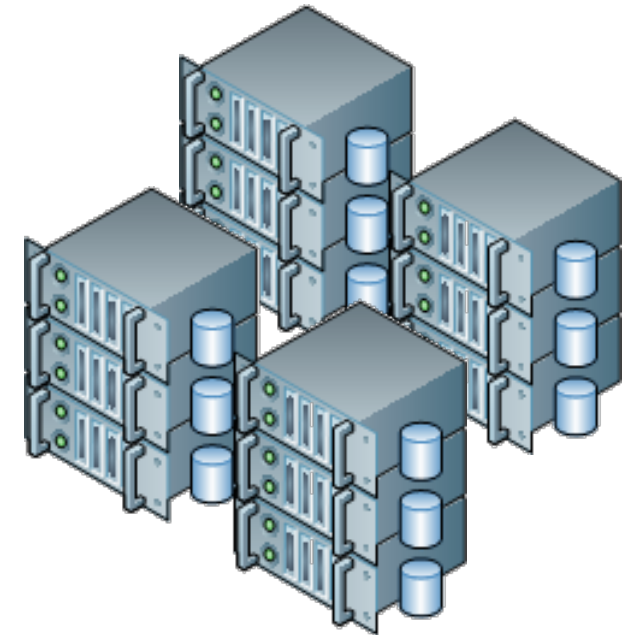


Honey pot improvement



Windows client type
(XP + 2000)

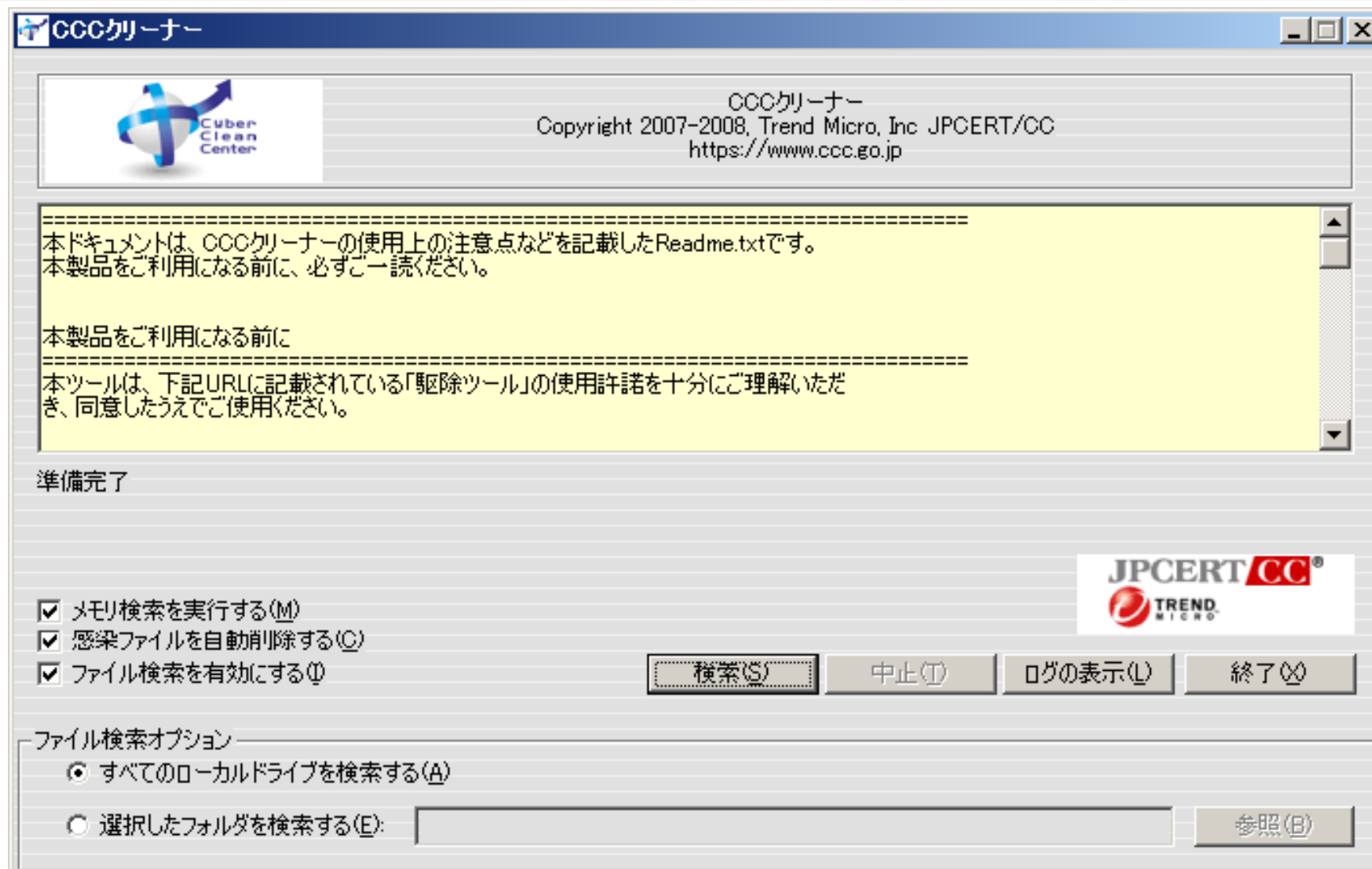
30 + 30



Exploit emulation

20

CCC Cleaner enhancement



CCC Cleaner enhancement

The image displays several overlapping screenshots of the CCC Cleaner application interface. The windows are titled "CCCクリーナー" (CCC Cleaner). The screenshots show various stages of the cleaning process and user prompts:

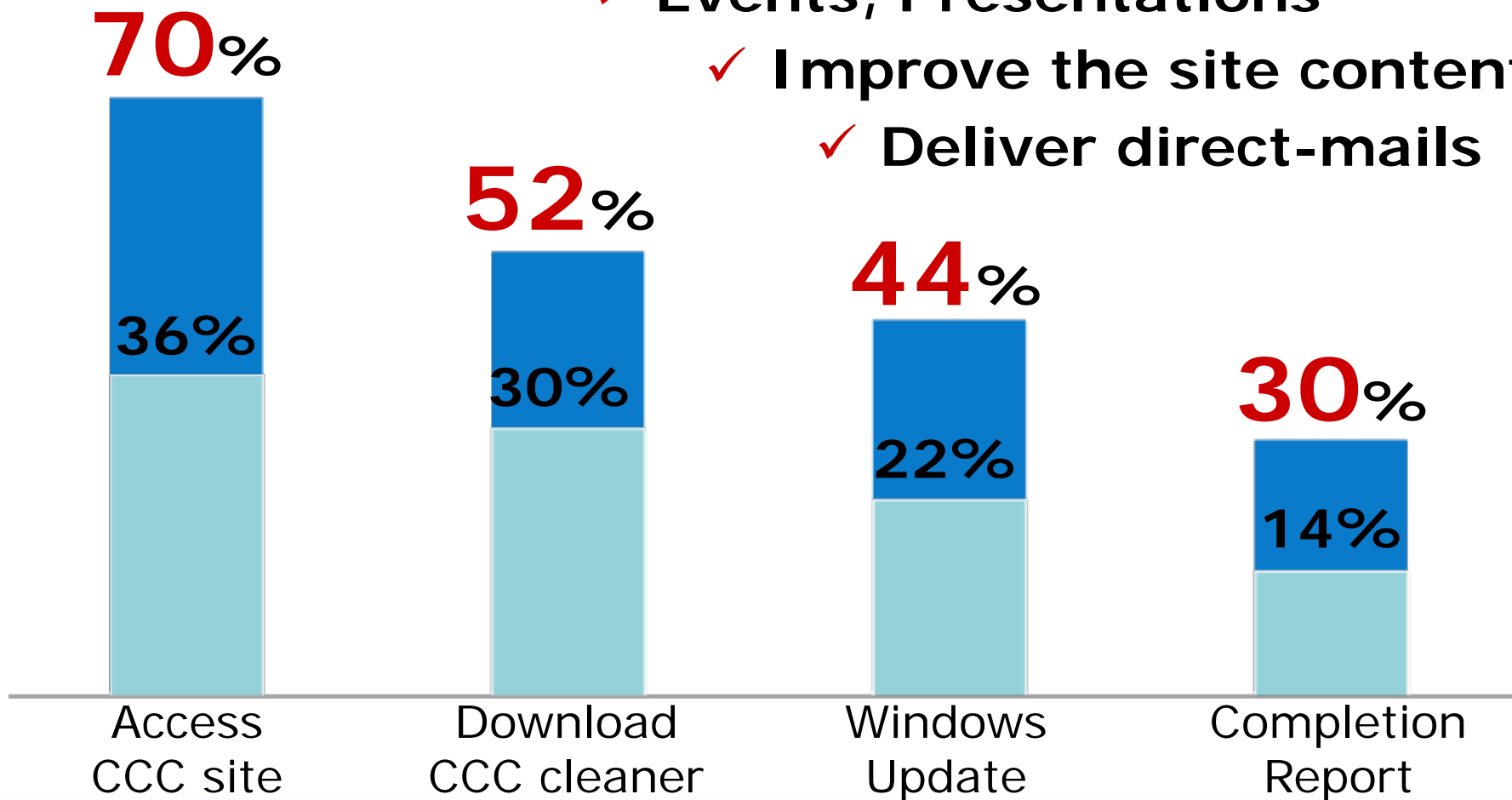
- IP address:** A window with a yellow warning icon and a red 'X' icon. The text reads: "感染しやすい接続環境のため対策が必要です。ブロードバンドルータを導入してください。" (Measures are necessary due to a connection environment that is easy to infect. Please introduce a broadband router.)
- Hosts file check:** A window with a yellow warning icon. The text reads: "hostsファイルの改ざんを検出しましたので復旧を行います。ウイルスが Windows Update やウイルス対策ソフトの定義ファイルの更新をできないようにするため、hostsファイルを改ざんした可能性があります。" (We detected tampering with the hosts file, so we will restore it. Because viruses can prevent Windows Update or antivirus software definition files from being updated, there is a possibility that the hosts file has been tampered with.)
- Report the results:** A window with a question mark icon. The text reads: "駆除結果をサイバークリーンセンターに送信します。よろしければ、インターネット回線を接続してから..." (We will send the removal results to the Cyber Clean Center. If possible, please connect to the Internet before...)
- Windows update:** A window with a yellow warning icon. The text reads: "駆除手順ページの「手順1. Windows Update」に従って Windows Update を実行後、CCCクリーナーによる駆除を再度実施してください。" (Please follow the "Step 1. Windows Update" on the removal procedure page, run Windows Update, and then perform removal again using CCC Cleaner.)
- Can not remove:** A window with a yellow warning icon. The text reads: "駆除を中止しました。このシステム領域でファイル感染型ウイルスを検出しました。" (Removal has been stopped. A file-infecting virus was detected in this system area.)

Overlaid on these screenshots are five blue callout boxes with white text:

- IP address**
- Hosts file check**
- Report the results**
- Windows update**
- Can not remove**

Activities of infected users

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



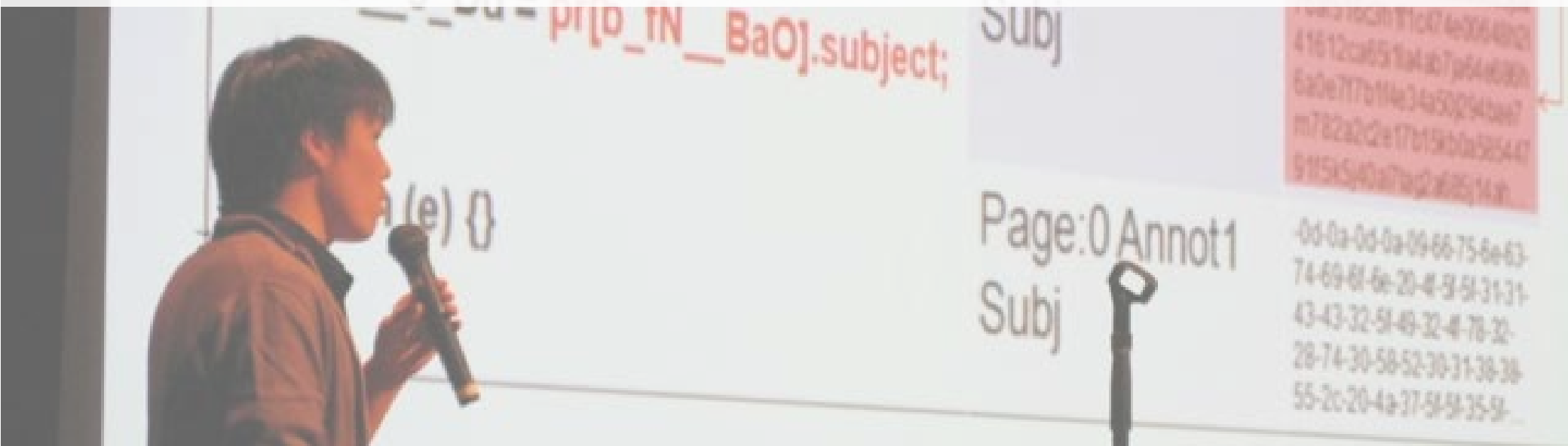
International cooperation

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

■ anti-Malware engineering WorkShop (MWS)

—Using "CCC's data" as shared dataset

—<http://www.iwsec.org/mws/2010/en.html>



■ IT specialist program to promote Key Engineers as security Specialists (IT Keys)

—<http://www.iwsec.org/mws/2010/en.html>



ACHIEVEMENTS

17,426,320 samples
(1,992,928 unique samples)

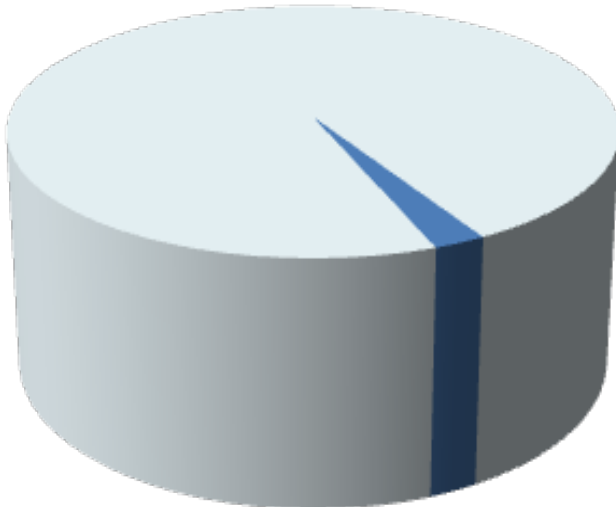
30,217 hash-unique unknown samples

206 updates

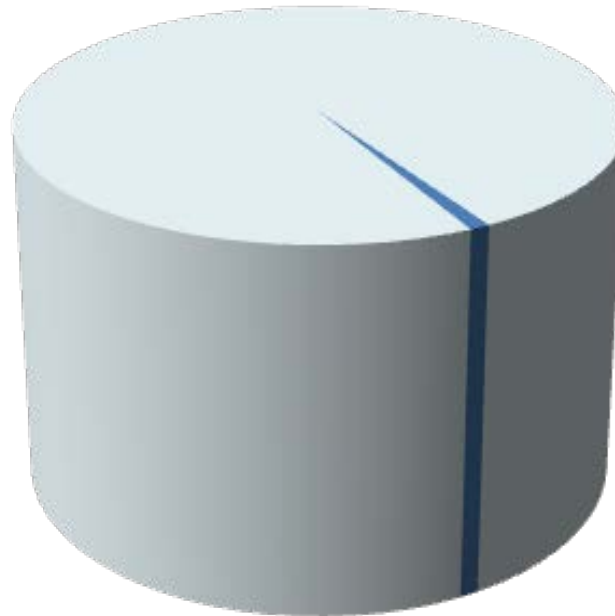
536,628 emails for **108,726** users

Infected PCs

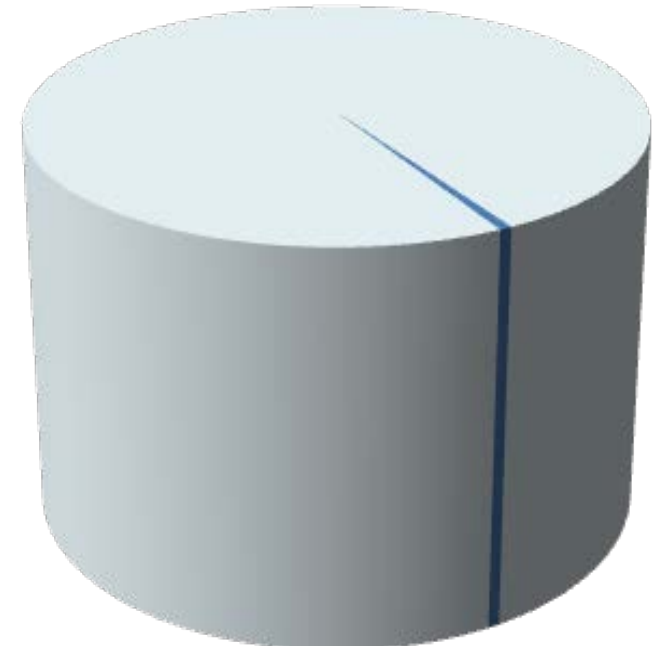
In **2005**
2.0 ~ 2.5%
450,000users



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



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



■ ITU-T Study Group 17

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

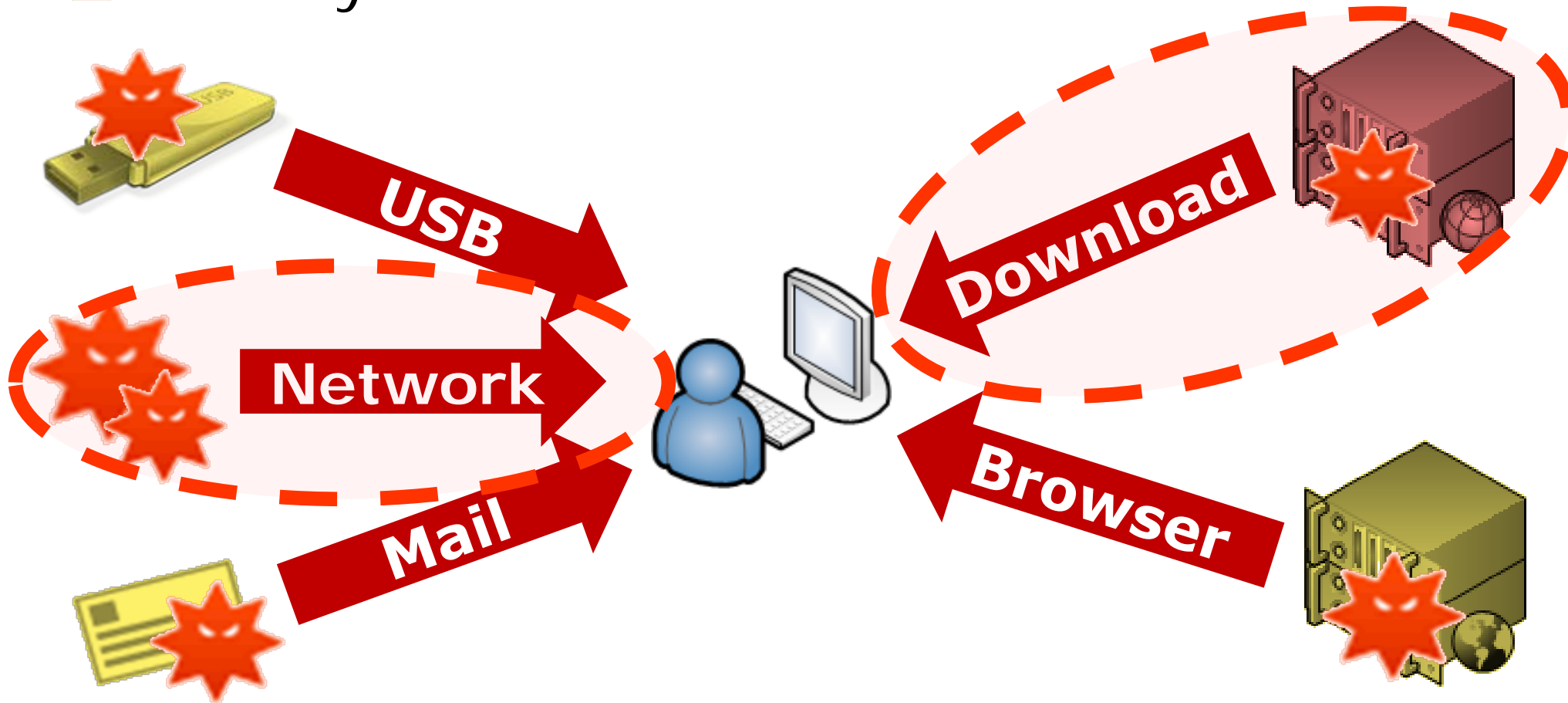


ITU-T X.1205
Supplement on best practices
against botnet threats
(Approved on 2010-12-17)

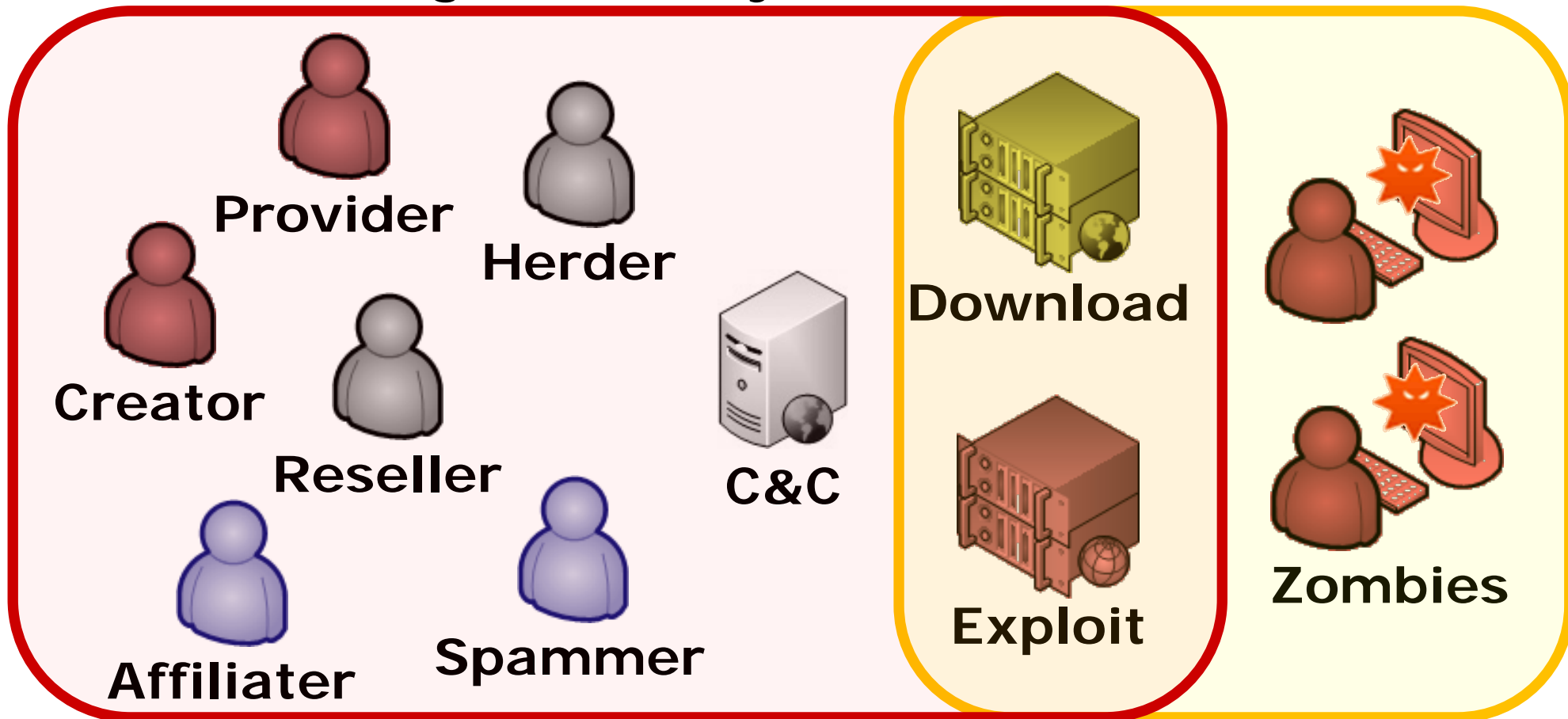
EXISTING ISSUES

Attack vector

■ Not only direct infection via networks



■ Considering other ways to reduce malwares



CCC as a national project

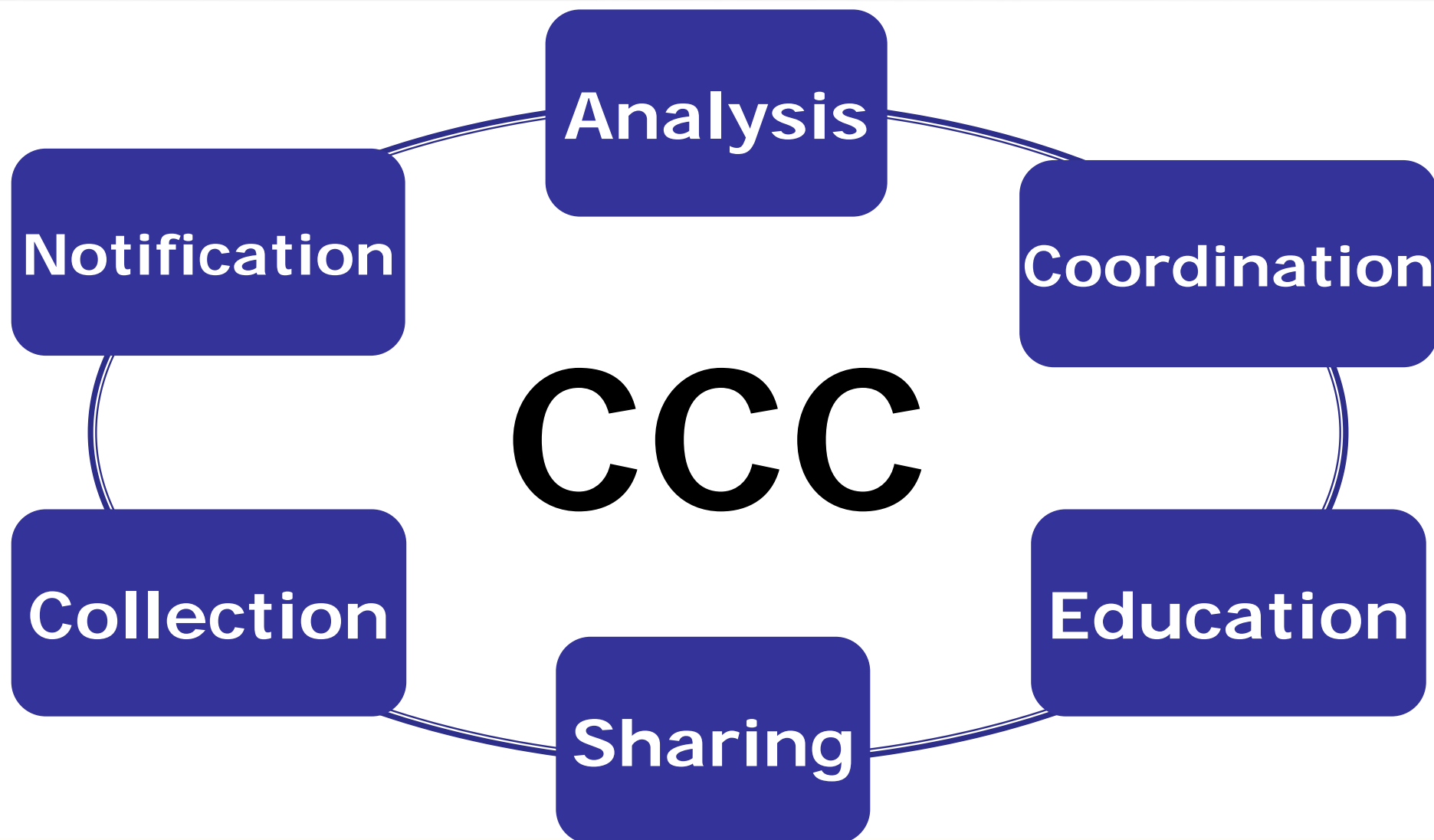
- a 5 year project



<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