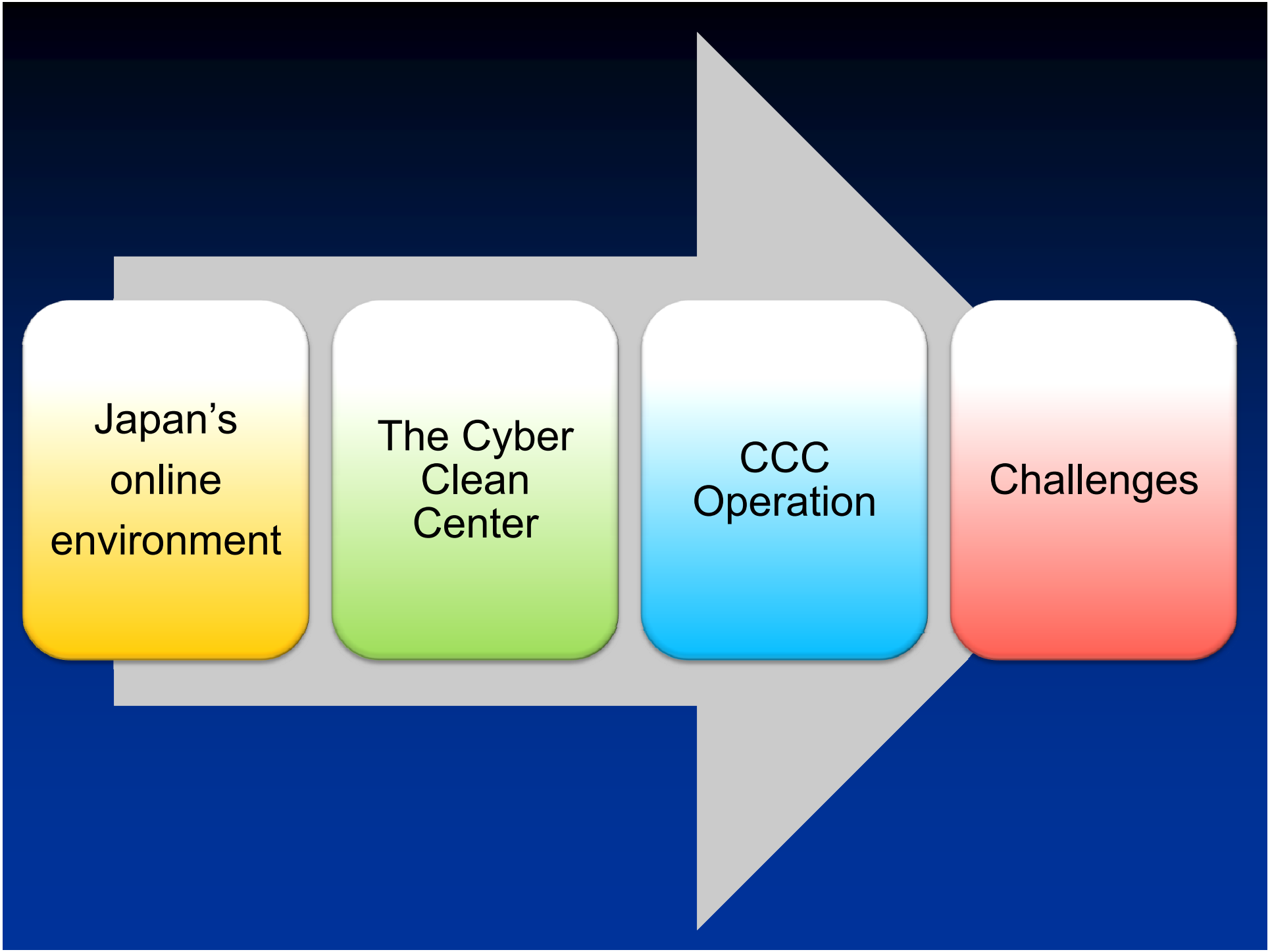
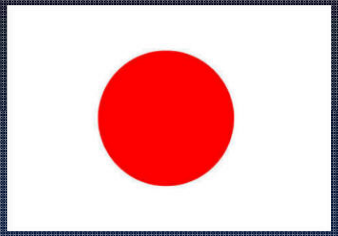
JPCERT CC®
Japan Computer Emergency Response Team Coordination Center
JPCERTコーディネーションセンター

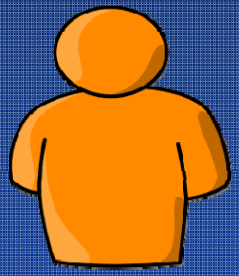
Anti-bot Countermeasures in Japan: Cyber Clean Center Update

Chris Horsley / Takashi Manabe
JPCERT/CC


Japan's online environment
The Cyber Clean Center
CCC Operation
Challenges



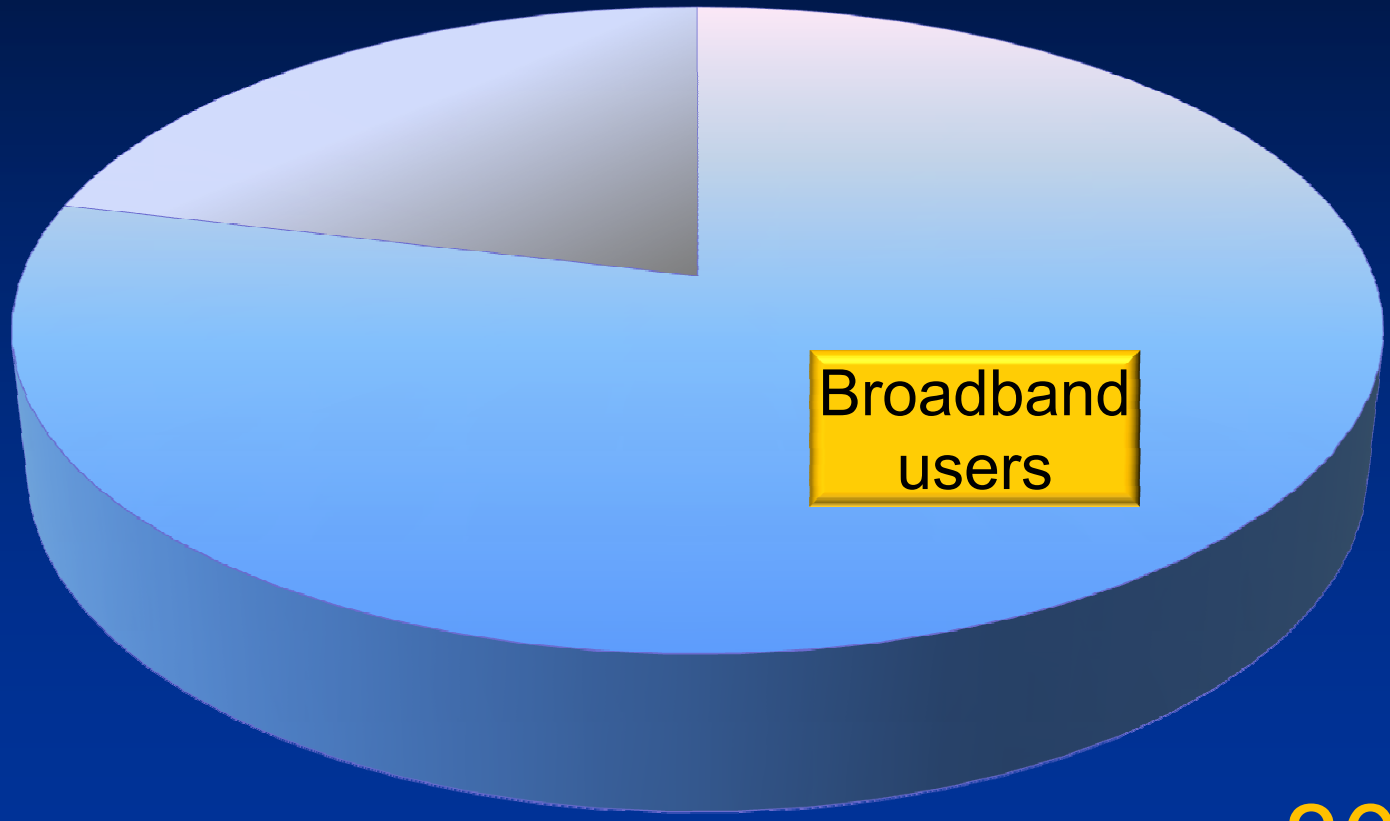
127 M

340  /km^2

31  /km^2

2.5  /km^2

Japan’s online environment



~80%

Average connection:

93.6 Mbps

$34.21 USD per month

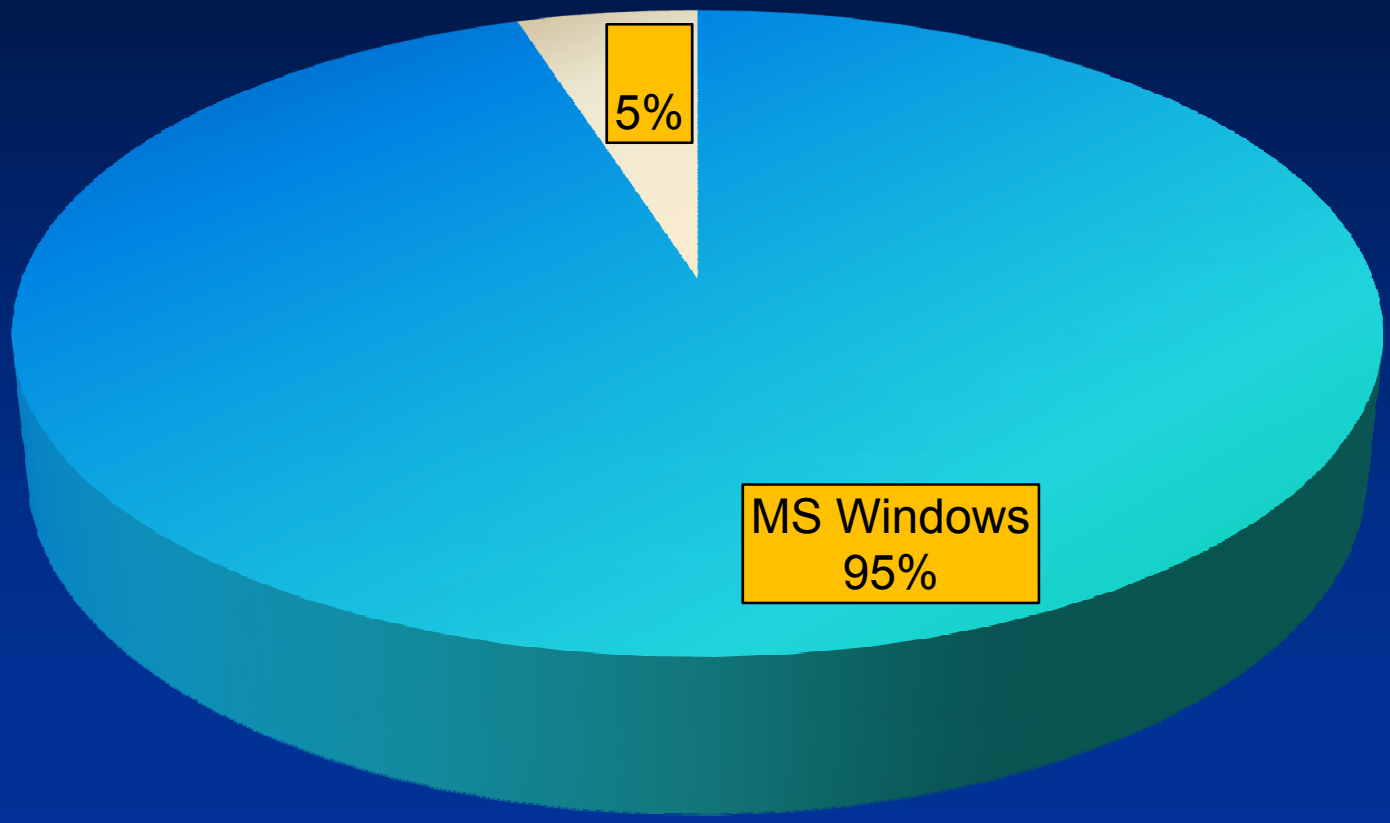
E-banking penetration:

45.9%

V

Google 日本

OS share



Threats

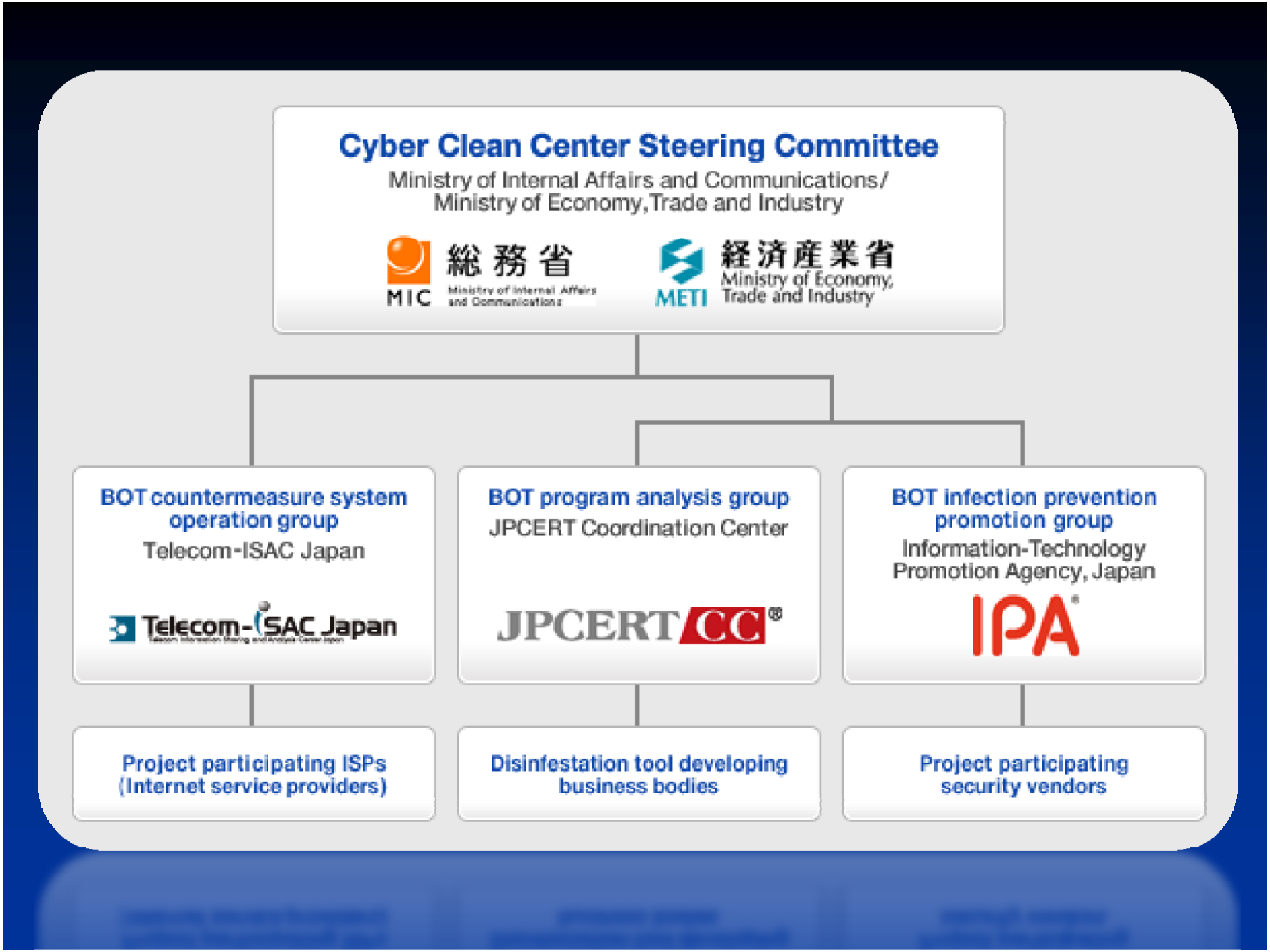
- Regional specialties
  - Winnie (P2P) data disclosure
- The usual
  - Malicious email attachments
    - Bots
  - SQL injection / malicious web sites
  - Targeted

Intro to the

Cyber Clean Center

(CCC)

A tool for cleaning botnet infections


Cyber Clean Center Steering Committee
Ministry of Internal Affairs and Communications/
Ministry of Economy,Trade and Industry
総務省
MIC
Ministry of Internal Affairs and Communications
経済産業省
METI
Ministry of Economy, Trade and Industry
BOT countermeasure system operation group
Telecom-ISAC Japan
Telecom-ISAC Japan
BOT program analysis group
JPCERT Coordination Center
JPCERT CC®
BOT infection prevention promotion group
Information-Technology Promotion Agency, Japan
IPA
Project participating ISPs (Internet service providers)
Disinfestation tool developing business bodies
Project participating security vendors

www.ccc.co.jp

Project coordinated between Ministry of Internal Affairs and Communications and Ministry of Economy, Trade and Industry

Cyber Clean Center

Cyber Clean Center

- What is BOT?
- What is Cyber Clean Center?
- Attention Rousing Activity
- Procedure of BOT cleaning
- Some hints to prevent BOT infection
- FAQ
- Links
- HOME (ENGLISH)
- JAPANESE

For your safety net life

BOT is a type of computer viruses and a program that a third party has developed with malicious intent to control your computer externally. Any computer could be infected by BOT once connected to the Internet. This site is to provide you information on how to clean BOT, as well as how to protect your computer from BOT.

INFORMATION

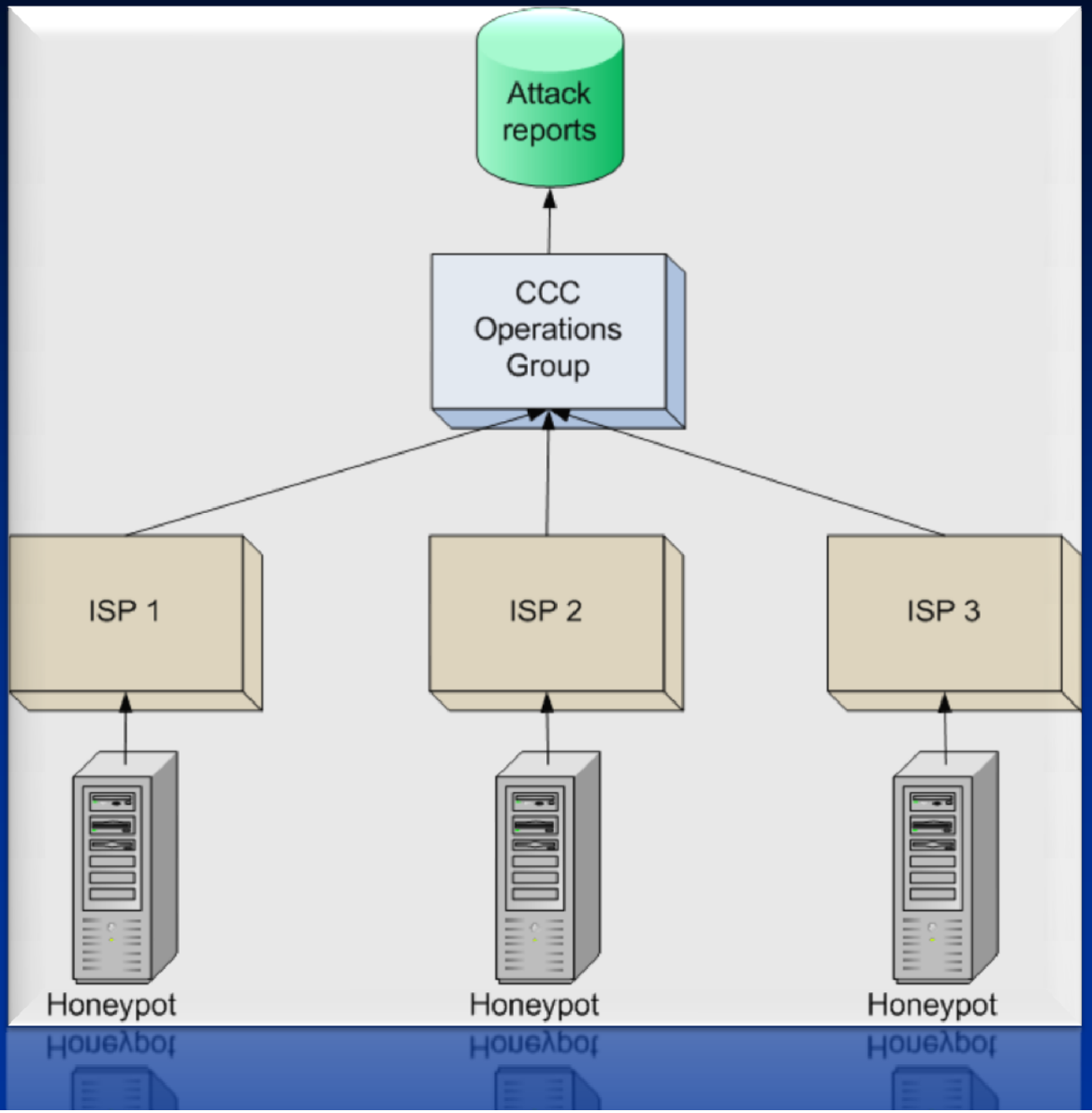
- Activity Report 2008-10
- Activity Report 2008-09
- Activity Report 2008-08
- Fiscal Year 2007 Activity Report on Cyber Clean Center(2008.10.07)

This is the FY 2007 activity report on "anti-bot measures project," jointly conducted by the Ministry of Internal Affairs and Communications(MIC) and the Ministry of Economy, Trade and Industry (METI) since December 2006, aiming to eliminate bot infection/bot-infected PCs in Japan through collaborative efforts by related organizations and companies.

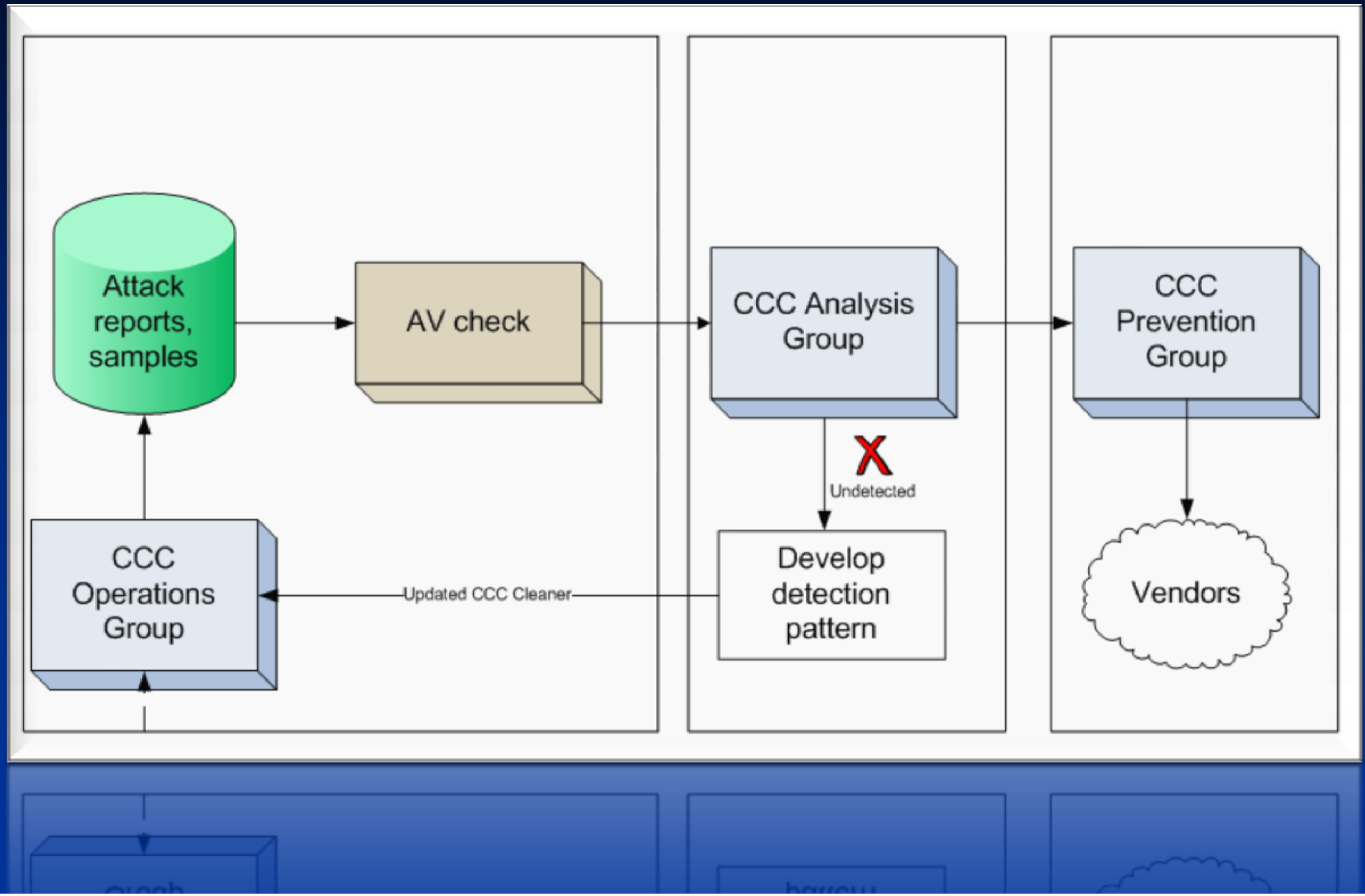
- Activity Report 2008-07
- Fiscal Year 2006 Activity Report on Cyber Clean Center(2007.05.25)

This is the FY 2006 activity report on "anti-bot measures project," jointly conducted by the Ministry of Internal Affairs and Communications(MIC) and the Ministry of Economy, Trade and Industry (METI) since December 2006, aiming to eliminate bot infection/bot-infected PCs in Japan through collaborative efforts by related organizations and companies.

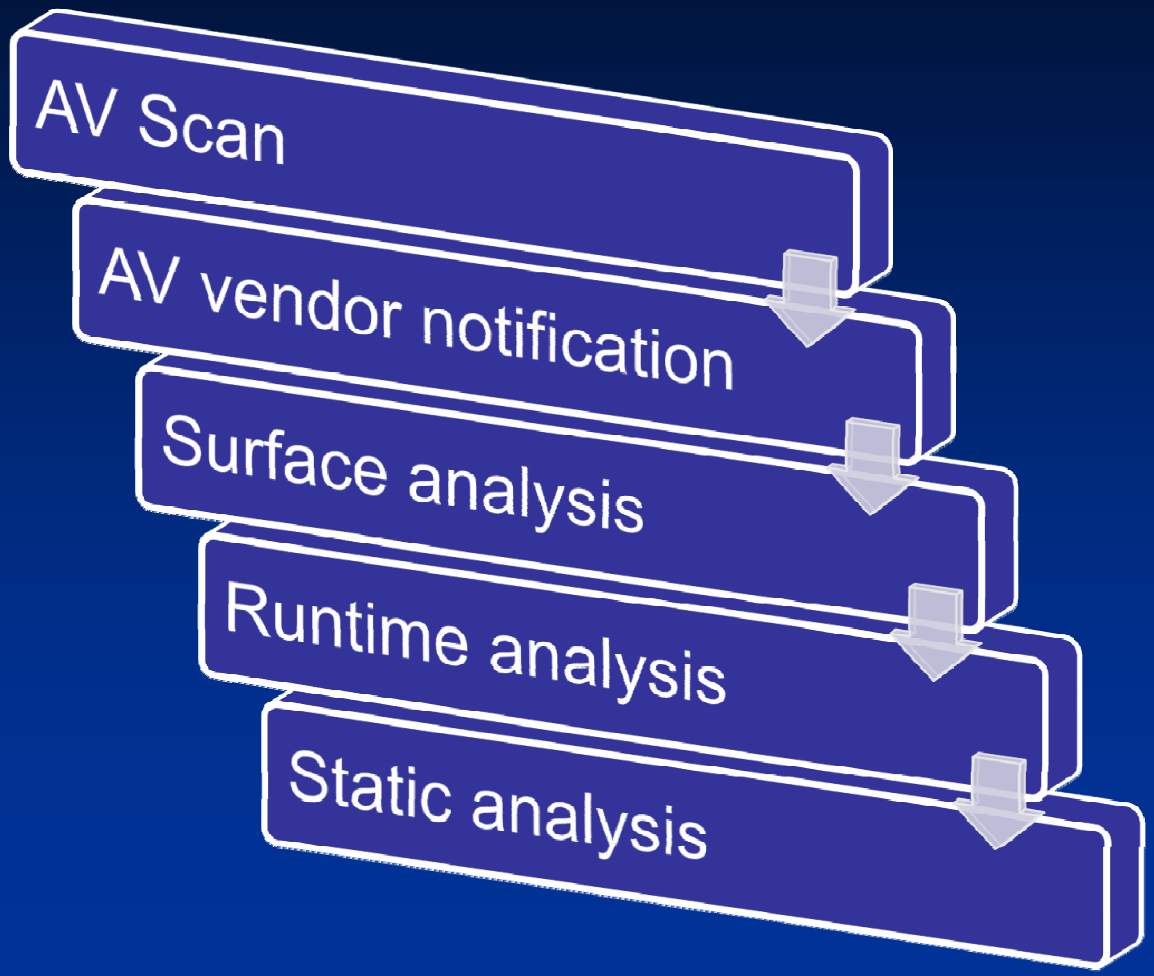
Collection


Attack reports
CCC Operations Group
ISP 1
ISP 2
ISP 3
Honeypot
Honeypot
Honeypot

Analysis


Attack reports, samples
AV check
CCC Analysis Group
CCC Prevention Group
X
Undetected
CCC Operations Group
Updated CCC Cleaner
Develop detection pattern
Vendors

Analysis

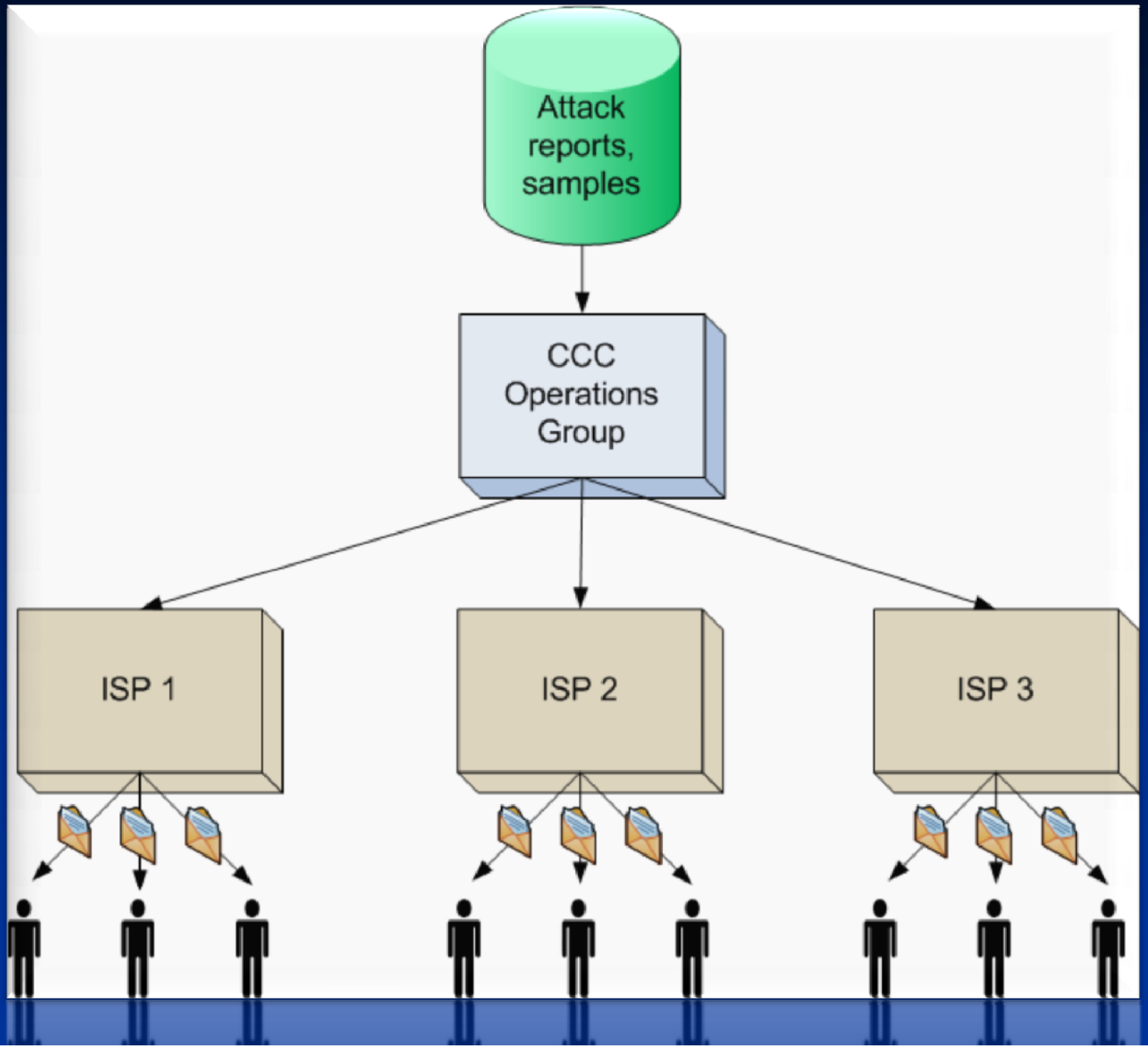

AV Scan
AV vendor notification
Surface analysis
Runtime analysis
Static analysis

Analysis

Goals:

- Trend prediction
- Countermeasure improvement
- Vendor tool improvement
  - via sharing samples
- Identify supporting infrastructure
  - Secondary malware hosts, C&Cs, config files

Notification



Monthly collection average until now:*

* Subject to significant variance each month

Results of alert activities in January of FY 2009

1 Total number of collected samples

This month: 432, 184

Cumulative sum: 12, 866, 088

Number of samples of BOT viruses, etc. collected from myriads of attacks on "decoy machines" (binary files)

2 Number of identified, unique samples

This month: 36, 196

Cumulative sum: 827, 687

As many of the same samples may be colleted, a process treats the samples with the same size and external features as one sample. This is the number of identified, unique samples derived from the process (binary files)

3 Number of unknown samples

This month: 314

Cumulative sum: 21, 827

The number of samples that cannot be detected by commercially available anti-virus software after isolating and searching for collected samples

6 Number of alerts

Number of emails

This month: 11, 034

Cumulative sum: 352, 616

Number of recipients

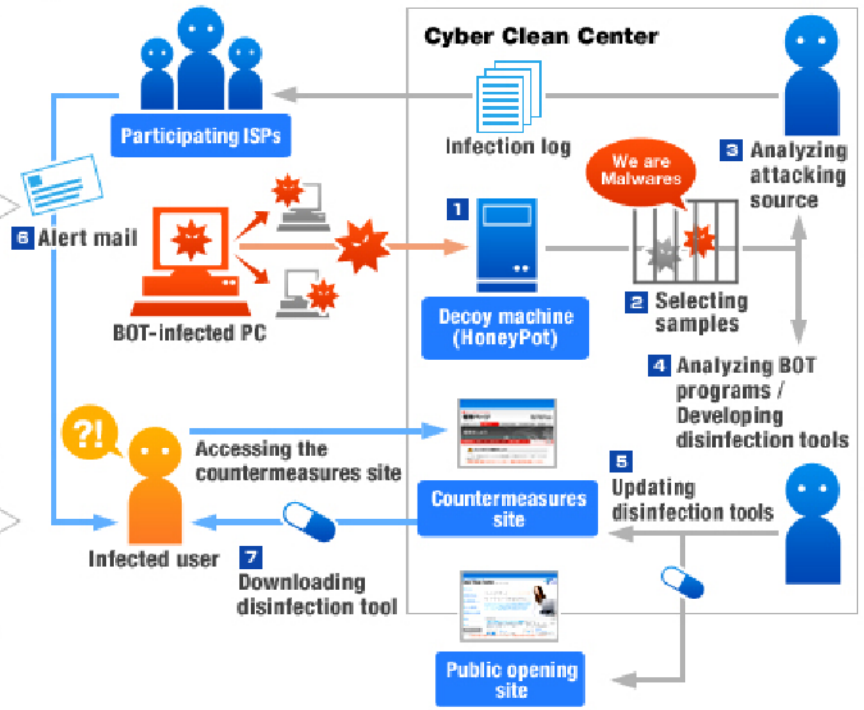
This month: 4, 926 (2, 442 new recipients)

Cumulative sum: 75, 531

The number of infected users and the number of alert mails sent to them by Project Participating ISPs

7 Rate of downloading disinfection tools by alerted users

30% (cumulative)



4 Number of samples for which disinfection tools have been developed

This month: 337

Cumulative sum: 17, 750

Number of samples that are highly dangerous and transmit infections to many users and for which disinfection tools have been developed

5 Disinfection tools

Cumulative sum of updates: 104

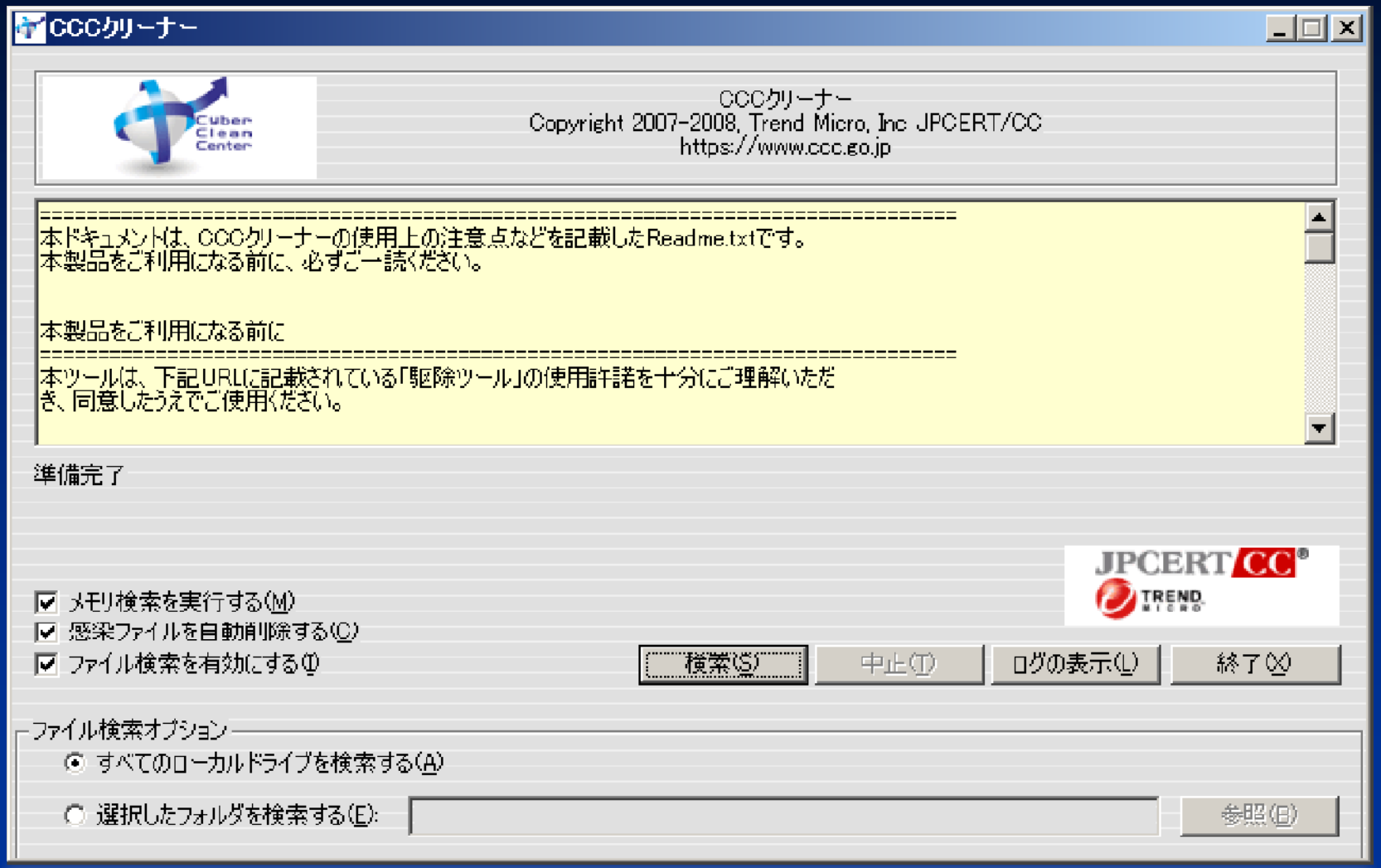
Disinfection tools are updated weekly

Total of disinfection tool downloads from the public opening site

Multiple downloads in the same timeslot are counted as one download

This month: 18, 809 Cumulative sum: 554, 684

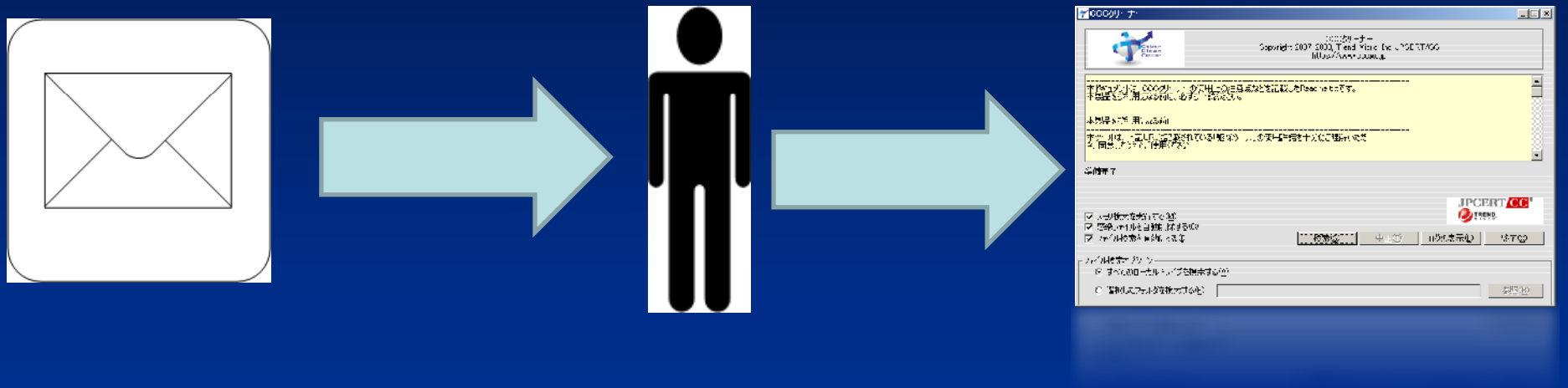
CCC Cleaner


CCCクリーナー
CCCクリーナー
Copyright 2007-2008, Trend Micro, Inc JPCERT/CC
https://www.ccc.go.jp
本ドキュメントは、CCCクリーナーの使用上の注意点などを記載したReadme.txtです。
本製品をご利用になる前に、必ずご一読ください。
本製品をご利用になる前に
本ツールは、下記URLに記載されている「駆除ツール」の使用許諾を十分にご理解いただき、同意したうえでご使用ください。
準備完了
JPCERT CC
TREND MICRO
メモリ検索を実行する(M)
感染ファイルを自動削除する(C)
ファイル検索を有効にする(I)
検索(S)
中止(T)
ログの表示(L)
終了(X)
ファイル検索オプション
すべてのローカルドライブを検索する(A)
選択したフォルダを検索する(F):
参照(B)

CCC features

- Check:
  - Windows Update on?
  - Broadband router?
  - Hosts file
- Explain:
  - Risk of running Win 9x
  - What to do if malware can’t be removed
- Report (optional)
  - Summary of scan results
  - Send to CCC for statistical purposes

CCC notification flow



363 559 notification emails

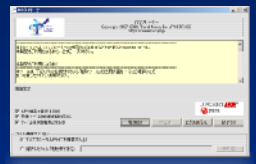
sent to

77 601 recipients

Around 47% of notifications are for re-infections.

Of
77601
email
recipients

65% go to CCC website.



38% download CCC cleaner.

21% file finish report

Improving user acceptance

1: Why don’t people download the tool?

Multi-page explanation
was too long and technical.

Use single page
Use simple language

Improving user acceptance

2. Engaging education

http://botkujo.jp

Improving user acceptance

3. Security software confusion

Anti-virus

Personal firewall

Anti-spyware

Security suites

What does what?

Improving user acceptance

4. ISP security services misunderstood

“I’m sure my ISP will protect me.”

Challenges

- Currently honeypots only
  - Honeypots + mail scanning + web site monitoring etc offer better coverage
- CCC only checks for Windows Update
  - Doesn't check 3rd party apps
- Can't repair infected system files
  - Current suggestion to users: format
- Bot countermeasures
  - Download site takedown work complex
  - Difficult dealing with "bullet-proof" hosting

JPCERT CC®
Japan Computer Emergency Response Team Coordination Center
JPCERTコーディネーションセンター

Thank you!

office@jpcert.or.jp