The incident response and the police in Japan

Yoshio Yamada
Assistant Director,
High-Tech Crime Technology Division,
National Police Agency, Japan

Agenda

- Structure of Japanese police
- Roles of High-Tech Crime Technology Division
- Cyber Force Center
- Cooperation among the organizations including the police
- Effort of early warning by the police
- Actual incident responses

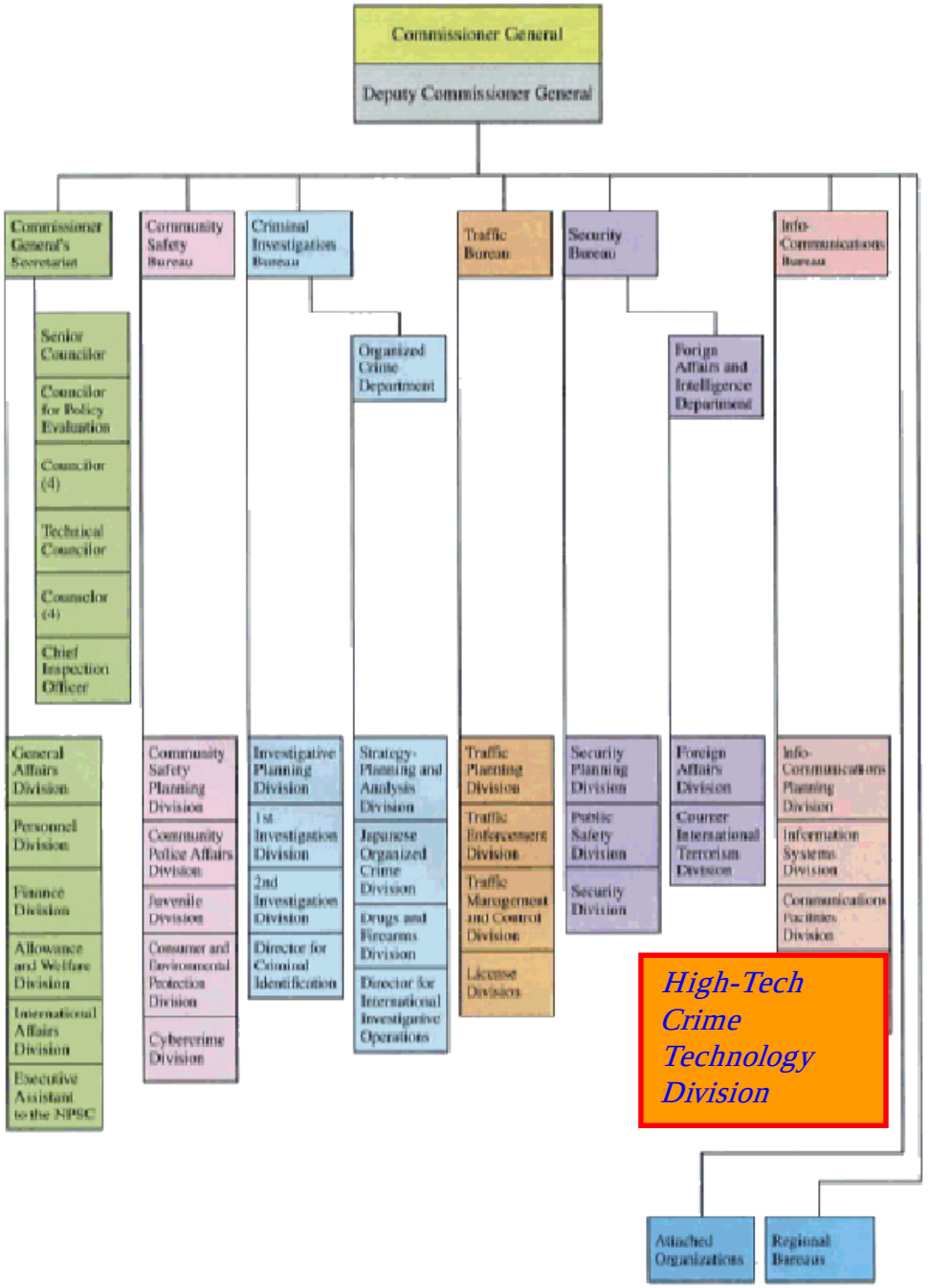
Organization of Japanese government

- **Diet**
  - House of Representatives
  - House of Councilors

- **Cabinet**
  - Cabinet Office
    - National Public Safety Commissions
      - National Police Agency
    - Other Agencies
  - Other Ministries

- **Courts**
  - Supreme Court
  - High Courts
  - District Courts
  - Summary Courts
  - Family Courts

Organization of National Police Agency (NPA)



Roles of the High-Tech Crime Technology Division (HTCTD)

- **Technical support**
  - Technical support for local police force's investigations
  - Technical analysis on the Internet activities
  - Provide training for staff (officers and engineers)
- **International cooperation on technical matters**
  - 24 hour point of contact in technical area (G8, ICPO, etc…)
  - Technical capacity building
- **Research and Development**
  - Research of emerging technologies
  - Development of technical tools and standards for investigation support

Roles of HTCTD

HTCTD plays an important role in the following areas:

Digital Forensics

Sophisticated analysis provided by forensic examiners (computer virus, malicious code, cyber crime and cyber-terrorism attempt.)

Computer Incident Prevention and Response at Critical Infrastructures

Support to limit the damage of attacks aiming at computer network systems of critical infrastructures on the Internet.

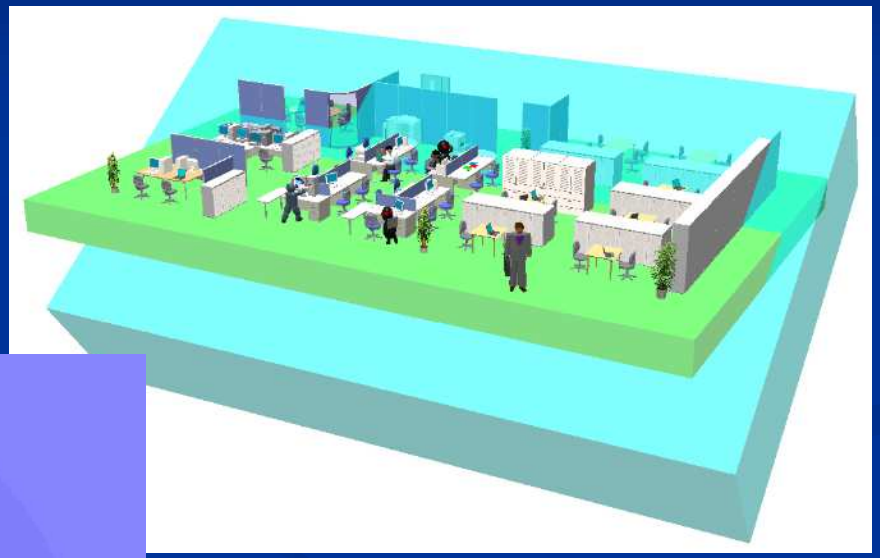
Cyber Force Center (CFC)

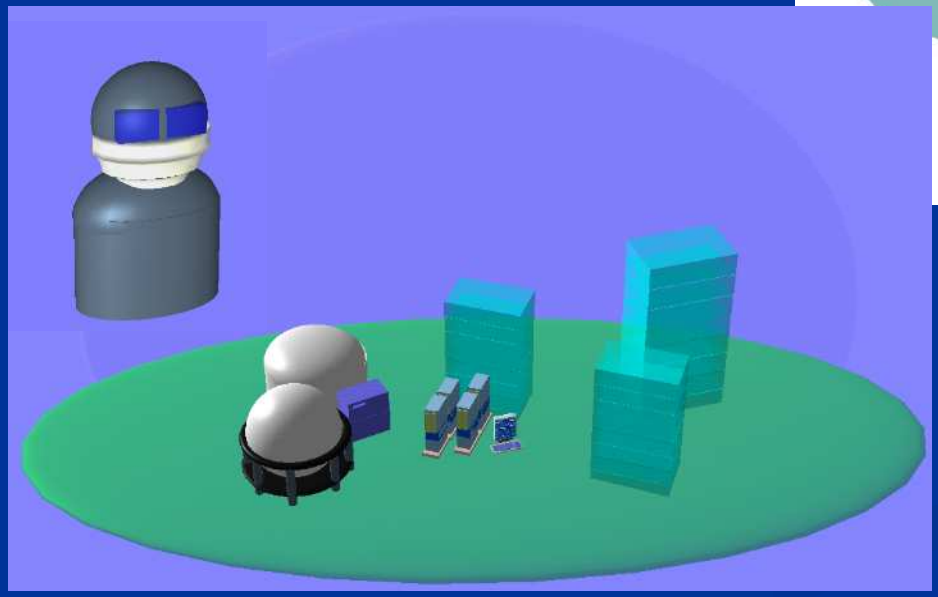
Duties:

- Technical matters to prevent crimes against information systems which could affect life, social and economic activities, and of incident response to control damage caused by the crimes (Cabinet Office Ordinance)

Counter cyber terrorism initiative by the police

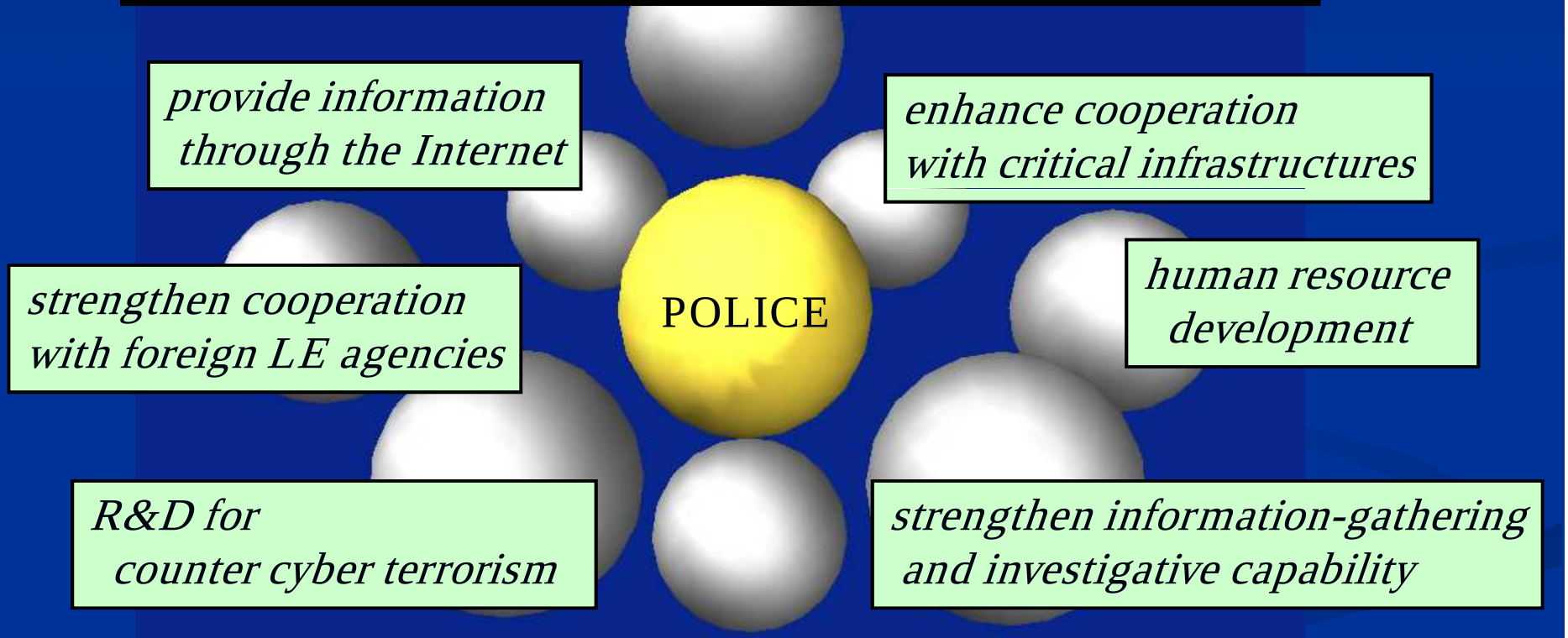
- objectives
  - prevention
  - damage control
  - arrests





Measures and policies

acquire predictive information and recognize cases at the 24h operating "cyber force"



provide information through the Internet

enhance cooperation with critical infrastructures

strengthen cooperation with foreign LE agencies

human resource development

R&D for counter cyber terrorism

strengthen information-gathering and investigative capability

Cyber Force Activities

operation of Internet threat monitoring systems

- IP packets monitoring
- Botnet monitoring
- Malware captue

cooperation with critical infrastructures

- periodical meetings
- contact points

Information-gathering and analysis

Security Planning Division

Cyber Crime Division, etc..

National Police Agency

cooperation with outside organizations

Information Security Center,
Cabinet Secretariat

Information dissemination

@police

Mailing list amongst critical infrastructures

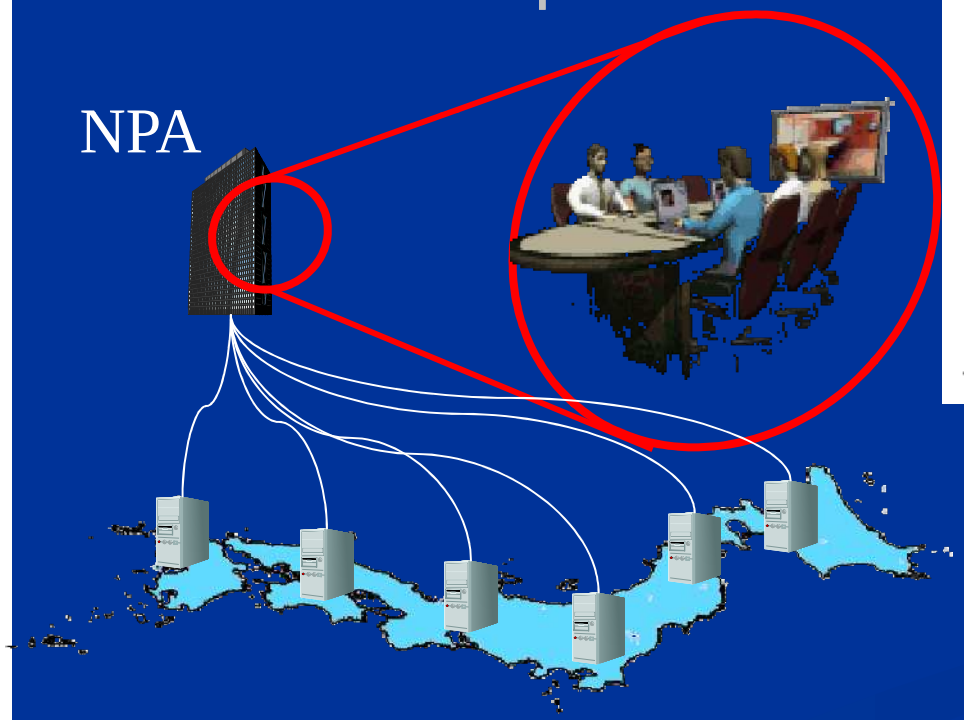
incident response at critical infrastructure

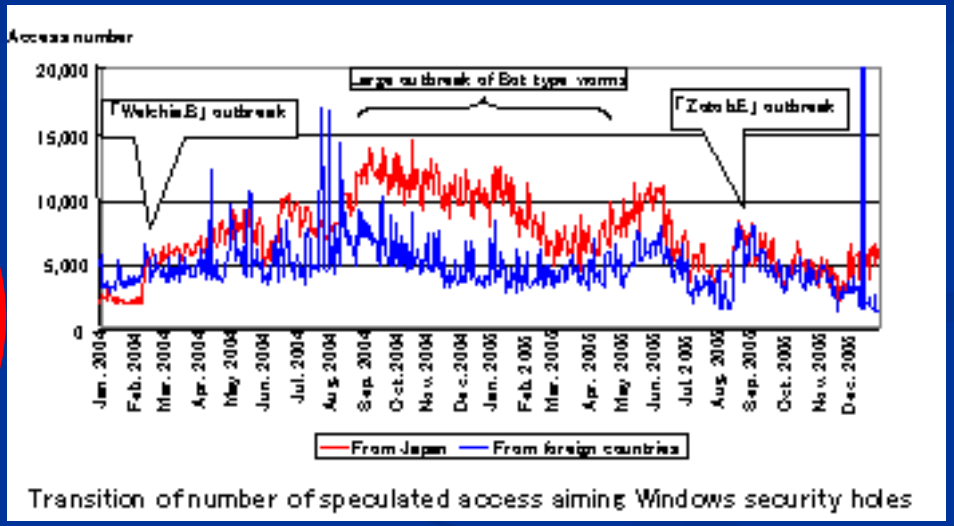
- Technical support for local police forces

Critical Infrastructure

Operation of Internet threat monitoring systems

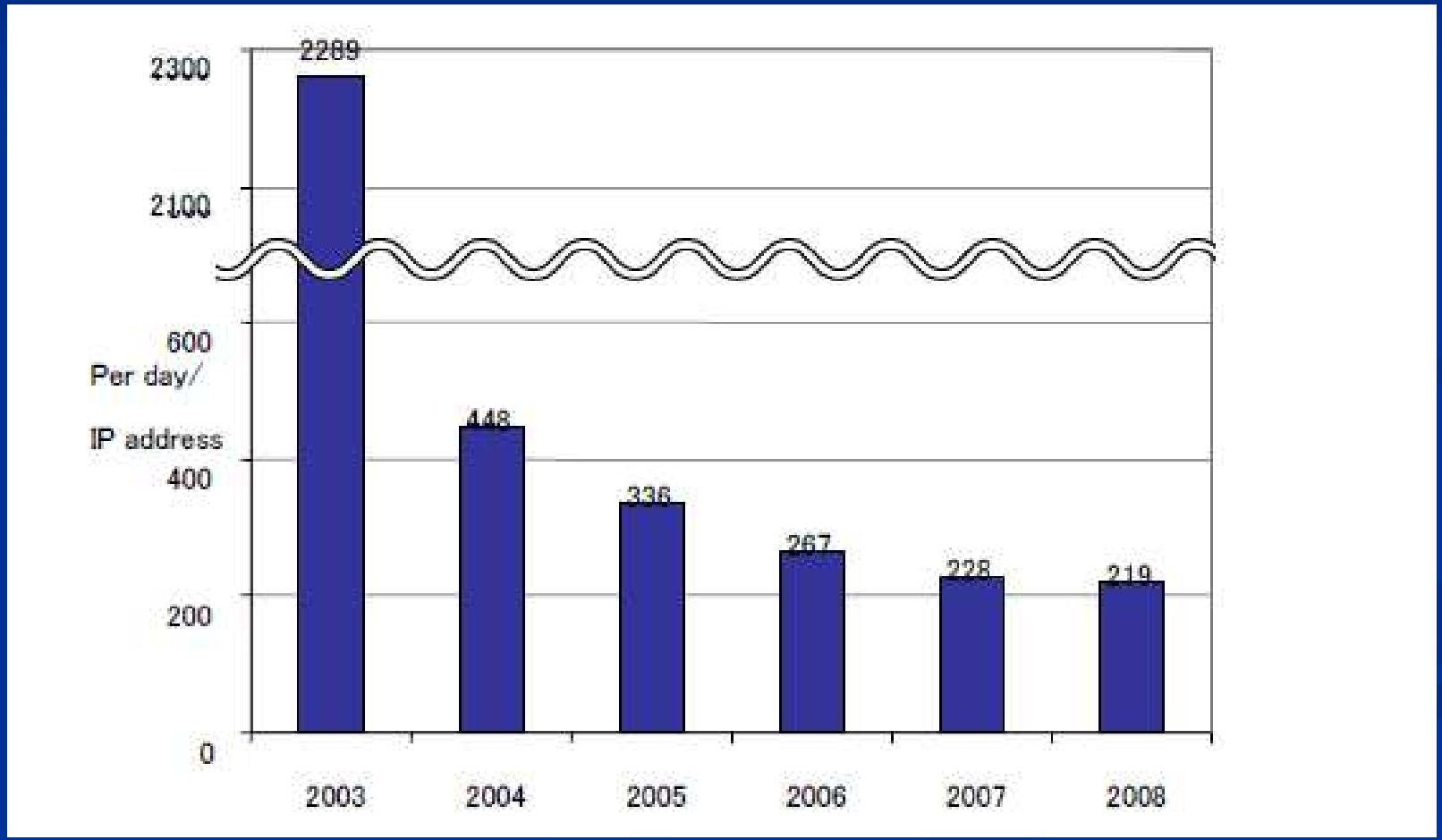
- IP packets monitoring
- Botnet monitoring
- Malware capture



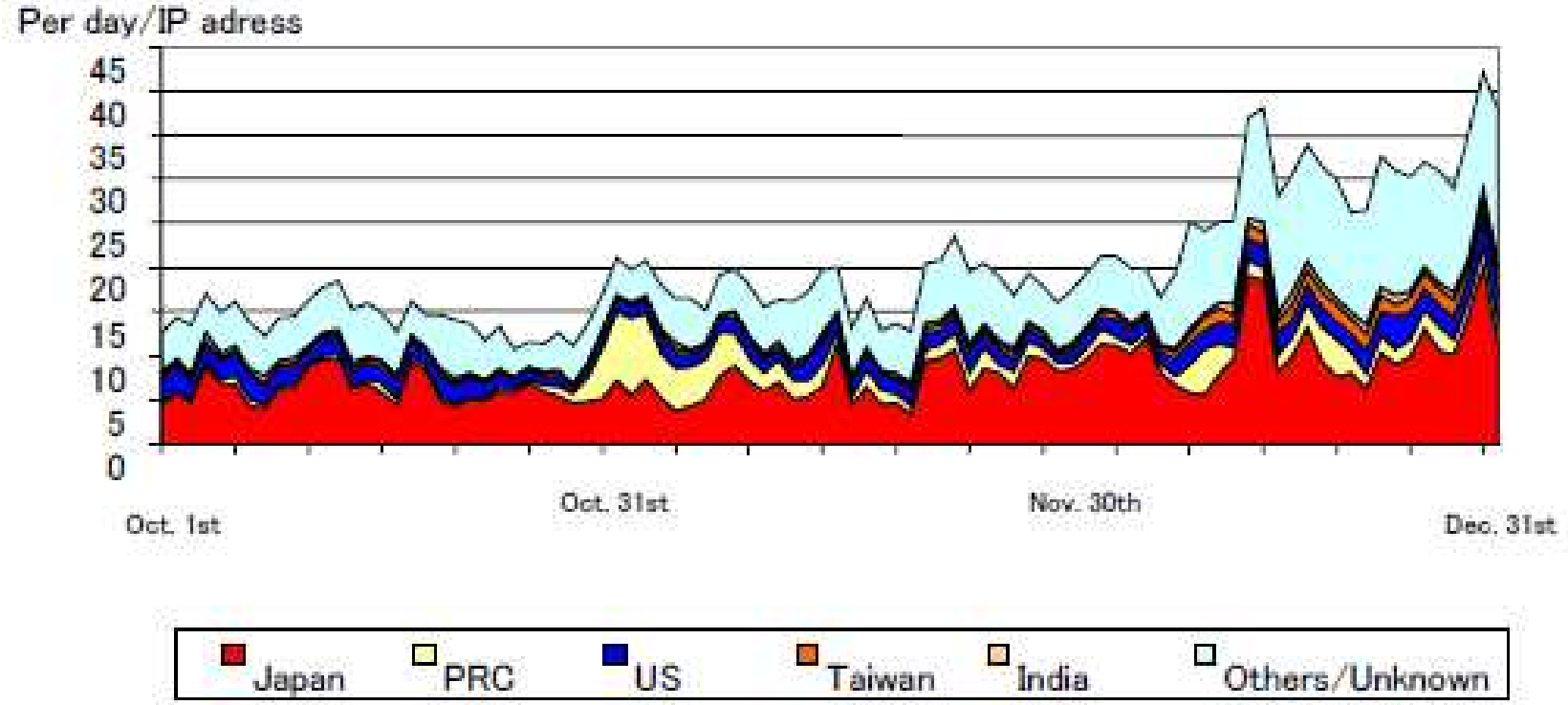


Transition of number of speculated access aiming Windows security holes

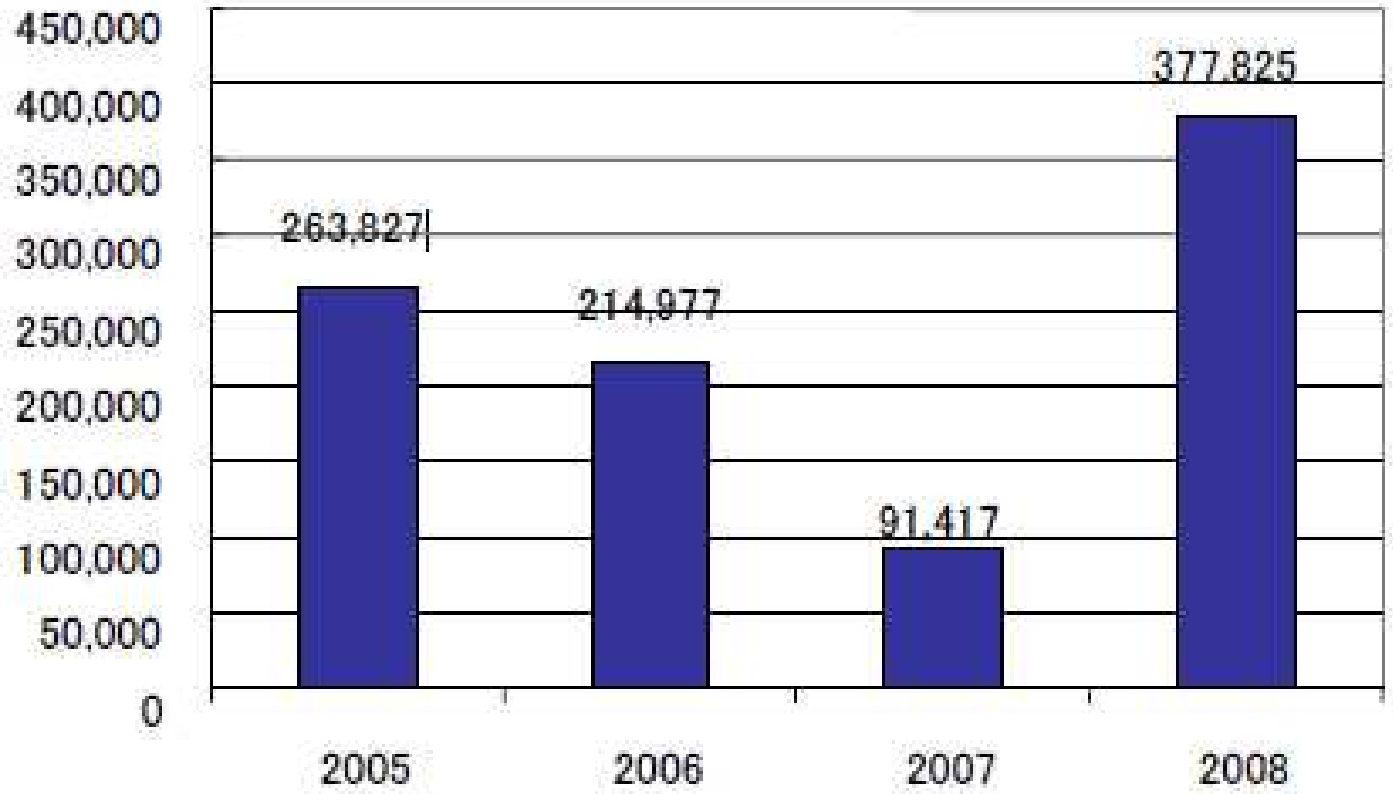
Changes of the number of accesses against firewall



Changes of the number of access to destination TCP port 445

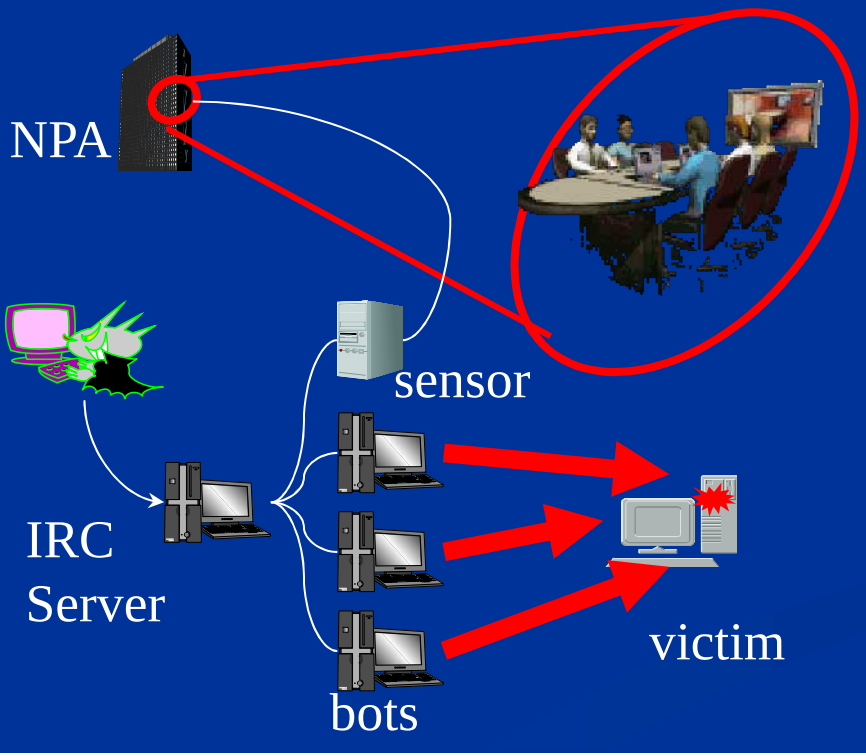


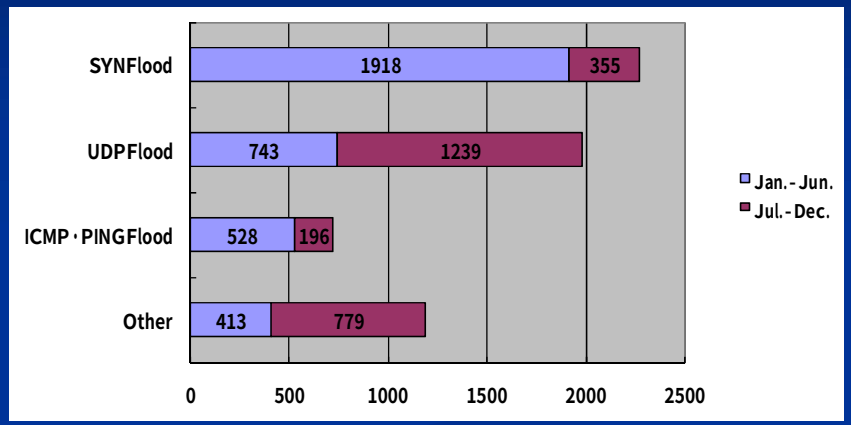
Changes of the detected number of SYN flood attacks

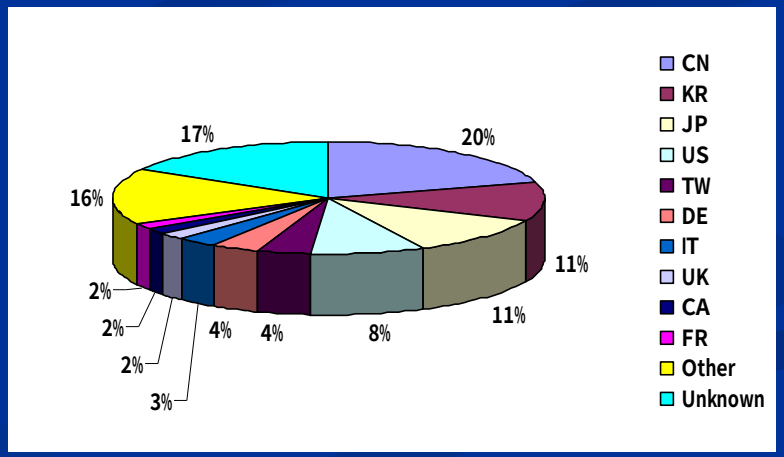


Operation of Internet threat monitoring systems (contd.)

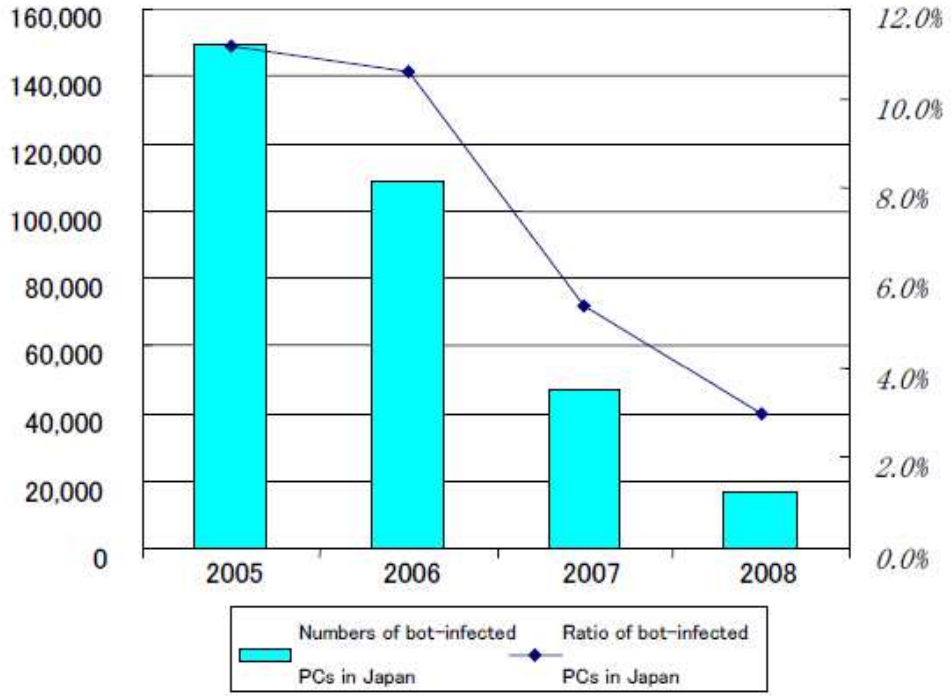
- IP packets monitoring
- Botnet monitoring
- Malware capture





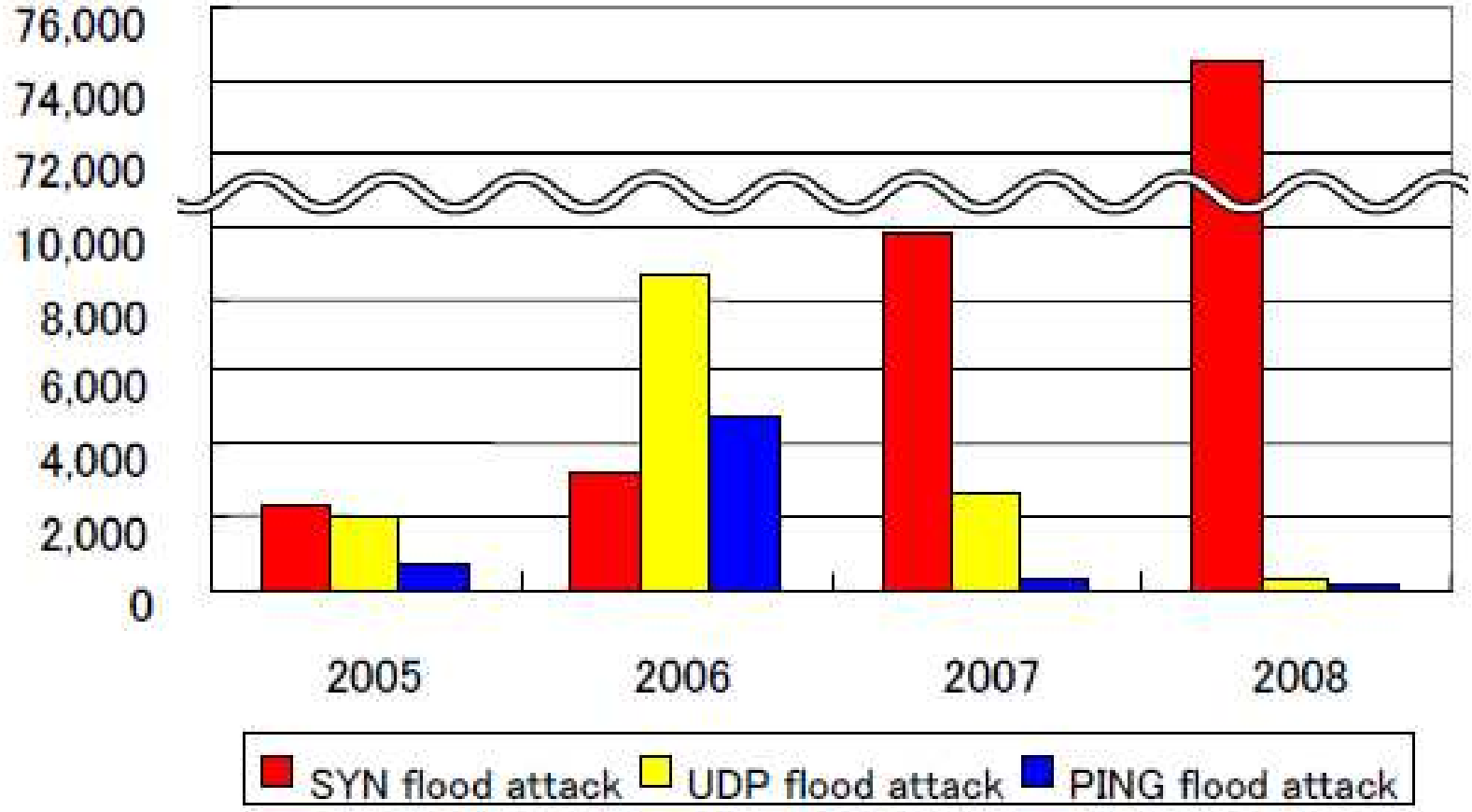


The number of bot-infected PCs in Japan



	2005	2006	2007	2008
Number of bot-infected PC in Japan	149,609	108,626	46,953	16,529
Number of bot-infected PC in the world	1,337,167	1,025,253	874,980	551,226
The ration of bot-infected PCs in Japan	11.2%	10.6%	5.4%	3.0%

The number of DoS attack commands in botnet



A example of our incident responses -1

Victim: a local government
Damage: webpage defacement

Our Action

We preserved its HDD as an evidence and advised the victim to limit the access permitted IP address; verify the web server's vulnerabilities.

further investigation…

A example of our incident responses -2

Victim: a financial institution
Damage: DoS (web)

Our Action

We gave mitigating countermeasure to the victim, then collect attacker's information from the server's access log for further investigation.

further investigation…

End