Internet Security Days 2015
16th & 17th September 2015
Phantasialand Brühl, Germany

ACTIVE Project
ISP's efforts to fight against malware in Japan

16th September 2015

Satoshi Noritake
NTT Communications Corporation/Telecom-ISAC Japan

Telecom-ISAC Japan
Telecom Information Sharing and Analysis Center Japan

Today's agenda

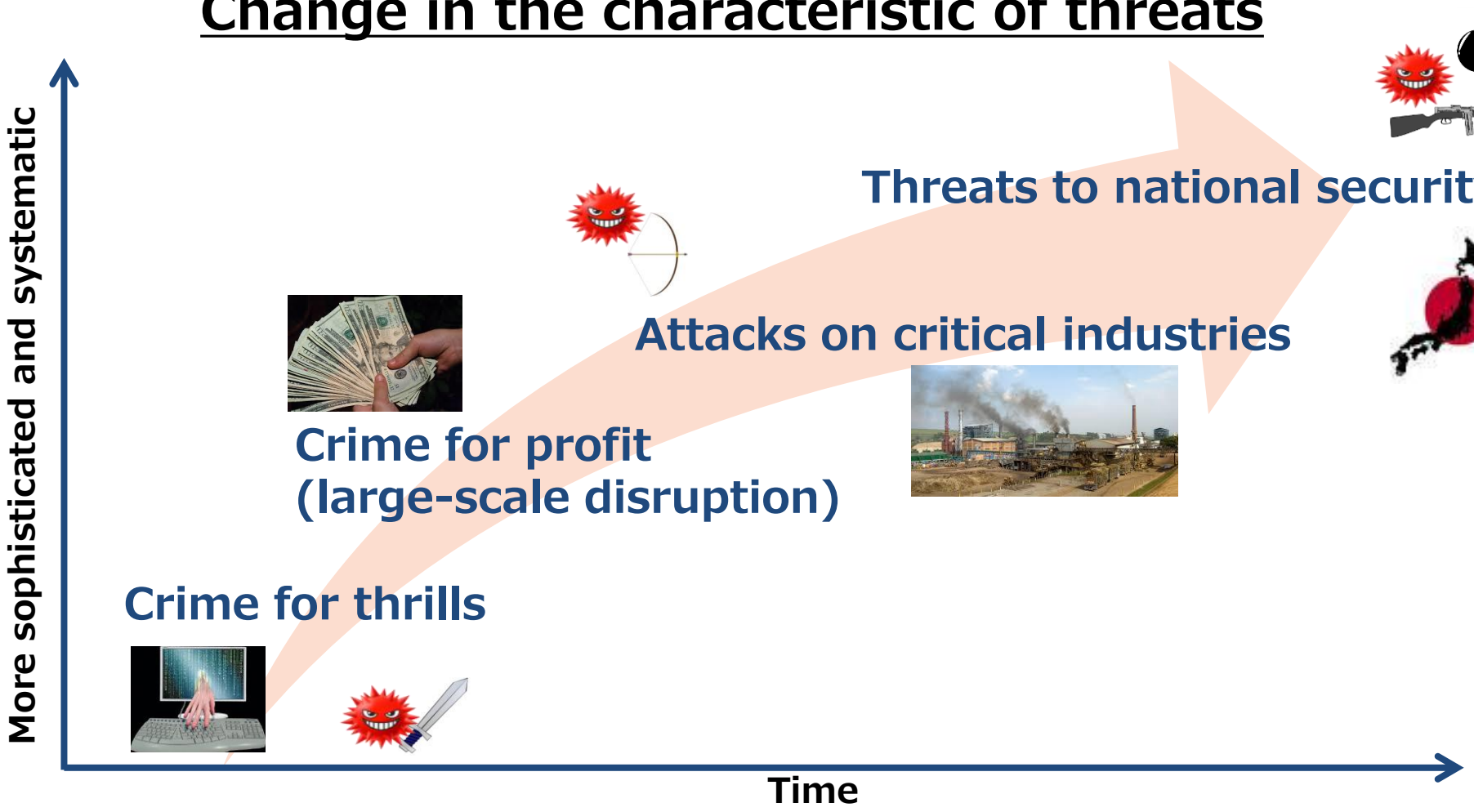
- **Security issues in Telecom industry**
- **Telecom-ISAC Japan's activities**
- **ACTIVE Project**

Security issues in Telecom industry

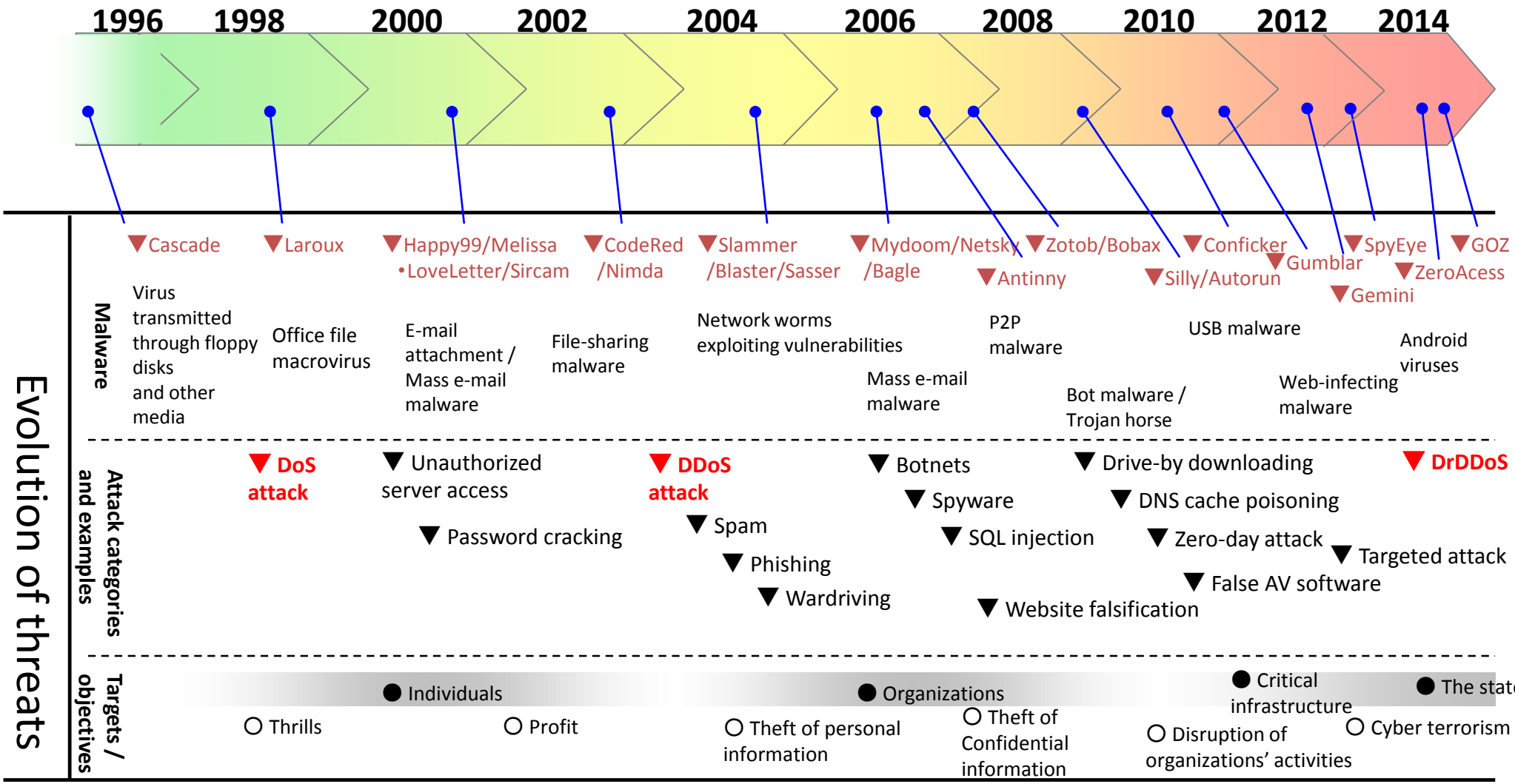
Change in Internet-Based Security Threats

- Methods of attack are growing ever more sophisticated and systematic
- Characteristic of threats is changing

Change in the characteristic of threats



Security Threats chronology



Why ISPs need to fight

Many reasons ISPs need to fight against security threats

- The internet is essential for our business, our users and our society.
- But ISPs are facing various types of security threats.
- ISPs need to fight against security threats in order to protect
  - *network (Business)*
  - *users*
  - *society*

Telecom-ISAC Japan's activities

Introduction of Telecom-ISAC Japan

Established in July 2002

- as the first Information Sharing and Analysis Center (ISAC) in Japan
- with 20 member companies including telecommunications carriers and ISPs
- to enhance security countermeasures for the information and telecommunication industry, by establishing a mechanism to share and to analyze the security incidents within the members

Telecom-ISAC Japan
Telecom Information Sharing and Analysis Center Japan

Cyber attack defense exercise

Cyber Clean Center

20 member companies

Anti-bot countermeasures project

Wide area monitoring

Information sharing

Incident handling

Reputation database system

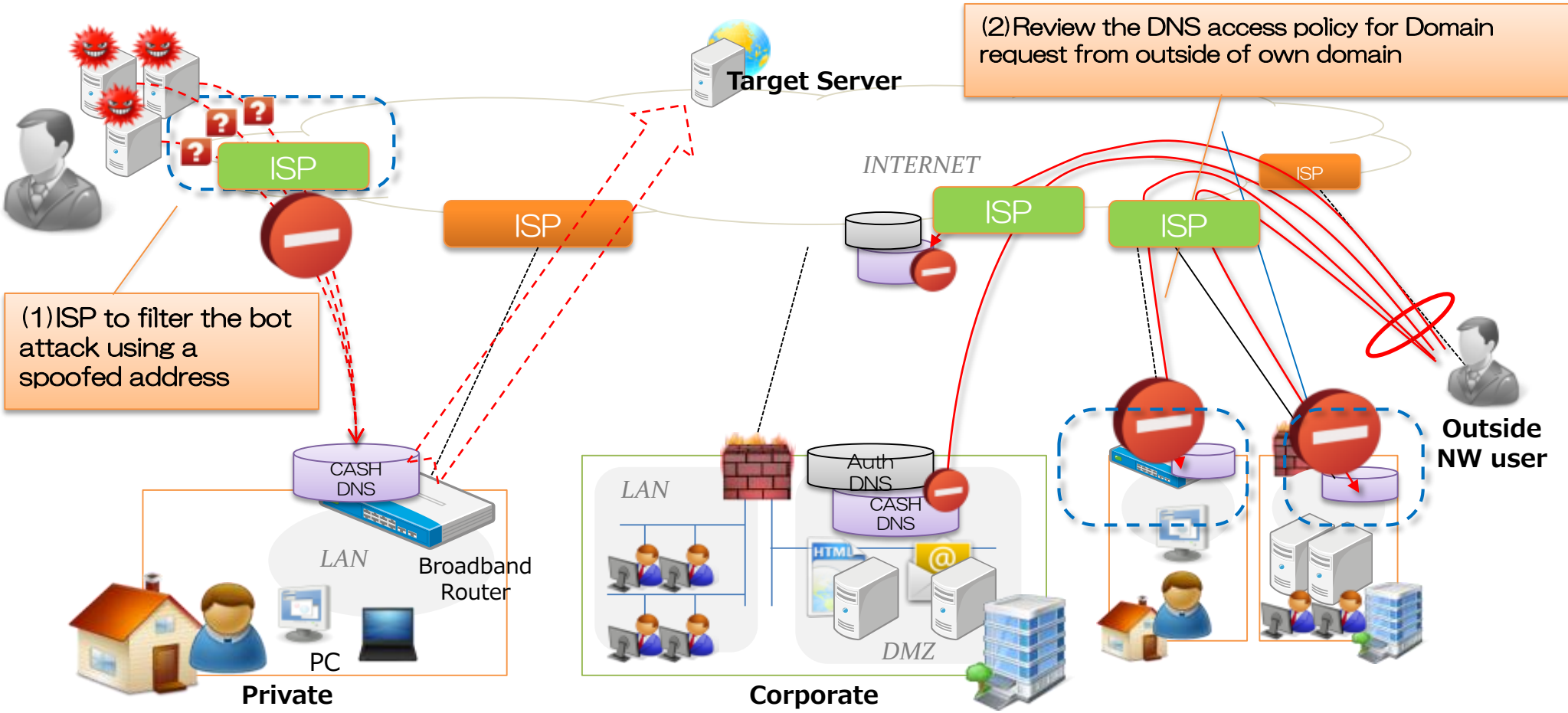
Route monitoring system

ACTIVE
Advanced Cyber Threats response InitiatiVE

PRACTICE
Proactive Response Against Cyber-attacks Through International Collaborative Exchange

Necessity of Cooperation and Coordination

Case of Cooperation and Coordination: DNS Reflection attack



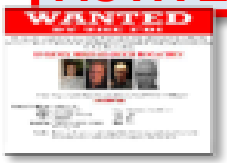
Single organization can do only a few things for Large scale DNS Reflection attack. Cooperation and Coordination is necessary!

Recent topics on Telecom-ISAC Japan's measures

Telecom ISAC Japan

Pur-pose	Year 2011	Year 2012	Year 2013	Year 2014
Monetary	Prevalence of phishing sites		Illegal remittance malware on the rise (Oct)	Jun, Aug
Personal info. leak・intelligence leak	Manifestation of intel. activities between companies/nation (Jul～Nov, Sept)		Mar, Jun, Aug; Feb; Illegal access to service site/multiple info. theft (Jun, May～Oct)	Info. leak risk manifested by spreading of cloud using apps (Dec, Aug)
Destruction, industrial action	Rise of hacktivism (Apr, Jun, Sept)		Occurrence of large-scale DrDoS attack becomes norm (Mar, Feb, May～Jul, Aug); Manifestation of large-scale cyber attack that span nations (Mar, Dec)	
Misc.			ion of the vulnerability in important MW protocol (preliminary survey?) (May, Sept, Oct); Out-of-date software and firmware (May～Jun, Feb, Apr, Aug, Nov)	

Participation in the GOZ takedown strategy through ACTIVE Project



Efforts against reflection attack

Exposing illegal proxy server operators and problem of BB Router vulnerability

ACTIVE Project

Malware Countermeasures through Public-Private partnership

Telecom-ISAC Japan promotes various projects with the support of Ministry of Internal affairs and Communications in order to establish the safe and secure Internet society.

Malware Trend

More sophisticated and various malwares

Emergence of more sophisticated and more various malware

Drive-by-download

Appearance of web-based infection malware which infects by merely viewing web sites

Bot

Bot which infects without the users' awareness by merely accessing the Internet is in the majority

PRACTICE 2011～2016

Field Trial of Proactive Response Against Cyber-attacks Through International Collaborative Exchange

Field Trial which collects and analyzes various cyber-attack information, establishes a quick-response scheme through International collaboration.

RDB 2009～2012

System field trial to prevent access the hazardous web sites (example: malware embedded sites)

Field Trial which creates lists of malware embedded sites and avoids accessing the hazardous web sites in order to protect people from malware infection by merely viewing web sites

Cyber Clean Center 2006～2011

Anti-botnet Countermeasures Project

Project which detects bot infected PCs, and sends notification to the owner of bot infected PC, in order to remove malware from the PC.

ACTIVE 2013～2018

Challenge for preventing malware infection and removing malware

Challenge to prevent malware infection by blocking access to malware embedded websites and to issue the warning to notify malware infection and to request malware removal through collaboration among telecom carriers and security vendors., and to realizes safe and secure network environment.

Background of Telecom-ISAC Japan which deals with cyber-attack response

Motivation of Malware creation
Change from criminal for pleasure to pecuniary motive

Change of Malware Infection Technique
Emergence of more advanced and complicated attack techniques

Current Social Circumstances
Various social activities depend on the Internet

Overview of ACTIVE Project

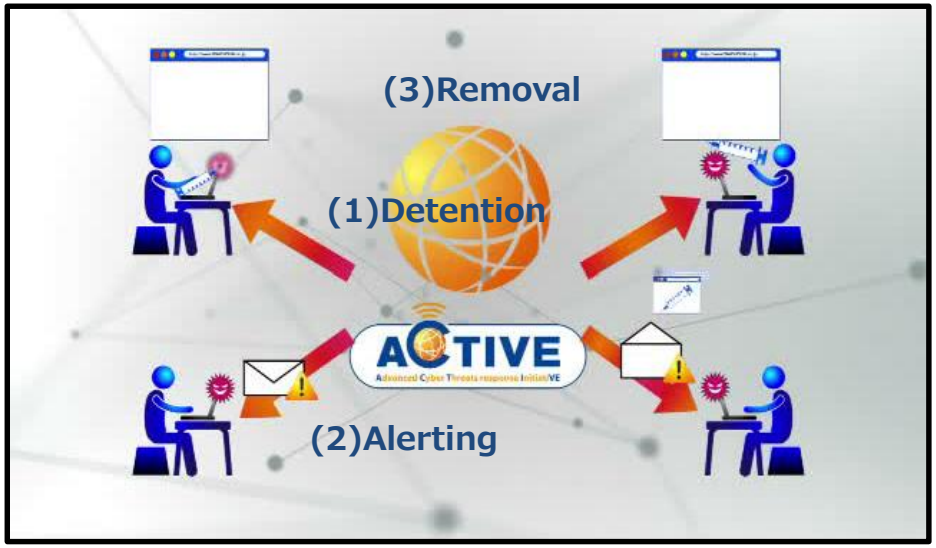
ACTIVE Project

Advanced Cyber Threats response InitiatiVE

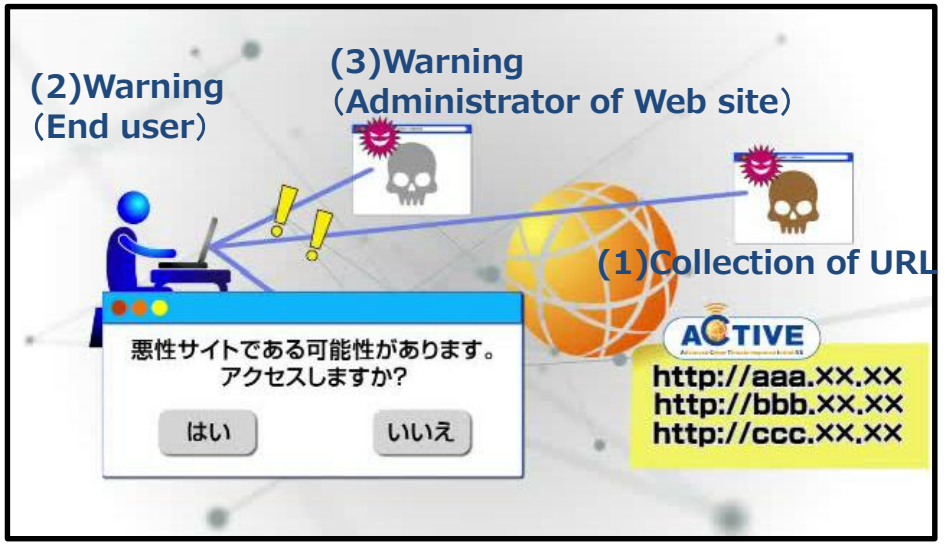
ACTIVE is a comprehensive malware countermeasures project to establish safety Internet society.

- Public-Private Partnership project funded by MIC
- Five years project (November, 2013 – March, 2018)
- To provide Comprehensive Malware Countermeasures
  - Removal of Malware
  - Prevention of Malware infection

Removal of Malware



Prevention of Malware infection

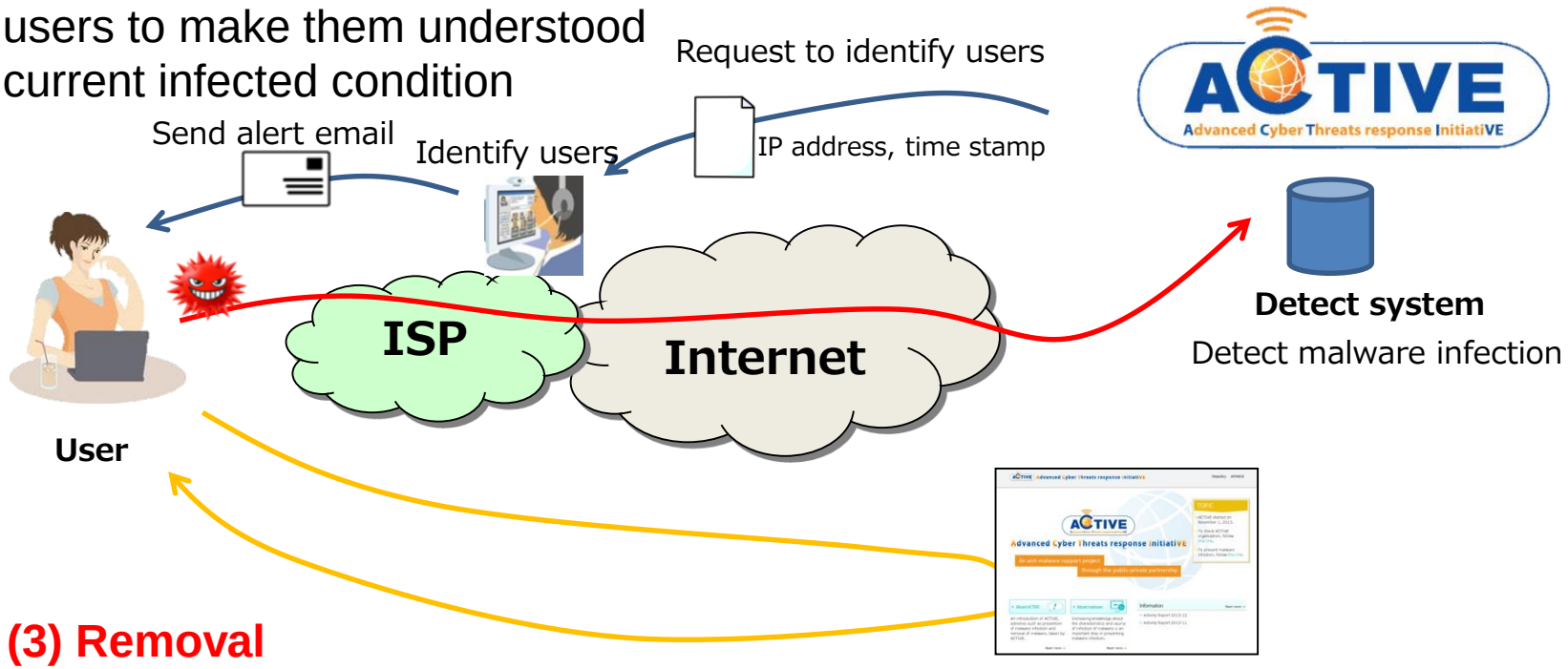


Effort to remove malware

- **ACTIVE detects malware infected PCs and notifies users.**
- **ACTIVE provides information on how to remove malware to users.**

(1) Detection
To Identify individual users whose PCs are infected with malware(s)

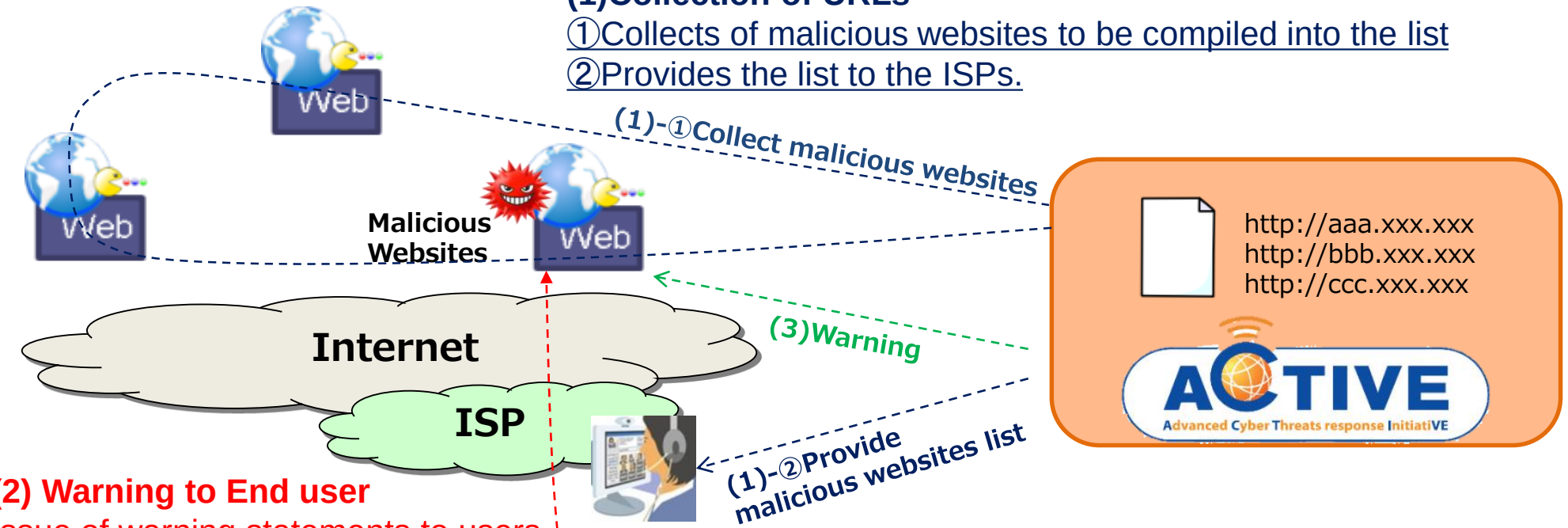
(2) Alerting
To Send an alert email to the users to make them understood current infected condition



(3) Removal
To Remove malware in accordance with the instruction in the alert email

Effort to prevent malware infection

ACTIVE prevents users from being infected with malware when the users try to access malicious website.



Take Down of Game Over Zeus
Participation in the GOZ takedown campaign

As Game over Zeus (GoZ) is taking major role in cybercrime around the world, FBI and Europol has organized the large scale take down which involved law enforcement agencies around the world including Japan.
With this operation, goal is to confiscating the servers that is used by criminal and finding out PC that is infected by malware and notify the user.

(出典)
http://www.fbi.gov/news/stories/2014/june/gameover-zeus-botnet-disrupted

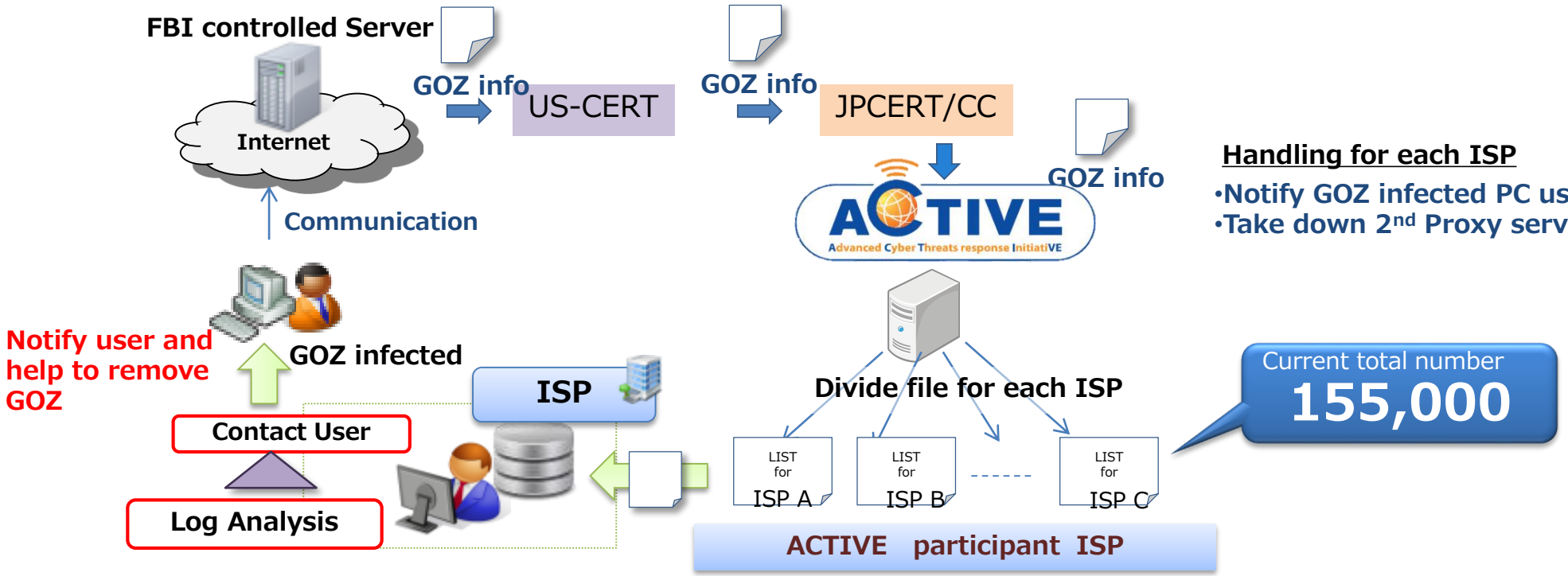
(出典)
http://www.npa.go.jp/cyber/goz/

Operational Detail

- Take down of C&C Server and there proxy
- Monitor the C&C server activity and notify the user for infection.

Take Down of Game Over Zeus
Role of ACTIVE Project

•Contacting individual ISP from Police and JPCERT/CC is a huge burden for them
•ACTIVE Project plays a role in contacting point for each ISP



※ VAWTRAK infected PC users also have been notified by ISPs through ACTIVE scheme .

Past Achievements (1st Nov.,2013 – 28st Feb., 2015)

- ACTIVE started on 1st November, 2013 supported by MIC.
- Many ISPs and security experts join ACTIVE.
- Issued 1,342 alerts to malware infected PC users.
- Issued 472 alerts to malicious access.
- Established malicious web crawling scheme which enables to check 100,000 web sites a day.
- Added darknet sensor information provided by NICT to remove malware.
- Alerted 155,000 GOZ users based on FBI data.
- Alerted 33,000 VAWTRAK users based on MPD data.

We have to improve and promote ACTIVE to establish more secure and more safely ICT society!

Our challenge in 2015

Establish safety internet society by mitigating cyber-attacks through the cooperation with ISPs and other organizations

Activities

1. **Alerting & Access control based on ISP service(ISP's effort)**
   - Alerting to users
   - Alerting to Website master
   - Filtering malicious website access
   - Filtering C&C access

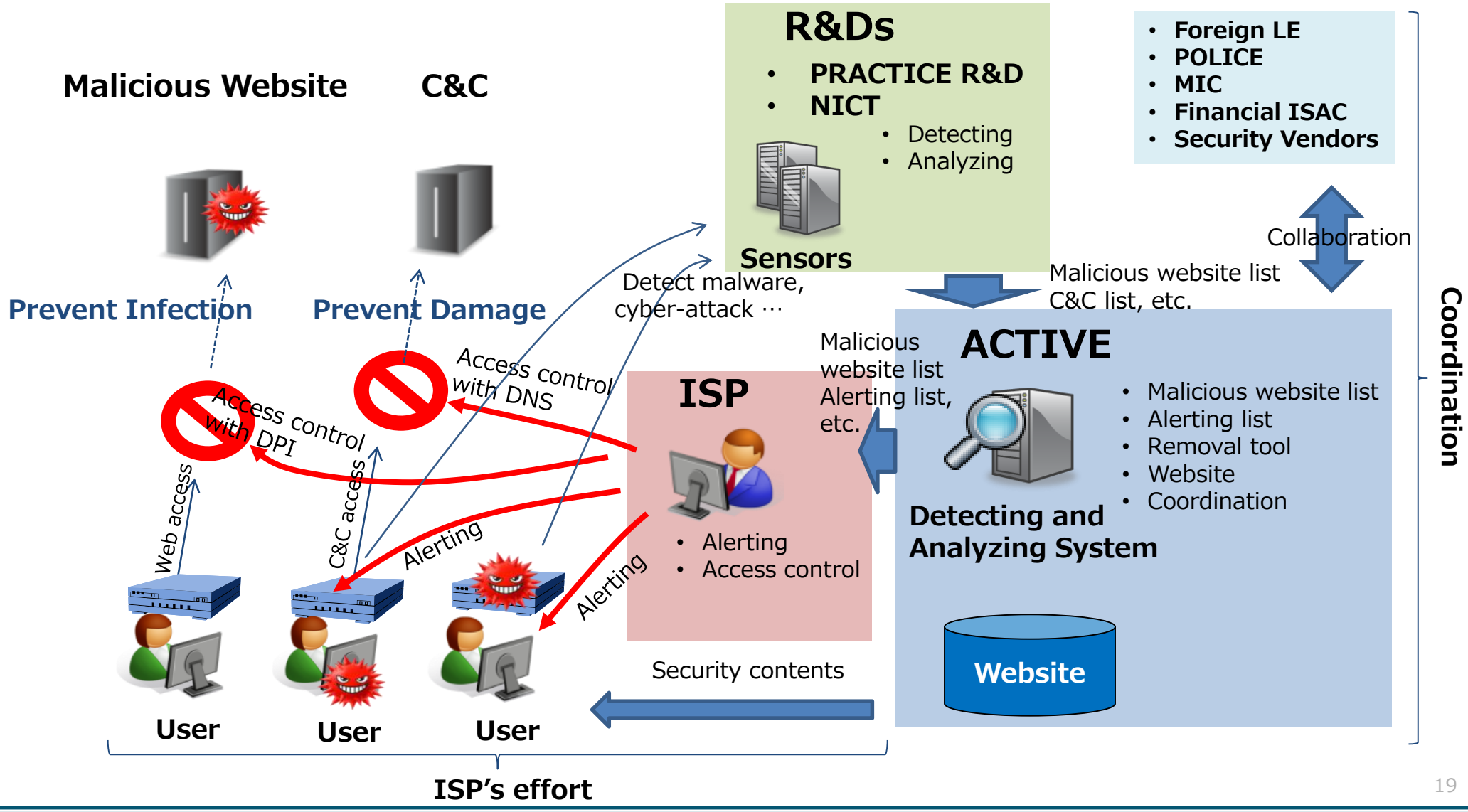
2. **Countermeasures through collaboration(Coordination)**
   - Participate in large-scale takedown
   - Information Sharing and Alerting based on shared information

Key Success Factors

- Promote effective activities(Legal issue should be cleared.)
- Promote more ISP participations(Local ISPs, CATV, etc.)
- Collect reliable data from other organizations(ACTIVE Honeypot is to be discontinued.)

Activities in 2015

1. Alerting & Access control based on ISP service(ISP's effort)
2. Countermeasures through collaboration(Coordination)



Thank you for your time and consideration.

We are looking forward to collaborating with you!

- *Telecom-ISAC Japan*
  https://www.telecom-isac.jp/english/index.html

Satoshi Noritake
NTT Communications Corporation
s.noritake@ntt.com