May 14, 2014

JPCERT CC®

Internet Security and CSIRT's mission

Osamu (Sam) Sasaki

Deputy Manager, Global Coordination Division
JPCERT Coordination Center, Japan

Computer Security Incident Response Team

CSIRT

What is CERT/CSIRT?

- CSIRT =Computer Security Incident Response Team
- The first CSIRT founded was CERT/CC in U.S. in 1988
- A CSIRT is an organization or a team responsible for receiving, reviewing, and responding to computer security incident* reports and activity

  * network or host activity that potentially threatens the security of computer systems
- CSIRT is a proven approach to formalize and implement the information security vision/strategy
- CSIRT's services are usually performed for a defined constituency

CSIRT's mission

- Provides a single point of contact (POC)

JPCERT/CC provides:

  - info@jpcert.or.jp for reporting incident
  - icsr-ir@jpcert.or.jp for reporting ICS incident
  - office@jpcert.or.jp for general contact

- Assists the constituency and community in preventing and handling computer security incidents

- Share information and lessons learned with other CSIRT / response teams and appropriate organizations and sites.

CSIRT Services

- Firstly, responding “Incident”
  - Incident Handling
    - Incident response
    - Incident analysis
    - Incident coordination

- Other services
  - Vulnerability Handling
  - Artifact Analysis
  - Education / Training
  - HDD forensics / Mobile forensics

more on http://www.cert.org/csirts/services.html

CSIRT Services - Reactive

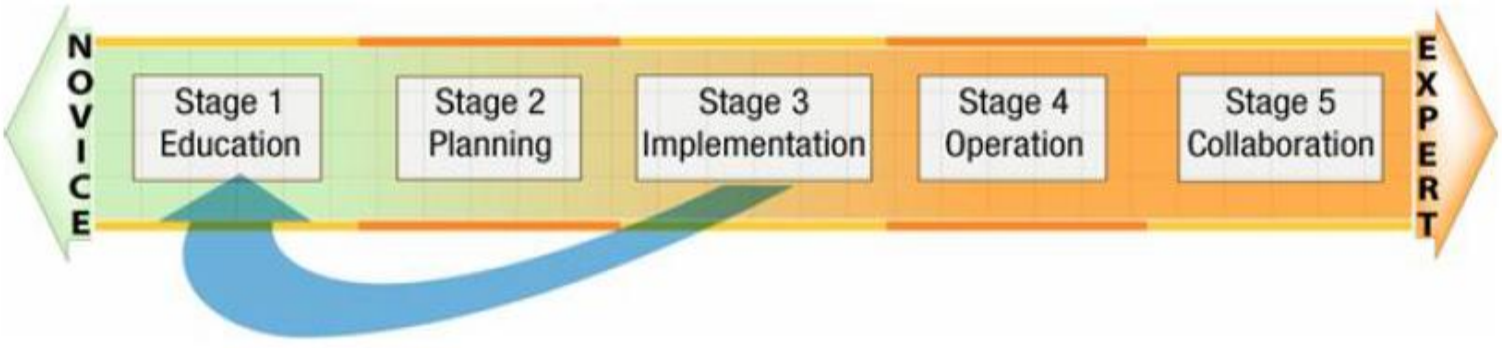
- Reactive
  - to respond requests for assistance
  - reports of incidents from your constituency, and any threats or attacks against CSIRT systems.

- Incident Handling
  - Incident analysis
  - Incident response on site
  - Incident response support
  - Incident response coordination

CSIRT Services - Proactive

- Proactive
  - to improve the infrastructure and security processes of the constituency before any incident or event occurs or is detected.
  - The main goals are to avoid incidents and to reduce their impact and scope when they do occur.
- Ex) Provide Security Information
  - Security Bulletin
  - Advisories/Guideline for users
  - Research Paper
- Any other service?

High-Level Steps for Creating a CSIRT

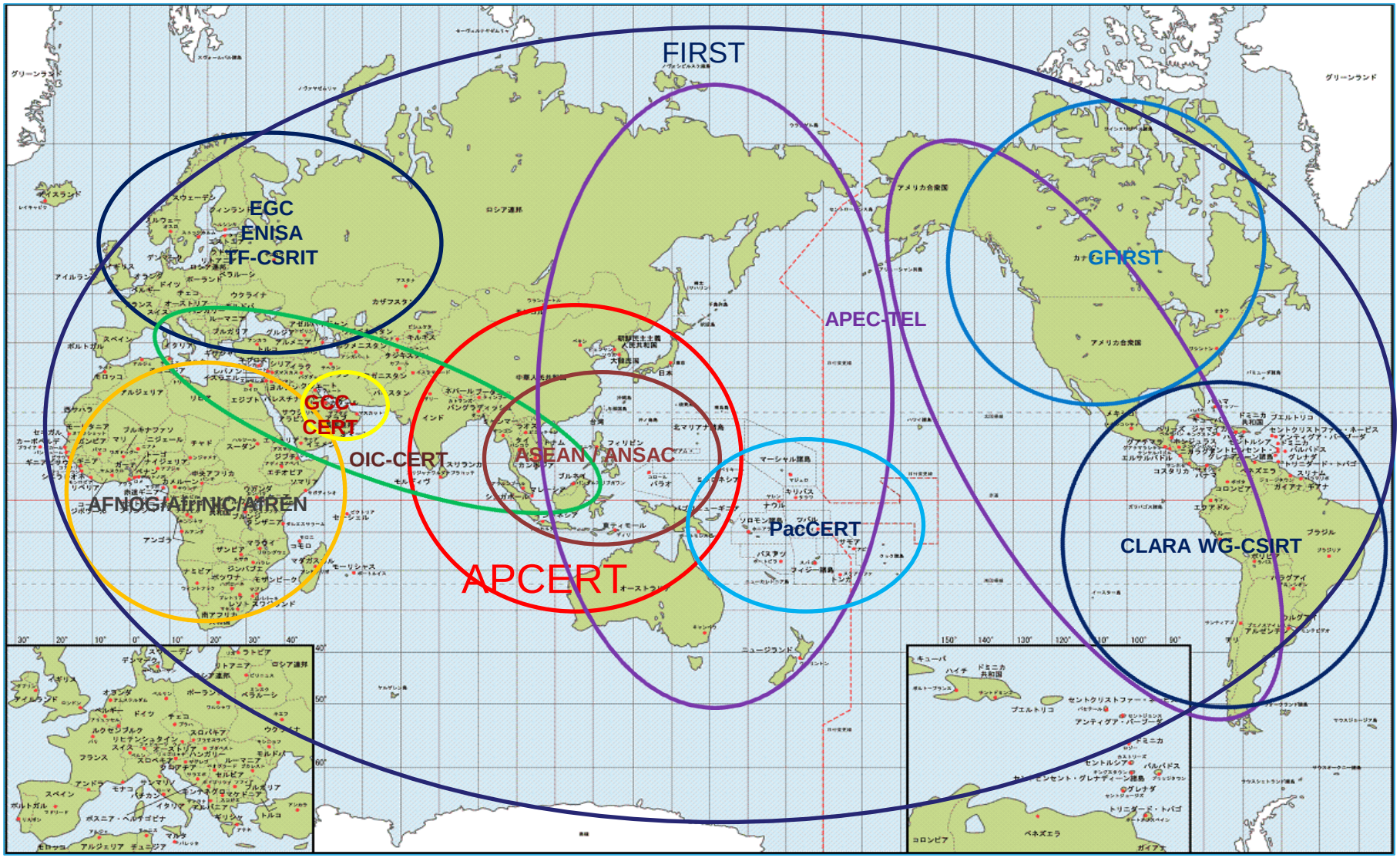


- Stage5: Collaboration **<-Thailand(ThaiCERT)**
- Stage4: Operation
- Stage3: Implementation
- Stage2: Planning
- Stage1: Education

Funding Model

- By Government
  - —National CSIRT mostly sponsored by any of Gov. Dept
- By Academia
  - —AusCERT, PacCERT(Pacific islands)
- By Industry(ISP, etc)
  - —CERT.br(Brazil)
- By Industry(Security venders)
  - —CERT-GIB(Russia)
- By international organization

CSIRT community in the world



Cyber Security Drill

Timeline

- **0700** Lord of Armageddon (LoA) declare cyber war on Beijing Olympics
- **0900** Co-ordinated **botnet attacks** from AP region causing **media sites and government portals inaccessible**
- **1100 Spam containing malware** that turns PC into zombies were filling up mailboxes in AP economies
- **1300** Border and Core routers crashing and rebooting frequently. **0-day exploit for Cisco IOS** rumoured to be available. Cisco promise to release fix in a few hours
- **1430** – Cisco released patch and advisory on critical IOS vulnerability
- **1600** – Security analysts announced that bots automagically removed themselves, no more attacks

APCERT

Especially if you want to be --

- National CSIRT
  - —National focal point within a country to coordinate incident handling activities
  - —Analyze incident and vulnerability information along with other teams, vendors, and technology experts to provide assessment for your constituency and communities
  - —Bridging the gaps – brings together multiple different sectors (cross domain, cross public private sectors, cross boarder)
  - —Developing mechanism for trusted communication for your community

JPCERT/CC

About JPCERT/CC

- Foundation
  - October, 1996

- Organization status
  - An independent, non-profit organization
  - Assigned by METI* as the vulnerability handling organization.

    * Ministry of Economy, Trade and Industry

About JPCERT/CC

- Constituency

- Internet users in Japan, mainly for enterprises
- Mainly providing service through technical staffs with high degree of professionalism (e.g. system administrators) in the enterprises

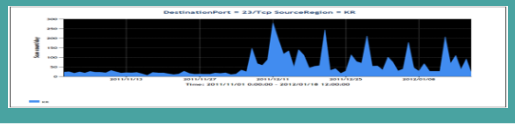
About JPCERT/CC - 3 pillars and 4 foundations -

Prevent
-Vulnerability Information Handling
- Coordinate with developers on unknown vulnerability information
- Secure Coding

JVN Japan Vulnerability Notes

Watch
-Information gathering / analysis / sharing

-Internet Traffic Monitoring
- Alerts / Advisories



Respond
- Incident Handling
- Mitigating the damage through efficient incident handling
- Information sharing to prevent similar incidents

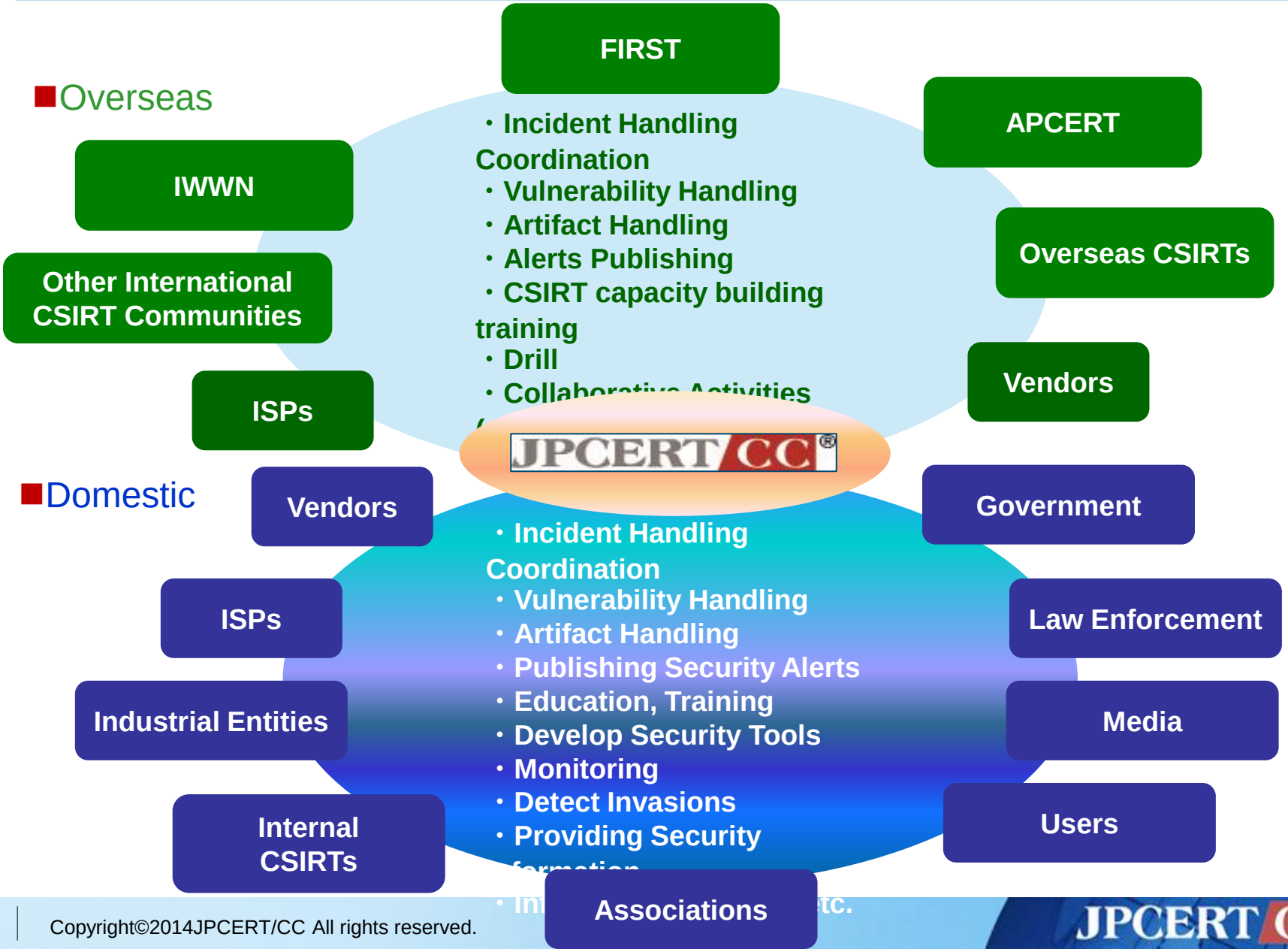
Early Warning Information
Information sharing with critical infrastructure enterprises, etc.

CSIRT Establishment Support
Capacity building for internal CSIRTs in enterprises / overseas national CSIRTs

Artifact Analysis
Analysis on attack methods / behavior of malware (unauthorized program)

International Collaboration
Collaboration with overseas organizations for smoother handling of incidents and vulnerabilities

About JPCERT/CC



Collaborative activities in Japan

Council of Anti-Phishing Japan(APC)

フィッシング対策協議会
Council of Anti-Phishing Japan

- Secretariat

Nippon CSIRT Association (NCA)

CSIRT
日本シーサート協議会

- Founding member
- Chair
- Secretariat

FYI: CSIRTs in Japan

NCA's Founding Member

- HIRT (Hitachi Incident Response Team)
- IIJ-SECT (IIJ group SEcurity Coordination Team)
- JPCERT/CC
- JSOC (Japan Security Operation Center)
- NTT-CERT (NTT Computer Security Incident Response and Readiness Coordination Team)
- SBCSIRT (Softbank Telecommunications Security Incident Response Team)

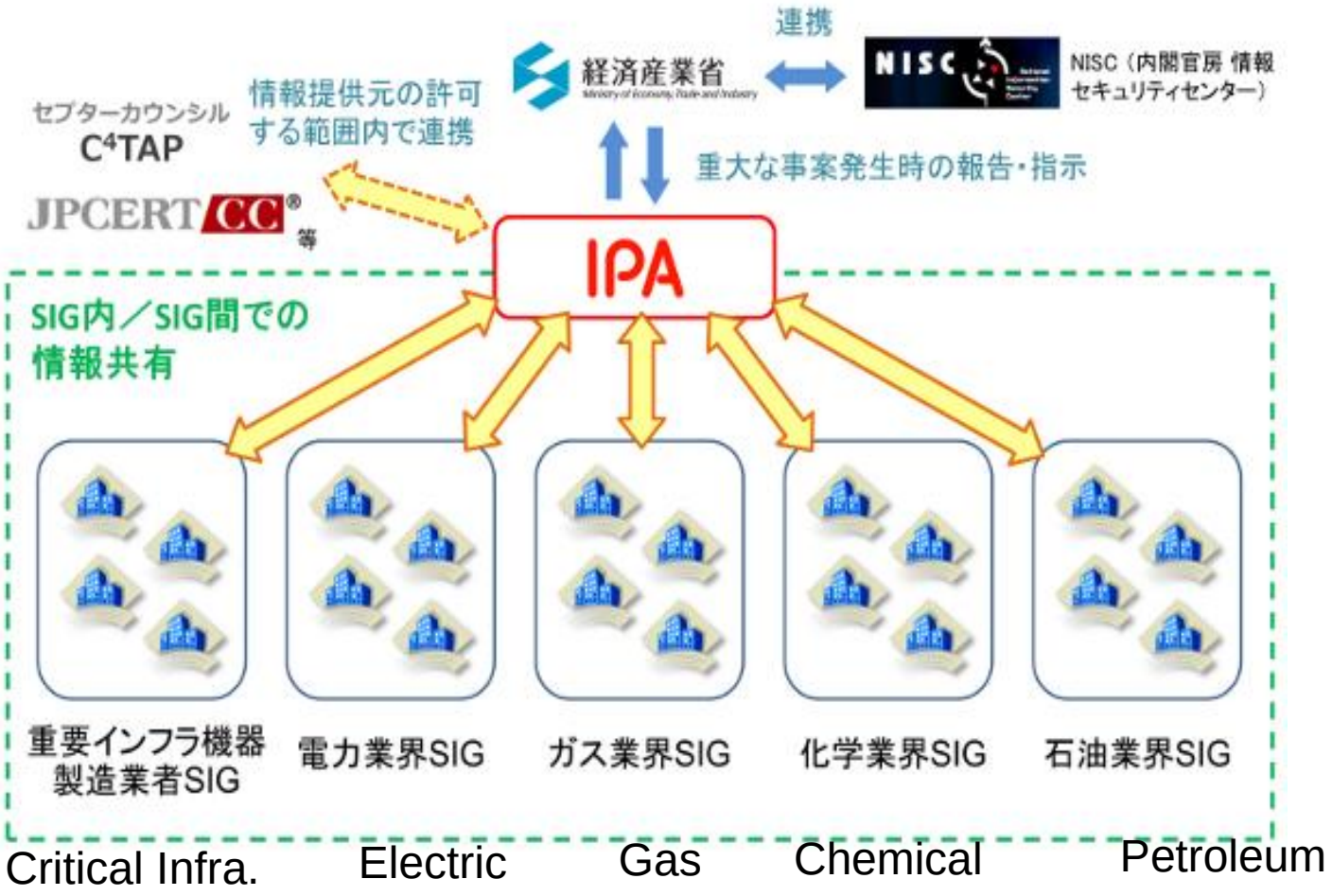
NCA's Current Member (as of April 2014)

- 49 teams
- Mainly from the CSIRTs in Japanese ICT companies and financial companies

Collaborative Activities with partners in Japan

Initiative for Cyber Security Information Sharing Partnership of Japan

J-CSIP



International and Regional Collaborative Activities

- Forum of Incident Response and Security Teams (FIRST)

  - The first Japanese CSIRT to obtain membership
  - Current Steering Committee Member

- Asia Pacific Computer Emergency Response Team (APCERT)

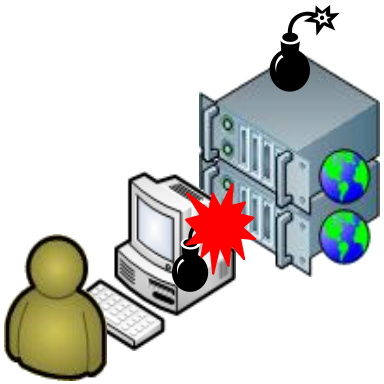
  - Founding member
  - Current Chair
  - Current Steering Committee Member
  - Secretariat since its foundation

About JPCERT/CC

- Our services

Reactive Service	Proactive Service	Security Quality Management Service
•Incident handling •Industrial Control System Incident Handling •Vulnerability handling •Artifact (malware) analysis	•Alert and advisory •Network traffic monitoring (TSUBAME)	• Control system security awareness building • Secure coding awareness building • Capacity building for overseas CSIRTs

Incident Handling Flow (Simplified)



- Victim
- Incident Detectors
- Relevant Parties, etc.

1

Incident Report
(Request for countermeasure)

JPCERT/CC®

2

Appropriate Parties

- ISP/ASP
- System administrators
- CSIRTs, etc.

3

4

Feedback Report

Countermeasure Response

Incident Handling in 2013

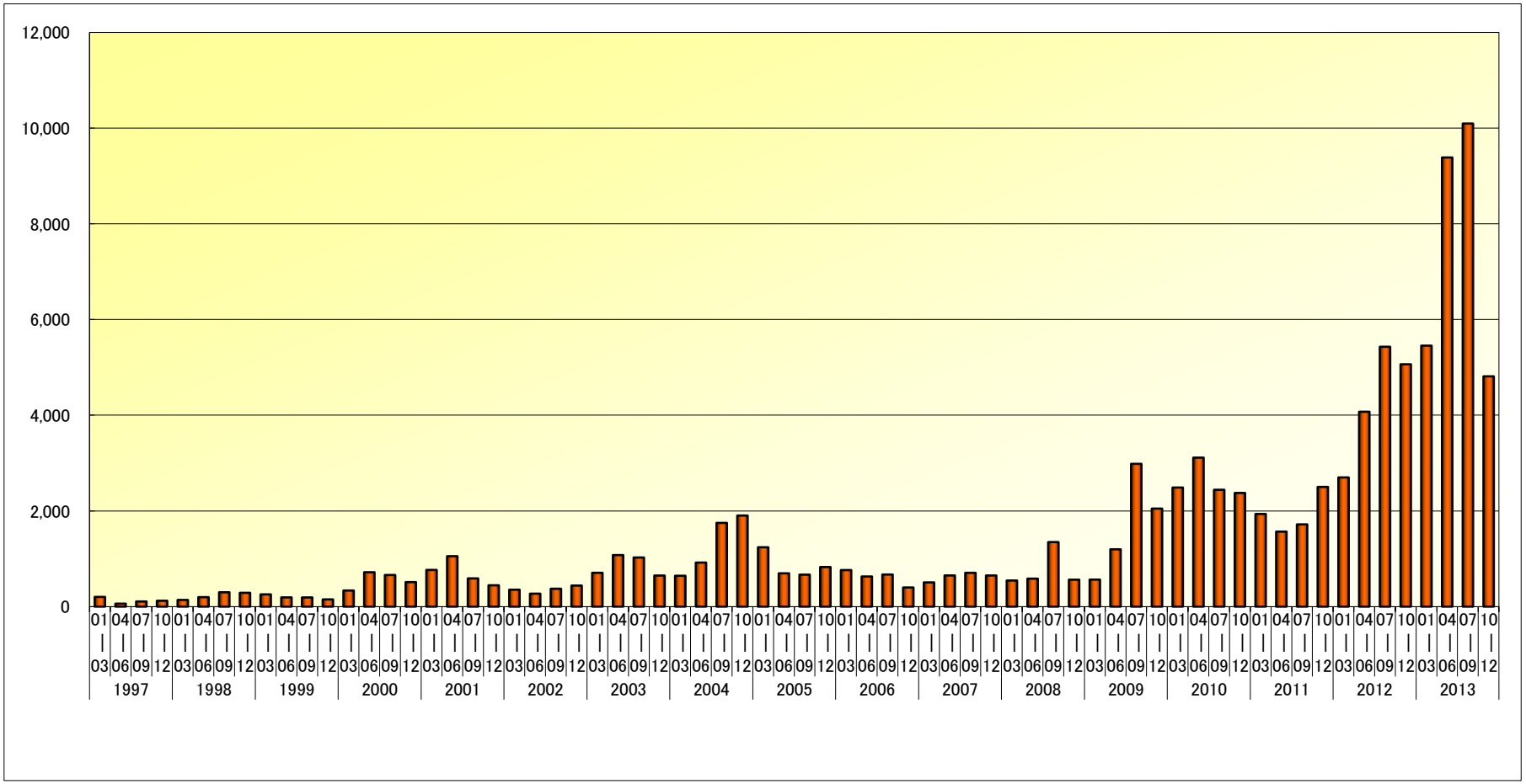
- 29,746 incident reports received (2013)

1st Quarter	2nd Quarter	3rd Quarter	4th Quarter	Total
5,453	9,386	10,095	4,812	29,746

cf. 17,265 (2012)

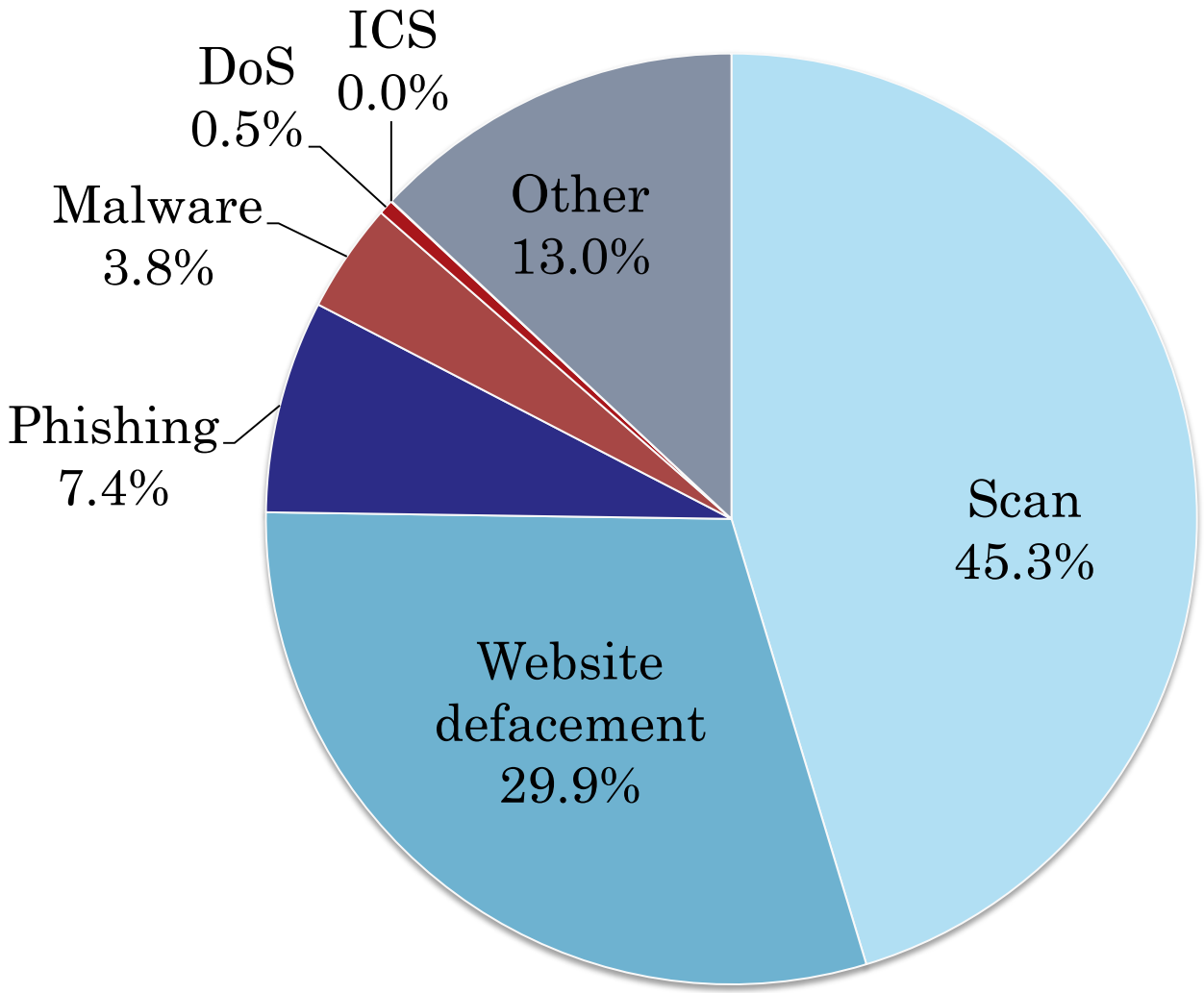
Incident Handling in 2013

- Number of incident reports received



Incident Handling in 2013

- What kind of incidents have been reported?



Vulnerability Handling

- Vulnerability: A weakness in a product which may allow an attacker to reduce a system's security.

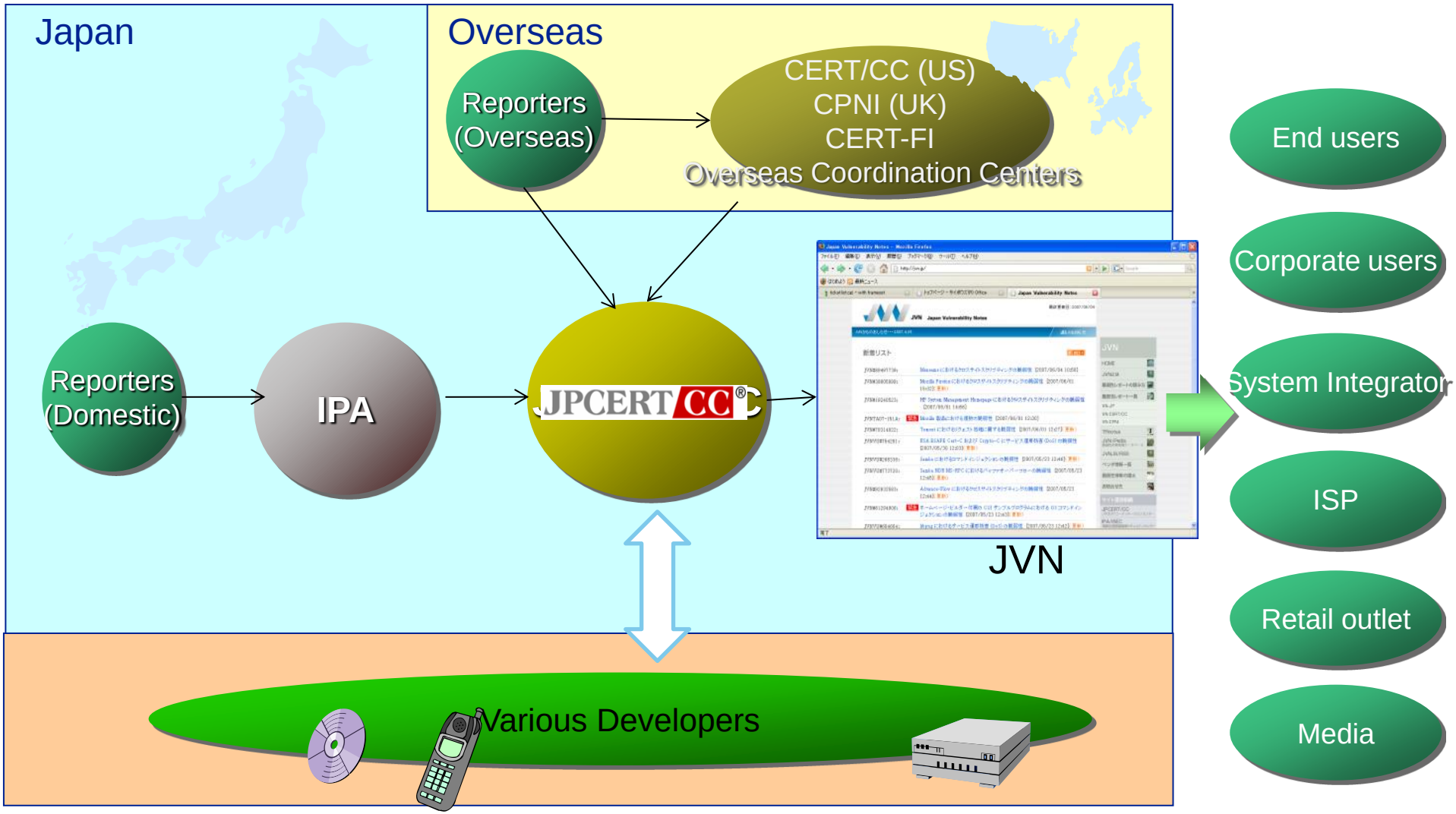
- JPCERT/CC is assigned by the Ministry of Economy, Trade and Industry (METI) to coordinate and communicate with the vendors and vulnerability disclosures. (Announcement #235)

- Information being published on JVN (https://jvn.jp/en/)

- In 2010, JPCERT/CC was approved by the MITRE Corporation*1 as CNA (CVE*2 Numbering Authority).

*1 An American not-for-profit organization
*2 Common Vulnerabilities and Exposures

Vulnerability Handling



Artifact (Malware) Analysis

- What is malware?

  Malicious Software

  - Broader in concept than a computer virus
  - Virus, Worm, Trojan Horse, Rootkit, Bot, DoS Tool, Exploit kit, Spyware

- Why do CSIRT need Malware Analisis?
  - To utilize the analysis result for CSIRT's basic activities
  - To verify the public information (it could be wrong)
  - To keep up on the attacking trends
  - To evaluate threat

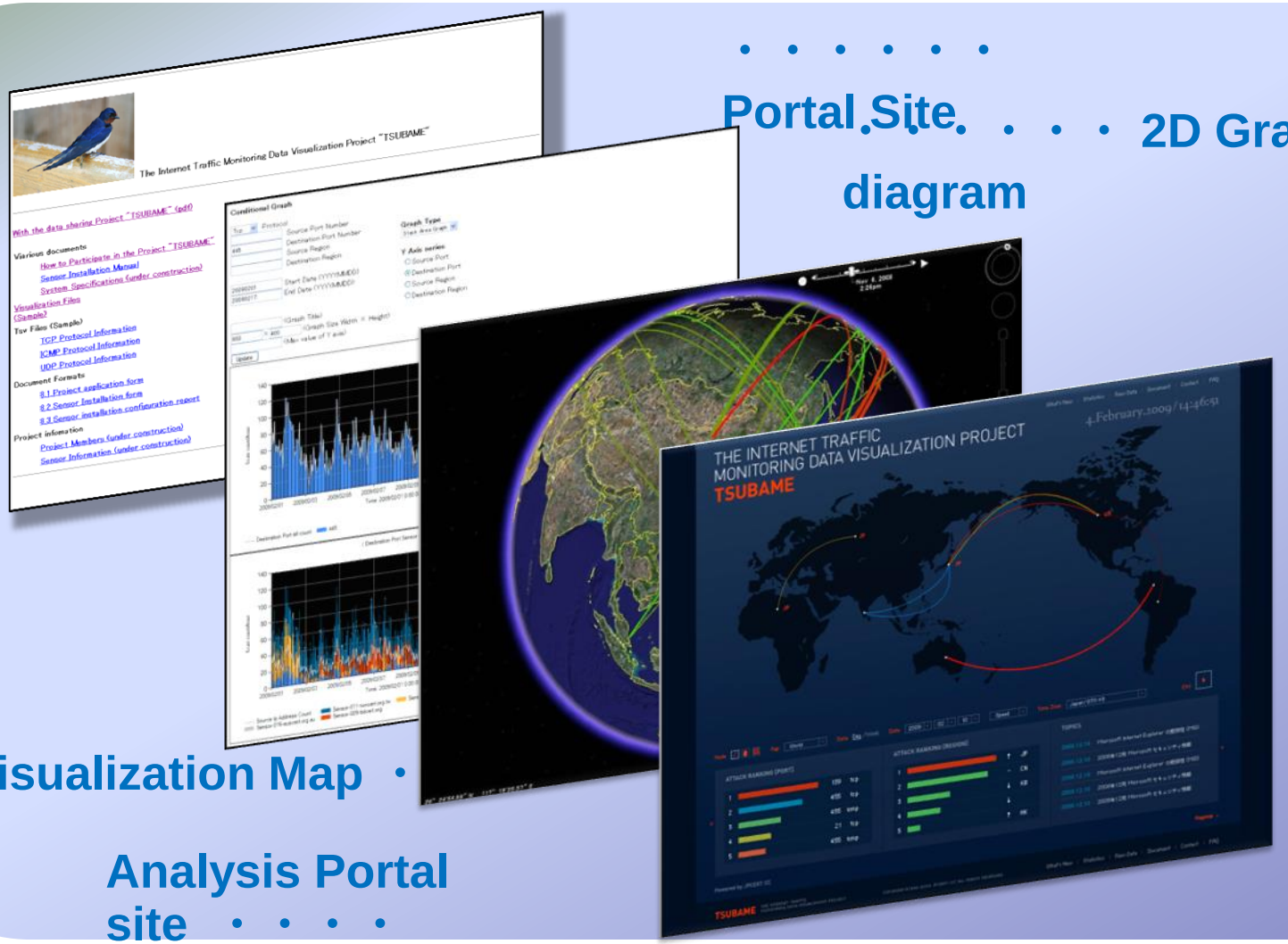
Alerts and Advisories

- Security Alerts
  - Issued when necessary (about 20-30/year in average)
  - Countermeasures for incidents with high impact
- Early Warning Information
  - Issued when necessary
  - Security alerts with confidentiality
  - For critical infrastructure entities
- Vulnerability Information
  - Issued when necessary
  - Provided via portal site (JVN)
- Analyst Note
  - Issued every working day
  - Useful security information gathered by the analysts

Alerts and Advisories

- JPCERT/CC Weekly Report
  - Vulnerability information and security tips
- JPCERT/CC Artifact Analysis Report
  - Monthly issue
  - Trend and latest information on malware
  - Delivered to the interested teams in overseas
- JPCERT/CC Industrial Control System News Letter
  - Monthly issue
  - Delivered to the interested Japanese companies
- TSUBAME News Letter
  - Issued when necessary
- Twitter

TSUBAME Project



Portal Site . . . . . 2D Graphic diagram

3D Visualization Map . . . . . Analysis Portal site

Control System Security Awareness Building

- ICS (Industrial Control System) :

"System which controls and manages other devices or systems"

  - Electric power grid, gas, water supply and sewerage
  - Traffic and transportation
  - Environmental monitoring
  - Manufacturing facilities in plants…etc.

Control System Security Awareness Building

- What JPCERT/CC does for ICS Security:

- Incident and vulnerability handling operation to the ICSs in Japan
- Annual technical conference on ICS security
  - Information sharing opportunities for ICS engineers
- Monthly newsletter (in Japanese)
  - Citation of major global news on ICS security
- Distribution of ICS security self assessment tool “SSAT”
  - Simple MS/Excel-based tool for asset owners to assess their level of ICS security
  - Originally developed by CPNI*1 in U.K

*1 : Centre for the Protection of National Infrastructure (CPNI)

Secure Coding Awareness Building

- Why do we need secure coding?
  - Vulnerabilities exist in IT products
  - Products should be secure from coding process
- In which programming language?
  - C/C++
  - Java

Japanese materials were translated recently by JPCERT/CC. Original material were composed by CERT/CC.

  - Android
- Seminars are conducted in Japan and overseas to:
  - Have the engineers understand vulnerabilities and attack mechanisms
  - Have the engineers learn useful examples of actual secure coding methods, and how to study further

Capacity Building for Overseas CSIRTs

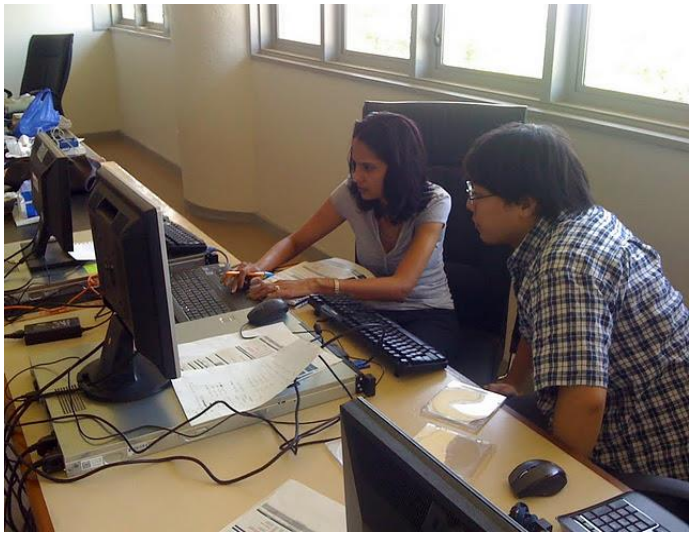
- CSIRT Development Training
  - Cambodia(’07,’08), Indonesia(’10), Lao(’07, ’09,’12 , ‘13), Mongolia(’09, ‘13), Myanmar(’07, ’11x2, ’12x2), Qatar (’06), Thailand(’12), Vietnam(’10x2)
  - Pacific Islands (PacCERT) ’11 - (ongoing)
  - Africa (AfricaCERT) ’10 - (ongoing)

- C/C++ Secure Coding Seminar
  - India(’10), Indonesia(’09, ’11), Philippines(’10), Thailand(’09, ’11), Vietnam(’10x2)

- Java Secure Coding Seminar
  - Indonesia(’12), Thailand(’12)
- Android Secure Coding Seminar
  - Thailand(’12)
- AOTS Information Security Training in Tokyo for ASEAN countries (’08 -’11)
- Information security training for ASEAN countries as part of the ASEAN-Japan Information Security Training in Tokyo, organized and hosted by NISC (’11)

Capacity Building for Overseas CSIRTs

- Support for Pacific Islands
  - “PacCERT” newly established
  - Supported by JICA
  - Dispatching short-term experts starting from July, 2011
  - On–the-job training in September, 2012
  - Provision of “CSIRT in a Box”



Capacity Building for Overseas CSIRTs

- On-site Training for Africa
  - Training during AFRINIC-19, 2013 (Côte d'Ivoire)

Current / future collaboration with Thailand

- with ThaiCERT/ETDA
  - Concluded MOU(Memorandum of Understanding) in April, 2012.
  - Organized Java/Android secure coding seminar in 2012.
  - Collaborating through FIRST, APCERT and TSUBAME project.
  - Joint acitivities:
    - Conduct training for LaoCERT
      - October 2012/2013, and May 2014(next week)
      - ThaiCERT colleagues kindly have charge of RTIR(Request Tracker for Incident Response).
      - As a bridge between JP and Lao to overcome the language barrier.
- JPCERT/CC is willing to expand our collaboration with EGA!

TRENDS OF CYBER ATTACKS IN JAPAN

Contents

1. Why do cyber attacks happen?
2. Overview of recent cyber threats in Japan
3. Case study on Incident
4. Conclusion

1. Why do cyber attacks happen?

- The intent and motive of cyber criminals
  - Past

Most of the hackers engage in cyber attacks in order to proof their cyber capability. It was like a trick rather than a seriously harmful attacks.

  - Recent

Hackers nowadays are after monetary gain, commercial gain and national gain. They are to steal money from banks, pull out confidential information from firms and to monitor or restrain hostile countries by displaying their cyber capabilities at national level.

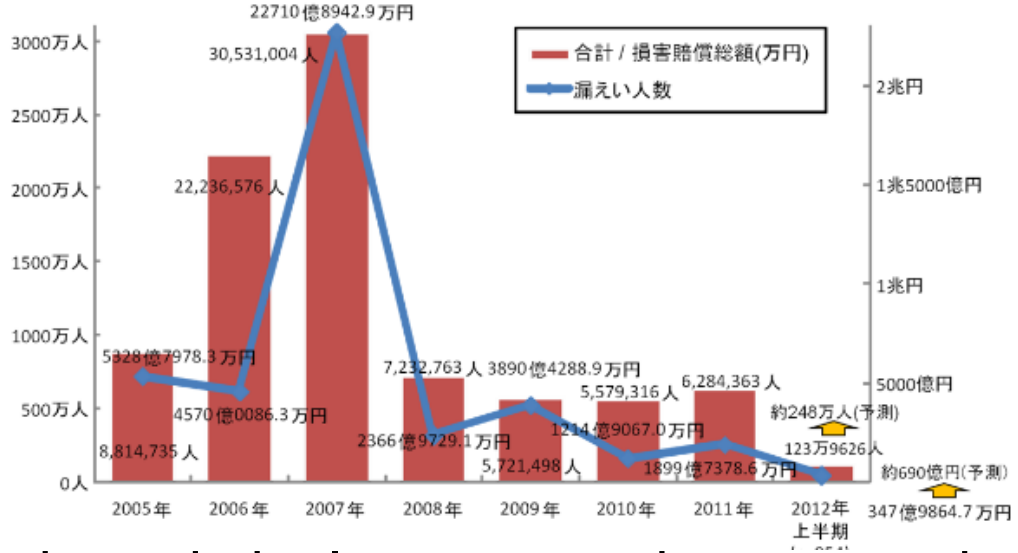
→ Attacks are more organized and sophisticated

1. Why do cyber attacks happen?

- Impact of loss in Japan

  Overall loss in year 2011 caused by Information leakage

Approx. ¥190 billion(JPY) ≈ $ 2,400 million(USD)



The rate of cyber criminal arrestment is comparatively lower than other crimes. Therefore, cyber crimes has become a major issue.

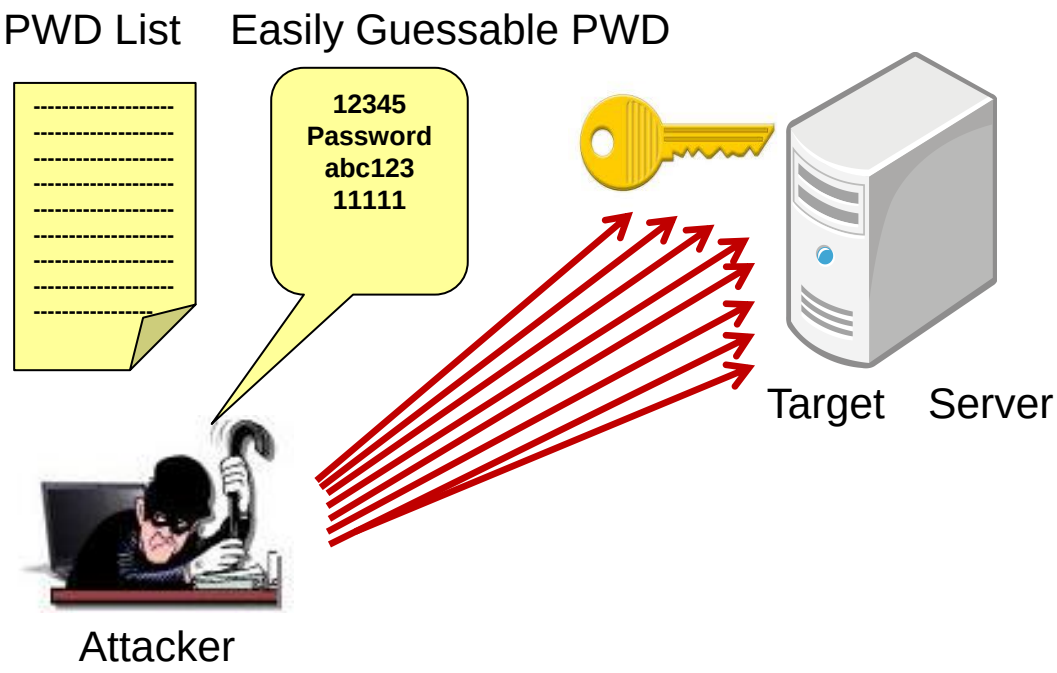
Source :Japan Network Security Association (JNSA)
http://www.jnsa.org/result/incident/data/2012H1_incident_survey_sokuhou_v1.0.pdf

2. Overview of recent cyber threats in Japan

- Brute Force Attack (Using Password List)
- Website Defacement
- DDoS Attack
- Phishing
- ICS (Industrial Control System)
- Targeted Email Attack

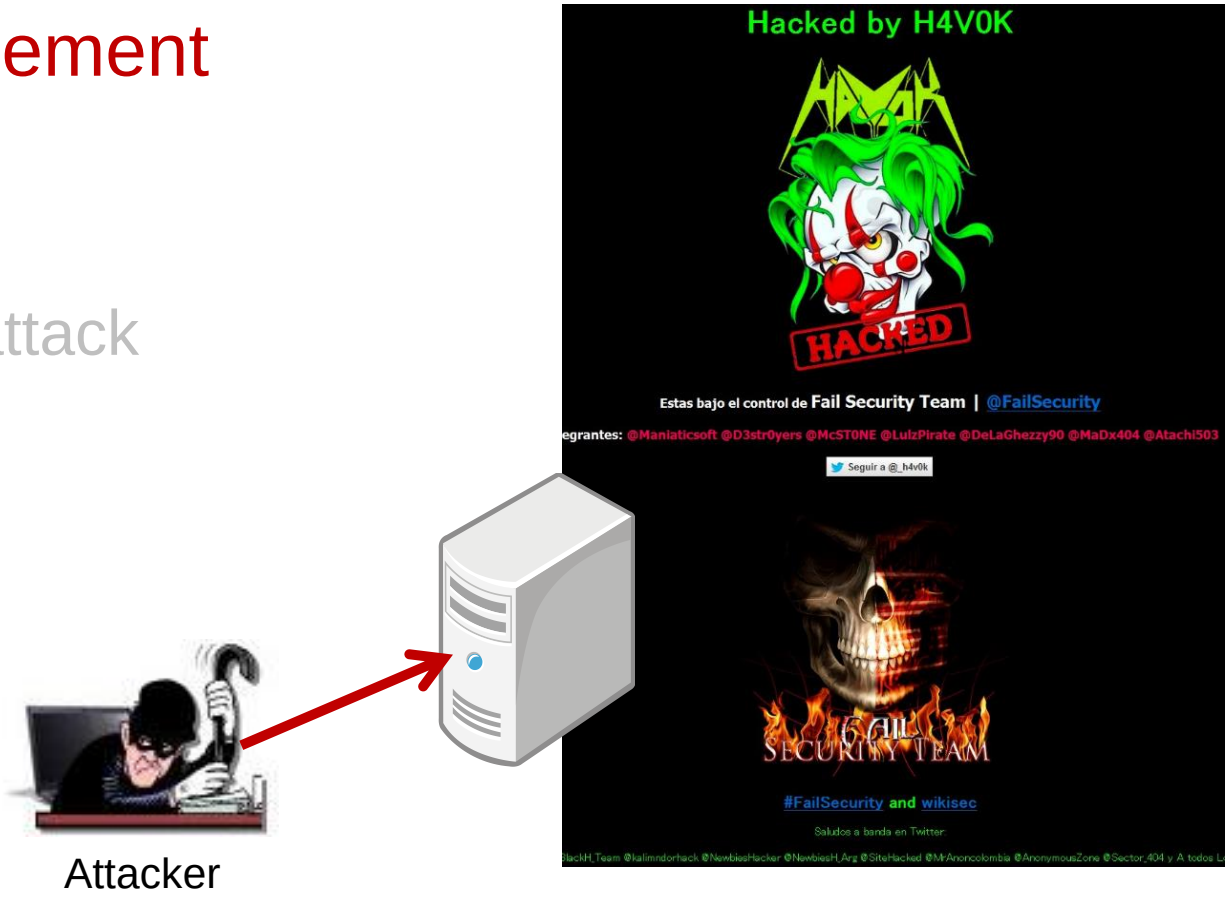
2. Overview of recent cyber threats in Japan

- Brute Force Attack (Using Password List)
- Website Defacement
- DDoS Attack
- Phishing
- Targeted Email attack



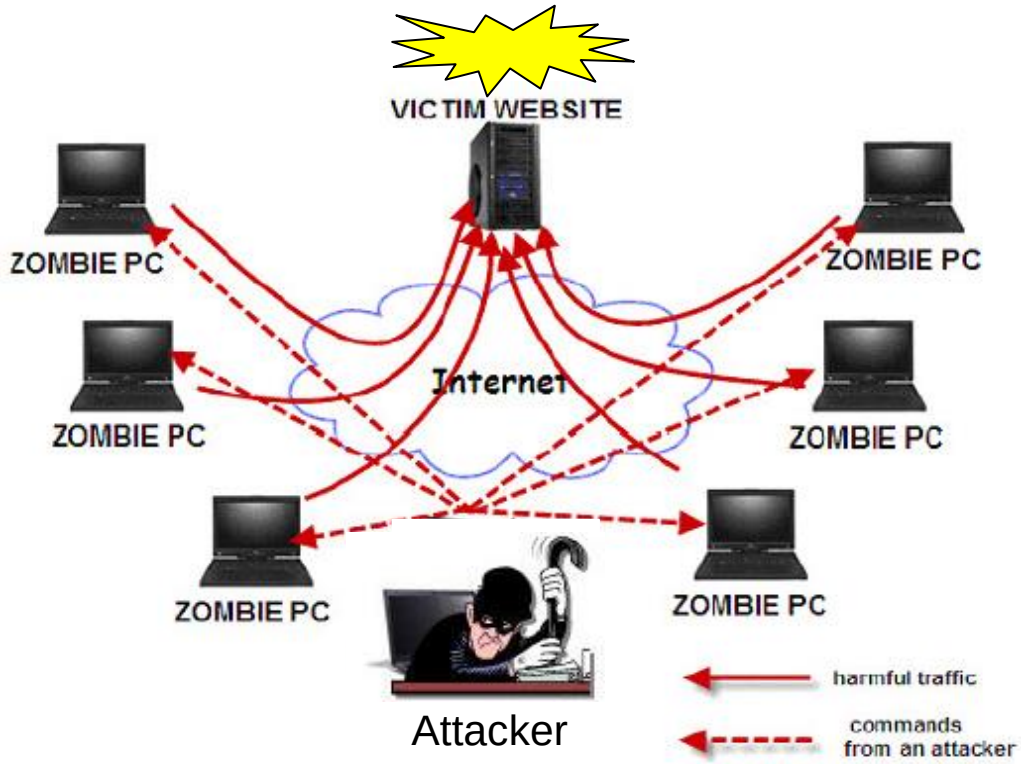
2. Overview of recent cyber threats in Japan

- Brute Force Attack
- Website Defacement
- DDoS Attack
- Phishing
- Targeted Email attack



2. Overview of recent cyber threats in Japan

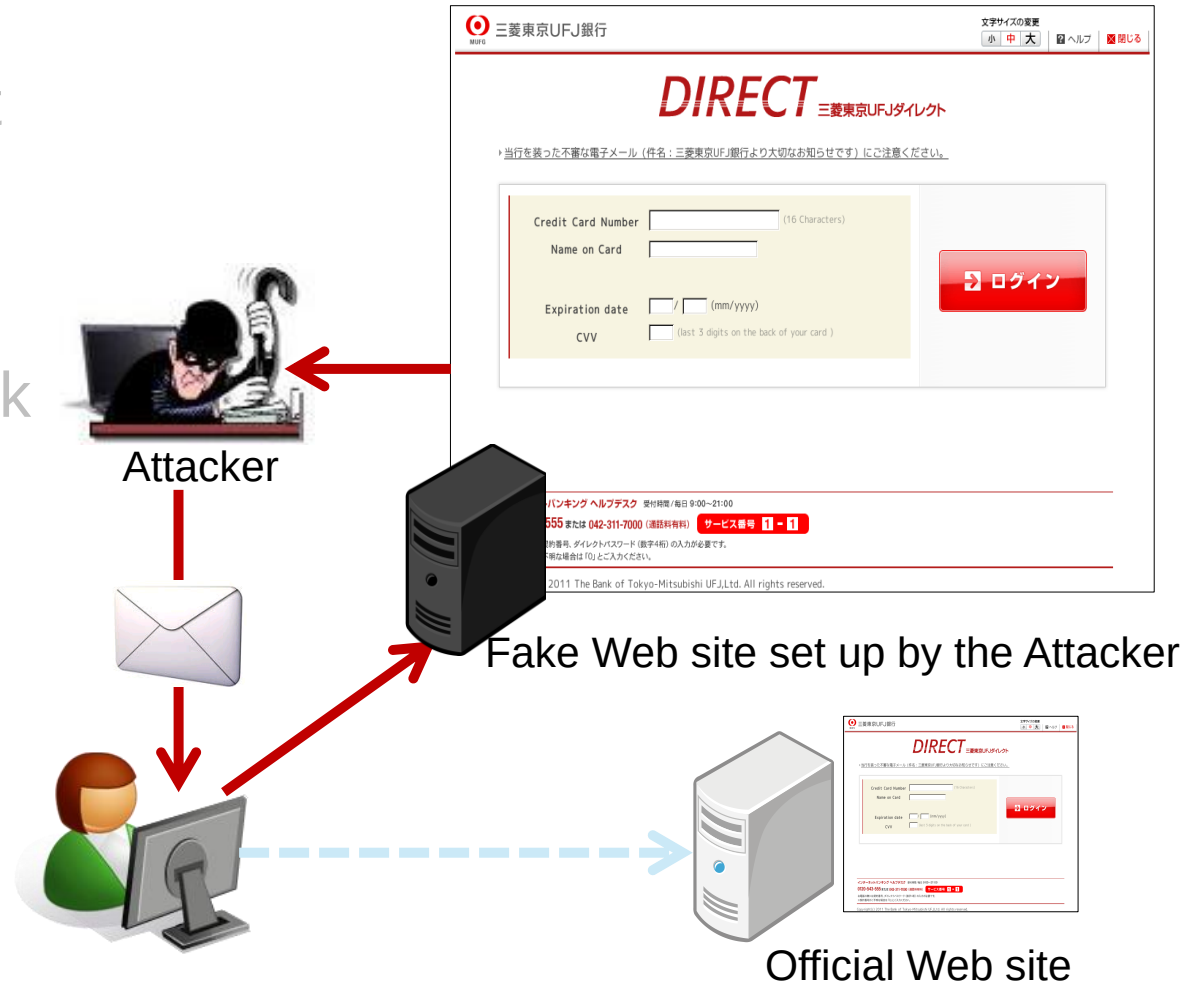
- Brute Force Attack
- Website Defacement
- DDoS Attack
- Phishing
- Targeted Email attack



Source : Computer Tips
http://yourpctips.com/Computer-Tips-and-Tricks/prevent-ddos-attacks.html

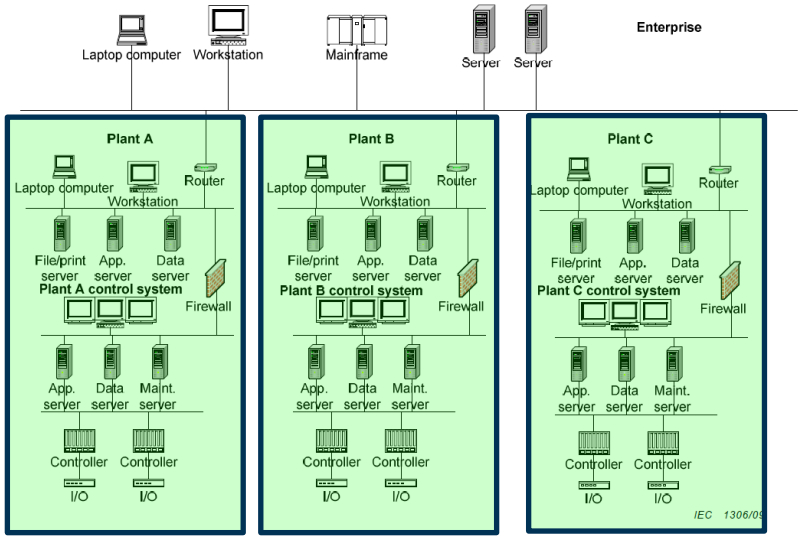
2. Overview of recent cyber threats in Japan

- Brute Force Attack
- Website Defacement
- DDoS Attack
- Phishing
- Targeted Email attack

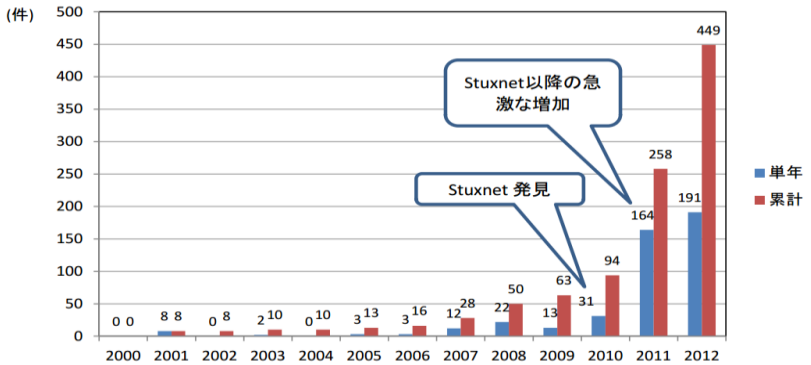


2. Overview of recent cyber threats in Japan –
Not Limited To Just ICT !!!

Industrial Control Systems Network



Publication of the ICS Vulnerabilities



（出所：OSVDB データより作成）

Stuxnet is a computer worm discovered in June 2010 that is believed to have been created by the United States and Israel to attack Iran‘s nuclear facilities. Stuxnet initially spreads via Microsoft Windows, and targets Siemens industrial control systems. It is the first discovered malware that spies on and subverts industrial systems, and the first to include a programmable logic controller (PLC) rootkit.

Symantec W32.Stuxnet
http://www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99

2. Overview of recent cyber threats in Japan

- Brute Force Attack
- Website Defacement
- DDoS Attack
- Phishing
- Targeted Email Attack

Let’s see a case study on this incident.

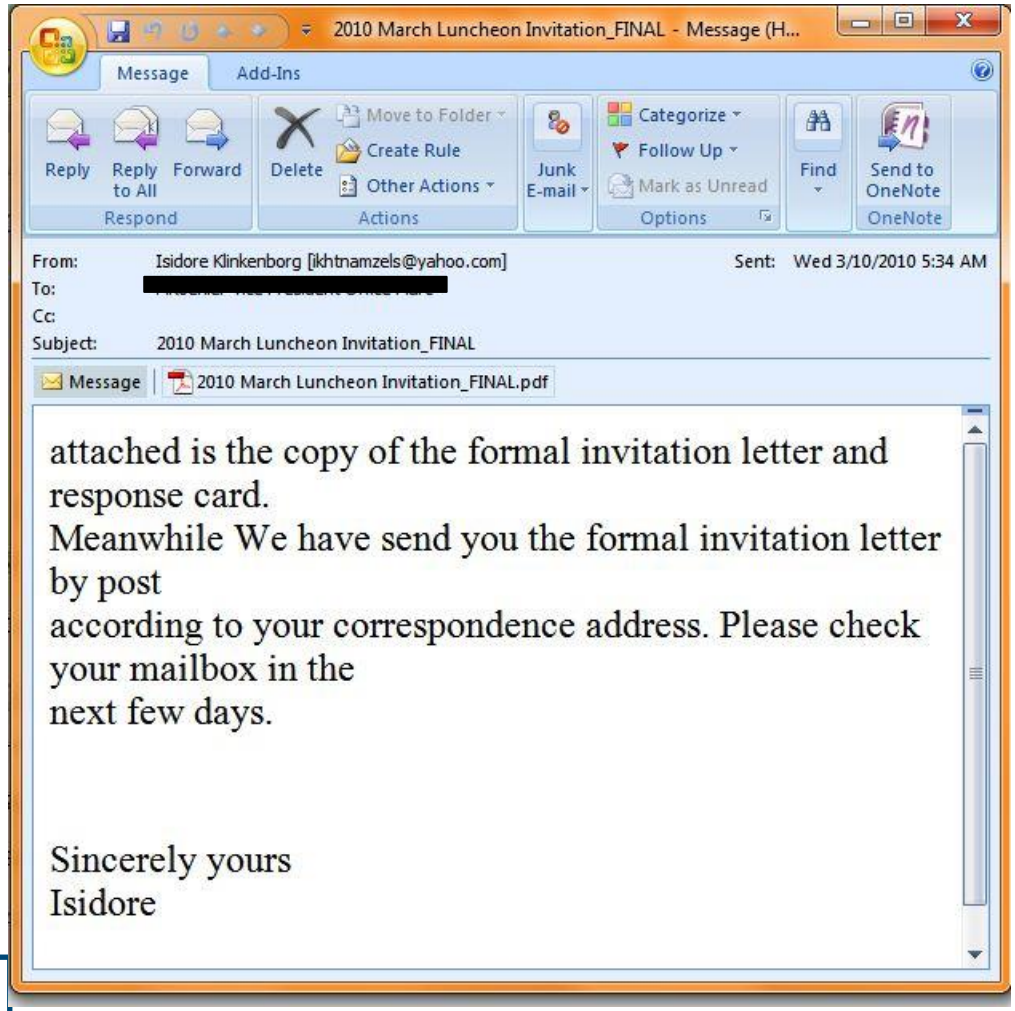
3. Case study on Incident - Targeted Email Attack -

- Is this email malicious?

From: Isdore Klimkenborg

Subject: 2010 March Luncheon Invitation_FINAL

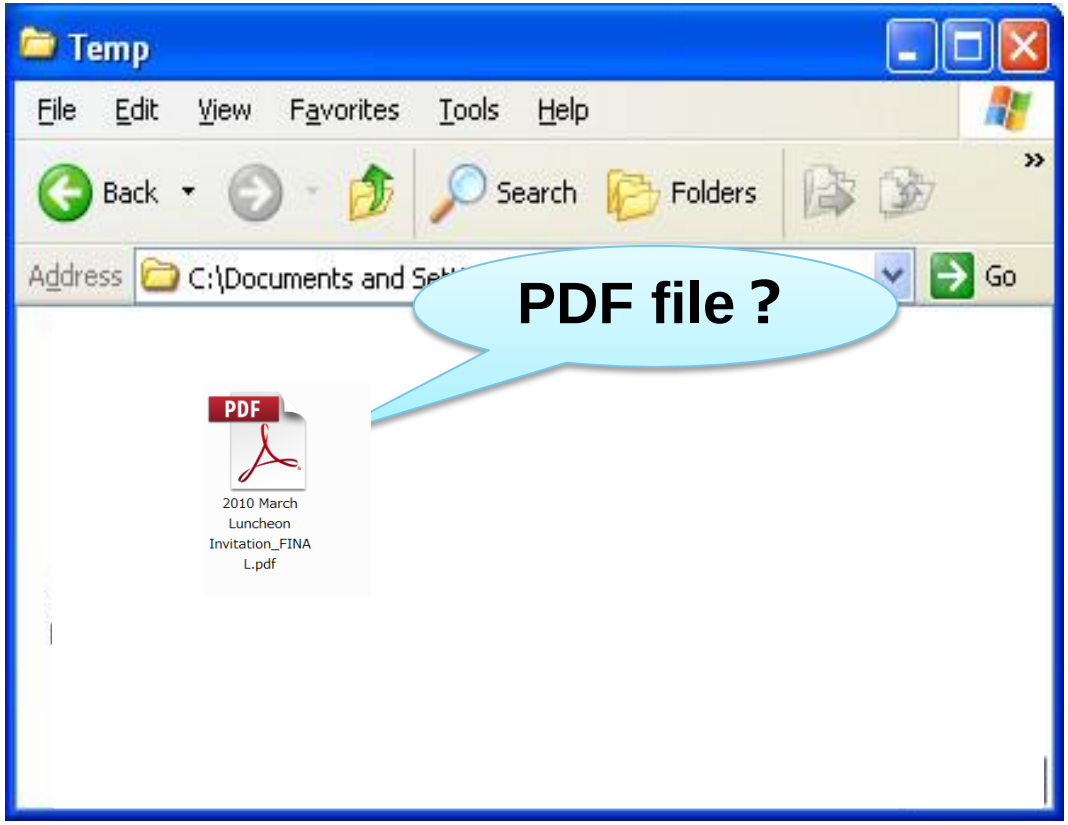
Attachment: 2010 March Luncheon Invitation_FINAL.pdf



Source: F-secure blog
http://www.f-secure.com/weblog/archives/00001908.html

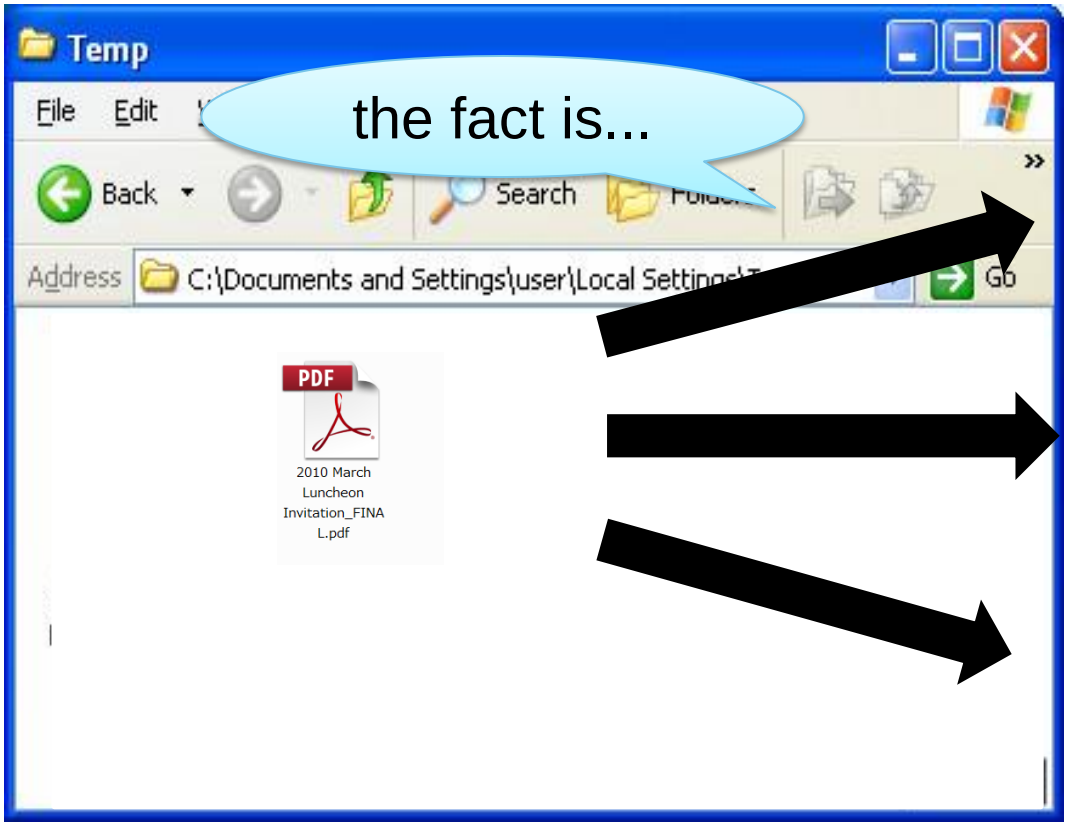
3. Case study on Incident - Targeted Email Attack -

- What is the type of the attached file?



3. Case study on Incident - Targeted Email Attack -

At a glance, it looks like a PDF file...



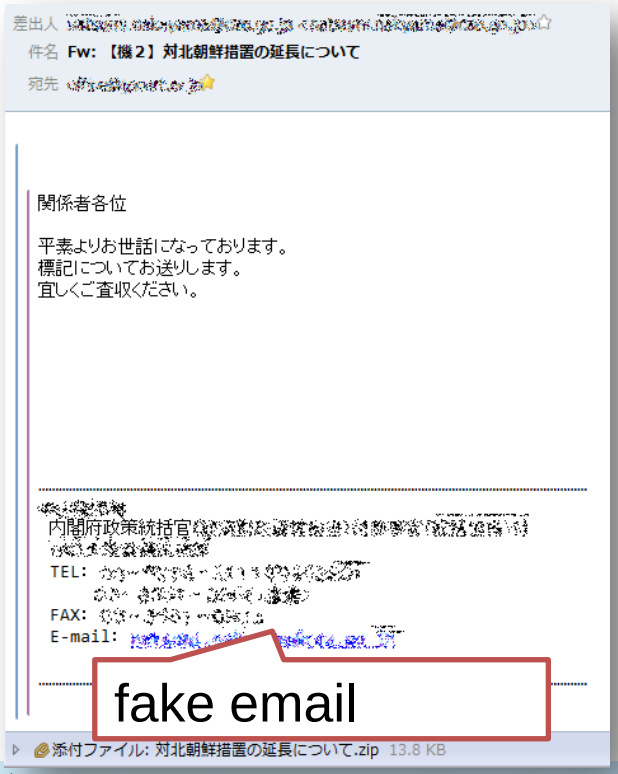
Application file
File icon is disguised as PDF file

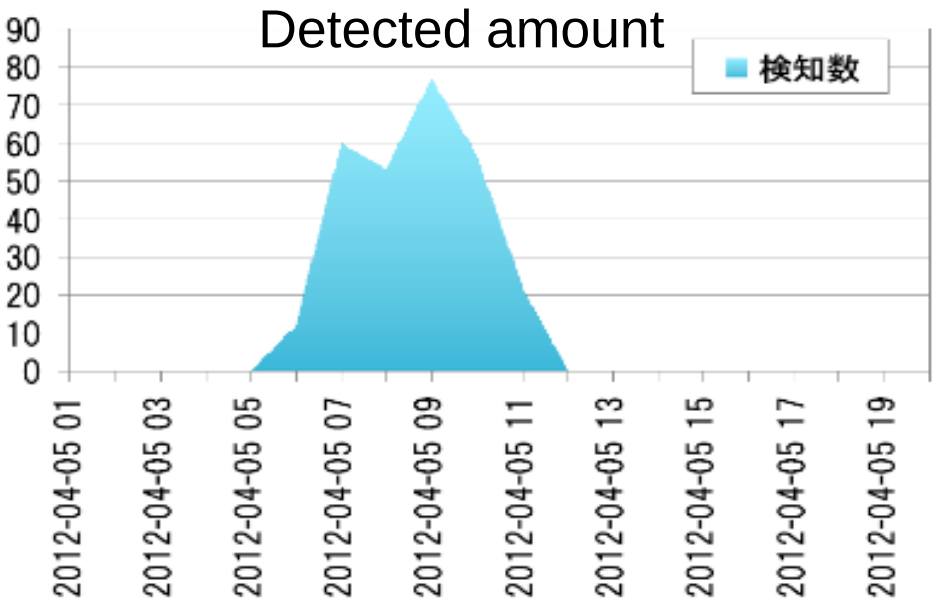
Application file
Portion of the file name is displayed in reverse order by RLO

Application file
Exe is not displayed due to long-continued file name

3. Case study on Incident - Targeted Email Attack -

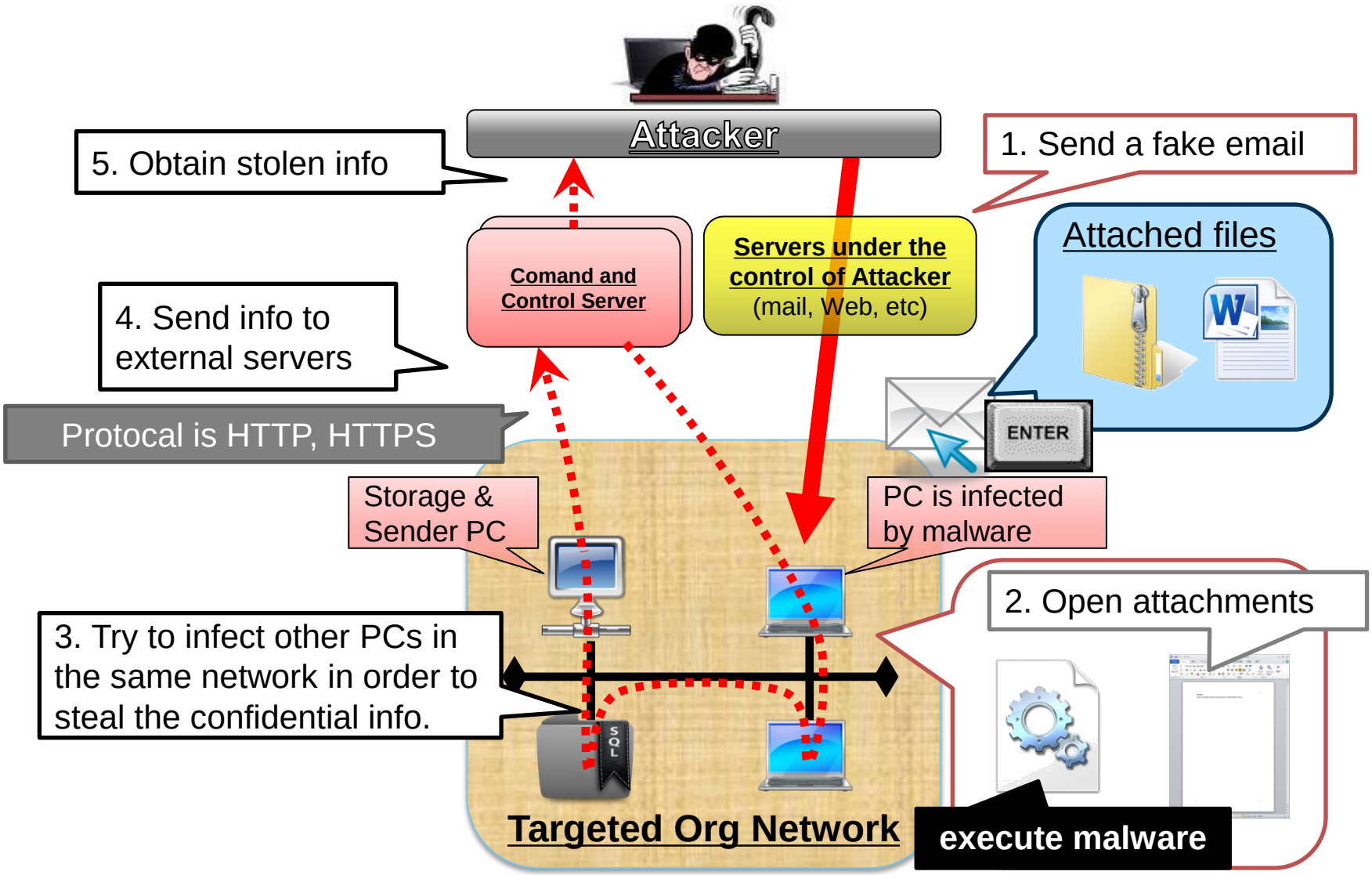
JPCERT/CC has also received a targeted email which impersonates a sender as a government agency. The attached malware was Poison Ivy, a type of RAT (Remote Access Trojan).





Source: Tokyo SOC Report
https://www-304.ibm.com/connections/blogs/tokyo-soc/entry/virus_mail_20120405?lang=ja

3. Case study on Incident - Targeted Email Attack -



4. Conclusion

“My security is your security.

Your security is my security.”

We hope that JPCERT/CC presentations contribute to your security awareness, and now is your turn to accelerate your activity in Thailand!

Thank you! / Khob khun!

- JPCERT/CC (office@jpcert.or.jp)
  - Tel: +81-3-3518-4600
  - https://www.jpcert.or.jp
  - http://jvn.jp
- JPCERT/CC Global Coordination Division
  - Email: global-cc@jpcert.or.jp
- Incident Report
  - Email：info@jpcert.or.jp

PGP Fingerprint：
BA F4 D9 FA B8 FB F0 73 57 EE 3C 2B 13 F0 48 B8

SUPPLEMENT

References 1

CERT Coordination Center - CSIRT Development
http://www.cert.org/csirts/

Handbook for CSIRTs
http://www.cert.org/archive/pdf/csirt-handbook.pdf

CSIRT Services
http://www.cert.org/archive/pdf/CSIRT-services-list.pdf

Organizational Models for Computer Security Incident Response Teams
http://www.cert.org/archive/pdf/03hb001.pdf

References 2

Forum of Incident Response and Security Teams
http://www.first.org/

Alphabetical list of FIRST Members
http://www.first.org/members/teams/

Members around the world
http://www.first.org/members/map/

TERENA - CSIRT Starter Kit
http://www.terena.nl/activities/tf-csirt/starter-kit.html

Asia Pacific Computer Emergency Response Team
http://www.apcert.org/

References 3

- *CSIRT Culture*
  - *My security is depending on your security*

1. *Collaboration*
   - *Security is not competition*
   - *Share Expertise/Resource*
   - *Share best practices*

2. *Web of TRUST*
   - *most important thing for CSIRT*
   - *High level service is required to get the TRUST*
   - *Reputation business – you live or die with this*