

Incident Handling Cases of Japan ~ JPCERT/CC experiences ~

Keisuke Kamata

Deputy Director
Global Coordination Division
JPCERT/CC, Japan

How JPCERT/CC work with IT industry in Japan ?

- * Building trust relationship Japanese IT stakeholders
 - * Japanese Government
 - * Ministry, Agency, Law enforcement, and so on
 - * Critical Infrastructures
 - * Electricity, Gas, Airline, Train Transportation, Water, Finance
 - * Medical, Logistics, Government Service, Telecommunication
 - * Associations
 - * Bank, ISP, IT service, Hardware Vendors, Software developers
 - * Others
 - * Individual Organizations
 - * IT related company, Academic organization
 - * Non profit organization, Media, and so on



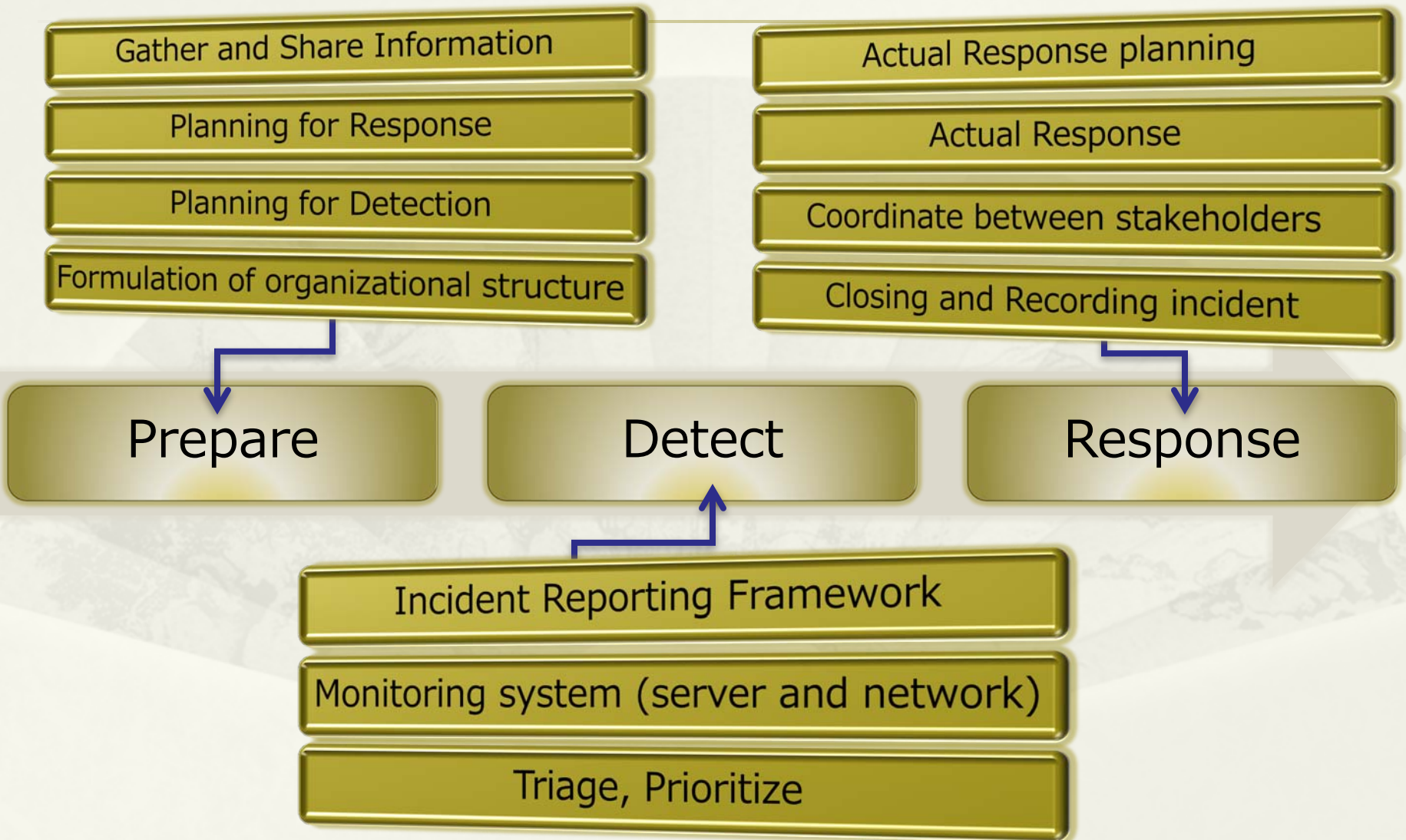
Incident Handling Cooperation Overview





Domestic Cooperation

Incident Response overview



Who is key entity of public sector ?

* Public sector

- * National Information Security Center : NISC
- * Ministry of Economy, Trade and Industry : METI
- * Ministry of Internal affairs and Communication : MIC
- * Ministry of Defense, National Police Agency of Japan, other ministries
- * Local Government
- * Information technology Promotion Agency
- * And so on

Who is the key entity of private sector ?

- * Private sector
 - * Critical Infrastructure Companies
 - * Especially with ISP, Bank
 - * Associations
 - * IT area
 - * Hardware Software vendors
 - * Microsoft, Hitachi, Fujitsu, NEC ...
 - * System Integrators
 - * Web commerce company
 - * Portal site
 - * Research Institutions
 - * Companies
 - * Academic institutions

Others ?

- * JPRS or JPNIC
- * Internet exchange
- * Japan Network Operators Group : JANOG
- * JEAG : anti-spam group
- * Anti-phishing Council of Japan
- * Open Source Community
- * Personal software developers
- * User community
- * End users

How we are working with them ?

1. Obtain suitable point of contact in each organizations
2. Building Trust Relationship
3. Information exchange, interaction, and keep in touch
4. Respond to their request seriously
5. Work as a Coordinator, Provide technical information, Technical assistant

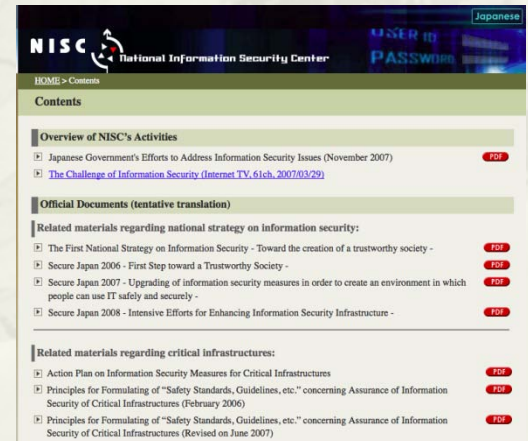


Case study

- * Conduct meeting for organizations who have similar problem
 - * Hardware vendors for some specific vulnerability information
 - * Anti Abuse Group
 - * Discussion with world well known security expert
- * Face to Face meeting
 - * To understand each other
 - * To make them understand “What is jpcert ?”
- * Malware analyst community
- * Talk to community of open source software

National Cyber Security Strategies of Japan ?

- * National Information Security Center : NISC
 - * Japanese Government initiative of information security
 - * Under the Cabinet Secretariat
- * Materials are available in English
 - * <http://www.nisc.go.jp/eng/index.html>
 - * National Policy
 - * Guideline for systems
 - * Security Standard
- * Closely work with JPCERT/CC



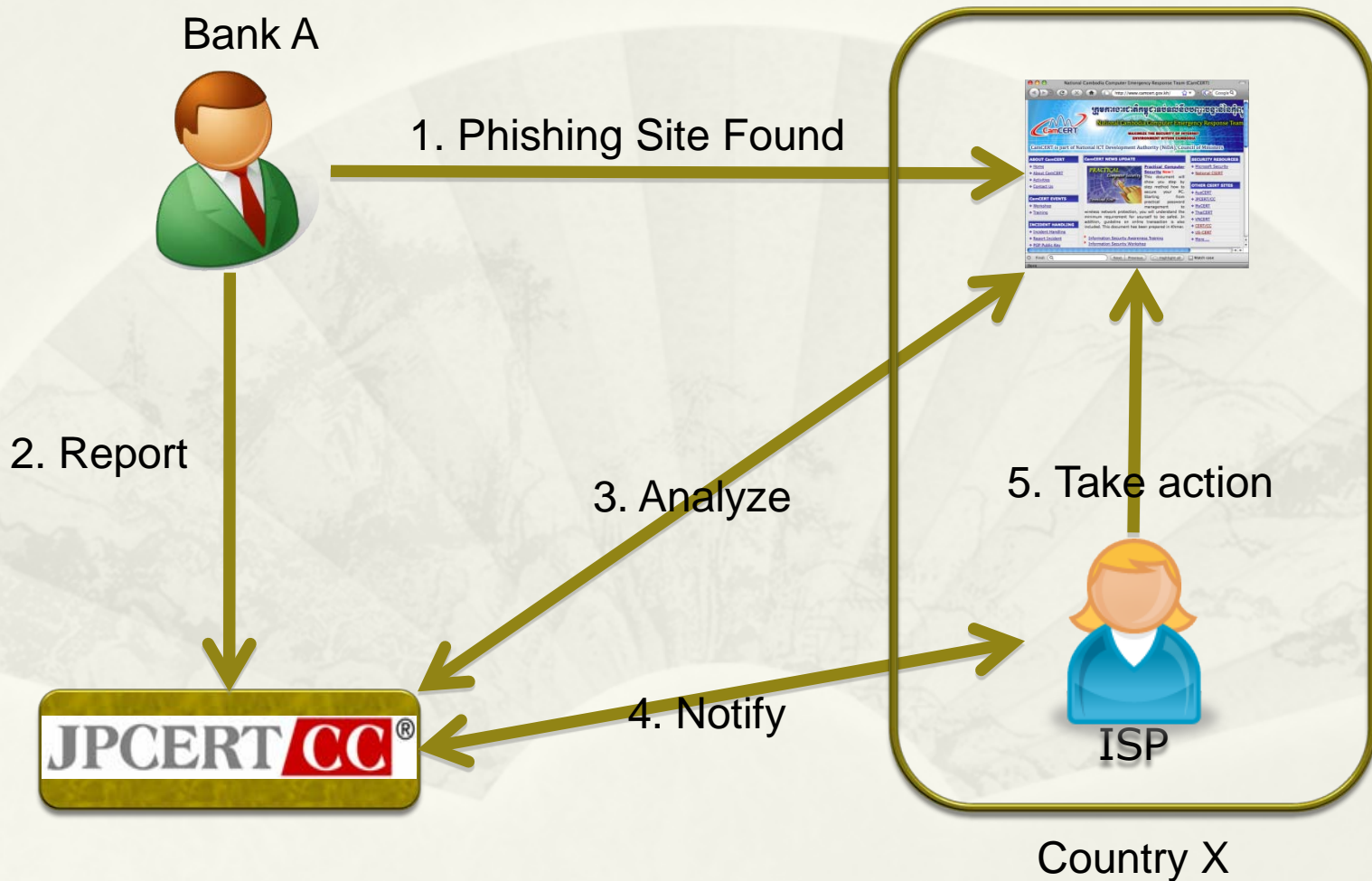
Case examples from JPCERT/CC activity

1. Phishing
2. Malware
3. SQL Injection
4. VoIP Spam

1. Phishing

- * Japanese bank A found their phishing site
- * Report it to JPCERT/CC
- * JPCERT/CC Coordinate to ISP in Country X
- * ISP in Country X notify about the phishing site to the administrator of phishing site
- * Phishing site was launched because of hacking, administrator took immediate action and phishing site was closed

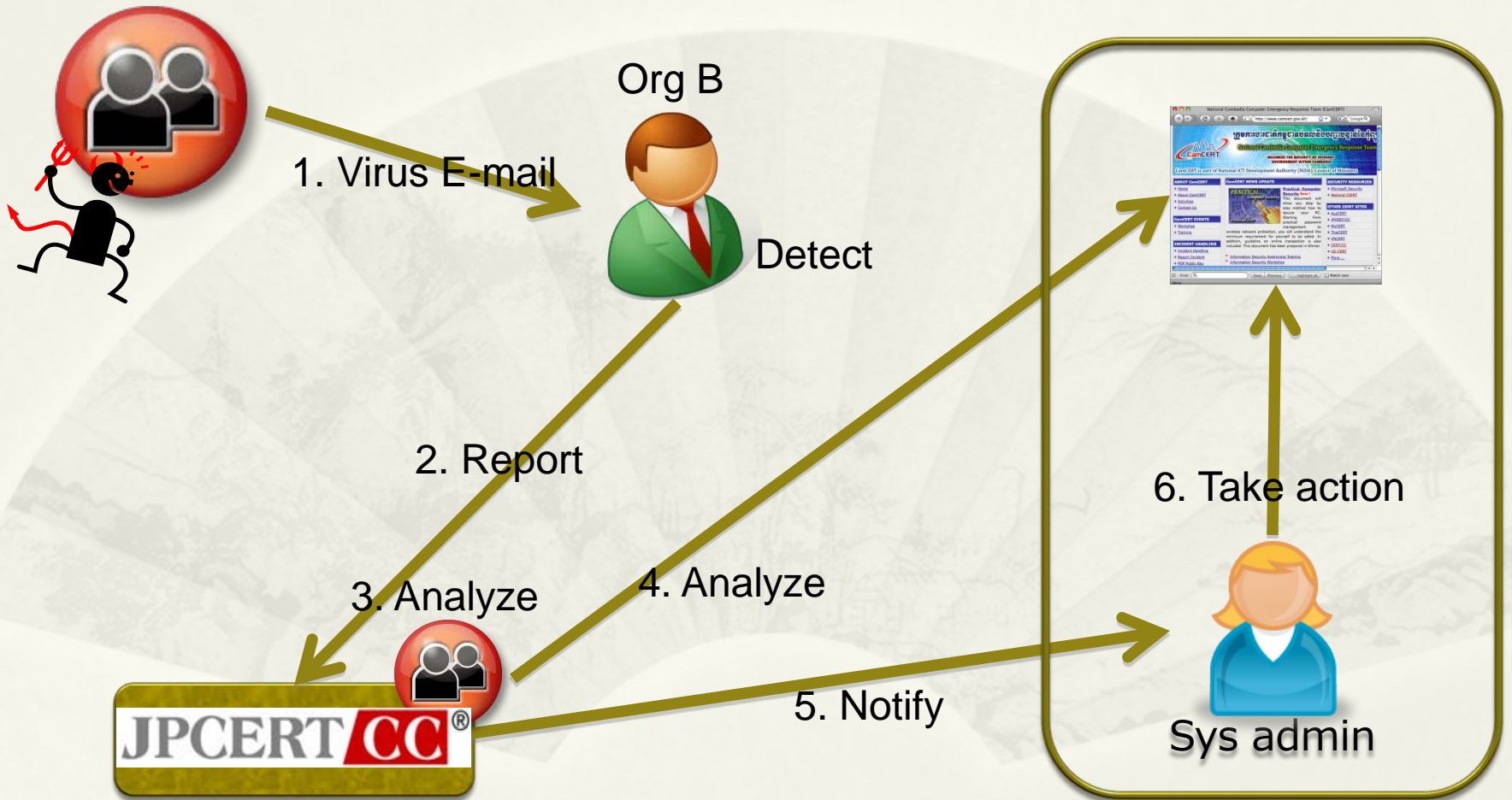
Phishing



2. Malware

- * Japanese government related organization B receive an e-mail attached with unknown virus
 - * The virus could not detect by anti virus software
- * JPCERT/CC analyze the virus and found that infected computer will access to some website to update virus
- * JPCERT/CC send analysis result to reporter, to take appropriate action
- * JPCERT/CC coordinate to virus update website administrator for stopping website
- * Website administrator took immediate action, and stop the website

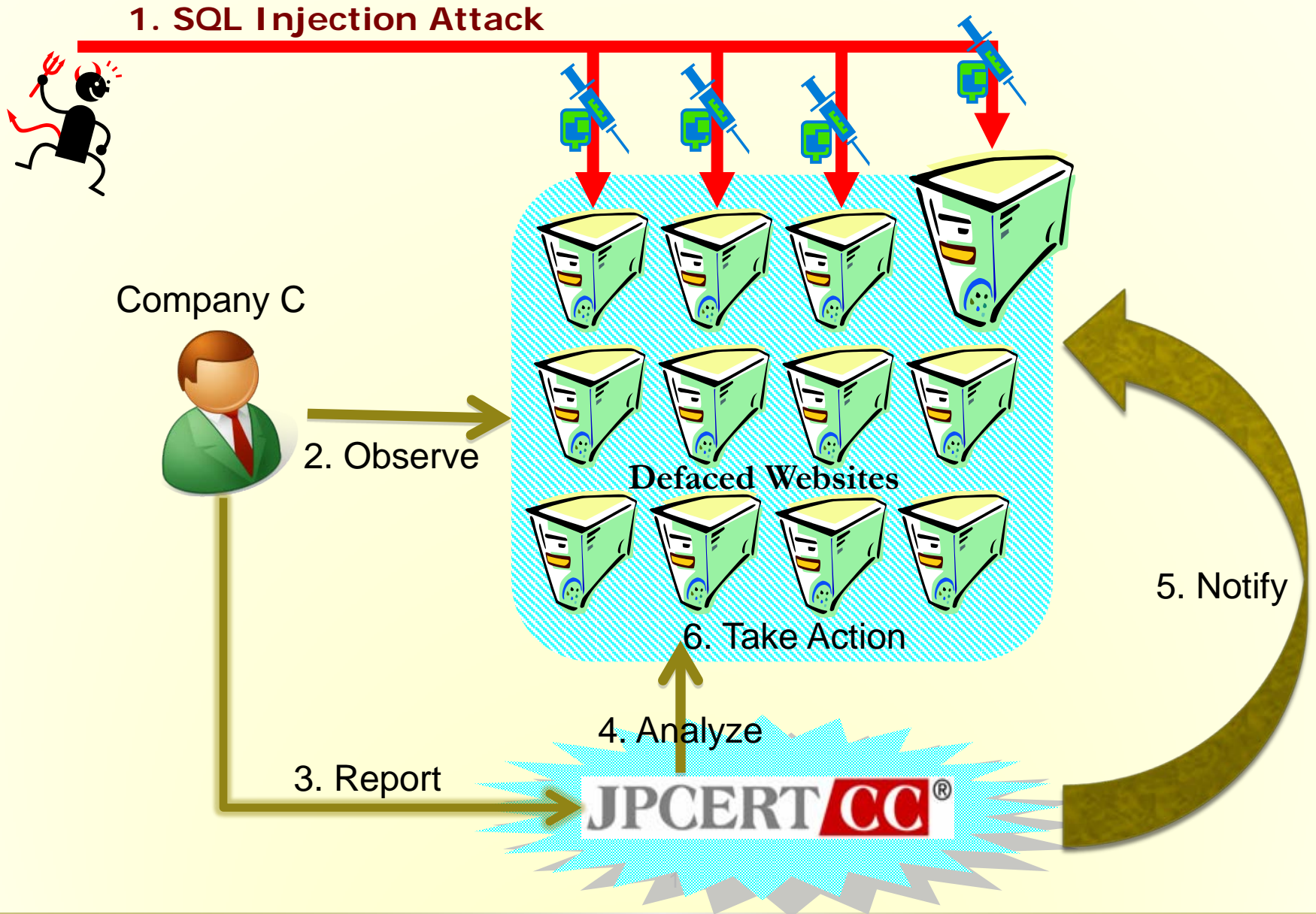
Malware



3. SQL Injection

- * A Japanese company C report to JPCERT/CC about many SQL injection attacks
- * JPCERT/CC analyze that attack and found many websites were defaced by that SQL Injection attack
- * JPCERT/CC notify to each website administrator about web defacement
- * Each website administrator took appropriate actions

SQL Injection attack case

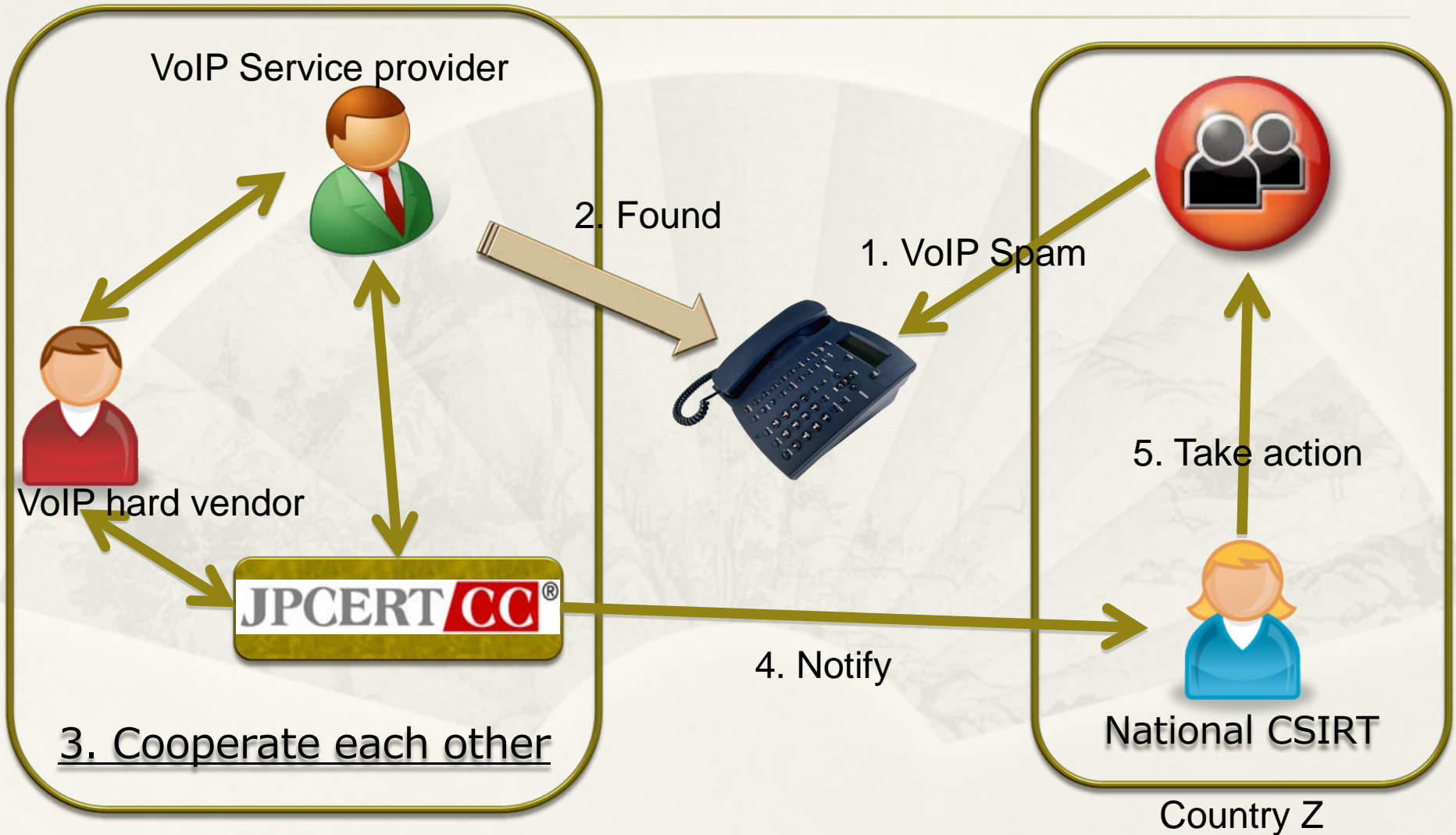


4. VoIP Spam

- * Strange VoIP accesses were happened
- * JPCERT/CC, VoIP hardware vendors and some Japanese IT service company were cooperate to handle the strange VoIP access
- * JPCERT/CC coordinate the issue to National CSIRT in Country Z to stop the strange access



VoIP Spam



Lessons learned

Cooperation

Analysis

Report

Point of
Contact

Detection

Conclusion

- * Inter organizational **cooperation** is important, because multiple stakeholders will be involved to handle computer security incident
- * Technical **analysis** capability is needed to know what is happening
- * **Reporting** to single point of contact is easier to handle multi organizational computer security incident
- * Inform RIGHT person (**PoC**) who can handle the situation !
- * Prepare to **detect** computer security incident to reduce the damage within your organization.

Role of National CSIRT

