ISOG-J's guide for SOC/CSIRT members on security information sharing

Yasunari Momoi momo@iij.ad.jp

Internet Initiative Japan Inc. / ISOG-J

Agenda

- about me
- what is ISOG-J?
- past ISOG-J’s activities
- “Six Ws on cybersecurity information sharing for enhancing SOC/CSIRT”

About me

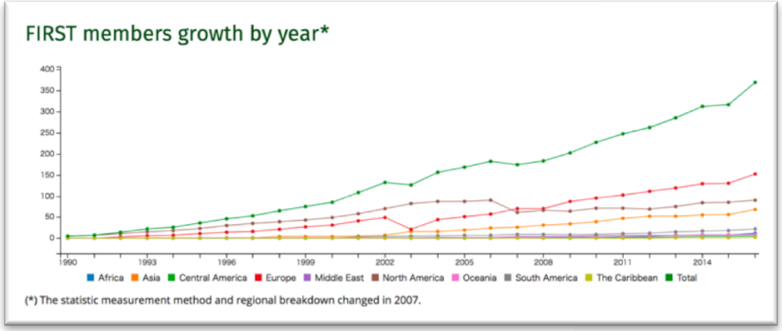
- momo: Yasunari Momoi
  - Internet Initiative Japan Inc., IIJ-SECT member
  - Office of Emergency Response and Clearinghouse for Security Information, Advanced Security Division
  - Facebook ymomoi Twitter @sbg
- Security, SOC/CSIRT, Software Developer, Network Engineer, Server Engineer
  - Develop some managed security services, operators dashboard, software tools for analyzing security logs, etc…
- Acting as a CSIRT member
  - FIRST, FIRST Japan Teams, NCA (Nippon CSIRT Association), ISOG-J
  - ICT-ISAC
- Special Interest
  - local foods, Heavy Metal music, cats

What is ISOG-J

- the Information Security Operation providers Group Japan
  - established 2008
  - ISOG-J is a professional community for security operation providers
  - a forum to share information about security operation and resolve common issues.
- ISOG-J's pronunciation is "ee-sog-jay"
  - the meaning is "Got to hurry, Japan!"
- http://isog-j.org/e/

ISOG-J member growth

FIRST members growth by year*



(*) The statistic measurement method and regional breakdown changed in 2007.

42 membership organizations
(2018-02)

2008
established
IIJ, IIJ Technology, NTT Data, NEC, NTT, Hitachi Systems, Fujitsu, MBSD, NRI Secure, LAC

2009
BBSec, NECXS, NTTCom, DIT, Fujitsu SSL, IBM Japan

2010
Kaspersky labs Japan, Softbank Technology

2011
NTT Data Security, UBsecure

2012
MIND, UNIS, UNIADEX

2013
Tricoder, SECOM Trust Systems, SCSK

2014
NTT Software, Securesoft

2015
Softbank mobile, NES

2016
PERSOL Technology Staff, Cybozu

2017
NISSHO ELECTRONICS, Recruit Technologies, KDL

2018
GSX, NRI Secure, JRI, Marubeni
OKI, Net One Systems, PFU, PwC,
KOANKEISO, SecureWorks Japan

Activities of ISOG-J Working Groups (1)

- Security Operation Guideline WG
  - collaborate with OWASP Japan
  - creates Pentesters' skill map and syllabus
- Security Operation Technology WG
  - to promote friendship among the members
  - hold an internal seminar of technical topics, then drink together
  - we called these timetable "sub part" and "main part"
    - It's ok to join only "main part" :D

KILKENNY
KILKENNY

Activities of ISOG-J Working Groups (2)

- Security Operation-related Laws Research WG
  - research the laws and systems related to the SOC business
  - Handy Compendium of Information Security Laws in Japan
- Security Operation Recognition and Propagation WG
  - increase awareness of security operations to customers
  - event and publicity planning
- Security Operations Chaos WG
  - discussing any issues on security operation chaos
  - taking an acronym: SOC

ISOG-J
WG6
第10回会合(合宿)

Past ISOG-J publications (1)

- 2008 Service map of Managed Security Services (listed up and categorized)
- 2009 Guidelines to choose Managed Security Service
  - How to choose Managed Security Service fit your organization
- 2011 Survey report on IPv6 ready status of security equipment
- 2011 Handy Compendium of Information Security Laws in Japan
  - revised at 2012 and 2015

Past ISOG-J publications (2)

- 2013 How to defend your business – a guide for security assessment service (book)
- 2014 Skillmap and syllabus of web pentesters (with OWASP Japan Pentester Skillmap Project JP)
- 2015 Self-check sheet: prepare for information security incident response (for beginners)
  - just a few pages summary
- 2016 Skillmap and syllabus of platform pentesters (with OWASP Japan Pentester Skillmap Project JP)
- 2017 Guideline for web application penetration testing (with OWASP Japan Pentester Skillmap Project JP)

Past ISOG-J publications (3)

- 2016 Overview of SOC members and their skills
- 2016 Textbook to build SOC/CSIRT ver.1.0
- 2017 Textbook to build SOC/CSIRT ver.2.0
- 2017 5W1H on cybersecurity information sharing for enhancing SOC/CSIRT ver.1.0
- 2018 Security topics world map in 2017

MITRE
Ten Strategies of a World-Class
Cybersecurity Operations Center
Carson Zimmerman

But these publications are...

- in Japanese
- because of many SOC/CSIRT member in Japan
  - can read English but so slow (and sometimes wrong)
  - prefer read in Japanese
- we planned some documents English edition
  - but we could not for various reasons
  - but now...

Six Ws on cybersecurity information sharing for enhancing SOC/CSIRT

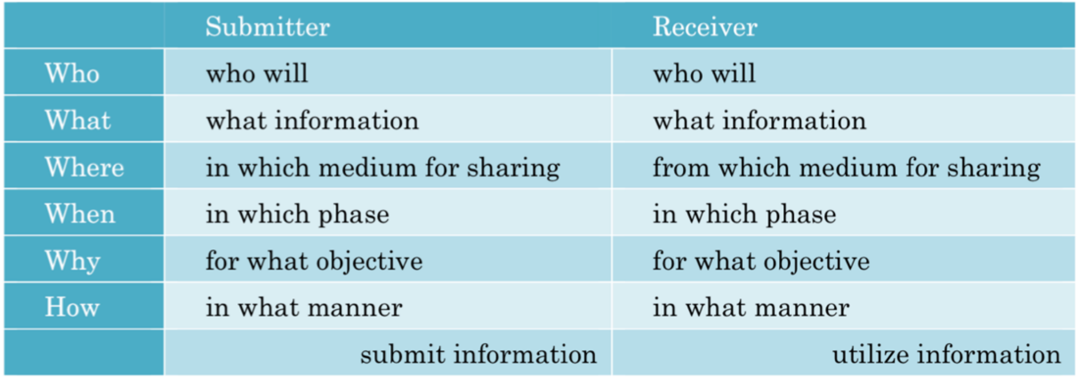
- Released!
  - We did our best
    - however, I think there are still unclear sentences...
  - The referral destination documents are only in Japanese
    - we will make summary of necessary parts in English
- Please feedback us!

download here https://goo.gl/qoCHtn

or from http://isog-j.org/e/

the point of this Six Ws document

- the basics of security information sharing for members of SOC/CSIRT
- Why mismatches when sharing information?
  - rethinking back to basics



	Submitter	Receiver
Who	who will	who will
What	what information	what information
Where	in which medium for sharing	from which medium for sharing
When	in which phase	in which phase
Why	for what objective	for what objective
How	in what manner	in what manner
	submit information	utilize information

Table 1：Six Ws in cybersecurity information sharing

Phasing incident handling triggered by shared information

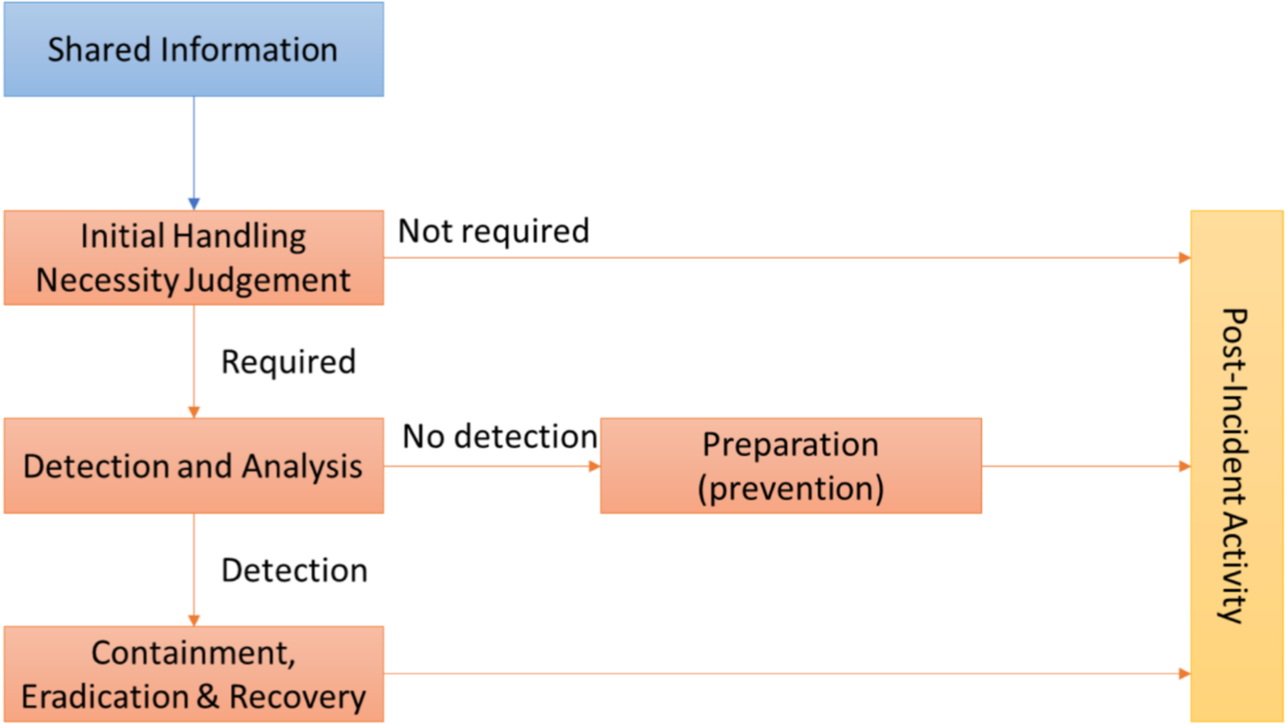
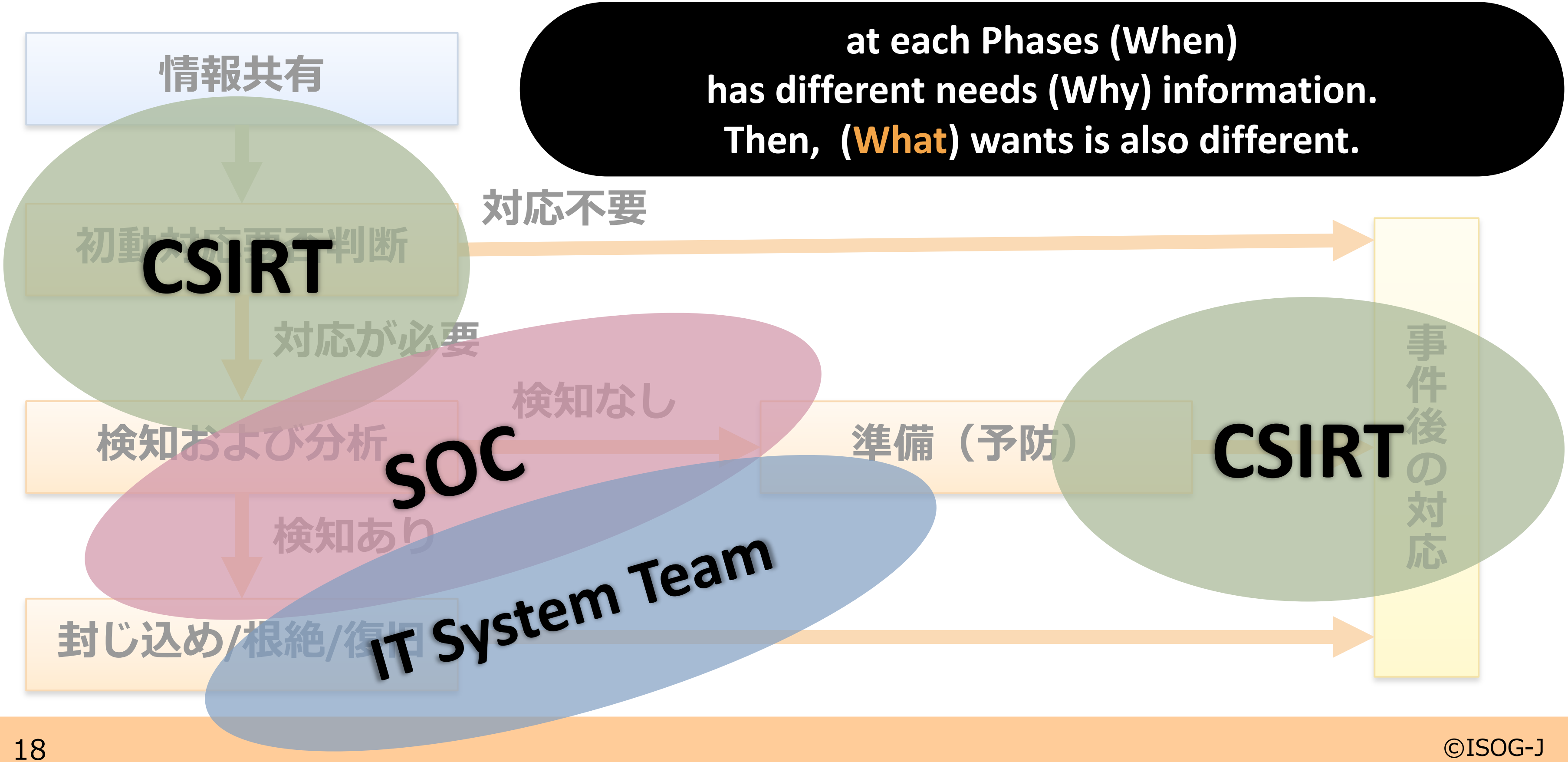
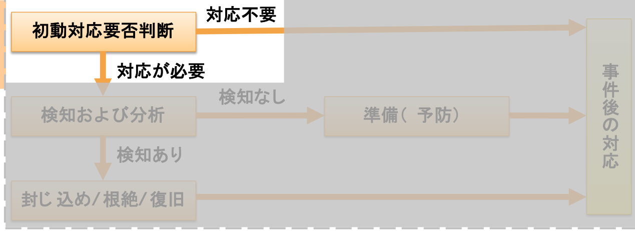


Figure 3：Incident handling triggered by shared information

Difference between each phases

at each Phases (When)
has different needs (Why) information.
Then, (What) wants is also different.





When

Initial handling necessity

Why

This information affects our organization?

Vulnerability information (What)

- vulnerability identifier
  - CVE or patch number
- affected systems
  - system type
  - version
  - conditions (e.g. configuration)
- can security products prevent it?

Attacking related information (What)

- name that specifies the attack
  - campaign
  - malware/incident name
- target of attack
- attack vector
  - from where the attack comes

reports afterward

- how to drive the place for information sharing?
  - works better when a certain number of sender is there
- experiences will be helpful
  - when facing a similar attack
  - for similar type, similar business organization
    - ISACs
- feedback is important
  - fix if wrong
  - a hint to improve handling in the future

Information sharing triangle

- take two
  - Fast, Accurate, Comprehensive

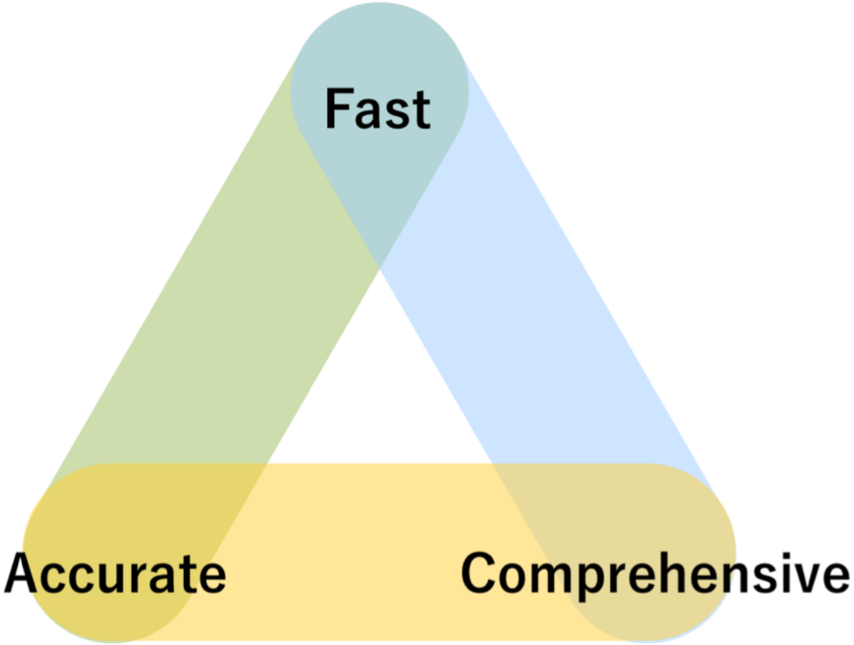


Figure 4 : Triangle in information sharing

27th Annual FIRST Conference (2015), Lightning Talk: "Four Easy Pieces", Tom Millar (US-CERT, NIST)

Thanks!

- ISOG-J discussed information sharing on cybersecurity from the fundamentals and summarized it.
- Issues
  - automation
  - visualize reliability of the information
  - How to encourage good feedback cycle
- Please feedback us!

download here https://goo.gl/qoCHtn
or from http://isog-j.org/e/