How CSIRT can help us
- CSIRT Activities in Japan -

July 13, 2016

Yoshiki yo!! Sugiura

NTT Intellilink Corporation

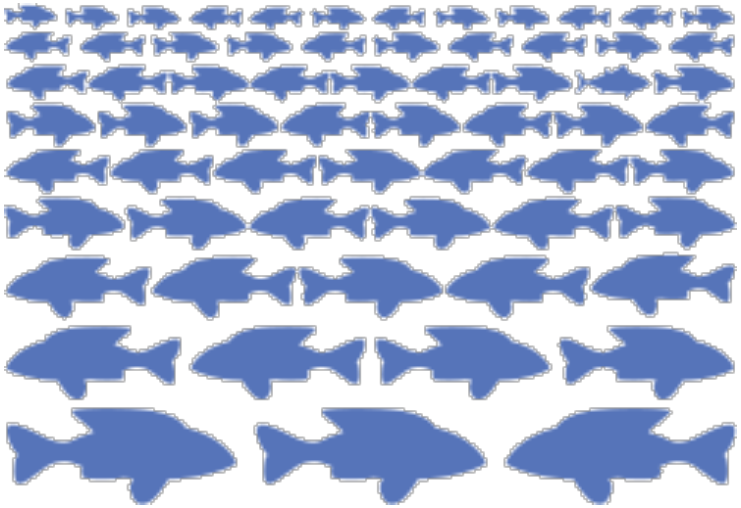
Nippon CSIRT Association

Introduction

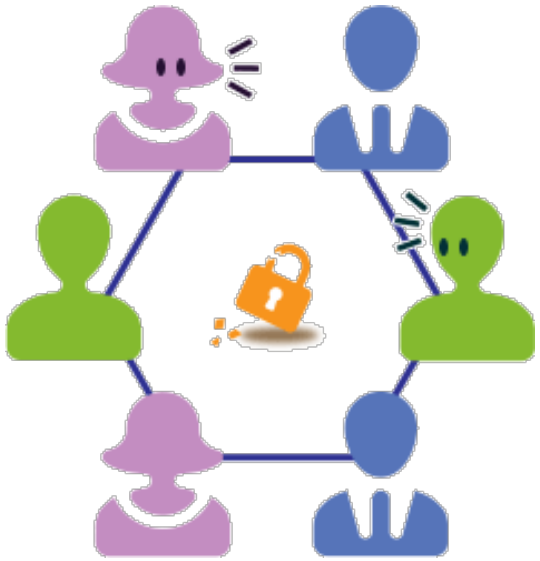
Yoshiki Sugiura

- CSIRT Evangelist
  - JPCERT/CC from 1998 to 2002
  - NTT-CERT and Intelli-CSIRT
  - Steering committee of Nippon CSIRT Association
- Guest researcher of Meiji Univ.
  - Team building
  - Theory of management and Social psychology

What We Can Learn From



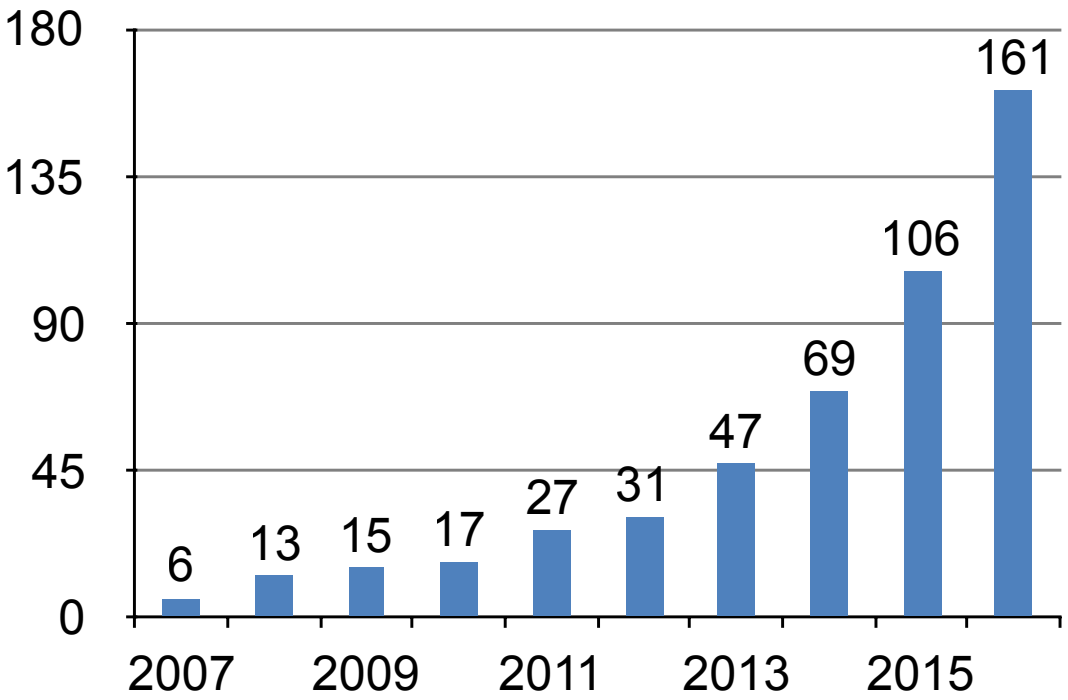
Easy to miss…

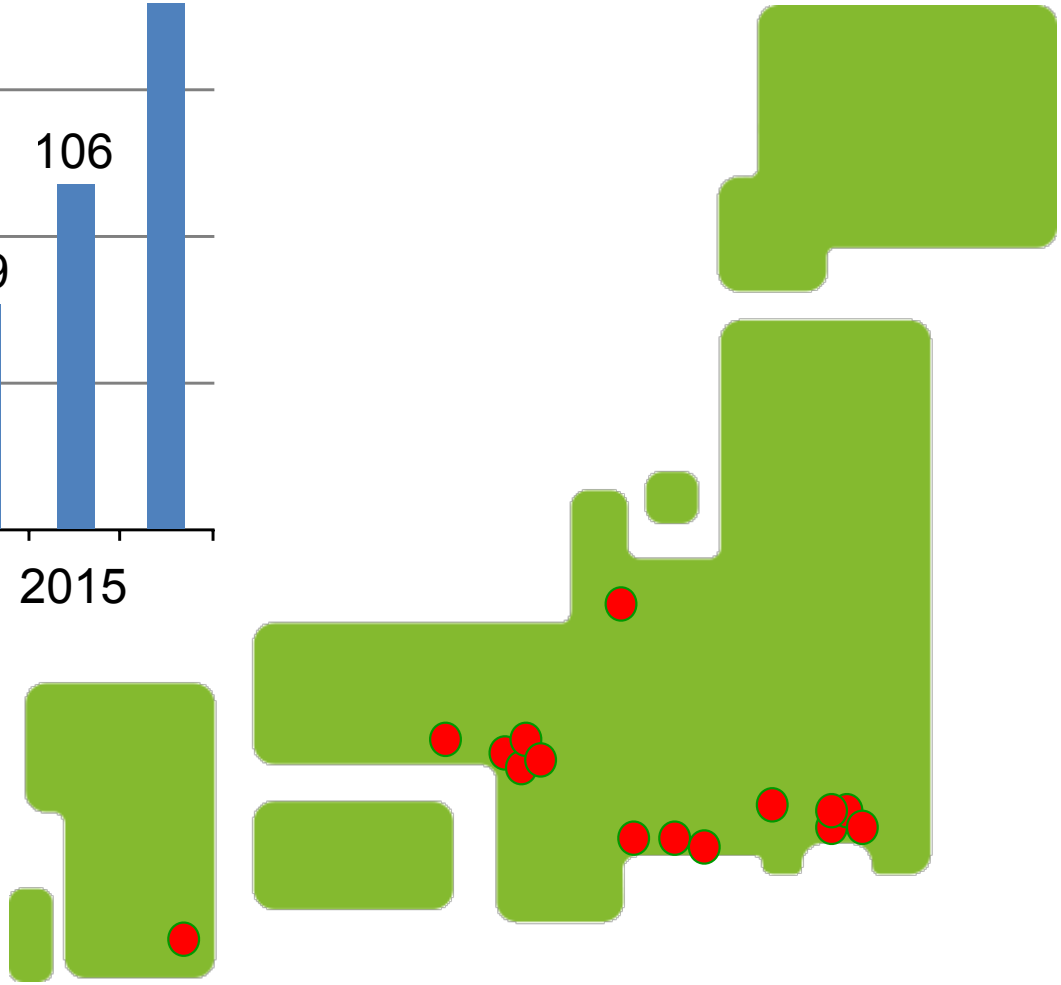


Can find it if we are in a team

Easy to see if we knew it

Number Of Member Teams





Growth Factors - Policy

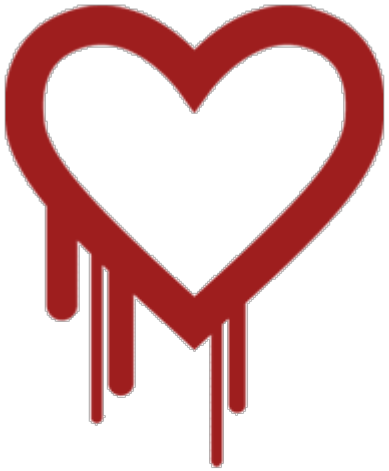
NISC “Information Security 2012”

「　このため、国等においては、標的型攻撃に係る官民連携の枠組みを構築し、情報共有・分析検討を進めるとともに、それぞれがCSIRT等の機能を有する体制を構築し、関係機関を跨ぐ情報セキュリティ緊急対応要員の整備・充実が求められる。また、研究開発等を進め、標的型攻撃に対する効果的な対応に向けた取組を推進することが重要である。」

"for public private sector partnerships concerning targeted attacks and continuing with the sharing, analysis and examination of information, each entity is required to establish a system having CSIRT and other such functions, and ensure the staffing and enhancement of necessary personnel for emergency information security measures to cover the related agencies. It is also important to proceed with R&D and other activities and promote initiatives for effective measures to address targeted attacks."

Current Issues

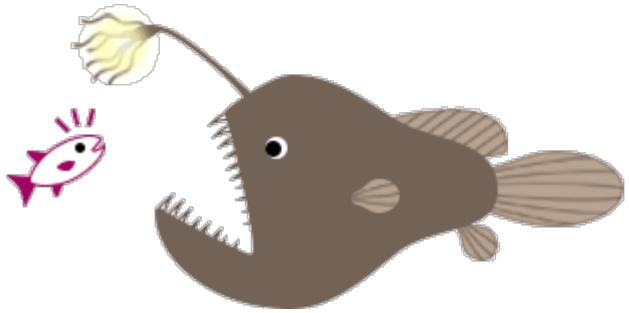
- Huge Vulnerabilities



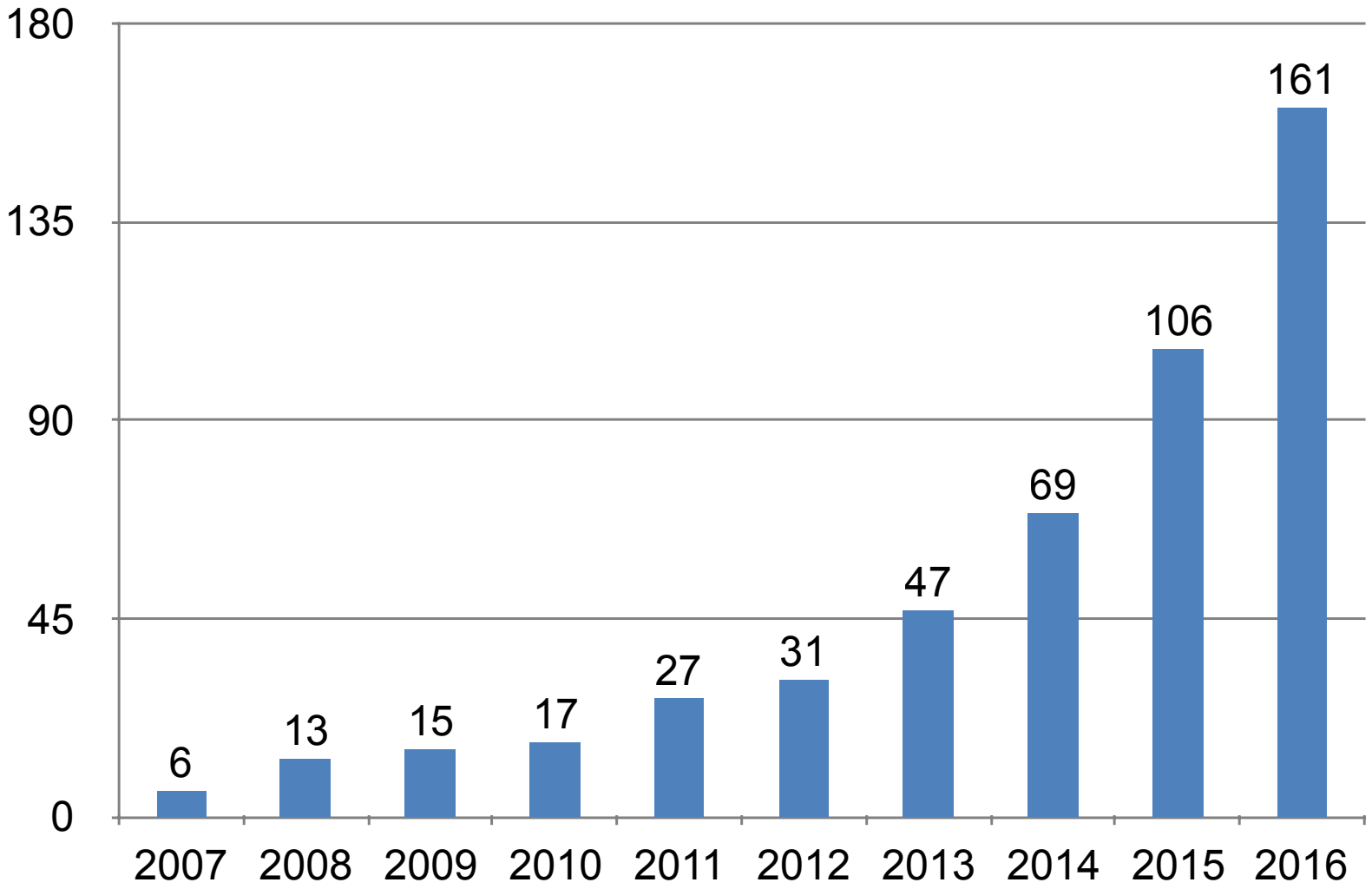
Source: http://heartbleed.com/

- Data Breach

- Bank Phishing



Number Of Member Teams



Field Study About CSIRTs

CSIRTが“期待したレベルを満たしている”と回答した割合は米国45.3%、欧州48.8%に対し日本は14%となり、欧米の3分の1と大きく差が開く結果となった。

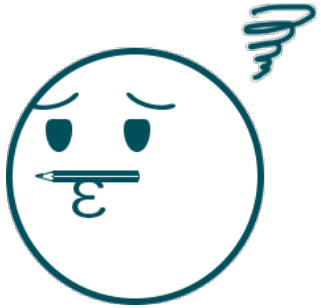
The percentages who answered “CSIRT meets the expected level” are in the United States 45.3%, Europe 48.8% and Japan 14%.

There is a big gap of CSIRT’s capacity between Japan and the Western.

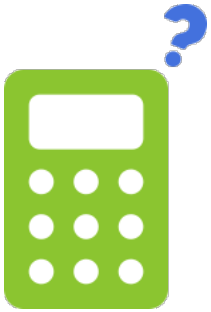
Source: IPA report - https://www.ipa.go.jp/security/fy27/reports/ciso-csirt/

Why?

- Just order from managements
  - No motivation
  - They don’t know what they should do



- Panacea
  - No real operations



- Managements don’t think about Security
  - Already enough rules and firewalls and IDSs and so never happens security incident
  - Don’t care about the costs of security and CSIRT

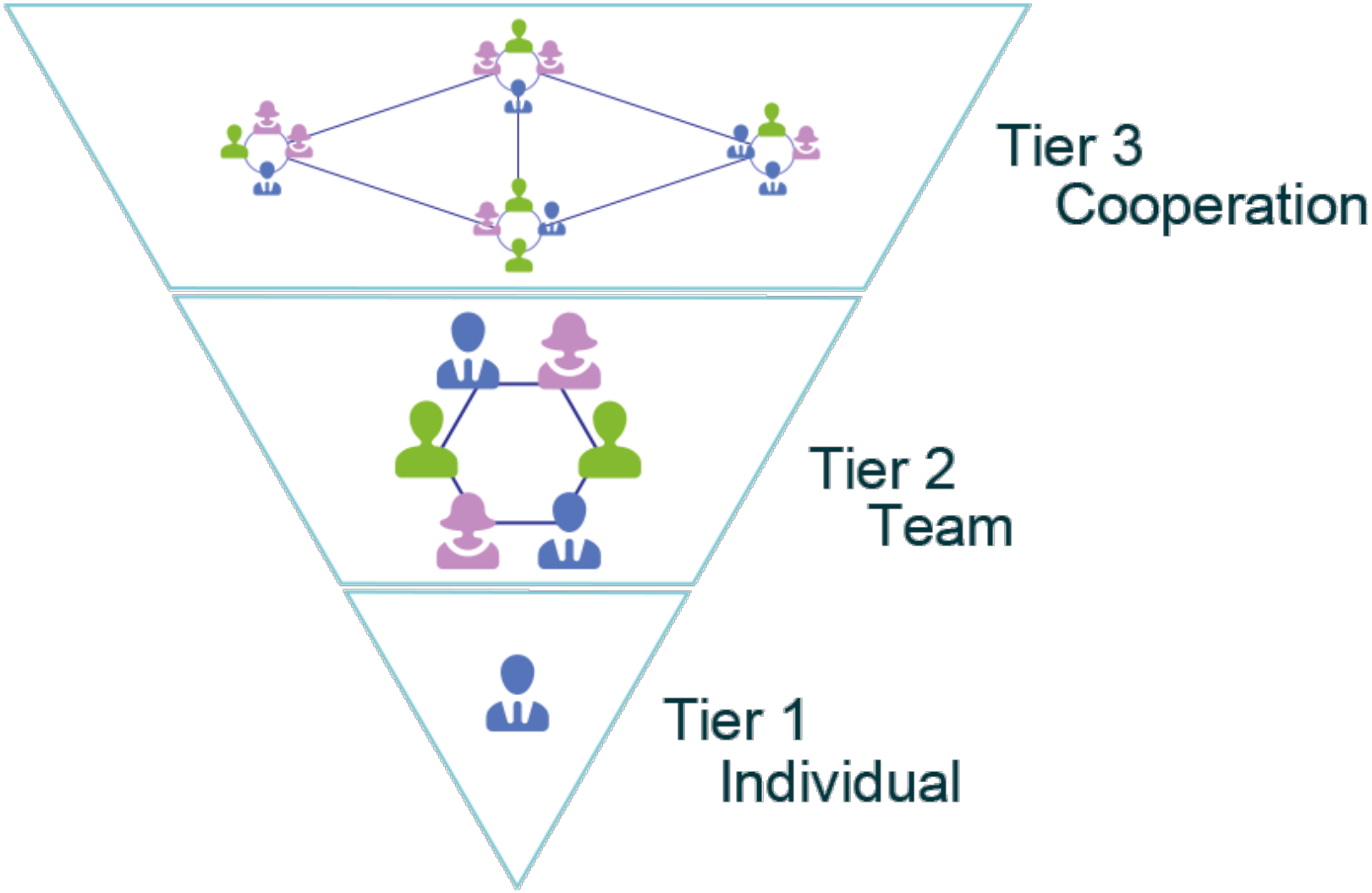
Why?

No person

White Hackers

Supermen

CSIRT 3Tier



TRANSITS

- Training program for CSIRT
  - TERENA (currently GÉANT)
  - http://www.geant.org/
- 4 Modules
  - Organization
  - Operation
  - Technical
  - Law
- Translated in Japanese

One Scene Of Our TRANSITS

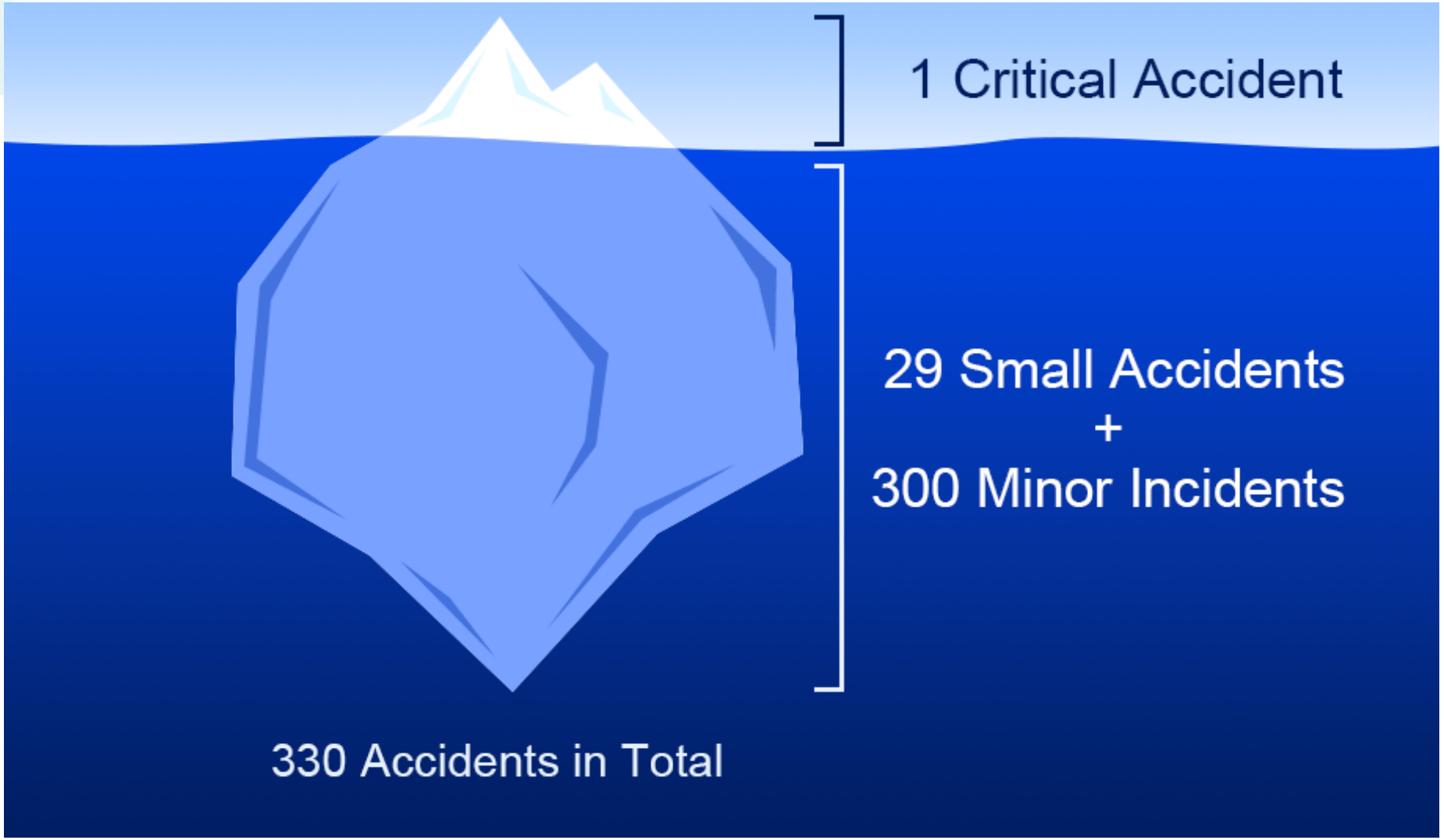
- 17 - 19 February 2016
- At the training institute of Fuji Xerox Co., Ltd in Kobe
- 41 Attendees

Discussion, discussion, discussion!

What's The Purpose Of CSIRT

Respond to emergency

Heinrich's Law



Maturity

Unclear the activities or no activity

- Documented and reviewed
- Clear the activities
- Involvements of Managements

- How much recognise the CSIRT activities in their organisation
- How much level of the CSIRT

Source: https://www.terena.org/activities/tf-csirt/publications/SIM3-v15.pdf

Introduction Of SIM3

4 quadrants

- O - Organization
- H - Human
- T - Tools
- P - Process

Introduction Of SIM3

- Level Set
  - 0 = not available / undefined / unaware
  - 1 = implicit (known/considered but not written down, “between the ears”)
  - 2 = explicit, internal (written down but not formalised in any way)
  - 3 = explicit, formalised on authority of CSIRT head (rubberstamped or published)
  - 4 = explicit, audited on authority of governance levels above the CSIRT head(subject to control process/audit/enforcement)
- for next level
  - 0 -> 1 : addition of consideration - “listen, we are aware of this”
  - 1 -> 2 : addition of written description - “read, this is the way we do it”
  - 2 -> 3 : addition of accountability - “look, this is what we are bound to do”
  - 3 -> 4 : addition of control mechanism – “and this is how we make sure that it happens”

Source: https://www.terena.org/activities/tf-csirt/publications/SIM3-v15.pdf

Introduction Of SIM3

O - “Organisation” Parameters

O-1 : MANDATE

Description: The CSIRT’s assignment as derived from upper management.

O-2 : CONSTITUENCY

Description: Who the CSIRT functions are aimed at – the “clients” of the CSIRT.

O-3 : AUTHORITY

Description: What the CSIRT is allowed to do towards their constituency in order to accomplish their role.

O-4 : RESPONSIBILITY

Description: What the CSIRT is expected to do towards their constituency in order to accomplish their role.

Source: https://www.terena.org/activities/tf-csirt/publications/SIM3-v15.pdf

Introduction Of SIM3

H - “Human” Parameters

H-1 : CODE OF CONDUCT/PRACTICE/ETHICS

Description: A set of rules or guidelines for the CSIRT members on how to behave professionally, potentially also outside work.

Clarification: E.g. the TI CCoP3. Behaviour outside work is relevant, because it can be expected of CSIRT members that they behave responsibly in private as well where computers and security are concerned.

H-2 : PERSONAL RESILIENCE

Description: How CSIRT staffing is ensured during illness, holidays, people leaving, etc. Minimum requirement: three (part-time or full-time) CSIRT members.

H-3 : SKILLSET DESCRIPTION

Description: Describes the skills needed on the CSIRT job(s).

H-4 : INTERNAL TRAINING

Description: Internal training (of any kind) available to train new members and to improve the skills of existing ones.

H-5 : EXTERNAL TECHNICAL TRAINING

Description: Program to allow staff to get job-technical training externally – like TRANSITS, ENISA CSIRT Training, or commercial training programs (CERT/CC, SANS, etc.)

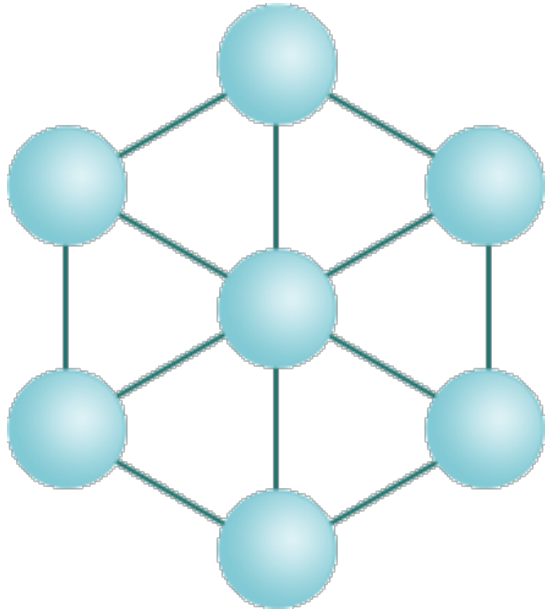
Source: https://www.terena.org/activities/tf-csirt/publications/SIM3-v15.pdf

Why We Need Cooperation?

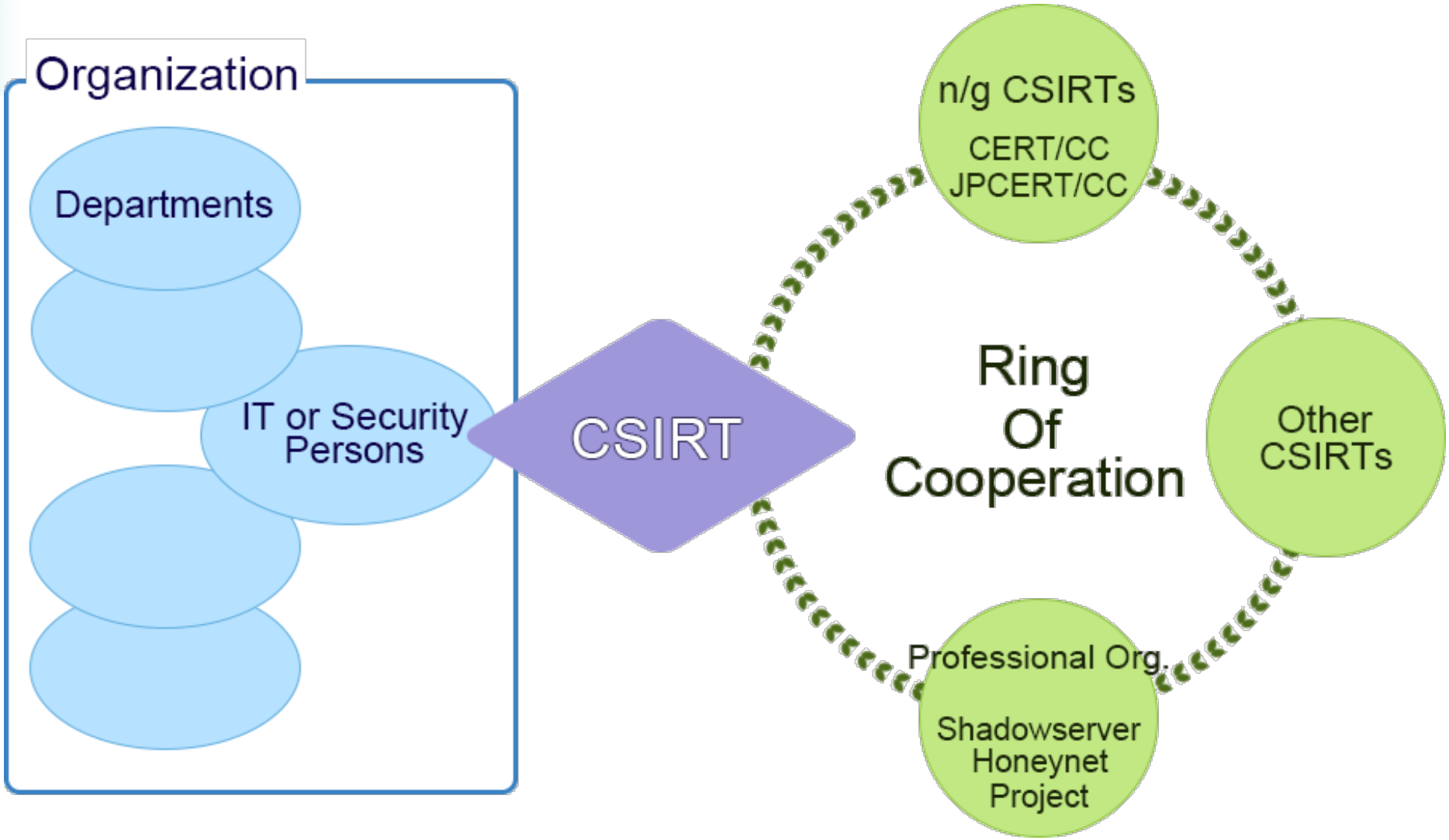
Sharing

Learning

To The Crunch



Ring Of Cooperation



Wrap-up

- Needs CSIRTs in each organisations.
- Current Issues and Challenges on CSIRTs
  - CSIRTs doesn't work
- Why sometimes CSIRT doesn't work effectively
- What we should do with CSIRTs
  - Training and Educations
  - Mature Teams
  - Cooperation

Thank you for your attention!

多謝

CSIRT Distiller

Email:
yoshiki.sugiura@bornfromegg.net

Twitter: csirt_jp(CSIRT)
yocompas(Music)
Facebook:
https://www.facebook.com/yo.compas