CSIRT and Information Security Governance

Joint Workshop on Security 2008, Tokyo

26 March 2008

Tomohiko Yamakawa

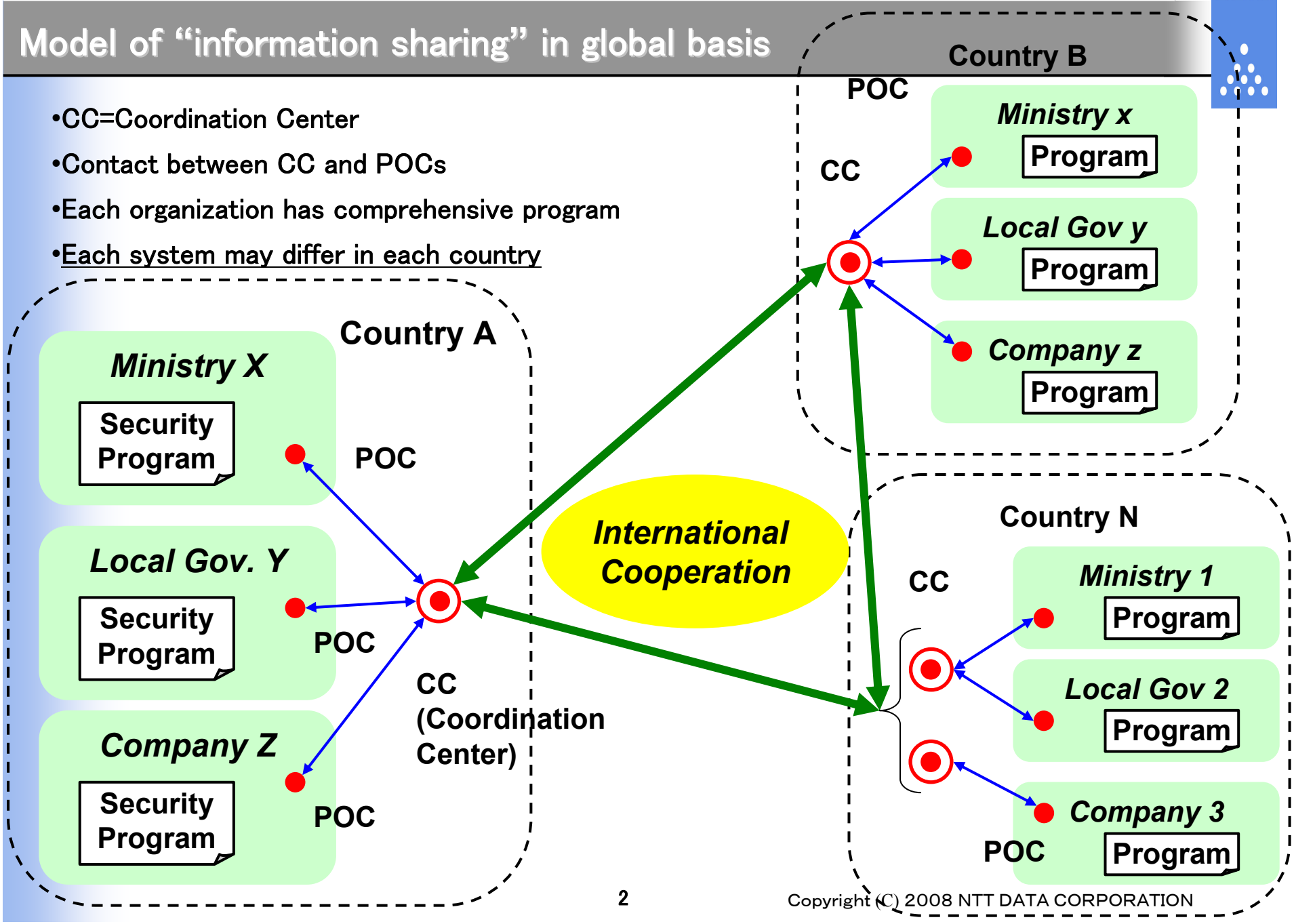
NTTDATA Corp.

CSIRT for the business enterprises

- Issues for business
  - Globalization of the threat e.g. Estonia case
  - Business enterprises with *Global Supply Chain* depend on IT
  - Importance of *IT Risk*
  - Overregulation or not？
    - Information security＝protect information asset (for ourselves)
    - Compliance ＝ required from outside (by stake holders)
    - Critical Infrastructure Protection --- For Whom?
- CSIRT for business enterprises
  - What is the advantage?
  - How to take advantage of the framework of “CSIRT”?
    - In-house or outsource
    - In the context of “international cooperation”

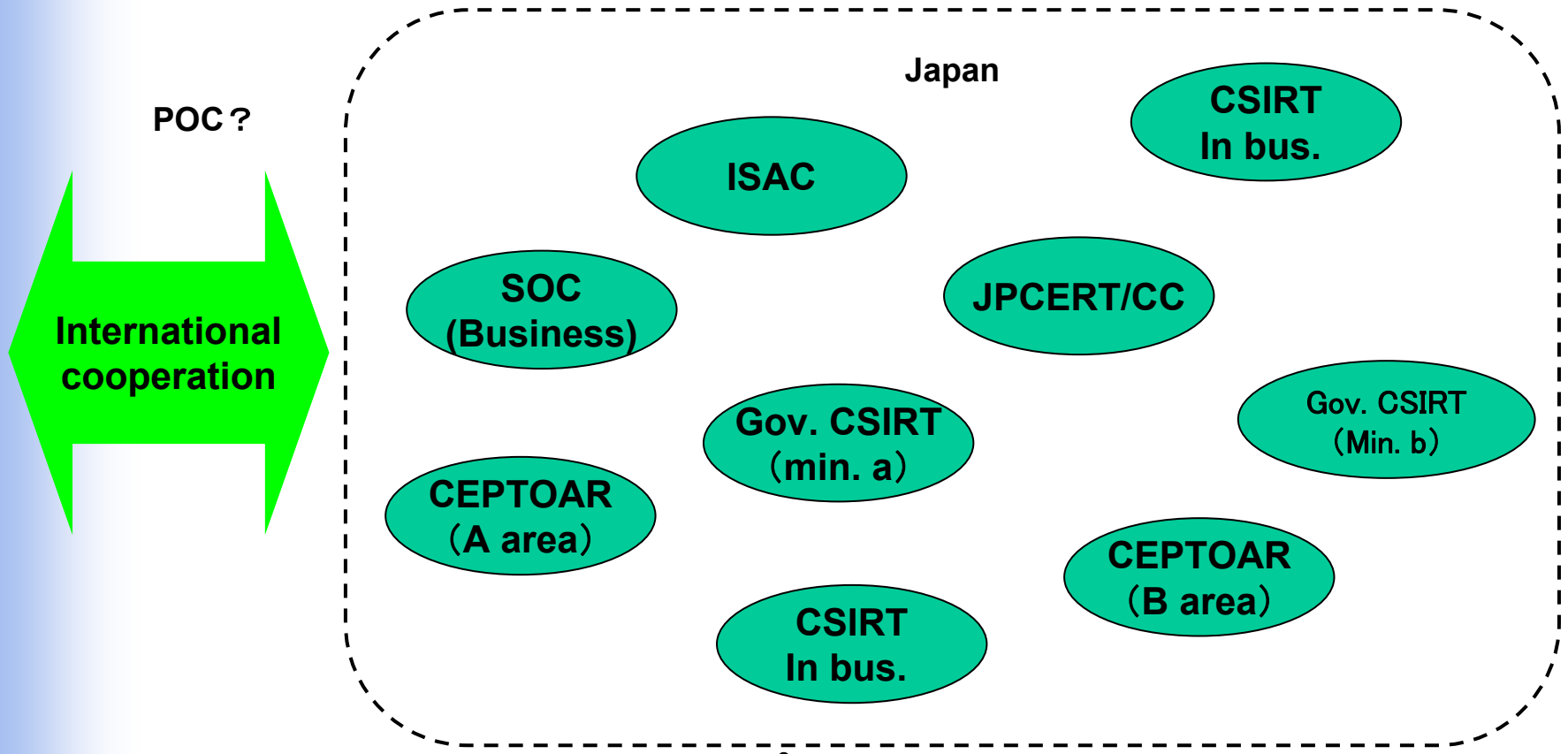
Model of "information sharing" in global basis

- CC=Coordination Center
- Contact between CC and POCs
- Each organization has comprehensive program
- Each system may differ in each country



How to build us “domestic model” in Japan?

- What is the role of Government, CIP, and business enterprises?
  - How to merge with law and regulation in Japan?
  - What is the role of each player, such as CEPTOAR, GSOC, JPCERT/CC, etc.?
  - Who or what division should act as “POC” for each organization?



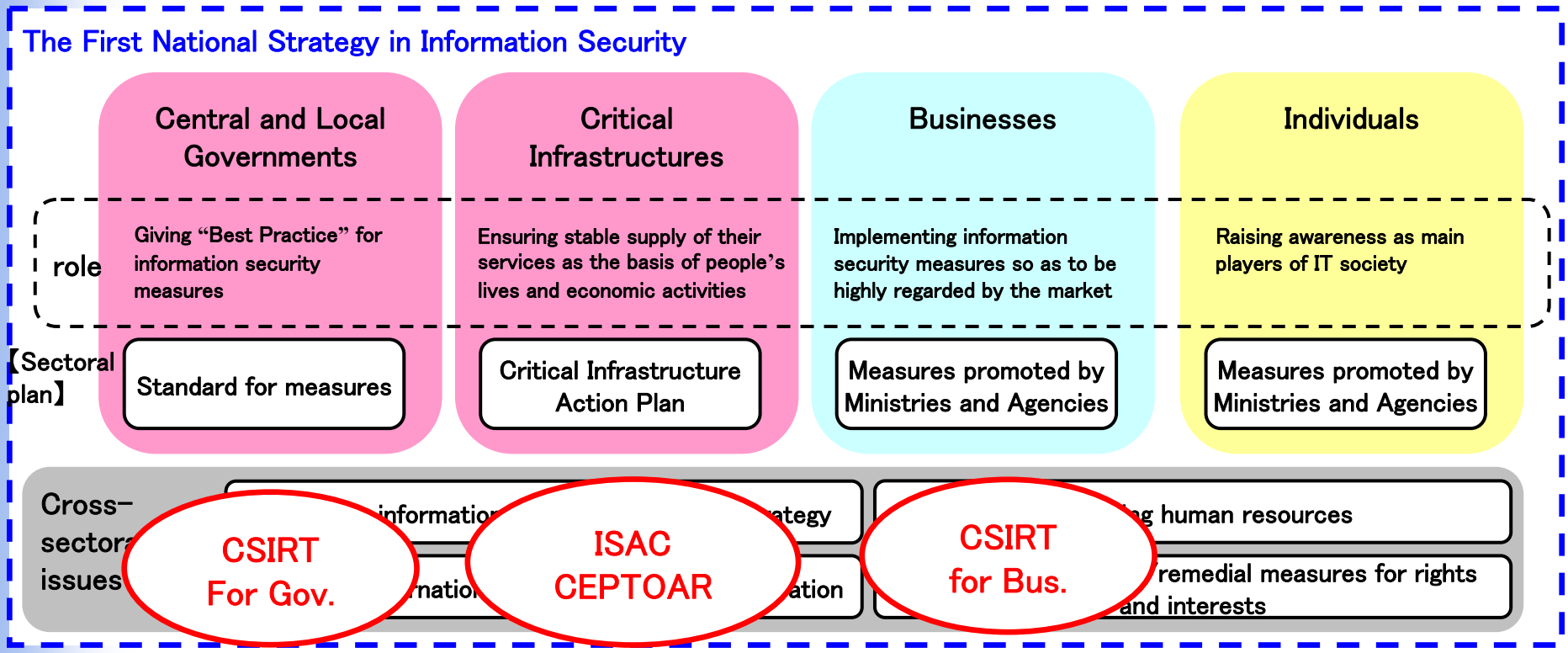
Policy of “Security” as a background of CSIRT

Cybersecurity or Information Security?

Information Security Policy in Japan

- 02 Feb. 2006; The First National Strategy on Information Security
- 15 June 2006; Secure Japan 2006
- 14 June 2007; Secure Japan 2007

＊ ref. http://www.nisc.go.jp/eng/pdf/overview_eng.pdf



"Information Security"＝"Cybersecurity"?

	Japan	USA
Idea	Information Security Governance	Cybersecurity
What?	•Protect *CIA* of information assets –Confidentiality –Integrity –Availability •Incorporate Information Security into a part of corporate governance	•Prevent cyber attacks against America's critical infrastructure •Reduce national vulnerability to cyber attacks •Minimize damage and recovery time from cyber attacks that do occur*
National security	No	Yes
Volunteer basis or not	Voluntary measures by businesses	National Strategy to Secure Cyberspace (partly compulsory?)
Incident response and information sharing	Government: standards for measures CIP: CEPTOAR Business: –Nippon CSIRT Association –Confusing obligation of report and incident response	•Government: FISMA •CIP: ISAC •Business: –IT-ISAC and several activities on volunteer basis in IT providers

*= strategic object of *National Strategy to Secure Cyberspace*

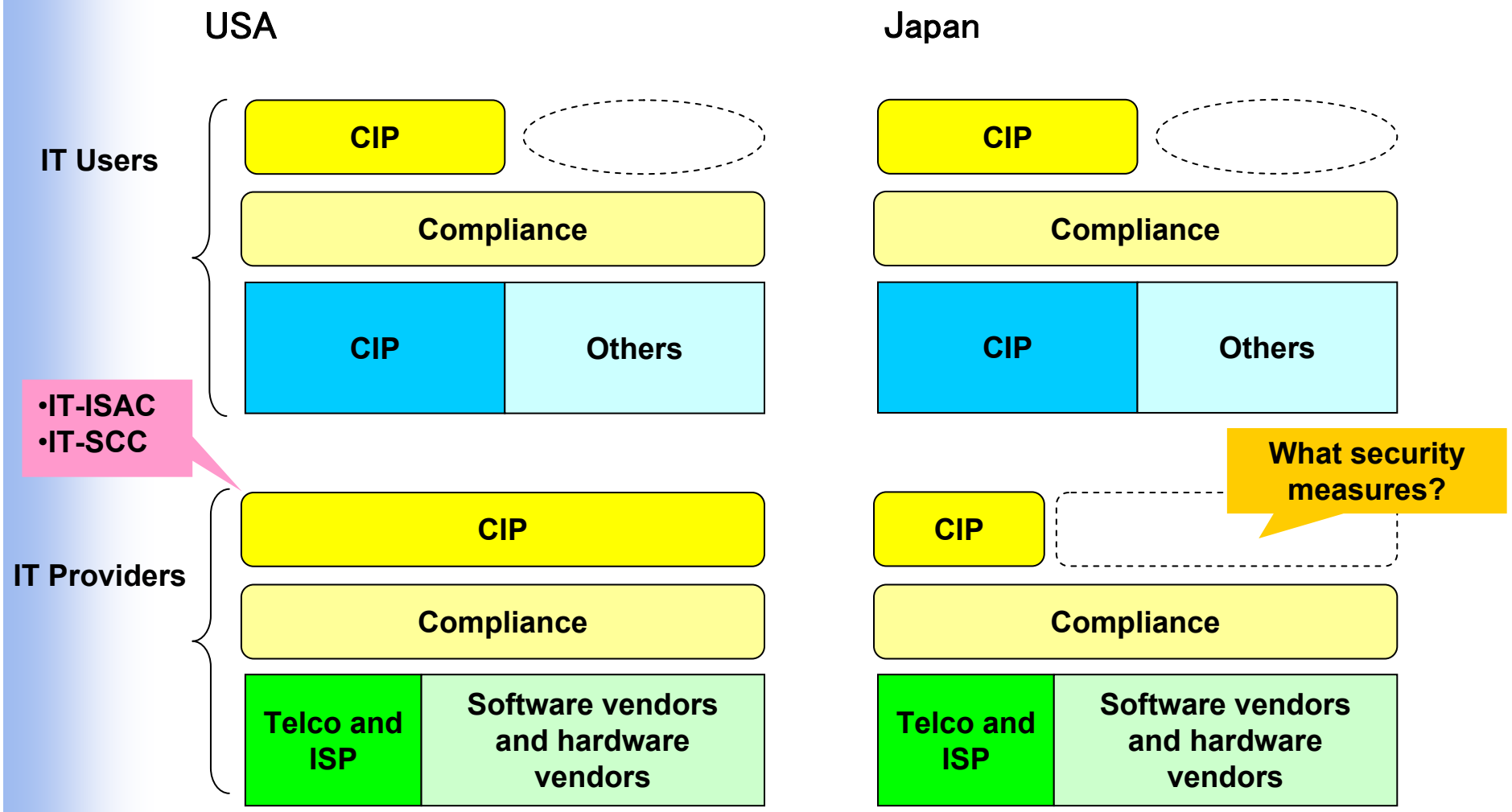
CSIRT regulations for Governments (Japan and USA)

	USA	Japan
Ministry	DHS/NCSD	NISC
Law	•FISMA	–
Standards	•NIST SP 800-61 •CERT/CC "Incident Management Capability Metrics"	•Standards for Information Security Measures for the Central Government Computer Systems (Dec. 2005)
Outline	•Federal agency responsibilities… –Each agency shall develop, document, and implement an agency wide information security program (§ 3544 (b)) –(7) procedures for detecting, reporting, and responding to security incidents •Federal Information Security incident Center (§ 3543 (a) (7)、 § 3546)	•Standards for… –Advance Preparation for Possible Malfunction –Reporting and Taking Emergency Measures on Malfunctions –Cause investigation and to Prevent the Recurrence of malfunction •Domestic system for reporting and incident response

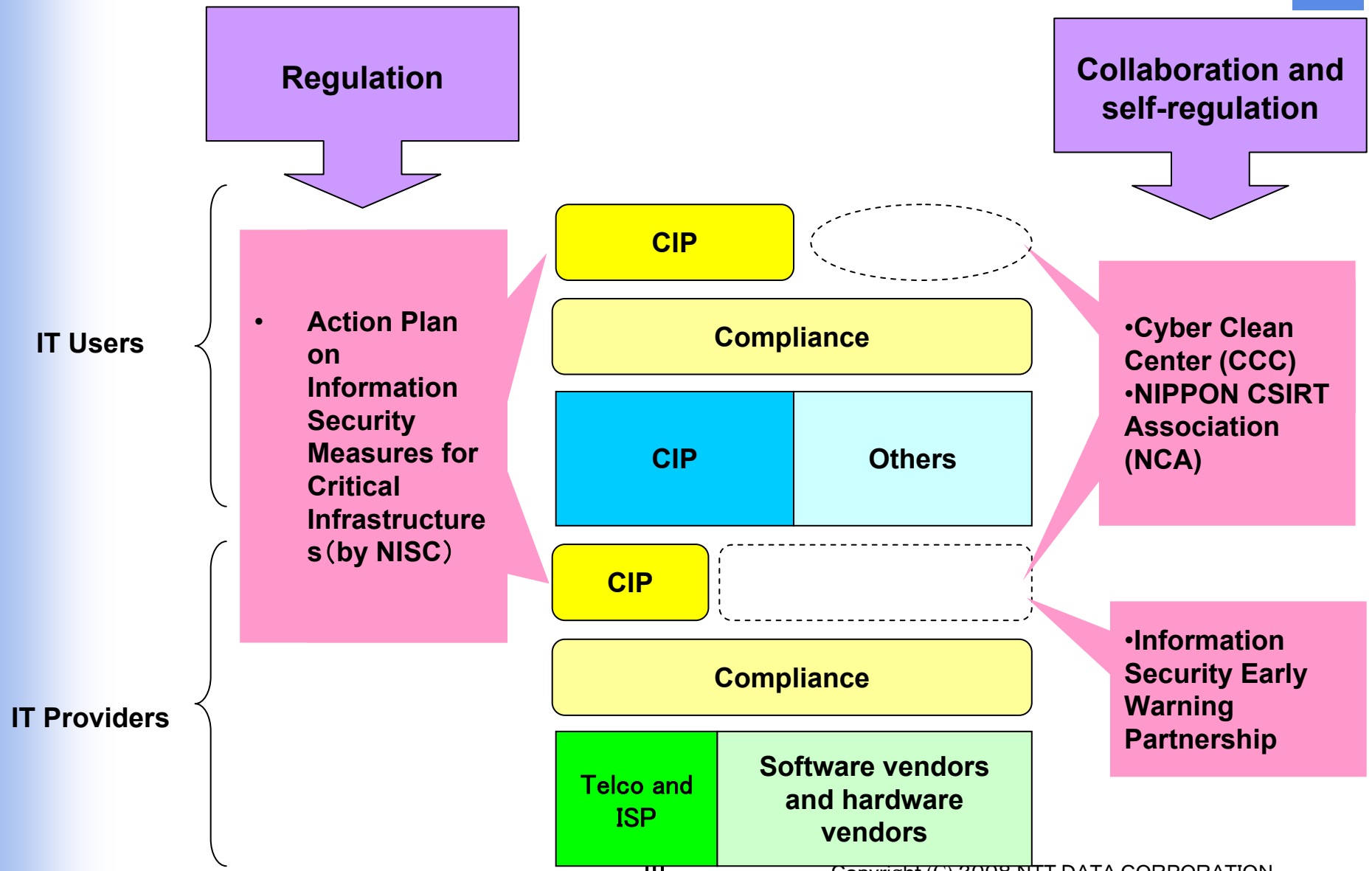
CIP (Japan and USA)

	USA		Japan	
Ministry	DHS/NCSD		NISC	
Measures	National infrastructure protection Plan (NIPP) •As a major component of the IT sector's responsibility •17 sector-specific plans, identified in U.S. Homeland Security Presidential Directive 7		•Action Plan on Information Security Measures for Critical infrastructures –"Security Standards, Guidelines etc." –Strengthening the Information Sharing Frameworks –Analysis of interdependencies –Cross-Sectoral Exercise …	
Sectors	17	Agriculture and Food, Health, Water, DIB, Energy, Chemical, Communications, IT, Transportation, Emergency Services, Dams, Postal and Shipping, Government Facilities, Commercial Facilities, Nuclear, Banking and Finance, Monuments and Icon (10 by DHS)	10	Telecommunications, Finance, Civil aviation, Railways, Electricity, Gas, Government/Administrative Services, Medical Services, Water Works, Logistics
IT	•IT Sector partnership model –IT Sector Coordinating Council (SCC) –IT Sector Specific Agency (SSA) •IT Sector Specific Plan (SSP), May 2007		Nothing special…	

CIP, critical infrastructure protection



CIP in Japan



"Information sharing" in CIP of Japan

- Action Plan on Information Security Measures for Critical Infrastructures (13 Dec., 2005)
  - "Security Standards, Guidelines etc." concerning Assurance of Information Security of Critical Infrastructure
  - Strengthening the Information Sharing Frameworks
  - Analysis of interdependencies
  - Cross-Sectoral Exercise

Information provision and liaisons between public and private sectors

- Provide information to the business entities
- Liaison from business entities
- Information providing and reporting procedures

CEPTOAR

- Function/Role
  - Contact section for information provided by the government
  - Sharing information with related organizations

CEPTOAR-Council

- Cross-sectoral information sharing environment
- Formation and functions of "CEPTOAR Council"
- Procedure for establishment

- NISC → Ministries → CIP business entities

- IT-malfunction
- By cyber attack, by unintentional factors, by disasters
- Include incidents, failures, delays of operation, etc. obliged to be reported by statutes and those the business entities engaged in critical infrastructures consider to be especially reported

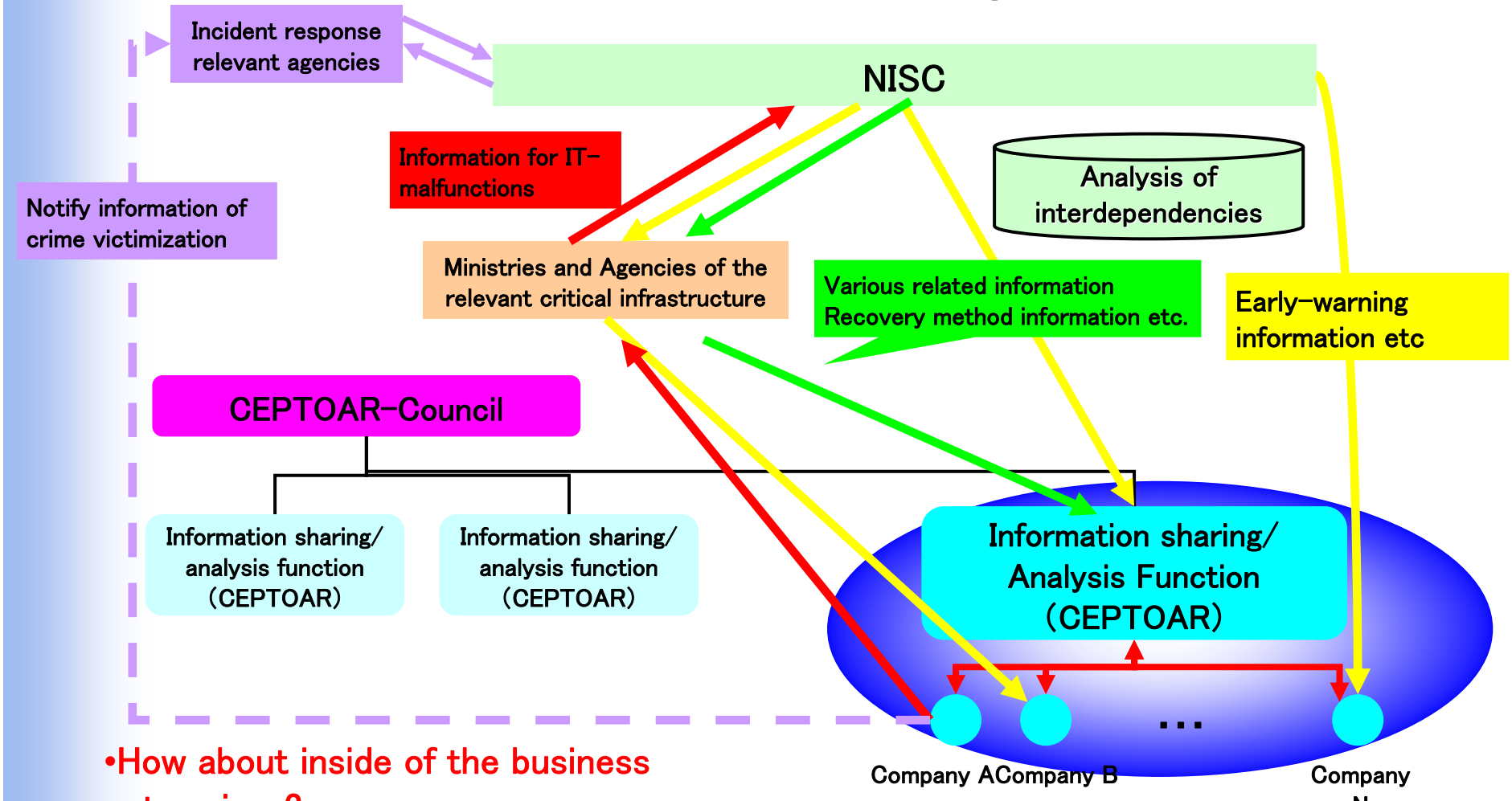
CSPTOAR= Capability for engineering of Protection, Technical Operation, Analysis and Response

Let's look into the details of CEPTOAR…

December 13, 2005 Decision by the Information Security Policy Council

"Action Plan on Information Security Measures for Critical infrastructures" Attachment 3-1

To realize and enhance information sharing frameworks…



•How about inside of the business enterprises?

Issue for business enterprises

- How to build up departments *inside*
  - Chief Information Security Officer, CISO
  - Information Security Department
  - Divide role and responsibility between each business unit and corporate staffs
- How to react to stakeholders *outside*
  - Disclosure by publishing "Information Security Report" to stakeholders
  - Report to ministries as follows;

Kind of the response	•Receive early warning information to transfer for sharing in-house	•Information for IT-malfunctions •Various related information •Recovery method information etc	•Notify information of crime victimization
Report to	NISC	Relevant Ministry	Law enforcement
POC	•Information Security Department	•Information Security Department •General Affairs Department	•General Affairs Department •Legal Department
Points and issues	•Via CEPTOAR or NISC	•Report to relevant ministry •Information Sharing with CEPTOAR	•Decide independently

CSIRT awareness raising for business

How to build up “CSIRT” in business enterprises

Business voices

Misunderstanding at security division

- Law and regulation define the details of CSIRT.
- Lack of flexibility for responding to the uniqueness of each business enterprises

- CSIRT needs too much money
- "My company is not so big as XXX to pay for start up CSIRT!"

- Need too much human resources, sometimes reform of corporate structure is required

Fact of CSIRT

- Organization and details of all CSIRTs are not same.
  - JPCERT/CC、HIRT、NTT-CERT、NIRT・・・

- Usual security measures or organizations may easily shit to CSIRT
  - Persons are same
  - Just do same things as before

- By declaring itself as CSIRT, you can easily cooperate with CSIRT colleagues

- Please do not worry by yourself ! It's a CSIRT !!

Points of CSIRT（RFC2350）

Application to each business enterprises may differ depending on various conditions

3.3 Charter

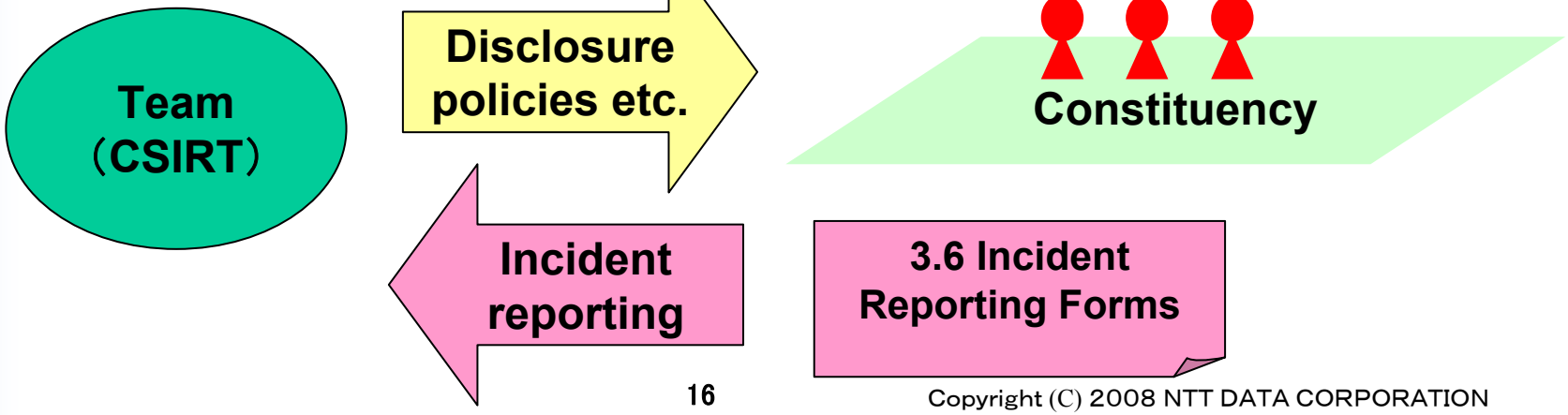
- Mission statement
- Constituency
- Sponsorship/ affiliation
- Authority

3.4 Policies

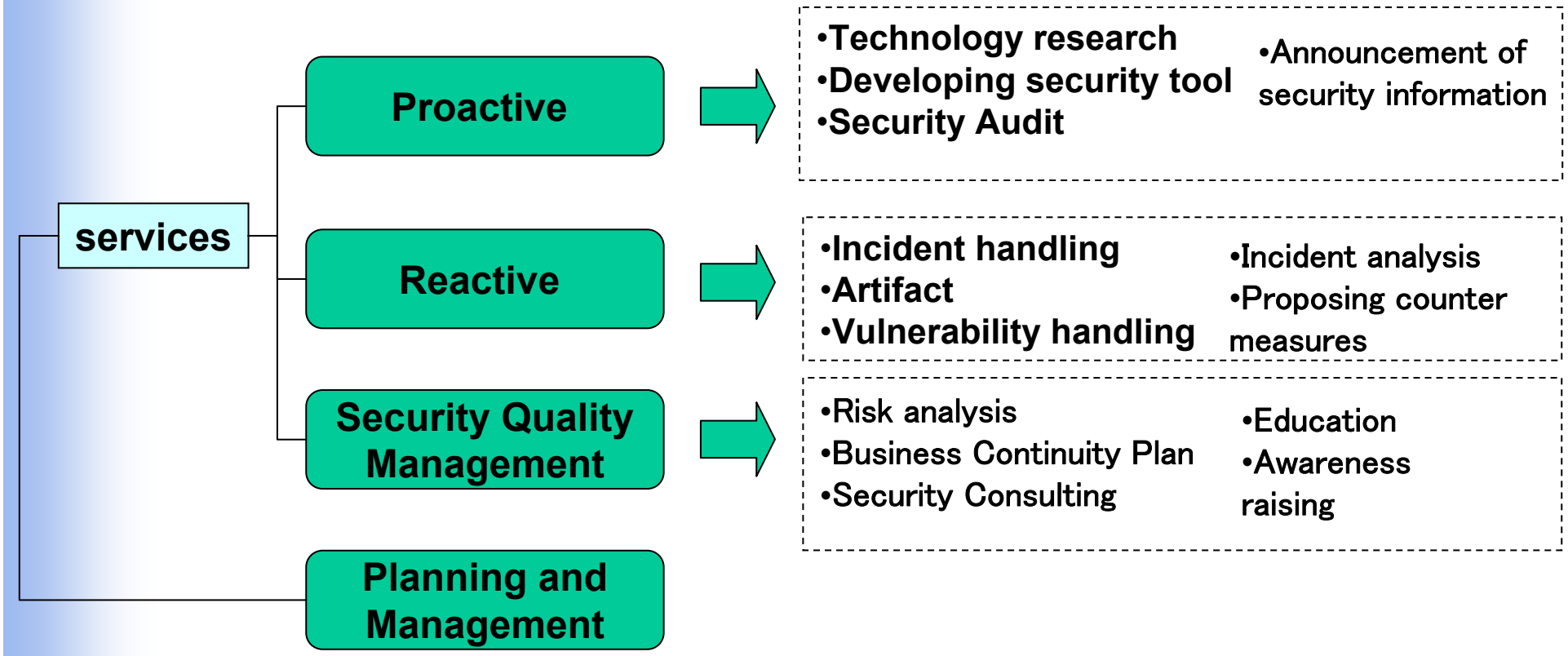
- Type of Incidents and level of Support
- Co-operation, Interaction and disclosure of information
- Communication and Authentication

3.5 Services

- Incident Response
  - Incident Triage
  - Incident Coordination
  - Incident Resolution
- Proactive Activities
  - Proactive services



The organization of CSIRT



Suggestion for Information Security Governance

- Compliance and/or information sharing
  - Not an alternative but "Both Sides of the Coin"
  - Without effective communication either of them cannot work for business enterprises

- Merits of CSIRT for corporate governance
  - Sharing information of threat by cooperation
  - Technology and tools brought by information sharing

- Basic framework of CSIRT, shown in slide No.16, would be quite effective when applied as a part of corporate governance
  - "A Culture of Security" by OECD Guidelines

Thank you very much!

Mail to: yamakawat@nttdata.co.jp