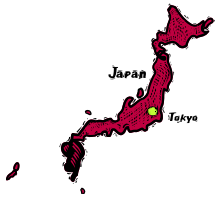
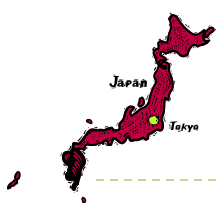


CyberDefense

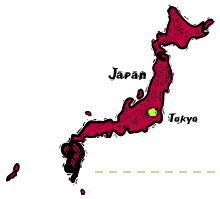
CSIRT Models in Japanese Large Companies

Toshio NAWA

Cyber Defense Institute, Inc.

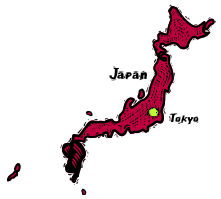


Do you know the real Japan?



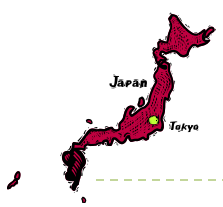
AGENDA

1. Cyber Security Threats in Japan
2. Efforts Against Cyber Security Threats in Japan
3. CSIRT models in Japanese Large Companies
4. Process for Developing CSIRT in Japan
5. Lessons Learned from CSIRT Operation in Japan



Topic 1

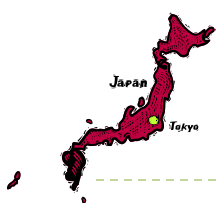
CYBER SECURITY THREATS IN JAPAN



Cyber Security Threats in Japan

Rank Order	10 Major Security Threat
1st	Ever-Changing Tactics for Website Defacement
2nd	Client Software Not Updated
3rd	A Variety of Purposes/Objectives of Computer Virus and Bots
4th	Vulnerability in Unsecured Server Products
5th	Be Sure to Take Incident Response to Information Leakage
6th	Targeted Attacks Carried Out Without Victims' Noticing
7th	DDoS Attacks That Cause Serious Damages
8th	Unauthorized Use of A Legitimate Account
9th	Security Holes in Cloud Computing
10th	Vulnerability in the Protocol Supporting the Internet Infrastructure

(Source: http://www.ipa.go.jp/security/english/third.html#10threats2010)

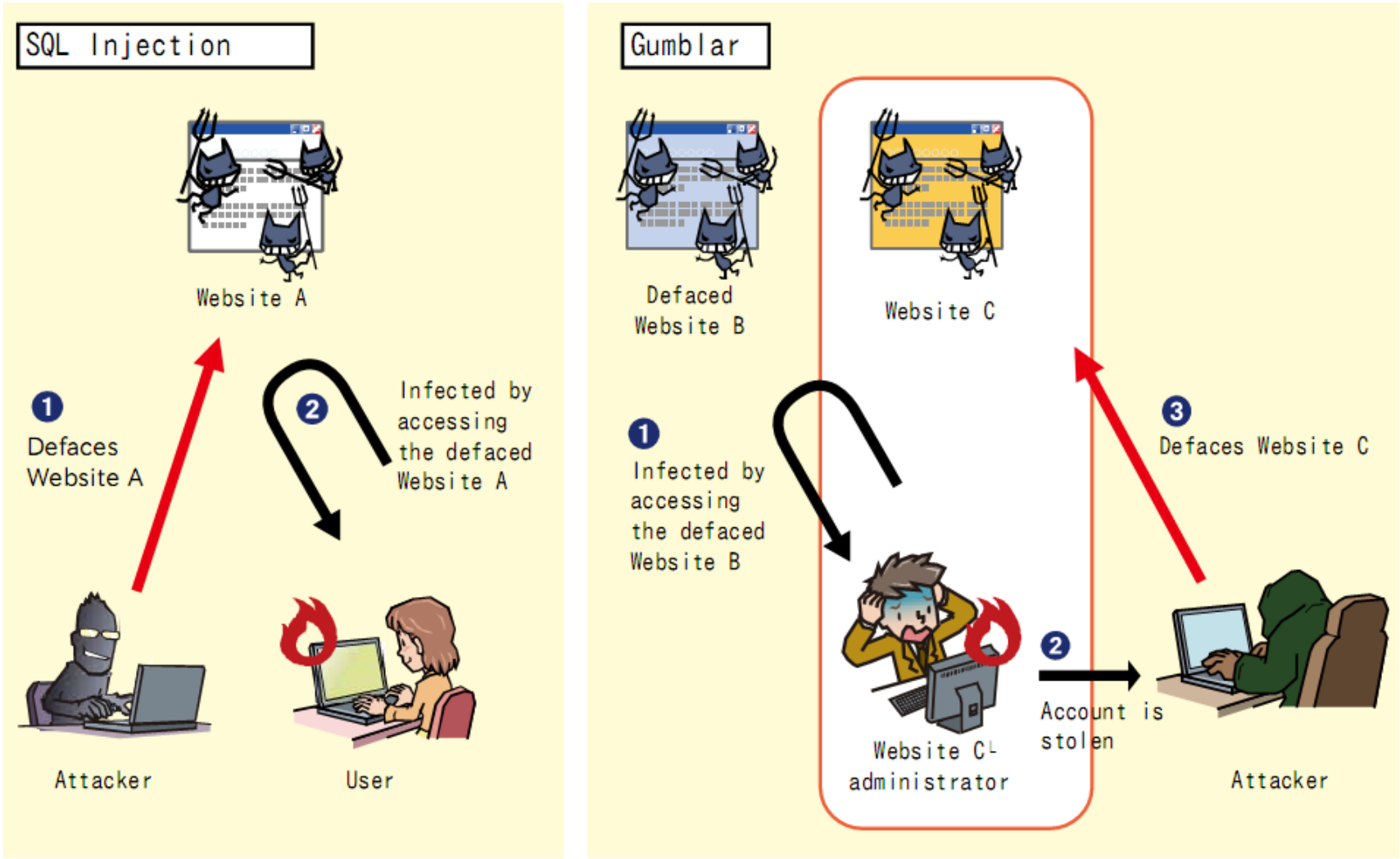


Cyber Security Threats in Japan

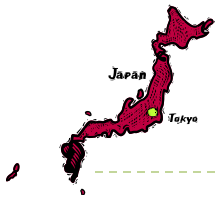
Rank Order	10 Major Security Threat
1st	**Ever-Changing Tactics for Website Defacement**
2nd	**Client Software Not Updated**
3rd	A Variety of Purposes/Objectives of Computer Virus and Bots
4th	Vulnerability in Unsecured Server Products
5th	**Be Sure to Take Incident Response to Information Leakage**
6th	**Targeted Attacks Carried Out Without Victims' Noticing**
7th	DDoS Attacks That Cause Serious Damages
8th	Unauthorized Use of A Legitimate Account
9th	Security Holes in Cloud Computing
10th	Vulnerability in the Protocol Supporting the Internet Infrastructure

(Source: http://www.ipa.go.jp/security/english/third.html#10threats2010)

Ever-Changing Tactics for Website Defacement



(Source: http://www.ipa.go.jp/security/english/third.html#10threats2010)



Client Software Not Updated

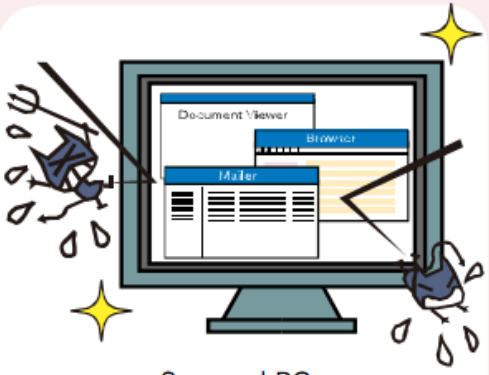
If no measure is taken against influenza …

Person taking countermeasure

Person not taking countermeasure

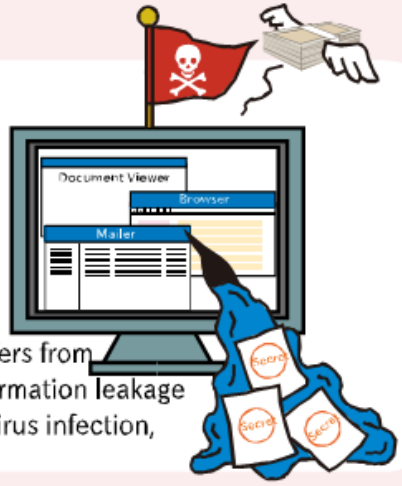
Comes down with influenza

If the client software is not updated …



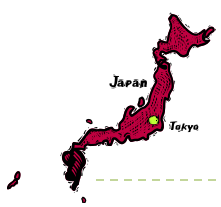
Secured PC

Unsecured PC



Suffers from information leakage or virus infection, etc.

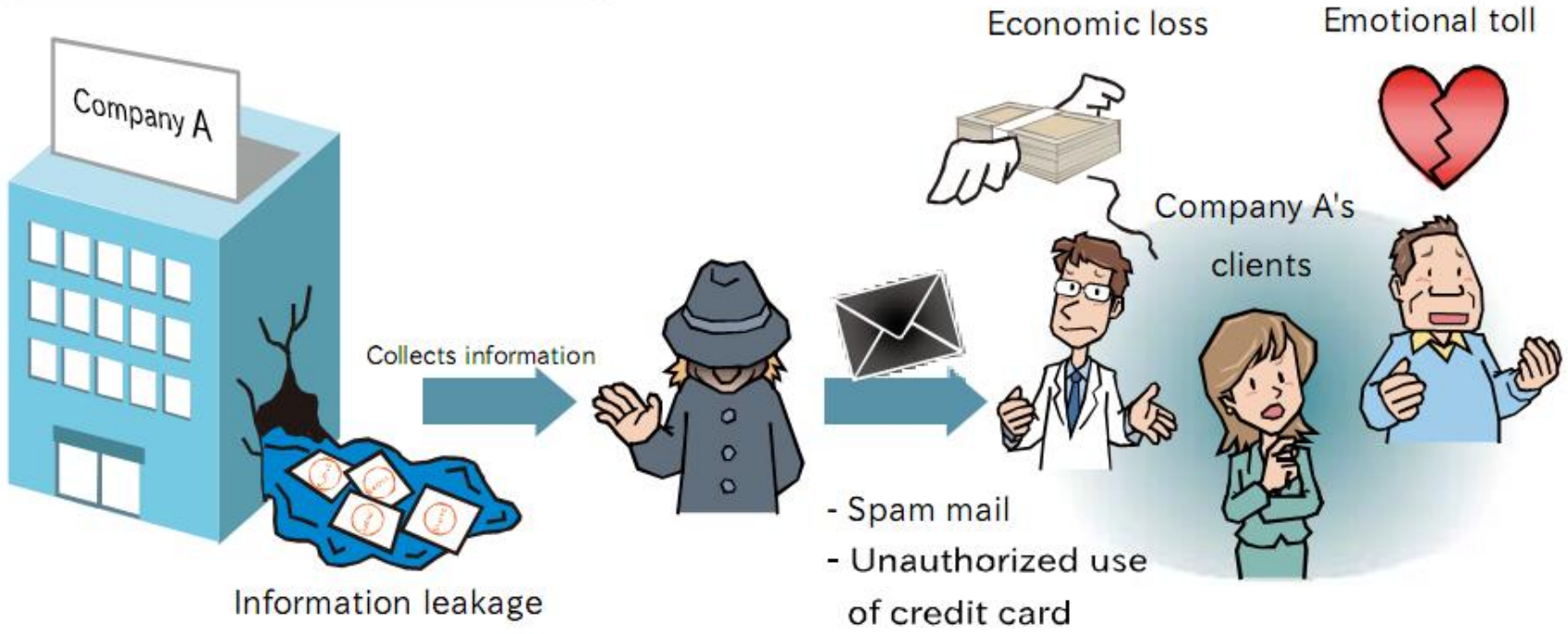
(Source: http://www.ipa.go.jp/security/english/third.html#10threats2010)



Be Sure to Take Incident Response to Information Leakage

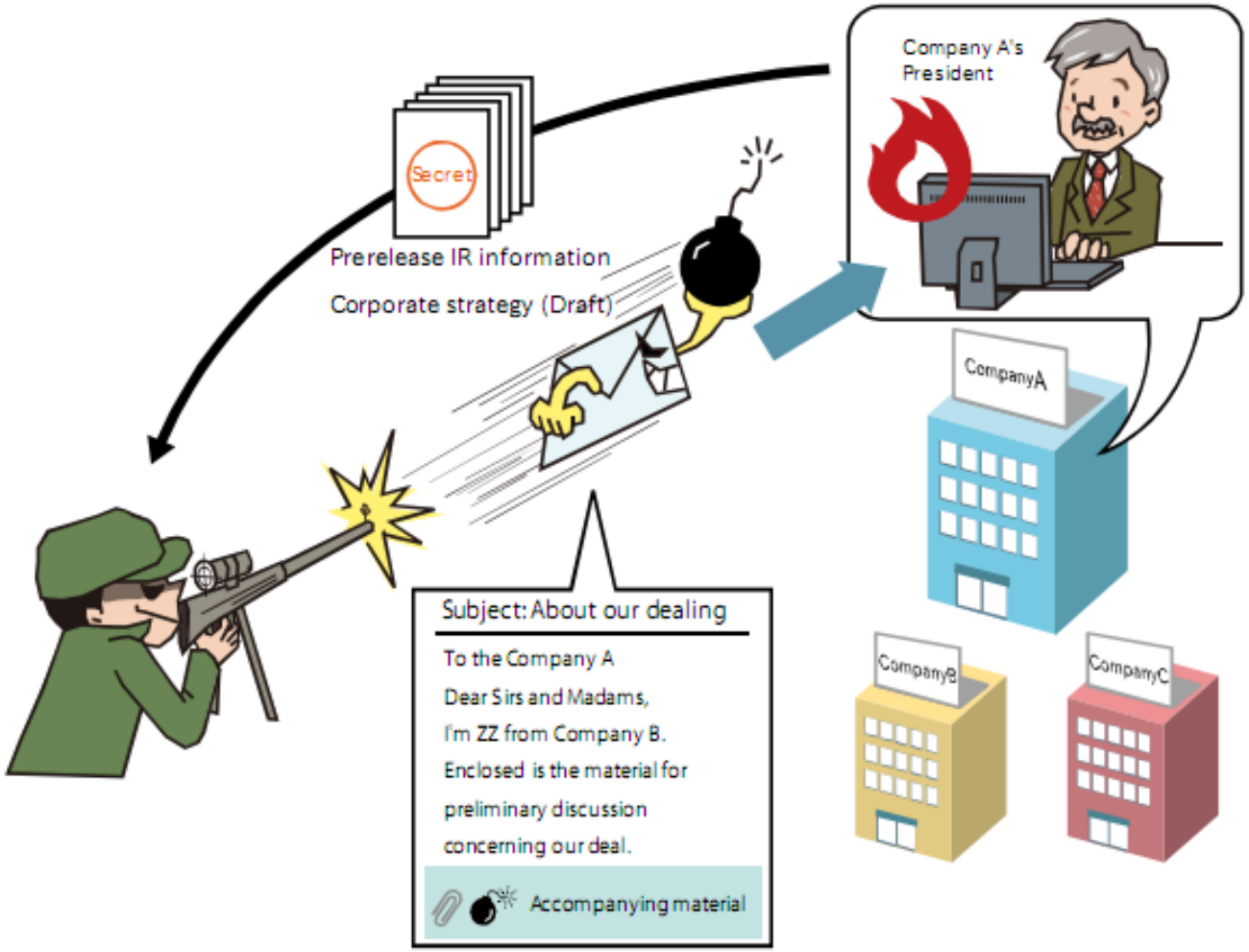
Damages suffered by Company A

- Losing its existing clients
- Having difficulty in getting new clients
- Decline in the stock market price
- Harmful rumors

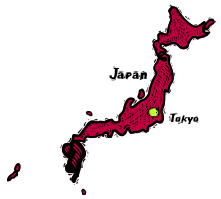


(Source: http://www.ipa.go.jp/security/english/third.html#10threats2010)

Targeted Attacks Carried Out Without Victims' Noticing

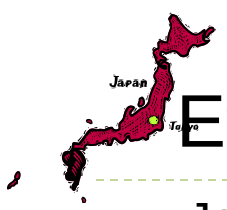


(Source: http://www.ipa.go.jp/security/english/third.html#10threats2010)



Topic 2

EFFORTS AGAINST CYBER SECURITY THREATS IN JAPAN



Efforts Against Cyber Security Threats in Japan

- Japanese Government created Strategy and Plan
  (Examples)
  - 1st National Strategy for Information Security (FY2006 to FY2008)
    - "Toward the realization of a trustworthy society"
  - 2nd National Strategy for Information Security (FY2009 to FY2011)
    - Aiming for Strong "Individual" and "Society"

  (Source: http://www.nisc.go.jp/eng/)

- Various Communities Created
  (Examples)
  - Public Sector: CEPTOAR-Council
  - Private Sector: Nippon CSIRT Association

- Cyber Security Exercise
  (Examples)
  - The Exercise against Cyber Terrorism in electricity sector (FY2004)
    - Sponsor is METI (Ministry of Economy, Trade and Industry).
    - Planner is CRIEPI (Central Research Institute of Electric Power Industry).

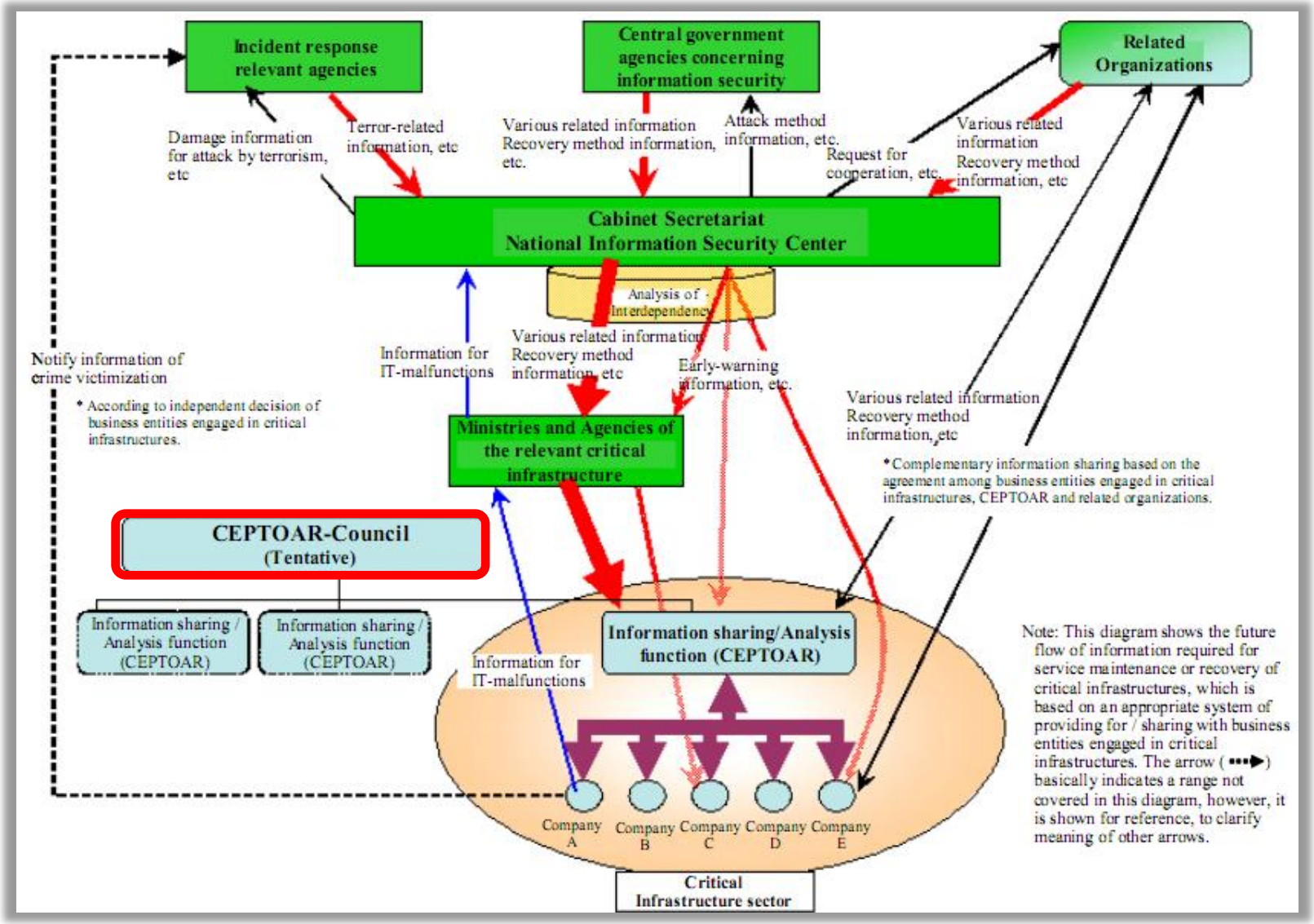
    (Source: http://criepi.denken.or.jp/jp/civil/result/presentation/report_shakai_risk2007/37.pdf)
  - The Exercise for Cyber Attacks in the telecommunications field (FY2006 to FY2008)
    - Sponsor is MIC (Ministry of Internal Affairs and Communications)
    - Planner is Telecom-ISAC Japan (Telecom Information Sharing and Analysis Center Japan)

    (Source [Movie]: http://www.soumu.go.jp/menu_kyotsuu/media/080401_1.html)
  - Implementing Cross-sectoral Exercises (FY2006 to FY2008, FY2009)
    - Sponsor is NISC (National Information Security Center)
    - Planner is MRI (Mitsubishi Research Institute)

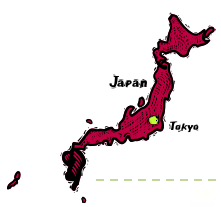
    (Source: http://www.nisc.go.jp/eng/pdf/overview_eng.pdf)

- CSIRT Developing in Major Large Companies

CEPTOAR-Council



(Source: http://www.nisc.go.jp/eng/pdf/actionplan_ci_eng.pdf)



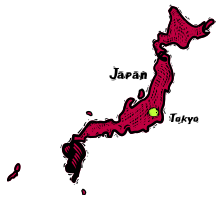
Nippon CSIRT Association

CSIRT
日本シーサート協議会

http://nca.gr.jp/

- Mission
  - Establish collaborative environment for member CSIRTs to work on common security concerns and issues
  - Member driven initiative to contribute to better secured information society
- History
  - March 27th, 2007 Founded by 6 CSIRTs (five of which are from commercial enterprises)
  - July 31st, 2007 Established operational framework
  - August 1st, 2007 Steering committee formed

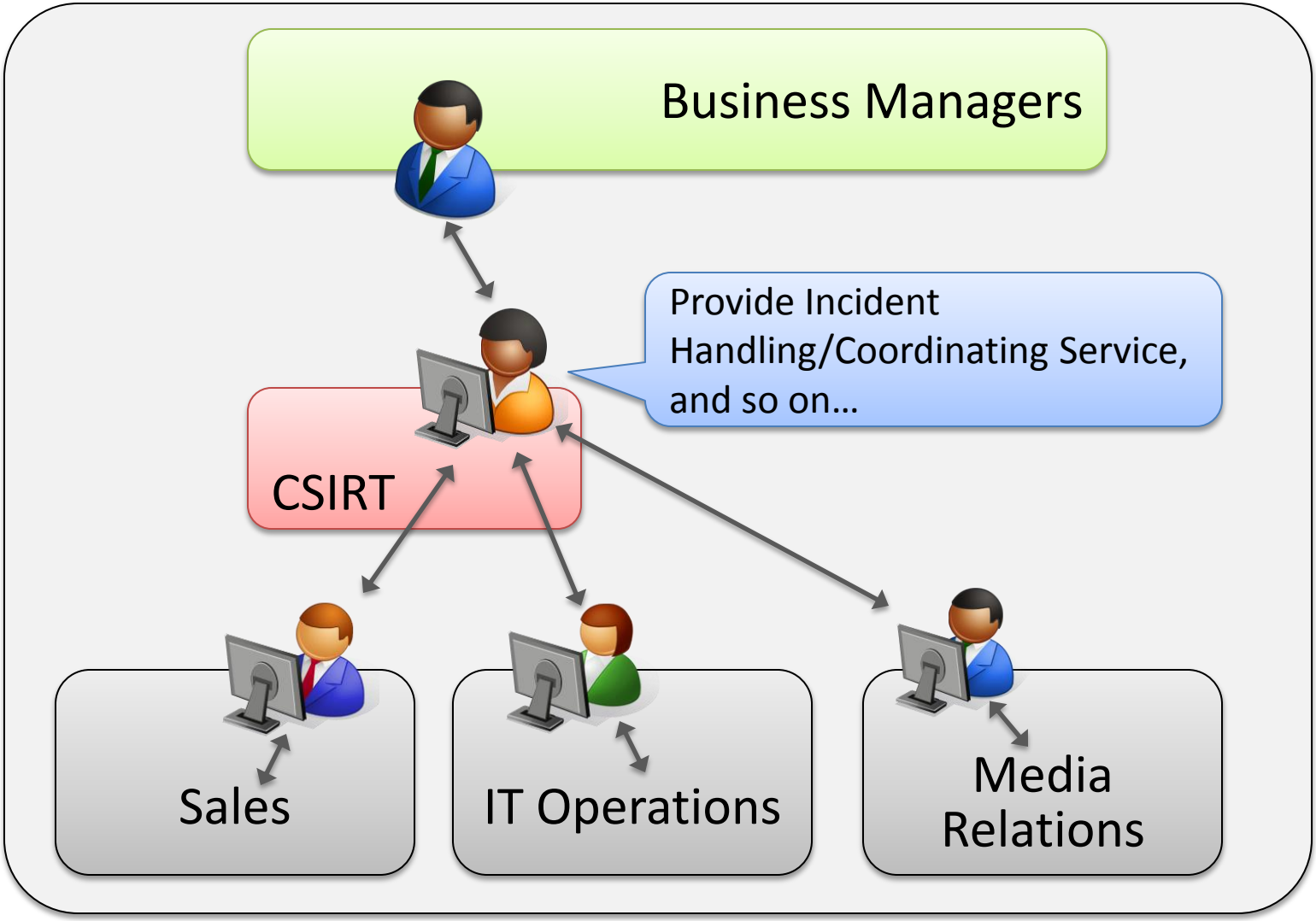
【Shīsā】lion-shaped roof ornament of Okinawa
(http://en.wikipedia.org/wiki/Shisa)



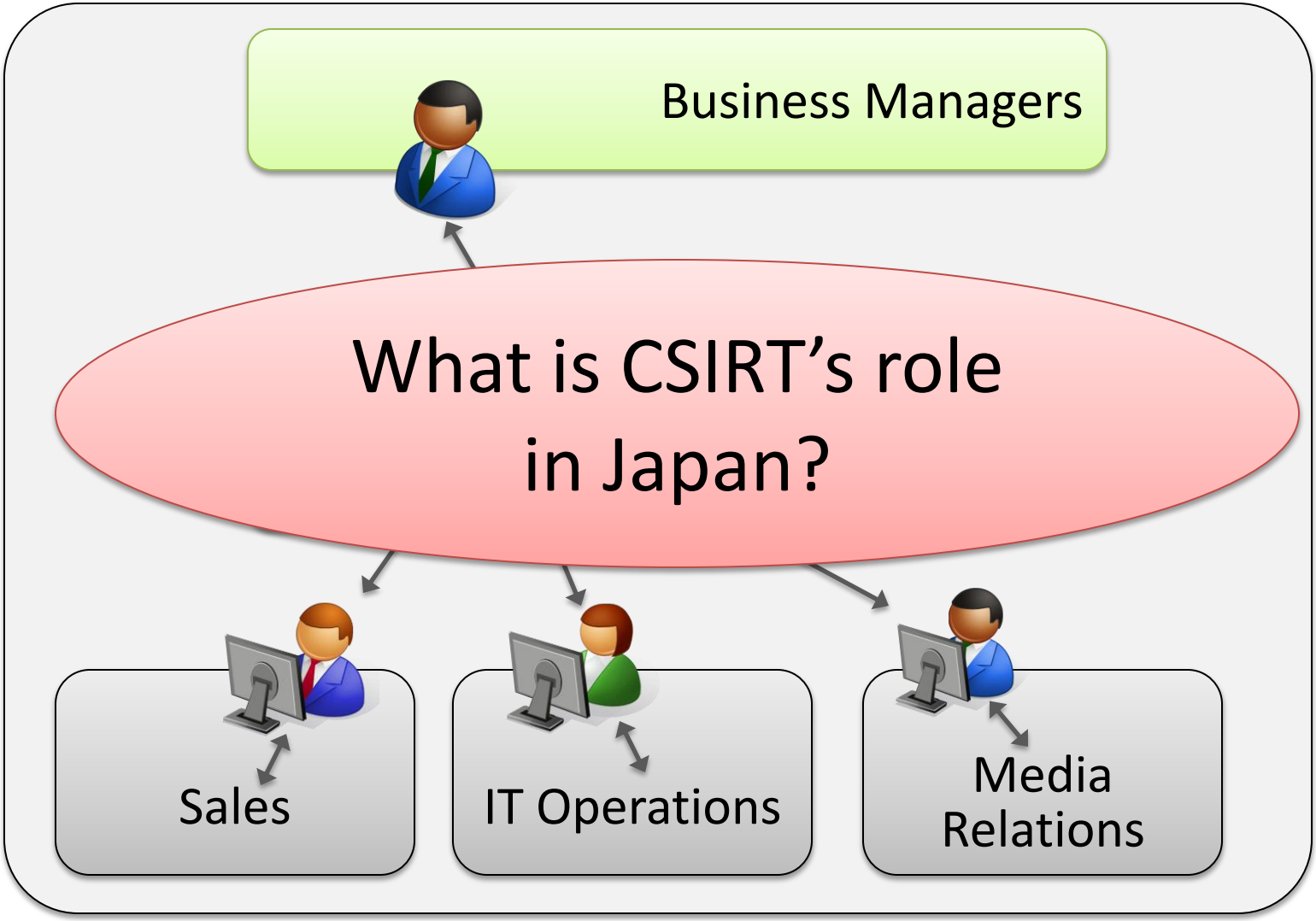
Topic 3

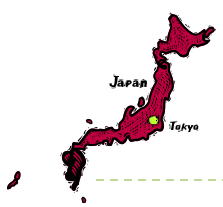
CSIRT MODELS IN JAPANESE LARGE COMPANIES

General approach to Develop CSIRT



An approach to Develop CSIRT in Japan

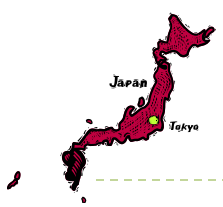




Developing CSIRTs in Japan (1)

: NCA members
: Non NCA members
: New CSIRT

1996	JPCERT/CC
1998	HIRT (in Hitachi)
2001	IBM X-FORCE IRT (in IBM Japan)
	IIJ-SECT (in Internet Initiative Japan)
2003	JSOC (in Lac)
	NTT-CERT (in NTT)
	YIRT (in Yahoo Japan)
2004	KLIRRT (in Kaspersky Labs Japan)
	SBCSIRT (in Softbank)
2005	KDDI-SOC (KDDI)
2006	NEXS.STC (in NEC Nexsolutions)
2007	KKCSIRT (in Kakaku.com)
	NCSIRT (in NRI Secure Technologies)
	(CSIRT in Infrastructure Business Group A)
	Rakuten-CERT (in Rakuten)
2008	mixirt (in mixi)
	OKI-CSIRT (in OKI)
	(CSIRT in Bank A)
2009	CDI-CIRT (in Cyber Defense Institute)
2010	Panasonic PSIRT (Panasonic)
	(CSIRT in Infrastructure Business Group B)



Developing CSIRTs in Japan (2)

: NCA members
: Non NCA members
: New CSIRT

1996 JPCERT/CC

1998 HIRT (in Hitachi)

2001 IBM X-FORCE IRT (in IBM Japan)
IIJ-SECT (in Internet Initiative Japan)

2003 JSOC (in Lac)
NTT-CERT (in NTT)
YIRT (in Yahoo Japan)

2004 KLIRRT (in Kaspersky Labs Japan)
SBCSIRT (in Softbank)

2005 KDDI-SOC (KDDI)

2006 NEXS.STC (in NEC Nexsolutions)

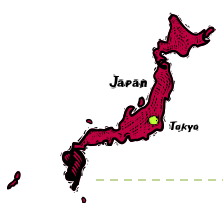
2007 KKCSIRT (in Kakaku.com)
NCSIRT (in NRI Secure Technologies)
(CSIRT in Infrastructure Business Group A)
Rakuten-CERT (in Rakuten)

2008 mixirt (in mixi)
OKI-CSIRT (in OKI)
(CSIRT in Bank A)

2009 CDI-CIRT (in Cyber Defense Institute)

2010 Panasonic PSIRT (Panasonic)
(CSIRT in Infrastructure Business Group B)

Web Portal Companies



Developing CSIRTs in Japan (3)

: NCA members
: Non NCA members
: New CSIRT

1996 JPCERT/CC

1998 HIRT (in Hitachi)

2001 IBM X-FORCE IRT (in IBM Japan)
IIJ-SECT (in Internet Initiative Japan)

2003 JSOC (in Lac)
NTT-CERT (in NTT)
YIRT (in Yahoo Japan)

2004 KLIRRT (in Kaspersky Labs Japan)
SBCSIRT (in Softbank)

2005 KDDI-SOC (KDDI)

2006 NEXS.STC (in NEC Nexsolutions)

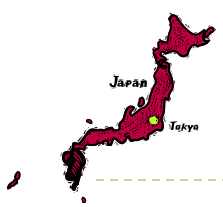
2007 KKCSIRT (in Kakaku.com)
NCSIRT (in NRI Secure Technologies)
(CSIRT in Infrastructure Business Group A)
Rakuten-CERT (in Rakuten)

2008 mixirt (in mixi)
OKI-CSIRT (in OKI)
(CSIRT in Bank A)

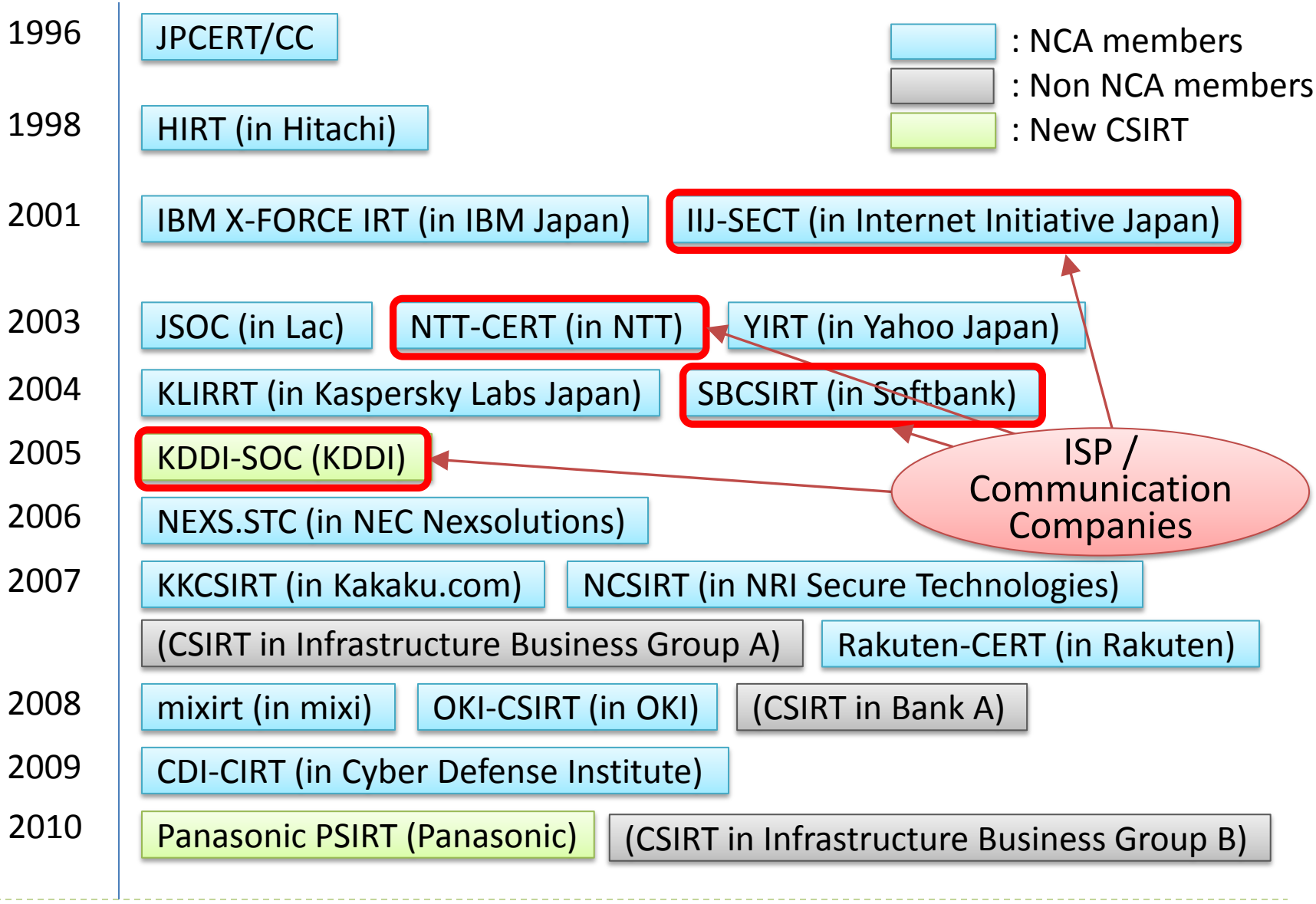
2009 CDI-CIRT (in Cyber Defense Institute)

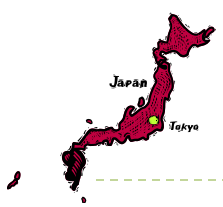
2010 Panasonic PSIRT (Panasonic)
(CSIRT in Infrastructure Business Group B)

Industrial Companies



Developing CSIRTs in Japan (4)





Developing CSIRTs in Japan (5)

: NCA members
: Non NCA members
: New CSIRT

1996 JPCERT/CC

1998 HIRT (in Hitachi)

2001 IBM X-FORCE IRT (in IBM Japan)
IIJ-SECT (in Internet Initiative Japan)

2003 JSOC (in Lac)
NTT-CERT (in NTT)
YIRT (in Yahoo Japan)

2004 KLIRRT (in Kaspersky Labs Japan)
SBCSIRT (in Softbank)

2005 KDDI-SOC (KDDI)

2006 NEXS.STC (in NEC Nexsolutions)

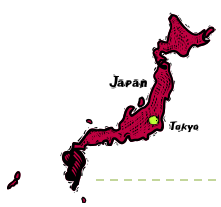
2007 KKCSIRT (in Kakaku.com)
NCSIRT (in NRI Secure Technologies)
(CSIRT in Infrastructure Business Group A)
Rakuten-CERT (in Rakuten)

2008 mixirt (in mixi)
OKI-CSIRT (in OKI)
(CSIRT in Bank A)

2009 CDI-CIRT (in Cyber Defense Institute)

2010 Panasonic PSIRT (Panasonic)
(CSIRT in Infrastructure Business Group B)

Security Venders



Organizational model for CSIRT

Outside Japan

With Strong Authority

Management

CIO

CSIRT

Transfer of authority from CIO

IT Operations

Customer Service

Other Departments

Subject to the authority of CIO (via CSIRT)

Japan

Consensual decision making

Management

CSIRT

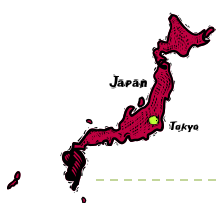
Lack of sufficient authority (No Transfer of authority)

IT Operations

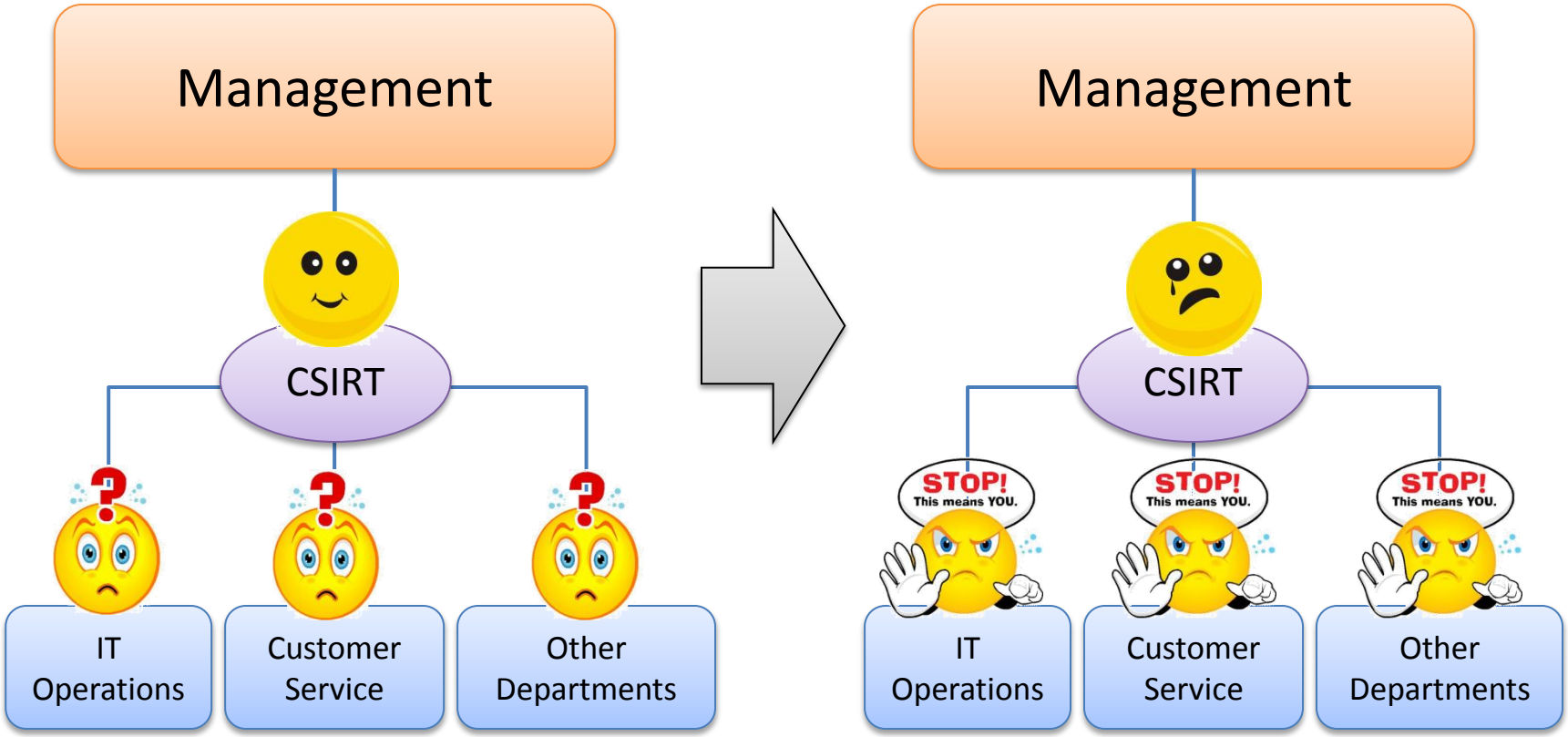
Customer Service

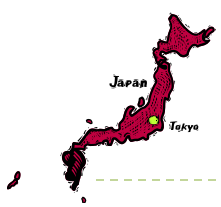
Other Departments

Difficult to follow CSIRT instructions (Field has authority to respond)

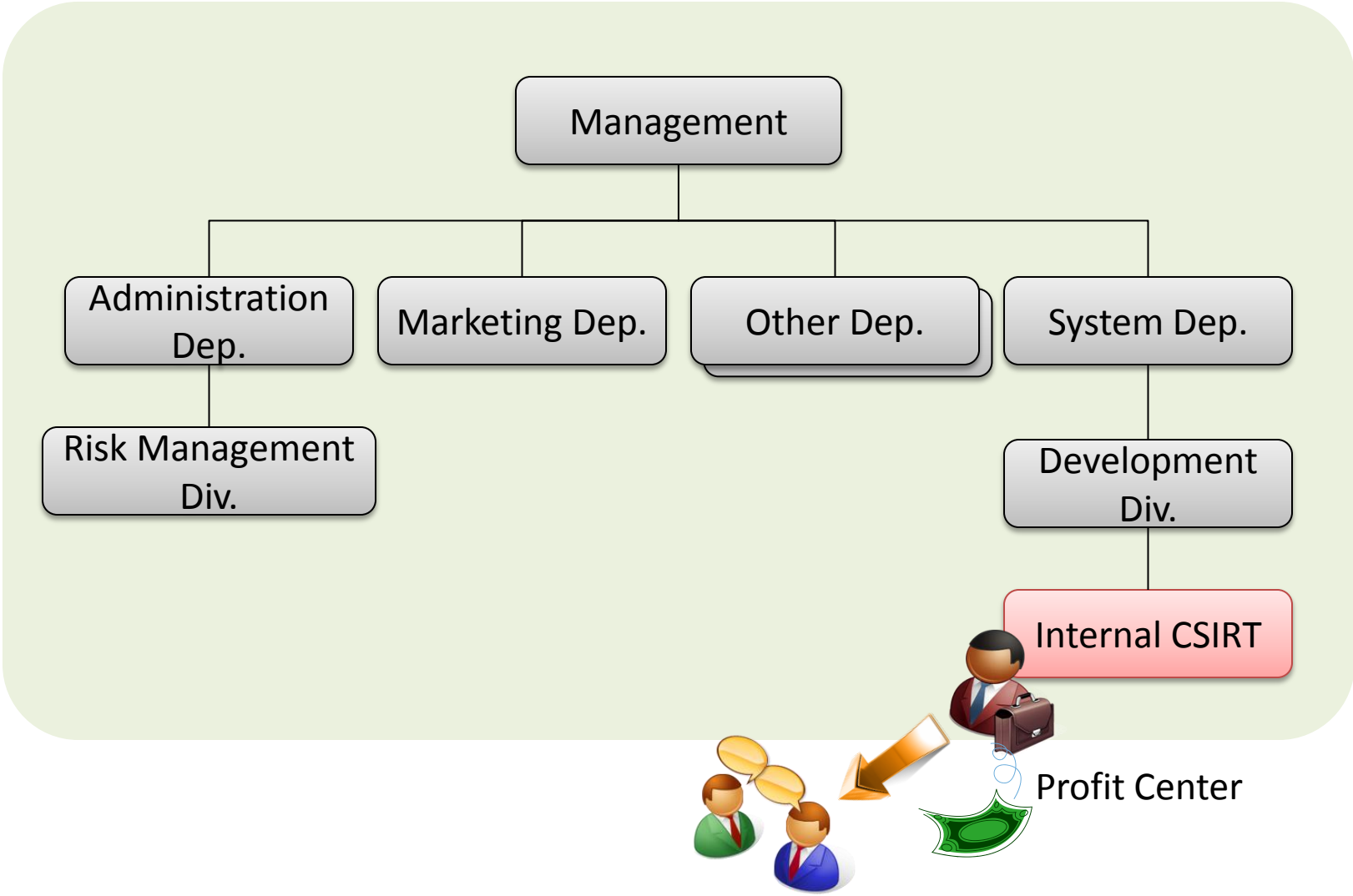


If developing CSIRT … in Japan

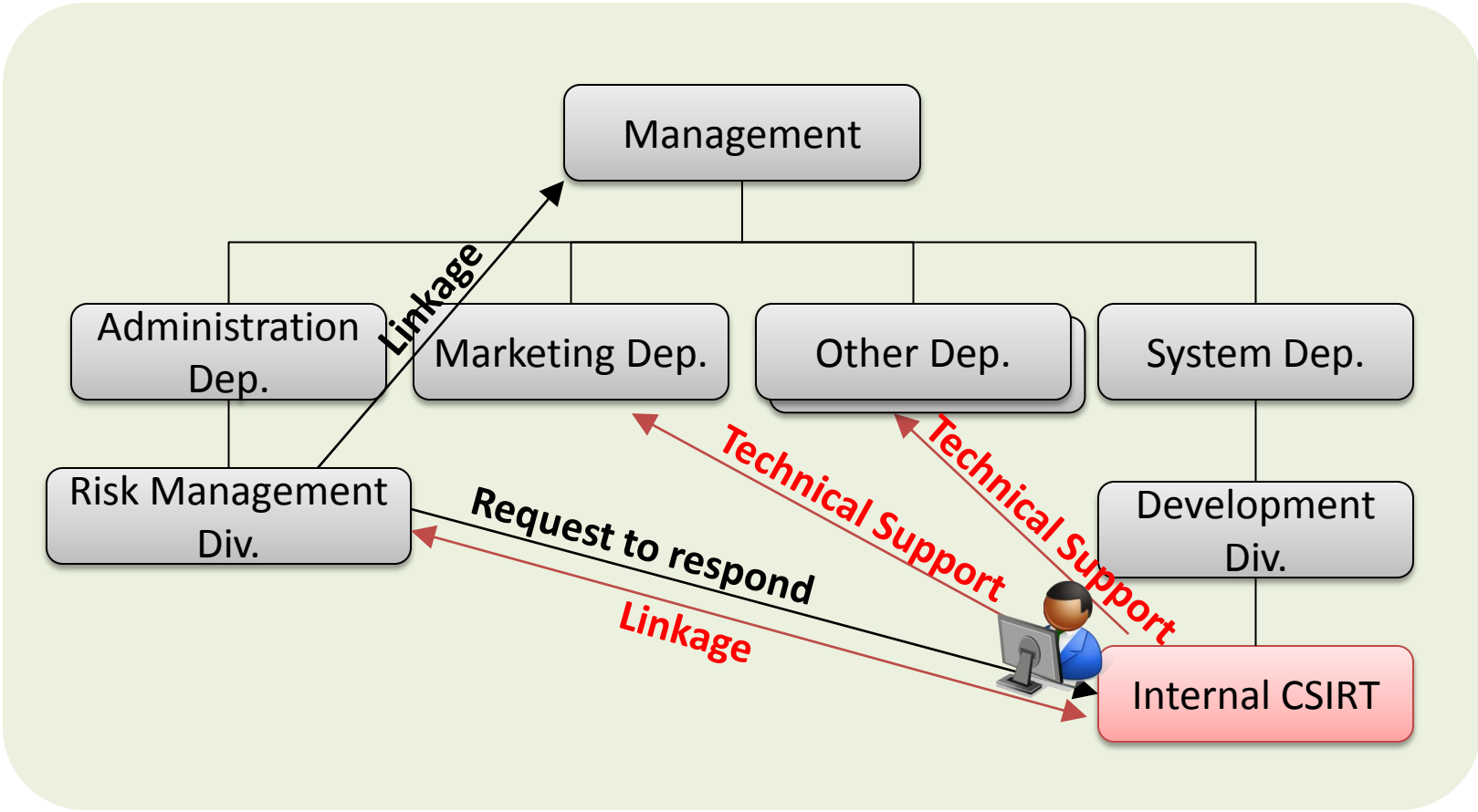




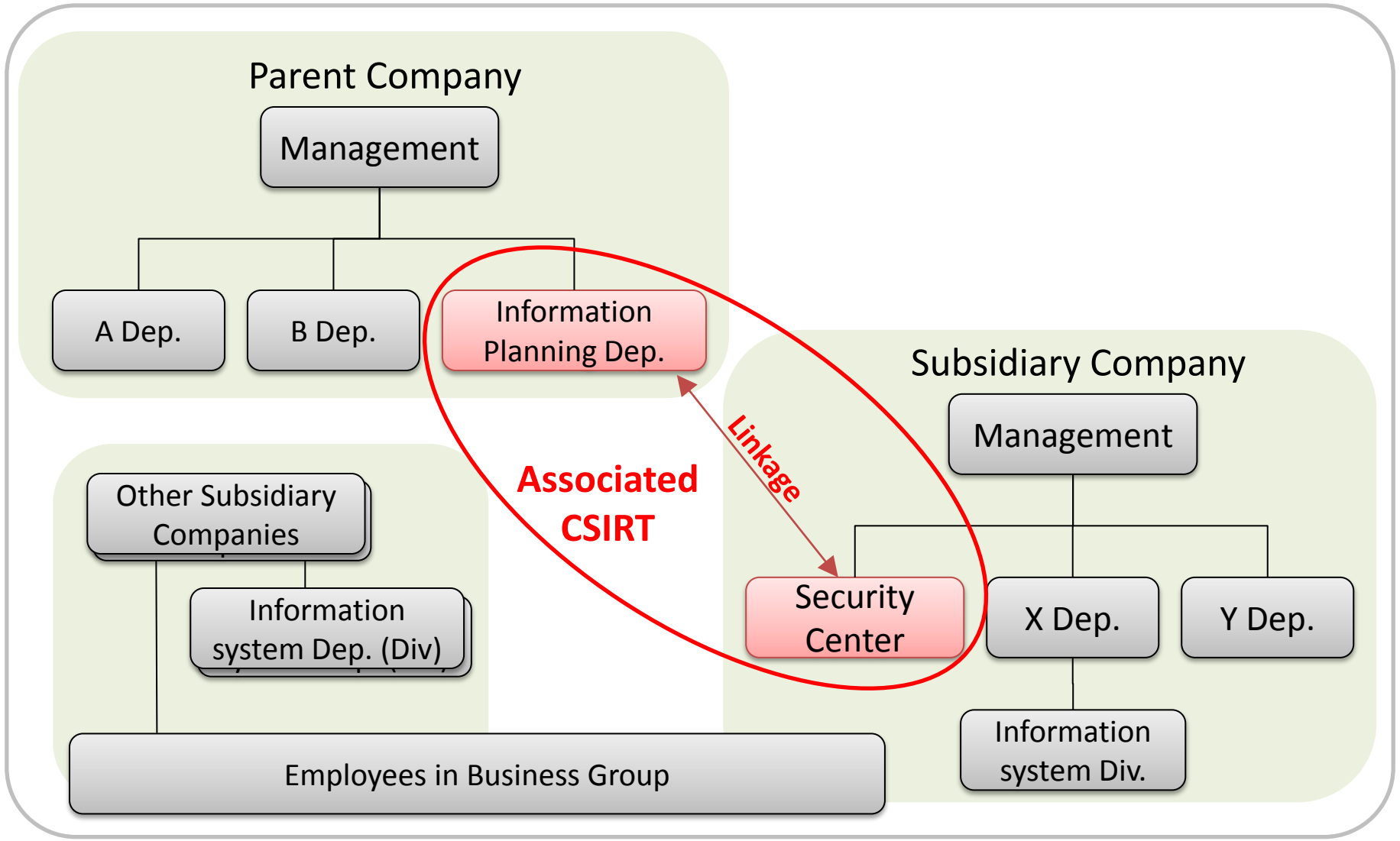
Organization Model 1: Large Company (1)



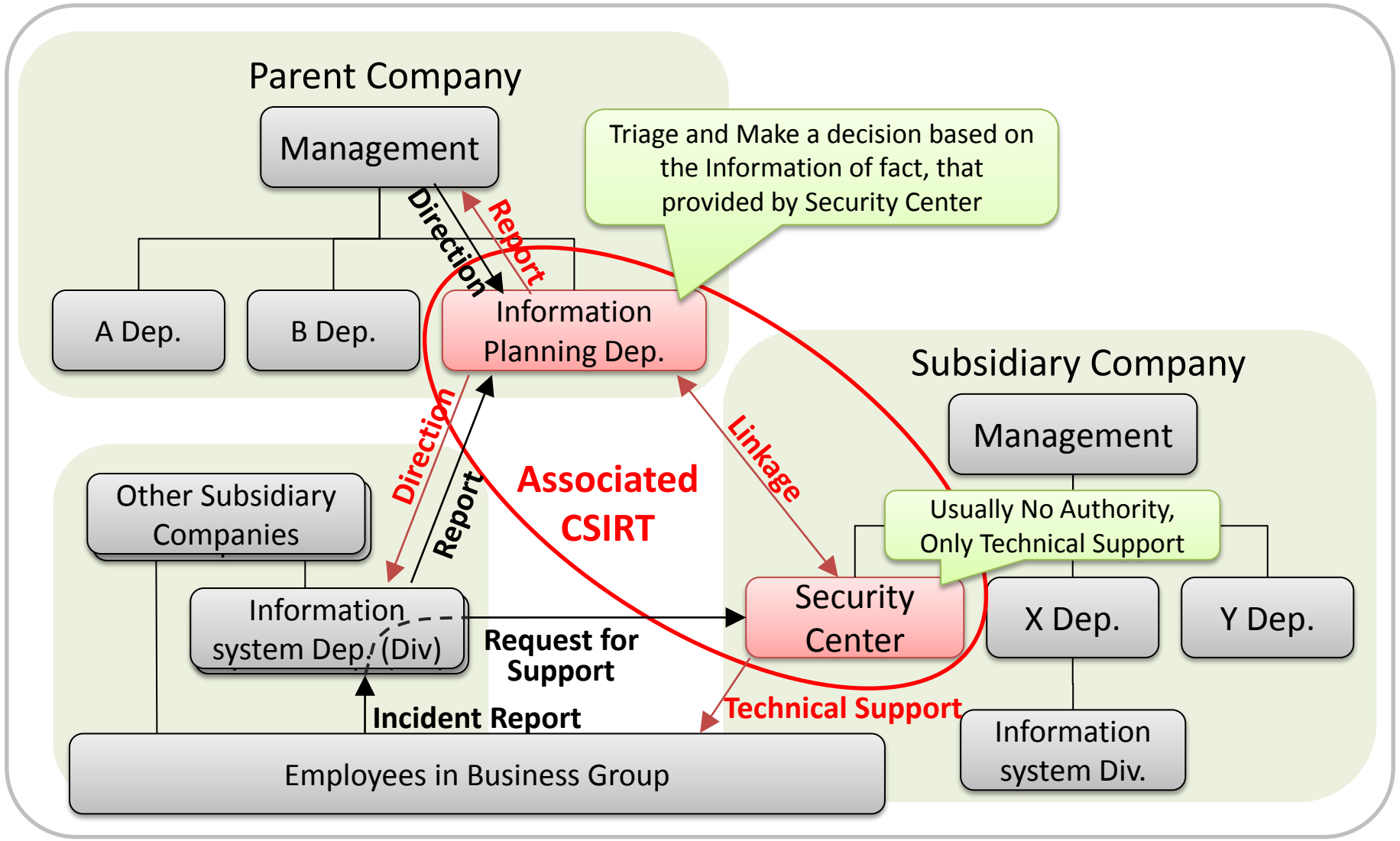
Organization Model 1: Large Company (2)



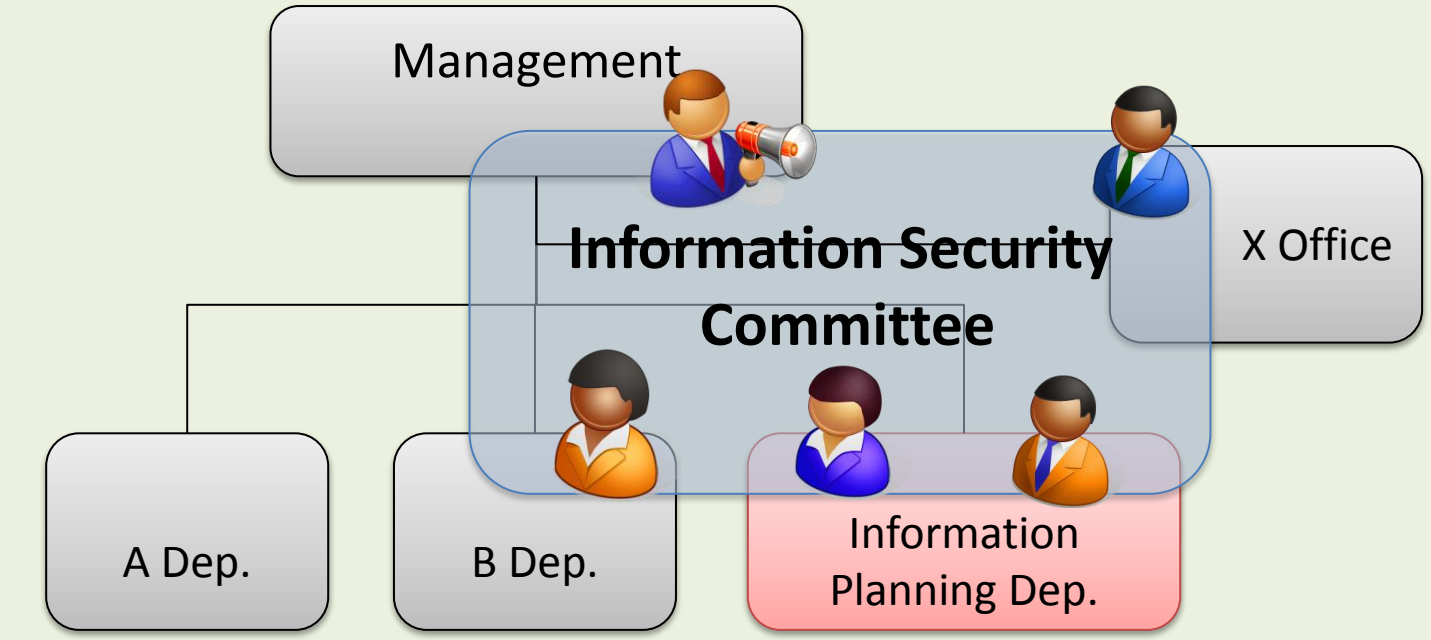
Organization Model 2: Business Group A (1)

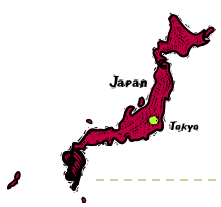


Organization Model 2: Business Group A (2)



Organization Model 2: Business Group A (3)





Organization Model 3: Business Group B (1)

Parent Company

Management

Administration Dep.

Other Dep.

X Institute

Other Institute

Y Laboratory

Other Laboratories

Group CSIRT

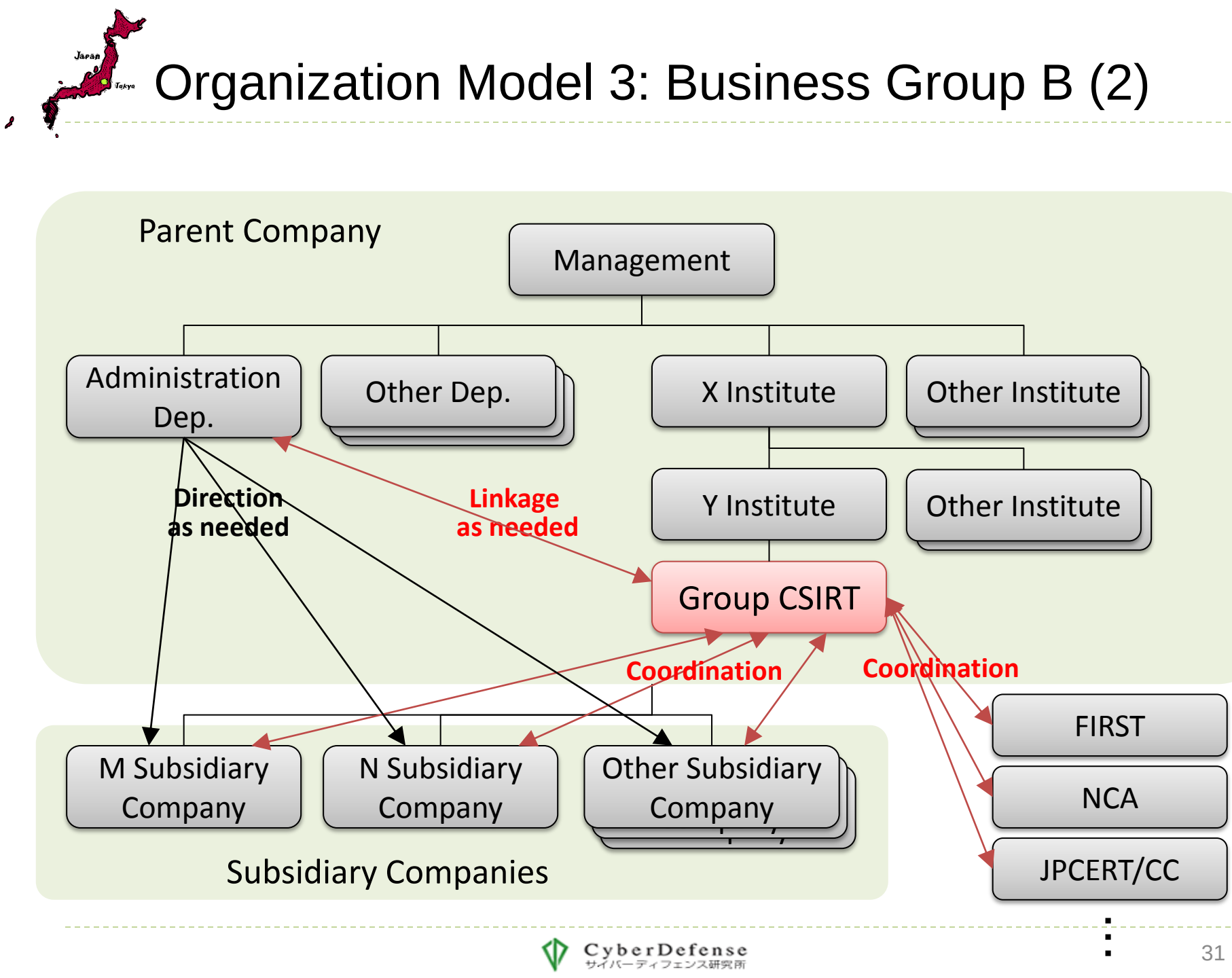
M Subsidiary Company

N Subsidiary Company

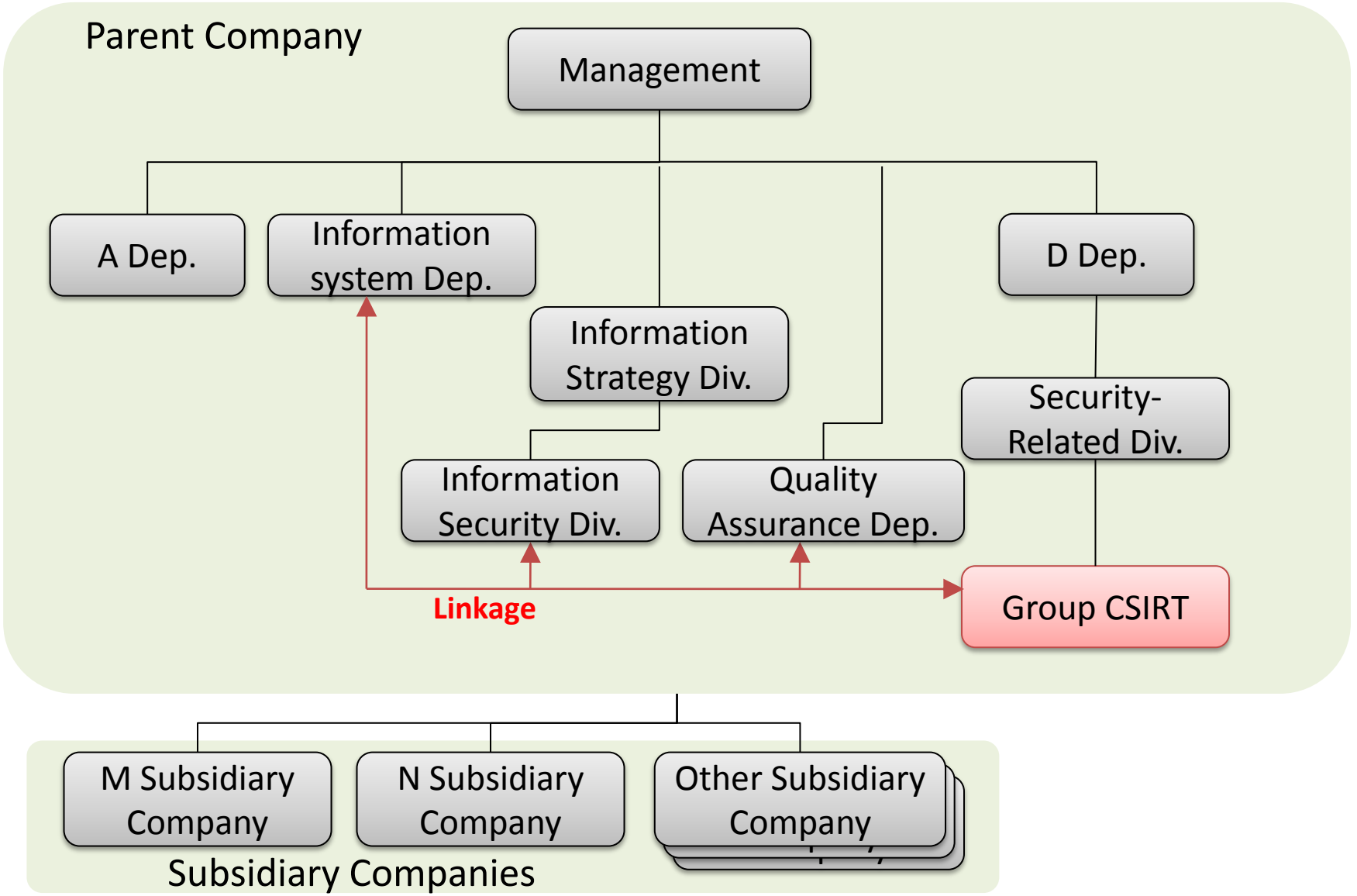
Other Subsidiary Company

Subsidiary Companies

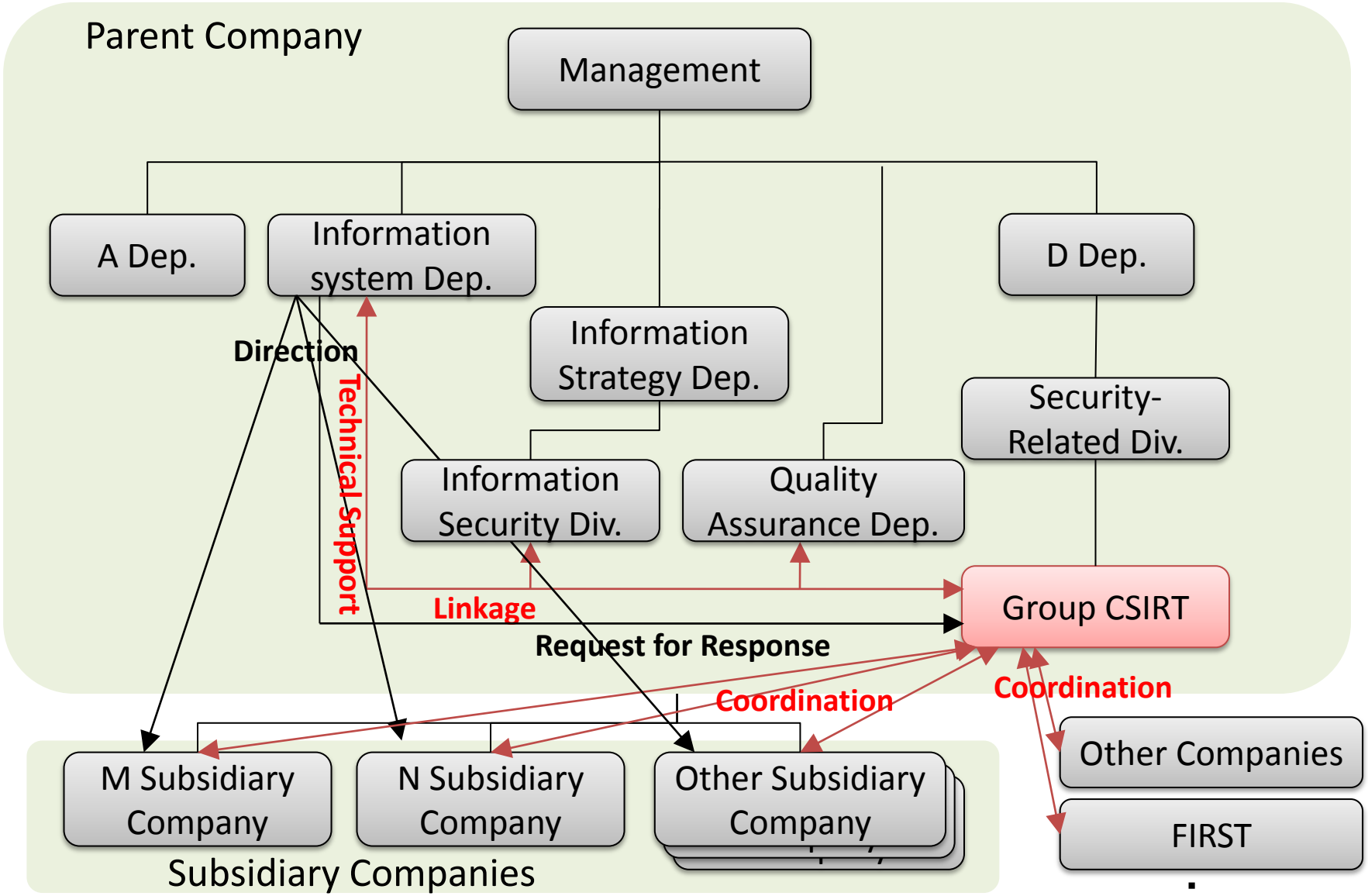
Organization Model 3: Business Group B (2)

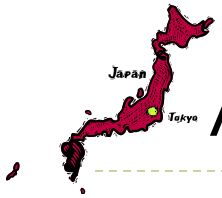


Organization Model 4: Business Group C (1)



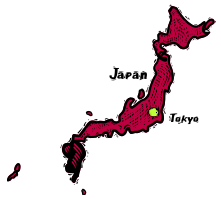
Organization Model 4: Business Group C (2)





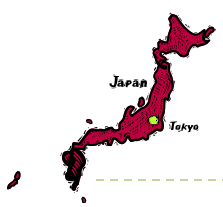
Analysis of CSIRT Organization Models in Japan

- **Lack of authority**
- Main service is **technical support** with relying on other division
- **Existence of the response team** for natural disasters (Earthquake, Typhoon, Tsunami and so on)
- Tendency to look on CSIRT as a (security) **technical service cente**r.
- Many **oppositions occur**, if there are any modifications of existing organization structure to set up CSIRT.
- Tendency to operate as **(technical) analysis centers**
  - Not necessary of investigative and analytical capabilities
  - Use the outside specialist



Topic 4

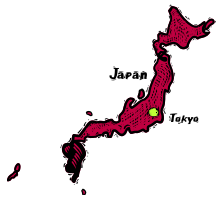
PROCESS FOR DEVELOPING CSIRT IN JAPAN



Process for developing CSIRT in Japan

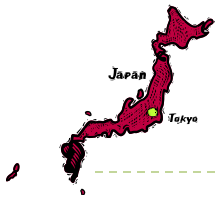
	Outside Japan (CERT/CC)	Japan
Step 1	Obtain management support and buy-in	**Obtain colleague's support and assistance**
Step 2	Determine the CSIRT strategic plan	**Determine the persuasion plan**
Step 3	Gather relevant information	**Gather negative information**
Step 4	Design the CSIRT vision	**Design the CSIRT organization model**
Step 5	Communicate the CSIRT vision and operational plan	**Communicate with external CSIRT expertise**
Step 6	Begin CSIRT implementation	**Begin CSIRT documentation**
Step 7	Announce the operational CSIRT	**Propose the idea of CSIRT to management**
Step 8	Evaluate CSIRT effectiveness	**Get the CSIRT budget**

↑(Source: http://www.cert.org/csirts/Creating-A-CSIRT.html)



Topic 5

LESSONS LEARNED FROM CSIRT OPERATION IN JAPAN



Lessons Learned from CSIRT Operation

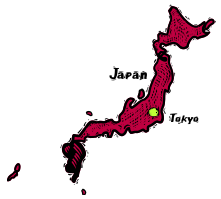
- After developing CSIRT, **critical incidents do not occur frequently**.
  - Management tends to consider CSIRT to be not necessary.
  - Lack of opportunity for skill development for new CSIRT staff
  - Not increase perceived reliability of CSIRT

- **Not easy to collaborate** with other CSIRT
  - Difficult to let outsiders know in-house information
  - Some CSIRT are predicated on no collaboration with outsiders

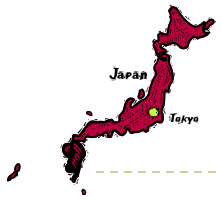
- CSIRT Staff tend to **double as other security related roles**.
  - Difficult to secure adequate human resources

- CSIRT Staff is **difficult to have the business management viewpoint**, so CSIRT is needed to collaborate with other related divisions.
  - Assign the appropriate staff in other related divisions as CSIRT member

- **All of the incident reports can not received**.
  - Some incidents were resolved in each division.
  - If received all, CSIRT will become overwork.

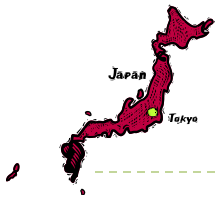


SUMMARY



Summary

- Classic CSIRT textbook says to set up CSIRTs **directly below the management**.
- In Japan, it is difficult because Japanese (large company) have **very different culture and structure**.
- Most of **Japanese CSIRT don’t have good authority** to deal with the incident, but work with existing department and organization that have the authority.
- Main service of Japanese CSIRT is **(security) technical support**.



Contact Information

Toshio NAWA

Cyber Defense Institute, Inc.

Email: nawa@cyberdefense.jp

Web: www.cyberdefense.jp (Office)

www.cirt.jp (Response Team)

Tel: +81-3-5209-4335

PGP Fingerprint:

5086 9036 0BEB 4A24 89FC 9D35 230A 311B 79A1 78CA