

## Development of Information Security-Focused Incident Prevention Measures for Critical Information Infrastructure in Japan

October 1, 2009

**Hideaki Kobayashi \*1, Kenji Watanabe \*2,  
Takahito Watanabe \*1, and Yukinobu Nagayasu \*1**

**\*1 Security Engineering Laboratory, IT Security Center,  
Information-technology Promotion Agency, Japan (IPA)  
{hd-koba, t-watana, y-nagaya}@ipa.go.jp**

**\*2 Nagaoka University of Technology  
watanabe@kjs.nagaokaut.ac.jp**



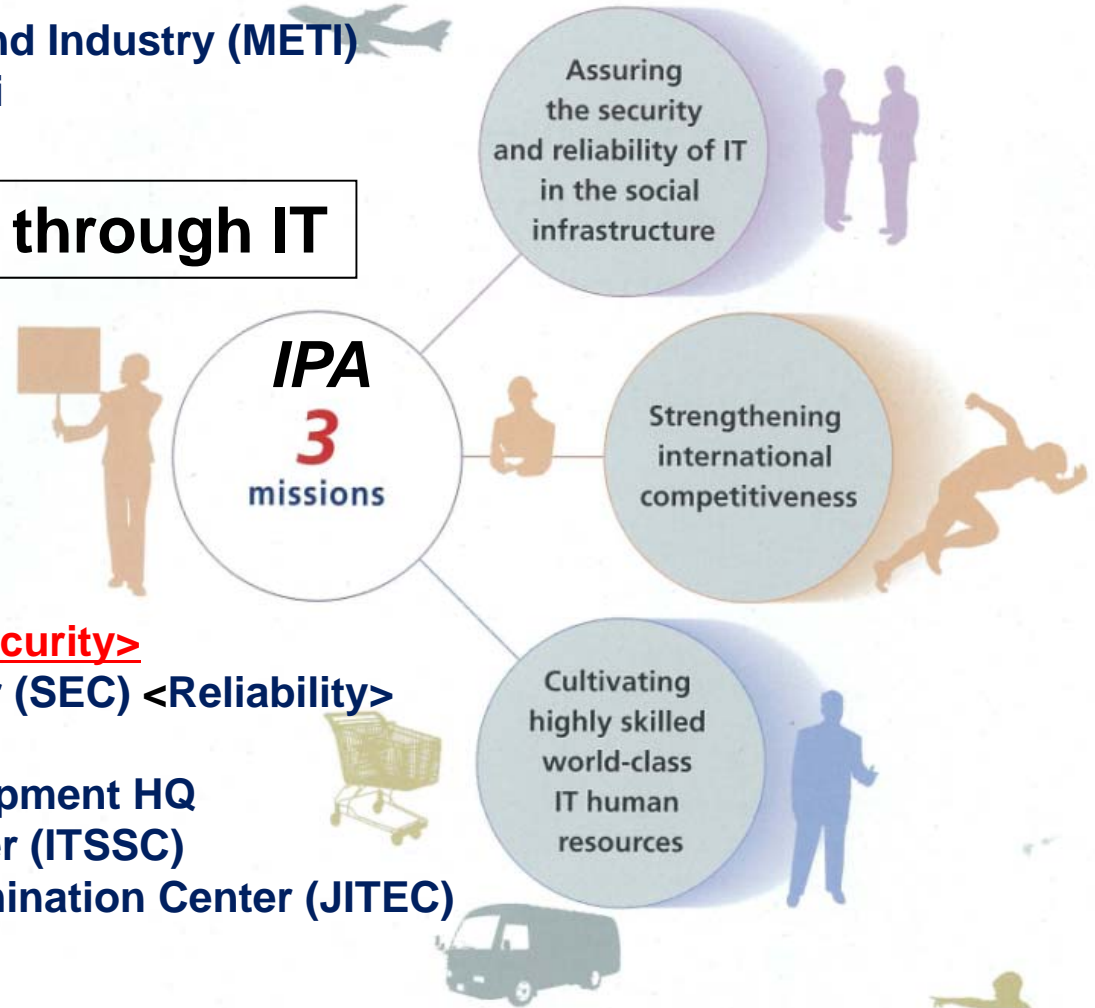
- 1. Overview of Information-technology Promotion  
Agency, Japan (IPA)**
- 2. National Strategy on Information security for Critical  
Infrastructure in Japan**
- 3. 4 Step Approach and Self-evaluation**
  - Step 1 : Collection of Published Information**
  - Step 2 : Systematization of Causes (5 Types)**
  - Step 3 : Identification of Causes (14 Types)**
  - Step 4 : Recurrence Prevention Measure Table**
  - Self-Evaluation of System Security Level**
- 4. Conclusion and Future Direction**

# Information-technology Promotion Agency, Japan (IPA)



Government Organisation under  
the Ministry of Economy, Trade and Industry (METI)  
Chairman : Mr. Koji Nishigaki

## Invigorating Japan through IT



## Organisation Structure

**IT Security Center (ISEC) <Security>**

**Software Engineering Center (SEC) <Reliability>**

**Open Software Center (OSC)**

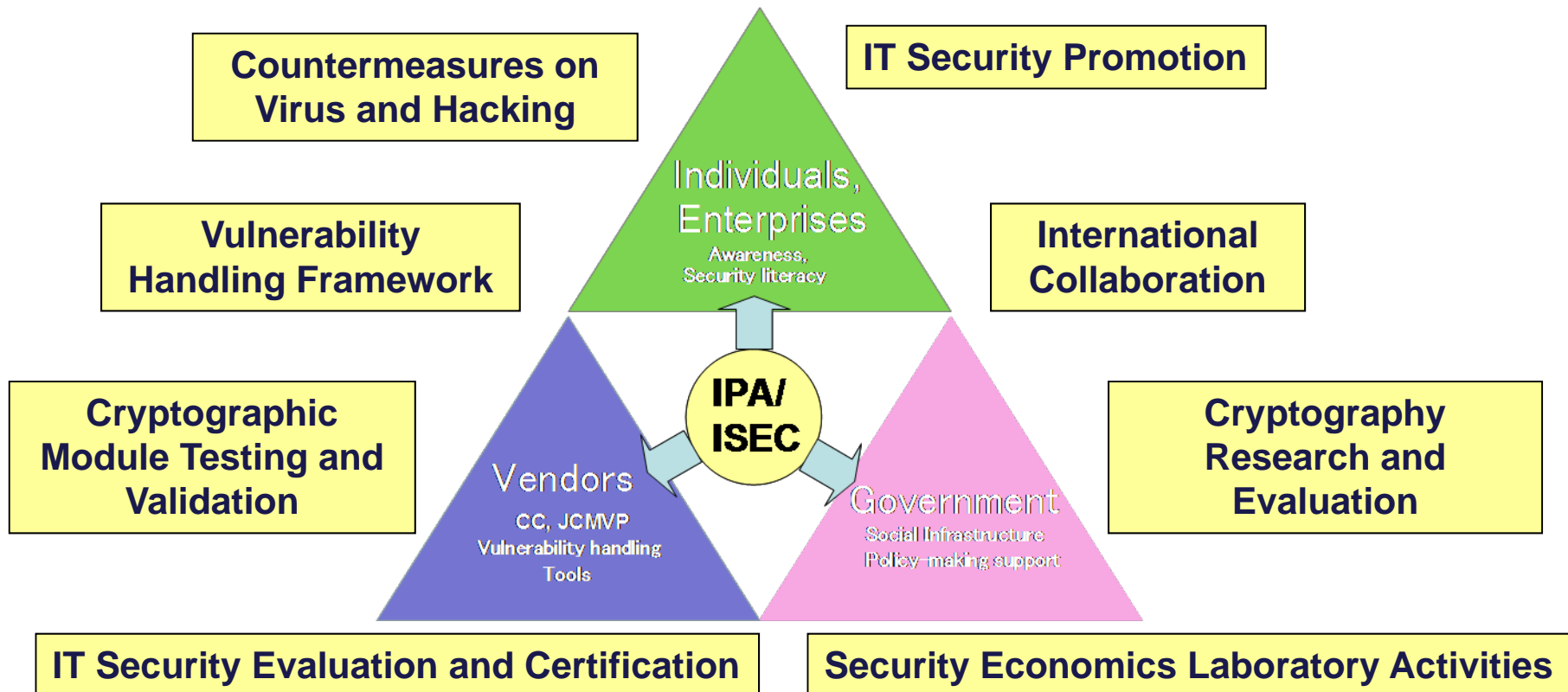
**IT Human Resources Development HQ**

**IT Skill Standards Center (ITSSC)**

**Japan IT Engineer Examination Center (JITEC)**

# Mission of IT Security Center (ISEC), IPA

The IT Security Center (ISEC) is the core and leading unit for promoting Japanese IT security countermeasures, including diffusing and enlightening security awareness to the Japanese citizens, providing alert information on latest security vulnerabilities and publishing security guidelines for enterprises and personal computer users.



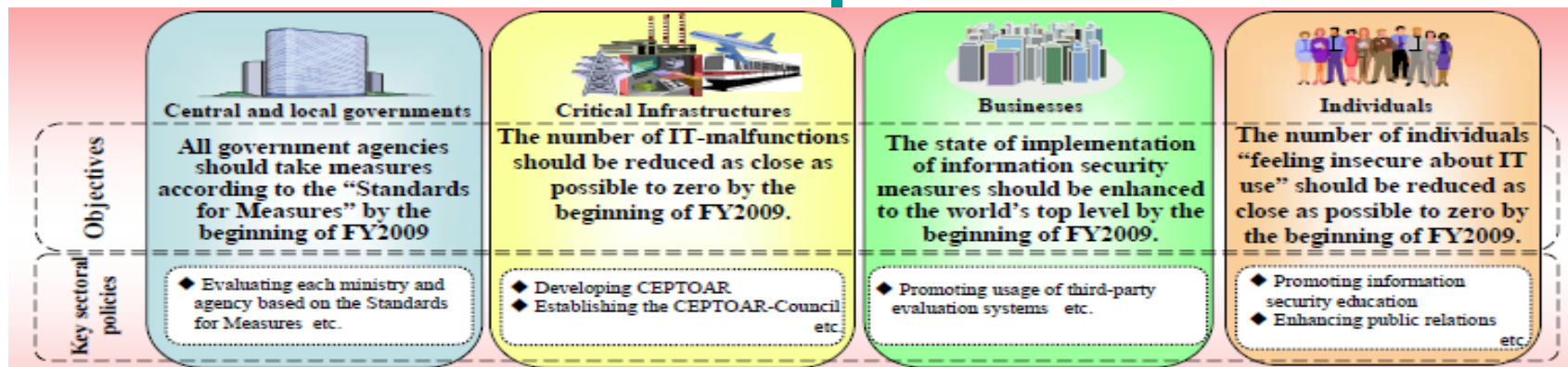
# National Strategy on Information Security and Critical Infrastructures in Japan



NISC has been established since April 25, 2005 in the Cabinet Secretariat.

**"The First National Strategy on Information Security"**  
 -Aiming to make Japan an Information Security Advanced Nation through Establishment of a New Public- Private Partnership Model –  
 - First Step toward a Trustworthy Society -

[http://www.nisc.go.jp/eng/pdf/overview\\_eng.pdf](http://www.nisc.go.jp/eng/pdf/overview_eng.pdf)



**10 sectors are identified:**  
 "Telecommunications", "Finance",  
 "Civil aviation", "Railways",  
 "Electricity", "Gas",  
 "Governmental/Administrative services (including local governments)",  
 "Medical services", "Water works" and "Logistics"

**"The Second National Strategy on Information Security"**  
 -Aiming for Strong "Individual" and "Society" in IT Age –  
 "Accident Assumed Society"

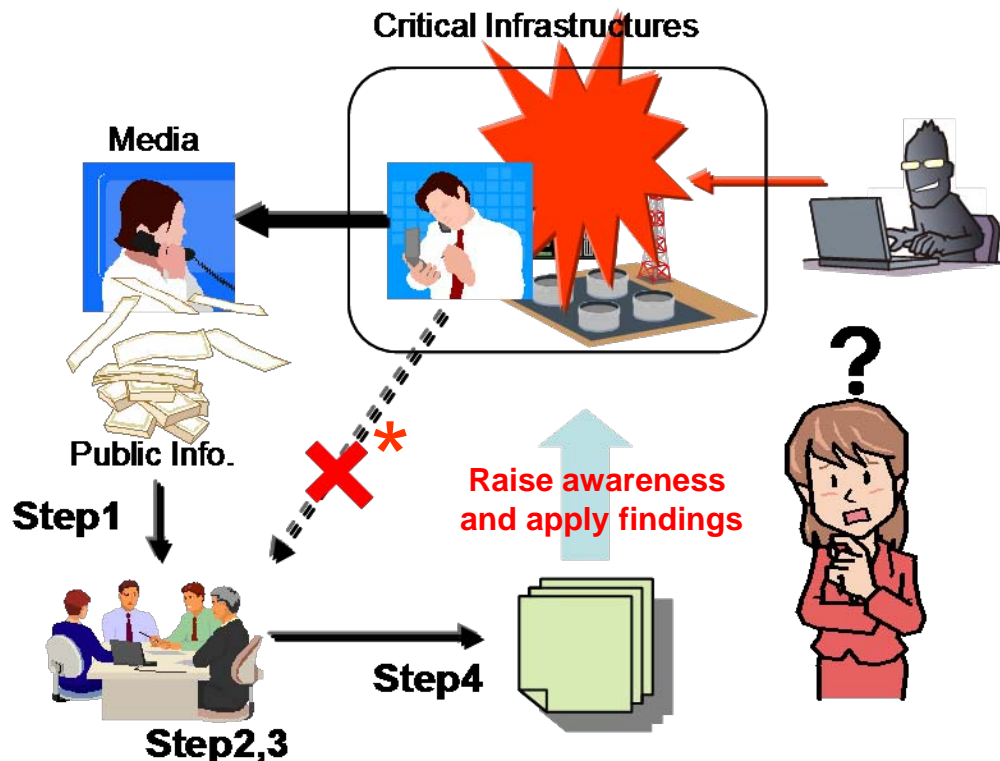
**Preparedness and enhancement of security measures against the incidents.**

# Development of Information Security-Focused Recurrence Prevention Measures Overview

4 step approach



Step1	Collection of Published Information
Step2	Systematization of Causes
Step3	Identification of Causes
Step4	Recurrence Prevention Measure Table



\* Critical infrastructure operators are reluctant to disclose information regarding their security breaches

# Step1



## Collection of Published Information

Analysis of Case Studies on Security Incidents in Critical Infrastructures

### Approach to Incident Information Gathering

two methods to collect information concerning security incidents experienced in critical infrastructures :

- to gather information through publications in the media
- to gather information directly from critical infrastructure operators

**Critical infrastructure operators are reluctant to disclose information regarding their security breaches**

#### From publications in mass media

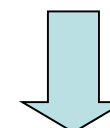
Time period : 2000 to 2008 in Japan  
( Foreign news : 2007 and 2008 )  
News sources : 21 domestic news sites  
17 foreign news sites

Step1



**58 Security Incident cases**

38 domestic incidents  
20 foreign incidents



Step2

e.g., Asahi.com (The Asahi Shimbun Company) <http://www.asahi.com/>,  
NIKKEI NET (Nikkei Inc. / Nikkei Digital Media, Inc.) <http://www.nikkei.co.jp/>,  
ITmedia (ITmedia, Inc.) <http://www.itmedia.co.jp/>

e.g., DHS Daily Open Source Infrastructure Report [http://www.dhs.gov/files/programs/editorial\\_0542.shtm](http://www.dhs.gov/files/programs/editorial_0542.shtm),  
Industrial Defender <http://www.industrialdefender.com/>,  
Cyber Security News [http://cicentre.com/news/cyber\\_security.html](http://cicentre.com/news/cyber_security.html)

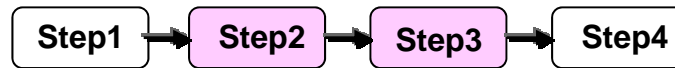


# Incident Information Items

**Table 1. Incident Information Items**

<b>No.</b>	Identification number of the information security incident case.
<b>Incident Case Title</b>	Incident case title including main security causes and the infrastructure operator.
<b>Date of Incident</b>	Occurrence date of the information security incident. In the case that the occurrence date is unknown/unavailable, the date the information security incident was discovered. In the case the discovery date is also unknown/unavailable, the date the information security incident was published
<b>Incident Summary</b>	The summary of the information security incident should be stated. <b>The attacker, victim party, attack method, and damage information should also be extracted and summarized concisely in several lines.</b>
<b>Main Causes</b>	The excerpt of published information word for word from an article should be avoided and the causes are categorized into several types.
<b>Impact Range</b>	The extent of damage generated by the occurrence of the information security incident. <b>Particularly, numerical recording is encouraged.</b> For example, in case of a data breach, the exact number of cases leaked should be recorded. In case of denial of service incident, the extent (number of services) and period of time services were suspended. In the case of monetary damage, the total sum of loss should be recorded.
<b>Recurrence Prevention Measure</b>	In accordance with the analysis summarized later, a recurrence prevention measure should be proposed, and the recurrence prevention measure ID should be recorded.
<b>Remarks</b>	Information worth noting, such as the manner in which the information security incident was discovered and the countermeasure(s) the critical infrastructure operator implemented should be recorded.
<b>Source</b>	The source of the security incident information.

# Step 2 and Step 3



# Systematization and Identification of Causes

Systematization (5) and Identification (14) of Causes (58)

## (1) Unauthorized Access

- a. Denial of Service (DoS) Attack by External Sources (6 cases)
- b. SQL Injection (3 cases)
- c. Unauthorized Access by External Sources (10 cases)
- d. Unauthorized Access by Former Personnel (3 cases)
- e. Unauthorized Access by Internal Personnel (2 cases)
- f. Unauthorized Access (5 cases)

## (2) Inappropriate Use of Winny (File sharing software used in Japan)

- a. Inappropriate Use of Winny (8 cases)

## (3) Issues in System Development

- a. Inadequate Design (5 cases)
- b. Inappropriate Server Configuration (2 cases)
- c. Insufficient System Independency (1 case)
- d. Network Route Compromise (1 case)

## (4) Human Error

- a. Error by Internal Personnel (4 cases)
- b. Error by Contracted Personnel (1 case)

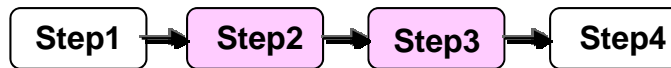
## (5) Phishing

- a. Phishing (4 cases)

There were 4 cases with unknown causes, and 1 case that included 2 causes.



Incident  
Analysis  
Table



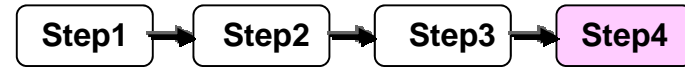
# Incident Analysis Table Excerpt : Case #52

**Table 2. Incident Analysis Table Excerpt : Case #52**

<b>No.</b>	52
<b>Incident Case Title</b>	Unauthorized Access and Website Falsification of an JOGMEC 's Public Server
<b>Date of Incident</b>	27 July 2008
<b>Incident Summary</b>	Japan Oil, Gas and Metals National Corporation (JOGMEC) server was compromised by SQL injection. Viewers may have contracted a virus. The computers that accessed the falsified website were automatically redirected to a server (storage site of malicious programs) set up by the attacker and malicious programs may have been downloaded forcefully.
<b>Main Causes</b>	SQL Injection
<b>Impact Range</b>	JOGMEC as well as viewers/users of the website may have contracted a virus.
<b>Recurrence Prevention Measure</b>	L3-P1, L2-D1, L2-D3, L2-D4, L3-O1, L3-M1
<b>Remarks</b>	Critical Infrastructure Sector: Governmental/Administrative services (including local governments)
<b>Source</b>	<a href="http://www.asahi.com/national/update/1020/TKY200810200153.html">http://www.asahi.com/national/update/1020/TKY200810200153.html</a> <a href="http://www.jogmec.go.jp/news/release/docs/2008/pressrelease_080918.pdf">http://www.jogmec.go.jp/news/release/docs/2008/pressrelease_080918.pdf</a>

# Step 4 Recurrence Prevention Measure Table

## Lifecycle and Security Level



The following two points were taken into consideration :

### \* The Lifecycle of Information Systems

“Planning”, “Development”, “Operation”, or “Maintenance” phase

Information security measures are necessary at each phase of the lifecycle. Even if information systems are securely guarded at one point, they will inevitably become unsecure at a later point in time if neglected.

### \* Security Level

The degree of information security fulfillment is labeled as a “security level”.

Table 3. Assumed Systems and Their Required Security Levels (based on system criticality)

Assumed System (Category)	Required Security Level
Backbone Information Systems in Critical Infrastructure	LV4
Backbone Information Systems in Business	LV3
Systems with Minimal Social Effect	LV2
Office and Local Systems	LV1

The necessity of security measures differs depending on the purpose of each system.

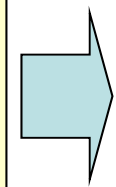
# Result :



## Recurrence Prevention Measure Table

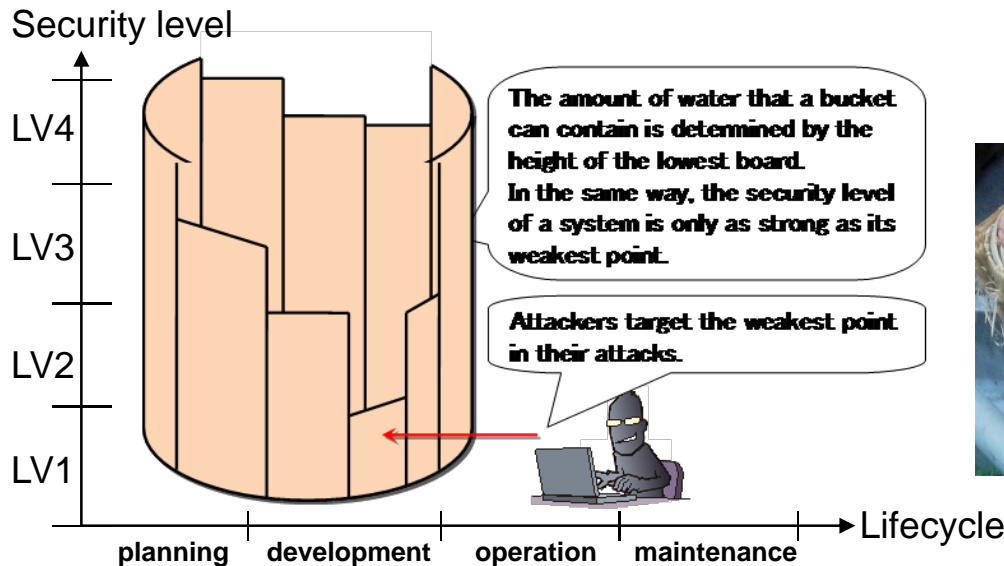
### Recurrence Prevention Measure Table

In this analysis, each individual recurrence prevention measure was analyzed and categorized into four security levels and also positioned at the appropriate phase of the lifecycle.



LV4	Planning		
	Development		
	Operation		
	Maintenance		
LV3	Planning		
	Development		
	Operation		
	Maintenance		
LV2	Planning		
	Development		
	Operation		
	Maintenance		
LV1	Planning		
	Development		
	Operation		

**Weakest Link Principal :Rule of Bucket (Oke or Taru) in Japan**  
 If one's security level is said at a certain level, that means the certain recurrence prevention measures must be continually fulfilled.



### Rule of Bucket Oke or Taru

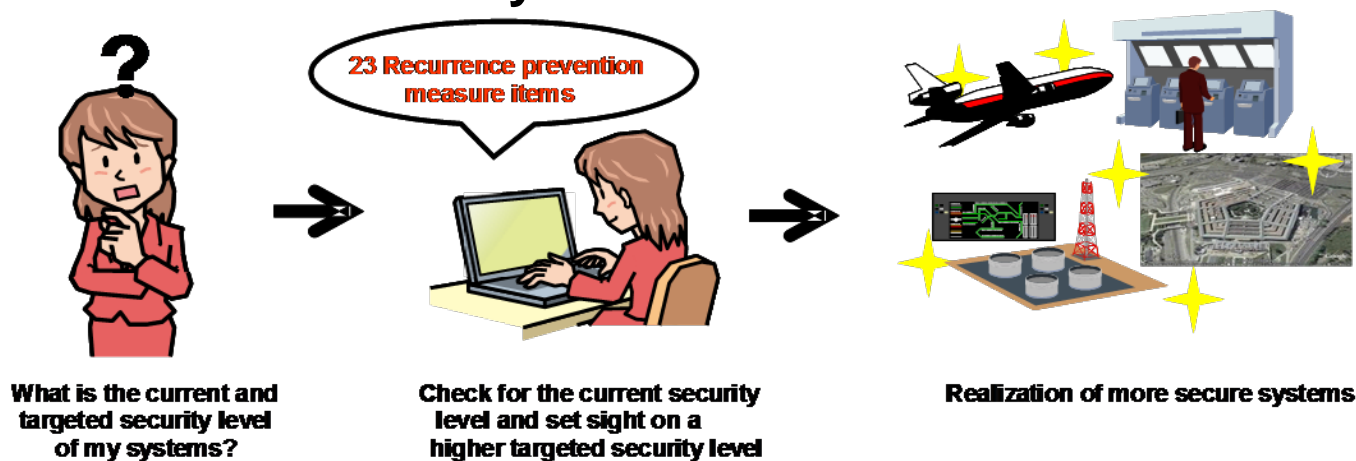


23 check items

The safety offered by the information security measures is only as good as its weakest point.

# Self-Evaluation of System Security Level

## Evaluation Method of Security Level



### Identify the targeted security level

Table 3. Assumed Systems and Their Required Security Levels (based on system criticality)

Assumed System (Category)	Required Security Level
Backbone Information Systems in Critical Infrastructure	LV4
Backbone Information Systems in Business	LV3
Systems with Minimal Social Effect	LV2
Office and Local Systems	LV1

Table 5. System Security Level Achievement Requirements

System Security Level (Category)	Criteria to Achieve Level
LV4 Backbone Information Systems in Critical Infrastructure	All measures for LV4, LV3, LV2, and LV1 have a C3 or C4 fulfillment status.
LV3 Backbone Information Systems in Business	All measures for LV3, LV2, and LV1 have a C3 or C4 fulfillment status.
LV2 System with Minimal Social Effect	All measures for LV2 and LV1 have a C3 or C4 fulfillment status.
LV1 Office and Local Systems	All measures for LV1 have a C3 or C4 fulfillment status.

### Judge the current fulfillment status

Table 4. Category of Implementation Condition for Security Measures

C4:	The implemented measures are practically complete now and in the foreseeable future.
C3:	All of the measures currently necessary are implemented.
C2:	Some measures are implemented and others are not.
C1:	The measure is not implemented, or it is unclear whether it is implemented

Targeted security level : LV3 & LV4

satisfactory level : C3 & C4

# Conclusion and Future Direction

This result from our study may be utilized as guideline toward the recurrence prevention measures for mitigation of ICT incidents.



However, with the sophistication of attacking methods and advancement of information technology, it is necessary for countermeasures to constantly evolve as well, and so as our recurrence prevention measures against new threats.

From this point of view, the ways to share and analyze more detailed security incident information instead of just published reports, and develop up-to-date countermeasures based on those detailed information would be studied and improved in the future.

Thank You !

# IT Security Center Information-technology Promotion Agency, Japan

<http://www.ipa.go.jp/index-e.html>

2-28-8 Honkomagome  
Bunkyo, Tokyo 113-6591, Japan  
Tel: +81-3-5878-7501  
Fax: +81-3-5978-7510



Kagami Biraki: literal translation is "mirror opening ceremony."  
In this ceremony, mirror represents **happiness and peacefulness** and opening means **infinite extension of possibility**.

