ICSJWG International Partners Day

UPDATE OF ICS SECURITY POLICIES OF JAPAN

Akio Sato
Deputy Director
Commerce and Information Policy Bureau
Office of IT Security Policy
Ministry of Economy, Trade and Industry

Kazutaka Matsuzaki, Ph.D
Researcher
Control System Security
Center (CSSC)

Table of Contents

- Information Sharing Partnership (J-CSIP)
- Plan for ICS-CERT in Japan
- Cyber Security Exercises in Japan - Power plant, Gas, and Building Automation
- Control System Security Center (CSSC)

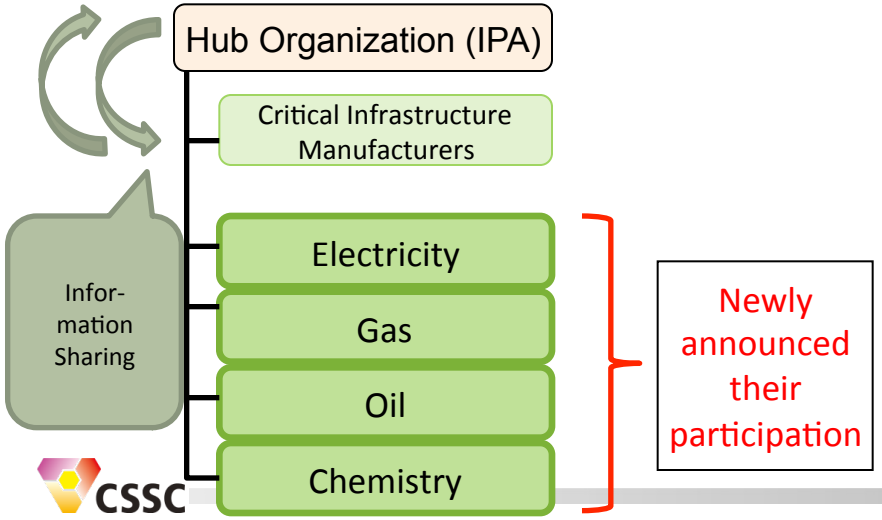
Information Sharing Partnership (J-CSIP)

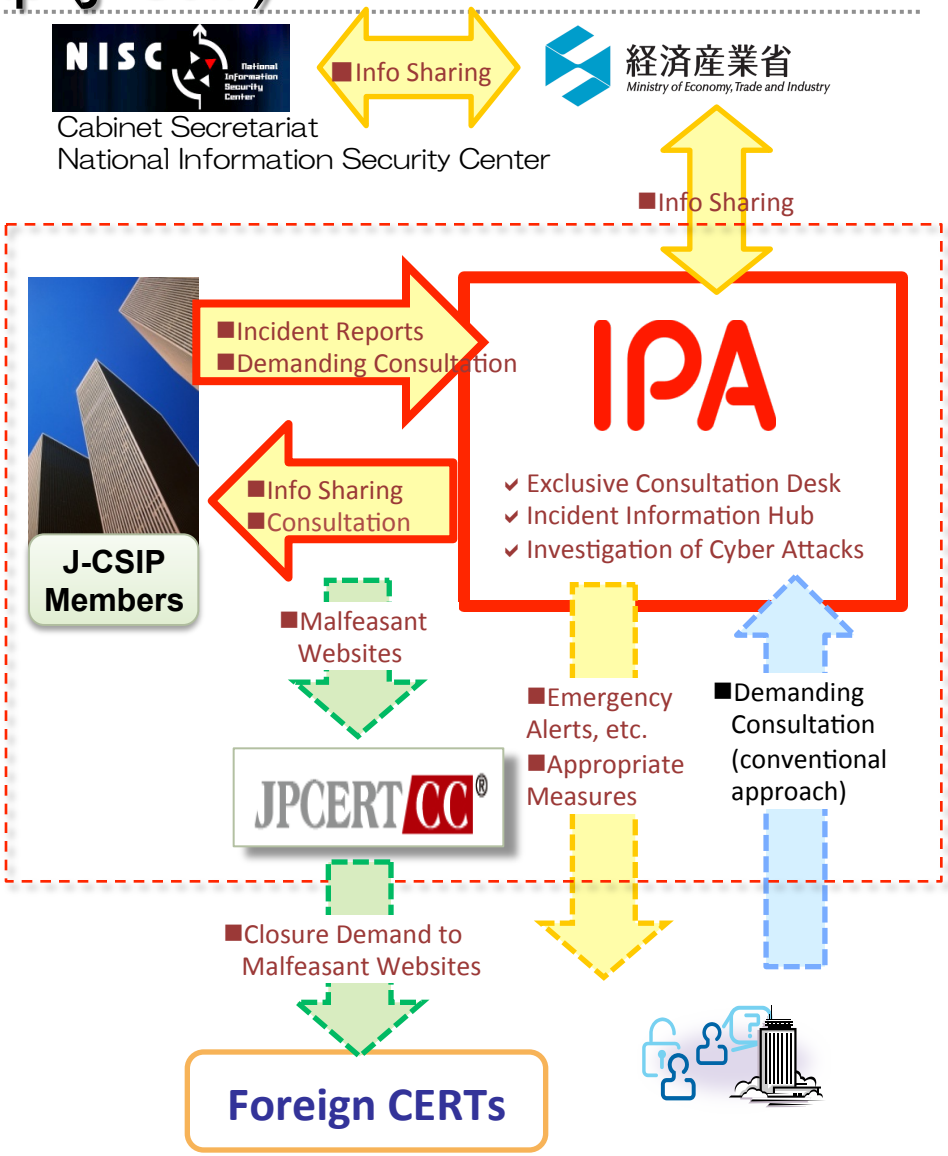
1. Information Sharing Partnership (J-CSIP)

Establishment of Information Sharing Partnership(J-CSIP)

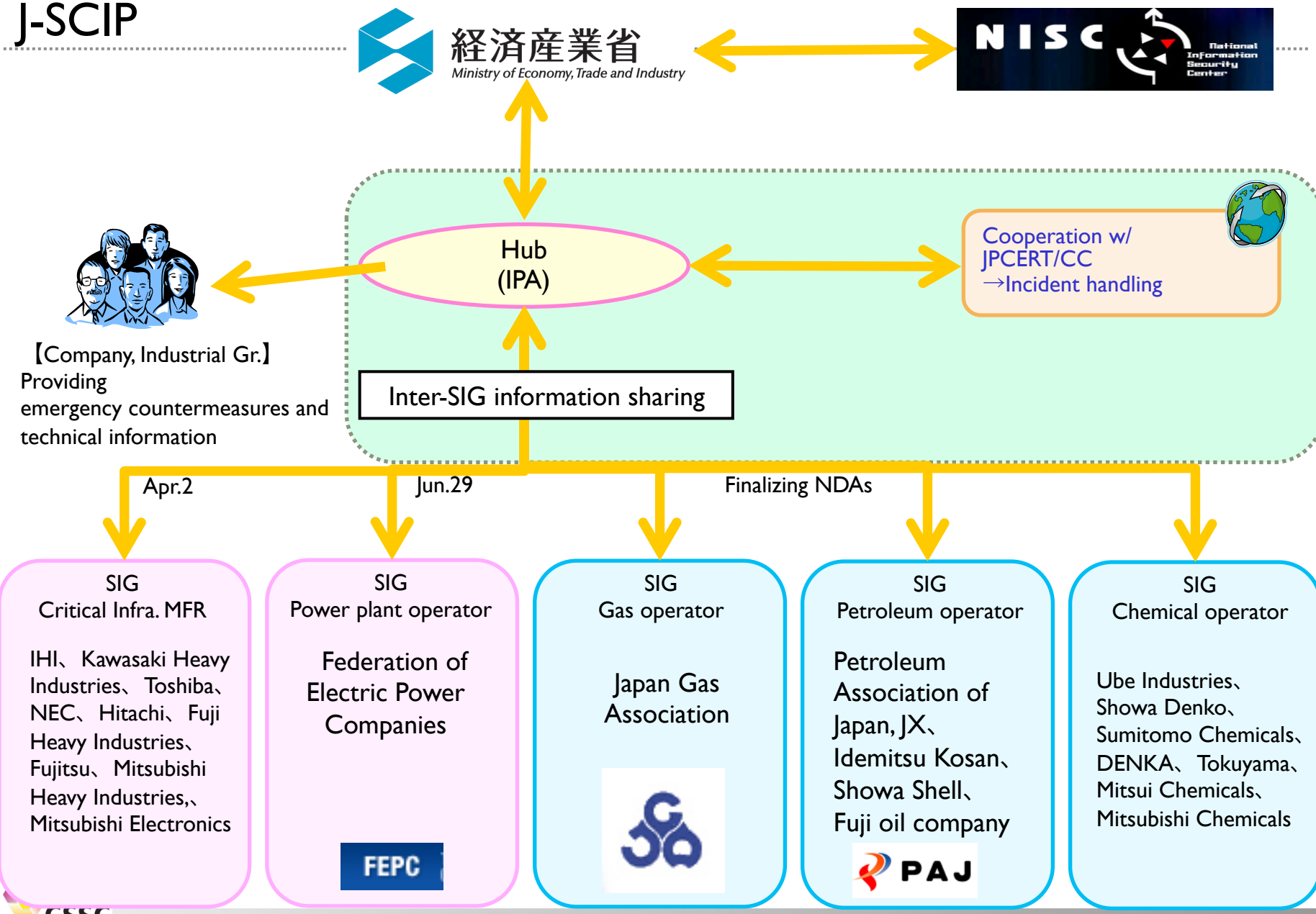
- ■J-CSIP was establish in 2011 as a partnership platform among manufacturers to prevent the spread of damage caused by cyber attacks.
- ■J-CSIP shares each member's measures for information security including the measures against actual cyber attacks.
- ■J-CSIP agreed Information sharing rules in FY 2011 and is now expanding the member groups (Total 5 Groups and 25 Members).

*J-CSIP : Initiative for Cyber Security Information sharing Partnership of Japan





J-SCIP

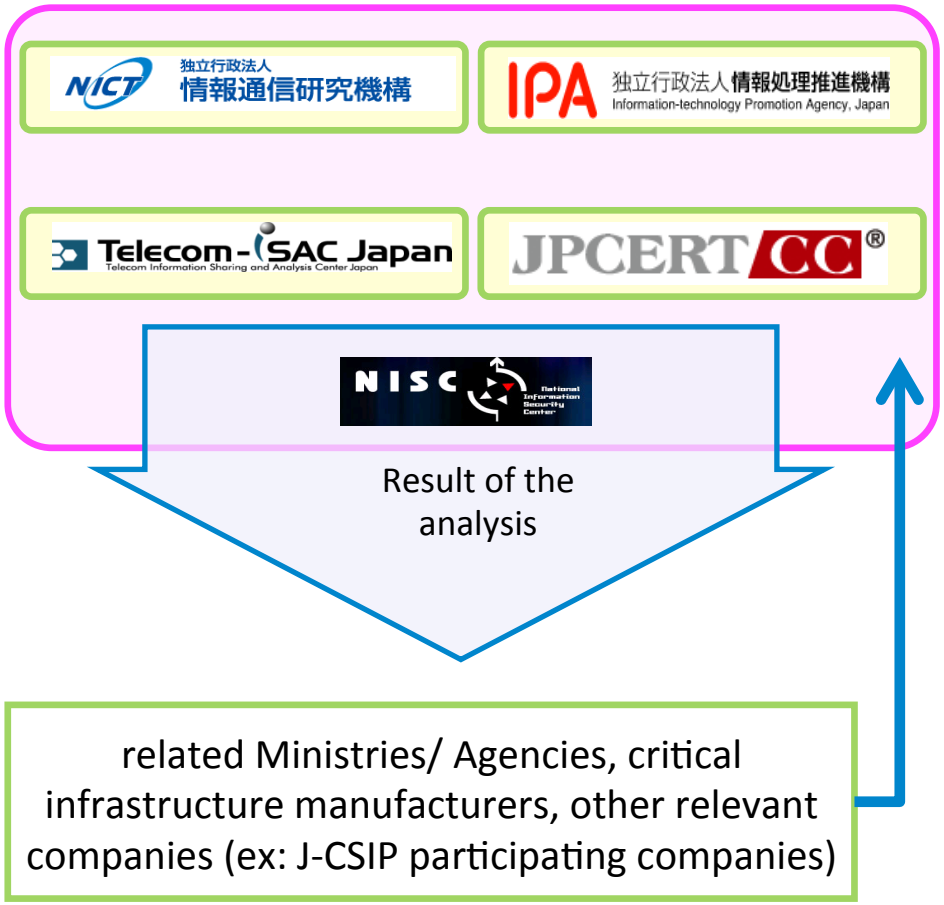

経済産業省
Ministry of Economy, Trade and Industry
NISC
National Information Security Center
Hub
(IPA)
Cooperation w/
JPCERT/CC
→Incident handling
【Company, Industrial Gr.】
Providing
emergency countermeasures and
technical information
Inter-SIG information sharing
Apr.2
Jun.29
Finalizing NDAs
SIG
Critical Infra. MFR
IHI、Kawasaki Heavy Industries、Toshiba、NEC、Hitachi、Fuji Heavy Industries、Fujitsu、Mitsubishi Heavy Industries,、Mitsubishi Electronics
SIG
Power plant operator
Federation of Electric Power Companies
FEPC
SIG
Gas operator
Japan Gas Association
SIG
Petroleum operator
Petroleum Association of Japan, JX、Idemitsu Kosan、Showa Shell、Fuji oil company
PAJ
SIG
Chemical operator
Ube Industries、Showa Denko、Sumitomo Chemicals、DENKA、Tokuyama、Mitsui Chemicals、Mitsubishi Chemicals

Council for Advanced Analysis of Cyber Attacks

Strengthen Advanced Analysis Function against Cyber Attacks

- To deal with the sophisticated and complex cyber attack recent years, the council for advanced analysis of cyber attacks was established in July, 2012.
- Based on the information held by each member, the council conducts necessary advanced analysis for protection against cyber attacks.
- Result of the analysis will be provided to related Ministries/ Agencies and critical infrastructure manufacturers through NISC in order to contribute to develop countermeasures against cyber attacks.

Council for Advanced Analysis of Cyber Attacks



Countermeasures against targeted cyber attacks

■ Providing wide defense by J-CSIP

We will consider expanding the network that can receive the impacts of information sharing large enough to maintain a relationship of trust. At the same time, we will extend the techniques of attacks that we share based on the actual state of targeted attacks and increase the impact of information sharing. We will also examine the way that countermeasures are taken.

■ Coordination between J-CSIP and the Council for Advanced Analysis of Cyber Attacks

Working together with the Council of Advanced Analysis of Cyber Attacks, we will make the use of their information related to cyber attack defense as a feedback.

■ Consolidation and advanced analyses of cyber attack information

The working group consisting of related organizations under the Council for Advanced Analysis of Cyber will deliberate on and sort out the requirements for collected information, provided information and sources of information and report the results to the Council by the end of this fiscal year.
(The first council was held on July 12, 2012 and the first working group was held on July 31, 2012.)

■ Collection of malware and unauthorized access information

We will continue asking IPAs for cooperation to provide information of malware and unauthorized access and make the use of the collected information to protect from cyber attacks.

Plan for ICS-CERT in Japan

Information security early warning partnership
Vulnerability information handling framework in Japan

2003 | 2004 | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 | 2011 | 2012

▲ **Jul 7, 2004: Information Security Early Warning Partnership**

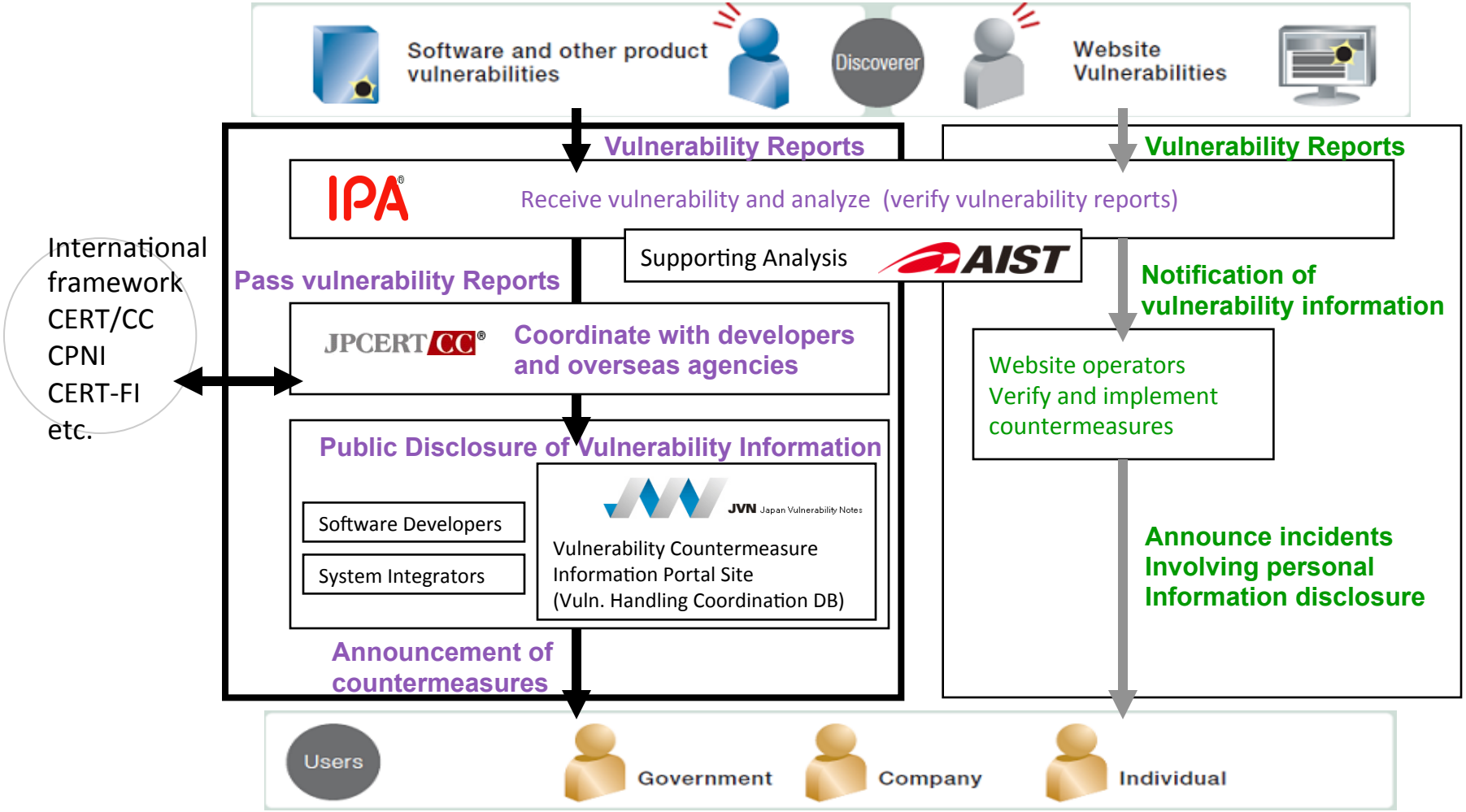
▲ **Jul 8, 2004: Portal Site, JVN started (Vuln. handling coordination DB)**

▲ **Apr 2007: Portal Site, JVN iPedia (Vuln. archiving DB)**

- Information Security Early Warning Partnership
  A public-private partnership framework pursuant to the METI (Ministry of Economy, Trade and Industry) Directive #235, 2004, has been established to promote software product and web site security and prevent the damage to spread to the vast range of computers due to computer viruses or unauthorized access.

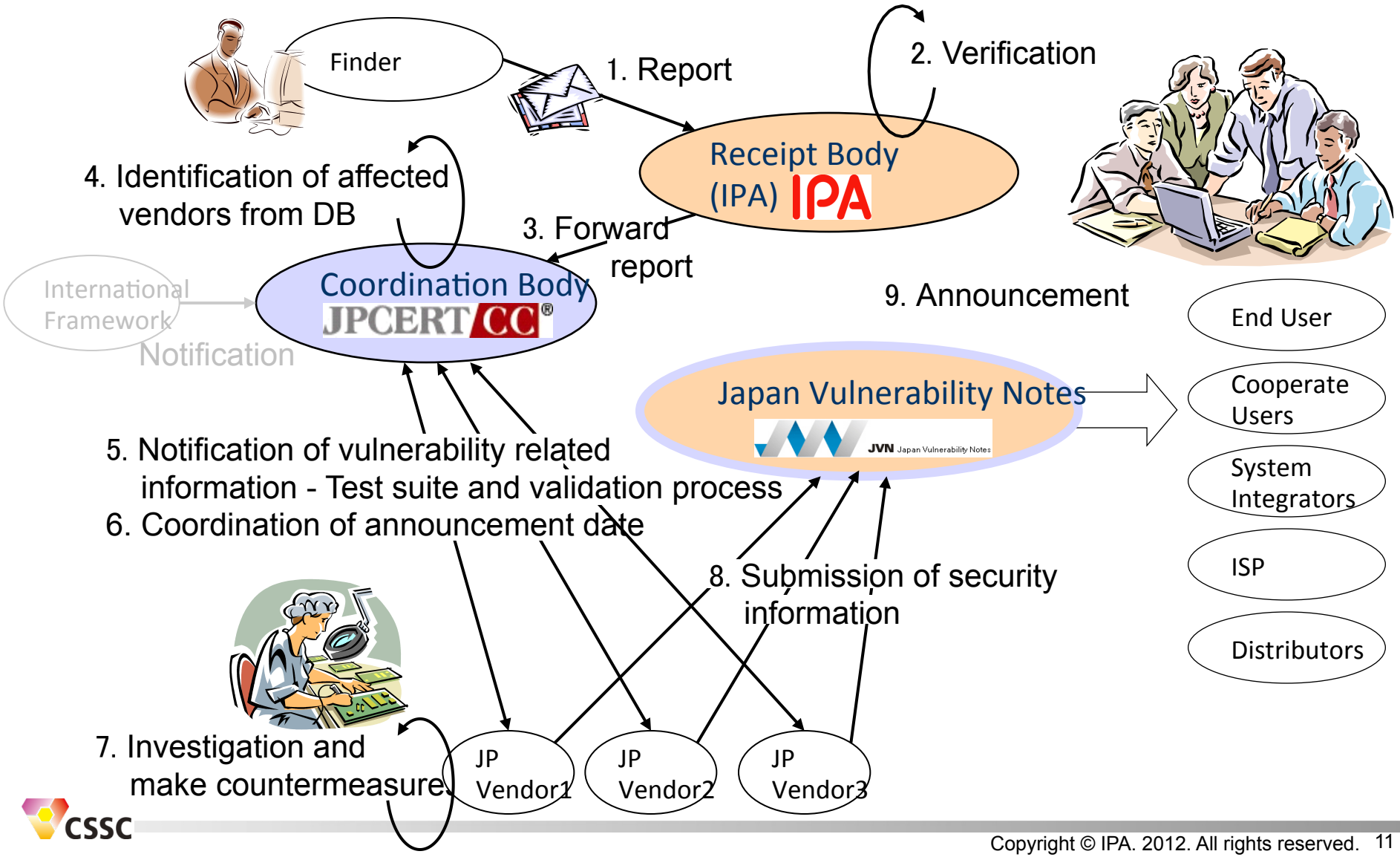
Copyright © IPA. 2012. All rights reserved.

Information security early warning partnership
Vulnerability information handling framework in Japan



Copyright © IPA. 2012. All rights reserved.

Information security early warning partnership
Vulnerability information handling framework in Japan

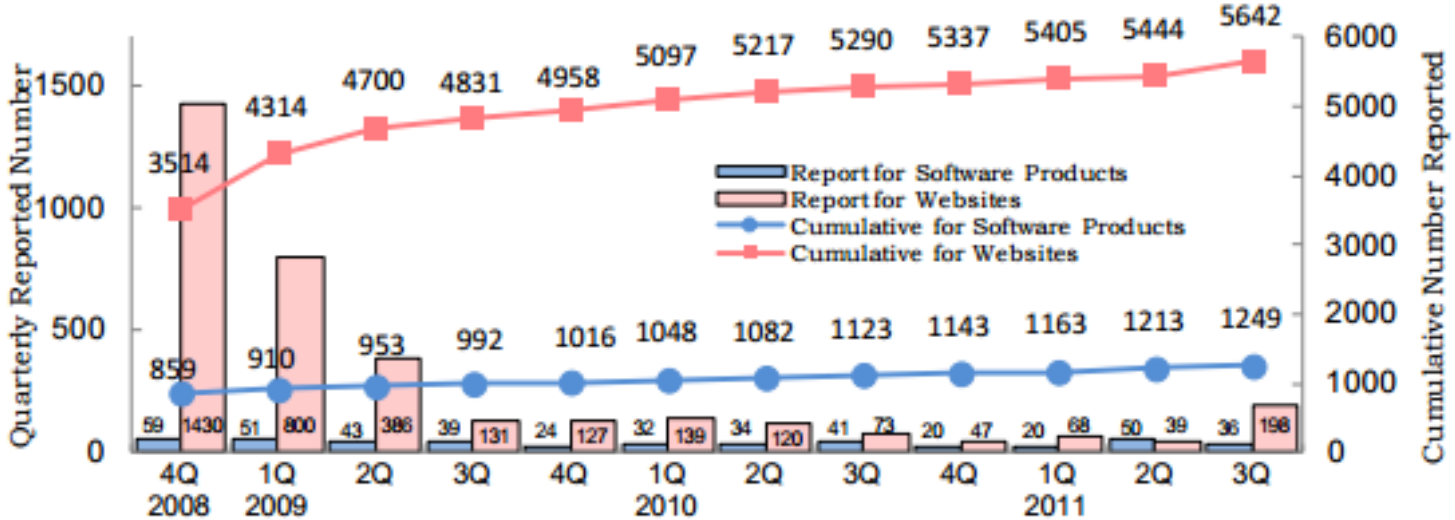


Copyright © IPA. 2012. All rights reserved.

Information security early warning partnership
Vulnerability information handling framework in Japan

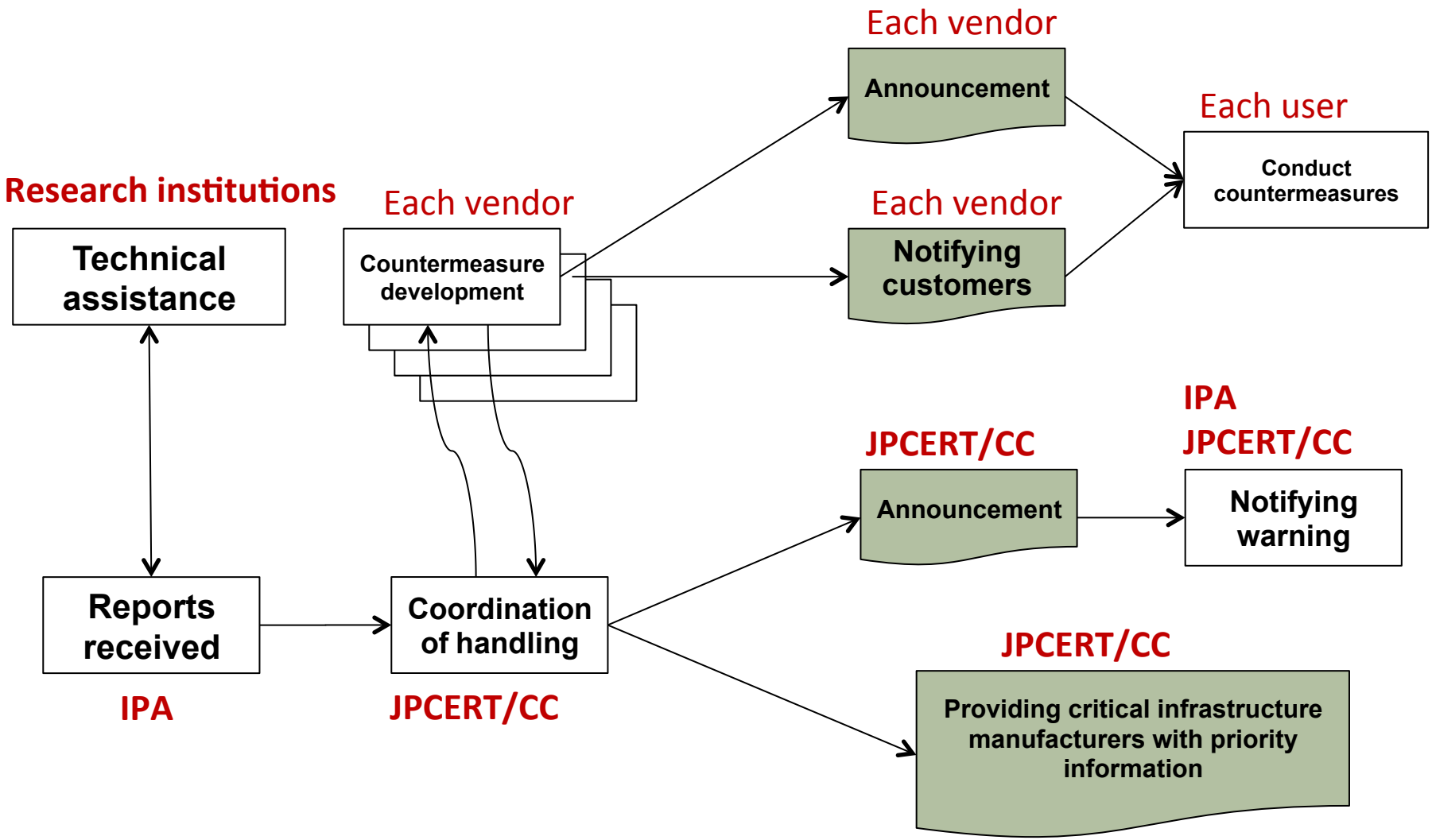
- The total number of vulnerability-related information reported to IPA from July 1 to September 30, 2011 was 234: 36 of them were about Software products and the rest of 198 were about Websites.
- The cumulative number of reports made to IPA since the framework started (July 8, 2004) was 6891: 1249 of them were about Software products and the rest of 5642 were about Websites.

Reported Number/Business Day								
3Q/2009	4Q/2009	1Q/2010	2Q/2010	3Q/2010	4Q/2010	1Q/2011	2Q/2011	3Q/2011
4.56	4.47	4.40	4.32	4.22	4.10	4.00	3.92	3.91



Copyright © IPA. 2012. All rights reserved.

Operations Related to Vulnerability Information Handling



Future outline

Issues

In order not to be affected by oversea actions:
- Set the policies for product venders to respond to vulnerabilities.
- Strengthen the ability for domestic product vendors to handle
- To establish a relationship to negotiate equally with overseas agencies

Applying rules of handling vulnerability information at control systems to the society rationally.

Points

The way that control system product vendors handle vulnerabilities

Alignment with existing related systems

Outputs

Model guidelines related to vulnerability information handling for ICS vendors

Revised proposals of existing related systems

<< Creating an industrial consensus>>

The way that control system product vendors handle vuln.

- Basic guidelines of vulnerability handling
  - Product vendors develop countermeasures (patch and workaround measures) and notify customers.
  - Product vendors develop internal systems and procedures for quick responses.
- Internal systems and procedures
  - Information counters from the outside
  - Coordination among internal authorizations and related departments
  - Procedures: Receipt→Investigation→Countermeasure development→Notification
- How to notify
  - Make sure to notify all customers necessary
  - Make a judgment based on the merits of announcements and practicality of countermeasures
- Conduct countermeasures in the field
  - Explanation of vulnerability risks to customers
  - Alignment with maintenance operations

Alignment with existing related systems

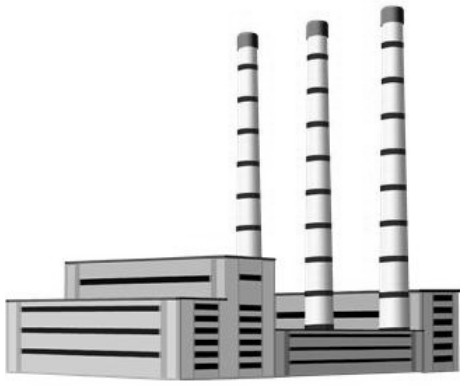
- Whether to handle control system vulnerabilities in pursuant to "the Standards for Handling Software Vulnerability Information and Others" (Directive 235, METI, 2004).
- The issues that could arise in that case.

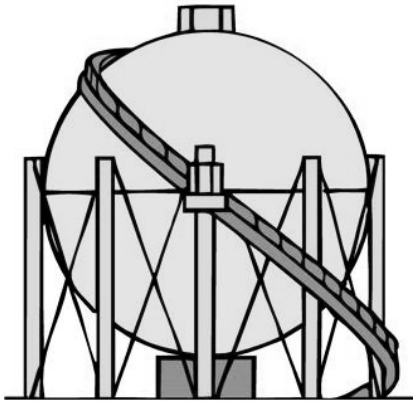
● (Whether the issues could be solved by the revisions of announcements and partnership guidelines.)

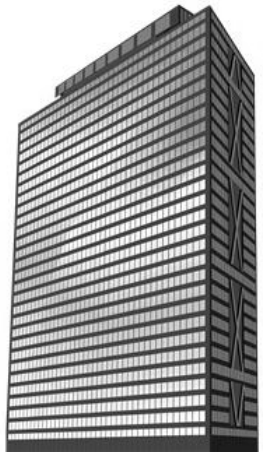
Cyber Security Exercises in Japan
- Power plant, Gas, and Building Automation

Cyber security exercises

- Cyber security exercises (table-top exercise and functional exercise) in 3 sectors of power plant, gas and building automation
- Timing: Jan-Mar, 2013
- Budget size: $ 5.1M (FY2012)
- Major targets: Field staff, technical staff, vendors etc. in 3 sectors



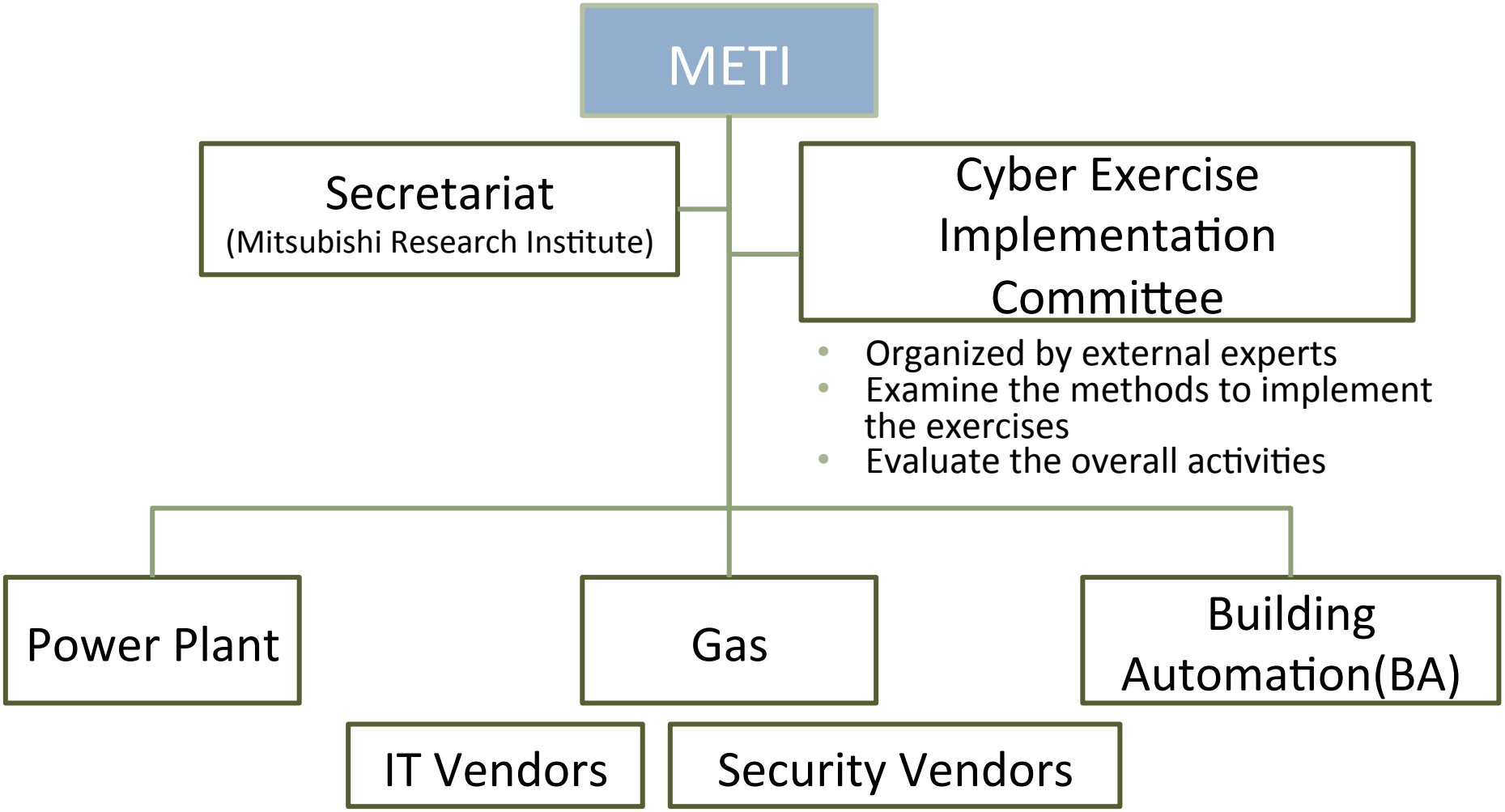




Objectives of the exercises

- In order for field staff, technical staff and vendors and such in the power plant, gas and building automation sectors to identify the threats against their control system security.
- To examine validity of procedures to detect and to respond to the security incidents.
- To examine continued operations of voluntary exercises by the participants.

Implementation structure



Implementation process

1) Clarify objectives and outputs of the exercises

2) Create implementation scenarios

3) Building simulated systems

4) Examine the methods to implement the exercises

5) Implementation of the exercises (table-top exercise / functional exercise)

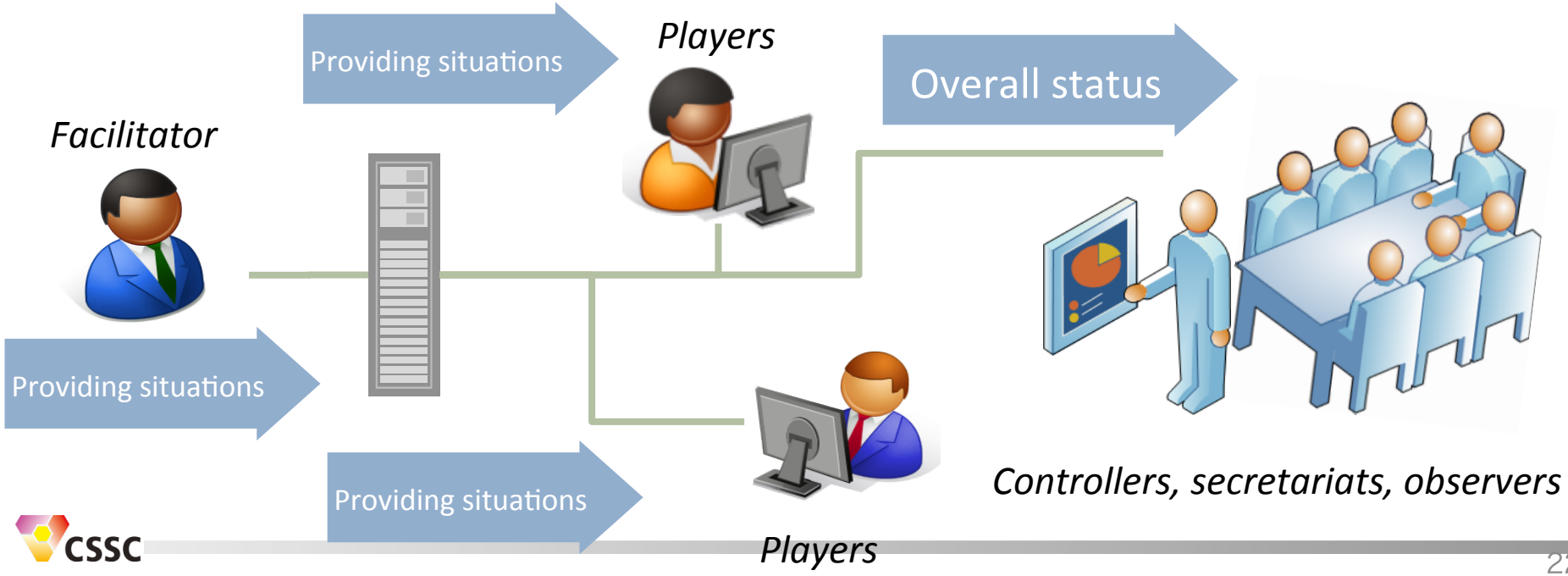
6) Evaluate the exercises

Building simulated systems

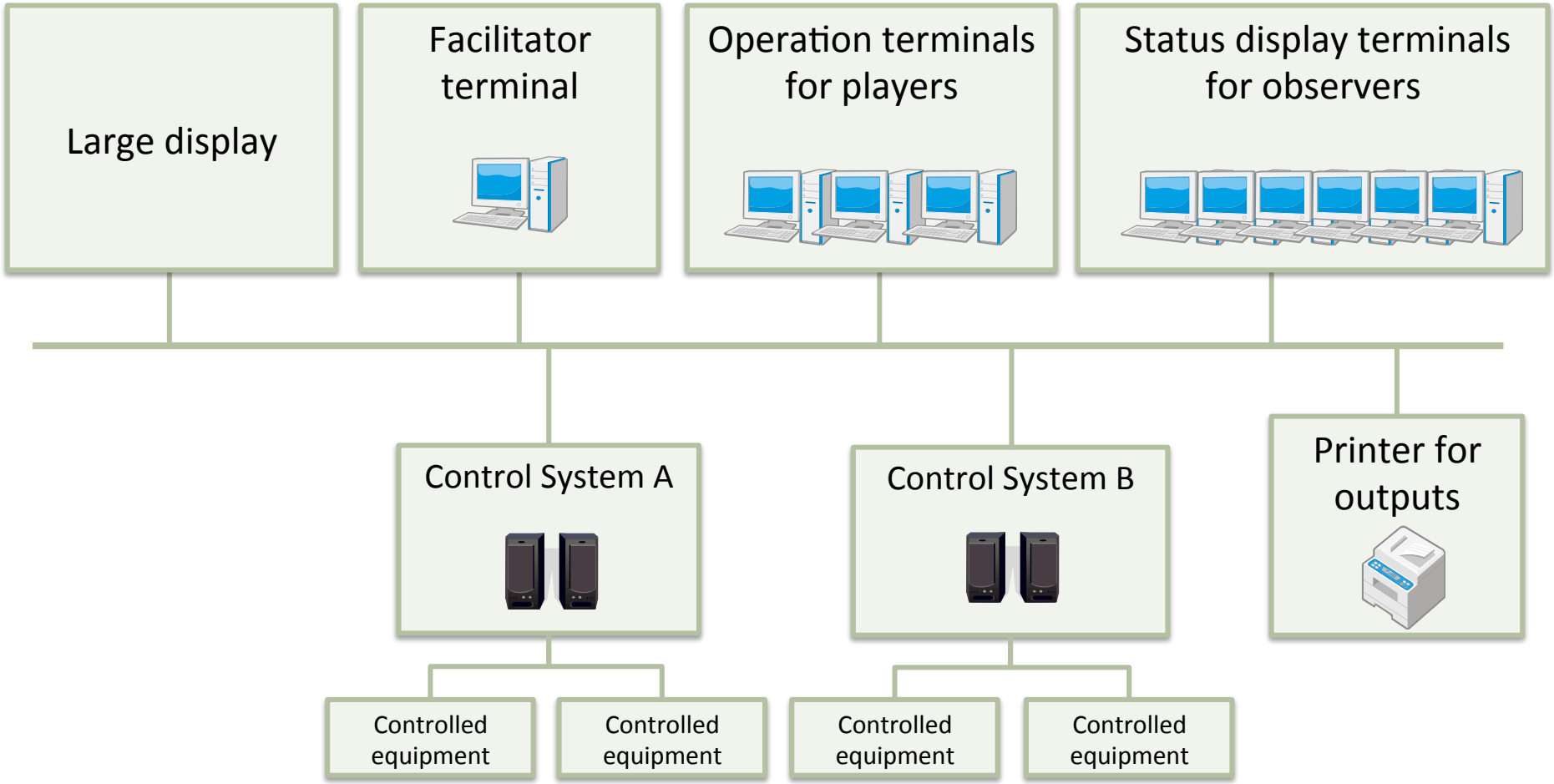
Functions equipped with the simulated systems

- Prior creation of cyber attack scenarios
- Implementation of scenario selection by facilitators
- Providing the situations of each scenario by facilitators
- Sharing the status with other players
- Providing the graphical presentation of the overall status
- Recording of scenario progress and player's operations

etc.



Examples of structures of simulated systems



Power plant: outline of exercises

Targeted systems	Control systems of thermal power plants
Exercise participants **(Main players are highlighted in red)**	• **Electric power suppliers (technical staff of control systems at power plants or trainers of these control systems)** • Industry groups • Research institutes • Vendors • Secretariat
Objectives of the exercises	In order for those who are involved with control systems of power plants to identify the reality of threats against control systems by latest malware including Stuxnet.
Simulated threats	Infection of malware including Stuxnet to control systems of power plants

Power plant：Points of exercises

- To provide exercise participants with the opportunity to experience the damages of cyber attacks.
  - ✓ To present that cyber attacks can create situations which affect security of thermal power plants depending on the targets and methods of attacks.

- To build simulated systems as real as actual ones in order to provide exercise participants with real experience
  - ✓ Instead of creating systems that are easy to be attacked, build simulated systems with the same security measures as the real ones.

- Follow-ups of table-top exercises at functional exercises
  - ✓ To give a step-by-step explanation along with the scenarios
  - ✓ To create a moment for exercise participants to examine how to detect and prevent the attacks and to mitigate damages etc.

Gas：outline of exercises

Targeted systems	Manufacturing or supply systems of gas
Exercise participants **(Main players are highlighted in red)**	• Industry organizations • **Gas suppliers (technical staff of manufacturing or supply systems of gas)** • Vendors • Security specialists • Secretariat
Objectives of the exercises	• In order for the main players of the exercises to identify the reality of latest threats like Stuxnet against control systems . • In order for the main players of the exercises to learn technical and operational measures against threats.
Simulated threats	Infection of malware, such as Stuxnet, to gas manufacturing and supply systems.

Gas： Points of exercises

- To create the simulated system structures and scenarios after investigating the characteristics and threats unique to the gas control systems through interviews with suppliers.
- To simulate the latest cyber security attacks
- Major reasons for successful attacks in exercise scenarios：
  - Vulnerabilities of versatile software
  - Functions and setups remaining on computer systems without purposes (no operational needs)
  - Operators' own flow of data, which is not built nor recommended by vendors.

BA： outline of exercises

Targeted systems	BA (Building Automation) systems - Simulating air conditioning and electricity systems etc.
Exercise participants **(Main players are highlighted in red)**	• **Building Developers** • Building tenants • Vendors • Simulated attackers • Secretariat
Objectives of the exercises	To identify potential vulnerabilities and risks of BA systems and to conduct (technical and operational) measures at proper levels after assessing their impacts.
Simulated threats	Internal and external attacks against BA systems of buildings

BA：points of exercises

- Table-top exercises:
- To identify vulnerabilities of control systems (BA systems) of buildings by exercise participants and security experts.
- To examine reasonable measures combining both technical and operational countermeasures
- Functional exercises：
- To replicate the real human attacks in cooperation with simulated attackers
- To simulate both internal (such as vendors) and external (via internet) attacks
- For exercise participants to monitor the state of attacks on a real-time basis
- To check if we can detect attacks with current countermeasures. If not, explore the area for improvements.

Application of outcomes

- As for the location of installation after the next fiscal year, simulated systems will be set up at the cyber security test bed of Control System Security Center (CSSC) in Tagajo City.
- The main players of the exercises in each sector are expected to make the best use of the documents of manuals and procedures of the cyber exercises.
- While we will create the exercise scenarios which will reflect the situations of suppliers in each sector, we will pay attentions to its versatility and scalability so that the scenarios will be used widely for continued usage.

Control System Security Center (CSSC)

Control System Security Center (CSSC)

- Overview
  - Chair
    - Dr. Seiichi Shin (Professor, The University of Electro-Communications)
  - Association members (Oct. 2012)
    - Advanced Industrial Science and Technology(AIST), Azbil, Toshiba, Hitachi, Mitsubishi Heavy Industries, Mitsubishi Research Institute, Mori Building, Yokogawa Electric Corporation, Information-technology Promotion Agency (IPA), Fuji Electric, NRI Secure, Toyota IT center, Omron, Mitsubishi Electric
  - Location
    - Miyagi Recovery Park, Tagajyo City, Miyagi Prefecture (Testbed)
    - Odaiba waterfront, Tokyo (Main office)
  - Established in March, 2012

Control System Security Center (CSSC)

- **Testbed**
  - Miyagi Recovery Park, formerly operated as SONY's factory before the earthquake
  - 8 simulated plants are under development
    - Plant automation systems (Azbil, Yokogawa)
    - Factory automation (Fuji Electric)
    - Building automation (Mitsubishi Heavy Industries, Mori)
    - Electrical substation (Toshiba)
    - Electrical generating plant (Hitachi)
    - Gas automation(Azbil)
- Office operation
  - FT/PT 10 people from the member companies

- **Task Committees**
  - R&D and Testbed
  - Evaluation/Certification and Standardization
  - Public Awareness and HRD

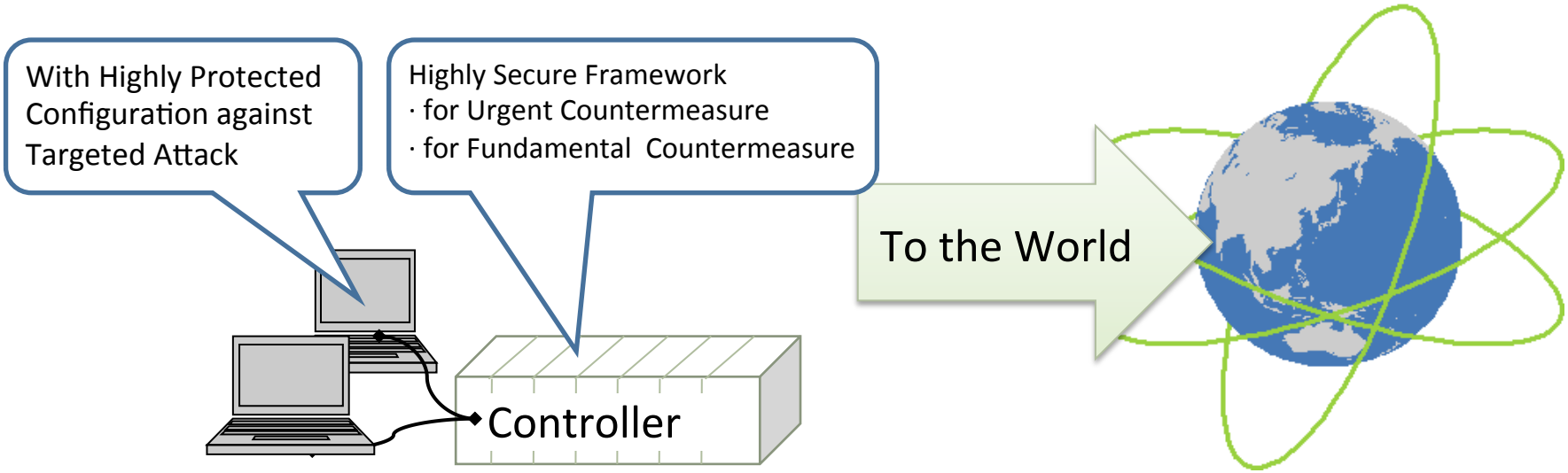
Testbed based inTagajo

Tokyo Odaiba Waterfront Office

© 2012 Mapabc.com
Data SIO, NOAA, U.S. Navy, NGA, GEBCO
© 2012 ZENRIN
Google earth

R&D / Testbed Task Committee

- Objectives
  - Promote R&D related to control system security through discussions about how R&D and testbed should be in CSSC.
- Topics
  - Direction of R&D
  - Design, develop, and manage the testbed
  - R&D progress review



Security Training w/ Simulated Plants

- We will use simulated plants for R&D, situational awareness, and HRD

- We are collaborating with JCIA - Japan Chemical Industry Association
  - Requirements for simulated plants
  - Use-case scenario review
  - Examples:
    - The testbed should make managers think like: "In order to protect plants from cyber-security threat, we need these investments…"
    - The testbed should be future-oriented: smart-phone, iPad, wireless should be deployed.
    - Scenarios such as malware preventing from properly interlock or causing unintended halt of pumps should have impact for testbed users.

SHOWA DENKO

SUMITOMO CHEMICAL

Mitsui Chemicals

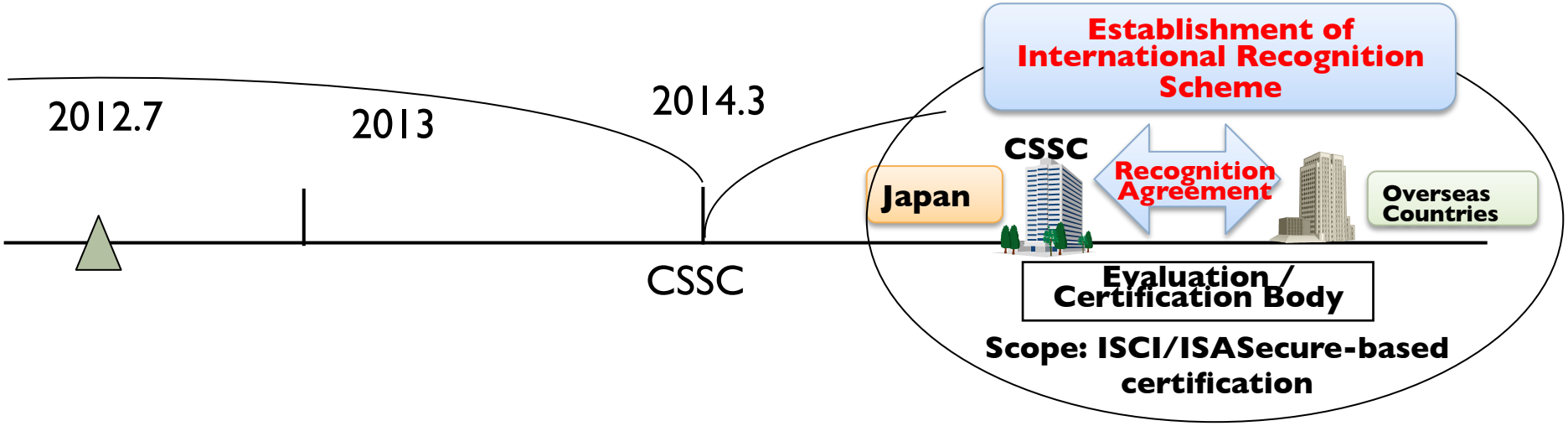
MITSUBISHI CHEMICAL

Evaluation/Certification and Standardization Task Committee

- Objectives
  - Develop strategies and policies for CSSC such as authentication with existing international standard and standardizing related to control system security
  - Shorten the time to acquire international certificates based on the evaluation criteria by third parties
  - Establish an international recognition scheme for ICS security evaluation and certification, promoting standardization, and contributing to the enhancement of ICS security at the global level
- Topics
  - Direction for authentication and standardization as CSSC
  - Effective use of test bed for certification and standardization.
  - Issues for authentication and standardization in control system security

Evaluation/Certification&Standardization Committee

●Schedule for Committee Activities



<Domestic Evaluation and Certification Trial> <International Recognition Scheme><Utilization of Research Outcome>

Trial operation of a domestic evaluation and certification scheme using criteria equivalent to that used by ISCI/ ISASecure certification

Establishment of an international recognition scheme for an ISCI/ ISASecure-based certification

Utilization of the outcome of CSSC research

Evaluation/Certification&Standardization Committee Activities

●Standardization

Standardization Activities for IEC62443 (Industrial Network and System Security Standards)	
For Devices (IEC62443-4) **For Systems (IEC62443-3)** **For Operation Management（IEC62443-2）**	
＜Past and Current Activities＞ - Submitted over 50 comments on the drafts(IEC62443-3-3) - Translate the international standards into Japanese and publish, and promote the use of the standards	**＜Planned Activities＞** - Propose the standardization of the outcome (new technologies) of CSSC research - Develop future specifications for evaluation and certification, and test facilities in the future

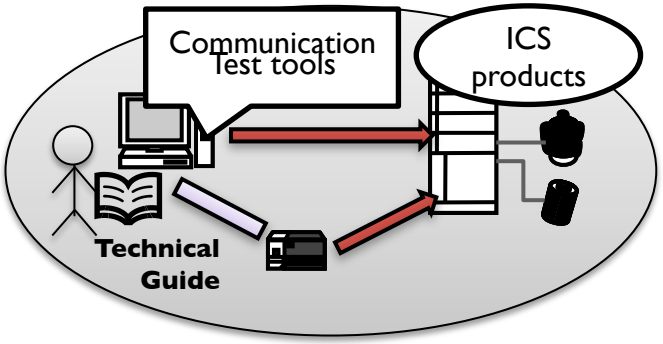
ISCI : ISASecure Compliance Institute; ISMS: Information Security Management System; IACS-SMS: IACS Security Management System

Evaluation/Certification&Standardization Committee Activities

- Evaluation and Certification

Support for ICS* Security certification scheme to promote global ICS business

Trial Evaluation of Communication Robustness with Fuzzing



Prior to establishing certification schemes, we're setting up a trial evaluation environment

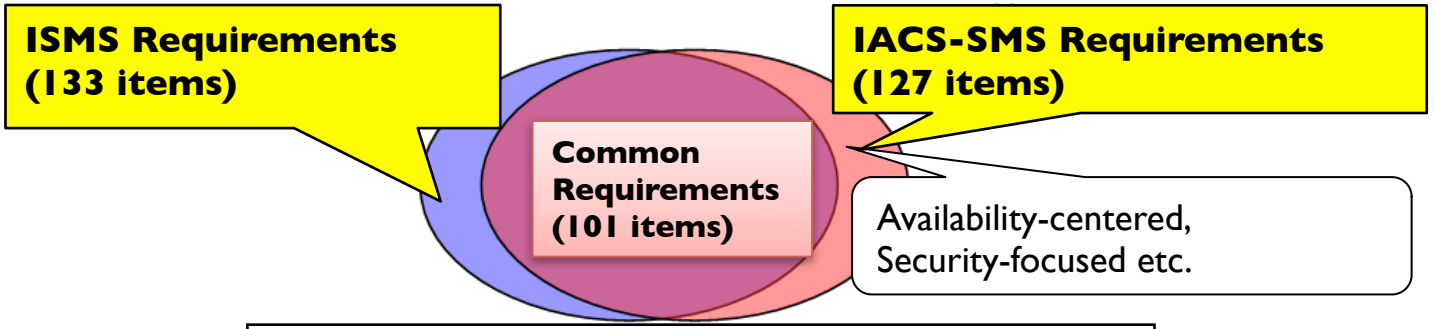
Establish an evaluation and certification scheme based on standardized criteria

Evaluation/Certification&Standardization Committee Activities

- Evaluation and Certification

Enhancing security of Domestic Critical Infrastructures

Considering Introduction of the IACS-SMS Conformity Assessment Scheme

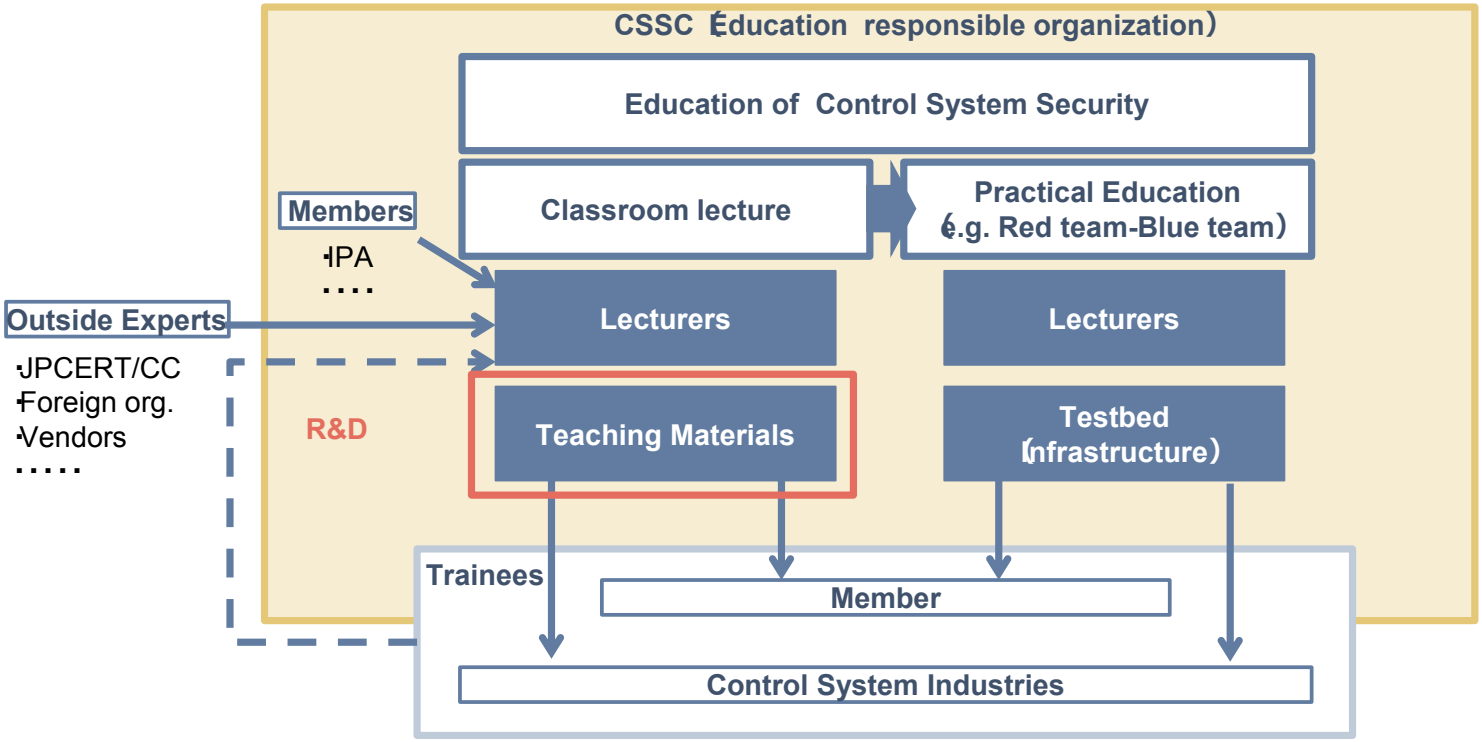


・IACS-SMS(IEC62443-2-1) for control systems, which is equivalent to ISMS for information systems, has been developed
・Consider whether introduction of an ISMS-like conformance assessment scheme can improve the security level of domestic control systems.

Establish a **IACS-SMS** evaluation and certification scheme

Public Awareness / HRD Task Committee

- Objectives
  - Promote R&D for pubic awareness and the desirable situation for HRD in CSSC.
- Topics
  - Direction for public awareness and HRD for control system security
  - Effective use of testbed for public awareness and HRD



Overview of training programs

- Multiple training programs are available depending on the targets and objectives of promotion and human resource development.
- The human resource development business offers a full training, while the training for the general public and executives will be an excerpted version of the full training.

Full training

Objectives	A. The General Public	B. The Executives	C. User Companies
Methods	Open to the public (Free of charge)	Observation (Free of charge)	Educational training (fee charging)
Location	Tagajo/Odaiba	Tagajo	Tagajo
Target	The general public, the media	The executives, the media	Mainly the executives of user companies
Duration	Half day	Half day	One and a half day – two days (A large-scale version will be held once-twice a year.)
Frequency	Two-three times a year	Upon request on an ad hoc basis	One a month (The timing will be considered further.)
Communication	HP, via members	HP, via members, individual invitations	HP, via members
Instructors	CSSC, external instructors	Mainly CSSC	CSSC, external instructors
Contents	Introduction of CSSC Trends of latest threats Simulated plant demonstration	CSSC facility visit Introduction of human resource development	Training using simulated plants Discussion by participants

Future plan

- Our testbed will open in Mar. 2013

	2012	2013	2014	2015	2016	2017
System security verification	R&D					
Establishment of structures and technology to enhance security	R&D					
Security international standard	Preparation		International standardization operations			
International standard compliance certification	Preparation		Evaluation certification operations			
Incident support	Preparation	Incident handling operations				
Human resource development	Preparation	Human resource development operations				
Promotion	Preparation	Publicity operations				
Testbed construction	Construction					