Vulnerability in Control System Handling and Disclosure Policy

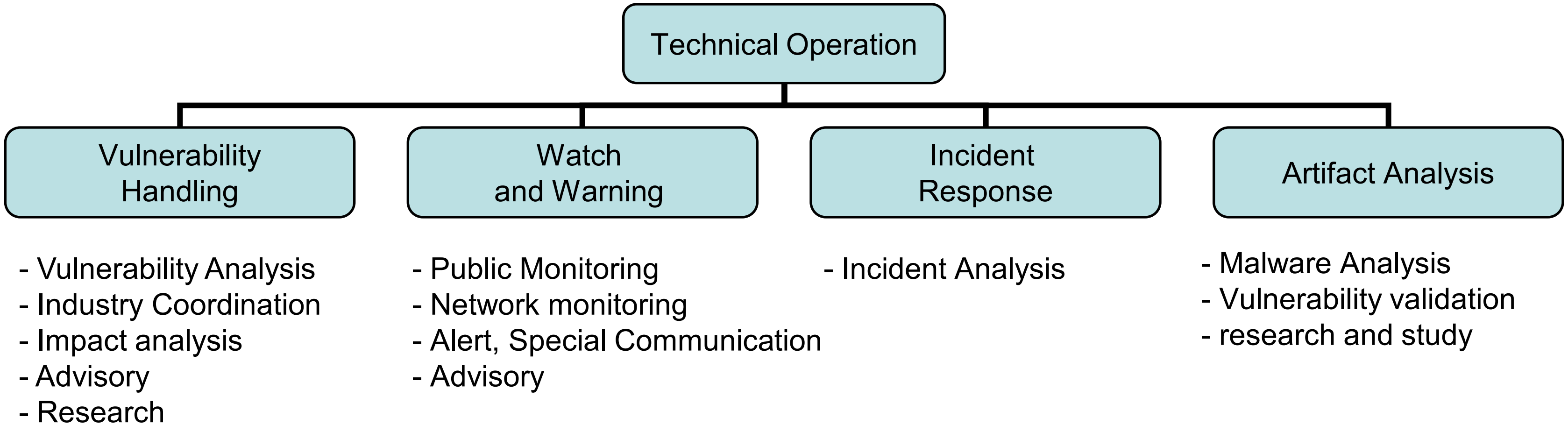
Yurie Ito
Director, Technical Operation
JPCERT/CC

JPCERT/CC is an independent non-profit organization, acting as a national point of contact for the other CSIRTs in Japan. Since its establishment in 1992, the center has been gathering computer incident and vulnerability information, issuing security alerts and advisories, and providing incident responses as well as education and training to raise awareness of security issues.

2008/08/26

JPCERT/CC introduction

- Fully budgeted by METI (Ministry of Economy, Trade and Industry)
- Non-governmental, Not for Profit Organization
- National POC CSIRT in Japan (Point of Contact for International relations)
- FIRST (Forum of Incident Response and Security Team) Full member (since 1998)
- APCERT (Asia Pacific Computer Emergency Response Teams) SC member, Secretariat



Technical Operation

Vulnerability Handling

- Vulnerability Analysis
- Industry Coordination
- Impact analysis
- Advisory
- Research

Watch and Warning

- Public Monitoring
- Network monitoring
- Alert, Special Communication
- Advisory

Incident Response

- Incident Analysis

Artifact Analysis

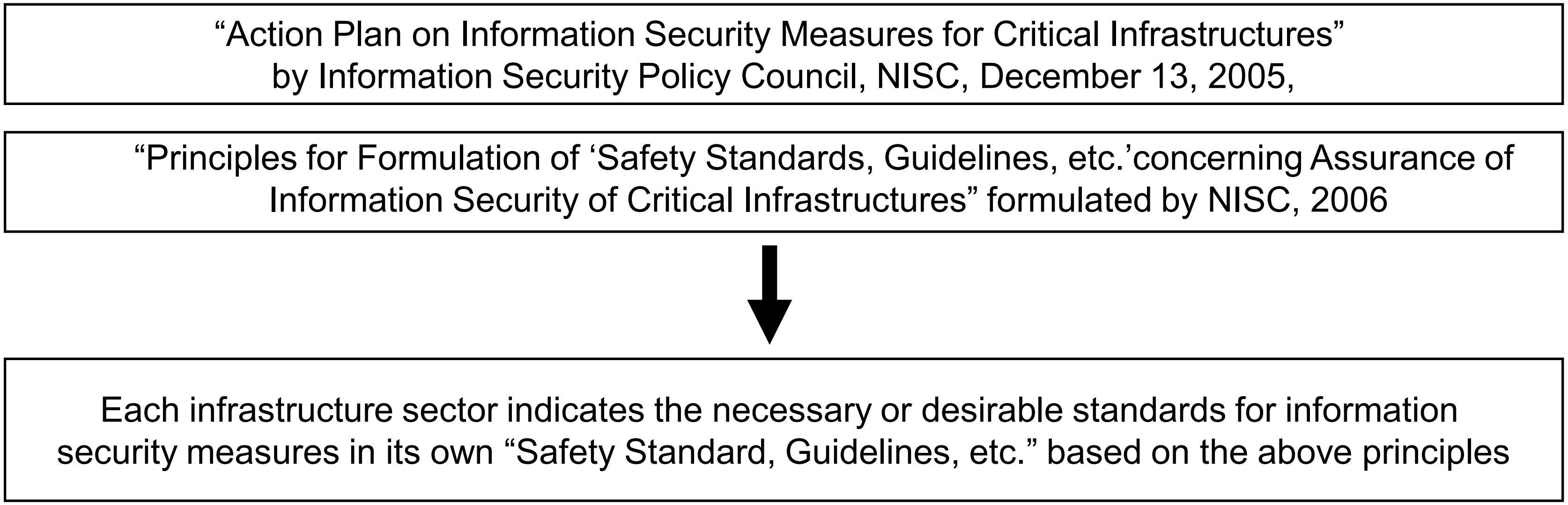
- Malware Analysis
- Vulnerability validation
- research and study

Vulnerability Handling/disclosure Standard and Guidelines in Japan

Vulnerability Handling and Disclosure Guidelines

- Ministerial announcement by METI “**Standard of the Vulnerability handling and disclosure**”, July 7, 2004
  - JPCERT/CC is designated as a coordination center in this document
- Industry guideline – JPCERT/CC, JEITA, JNSA, JISA, CSAJ, IPA jointly published guideline

General information security measures for Critical Infrastructures



“Action Plan on Information Security Measures for Critical Infrastructures”
by Information Security Policy Council, NISC, December 13, 2005,

“Principles for Formulation of ‘Safety Standards, Guidelines, etc.’concerning Assurance of Information Security of Critical Infrastructures” formulated by NISC, 2006

Each infrastructure sector indicates the necessary or desirable standards for information security measures in its own “Safety Standard, Guidelines, etc.” based on the above principles

Handling and Disclosure policy

- Vulnerabilities in general purpose software must be disclosed
  - Attackers will discover them and disclose them in ways that promote compromise
  - Administrators must be motivated to apply patches

- Vendor coordination, then <u>if needed</u> advise critical infrastructure sites in advance with vendors understanding (Not all compromises are created equal)
  - Securely, Discreetly, Under NDA where appropriate

- Disclosure guideline
  - Respect Information source's disclosure guideline

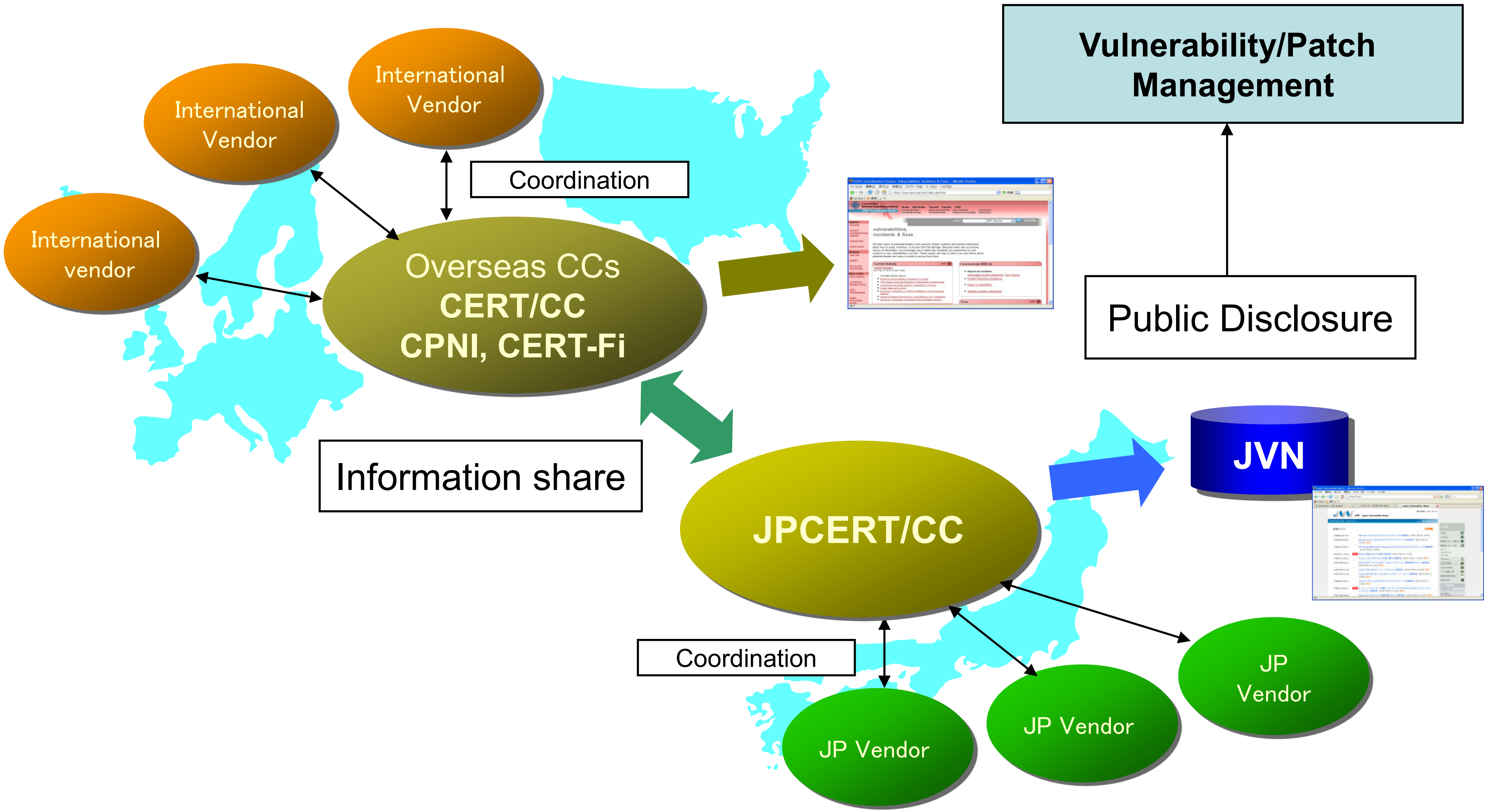
- In case vendor holds all the system users information, and be able to notify them directly, could be no public disclosure

- Information about Vulnerability to disclose at JVN (http://jvn.jp)
  - Advisory always with remediation
  - No full disclosure – no POC, no detail reproduction/validation process in the advisory
  - Vendors Status and announcement

JPCERT/CC's POC Registered Vendors Group

- 200+ vendors registered the point of contact for vulnerability handling to "JPCERT/CC's vendor POC group database" with technology keywords and signed agreement.
  - including Control system vendors
- Now developing separate information sharing task force among CS vendors and researchers
  - Advising group for CS protocol vulnerabilities handling
  - Annual Event

International partnership and framework



International Vendor

International Vendor

International vendor

Coordination

Overseas CCs
CERT/CC
CPNI, CERT-Fi

Vulnerability/Patch Management

Public Disclosure

Information share

JVN

JPCERT/CC

Coordination

JP Vendor

JP Vendor

JP Vendor

Contact

- Monitoring and Control System Protocol, SCADA Security
  - Email： scada@jpcert.or.jp
- General inquire
  - Email： office@jpcert.or.jp
  - http://www.jpcert.or.jp/
- Incident Report
  - Email： info@jpcert.or.jp