Information-Sharing System for Vulnerability Information Dissemination in Large-Scale Organization

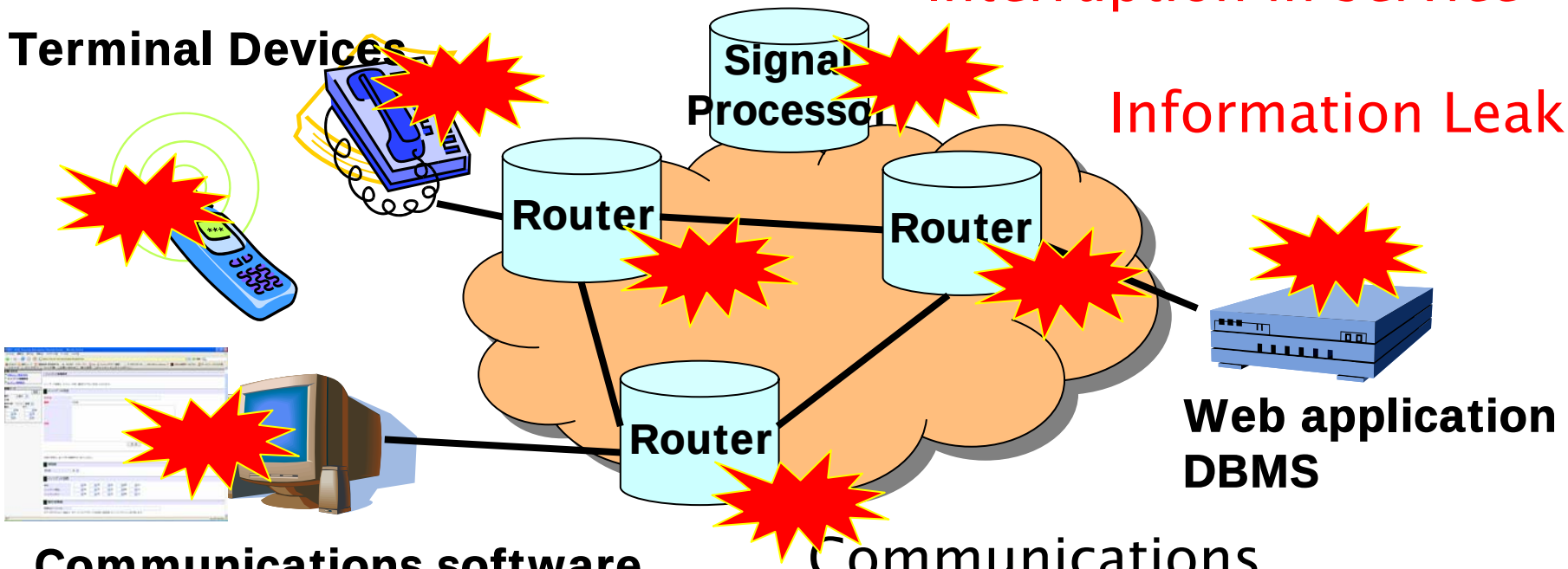
11th Sep 2007
NTT-CERT
Jumpei Watase
watase.jumpei@lab.ntt.co.jp

Agenda

- Vulnerability Handling
- Issues on handling process in an large-scale organization
- Our proposed system
  - SIXI(Security Information eXchange Infrastructure)

Vulnerability Handling

To maintain the security of computer networks, it is critical to deal with vulnerabilities related to information technology products, such as servers, routers, application software and terminal devices.



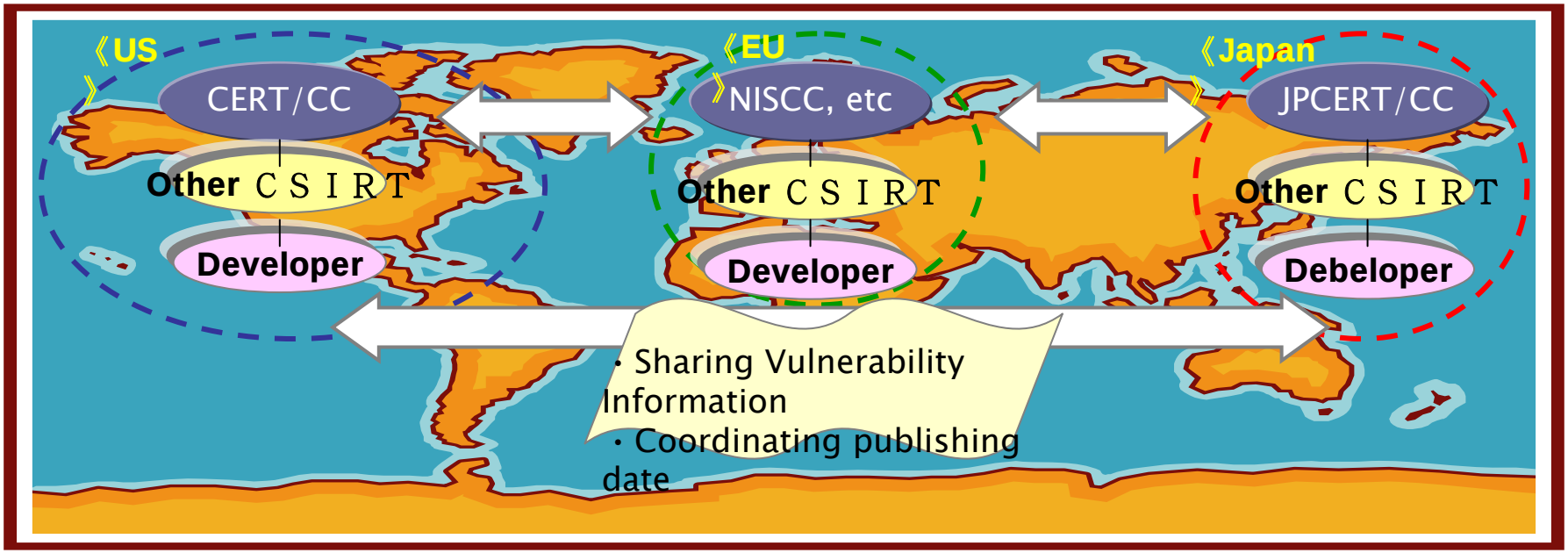
Types of Vulnerability information

NTT-CERT

- Public
  - Has been disclosed to the public on some web sites or mailing lists
  - Do not require high confidentiality in information handling
  - But sometimes quick responses are required for minimize the potential damages by exploitation
- Undisclosed
  - Should be secretly shared among one or more specific entities, such as vendors and coordinators
  - Require high confidentiality in information handling.
  - Solution should be prepared before disclosure to public

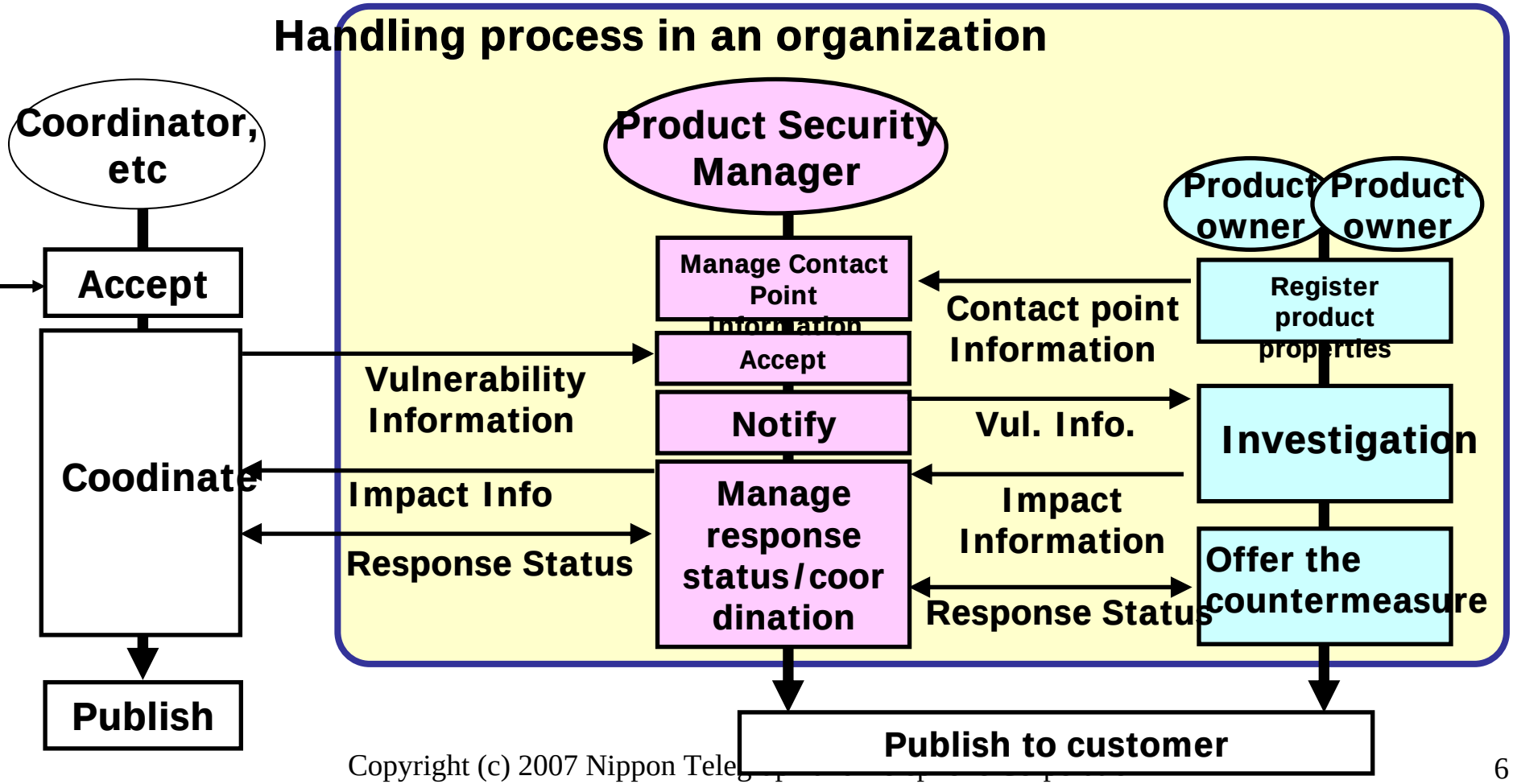
Global Information Sharing

- **Information about vulnerability affected on multiple products and to expose the Internet at risk are shared among local coordination globally.**
- **The coordination centers are trying to share the information among vendors and coordinate an uniform update release date globally.**
- **In Japan, JPCERT/CC takes charge of the local coordinator.**



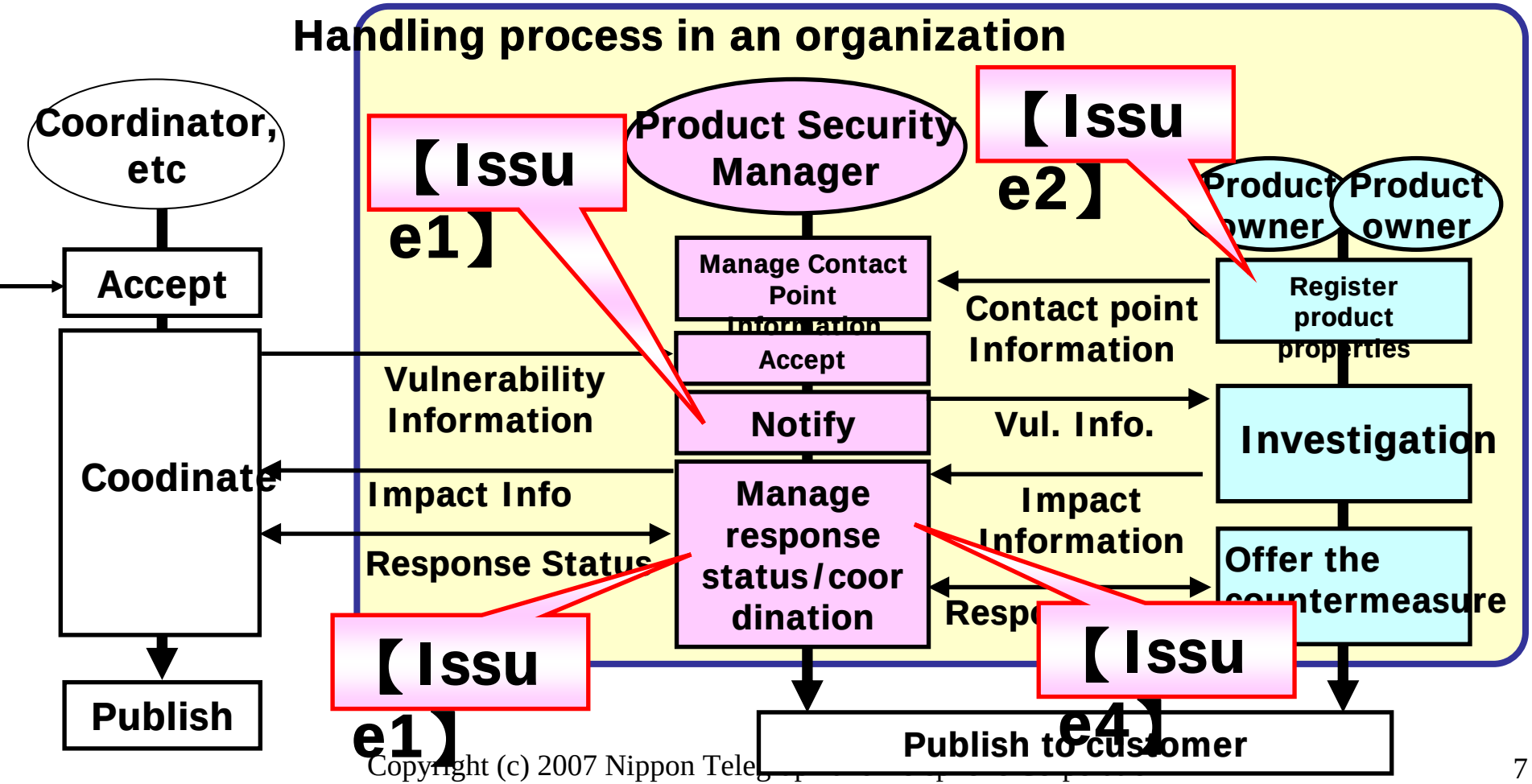
Handling process in large-scale organization

- ◆An organization should disseminate vulnerability information in a timely manner to the appropriate product owners who are in charge of affected products/services
- ◆Keep confidentiality until publishing date
- ◆Offer solutions on schedule (and, if needed, coordinate release schedule with external parties)



Vulnerability Handling Issues

【Issue1】Notification to everyone who needs vulnerability informatio
【Issue2】Accurate understanding of product composition
【Issue3】Observation of vulnerability information distribution and re
【Issue4】Centralized control of vulnerability information



Notification to everyone who needs vulnerability information

- Contact point information management
  - Manage the list of the products in an organization
  - Manage the list of the person in charge of the products
- Difficulties
  - A lot of products, sections, people
  - Products component often change
    - Startup of new development project
    - Changes in product specifications
    - Reassignment of product owners (person transfer)
- Effective management methods are required
  - Maintain up-to-date product listing, product components and product owner effectively

Accurate understanding of product composition

- Accurate understanding of product composition
  - Protocol
  - OS, Middleware, Library
- Difficulties
  - Every product owner is not necessarily understand whole composition of their products
    - Outsourcing
    - Failure to transfer knowledge when personnel transfers
- Effective methods to understand product component are required

Observation of vulnerability information distribution and response status

- Monitor the information distribution and response status for risk management and internal/external coordination
  - Who knows this information?
  - Which products are affected?
  - Who work to solve the problem and how is current status
- Difficulties
  - Conventional information distribution method by means of e-mail doesn’t allow security manager to comprehend the distribution status
- Effective monitoring methods are required

Centralized control of vulnerability information

- Undisclosed vulnerability information distribution by e-mail has another problem
  - PGP is not familiar with ordinary product owners
  - Difficult to control boundary of information disclosure
  - Cannot control confidentiality by an organization
- Centralized control of vulnerability information distribution in an organization is required to control confidentiality

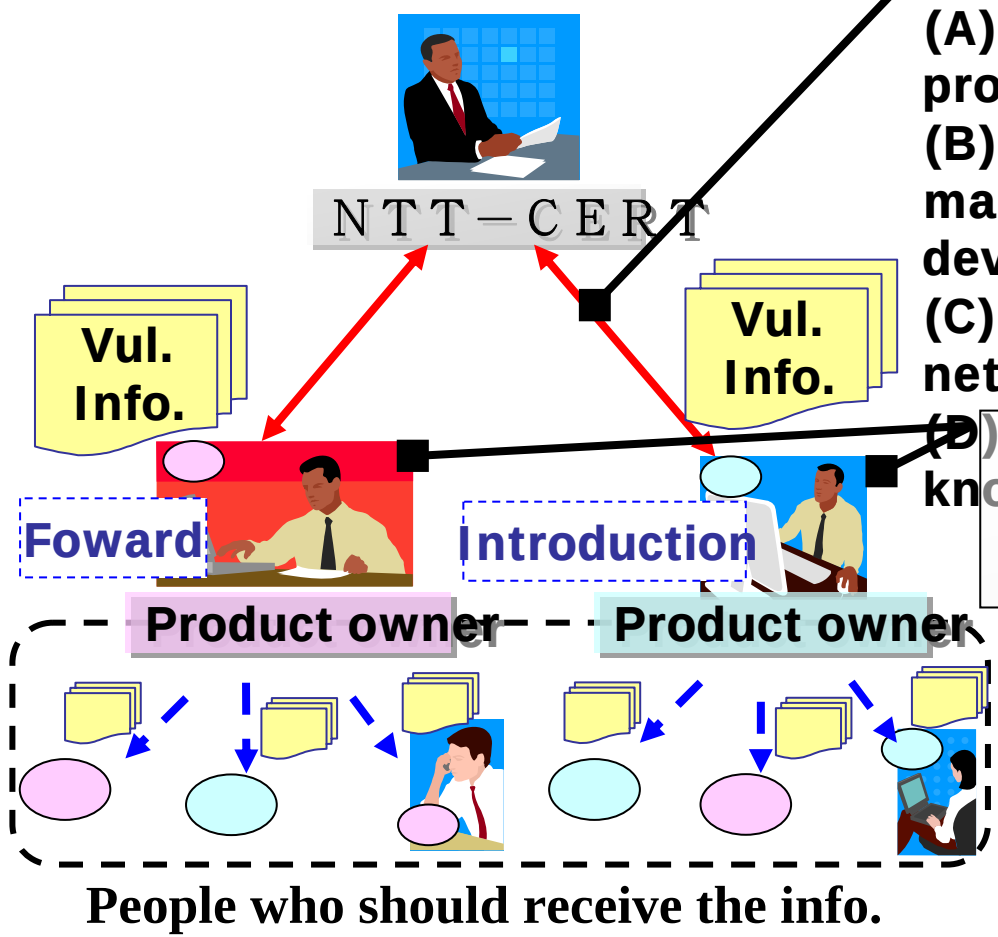
Our Goal

- Integrate a system that comprehensively manages vulnerability information.
  - Enables an organization to distribute vulnerability information in a timely and secure manner to product owner in an organization.
  - With vulnerability response status trucking.
- Security Information eXchange Infrastructure (SIXI)

Conventional Practice

◆**Introduction and forwarding played very important role exhaustive notification.**

Handling Undisclosed Vulnerability



The first contact

(A) Product owners in charge of affected product
(B) People who are in charge of managing the point of contact of development sections
(C) People who have wide human networks in related fields
(D) People who have extensive knowledge of related technologies

Distributed more widely and prope
Due to the introductions or forwar
By cooperative people

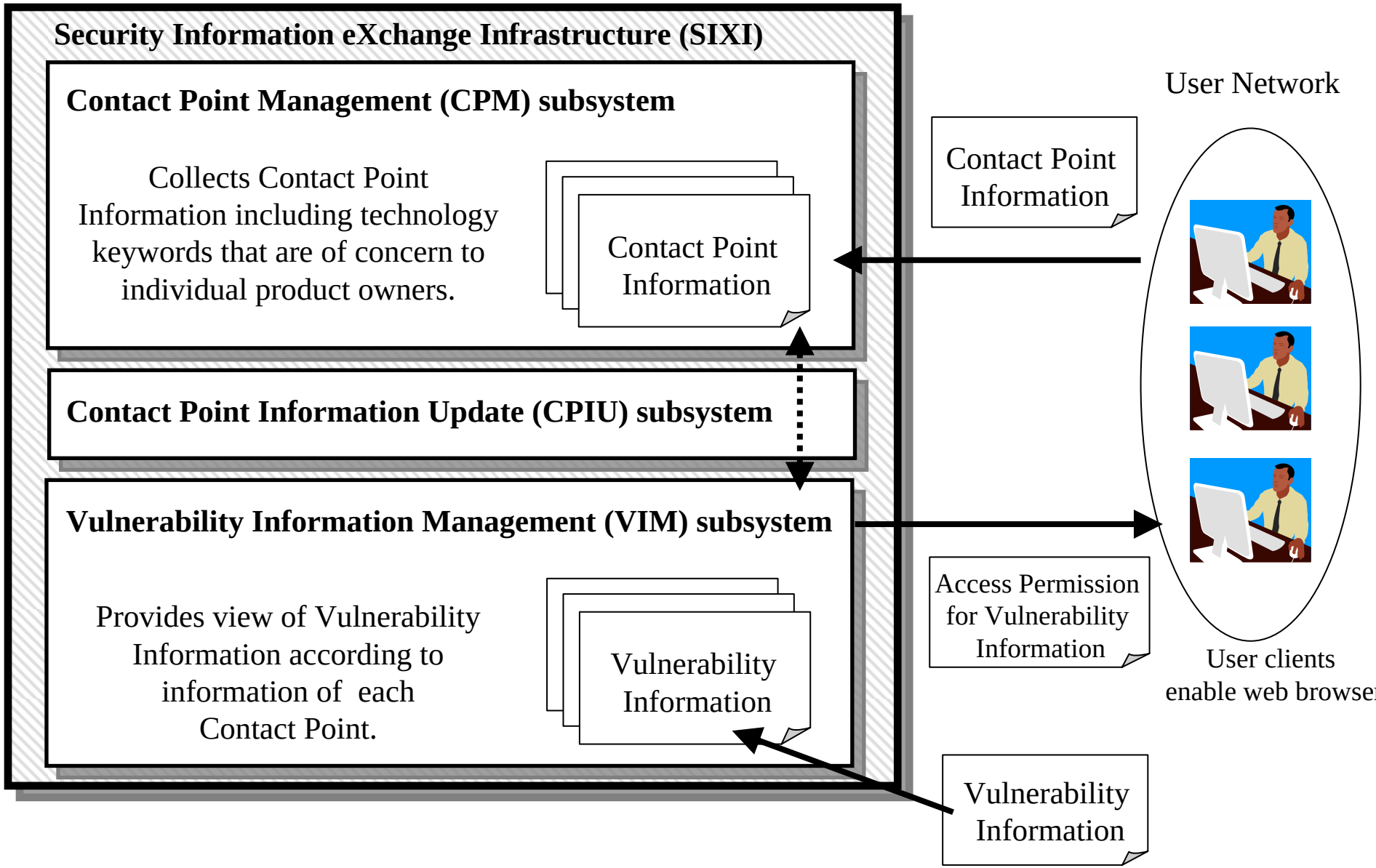
Check point

People are truly eligible to recei

People who received the info.

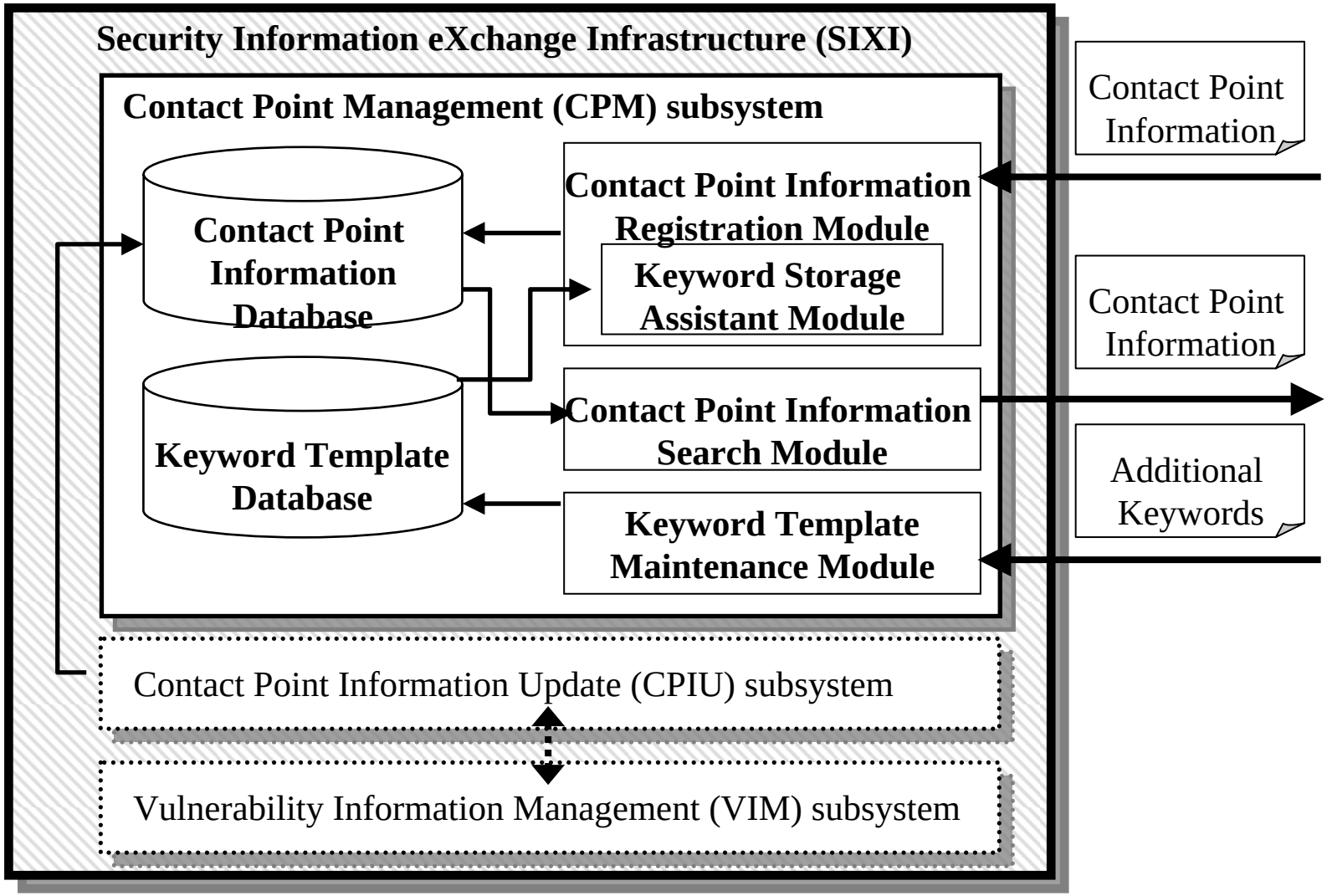
- Provide effective function for organizational vulnerability handling
  - An efficient management of contact point information and dissemination of vulnerability information
- Based on a social network approach
  - Take advantage of real world social network in an organization
- Consists of three subsystems
  - Contact Point Management (CPM)
  - Vulnerability Information Management (VIM)
  - Contact Point Information Update (CPIU)

Conceptual Diagram



CPM Subsystem

Provide capability to search for product owners quickly a accurately



Contact Point Information

- User profile to be used to search and determine the product owners who should receive certain vulnerability information
- Information elements
  - Product owner's name
  - Product owner's contact information
  - Product names that he/she is responsible for
  - Product composition described as technical keywords set
  - Other technical keywords that the owner has an interest in
- Technical keywords – names of operating system, middleware, libraries and protocols.
- Contact point information is maintained by product owners themselves.

Keyword Template

- Keyword Template is a set of technical keywords to offer choices of keywords to register
  - To make keyword registration easy
- Keyword template require continuous maintenance
  - Change along with appearance of new technology.
- SIXI provide a method to update the keyword template
  - Every member in an organization can propose additions of keywords (like wiki)
  - Security manager accredited the proposal for preventing abuse

Keyword Storage Assistant

- Extract keywords candidate form existing documents in
- Users select the keywords to be registered from the can

Specification
Protocol
SMTP
POP
APOP
SSH

①Input docs

CPM
Keyword storage Assistant
Keyword Template
Match! SMTP Match! POP
Match! APOP SSL
Match! SSH

②Offer candidates

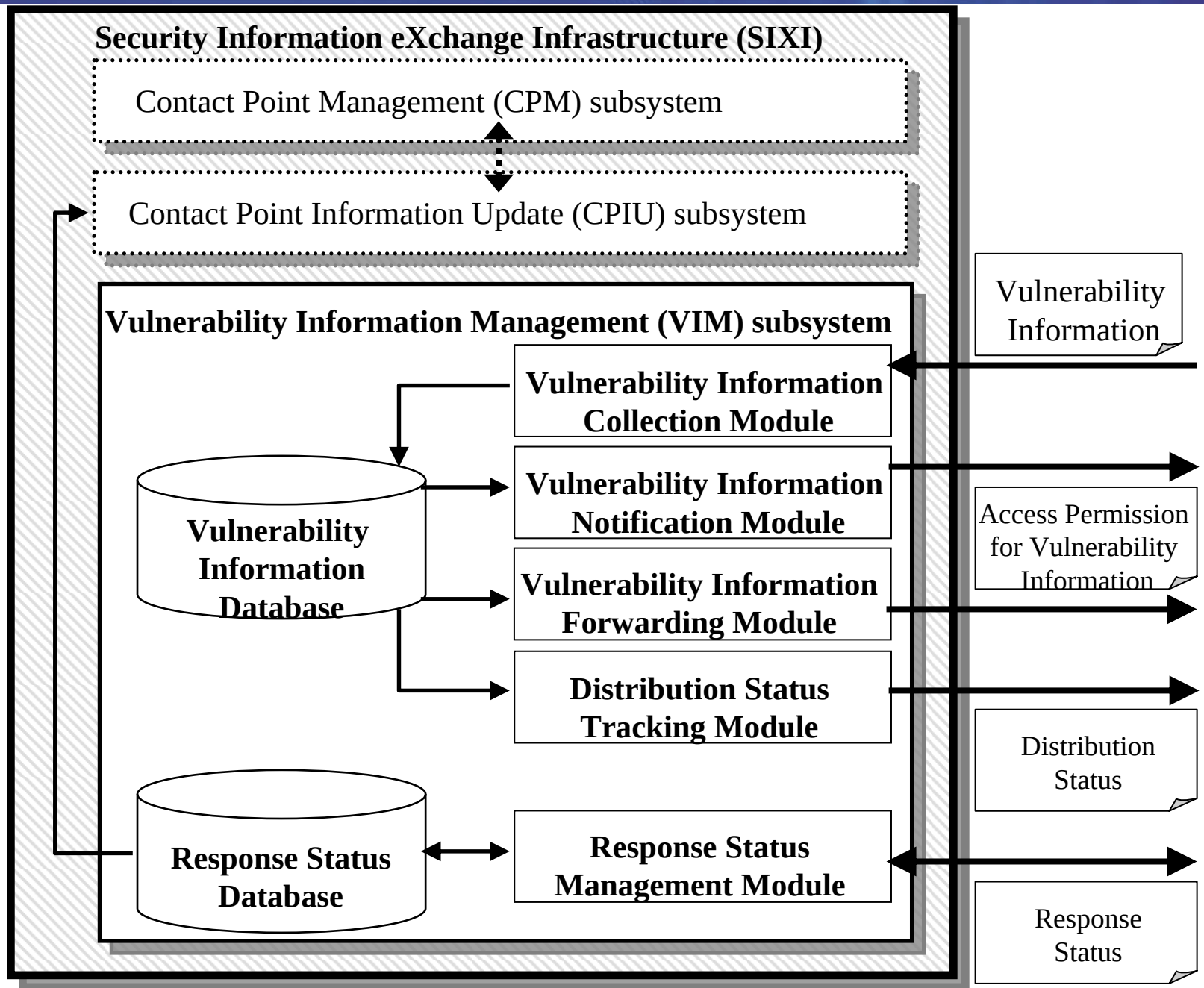
CPI
Keywords
☑ SMTP ☑ POP
☑ APOP ☐ SSL
☑ SSH

③Select and register

CPI-DB

Product : SIXI
Section : XXX
Name : Sato

VIM Subsystem



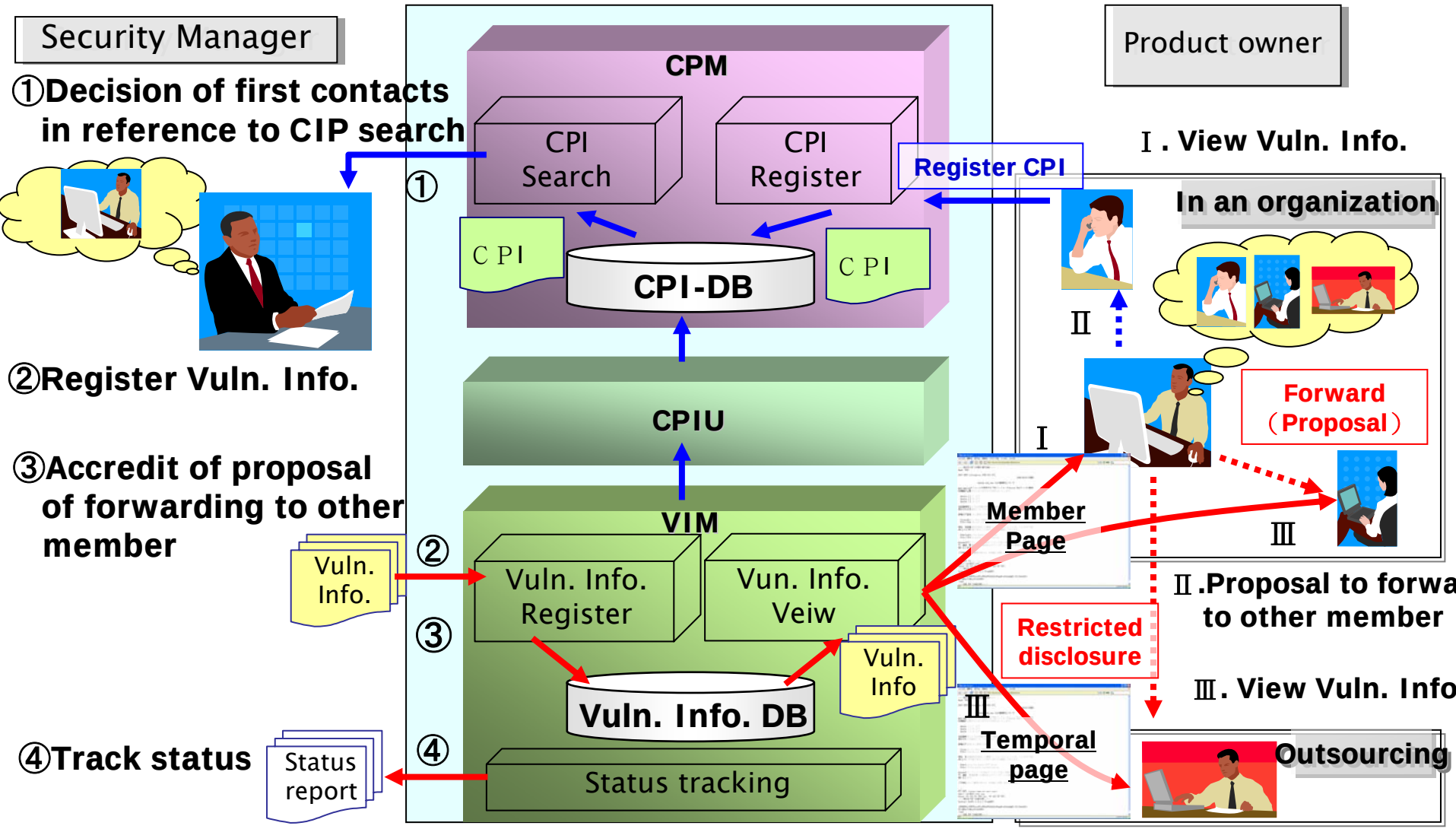
CPIU Subsystem

- Updates Contact Point Information regarding vulnerability information forwarding actions
  - The object to be updated is the keyword set of each product owner in Contact Point Information
- When a product owner receives an vulnerability information forwarded by other people and evaluate it useful, CPIU update the keyword set of him/her.
- This makes contact point information update easy and efficiently
- Other recommendation type should be introduced and evaluated in future development
  - He/She should be a owner of this product
  - This product should have this keyword in its keyword set
  - He/She should be notified information related to this keyword
  - Etc.

Vulnerability Information Forwarding

- Enables any person to forward certain information to other product owner
- Product owner who are informed a certain vulnerability information can view information dissemination status (who knows this information) about the vulnerability
- Person who noticed that another person should be also notified can forward the vulnerability information.
- In case of handling undisclosed vulnerability information, accreditation process by security manager has been introduced for preventing unauthorized access or information leakage.

Use case example



Summary

SIXI is an communications platform for organizational vulnerability h based on grass-roots social networks in an organization

Issue 1

Notification to everyone who needs vulnerability information

Solution 1

Share information about dissemination and second-handed forwarding mechanism + **Automation of contact point update in reference to information fowarding**

Issue 2

ccurate understanding f product compositio

Issue 3

bservation of vulnerability info distribution and response status

Issue 4

Centralized control of ulnerability information

Solution 2

Assisting technical keywor of product/system

Solution 3

Centralized management of information abo Vulnerability, contact point and various stat

Thank you

Contact:cert@ntt-cert.org