CSIRT Modeling Architecture

July 2, 2009

Takahiko Yoshida

吉田 尊彦

NTT-CERT

© 2009 NTT Information Sharing Platform Laboratories
Abstract

• This project focuses on the Modeling Architecture of CSIRT, NOT the modeling of CSIRT itself.

• The concept “Modeling Architecture” here comes from terminology of software development.

• “Modeling Architecture” consists of variety of components such as wisdoms, principles, stories, service templates, procedures and guidelines.

• From the viewpoints of services a CSIRT provides, Not CSIRT itself.

• Organization theories from social science are also considered and their inputs are to be applied.
Background

There are existing excellent tools and documents mainly to establish and operate CSIRTs.

However, there is not enough tools and documentation for amending CSIRT services and functions.

We need a method to adjust CSIRT’s services and functions based on the changes of its circumstances and contexts.

The demand for modeling architecture for up-to-date CSIRT services and functions.
## Gap Analysis

### Service-oriented approach

#### Differences from existing approaches

<table>
<thead>
<tr>
<th></th>
<th>Existing Approach</th>
<th>Our Works</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Objectives</strong></td>
<td>Construct CSIRTs from the beginning</td>
<td>Amend the services of existing CSIRTs</td>
</tr>
<tr>
<td><strong>Parameters</strong></td>
<td>Mission</td>
<td>?</td>
</tr>
<tr>
<td></td>
<td>Constituency etc.</td>
<td>Missing?</td>
</tr>
<tr>
<td></td>
<td>(Characterizing a CSIRT)</td>
<td></td>
</tr>
</tbody>
</table>
Concept

**CSIRT Modeling Architecture** consists of the components systematically collected and formalized.

- We need to model what service(s) to be added, modified, and/or suspended for existing CSIRTs.
- The modeling parameters are defined to analyze CSIRT services for that purpose.
- These parameters would be different time to time depending on the different services and circumstances.
- The more frequently changes occur, the more quickly the parameters could get outdated.

Modeling can be done easily and efficiently by the **CSIRT Modeling Architecture**.
Road map

We started our project from modeling services, followed by establishing **modeling architecture** right now.

**Modeling approach**

- **Completed!**
- **(1) Creation of a template for a specific CSIRT service**
- **(2) Parameter extraction**
  - Enhancing to other services
  - Parameter extractions for factors other than services
- **(3) Template generalization**

**Modeling**

**CSIRT Modeling Architecture**

- **Social psychology approach and organization theory approach**
  - **(a) Formulation of maxims regarding CSIRTs and/or CSIRT-related incidents**
  - **(b) Extraction of parameters of maxims related to service and CSIRT organization**

**2008  2009  201X**

© 2009 NTT Information Sharing Platform Laboratories
Current status

We have developed a first model for information leakage incident handling service.

Factors which characterize this service.

* CSIRT type
* Mission/Objectives
* Service offer time
* Interface
* Service list
* Business Relationship with Internal Sections
* Relation with Other entities
* Policy
* Procedures
* Facilities
* Counter-plan
* Resource

This exercise also helped us review our current service in detail.
Next Steps

- Consider and possibly adopt lessons and inputs from organization theories to look for factors characterizing a CSIRT for possible additional modeling parameters.

- Expand models into more services
  (Information leakage incident ➔ Incident handling ➔ Other service)

- Collaborate with other CSIRTs through Nippon CSIRT Association
  ✓ Expecting more CSIRTs for more adoption for better analysis
  ✓ More participation should improve the Modeling Architecture
cert@ntt-cert.org

PGP KeyID: 7E34EEFD

Thank you!