The 8th World Multi-Conference on Systemics, Cybernetics and Informatics, Vol.X, pp.40-46 (Jul.18-21, 2004)

Proposal of the Security Information Sharing System with RDF Site Summary

Masato Terada [†]
Graduate School of Science and Technology,
Keio University.
3-14-1 Hiyoshi, Kohoku, Yokohama, Kanagawa 223-8522, Japan

and

Norihisa Doi [‡]
Graduate School of Science and Engineering,
Chuo University.
1-13-27 Kasuga, Bunkyo-ku, Tokyo 112-8551, Japan

ABSTRACT

Unauthorized access containing Malware propagation is activated and causes a lot of damage. In order to protect the unauthorized access and eliminate the vulnerability, it is necessary to improve the security information sharing environments about the Japanese domestic software and the equipments. When the new vulnerability is exposed or security advisory is released, the security administrators try to gather countermeasure information about that vulnerability. In this work, we have taken up this issue. We have examined - how we can provide a security information sharing service for the security administrators, while our operations of information gathering reduced.

We propose “JP Vendor Status Notes (JVN)” and “Status Tracking Notes (TRnotes)” as the security information sharing system. The former is the countermeasure information service of the vulnerability, and the latter is the event information service of the incidents. This paper discusses the requirements of these services and the XML formats for the security information sharing. Finally, we introduce our sharing framework.

Keywords: Unauthorized Access, Network Security, Vulnerability, Information Sharing

1. INTRODUCTION

Recently, Malware (Virus, Worm, Trojan Horse etc.) propagation is activated and causes a lot of damage broadly and variably. Especially, since the propagation of SQL slammer at January 2003 and MS-Blaster at August 2003, we should promote not only the countermeasure about prevention to the server systems but also client systems. In order to protect the unauthorized access and eliminate the vulnerabilities of information systems, it is necessary to improve the security information sharing about the Japanese domestic software and the equipments.

We propose “JP Vendor Status Notes (JVN)” and “Status Tracking Notes (TRnotes)” to solve the problems and improve the security information sharing. The JVN [1] is the trial portal site to provide the security information about Japanese domestic software and equipment vendors. TRnotes is the site to provide the time series events such as the followings.

- When was the exploit code exposed to the public?
- What kind of incidents did occur?
- What kind of countermeasure did apply to the incidents?

Furthermore, we propose the XML format of two types to support the operation of the information gathering. JVN RSS (RDF Rite Summary) [2] is XML format for the summary of the security information. And VULDEF (Vulnerability Data Publication Format) / Security Advisory Publication Format is XML format for the detail. These formats have the “Relational ID” and the “Published Date” element. Relational ID element is index to make a grouping of the security information and Published Date element is index to arrange the events based time series.

2. RELATED WORK

The related researches of the security information sharing are the followings.

CVE [3]
The Common Vulnerabilities and Exposures (CVE) is a list of standardized names (ex. CVE-1999-1011) for vulnerabilities and other information security exposures. CVE supports relationship among all publicly known vulnerabilities and security exposures. Many tools, Web sites, databases, or services use CVE names in a way that allows it to cross-link with other repositories that use CVE names.

[†]) Systems Development Laboratory, Hitachi Ltd.
890, Kashimada, Saiwa-ku, Kawasaki, 212-8567 Japan.
[‡]) Graduate School of Science and Technology, Keio University

NIST ICAT Metabase [4]
ICAT is a searchable index of information on computer vulnerabilities and refers to CVE. It provides search capability and links users to vulnerability and patch information.

AVDL [5]
The Application Vulnerability Description Language (AVDL) creates a uniform way of describing application security vulnerabilities using XML.

OSVDB [6]
Open Source Vulnerability Database (OSVDB) is the vendor neutral vulnerability database for utilization for the information security community. The goals of the project are to promote greater, more open collaboration between companies and individuals, eliminate redundant works and reduce expenses inherent with the development.

Our approach supports not only the vulnerability countermeasure information sharing but also the follow-up security events about vulnerability and incident.

3. THE REQUIREMENTS OF SECURITY INFORMATION SHARING

There are following requirements in the Japanese domestic security information sharing.

- CERT/CC provides timely information about current security issues, vulnerabilities, and exploits as CERT Advisory [7][a]. And CERT Vulnerability Notes [8] provide a mechanism to publish information about these less severe vulnerabilities such as portal site of the security in US. The portal site of the security information about the Japanese domestic software and equipments such as CERT/CC Vulnerability Notes is required.

- In 2002, a lot of vulnerabilities were reported in popular software such as SNMP, Apache, DNS resolver and OpenSSL. At March 2004, the vulnerability of TCP reported affects any network system. It is so important to understand how many take the impact of the vulnerability in the domestic software and equipments, and the shared mechanism of the vendor security information is required.

- The large incident by the worm has the following three steps.
  - ➢ The vulnerability is disclosed.
  - ➢ The exploit (Proof of Concept) code is released.
  - ➢ The appearance of a worm based on the exploit code that exploits a disclosed vulnerability.

For example, in 2003, the appearance process of the Blaster/Nachi worm matches this process (Figure 1). It is important to understand the current threat status to decide the next step countermeasure. Especially the interval from the vulnerability disclosure to the exploit code release has become short. The follow-up and sharing environment of security events about the vulnerability and incident is required.

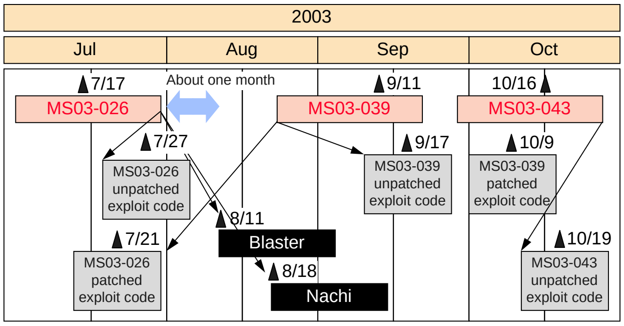

2003
Jul
Aug
Sep
Oct
7/17
About one month
9/11
10/16
MS03-026
MS03-039
MS03-043
7/27
9/17
10/9
MS03-026 unpatched exploit code
MS03-039 unpatched exploit code
MS03-039 patched exploit code
8/11
7/21
10/19
Blaster
MS03-026 patched exploit code
8/18
MS03-043 unpatched exploit code
Nachi

Figure 1: The appearance process of the Blaster worm.

4. THE SECURITY INFORMATION SHARING FRAMEWORK

We propose “JP Vendor Status Notes (JVN)” and “Status Tracking Notes (TRnotes)” to attempt to solve these requirements of improving the security information sharing.

4.1 JVN

JVN is trial portal site to Japanese domestic vendor's security information corresponding to CERT Advisories and CIAC Bulletins [9]. This site provides the Japanese domestic vendor's security information lists against a vulnerability and improves the security information environments for the security administrators. The each web page consists of the overview, impact, vendor information lists as a solution for the vulnerability and related information with PGP signature (Figure 2).

An example of JVN page is shown in the Figure 3. The characteristics of JVN page are the followings.

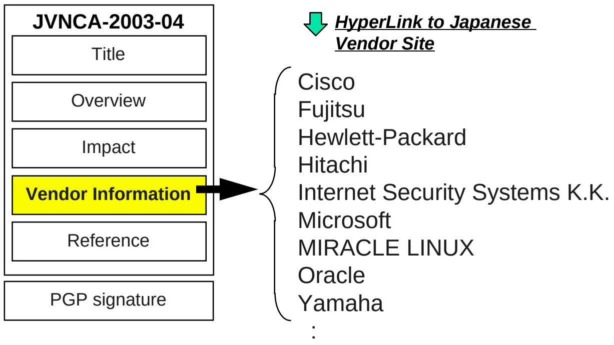
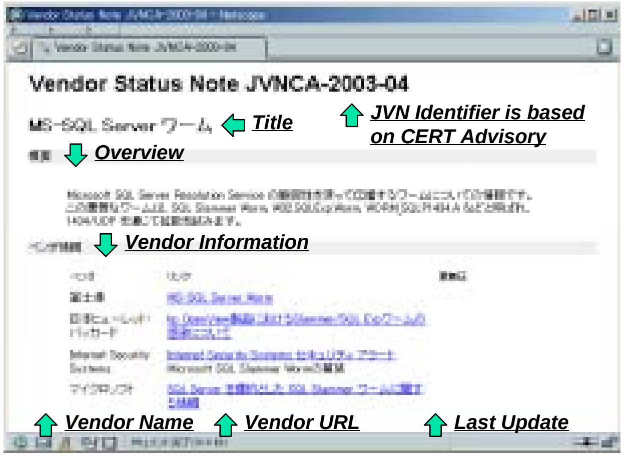


Figure 2: The structure of JVN web page.

[a] At April 2004, CERT advisories have become a core component of US-CERT's Technical Cyber Security Alerts.

- The JVN page structure is based on CERT Vulnerability Notes.
  In the first step, JVN main target is to make the aggregation page including the hyperlinks of the vendor security information. The security administrators can follow these hyperlinks and read the detailed vendor statements (called Vendor Status). The next step will include the detail of the vulnerability information such as CERT Vulnerability Notes.

- JVN Identifier is based on CERT Advisory or CIAC Bulletin Number.
  There is CVE as the vulnerability identifier and CVE name is standardized name of vulnerability. But we decide to refer to the CERT Advisory or CIAC Bulletin Number as JVN Identifier, because CERT Advisory and CIAC Bulletin is so well known security information in the world and many administrators refer to them.



Vendor Status Note JVNCA-2003-04

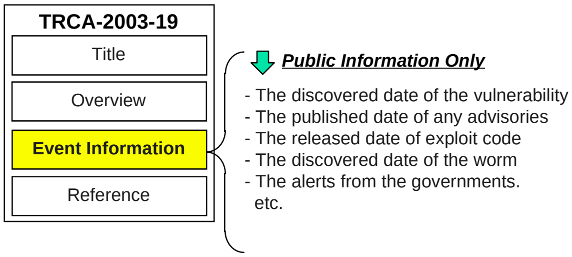
MS-SQL Server ワーム

Figure 3: An example of JVN about CA-2003-04 (MS-SQL Server Worm)

JVN site began from February 2003 and has about 200 entry pages corresponding to CERT Advisory or CIAC Bulletin. JVN always needs to maintain these pages at the latest version when the vendor security information is updated or new one is provided. It becomes important to construct the gathering mechanism of the vendor security information to reduce the operation cost (it means speedup of maintenance).

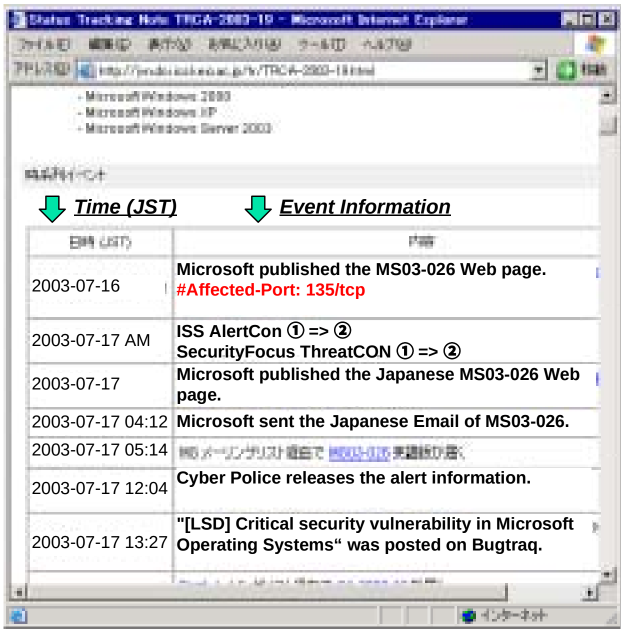
4.2 TRnotes

We should cooperate with other Internet sites to eliminate the security incidents and the event sharing is important to accomplish it. The purpose of TRnotes is in sharing the events of time series, which include worm activities, exploit codes releasing and the countermeasure of security incidents. The each web page consists of the overview, impact, the events of time series and related information (Figure 4). An example of TRnotes page is shown in the Figure 5. The characteristics of TRnotes page are the followings.



TRCA-2003-19
Title
Overview
Event Information
Reference
Public Information Only
- The discovered date of the vulnerability
- The published date of any advisories
- The released date of exploit code
- The discovered date of the worm
- The alerts from the governments.
etc.

Figure 4: The structure of TRnotes web page.



- Microsoft Windows 2000
- Microsoft Windows XP
- Microsoft Windows Server 2003

日時 (JST)	内容
2003-07-16	Microsoft published the MS03-026 Web page. #Affected-Port: 135/tcp
2003-07-17 AM	ISS AlertCon ① => ② SecurityFocus ThreatCON ① => ②
2003-07-17	Microsoft published the Japanese MS03-026 Web page.
2003-07-17 04:12	Microsoft sent the Japanese Email of MS03-026.
2003-07-17 05:14	[illegible]
2003-07-17 12:04	Cyber Police releases the alert information.
2003-07-17 13:27	"[LSD] Critical security vulnerability in Microsoft Operating Systems“ was posted on Bugtraq.

Figure 5: An example of TRnotes about CA-2003-19 (Exploitation of Vulnerabilities in Microsoft RPC Interface).

- The event indication time is based on hour unit level.
  The state is changing per hour, not per day, which is shown in Figure 5. In case of mailing list, the send or receive time becomes the event indication time. And in case of Web site, Last-Modified as header information on a HTTP protocol is used as the event indication time.

- TRnotes is made to have relations with Vendor Status information such as JVN.
  The security administrators catch up the countermeasure information at the various aspects. The purpose of TRnotes is the follow-up the security events, and leads the next step countermeasure.

- The event information is based on public information.
  It is important that the security administrators who belong to any organizations share the same event information to eliminate the incidents on the Internet. The public information has no restriction such as non-disclosure policy and becomes possible to share the information among more security administrators.

- Indicate the characteristics of the event.
  The event has the various characteristics. For example, in case of the disclosed vulnerability, there are the severity and the affected version as the characteristics. In case of the exploit code, there are the file name, confirmed test environment, and the behavior of code. TRnotes includes the items, which are shown in Table 1 to indicate the characteristics of the event. As for the expansion of the item list, it is a future work.

TRnotes site began from January 2004 and has about 30 entry pages corresponding to CERT Advisory, CIAC Bulletin or CERT Vulnerability Notes. TRnotes always needs to maintain these pages at the latest version when the events updated or new ones occur.

Table 1: The characteristic items of the event.

Item	Description
Affected-Port	The port number is affected by the vulnerability.
Affected-Version	The version number is affected by the vulnerability.
Severity-Rating	The relative severity of the vulnerability.
Cid	The file name of the exploit Code.
Tested	Confirmed test environment of the exploit Code.
Binding-Port	The port number is used by the exploit code.

Ex. The exploit code released

Time (JST)	Event Description
2003-11-12 21:40	Full-Disclosure "Proof of concept for Windows Workstation Service overflow" #Cid: 11.12.MS03-049PoC.c #Tested: Windows 2000 [EN] + SP4 #Binding-Port: 5555 #Post-Date: Wed, 12 Nov 2003 15:40:38 +0300

4.3 XML format for the security information sharing system

In TRnotes maintenance process, the gathering of the event information that related with the vulnerability and the extraction of the indication time of that event is required. The referring method of Last-Modified value as header information on a HTTP protocol has some problems.

- Last-Modified value may not be added on a HTTP protocol header.
- Last-Modified value may not match with the indication time of the event such as information opening to the public or discovering the worm.

Furthermore, the security information is distributed as Web page information on HTML base. In order to gather the information and perform the relationship between the gathered information, it is necessary to improve the method of the security information sharing. If the security information is machine readable, many Internet sites can reduce the cost of information gathering. Our security information sharing proposes the XML formats as to approach solving these problems. JVN RSS is the overview XML format based on RSS and VULDEF is the detail XML format (Figure 6).

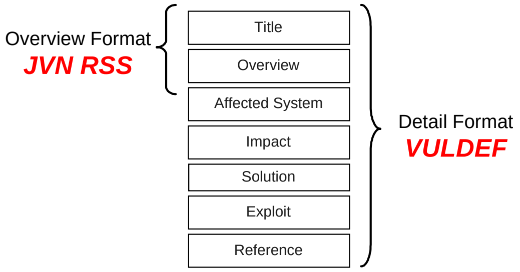


Figure 6: The classification of JVN RSS and VULDEF.

(1) JVN RSS

RSS is an XML-based format that allows the syndication of lists of hyperlinks. The original RSS, version 0.90, was designed by Netscape as a format for building portals of headlines to mainstream news sites. RSS 1.0 was based on RDF and designed by the original guiding principles of RSS 0.90.

JVN RSS is based on RSS 1.0 and use the field <dc:relation> of Dubline Core as index of grouping security information. JVN RSS with the Relational ID in <dc:relation> is shown in Figure 7. RSS contains a list of items, each of which is identified by a link. Each item can have any amount of metadata associated with it. The most basic metadata supported by RSS includes a title for the link and a description of it. And our proposal Relational ID allows the security information on the different sites to relate each other. URL of Common Vulnerability Exposure, CERT Advisory, CERT Vulnerability Note, US-CERT Technical Alert and CIAC Bulletin are used as Relational ID. These are best reference for Internet security information.

The RSS items with same Relation ID belong to same group. That is to say two RSS items in Figure 8 refer to same vulnerability and related with the US-CERT Technical Alert TA04-111A, “Vulnerability in TCP”.

JVN RSS has <dc:date> element as Published Date, <dc:relation> element as Relational ID. This XML format supports to make the page including the hyperlinks of the vendor security information such as Vendor Status Notes.

```
<item rdf:about="URL of vendor information">
  <title>Title</title>
  <link>URL of vendor information </link>
  <description>Outline of Security Information</description>
  <dc:publisher>Vendor Name</dc:publisher>
  <dc:identifier>Information ID</dc:identifier>
  <dc:relation>Relational ID { CVE | CERT-CA | CERT-VU | CIAC}</dc:relation>
  <dc:date>Last Updated Date</dc:date>
 </item>
```

Figure 7: JVN RSS XML format.

```
<item rdf:about="http://www.checkpoint.com/techsupport/alerts/tcp_dos.html">
  <title>TCP RFC Alert</title>
  <link>http://www.checkpoint.com/techsupport/alerts/tcp_dos.html</link>
  <description />
  <dc:publisher>Check Point</dc:publisher>
  <dc:identifier />
  <dc:relation>http://www.us-cert.gov/cas/techalerts/TA04-111A.html</dc:relation>
  <dc:date>2004-04-21</dc:date>
</item>

<item rdf:about="http://www.cisco.com/japanese/warp/public/3
              /jp/service/tac/707/cisco-sa-20040420-tcp-nonios-j.shtml">
  <title>TCP Vulnerabilities in Multiple Non-IOS Cisco Products</title>
  <link>http://www.cisco.com/japanese/warp/public/3/
              jp/service/tac/707/cisco-sa-20040420-tcp-nonios-j.shtml</link>
  <description />
  <dc:publisher>Cisco</dc:publisher>
  <dc:identifier>Cisco Security Advisory ID#50961</dc:identifier>
  <dc:relation>http://www.us-cert.gov/cas/techalerts/TA04-111A.html</dc:relation>
  <dc:date>2004-04-21</dc:date>
</item>
```

Figure 8: An example of JVN RSS.

(2) VULDEF

The purpose of the "Vulnerability Data Publication Format (VULDEF)/Security Advisory Publication Format" is to define data formats for the information related to security advisory typically published by the product vendors and Computer Security Incident Response Teams. VULDEF has some elements to describe the vulnerability, affected item and solution etc. UML of the VULDEF Data Model is shown in Figure 9.

The requirements of VULDEF are the followings.
As security advisory publication format

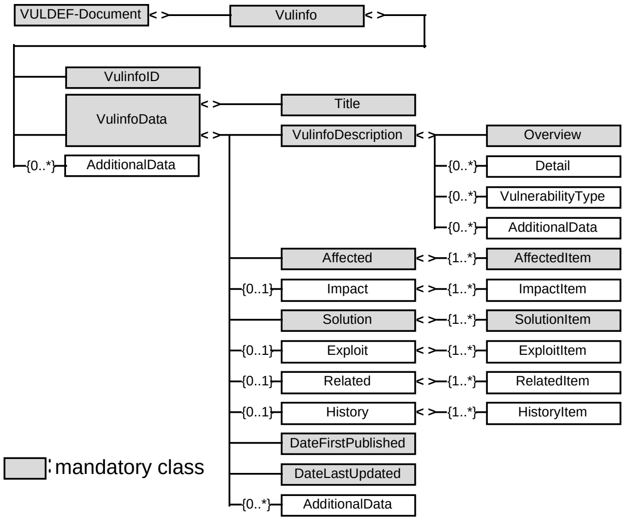
- It satisfies the core format of the countermeasure information provided by the vendor and organization.
- It has the extension parts of the describing exceptional details and the future works.

As format of our Security Information Sharing System

- It has the Relational ID element to make a group of security information.
- It has the Published Date element to indicate invoked event time.
- It has the extension parts to describe the characteristic items of the event.

The mandatory classes of VULDEF are Title, Overview, AffectedItem, SolutionItem, DateFirstPublished class and DateLastUpdate class only. And VULDEF has the following parts to describe the characteristic items of the event.

- **VulnerabilityType class**: Each vulnerability in such a way that one can understand the type of software problem that produced the vulnerability. The permitted values are based on NIST ICAT.
- **ImpactType class**: The type of impact in relatively broad categories. The permitted values are based on IODEF[10].
- **severity attribute**: An estimate of the relative severity of the vulnerability. The permitted values are based on IODEF.
- **orign attribute**: The name of the database to which the reference is being made. The permitted values are based on IODEF.
- **expolitrange attribute**: A vulnerability can enable either a "local" and/or "remote" attack.
  Etc.



Class	Description
Title	The title of the countermeasure information for eliminating the vulnerability.
VulinfoDescription	The detail of the vulnerability information.
Affected	The affected system. product, or version information.
Impact	A description of the technical impact due to the vulnerability.
Solution	The technical solution due to the vulnerability.
Exploit	The exploit activity due to the vulnerability.
Related	The references of vulnerabilities are related to the one described in the VULDEF document.
DateFirstPublished	The first published the VULDEF-Document.
DateLastUpdated	This is the date the VULDEF-Document was last updated.
AdditionalData	An extension mechanism for information not otherwise represented in the data model.

An example of AffecteItem and ExploitItem

```
<Affected>
  <AffectedItem affectedstatus="vulnerable" historyno="2">
     <Name>OpenSSH</Name>
    <ProductName>OpenSSH</ProductName>
    <VersionNumber range="begin" operator="ge">3.6</VersionNumber>
    <VersionNumber range="end" operator="le">3.7</VersionNumber>
  </AffectedItem>
  AffectedItem affectedstatus="notvulnerable" historyno="2">
    <Name>OpenSSH</Name>
    <ProductName>OpenSSH</ProductName>
    <VersionNumber operator="eq">3.7.1</VersionNumber>
  </AffectedItem>
 </Affected>

<Exploit>
  <ExploitItem exploittype="malware" historyno="1">
    <Description>Full-Disclosure "new openssh exploit in the wild!"</Description>
    <URL>http://lists.netsys.com/pipermail/full-disclosure/2003-September/010453.html</URL>
  </ExploitItem>
</Exploit>
```

Figure 9: UML of the VULDEF Data Model

4.4 The gathering and grouping approach of the security information sharing system

JVN RSS format is based on RSS 1.0, which is same RSS format by major news sites. Then once information about each item is in RSS format, an RSS-aware program can check the feed for changes and react to the changes in an appropriate way. JVN RSS service on JVN site began from July 2003 and provides four types of RSS, which are for JVN, JVN/CIAC, TRnotes and updated items.

When the security information is machine readable, many Internet sites can reduce the cost of information gathering and grouping. Our gathering and grouping approach using JVN RSS format has three steps, which are shown in Figure 10. The approach using VULDEF is same process.

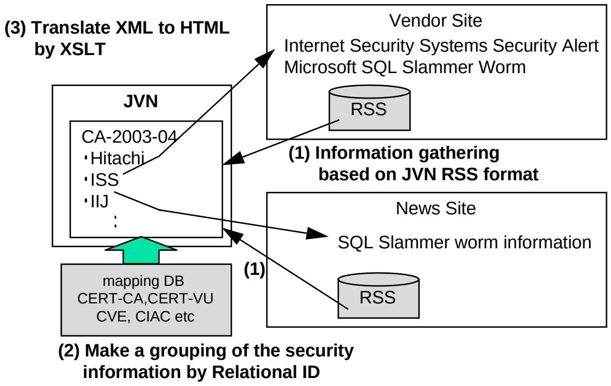
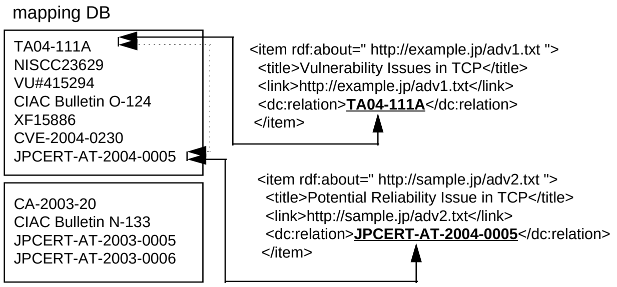

(3) Translate XML to HTML by XSLT
Vendor Site
Internet Security Systems Security Alert
Microsoft SQL Slammer Worm
RSS
JVN
CA-2003-04
･Hitachi
･ISS
･IIJ
:
(1) Information gathering based on JVN RSS format
News Site
SQL Slammer worm information
RSS
(1)
mapping DB
CERT-CA,CERT-VU
CVE, CIAC etc
(2) Make a grouping of the security information by Relational ID

Figure 10: Overview of the gathering and grouping approach with JVN RSS.

(1) The step of information gathering
The function of the information gathering using JVN RSS format checks the feed for changes and extracts the feed entry at the change.

(2) The step of information grouping
The information grouping function extracts the Relational ID from the feed entry. And the function using Relational ID as search key finds the same in the mapping DB. The mapping DB of Relational ID is shown as Figure 11. The upper group in mapping DB is the vulnerability information related TCP stack and the lower group is the incident information about MS-Blaster worm. The information entries belong to same group, which refer to same vulnerability or incident. In case of the feed entries have the different Relational ID, but they refer to same vulnerability, the mapping DB trace to the relationship between Relational IDs.



```
<item rdf:about=" http://example.jp/adv1.txt ">
  <title>Vulnerability Issues in TCP</title>
  <link>http://example.jp/adv1.txt</link>
  <dc:relation>TA04-111A</dc:relation>
</item>
```

```
<item rdf:about=" http://sample.jp/adv2.txt ">
  <title>Potential Reliability Issue in TCP</title>
  <link>http://sample.jp/adv2.txt</link>
  <dc:relation>JPCERT-AT-2004-0005</dc:relation>
</item>
```

Figure 11: The grouping mechanism using Relational ID and mapping DB.

(3) The step of transformation XML to HTML by XSLT
The translation function transforms XML documents into HTML.

5. CONCLUSION

We propose “JP Vendor Status Notes (JVN)” and “Status Tracking Notes (TRnotes)” as the security information sharing system to improve the environment for security administrators. The former is the countermeasure information service of the vulnerability, and the latter is the event information service of the incidents. This paper has described these services, the XML formats and the gathering and grouping approach for the security information sharing. The security administrators do information gathering to eliminate the threats at current status. Our activity supports these tasks. JVN and TRnotes are presently operational as shown in Figure 12.

For the future work, we will implement the RSS mechanism and clarify the “Vulnerability Data Presentation Format Data Model and XML Implementation” for Vendor Status Notes.

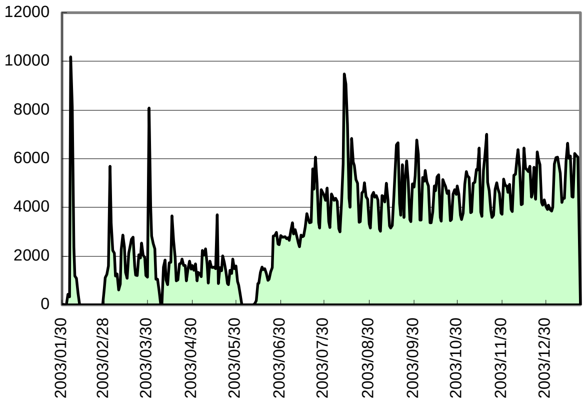


Figure 12: Total Access counts of JVN Web site.

6. REFERENCE

[1] Vendor Status Notes, http://jvn.doi.ics.keio.ac.jp/
[2] RDF Site Summary (RSS), http://web.resource.org/rss/1.0/
[3] Common Vulnerabilities and Exposures, http://cve.mitre.org/
[4] ICAT Metabase: A CVE Based Vulnerability Database, http://icat.nist.gov/
[5] AVDL, http://www.avdl.org/
[6] OSVDB, http://www.osvdb.org/
[7] CERT/CC Advisories, http://www.cert.org/advisories/
[8] CERT/CC Vulnerability Notes, http://www.kb.cert.org/vuls/
[9] CIAC Bulletins, http://www.ciac.org/cgi-bin/index/bulletins
[10] Incident Object Description and Exchange Format, http://www.terena.nl/tech/task-forces/tf-csirt/iodef/