



INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN



Proposal of RSS Extension for Security Information Exchange

18th Annual FIRST Conference

2006/06/30

Masato Terada
m-terada@ipa.go.jp
<http://jvn.jp/>

Prologue

My contribution to JVN

2004 - current

Visitor Researcher

IPA



2002 - current

HIRT Staff

Hitachi



2004 - current

Visitor Researcher

Chuo University



<http://jvn.jp/>



2003 - current

Associate staff

JPCERT/CC



April 2002 - March 2006

Graduate student

Keio University

Opening

We propose JVNRSS (JP Vendor Status Notes RSS) as a security information sharing and exchanging specification. JVNRSS is based on RSS 1.0 and uses the "<dc:relation>" field defined in the Dublin Core as a Relational ID to correlate security information issued by various sources. JVNRSS uses the reference URL specified in a security alert, for example, an URL of the Common Vulnerability Exposure, CERT Advisory, CERT Vulnerability Note and CIAC Bulletin.

In this presentation, firstly we'll explain the specification and applications of JVNRSS. Secondly, we'll introduce the result of our feasibility study on JVNRSS and lastly we'll propose the RSS Extension for security information sharing.

Contents

1. Vulnerability Information Handling Framework in Japan
2. JVN: JP Vendor Status Notes
3. Proposal of RSS Extension for Security Information Exchange



I skip section 1 and 2.

Please refer to conference CD-ROM.



INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN



Proposal of RSS Extension for Security Information Exchange



JVN
JP Vendor Status Notes

<http://jvn.jp/>

3.

Research motivation

- How we can provide a more efficient **PUBLIC** security information distribution service for the security administrators that helps them reduce their workload related to collecting and grouping various **PUBLIC** information and take care of security incidents.

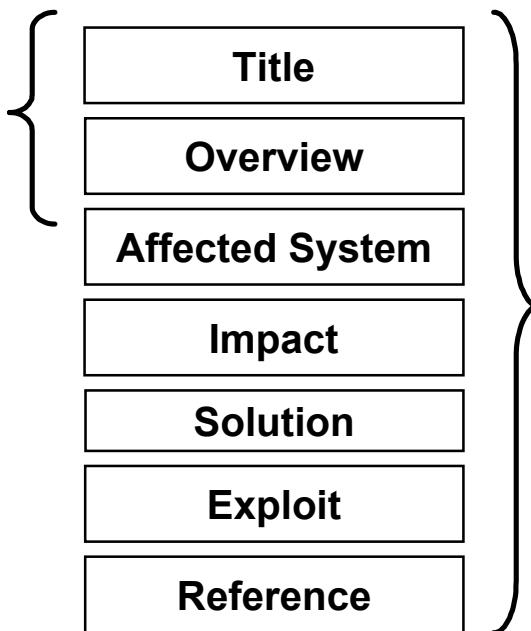
**Distribution designed to encourage
reusing of PUBLIC security information**

**More efficient aggregation of PUBLIC
security information from product vendors**

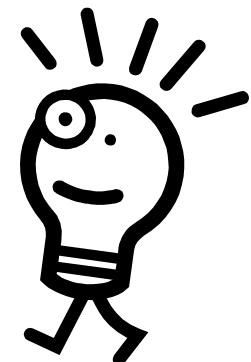


- Keywords for the solution
 - Semantic Web
 - RSS (RDF Site Summary)

Format for
the overview
JVNRSS



Format for
the details
VULDEF
and others



Using JVNRSS, an XML format to describe the overview, is an essential point in the security information exchange.

JVNRSS

Please refer to JVNRSS spec

<http://jvnrss.ise.chuo-u.ac.jp/jtg/jvnrss/>

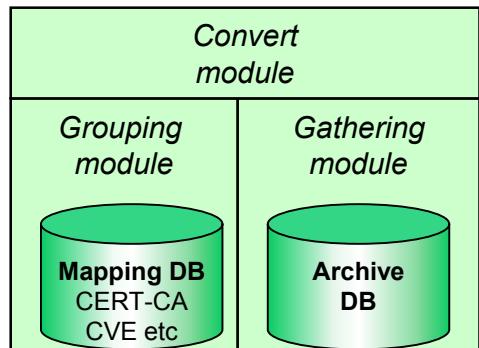
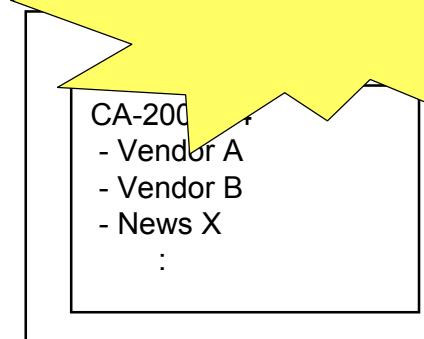
```
<item rdf:about="URL of security information">
  <title>Title</title>
  <link>URL of security information</link>
  <description>Outline of security information</description>
  <dc:publisher>Product vendor name</dc:publisher>
  <dc:creator>Contact point information</dc:creator>
  <dc:identifier>Security information ID</dc:identifier>
  <dc:relation>Relational ID (1) {CVE|CERT-CA|CERT-VU|etc.}</dc:relation>
  <dc:relation>Relational ID (2) {CVE|CERT-CA|CERT-VU|etc.}</dc:relation>
  <dc:relation>          :          : </dc:relation>
  <dc:date>Date last updated</dc:date>
  <dcterms:issued>Date first published</dcterms:issued>
  <dcterms:modified>Date last updated</dcterms:modified>
</item>
```

- **ID:** JVNVU#834865
- **Title:** Sendmail contains a race condition
 - **Reference:** <http://www.us-cert.gov/cas/techalerts/TA06-081A.html>
 - **Reference:** <http://www.kb.cert.org/vuls/id/834865>
 - **Reference:** <http://cve.mitre.org/cgi-bin/cvename.cgi?name=2006-0058>

```
<item rdf:about="http://jvn.jp/cert/JVNVU%23834865">
  <title>Sendmail contains a race condition</title>
  <link>http://jvn.jp/cert/JVNVU%23834865</link>
  <description>A race condition in Sendmail may allow a remote attacker ... </description>
  <dc:publisher>JVNRSS-DEV project</dc:publisher>
  <dc:creator>jvn@jvn.jp</dc:creator>
  <dc:identifier>JVNVU#834865</dc:identifier>
  <dc:relation>http://www.us-cert.gov/cas/techalerts/TA06-081A.html</dc:relation>
  <dc:relation>http://www.kb.cert.org/vuls/id/834865</dc:relation>
  <dc:relation>http://cve.mitre.org/cgi-bin/cvename.cgi?name=2006-0058</dc:relation>
  <dc:date>2006-04-03T10:30+09:00</dc:date>
  <dcterms:issued>2006-03-23T04:00+09:00</dcterms:issued>
  <dcterms:modified>2006-04-03T10:30+09:00</dcterms:modified>
</item>
```

The grouping mechanism using Relational ID without mapping

(3) Cor. Grouping Completed



(2) Grouping of the security information.

CA-2003-04

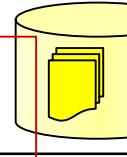
match

YES

(1) Gathering of the security information

Vendor A Site

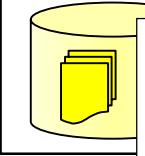
Microsoft SQL Slammer Worm



```
<item rdf:about=" http://A.JP/alert-sql.html ">
<title>SQL Slammer worm information</title>
<link>http://A.JP/alert-sql.html</link>
<dc:relation>CA-2003-04.html</dc:relation>
</item>
```

News X Site

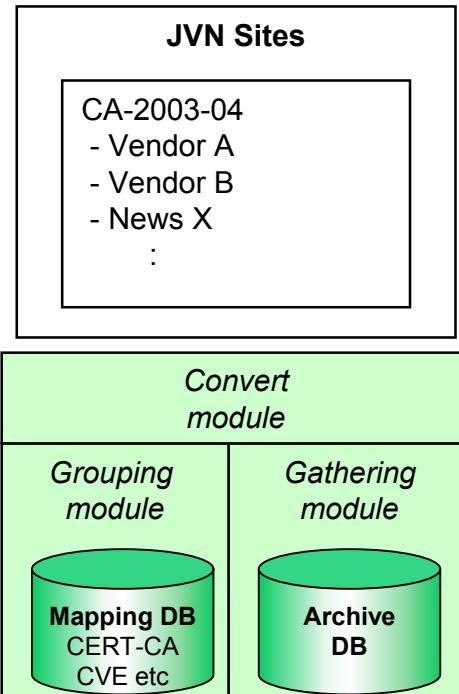
SQL Slammer worm information



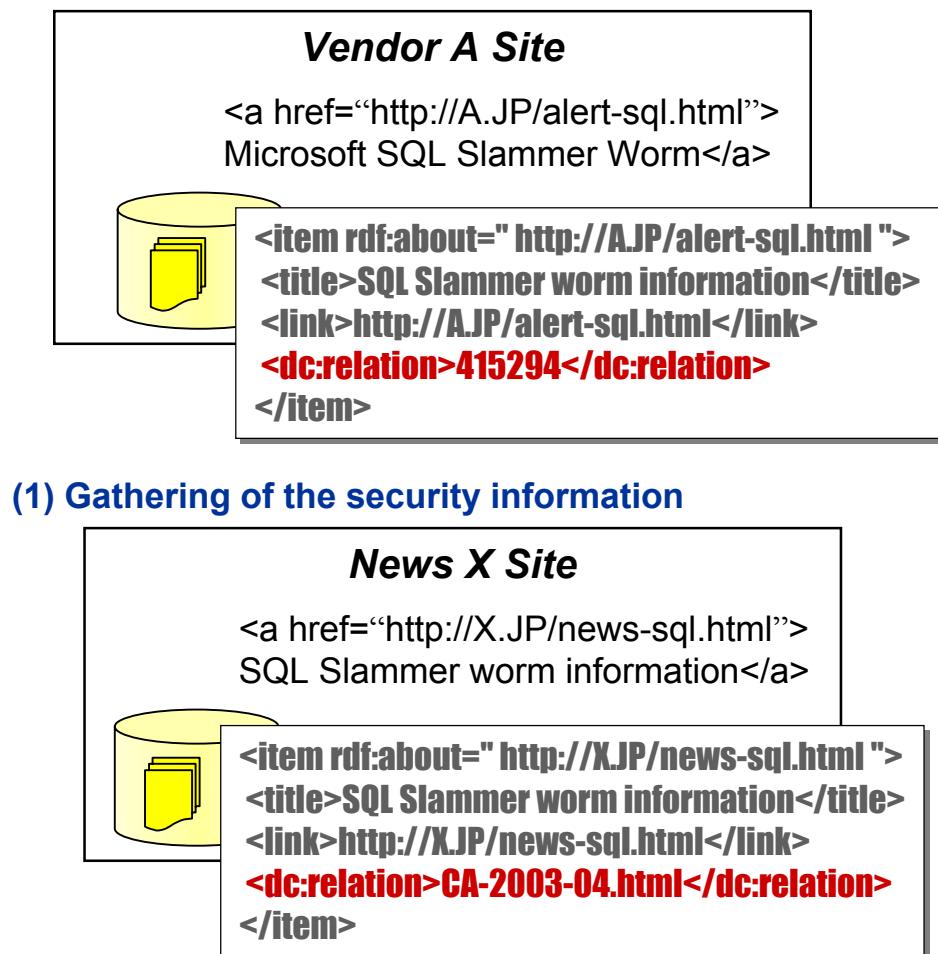
```
<item rdf:about=" http://X.JP/news-sql.html ">
<title>SQL Slammer worm information</title>
<link>http://X.JP/news-sql.html</link>
<dc:relation>CA-2003-04.html</dc:relation>
</item>
```

□ The grouping mechanism using Relational ID with mapping DB.

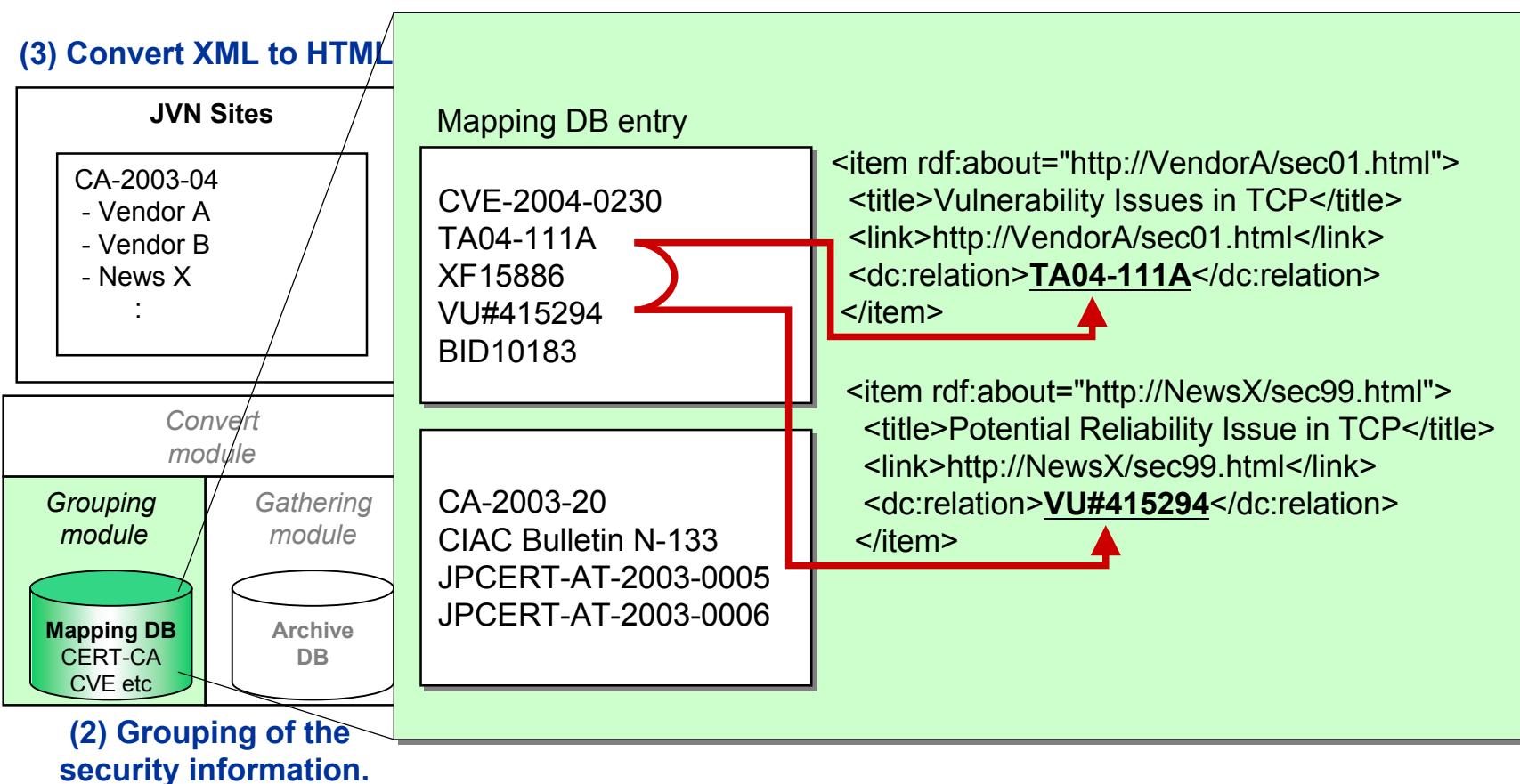
(3) Convert XML to HTML



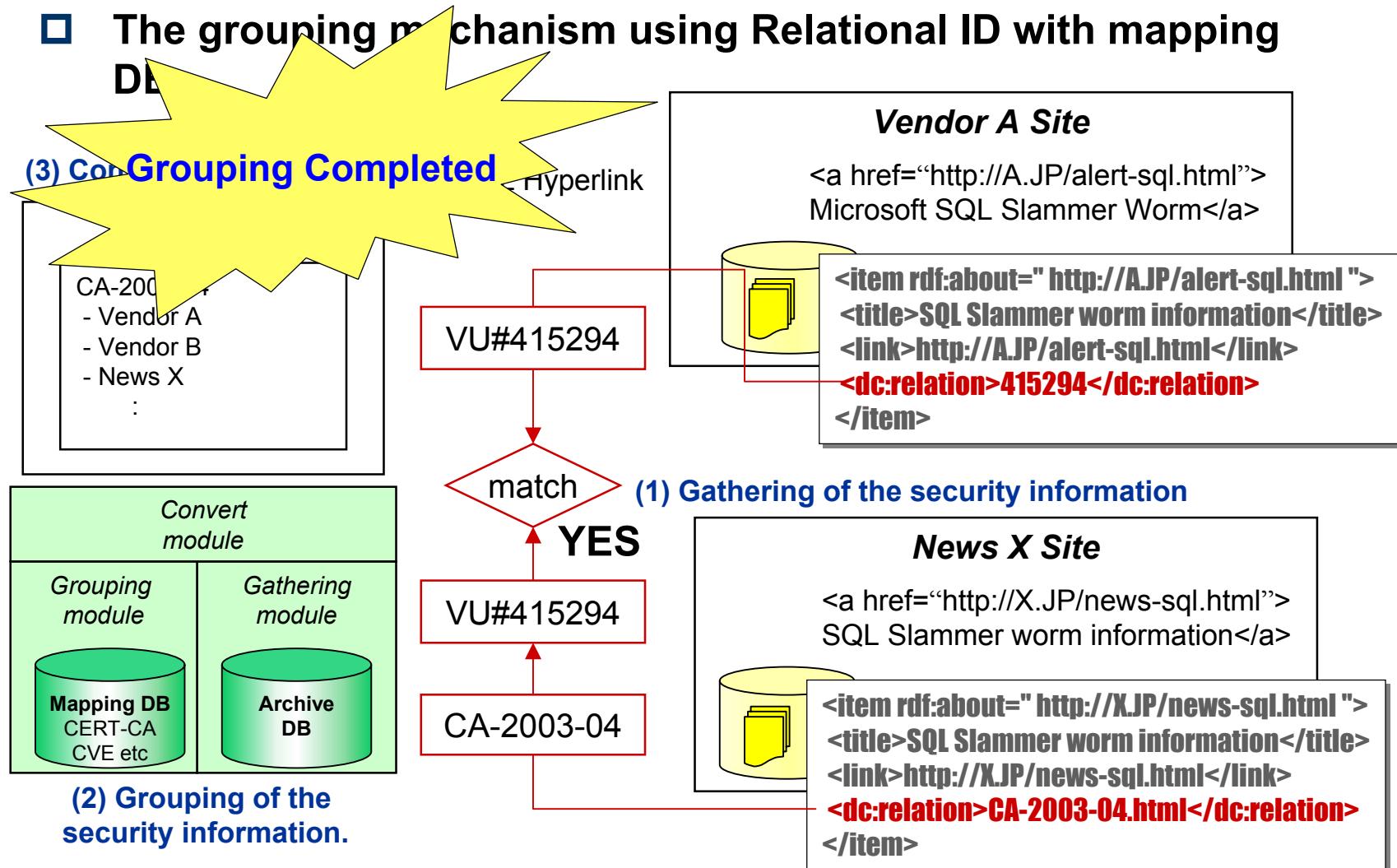
(2) Grouping of the security information.



□ The grouping mechanism using Relational ID with mapping DB.



□ The grouping mechanism using Relational ID with mapping



CVE+

[http://jvnrss.ise.chuo-u.ac.jp/jtg/cve+/-](http://jvnrss.ise.chuo-u.ac.jp/jtg/cve+/)

CVE+ is to make a relationship map between CVE and Japanese security information.

 TRnotes

<http://jvnrss.ise.chuo-u.ac.jp/jtg/trn/>

TRnotes provides HTML based information, JVNRSS format and Visualized TRnotes.

 XSL_swf

<http://jvnrss.ise.chuo-u.ac.jp/jtg/xswf/>

XSL_swf is FLASH tool for visualized JVNRSS and uses a part of XSL as a mechanism to describe how the document should be displayed.

 RSS_dir

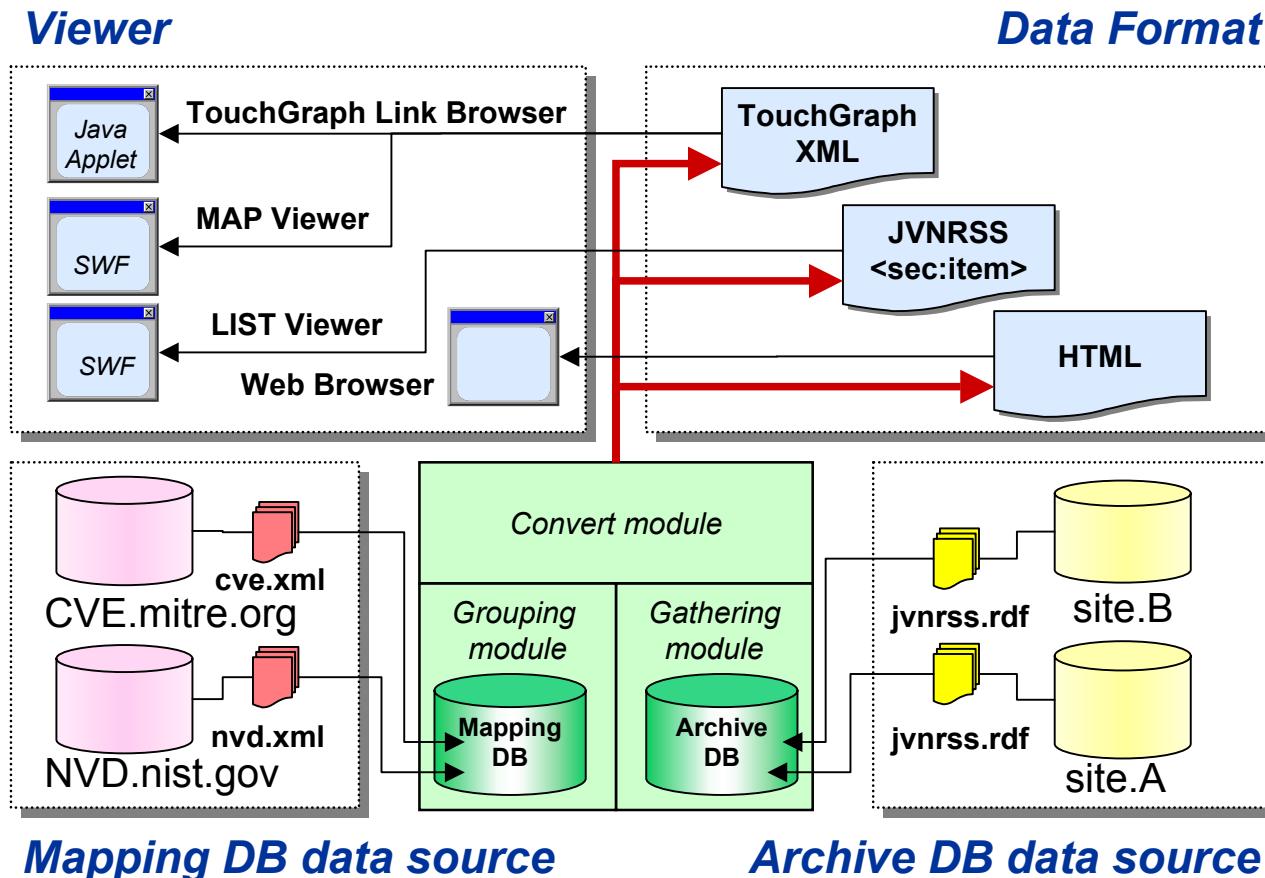
<http://jvnrss.ise.chuo-u.ac.jp/jtg/rssd/>

RSS_dir is concept of RSS directory for RSS channel. RSS directory describes a RSS channel tree with RSS format.

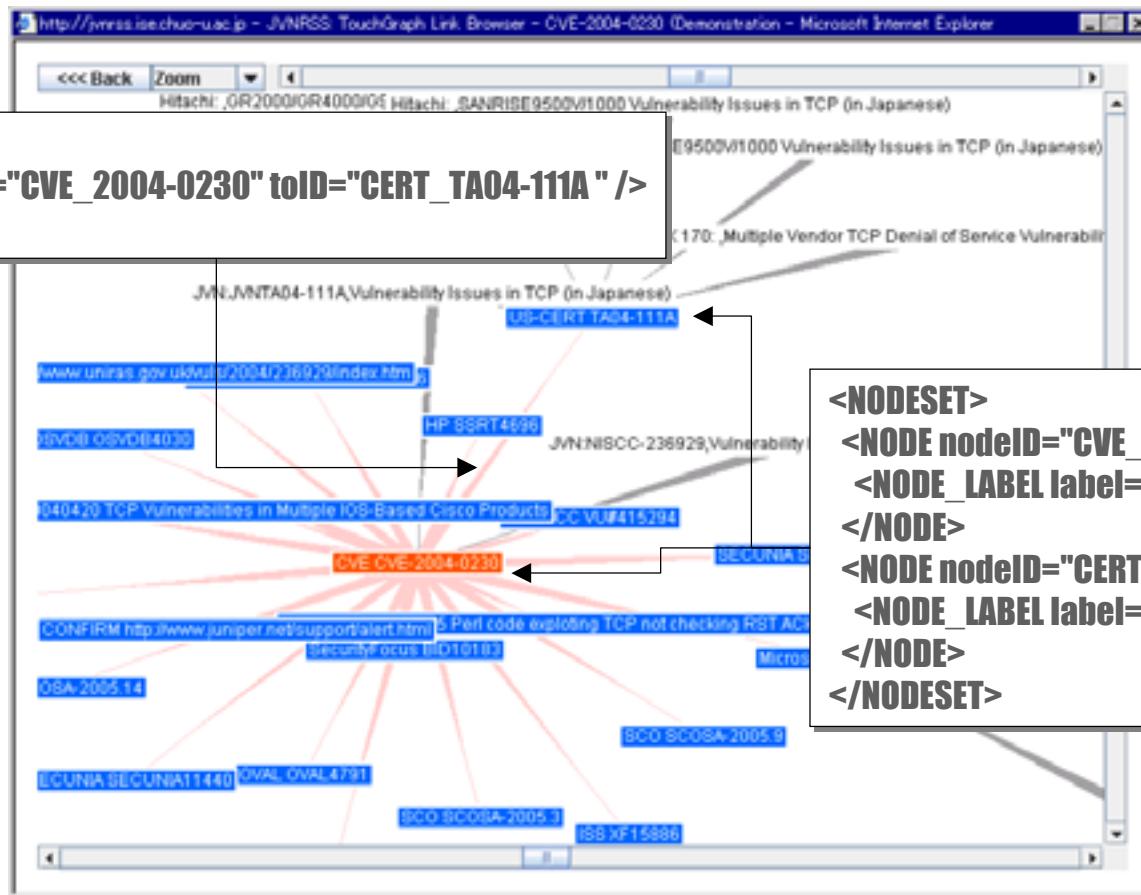
 SIG_rdf

<http://jvnrss.ise.chuo-u.ac.jp/jtg/xsig/>

- Prototype system
 - **Modules:** gathering, grouping and convert



- **Viewer:** TouchGraph Link Browser (Java Applet)
 - **Data Format:** TouchGraph XML format



- **Viewer:** LIST Viewer (SWF)
- **Data Format:** JVNRSS + <sec:item> format

The screenshot shows the JVNRSS List Viewer application running in Microsoft Internet Explorer. The main window displays a list of vulnerabilities under the heading "CVE 2004-0230 Extension (CVE+ project: Demonstration Example)". The list includes items such as "BID10183 : BID10183", "20040425 Perl code exploiting TCP not checking RST ACK : 20040425 Perl code exp...", and "TA04-111A : TA04-111A". One specific item, "JVNTA04-111A : Potential Reliability Issue in TCP (in Japanese)", is highlighted with a yellow background. On the left side of the interface, there is a sidebar with a red border containing the XML-like code for this specific item. Red arrows point from the highlighted item in the main list to the corresponding code block on the left.

```

<item rdf:about="http://www.us-cert.gov/cas/ ... ">
<title>TA04-111A</title>
<sec:item>
<item rdf:about="http://jvn.jp/cert/JVNTA04-111A">
<title>Potential Reliability Issue in TCP</title>
</item>
<item rdf:about="http://www.hitachi.co.jp/ ... ">
<title>GR2000/GR4000/GS4000/GS3000 ...</title>
</item>

</sec:item>
</item>

```

PUBLISHER:
JVN
DATE:
2005-04-01T10:00+09:00

CVE-2004-0230 : CVE-2004-0230

JVNTA04-111A : Potential Reliability Issue in TCP (in Japanese)
NISCC-236929 : Potential Reliability Issue in TCP (in Japanese)

Archive DB data source

- in Japanese (lang=ja)
 - http://www.hitachi.co.jp/hirt/security/archive2003.rdf
 - http://www.hitachi.co.jp/hirt/security/archive2004.rdf

I want to more data sources.

&

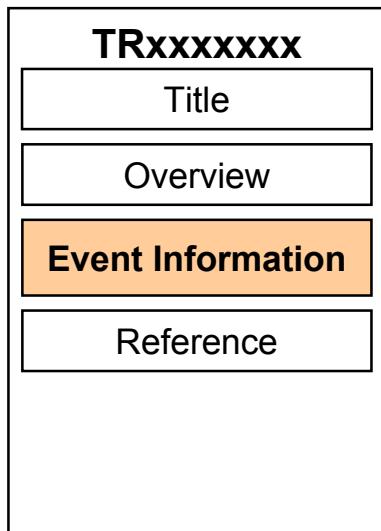
**Let's make a mechanism
for PUBLIC security information exchange.**

- http://www.hitachi.co.jp/hirt/security/archive2005.rdf
- http://www.hitachi.co.jp/hirt/security/archive2006.rdf

Please refer to CVE+

[http://jvnrss.ise.chuo-u.ac.jp/jtg/cve+/-](http://jvnrss ise chuo-u ac jp/jtg/cve+/)

- “Status Tracking Notes (TRnotes)” includes a list of event/time information on incidents concerning vulnerabilities.
 - Each web page consists of the overview, timeline concerning a vulnerability and related information.
 - The purpose of TRnotes is in sharing the timeline of the incident, which includes worm activities, the date exploit codes were released and the countermeasure against security incidents. The information is based on public information.



Event Information includes followings.

- Date the vulnerability was discovered
- Date any advisories are released
- Date exploit codes are published
- Date worms are produced
- Published alerts from governments.
- Additional resources, such as a government agency
- etc.

JP Vulnerability Notes - Status Tracking Note TRTA04-260A - Microsoft Internet Explorer

ファイル(F) 編集(E) 表示(V) お問い合わせ(T) ツール(U) ヘルプ(H)

About JVN
VN-JP
VN-CERT/CC
VN-NISCC
TRnotes
Product Vendor List

Related Sites
JPCERT/CC
ISDAS
IPA/SEC
Report a Vulnerability
CERT/CC
NISCC
CVE

Status Tracking Notes

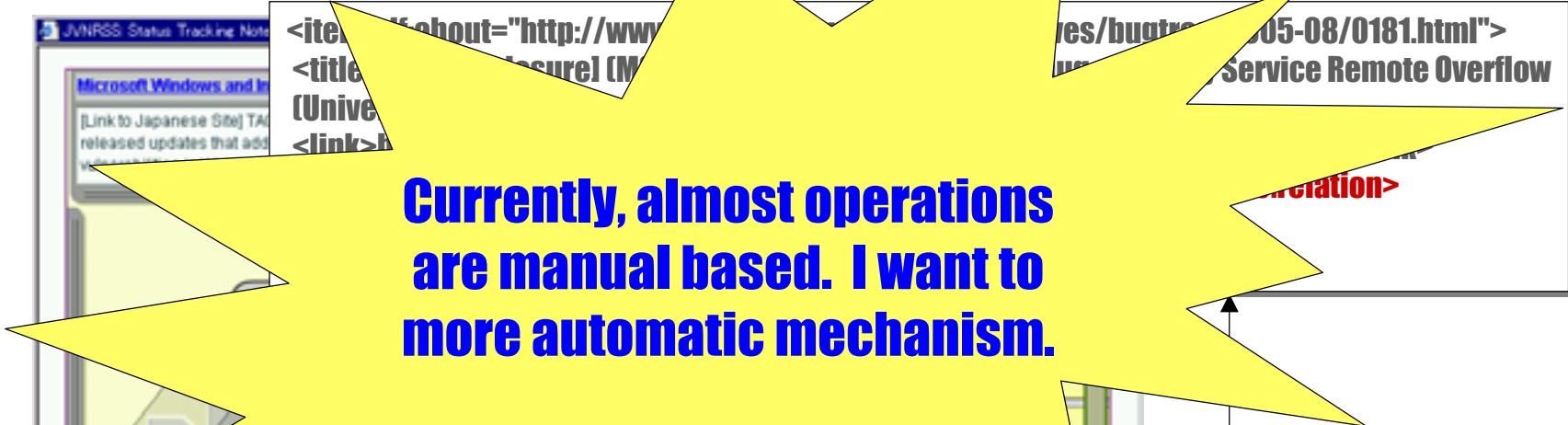
TRTA04-260A

Microsoft Windows JPEG component buffer overflow

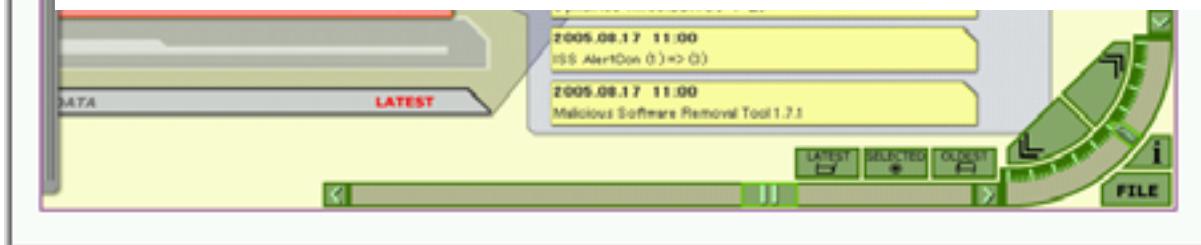
Event List

Time (JST)	Event Information
2004-09-15 05:22	Microsoft sent the Japanese Security information of Sep. 2004 by Email. #Post-Date: Tue, 14 Sep 2004 13:22:15 -0700
2004-09-17 04:58	US-CERT TA04-260A #Post-Date: Thu, 16 Sep 2004 15:58:16 -0400
2004-09-23 03:38	Full-Disclosure "Microsoft Windows MS04-028 JPEG Overflow Shellcoded Exploit" #Cid: ms04-28-cmd.c #Tested: Windows XP + SP1 #Post-Date: Wed, 22 Sep 2004 11:38:18 -0700 (PDT)
2004-09-23 15:22	Bugtraq "NEW GDI+ JPEG Remote Exploit" #Cid: JpegOfDeath.c #Tested: Windows XP + SP1 #Post-Date: 23 Sep 2004 06:22:54 -0000
2004-09-23 23:55	ISS AlertCon ① => ②
2004-09-24 13:49	ISSKK announces an alert "Microsoft GDI+ JPEG Processing Exploitation". #ISSCPU: Network Sensor 22.31 #Last-Modified: Fri, 24 Sep 2004 04:49:46 GMT

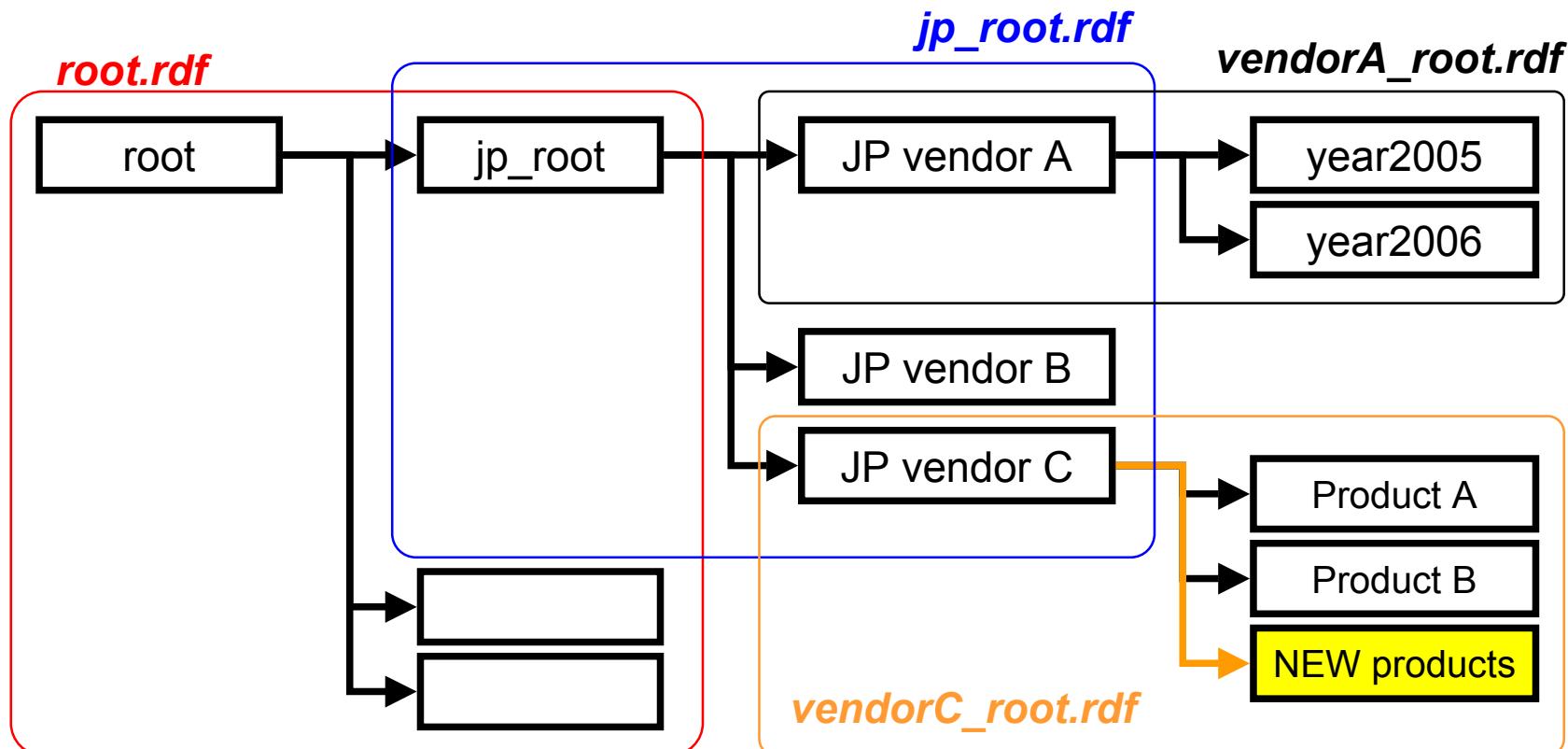
□ Visualized TRnotes: Arrange all events in time.



Please refer to TRnotes
[http://jvnrss.ise.chuo-u.ac.jp/jtg/trn/](http://jvnrss ise chuo-u ac jp/jtg/trn/)



- RSS_dir is a concept of the RSS directory for the RSS channel.
RSS directory describes a RSS channel tree using the RSS format.
 - Check the feed for changes and react to the changes in an appropriate way



- ❑ Use RSS_dir to selectively display the information collected/updated in the last 7 days



Title	Date
41. undefined : Cisco Security Advisory: AVS TCP Relay Vulnerability	2006-05-10
42. undefined : Public Exploit Code for Unpatched Vulnerability in Oracle	2006-05-03
43. undefined : Cisco Unity Express Expired Password Reset Privilege Escalation	2006-05-01
44. undefined : Cisco VPN 3000 Concentrator Vulnerable to Crafted HTTP Attack	2006-04-26
45. HS06-006 : Groupmax Mail Client Processing Is Stopped by an Email Attachment File	2006-04-26
46. HS06-007 : Vulnerability of DoB in JPI Products	2006-04-26
47. undefined : Public Exploit Code for a Vulnerability in Sendmail	2006-04-20

Updated in the last 7 days

Channel	Hitachi Security Information	
No.	ID	Title
45	HS06-006	Groupmax Mail Client Processing Is Stopped by an Email Attachment File
Date		Publisher
2006-04-26T00:00+09:00		Hitachi Ltd.
Description		
undefined		

- ❑ Use RSS_dir to selectively display the information collected/updated in the last 7 days

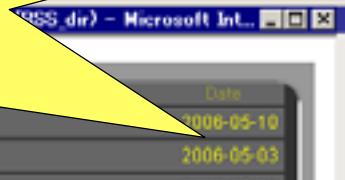
jp_root.rdf

IP root

**Let's make more machine
readable environment for
PUBLIC security information
exchange to reduce
workloads.**

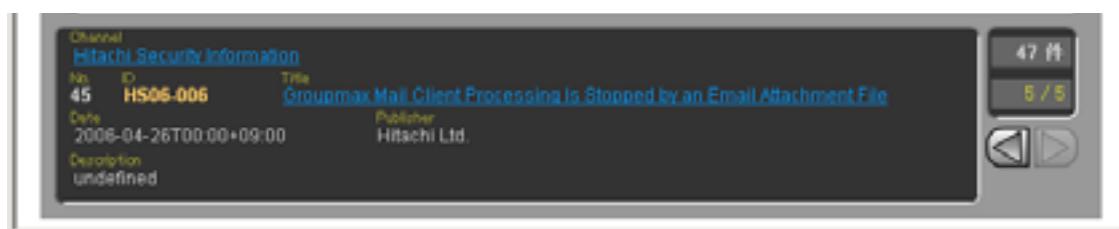
add top layer RDF

2nd layer RDFs



Please refer to **RSS_dir**

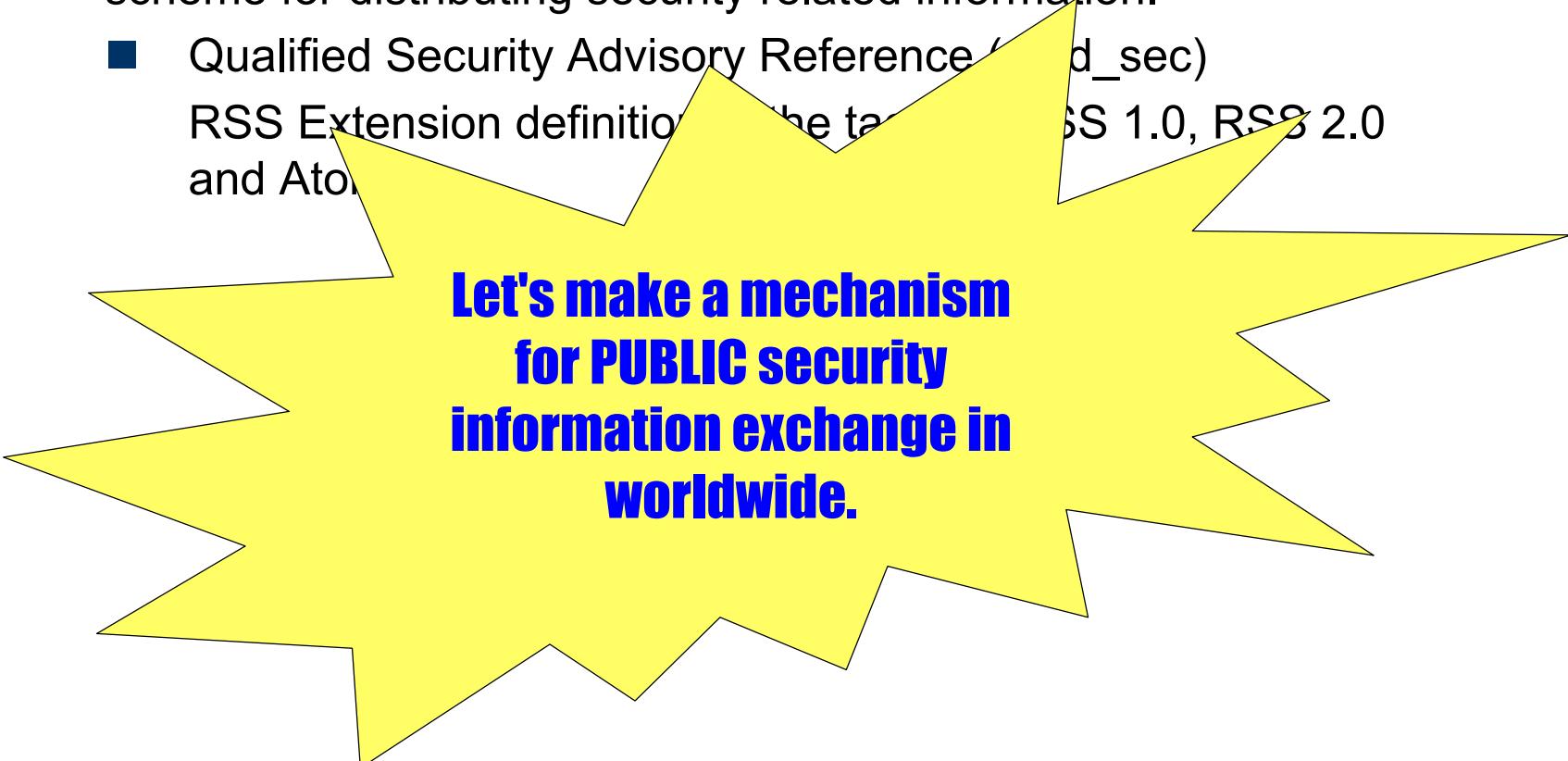
[http://jvnrss.ise.chuo-u.ac.jp/jtg/rssd/](http://jvnrss ise chuo-u.ac.jp/jtg/rssd/)



3.

Proposal RSS Extension

- JVNRSS is based RSS 1.0 and a proprietary format in Japan.
 - Exchange security information in worldwide.
 - The ability to use RSS holds the key to successfully implement a scheme for distributing security related information.
 - Qualified Security Advisory Reference (QSA_sec)
- RSS Extension definition is the target of RSS 1.0, RSS 2.0 and Atom.



**Let's make a mechanism
for PUBLIC security
information exchange in
worldwide.**

- sec:references is an element for a best reference (CVE, CERT Advisory, CERT Vulnerability Note, US-CERT Technical Alert etc.) to related security information.
- Syntax

<sec:references sec:source="%name" sec:id="%id">
%ResourceReference</sec:references>

- **%name**

An attribute is abbreviation name, which provides the best reference, such as CVE, JPCERT, CERT, CIAC, BID, CERT-VN, MS, OSVDB, XF etc.

- **%id**

An attribute is the unique identifier assigned by sec:source, such as VU#105259, MS01-044, CVE-2001-0525, CA-2001-14, TA05-111A etc.

- **%ResourceReference**

An entity value is a URI reference to a resource.

3.

MOD_SEC: sec:identifier

- sec:identifier is an element for the unique identifier assigned by vendor.
- Syntax

</sec:identifier>%id</sec:identifier>

- %id

An attribute is the unique identifier assigned by vendor, such as "Cisco Security Advisory ID#50960", HPSBMA01234 etc.

- **ID:** JVNTA06-109A
- **Title:** Oracle Products Contain Multiple Vulnerabilities
 - **Reference:** <http://www.us-cert.gov/cas/techalerts/TA06-109A.html>

```
<entry>
  <title>Oracle Products Contain Multiple Vulnerabilities</title>
  <link rel="alternate" type="text/html" href="http://jvn.jp/cert/JVNTA06-109A/">
  <id>http://jvn.jp/cert/JVNTA06-109A/</id>
  <summary type="text">Oracle products and components are affected by multiple
  vulnerabilities. </summary>
  <published>2006-04-20T11:30+09:00</published>
  <updated>2006-04-21T15:00+09:00</updated>
  <author>
    <name>JVN</name>
    <email>jvn@jvn.jp</email>
    <uri>http://jvn.jp/</uri>
  </author>
  <sec:identifier>JVNTA06-109A</sec:identifier>
  <sec:references sec:source="CERT" sec:id="TA06-109A">
    http://www.us-cert.gov/cas/techalerts/TA06-109A.html
  </sec:references>
</entry>
```

3.

JVNRSS: Please send your commnets to me.

**Please access my feasibility study site
and send your comments (typo,
discussions and questions etc.) to me.**

**[http://jvnrss.ise.chuo-u.ac.jp/](http://jvnrss ise chuo-u ac jp/)
E-mail: jvn@jvn.jp or
terada@sdl.hitachi.co.jp**

Reference

- **IPA (Information-technology Promotion Agency, Japan)**
 - <http://www.ipa.go.jp/english/about/index.html>
 - <http://www.ipa.go.jp/english/security/index.html>
- **JPCERT/CC**
 - <http://www.jpcert.or.jp/english/>
- **JVN (JP Vendor Status Notes)**
 - <http://jvn.jp/> (Japanese)
 - <http://www.ipa.go.jp/english/security/third.html>
- **JVNRSS (JP Vendor Status Notes RSS) Feasibility Study Site**
 - <http://jvnrss.ise.chuo-u.ac.jp/jtg/>

Ending

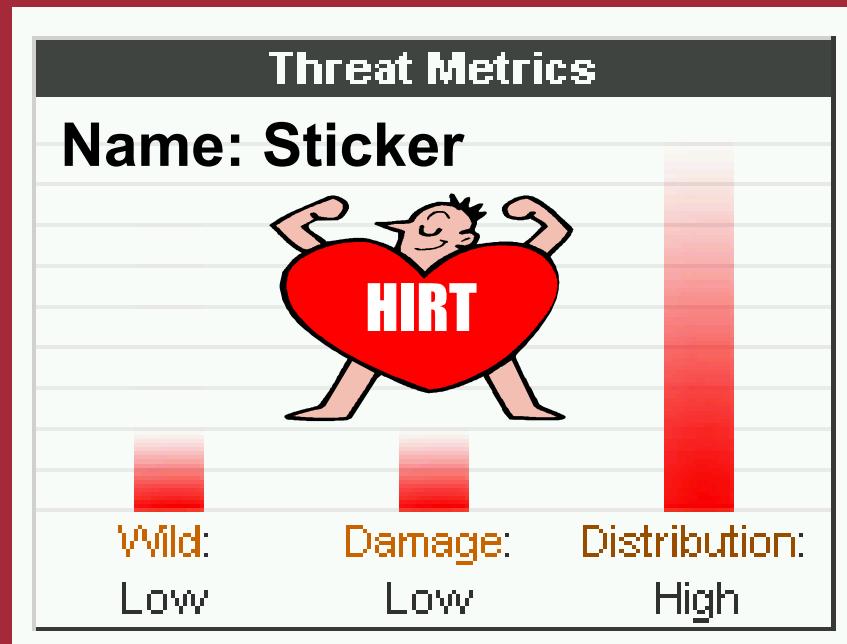
We propose "JVNRSS" to solve the problems and improve the security information exchange for security administrators. JVNRSS is based on RSS 1.0 and use the field <dc:relation> of Dubline Core as index of grouping security information. This presentation has discussed the specification of JVNRSS and the application, especially the gathering and grouping approach for the security information exchange. Furthermore, we introduce RSS extension of security information exchange.

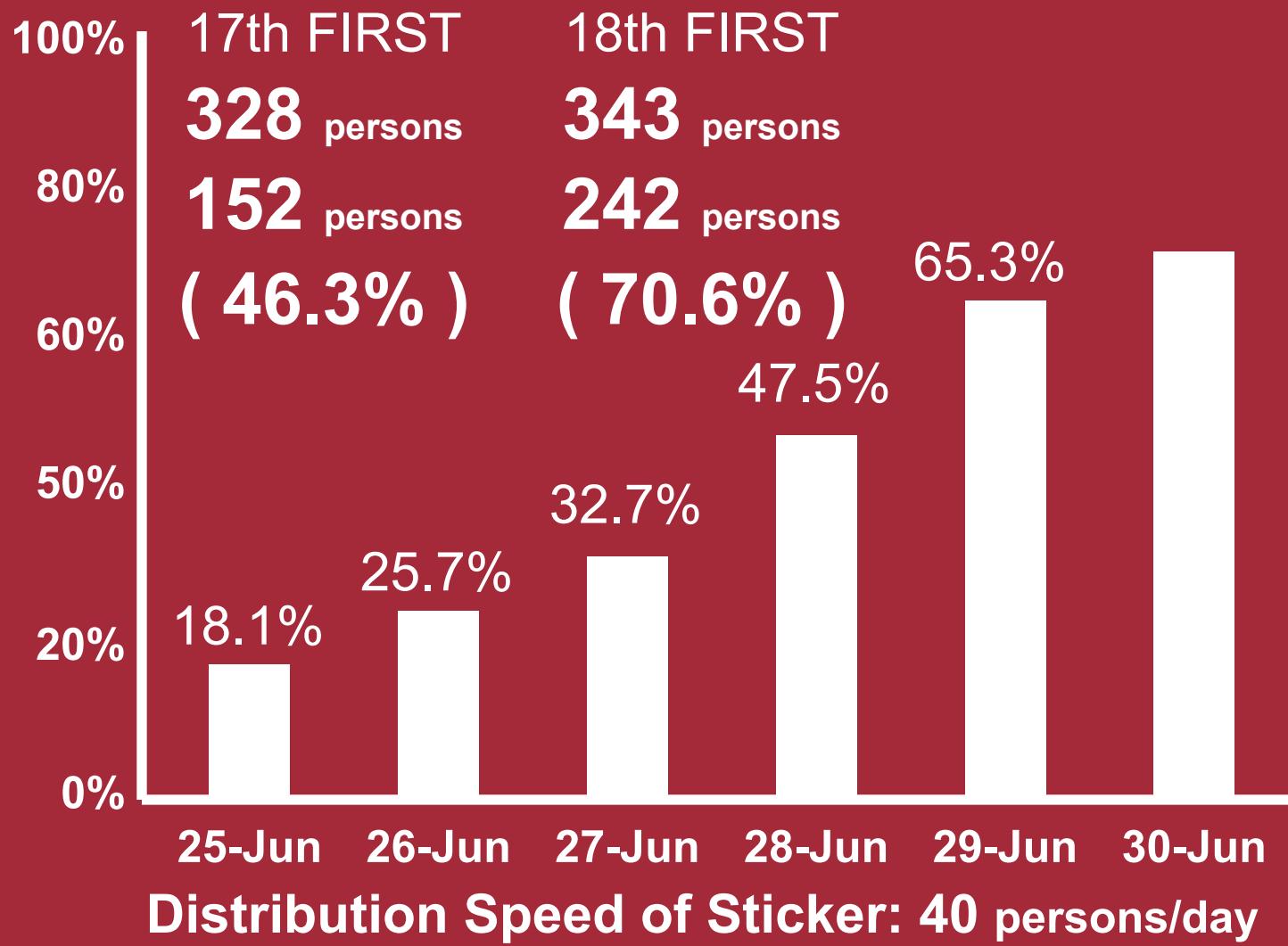
Epilogue

My project summary

Project Name: Talking with all participants.

Period: Jun 25, 2006 - Jun 30, 2006 (6 days)







INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN



Thank you

Proposal of RSS Extension for Security Information Exchange

2006/06/30

Masato Terada
office@jpcert.or.jp
<http://jvn.jp/>

IPA (Information-technology Promotion Agency, Japan)
JPCERT/CC (Japan Computer Emergency Response Team Coordination Center)