IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

JPCERT CC

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

2003 - current
Associate staff
JPCERT/CC

April 2002 - March 2006
Graduate student
Keio University

IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

JPCERT CC

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.

IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

JPCERT CC

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.

IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

JPCERT CC

Proposal of RSS Extension for Security Information Exchange

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

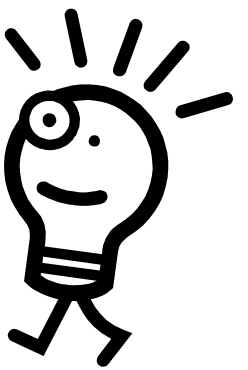
3. JVNRSS (JP Vendor Status Notes RSS)

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

Format for the overview ***JVNRSS***

- **Title**
- **Overview**
- **Affected System**
- **Impact**
- **Solution**
- **Exploit**
- **Reference**

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>
 <dscription>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</cterms:issued>
  <dcterms:modified>Date last updated</dcterms:modified>
</item>
```

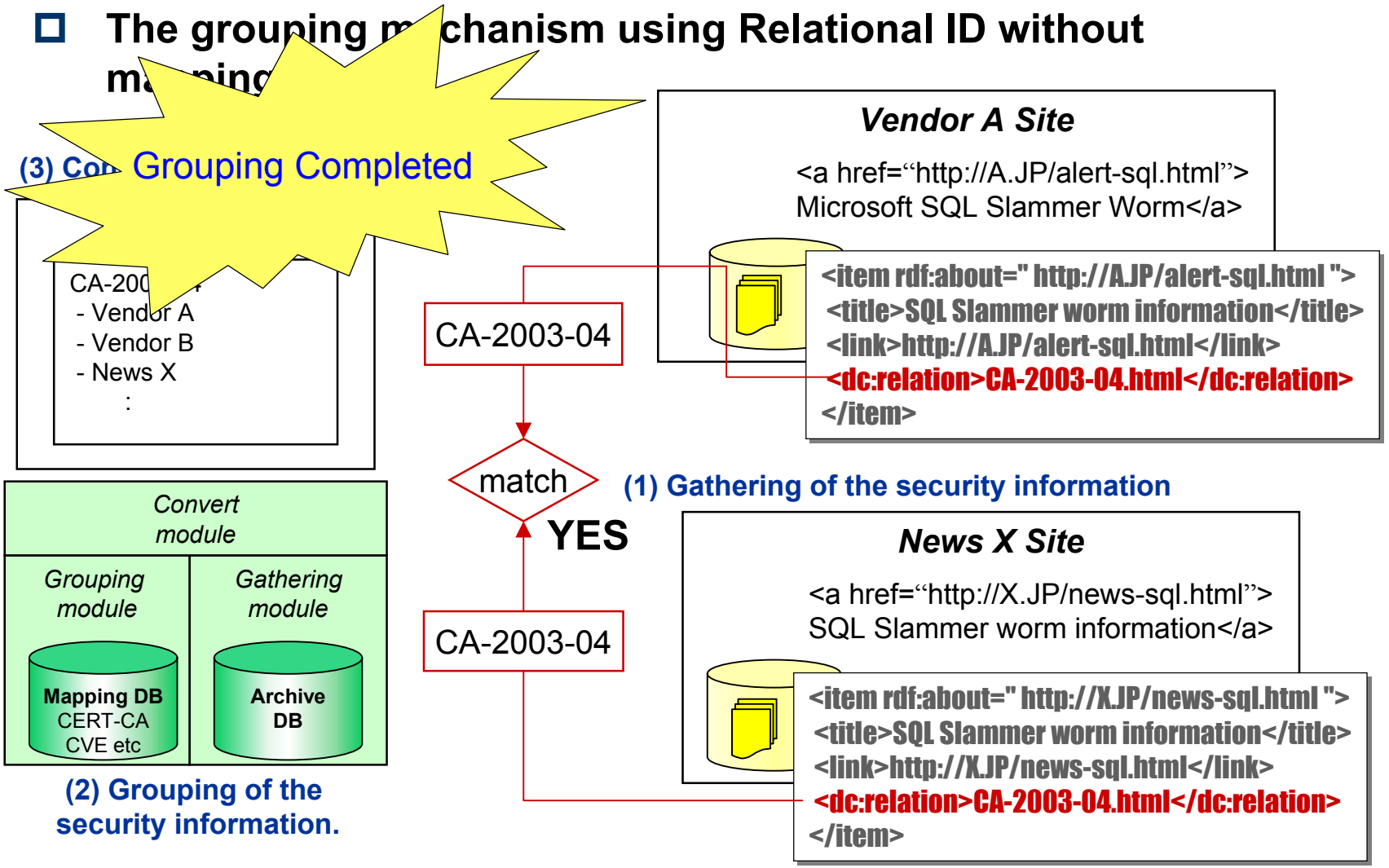
3. JVNRSS Example

- ***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>
```

3. JVNRSS: Proposal grouping (correlation) mechanism

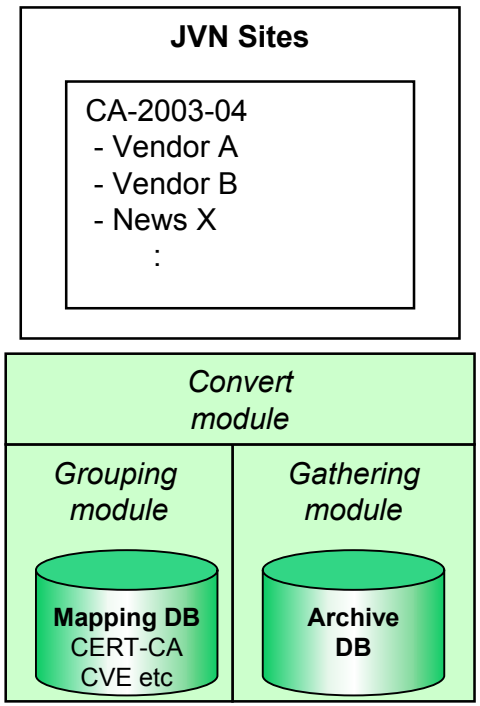
- **The grouping mechanism using Relational ID without mapping**



3. JVNRSS: Proposal grouping (correlation) mechanism

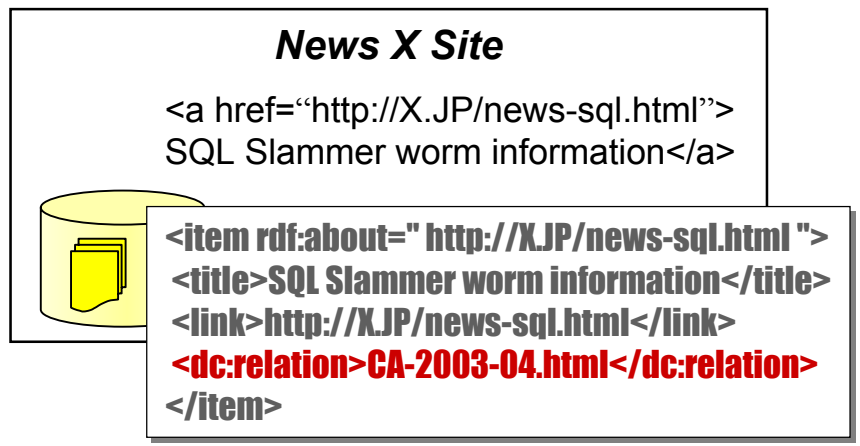
- **The grouping mechanism using Relational ID with mapping DB.**

(3) Convert XML to HTML



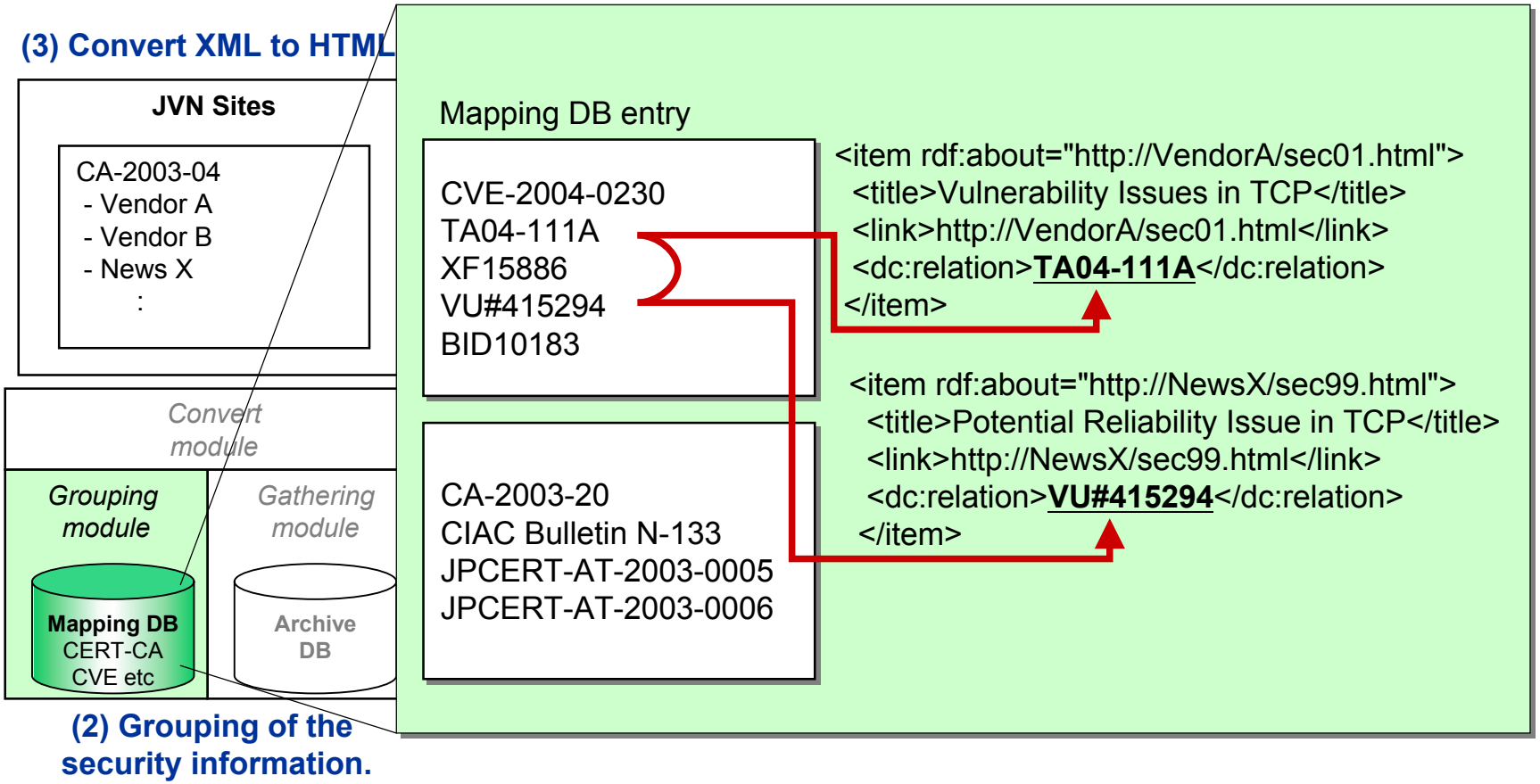
(2) Grouping of the security information.

(1) Gathering of the security information



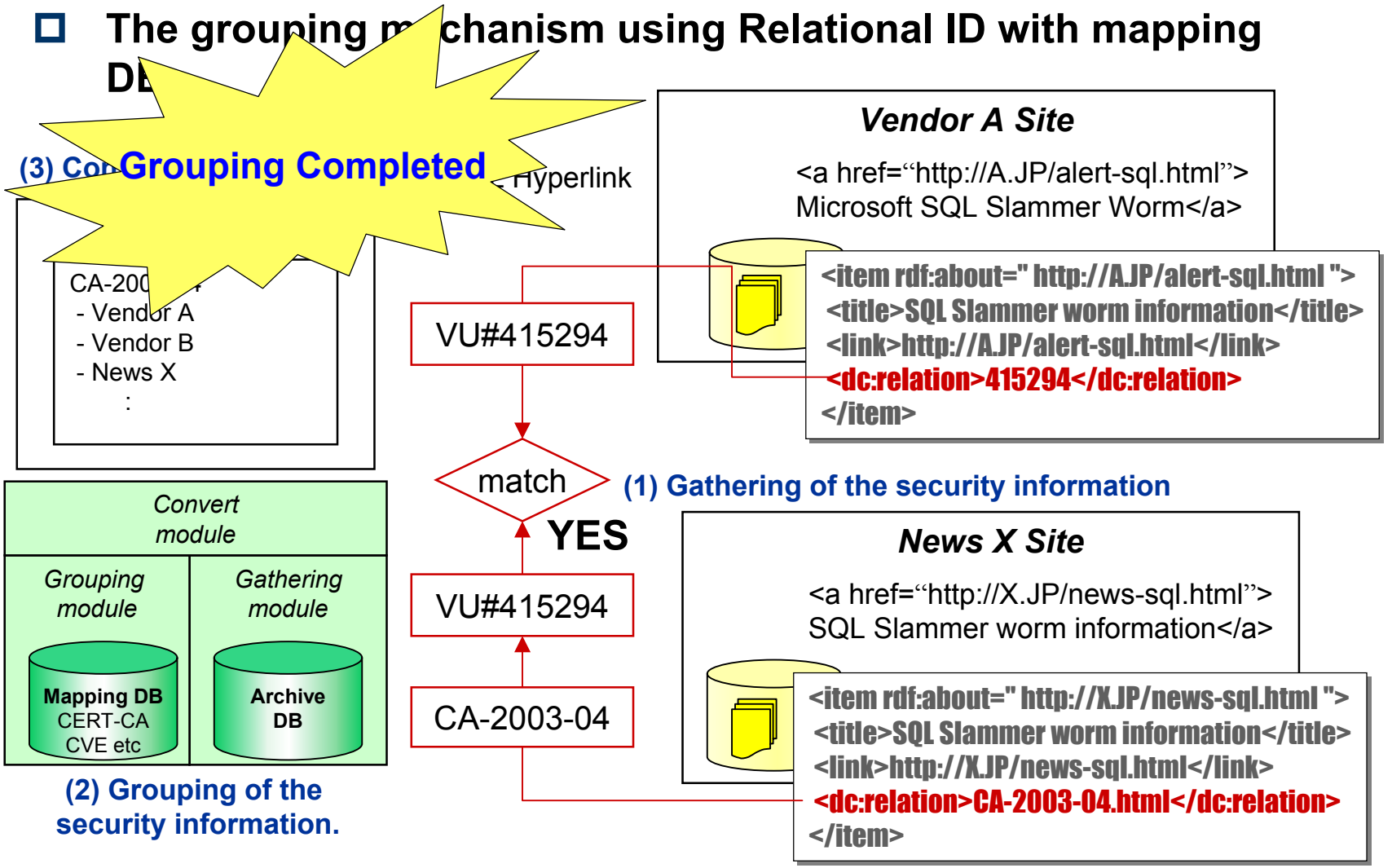
JVNRSS: Proposal grouping (correlation) mechanism

- **The grouping mechanism using Relational ID with mapping DB.**



3. JVNRSS: Proposal grouping (correlation) mechanism

- The grouping mechanism using Relational ID with mapping DB



3. JVNRSS practical activity

- ***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/

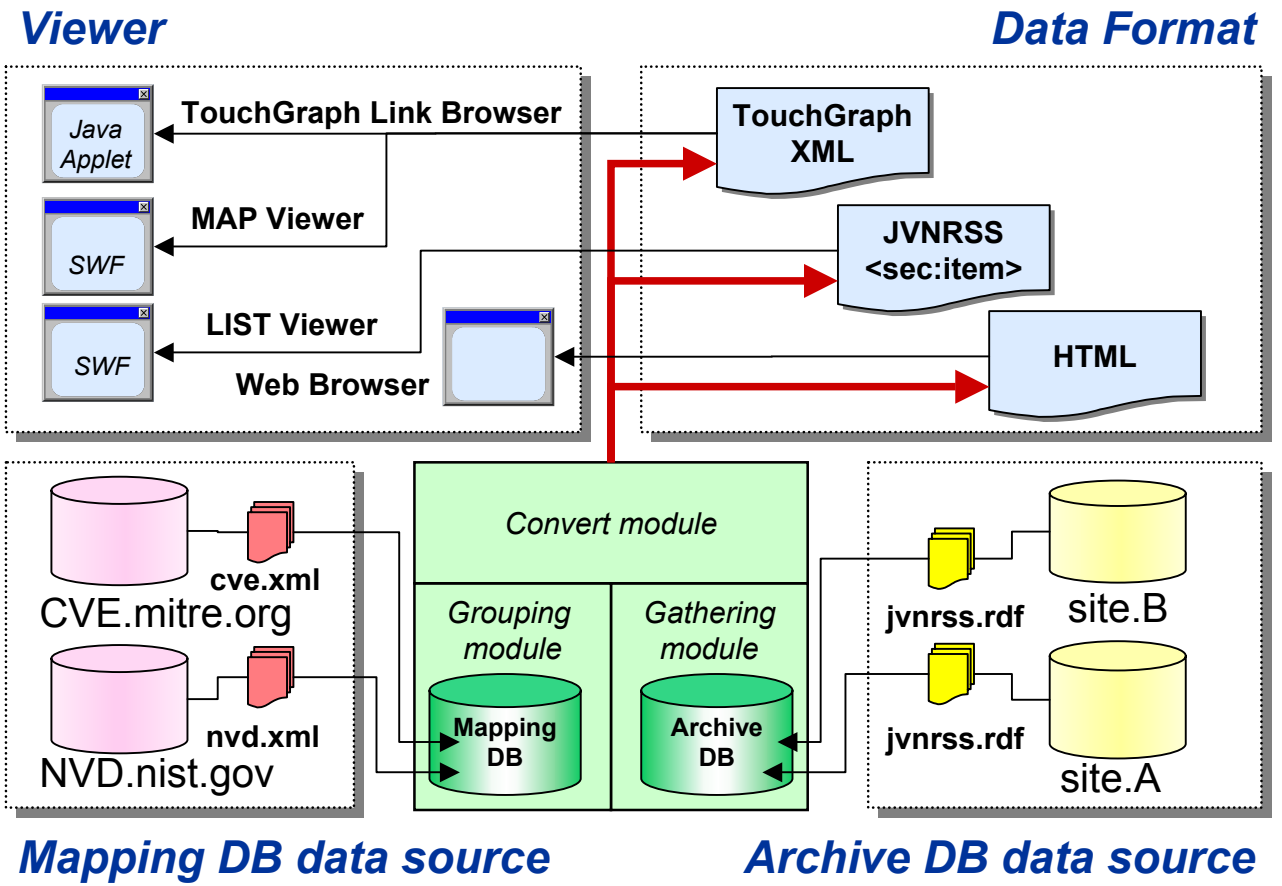
  XSL_swf is FLASH tool for visualized JVNRSS and uses a part of XSL as a mechanism to describe how the document should be displayed.

- ***RSS_dir*** http://jvnrss.ise.chuo-u.ac.jp/jtg/rssd/

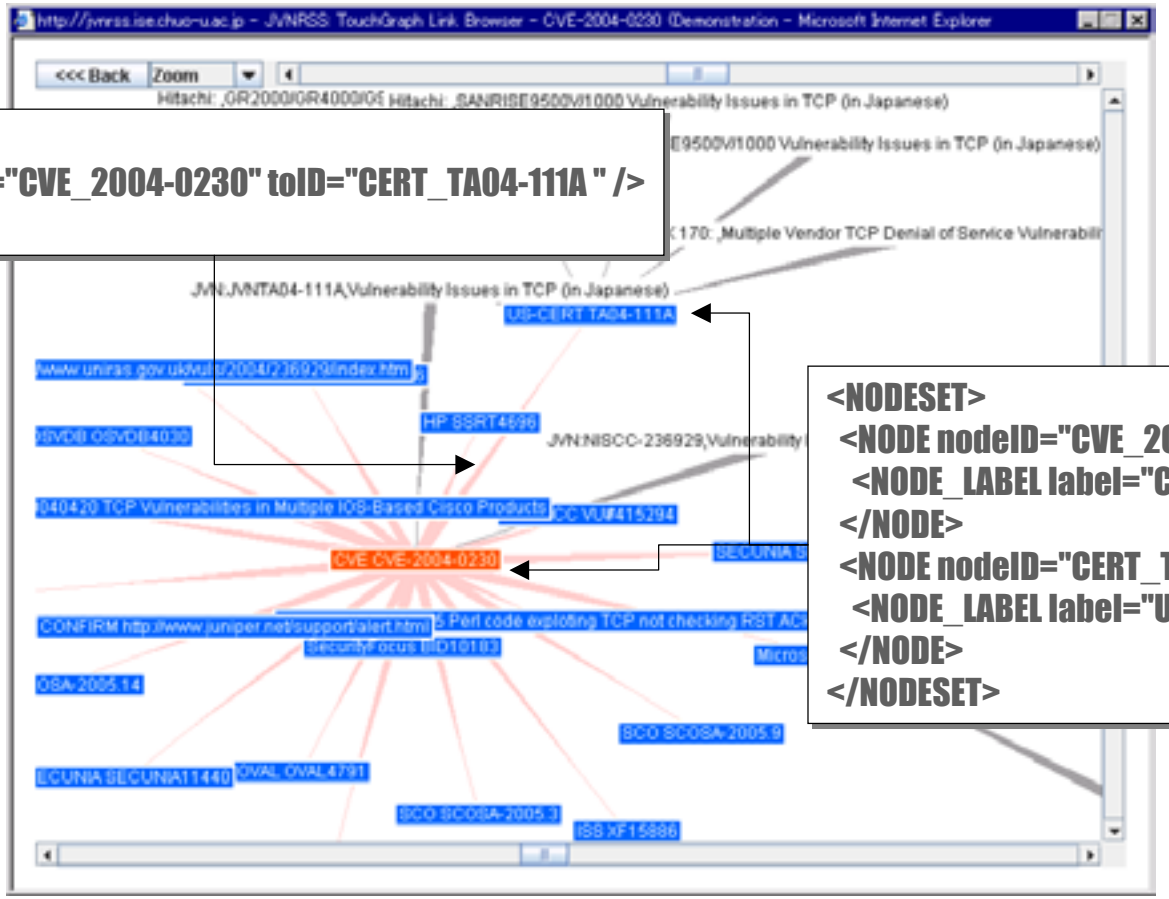
  RSS_dir is concept of RSS directory for RSS channel. RSS directory describes a RSS channel tree with RSS format.

- ***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



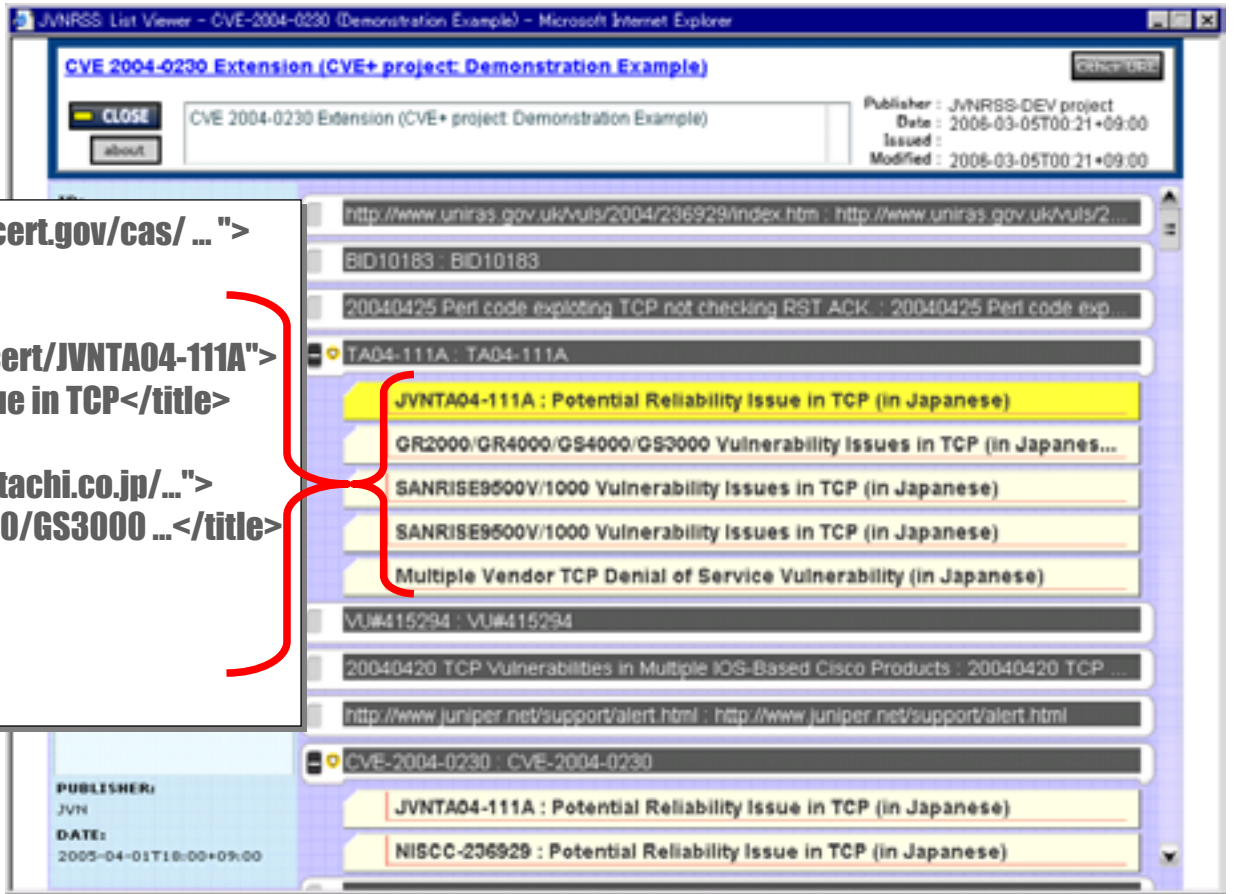

```
<EDGESET>
 <EDGE fromID="CVE_2004-0230" toID="CERT_TA04-111A " />
</EDGESET>
```

```
<NODESET>
 <NODE nodeID="CVE_2004-0230">
  <NODE_LABEL label="CVE CVE-2004-0230" />
 </NODE>
 <NODE nodeID="CERT_TA04-111A">
  <NODE_LABEL label="US-CERT TA04-111A“ />
 </NODE>
</NODESET>
```

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

```
<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>
```

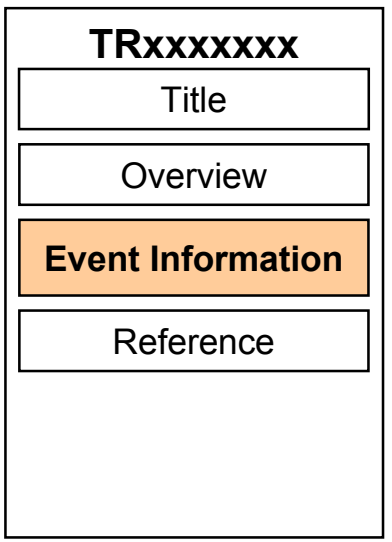


- ***Archive DB data source***
  - in Japanese (lang=ja)
    - http:
    - http://
    - rdf
    - e2003.rdf
    - urity/archive2004.rdf
    - http .hitachi.co.jp/hirt/security/archive2005.rdf
    - http://www.hitachi.co.jp/hirt/security/archive2006.rdf

I want to more data sources.
&
Let's make a mechanism
for PUBLIC security information exchange.

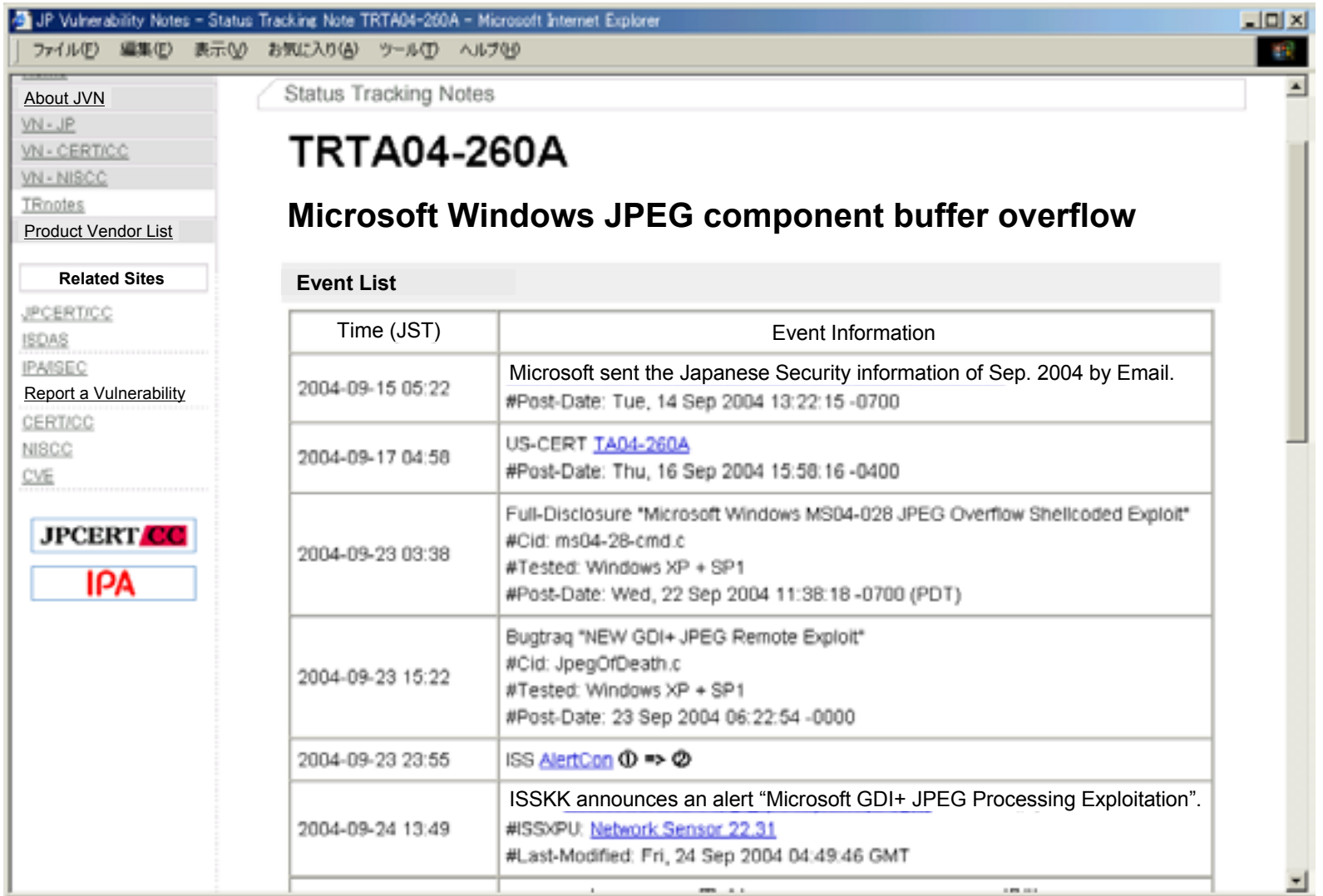
Please refer to CVE+
http://jvnrss.ise.chuo-u.ac.jp/jtg/cve+/

- “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.

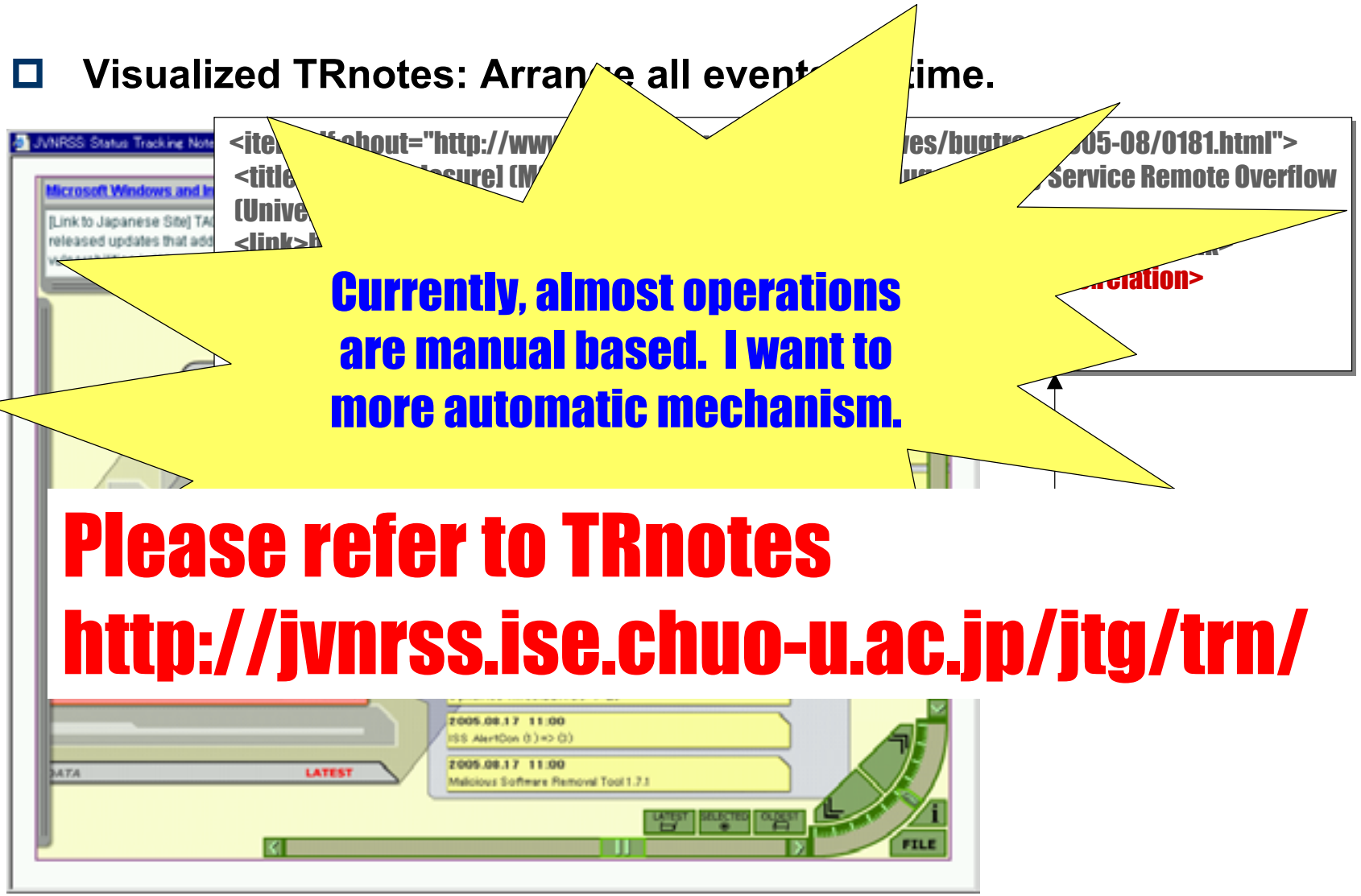


Event Information includes followings.

- Date the vulnerability was discvered
- 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.

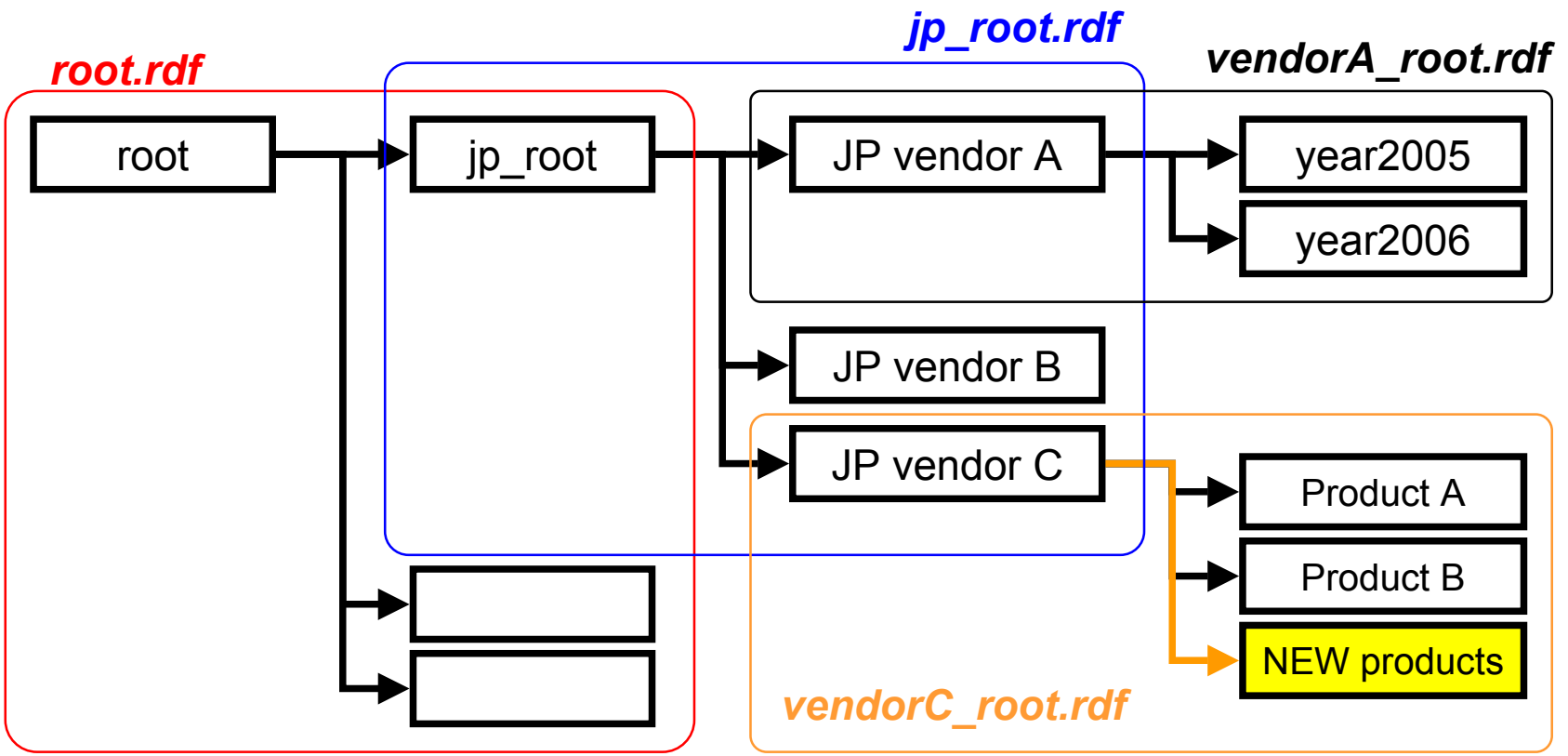


- Visualized TRnotes: Arrange all events in time.

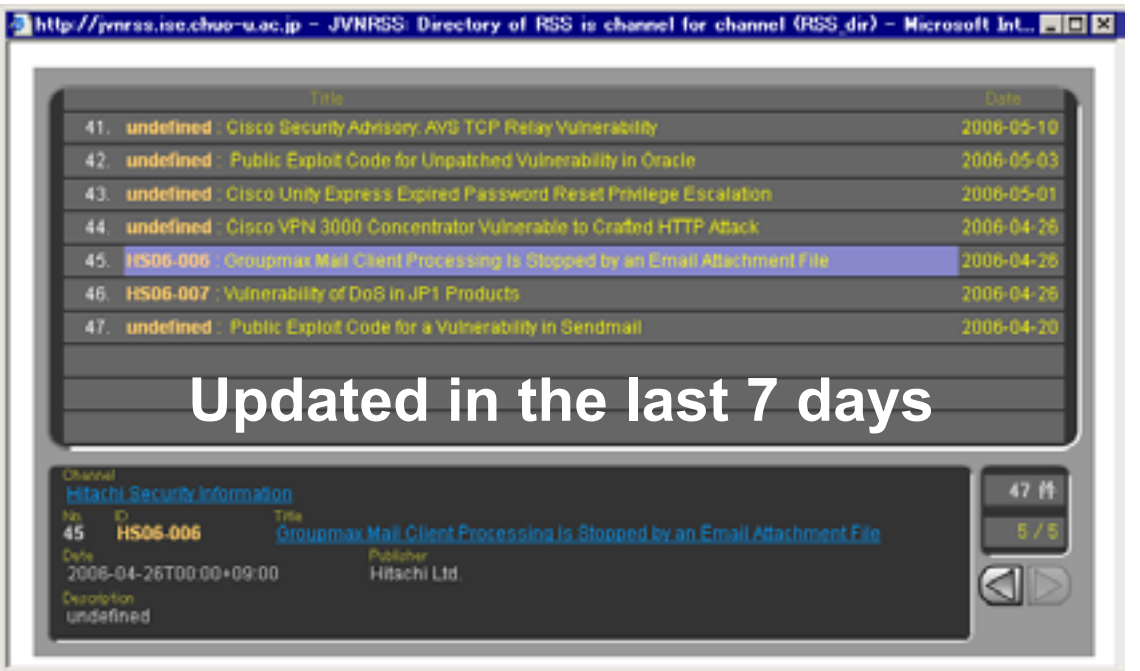


RSS_dir

- 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



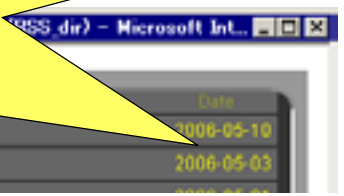
- Use RSS_dir to selectively display the information collected/updated in the last 7 days

jp_root.rdf

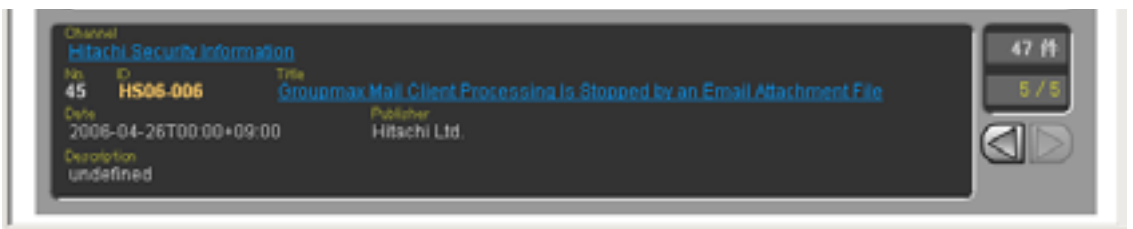
...ad top layer RDF

...2nd layer RDFs

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



Please refer to RSS_dir 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 (d_sec)

    RSS Extension definitio he ta SS 1.0, RSS 2.0 and Ato

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

3. MOD_SEC: sec:references

- 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.

3. MOD_SEC: Example
Atom + <sec:identifier> and <sec:references>

- ***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/
E-mail: jvn@jvn.jp or terada@sdl.hitachi.co.jp

IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

JPCERT CC

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/

IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

JPCERT CC

Ending

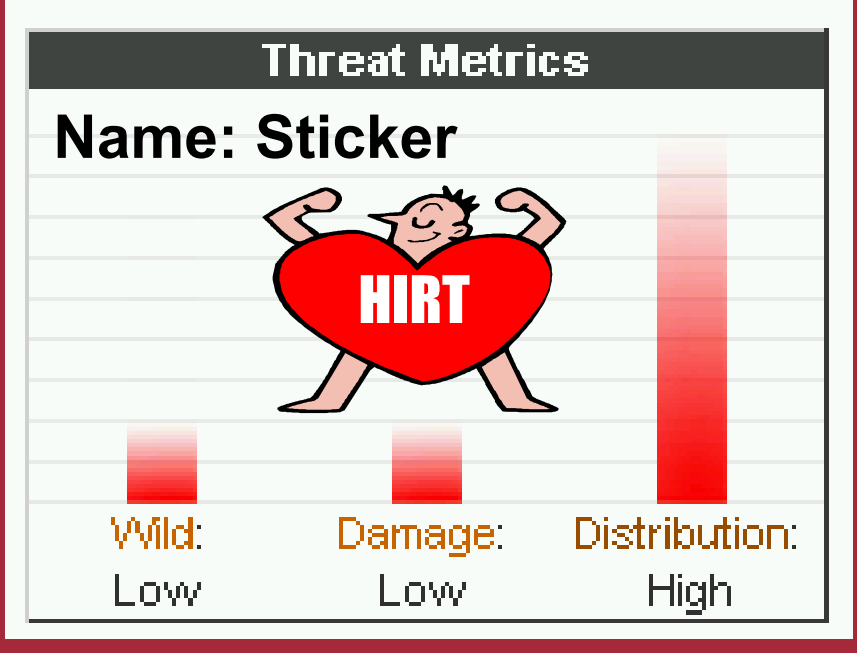
We propose "JVNRSS" to solve the problems and improve the security information exchange for security administrators. JVNRSS is based on RSS 1.0 and use the field <dc:relation> of Dubline Core as index of grouping security information. This presentation has discussed the specification of JVNRSS and the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

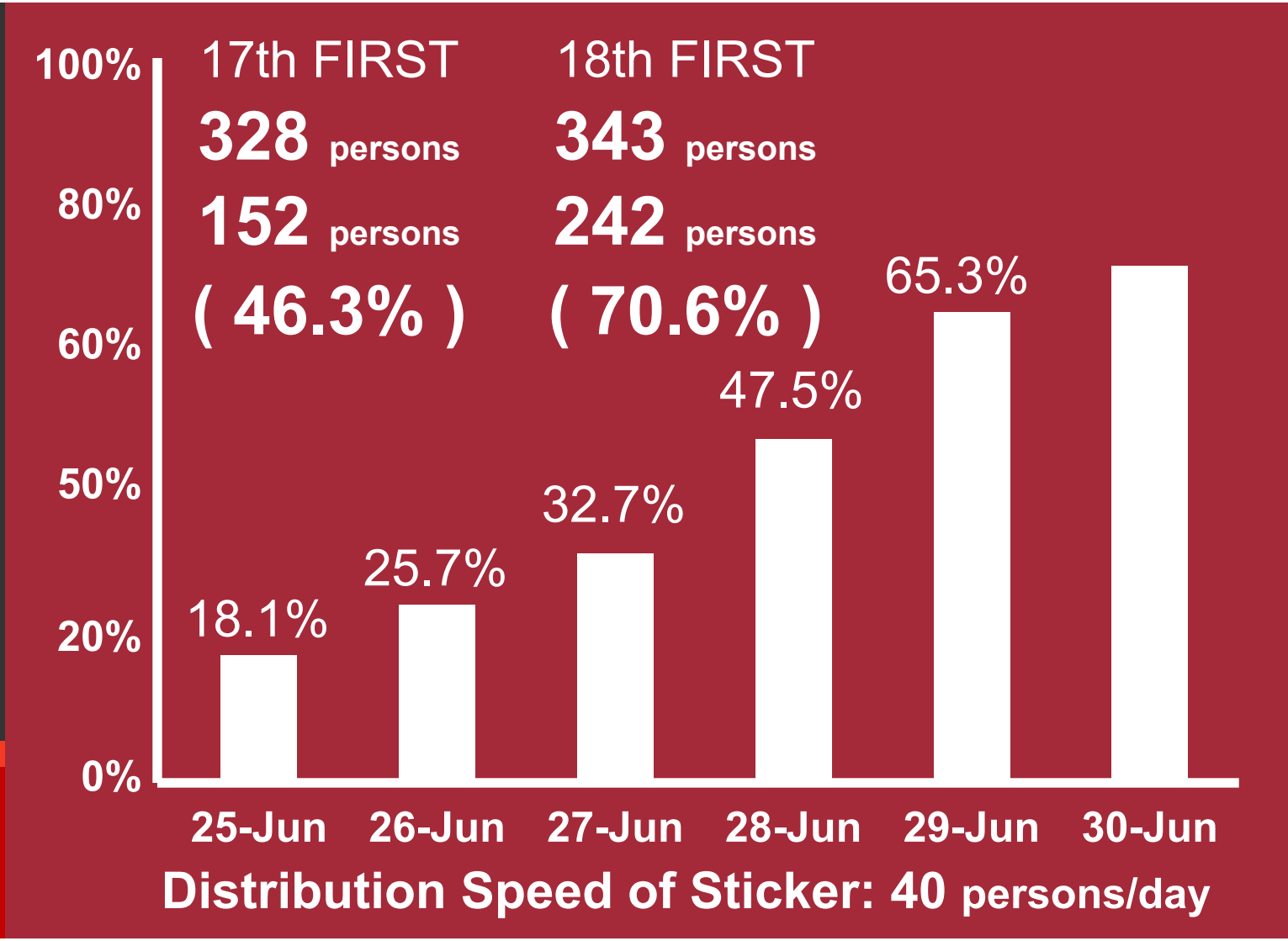
Epilogue

My project summary

Project Name: Talking with all participants.

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





HITACHI
Inspire the Next

IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

JPCERT CC

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)