情報処理学会 コンピュータセキュリティ シンポジウム 2006, pp.85-90 (Oct.25-27, 2006)

JVNRSS を用いた脆弱性対策情報の流通

寺田真敏[†1,†2]　宮崎清隆[†3]　山岸　正[†1]　土居範久[†4]

[†1)] 情報処理推進機構 (IPA)
〒113-6591　東京都文京区本駒込 2-28-8
[†3)] JPCERT コーディネーションセンター
〒101-0054　東京都千代田区神田錦 3-17
[†4)] 中央大学大学院 理工学研究科
〒112-8551　東京都文京区春日 1-13-27

概要：対策情報は主に HTML ベースの情報として構成されているために，脆弱性対策情報を展開する際に，Web サイトから情報を集め必要な部分を抽出して再構成する操作や集めてきた情報のグループ化操作など，情報の再活用において柔軟さが欠けている．本稿では，共通の書式でドキュメントの見出し，要約などのリストを提供する JVNRSS(JP Vendor Status Notes RDF Site Summary)を用いたセキュリティ情報の流通を提案すると共に，その試行について述べる．
キーワード：セキュリティ，脆弱性，JVNRSS

Proposal of JVNRSS for security information exchange

Masato Terada[†1†2]　Kiyotaka Miyazaki[†3]　Tadashi Yamagishi[†1]　Norihisa Doi[†4]

[†1)] Information-technology Promotion Agency. 2-28-8 Honkomagome, Bunkyo, Tokyo, 113-6591 Japan
[†3)] Janan Computer Emergency Response Team Coordination Center.
3-17 Kanda-nishikicho, Chiyoda, Tokyo 101-0054, Japan
[†4)] Graduate School of Science and Engineering, Chuo University.
1-13-27 Kasuga, Bunkyo-ku, Tokyo, 112-8551 Japan.

Abstract: Currently ,most of security information is deployed as Web page information on HTML base. In order to re-construct the information and perform correlation between collected information, it is necessary to improve the security information exchange environment. In this paper, firstly we will explain the specification of JVNRSS(JP Vendor Status Notes RDF Site Summary). Secondly, we will introduce our feasibility study on JVNRSS for security information sharing through the Internet.
Key words: Security, Vulnerability, JVNRSS

1. はじめに

国内においても，JVN(JP Vendor Status Notes)，製品開発ベンダ，コミュニティなど様々な層での脆弱性対策情報の提供が充実し始めている．しかし，対策情報は主に HTML ベースの情報として構成されているために，脆弱性対策情報を展開する際に，Web サイトから情報を集め必要な部分を抽出して再構成する操作や集めてきた情報のグループ化操作など，情報の再活用において柔軟さが欠けている[1].

本稿では，JVN，製品開発ベンダやニュースサイトが発信する脆弱性対策情報の利活用にあたり，掲載されている脆弱性対策情報の展開を支援するという視点から，JVNRSS(JP Vendor Status Notes RDF Site Summary)を用いた 2 つの課題解決の試行について述べる．

- 対策情報表示支援
  対策情報をセキュリティ情報発信サイト，各製品開発ベンダ，ニュースサイトなどの他サイトに掲載可能な形式で発信する仕組みを用意することで，脆弱性対策情報の利活用を促進する．
- 対策情報収集配信支援
  情報掲載サイトからの対策情報の収集，ならびに対策情報同士を関連付けられる仕組みを用意し，脆弱性対策情報のグループ化や抽出した情報の再構成を可能とすることで利活用を促進する．

2. JVNRSS

本章では，脆弱性対策情報の展開を支援するために前提とするフォーマットである JVNRSS につ

[†2)] JPCERT コーディネーションセンター専門委員
(株)日立製作所 システム開発研究所

いて説明する[2].

JVNRSS は，サイトの概要をメタデータとして簡潔に記述する XML フォーマットである RSS (RDF Site Summary) 1.0[3]の仕様に，下記のような利用上の規約を適用した仕様である(表 1).

- Dublin Core の基本要素[4]を用いた情報提供
  - 製品開発ベンダ固有のセキュリティ情報 ID がある場合には<dc:identifier>要素に記載する.
  - 参照先情報や関連情報の URI として，普及度の高いセキュリティ情報の URL を<dc:relation>要素に記載する.
  - 更新日を<dc:date>要素に記載する.
- Dublin Core の基本要素の意味を補完するための修飾子[5]を用いた情報提供
  - 発行日を<dcterms:issued>要素に記載する.
  - 更新日を<dcterms:modified>要素に記載する.

これらの仕様規定により，現行の RSS 1.0 の仕様範囲において，Web サイトから情報を集め必要な部分を抽出して再構成する操作や集めてきた情報のグループ化操作を実現可能としている．例えば，US-CERT Technical Alert TA04-111A に基づき発信された脆弱性対策情報の場合(図 1)，これら 2 つの対策情報のタイトル (<title>要素)や URL (<link>要素)からは同じ脆弱性に関する情報であると判断できないが，参照先情報や関連情報 URI の記載された<dc:relation>要素を用いることで<item>要素をグループ化できる.

3. 対策情報表示支援の試行

本章では，JVNRSS を用いた対策情報表示支援の試行として，JVN サイトへの適用と機能拡張について述べる.

```
<item rdf:about="http://jvn.jp/cert/JVNTA04-111A">
   <title>TCP にサービス運用妨害を伴う脆弱性</title>
   <link>http://jvn.jp/cert/JVNTA04-111A</link>
   <description />
   <dc:publisher>JVN</dc:publisher>
   <dc:identifier>JVNTA04-111A</dc:identifier>
   <dc:relation>http://www.us-cert.gov/cas/techalerts/
                TA04-111A.html</dc:relation>
   <dc:date>2005-04-01T18:00+09:00</dc:date>
   <dcterms:issued>2004-04-21T06:45+09:00</dcterms:issued>
   <dcterms:modified>2005-04-01T18:00+09:00</dcterms:modified>
</item>
<item rdf:about="http://www.hitachi.co.jp/…/network/notice/TCP.html">
   <title>TCP の RST/SYN 受信に関する脆弱性に関して</title>
   <link>http://www.hitachi.co.jp/…/network/notice/TCP.html</link>
   <description />
   <dc:publisher>Hitachi Ltd.</dc:publisher>
   <dc:identifier />
   <dc:relation>http://www.us-cert.gov/cas/techalerts/
                TA04-111A.html</dc:relation>
   <dc:relation>http://jvn.jp/cert/JVNTA04-111A</dc:relation>
   <dc:date>2004-04-26</dc:date>
   <dcterms:issued>2004-04-26</dcterms:issued>
   <dcterms:modified>2004-04-26</dcterms:modified>
</item>
```

図 1　JVNRSS の item 部分の一例

3.1　JVN サイトへの適用

JVN(JP Vendor Status Notes)は，セキュリティに関わるシステム管理者ならびにシステムエンジニア向けに脆弱性対策情報を広く告知することを目的とした情報公開サイトであり，2003 年 2 月に JPCERT/CC の試行サイトとして運用を開始し[6]，2004 年 7 月には経済産業省告示「ソフトウェア等脆弱性関連情報取扱基準」[7]を受け，日本国内の製品開発者の脆弱性対応状況を公開するサイト (http://jvn.jp/)として情報発信を行なっている.
JVN サイトにおける対策情報表示支援の利用は，利用者サイト，製品開発ベンダやニュースサイトなどの他サイトにも JVN が発信する対策情報を掲

表 1　JVNRSS の item 部分の説明

項目	内容
item [必須]	個々のセキュリティ情報自身に関する基本情報で，タイトル，概要，該当する情報への URL リンクなどから構成し，rdf:about 属性には，製品開発ベンダが掲載するセキュリティ情報の URI として,掲載する各セキュリティ情報自身の URI を記載する.
title [必須]	各セキュリティ情報のタイトルを記載する.
link [必須]	掲載する各セキュリティ情報自身の URI を記載し，item 要素の rdf:about 属性で参照する URI と同値をとる.
description [オプショナル]	掲載する各セキュリティ情報自身の概要を記載する.
dc:publisher [必須]	各セキュリティ情報を発信する組織名(製品開発ベンダ名など)を記載する.
dc:creator [オプショナル]	各セキュリティ情報を発信する組織(製品開発ベンダ)の問合せ先(メールアドレスを推奨)を記載する.
dc:identifier [オプショナル]	製品開発ベンダ自身が，各セキュリティ情報に付与したセキュリティ情報 ID を記載する.
dc:relation [必須]	参照先情報や関連情報の URI として，普及度の高いセキュリティ情報の URL を記載する. 注) 該当する関連情報の URL が無い場合は NULL(空欄)とする.
dc:date [必須]	該当するセキュリティ情報を更新した日付を記載する. dc:date 要素は，dcterms:modified 要素と重複する内容であるが，多くの RSS リーダが日付情報の参照先として，dc:date 要素を利用していることから必須項目とする. なお，記述形式として，YYYY-MM-DDThh:mmTZD (eg 1997-07-16T19:20+01:00)を推奨する.
dcterms:issued [オプショナル]	セキュリティ情報の発行日と更新日を明確に分けて取り扱うことができるよう，該当するセキュリティ情報を最初に発行した日付を記載する. なお，セキュリティ情報の発行日と更新日を明確に分けて取り扱うことを推奨する.
dcterms:modified [オプショナル]	セキュリティ情報の発行日と更新日を明確に分けて取り扱うことができるよう，該当するセキュリティ情報を更新した日付を記載する. なお，セキュリティ情報の発行日と更新日を明確に分けて取り扱うことを推奨する.

載することで対策情報の利活用を促進することであり，2005 年 9 月から JVNRSS フォーマットでの情報発信を開始した．しかし，利用者サイトにおいて，JVNRSS を用いた対策情報表示支援を実現するためには，次の課題を解決する必要がある．

- JVNRSS の Web ページ掲載の容易化
  Web ページに JVNRSS フォーマットの対策情報を掲載するための作業軽減は，利活用促進の面から重要である．
- 注意喚起に併せた対策情報の注目度変更
  脆弱性に対する注目度は，時間や環境と共に変化し，たとえ深刻度の高い脆弱性であっても，修正プログラムの適用が行き渡れば注目度を低くしても良い場合もある．また，インシデント発生により脆弱性への注目度をすぐに上げなければならない場合もある．現行の JVNRSS には，脆弱性の深刻度や緊急度などの情報エントリを含んでおらず，注意喚起に併せた対策情報の注目度を変更できない．

3.2 課題解決のための機能拡張

上述の課題を解決する Web ページ上の表示ツールとその付加機能について述べる．

(1) JVNRSS Web 表示ツール

JVNRSS Web 表示ツールとは，JVNRSS フォーマットで記載されたデータをボックス，ティッカー，パネルなどの形式で Web ページ上に表示する Flash ツールである(図 3の左) . 情報を掲載したいページの所定の箇所に表示用の HTML タグを挿入すれば JVNRSS フォーマットの対策情報を Web ページに掲載できる仕様となっている．

(2) 付加機能 XSL_swf

XSL_swf は XSL(Extensible Stylesheet Language) による記述処理の一部を取り込んだ JVNRSS Web 表示ツールである．JVNRSS には深刻度や緊急度などの情報エントリを含んでいない．XSL_swf では，深刻度や緊急度に関する情報を注目度として XSL ファイルに記述しておくことで，JVNRSS の該当する項目への注目度を 3 段階(赤，黄，青)で表示できる仕様を取り込んでいる(図 3の右).

4. 対策情報収集配信支援の試行

本章では，JVNRSS を用いた対策情報収集配信支援の試行として，2006 年 6 月に開設した試行サイト[8]における JVNRSS の利用について述べる。

4.1 CVE+

CVE+は，CVE(Common Vulnerabilities and Exposures)[9]の識別番号毎に国内の脆弱性対策情報を関連付けるための取り組みである．

4.1.1 概要

CVE は，脆弱性に対して割り当てられた一意の識別番号であり，脆弱性に関連する情報同士の関連付けを行なう際の識別子としても利用されている．また，CVE を運用している米 MITRE では，CVE の識別番号毎に該当する脆弱性対策情報の URL 一覧(以下, CVE リスト)を Web サイトから発信しており，関連する対策情報を検索する際の参照先としても利用されている．

しかし，国内の製品開発ベンダが発行している対策情報の多くは，この CVE リストに登録されているわけではなく，国内を対象として販売される製品の脆弱性対策情報が CERT Advisory や CERT Vulnerability Notes Database に掲載されていないことと類似している．これは掲載可能な国内の製品開発者が少ないだけではなく，国内向けに製品開発する製品開発者にとって，海外展開していない製品の脆弱性対策情報を掲載する利点は少ないということにも起因していると思われる．

CVE+は，上記の問題を解決するために，CVE の識別番号毎に国内の脆弱性対策情報を関連付けるための取り組みであり，JVNRSS の利用は効率的に国内の製品開発ベンダの脆弱性対策情報を収集し，整理する手順の整備を目的としている．

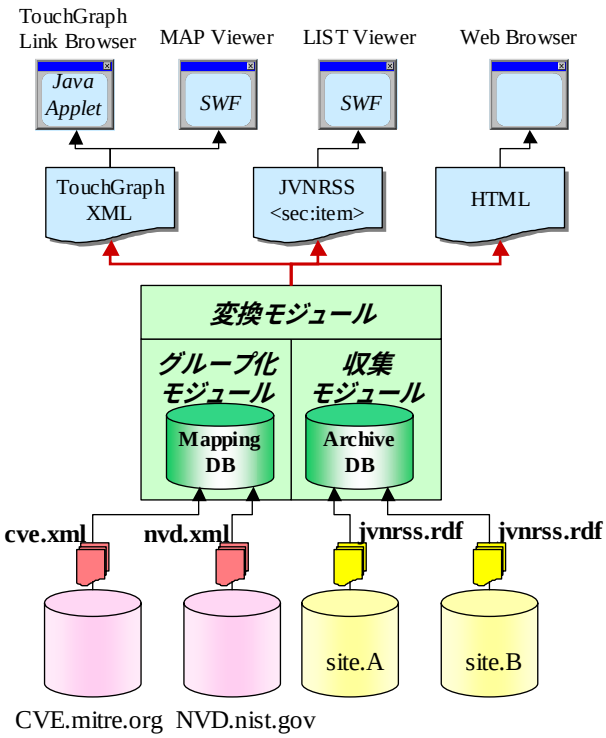

図 2 CVE+システムの概要

図 3　JVNRSS の Web 表示ツール: jvnbox(左)，XSL_swf 仕様の box(右)

4.1.2　試行サイトでの取り組み

CVE+では，JVNRSS フォーマットのデータを収集した後，JVNRSS フォーマットの<dc:relation>要素を用いた分類処理を行なうことにより，国内の脆弱性対策情報を CVE の識別番号に関連付ける．現在，試行サイトで稼動しているプロトタイプシステムのモジュール構成は，次の通りである(図 2).

(1) 収集モジュール

製品開発ベンダやニュースサイトなどに掲載されている JVNRSS の記載されたファイルを取得し，Archive DB に格納する．

(2) グループ化モジュール

Mapping DB は，”同一の脆弱性に関する情報に対して，異なる<dc:relation>値が付与されている JVNRSS エントリ同士”を同じグループに帰属させるためのデータベースである．また，JVNRSS に記載された対策情報のグループ化は，<dc:relation>要素と Mapping DB を用いて，下記の手順により実現する．

- <dc:relation>要素が一致する場合
  異なるサイトから発信されている情報であっても，<dc:relation>要素が一致するため，<item>要素は同一の脆弱性に関する情報を取り上げていると判断する．
- <dc:relation>要素が一致しない場合
  <dc:relation>要素が異なるため，直接比較では<item>要素が同一の脆弱性に関する情報を取り上げていると判断できない．このため，CERT Advisory, CERT Vulnerability Note, CVE, CIAC Bulletin など普及度の高くかつ主要な脆弱性対策情報が格納された Mapping DB を用いた間接的な一致性確認を行なう．図 4に示すように間接的に<dc:relation>要素が一致する場合には，<item>要素は同一の脆弱性に関する情報を取り上げていると判断する．これは，製品開発ベンダ A は CERT Advisory を情報源として参照しているのに対して，ニュースサイト X は CERT Vulnerability Note を情報源として参照している．このように，発信者は，必ずしも同じ情報源を参照するとは限らないので，主要な脆弱性対策情報の相互関連性が格納されたデータベース Mapping DB を用いて間接的な関連付け実現が必要となる．

なお，試行サイトの CVE＋プロタイプシステムでは，CVE サイトから取得した CVE リストを Mapping DB として利用し，この CVE リストと JVNRSS の<dc:relation>要素とを直接比較し，対策情報の記載された<item>要素を CVE の識別番号毎に関連付け操作を行なっている．

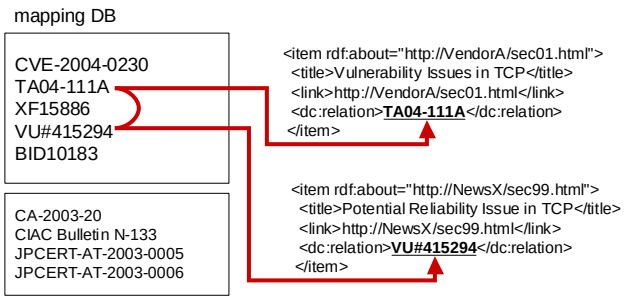

図 4　<dc:relation>要素と Mapping DB

(3) 変換モジュール

グループ化した<item>要素を，Web サイトで公開するために HTML 形式に変換したり，図 5 に示す<dc:relation>要素の参照関係を表示するための可視化用フォーマットに変換したりするなどの機能である。なお，試行サイトの CVE＋プロタイプシステムでは, TouchGraph XML [10], JVNRSS 拡張フォーマット(<sec:item>)[11]への出力をサポートしている.

4.2 TRnotes

TRnotes(Status Tracking Notes)を JVNRSS フォーマットで記載することによる情報の再活用と共に, JVNRSS フォーマットを用いた情報流通を通して, 各イベントの情報収集の省力化と，情報発信元が提示する時単位レベルの時刻情報を参照するための取り組みである.

4.2.1 概要

TRnotes は，報告された脆弱性に関して，「脆弱性の影響を受ける製品は？」「その製品ベンダの対策情報？」という脆弱性対策に加え，「いつ攻略コードが公開されたのか？」「脆弱性を悪用したインシデントは何があったのか？」「インシデントに伴いどのような対応がとられたのか？」という脆弱性に関わる状況変化時系列にまとめていくことで，脆弱性対策活動を支援する試みであり, 2004 年 7 月から JVN サイトで情報発信を開始している.

しかし，現行の JVN サイトの TRnotes 掲載情報は，HTML ベースの情報として構成しているために情報の再活用において柔軟さが欠けていること, 各イベントの時刻情報の収集方法としてメーリングリストの場合には投稿時刻，Web サイトの場合には HTTP プロトコルのヘッダ情報として提供される Last-Modified の時刻を参照し時単位レベルでの時刻情報の収集を一部代用している.

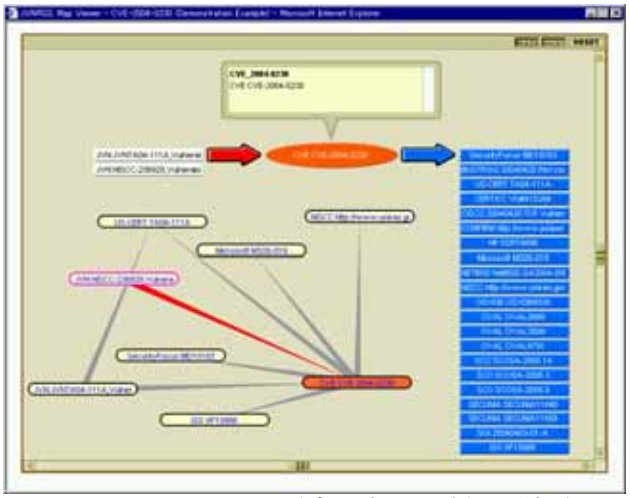

図 5 <dc:relation>要素の参照関係の可視化

4.2.2 試行サイトでの取り組み

試行サイトでは，TRnotes の各イベントを JVNRSS の各<item>要素として記述できることに着目し，TRnotes のトピックスを JVNRSS フォーマットで記載すること共に，各イベントを時刻ソートによる表示を行なっている．特に，試行サイトで稼動している各イベントの時刻ソート表示ツールでは，イベント間の時刻間隔を考慮した表示を実現すると共に，イベントを時単位でトラッキングする必要があることから，各イベントの時刻を利用者のタイムゾーンにあわせ表示する仕様としている(図 6).

4.3 RSS_dir

RSS_dir は，複数の JVNRSS ファイル(=JVNRSS チャンネル)を記載した JVNRSS ディレクトリを整備する取り組みである.

4.3.1 概要

複数存在する RSS ファイルの集約については, RSS ファイルを集めて一種のポータルサイトを構築したり，RSS に広告，ニュースという異なるサービスを組み合わせて提供するなど様々な試みが行なわれているが，RSS_dir では，製品開発ベンダ，ニュースサイトなどが掲載する JVNRSS ファイルの追加や削除などの変更を機械的に判定処理することに主眼を置いている.

例えば，製品開発ベンダが新たな製品の脆弱性対策情報の発信を JVNRSS ファイルで開始したり, 年度毎に JVNRSS ファイルを用意するなど，サイトが保持する JVNRSS ファイルの追加や削除といった変更を機械的に検知することにある.

4.3.2 試行サイトでの取り組み

上記の課題を解決するための試行サイトでの実現方式は次の通りである.

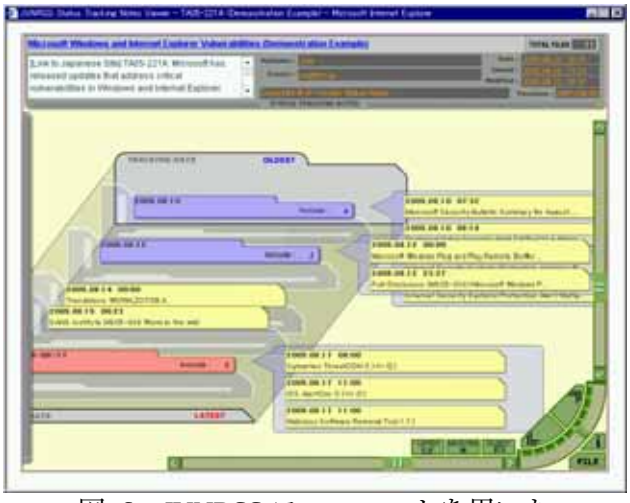

図 6 JVNRSS フォーマットを用いた TRnotes の表示

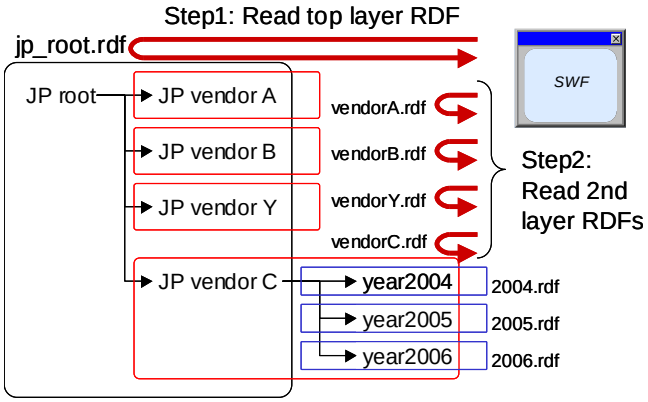

図 7　RSS チャンネルのためのディレクトリ

(1) 前提条件

RSS 1.0 の規約の範囲で実現すること.

(2) 実現方式

JVNRSS を用いて複数存在する JVNRSS の存在を階層記述することでディレクトリを構成する．すなわち，階層の上位に位置する JVNRSS ファイルを抑えておけば，下位に位置する JVNRSS ファイルが追加されたり，削除されたりなどの判定処理を機械的に取り扱えることになる(図 7). このコンセプトに基づき Flash を用いて実現した Web 表示ツールを図 8に示す．この Web 表示ツールは, 最上位の JVNRSS ファイルから順次探索を行い，更新日の確認機能をを行なう機能を備えている.

5. おわりに

本稿では，JVN，製品開発ベンダやニュースサイトが発信する脆弱性対策情報の利活用にあたり，掲載されている脆弱性対策情報の展開を支援するという視点から，JVNRSS を用いた支援とその試行について述べた.

本稿で提示した方法は，図 9に示すような各製品開発ベンダや各ニュースサイトが提供している JVNRSS による脆弱性対策情報から関連リンク集を作成するなどに応用できるであろう．また，JVNRSS のような脆弱性対策情報の発信が普及すれば，情報収集の省力化や収集した情報の再構成などの可能性が広がると共に，特定の脆弱性についてどの程度の数の情報発信がなされていたのかという効果測定も副次的に実現できると考えている.

謝辞

本研究の一部は科学技術振興調整費の支援を受け実施している．本研究を進めるにあたって有益な助言と協力を頂いた，貫井千鶴氏，高崎仁氏，調整費の関係者各位, JPCERT/CC 関係者各位ならびに，IPA の関係者各位に深く感謝致します.

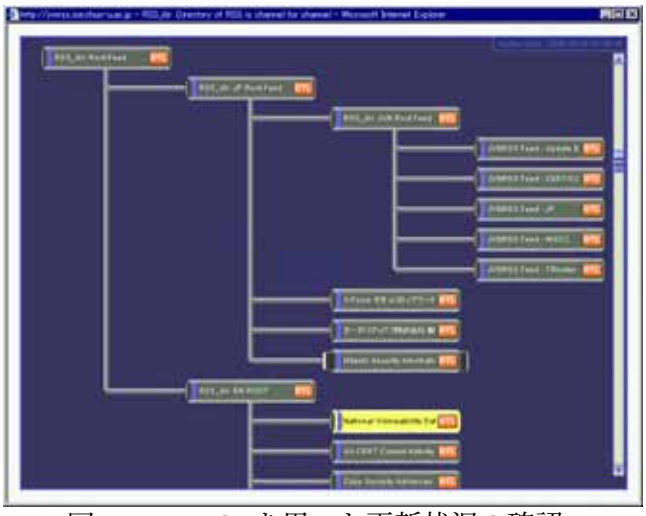

図 8　RSS_dir を用いた更新状況の確認

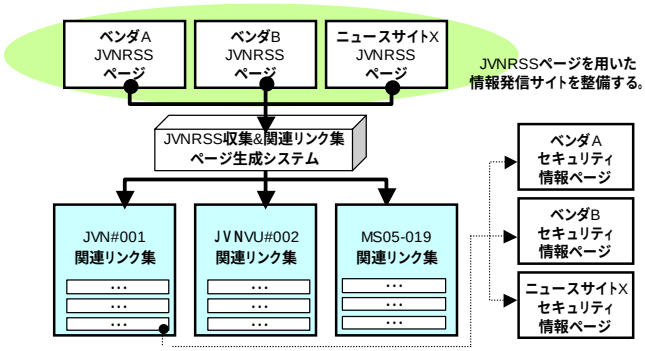

図 9　関連リンク集作成での活用例

参考文献

1) 寺田，土居, “RDF Site Summary を用いたセキュリティ情報流通に関する検討”, CSEC 研究報告 Vol.2003 No.022, (2003)
2) JVNRSS - JP Vendor Status Notes RDF Site Summary, http://jvnrss.ise.chuo-u.ac.jp/jtg/jvnrss/
3) RDF Site Summary (RSS) 1.0 http://web.resource.org/rss/1.0/spec
4) ISO 15836:2003(E):Information and documentation - The Dublin Core metadata element set http://www.niso.org/international/SC4/n515.pdf
5) The Dublin Core Metadata Registry http://dublincore.org/dcregistry/navigateServlet
6) 寺田，高田，土居, “脆弱性対策情報データベース JVN の提案”, 情処論文誌 Vol.46 No.5 (2005)
7) 経済産業省，「情報セキュリティ早期警戒パートナーシップ」の運用開始について http://www.meti.go.jp/policy/it_policy/press/0005399/
[8] JVNRSS feasibility site, http://jvnrss.ise.chuo-u.ac.jp/jtg/
9) CVE- Common Vulnerabilities and Exposures, http://cve.mitre.org/
10) TouchGraph Link Browser http://touchgraph.sourceforge.net/index.html#TGLB
11) Qualified Security Advisory Reference (mod_sec), http://jvnrss.ise.chuo-u.ac.jp/jtg/mod_sec/