RDF Site Summary を用いたセキュリティ情報流通に関する検討

寺田真敏 [*1, *a] terada@doi.ics.keio.ac.jp
土居範久 [*2, *1] doi@ise.chuo-u.ac.jp

[*1)] 慶應義塾大学 大学院 理工学研究科
〒223-8522 神奈川県横浜市港北区日吉 3-14-1

[*2)] 中央大学 理工学部 情報工学科
〒112-8551 東京都文京区春日 1-13-27

概要： 現在のセキュリティ情報の流通は、HTML ベースの Web ページ情報として構成されているために、散在している Web サイトから、情報の断片を集め再構成する、情報間の関連付けを行なうなどの情報の再活用において柔軟さが欠けている。本稿では、セマンティック Web のキー技術である RDF を使用して、XML フォーマットに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 RSS (RDF Site Summary) を用いたセキュリティ情報の流通の利用例について述べる。
キーワード：セキュリティ情報, RSS, Web サービス

Study of Security Information Distribution with RDF Site Summary

Masato Terada [*1 *a] terada@doi.ics.keio.ac.jp
Norihisa Doi [*2, *1] doi@ise.chuo-u.ac.jp

[*1)] Graduate School of Science and Technology, Keio University.
3-14-1 Hiyoshi, Kohoku-ku, Yokohama, Kanagawa 223-8522, Japan

[*2)] Faculty of Science and Engineering, Chuo University.
1-13-27 Kasuga, Bunkyo-ku, Tokyo 112-8551, Japan

Abstract: The security information is distributed as Web page information on HTML base. In order to re-construct the information and perform correlation between the collected information, it is necessary to improve the security information providing environment. This paper described the overview of the distribution of the security information using RSS which provides lists such as the title and a summary.
key words: Security Information, RSS, Web Service

*a) (株)日立製作所 システム開発研究所
セキュリティシステム研究部
〒212-8567 神奈川県川崎市幸区鹿島田 890
Systems Development Laboratory, Hitachi Ltd.
890 Kashimada, Saiwai-ku, Kawasaki, 212-8567 Japan

1. はじめに

セキュリティ情報提供ベンダ、製品ベンダ、コミュニティ、個人など様々な層で脆弱性対策のための情報提供がなれている。しかしながら、現在の情報の流通は、HTML ベースの Web ページ情報、すなわち、「人間が理解できる情報(ヒューマンリーダブルな情報)」として構成されているために、散在している Web サイトから、情報の断片を集め再構成する、情報間の関連付けを行なうなどの情報の再活用において柔軟さが欠けているように思われる。

このような課題を解決するひとつの流れとして「コンピュータなどの機械がその意味を理解できる情報(マシンリーダブルな情報)」とするために、XMLとRDF(Resource Description Framework)を用いて意味付けした文書を構成し、コンピュータで自動処理させるセマンティックWebがある[1]。

本稿では、セマンティックWebのキー技術であるRDFを使用して、XMLフォーマットに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ことで、サイトの更新情報などを効率的に配布するRSS (RDF Site Summary) [2]を用いたセキュリティ情報の流通の利用例について報告する。

2. 情報流通支援技術

本章では、セキュリティに関する情報流通を支援する技術について整理する。

2.1 既存技術

(1) 汎用的な情報流通支援

HTML ベースの Web サイトを対象とした情報流通支援技術としては、サイトの更新状況を更新時刻を元に確認する「アンテナ」、キーワードにより該当する情報を検索する検索サイトが利用されている。

(2) 脆弱性情報に特化した情報流通支援

脆弱性情報に対象を絞った場合には、脆弱性に対して一意の識別子(例: CVE-1999-1011)を付与し、それぞれ独自に名前付けされた脆弱性情報を相互に関連付けるためのリストCVE(Common Vulnerabilities and Exposures)[3]がある。現在、脆弱性を扱うツール、データベースなどがCVEを参照しており[4]、米国NIST (National Institute of Standards and Technology) が提供する脆弱性情報データベースICAT Metabase[5]でも利用されている。

この他にも、セキュリティ対策を支援するために、XMLフォーマットでセキュリティ関連情報を発信し、SOAPを使ってこれらの情報にアクセスするWebサービス構築の研究も行なわれている[6][7]。

2.2 RSS (RDF Site Summary)

RSSは、サイトの概要をメタデータとして簡潔に記述するXMLフォーマットであり、Netscape社が自社のポータルMy Netscapeに「チャンネル」を登録するための手段として 1999 年 3 月に開発されたバージョン 0.9 が基となっている[8]。1999 年 7 月には、概要を記述するdescriptionなど要素を取り入れたRSS 0.91[9]が登場し、現在は、2000 年 12 月に提案されたRSS 1.0 に至っている。RSS 1.0 は、RDFを中心としたモジュールによる拡張機能を備えており、モジュールのひとつであるDublin Coreは、Webや文書の作者、タイトル、作成日といった情報をメタデータとして記述するためのボキャブラリを定めている(図 2.1～図 2.3)[10]。国内においてもXMLを利用したコンテンツ配信手段のひとつとしてRSSを用いた情報発信が行なわれつつある[11][12]。

rdf:RDF	
channel	**チャンネルの**URI
title	**チャンネルのタイトル**
link	**チャンネルで対象とするサイトの**URI
description	**チャンネルの説明**
image	**チャンネルロゴなどの**URI
items	item**要素で記述するリソースの目次**
textinput	**フォームデータを送信する際に使用**
rdf:Seq	
rdf:li+	
item+	
title	**リソースのタイトル**
link	**リソースの**URI
description	**リソースの説明**

図 2.1 RSS 1.0 の要素 (抜粋)

title	**リソースに与えられた名前**
creator	**リソースの内容に責任を持つエンティティ**
publisher	**リソースを提供しているエンティティ**
date	**リソースの作成日、公開日**
indetifier	**リソースへの一意な参照**
realtion	**関連するリソースへの参照**
など	

図 2.2 Dublin Core の要素 (抜粋)

```
<?xml version="1.0" encoding="utf-8" ?>
<?xml-stylesheet href="jvn_rss_update.xsl" type="text/xsl" media="screen"?>

<rdf:RDF
 xmlns="http://purl.org/rss/1.0/"
 xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"
 xmlns:dc="http://purl.org/dc/elements/1.1/"
 xml:lang="ja">

 <channel rdf:about="http://jvn.doi.ics.keio.ac.jp/rss/jvn_rss_update.rdf">
  <title>JVN Update</title>
  <link>http://jvn.doi.ics.keio.ac.jp</link>
  <description>2003-03-16 から過去1週間分のJVNサイト更新情報</description>
   <dc:publisher>jvn@doi.ics.keio.ac.jp</dc:publisher>
   <dc:rights>Copyright(C) 2002,2003 Keio Univ. All rights reserved.</dc:rights>
   <dc:date>2003-03-16</dc:date>
  <items>
   <rdf:Seq>
    <rdf:li rdf:resource="ftp://ftp.iij.ad.jp/pub/IIJ/dist/iijnews/vol52-focus.pdf"/>
   </rdf:Seq>
  </items>
 </channel>

<item rdf:about="ftp://ftp.iij.ad.jp/pub/IIJ/dist/iijnews/vol52-focus.pdf">
  <title>SQL slammer ワームへの対応</title>
  <link>ftp://ftp.iij.ad.jp/pub/IIJ/dist/iijnews/vol52-focus.pdf</link>
  <description></description>
   <dc:publisher>インターネットイニシアティブ(IIJ)</dc:publisher>
   <dc:identifier>IIJ news vol.52 FOCUS(1)</dc:identifier>
   <dc:relation>http://www.cert.org/advisories/CA-2003-04.html</dc:relation>
   <dc:date>2003-03-10</dc:date>
  </item>

</rdf:RDF>
```

図 2.3　RSS 1.0 の例

3. JVN における RSS の適用

本章では、国内でのセキュリティ対策推進を支援するために、国内で利用されているソフトウェアや装置の脆弱性を対象とした対策情報データベース JVN (JPCERT/CC Vendor Status Notes Data Base) [13] を対象としたRSSの適用について述べる。

3.1　解決したい課題

JVN サイトにおいて解決したい課題として、以下の 2 つがある。

(1) 情報の再活用を考慮した配信

対策情報をまとめ上げることに主眼を置いていることから、HTML ベースの Web ページ情報として構成している。しかしながら、掲載情報を活用してもらうためには、マシンリーダブルな情報形式で提供するなど配信方法を再検討する必要がある。

(2) ベンダ情報収集に関するフレームワーク検討

ベンダからの対策情報収集のひとつとして、メールによる通知連絡を想定しており、CERT Advisory No.、ベンダ名、ベンダ固有の文書 ID、タイトル、URL、更新日から構成されるフォーマット(図 3.1)を用意しているが、メール以外の情報収集手段を整備していく必要がある。

```
〈例1〉富士通の情報
X-JVN-cano:    CA-2003-05
X-JVN-vendor:  富士通
X-JVN-id:      〈なし〉
X-JVN-title:   CA-2003-05に対する富士通の情報
X-JVN-url:     http://software.fujitsu.com/jp/security/cert.html#ca-2003-05
X-JVN-update:  2003.02.21

〈例2〉Solaris OEの情報
X-JVN-cano:    CA-2003-05
X-JVN-vendor:  富士通
X-JVN-id:      〈なし〉
X-JVN-title:   CA-2003-05に対するSolaris OEの情報
X-JVN-url:     http://software.fujitsu.com/jp/security/cert_pw.html#ca-2003-05
X-JVN-update:  2003.02.21
```

図 3.1　メール通知フォーマットの例
(ベンダ→JVN)

3.2　RSS を用いた情報配信と収集

JVN サイトが取り扱っている情報ならびに、メール通知フォーマットを、図 3.2に示すような RSS 要素に対応付けることにより、RSS を情報配信ならびに収集手段として利用することができる。

```
<item rdf:about="ベンダが掲載するセキュリティ情報のURL">
  <title>タイトル</title>
  <link>ベンダが掲載するセキュリティ情報のURL</link>
  <description>セキュリティ情報の概要</description>
   <dc:publisher>ベンダ名</dc:publisher>
   <dc:identifier>ベンダ固有の文書ID</dc:identifier>
   <dc:relation>関連情報のURL {JVN | CVE | CERT-CA | CERT-VU}</dc:relation>
   <dc:date>更新日</dc:date>
 </item>
```

図 3.2　JVN データと RSS 要素との対応付け

本節では、上記課題を解決する手段のひとつとして、RSS を用いた JVN データの配信と収集について述べる。

(1) RSS を用いた JVN データの配信

RSS を利用することにより、ニュースサイトが提供する RSS ニュースフィードと同様に JVN データを配信することとなり、既存の情報流通機構を活用できることになる。さらに、RSS によりデータが構造化されていることから、項目毎の追加ならびに更新状態を確認することも容易となる。具体的な適用事例としては、図 3.3に示すような RSS による「過去 1 週間の JVN サイトの更新情報」の提供が考えられる。

図 3.3　RSSを用いた「JVNサイトの更新情報」の提供 (XSLを介したRSS表示) [14]

(2) RSS を用いた JVN データの収集

上記と同様な枠組みを展開することにより、配信だけではなく、ベンダからの対策情報収集に利用でき、しかも、RSS 要素に記載した関連付け情報(dc:relation)を用いることで、ベンダサイトから、収集した対策情報を JVN ページとして再構成することも可能となる(図 3.4)。

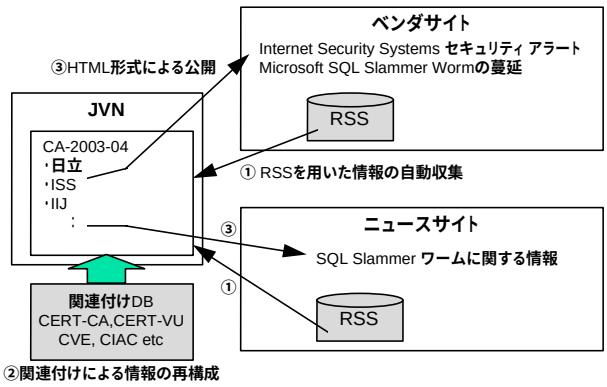

図 3.4　JVN サイトにおけるページの自動生成

ここで、操作ステップとしては、

①RSS を用いた情報の収集操作

②RSS要素に記載された関連付け情報(dc:relation)ならびに、CERT Advisory (CERT-CA) [15], CERT Vulnerability Note (CERT-VU)[16], CVE, CIAC Bulletin [17]などの主要なセキュリティ情報の相互関連性が格納されたデータベースを用いた情報の再構成操作

③HTML 形式でのページ公開操作により実現することができる。

したがって、セキュリティ情報を提供するRSSリスト(図 3.5)とCERT-CA, CERT-VU, CVE, CIAC Bulletinなどの相互関連性が格納されたデータベース[b]を整備することにより、セキュリティ情報を取り扱いたい他サイトでも同様な機構を備えることができ、セキュリティ情報収集に関する操作軽減につながるであろう。

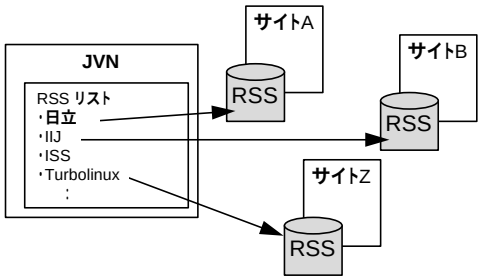

図 3.5　セキュリティ情報の RSS ポータル

(3) RSS 適用に伴う制約事項

JVN において RSS を適用するにあたっては、「RSS 要素 item で使用する URI を一意とする」という仕様が制約事項となる。以下、このような制約事項に該当する事例を示すとともに、その解決仕様を提示する。

(a) 事例 1：セキュリティ対策情報のリスト表記

CERT Advisory に関するセキュリティ対策情報をリストまたはテーブル表記などにより一覧としている場合、セキュリティ対策情報として同一の HTML ページを参照することがある(図 3.6)。このような場合、図 3.7に示すように RSS 要素 item で使用する URI が重複してしまうことがあり、RSS の仕様に従い実装されたビューアで参照すると、同一の item が複数表示されてしまうことがある(図 3.8)。

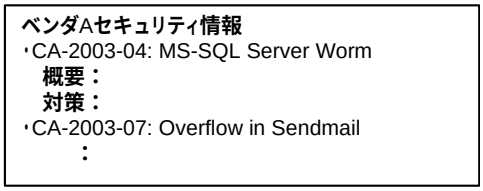

図 3.6　セキュリティ対策情報のリスト表記

b) データベースとして、脆弱性に対して識別子の割当てを行なっているCVEを利用することができる。ただし、CERT Advisory, CIACなどにおいて発行されるインシデント注意喚起情報に対してはCVEの識別子の割当ては行なわれていないので留意する必要がある。

```
<rdf:Seq>
  <rdf:li rdf:resource="http://software.fujitsu.com/jp/security/fjpatch/info/internet_navi200302.html"/>
  <rdf:li rdf:resource="http://www.jpn.hp.com/upassist/assist2/secbltn/HPSBUX0304-253.html"/>
  <rdf:li rdf:resource="http://www.debian.org/security/2003/dsa-278"/>
  <rdf:li rdf:resource="http://software.fujitsu.com/jp/security/cert_pw.html#ca-2003"/>
  <rdf:li rdf:resource="http://software.fujitsu.com/jp/security/cert_pw.html#ca-2003"/>
 </rdf:Seq>

<item rdf:about="http://software.fujitsu.com/jp/security/cert_pw.html#ca-2003">
 <title>Buffer Overflow in Sendmail</title>
 <link>http://software.fujitsu.com/jp/security/cert_pw.html#ca-2003</link>
 <description></description>
 <dc:publisher>富士通</dc:publisher>
 <dc:identifier></dc:identifier>
 <dc:relation>http://www.cert.org/advisories/CA-2003-12.html</dc:relation>
 <dc:date>2003-04-13</dc:date>
</item>

<item rdf:about="http://software.fujitsu.com/jp/security/cert_pw.html#ca-2003">
 <title>Multiple Vulnerabilities in Lotus Notes and Domino</title>
 <link>http://software.fujitsu.com/jp/security/cert_pw.html#ca-2003</link>
 <description></description>
 <dc:publisher>富士通</dc:publisher>
 <dc:identifier></dc:identifier>
 <dc:relation>http://www.cert.org/advisories/CA-2003-11.html</dc:relation>
 <dc:date>2003-04-13</dc:date>
</item>
```

図 3.7　RSS へのマッピングが適切ではない JVN データの事例

図 3.8　RSS 1.0 Validator and Viewer[18]を用いたマッピングが適切ではない JVN データの表示

セキュリティ対策情報をリストまたは、テーブル一覧としている場合には、RSS要素itemで使用するURIが一意となるよう、HTMLファイルに～を導入し、これを参照することで解決できる(図 3.9) [c]。

(b) 事例 2：アプリケーションごとのページ集約

セキュリティ対策情報をアプリケーションごとに集約している場合も、セキュリティ対策情報として同一の HTML ページを参照することがある(図 3.10)。さらに、アプリケーションごとのページ集約している場合には、ひとつの施策が、関連する複数の CERT Advisory を包括した対策として提供されることもある。このような場合にも、事例 1 と同様に RSS 要素 item で使用する URI が重複してしまう。

```
<item rdf:about="http://AAA/cert.html">
<title>MS-SQL Server Worm</title>
<dc:relation>CA-2003-04(*)</dc:relation>
        :
<item rdf:about="http://AAA/cert.html">
<title>Overflow in Sendmail</title>
<dc:relation>CA-2003-07(*)</dc:relation>
```

⇩

```
<item rdf:about="http://AAA/cert.html#ca-2003-04">
<title>MS-SQL Server Worm</title>
<dc:relation>CA-2003-04(*)</dc:relation>
        :
<item rdf:about="http://AAA/cert.html#ca-2003-07">
<title>Overflow in Sendmail</title>
<dc:relation>CA-2003-07(*)</dc:relation>
```

*) URL**による記述を省略している。**

図 3.9　URI 変更によるマッピング補正

```
ベンダBセキュリティ情報
・<a name="sendmail">sendmail の対策</a>
  CA-2003-07
  CA-2003-12
  概要:
  対策:
・<a name="bind">BIND の対策</a>
  CA-2002-31
        :
```

図 3.10　アプリケーションごとのページ集約

アプリケーションごとのページ集約している場合には、RSS 要素 item で使用する URI が一意となるよう、RSS 要素の関連付け情報(dc:relation)で複数の関連付け先を参照することで解決できる(図 3.11)。

```
<item rdf:about="http://BBB/sendmail.html">
<title>sendmail の対策</title>
```

⇩

```
<item rdf:about="http://BBB/sendmail.html">
<title>sendmail の対策</title>
<dc:relation>CA-2003-07(*)</dc:relation>
<dc:relation>CA-2003-12(*)</dc:relation>
```

*) URL**による記述を省略している。**

図 3.11　関連付け集約化によるマッピング補正

c) 富士通の場合には、下記のようにCERT CA#毎にURI指定できる形態にWebページの構成を変更して頂いた。なお、下記URLはサイト変更などの理由により将来変更される可能性がある。
http://software.fujitsu.com/jp/security/cert2003.html#ca-2003-xx

4. おわりに

本稿では、RDF Site Summary を用いたセキュリティ情報流通に関する検討として、「JVN データの配信ならびに収集」への RSS 適用について述べた。RSS を用いた JVN データの配信については、準備ができ次第試行公開していくことを考えている。また、RSS を用いた JVN データの収集については、運用形態、ツール整備などの検討を進めていく予定である。

謝辞

本研究は、JPCERT/CC の支援を受け実施しているものである。本研究を進めるにあたって有益な助言と協力を頂いた、JPCERT/CC 関係者各位、JVN ワーキンググループに参加して頂いている株式会社インターネットイニシアティブ(IIJ)の齋藤衛氏、インターネットセキュリティシステムズ(株)の高橋正和氏、徳田敏文氏、ベンダ情報提供にご協力を頂いた富士通(株)ソフトウェア品質検証部の豊田和男氏の皆様に深く感謝致します。

参考文献

1) 財団法人ニューメディア開発協会, セマンティックWeb 技術と次世代電子政府での活用方法に関する調査研究 2002.
http://www.nmda.or.jp/nmda/soc/3-1/3_1all.pdf
2) RDF Site Summary (RSS).
http://web.resource.org/rss/1.0/
3) Common Vulnerabilities and Exposures.
http://cve.mitre.org/
4) CVE-Compatible Products and Services.
http://cve.mitre.org/compatible/index.html
5) ICAT Metabase: A CVE Based Vulnerability Database. http://icat.nist.gov/
6) 中村, 戸村: XMLによるセキュリティ関連情報Web サービス, マルチメディア通信と分散処理ワークショップ論文集, 2002, pp.275-280.
7) 中村, 戸村: XMLとSOAPによるセキュリティ関連情報Web サービス, 情報処理学会第 65 回全国大会, 2003.
8) RDF Site Summary (RSS) 0.9 official DTD, proposed.
http://my.netscape.com/publish/formats/rss-0.9.dtd
9) RSS 0.91 Spec, revision 3. http://my.netscape.com/publish/formats/rss-spec-0.91.html
10) Dublin Core Metadata Element Set, Version 1.1: Reference Description.
http://dublincore.org/documents/dces/
11) CNET Japan RSS News Feed.
http://japan.cnet.com/info/rss/
12) RSS(RDF Site Summary)によるサイト情報の要約と公開. http://www.kanzaki.com/docs/sw/rss.html
13) 寺田, 土居: JPCERT/CC Vendor Status Notes DB 構築に関する検討, コンピュータセキュリティシンポジウム 2002, pp.173-177.
14) http://jvn.doi.ics.keio.ac.jp/rss/jvn_rss_update.rdf
15) CERT/CC Advisories,
http://www.cert.org/advisories/
16) CERT/CC Vulnerability Notes,
http://www.kb.cert.org/vuls
17) CIAC Bulletins ,
http://www.ciac.org/cgi-bin/index/bulletins
18) Redland RSS 1.0 Validator and Viewer,
http://www.redland.opensource.ac.uk/rss/