INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

JVNRSSを用いた
脆弱性対策情報の発信ガイド

JVNRSS: JVN RDF Site Summary

2009年10月

独立行政法人情報処理推進機構セキュリティセンター

INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

目次

IPAでは、2009年4月から、申請された製品開発者のWebサイトに掲載されているJVNRSS(Japan Vulnerability Notes RSS)形式の脆弱性対策情報を自動収集し、脆弱性の深刻度や対象製品の普及度を考慮してJVN iPediaに脆弱性対策情報を登録する試行を開始しました。

- 脆弱性対策情報の自動収集の試行について (2009-04-28)
  http://www.ipa.go.jp/security/vuln/jvnrss.html

本ガイドでは、製品開発者の皆様が試行に参加するにあたり、試行の背景となる脆弱性対策情報ポータルサイトJVNにおける取り組み、JVNRSSの概要と製品開発者の皆様がWebサイトに掲載するJVNRSS形式の脆弱性対策情報の作成にあたってのポイントを解説します。

INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

1. 脆弱性対策情報ポータルサイト JVNにおける取り組み

1.1 JVNの歩み
1.2 JVN、JVN iPedia、MyJVN連携
1.3 製品開発者の発信する脆弱性対策情報の自動収集

本章では、脆弱性対策情報の自動収集の試行の背景として、JVNでの取り組みについて紹介します。

2004年の情報セキュリティ早期警戒パートナーシップ発足以降、国内においても、JVN（Japan Vulnerability Notes）、ソフトウェア製品開発者、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てきています。しかし、対策情報の多くは主に文書として構成されているために、脆弱性対策情報を自動収集してJVNに登録したり、JVNに登録されている脆弱性対策情報の影響有無をチェックして対策を促すなどの脆弱性対策に関わる処理の機械化については発展途上にあります。

米NIST（National Institute of Standards and Technology：国立標準技術研究所）では、2006年からセキュリティ対策の自動化と標準化を目指したSCAP（セキュリティ設定共通化手順、Security Content Automation Protocol）の開発を推進しています。また、EU（European Union）では2006年から情報セキュリティ推進機関であるENISA（European Network and Information Security Agency：欧州ネットワーク情報セキュリティ庁）が中心となってセキュリティ関連情報の共有システムを実現するためのプロジェクトを推進しています。

JVNでは、このような状況を踏まえ、情報セキュリティの脆弱性対策が国内だけではなく、国際的にも対応可能なグローバルなJVN実現に向け、脆弱性対策に関わる共通基準を積極的に採用すると共に、脆弱性対策に関わる処理の機械化を目指すフレームワークを推進しています。

1.1 JVNの歩み

- 2003年2月
  JVN ワーキンググループ結成
  JVN 試行サイトの公開
- 2004年7月
  情報セキュリティ早期警戒パートナーシップ発足
  JVN は IPA と JPCERT/CC の共同運用形態に移行
- 2005年9月
  JVNRSS フォーマットによる情報配信サービスを開始
- 2007年4月
  JVN iPedia サイトの開設
- 2008年5月
  JVN 英語サイト、JVN iPedia 英語サイトの開設
- 2008年10月
  脆弱性対策に関わる処理の機械化を目指すフレームワーク
  “MyJVN” サービスの開始
- 2009年4月
  製品開発者の発信する脆弱性対策情報の自動収集の試行開始

JVNは、2003年2月に、JPCERT/CCの試行サイトとしてJVN (JPCERT/CC Vendor Status Notes) の運用を開始しました。
以降、
2004年7月：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」の施行、情報セキュリティ早期警戒パートナーシップの発足にあわせ、JVN (JP Vendor Status Notes) は、IPAとJPCERT/CCの共同運用形態に移行し、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としての役割を担うこととなります。

2005年9月：機械処理を見据えた脆弱性対策情報の配信する仕組みとして、RSS (RDF Site Summary) 1.0 の仕様をベースとした JVNRSSフォーマットによる情報配信サービスを開始しました。

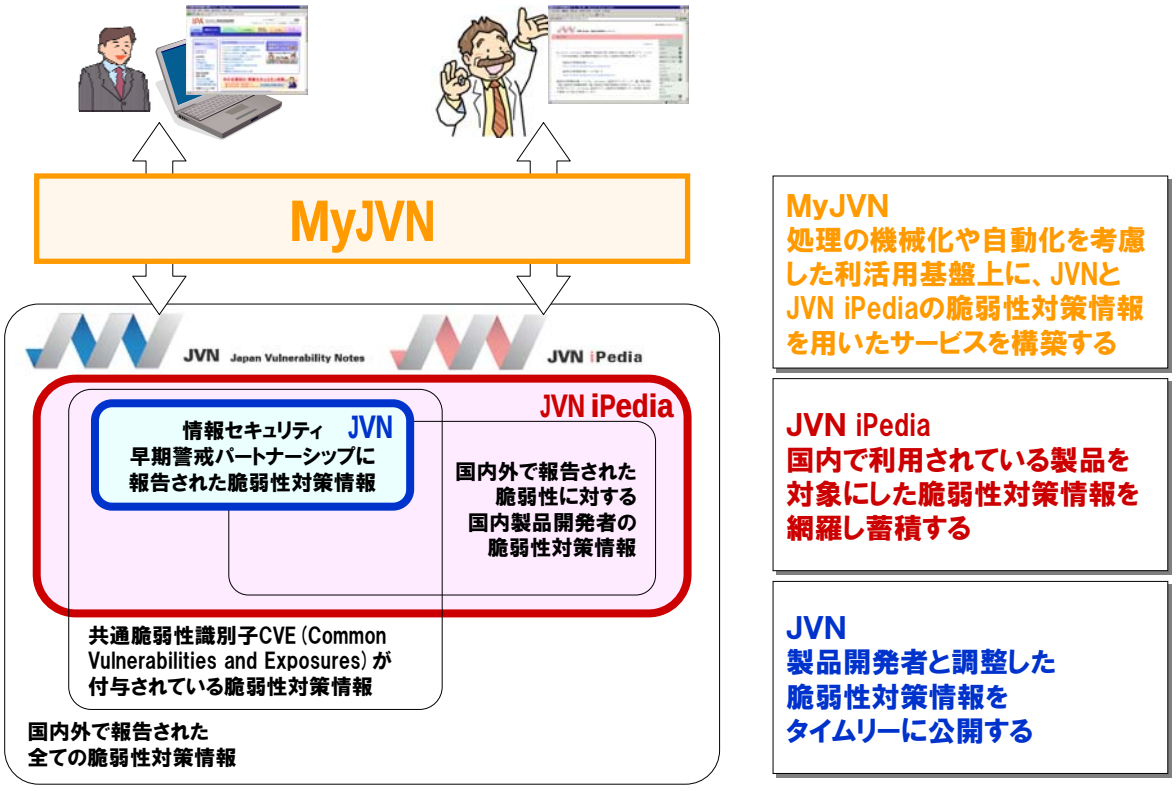
2007年4月：即時性と網羅性を備えた脆弱性対策情報の発信を実現するため、JVN (http://jvn.jp/) と JVN iPedia (http://jvndb.jvn.jp/) の2つのシステム構成に変更すると共に、名称をJVN (Japan Vulnerability Notes) に変更しました。

2008年5月：国際的にも対応可能なグローバルなJVN実現に向け、JVN 英語サイト (http://jvn.jp/en/) とJVN iPedia 英語サイト (http://jvndb.jvn.jp/en/) を開設しました。

2008年10月：脆弱性対策に関わる処理の機械化の利活用基盤を整備しつつ、日本という地域性を考慮した脆弱性対策の自動化を実現すべく、脆弱性対策に関わる共通基準を積極的に採用すると共に、脆弱性対策に関わる処理の機械化を目指すフレームワークMyJVNサービス (http://jvndb.jvn.jp/apis/myjvn/) を開始しました。

2009年4月に開始した脆弱性対策情報の自動収集の試行は、脆弱性対策に関わる処理の機械化など利活用基盤の整備と、JVN iPediaに登録する脆弱性対策情報として、国内で利用されている製品を対象にした情報を充実させていくことにあります。

1.2 JVN、JVN iPedia、MyJVN連携



MyJVN
処理の機械化や自動化を考慮した利活用基盤上に、JVNとJVN iPediaの脆弱性対策情報を用いたサービスを構築する

JVN iPedia
国内で利用されている製品を対象にした脆弱性対策情報を網羅し蓄積する

JVN
製品開発者と調整した脆弱性対策情報をタイムリーに公開する

ここまでに、JVN、JVN iPedia、MyJVNという3つの単語がでてきました。

JVNでは、 JVN、JVN iPedia、MyJVNの3つの機能を利用して、情報セキュリティの脆弱性対策が国内だけではなく、国際的にも対応可能とするグローバルなJVN実現に向けた取り組みを進めています。3つの役割分担は、次の通りです。

グローバルなJVN

国際性と地域性の両面から脆弱性対策を支援する
脆弱性対策情報ポータルサイトを目指しています。

JVN Japan Vulnerability Notes

http://jvn.jp/
国内の情報セキュリティ早期警戒パートナーシップ、および海外の調整機関に届けられた脆弱性関連情報に関して製品開発者と調整して、信頼性の高い対策情報をタイムリーに公開します。

JVN iPedia

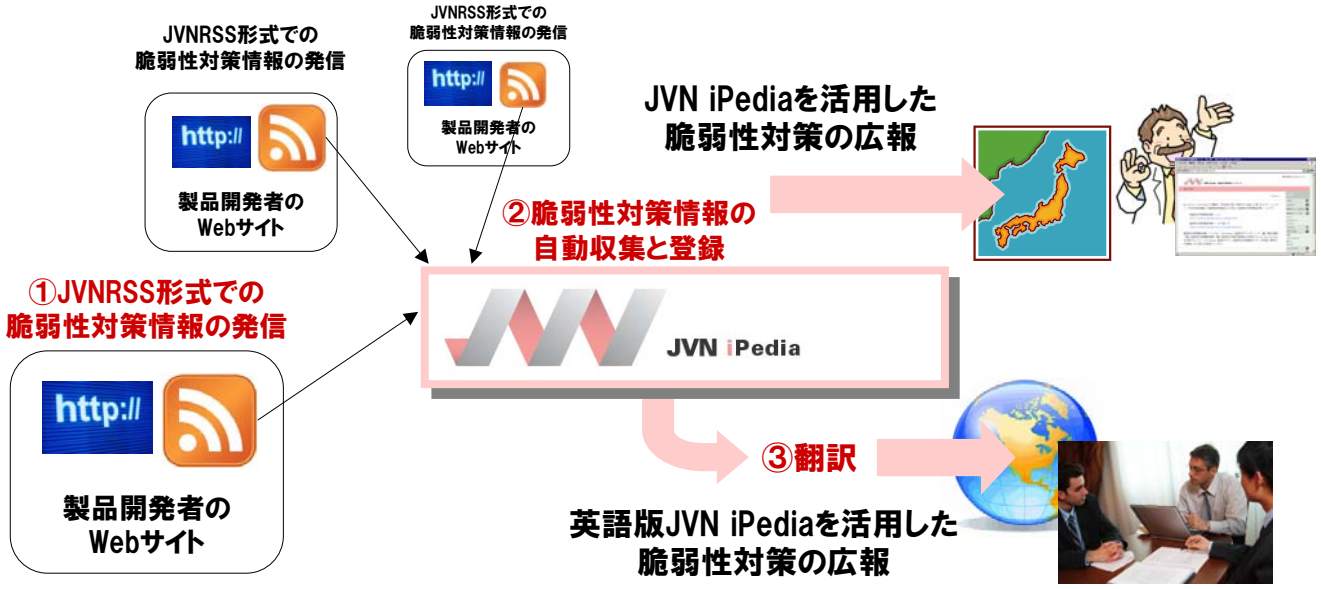
http://jvndb.jvn.jp/
国内の製品開発者ベンダから公開された対策情報、および海外の脆弱性対策データベースに登録された情報に基づき、国内で利用されている製品を対象にした脆弱性対策情報を網羅、蓄積することを目的としています。

MyJVN

http://jvndb.jvn.jp/apis/myjvn/
日本という地域性を考慮した脆弱性対策に関わる処理の機械化などの利活用基盤を整備し、JVNとJVN iPediaの脆弱性対策情報を用いたサービスを提供します。

1.3 製品開発者の発信する脆弱性対策情報の自動収集

- 処理の機械化や自動化を考慮した利活用基盤の整備
- 製品開発者のメリット
  - JVN iPediaへの脆弱性対策情報の掲載 ⇒ 国内向け
  - 英語版JVN iPediaへの脆弱性対策 翻訳 情報の掲載 ⇒ 海外向け



2009年4月に開始した取り組みは、国内のソフトウェア製品開発者から公開された脆弱性対策情報を網羅、蓄積すると共に、収集処理の機械化などの利活用基盤を整備するための、脆弱性対策情報の自動収集の試行です。

具体的には、IPAでは、申請された製品開発者のWebサイトに掲載されているJVNRSS(Japan Vulnerability Notes RSS)形式の脆弱性対策情報を自動収集し、脆弱性の深刻度や対象製品の普及度を考慮してJVN iPediaに脆弱性対策情報を登録します。また、この脆弱性対策情報を英語に翻訳し、英語版JVN iPediaへ登録します。

【 試行への参加手続き 】

脆弱性対策情報の自動収集を希望される製品開発者は、次の事項を記載の上、電子メールで申込み下さい。

(1) 申込み先メールアドレス: vuln-inq@ipa.go.jp

(2) メールの件名:脆弱性対策情報の自動収集の申込み

(3) 記載事項:

1. ソフトウェア製品開発者のウェブサイトのURL
2. 脆弱性対策情報をJVNRSS形式で発信するウェブページのURL
3. ソフトウェア製品の問合せ先が記載されているウェブページのURL
4. 申込者の氏名、所属、連絡先電子メールアドレス

【 試行への参加にあたり留意して頂きたい事項 】

JVN iPediaへの登録は、既にJVN iPediaに登録されている製品開発者の製品に関する情報を優先的に登録します。その他の製品に関しては、脆弱性の深刻度や対象製品の普及度を考慮して登録していきます。

登録までの目安は2週間～4週間を予定しています。ただし、情報の信頼性確保、製品開発者の対策状況、優先度、収集した脆弱性の件数等との兼ね合いにより、対応期間が目安よりも長くなる場合がありますので、ご了承ください。

INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

2. JVNRSSの概要

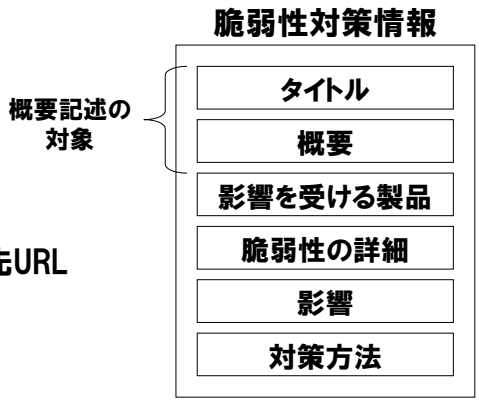
2.1 JVNRSSの概要
2.2 JVNRSSの構成

本章では、「脆弱性対策情報の自動収集の試行」で利用するJVNRSS形式について紹介します。

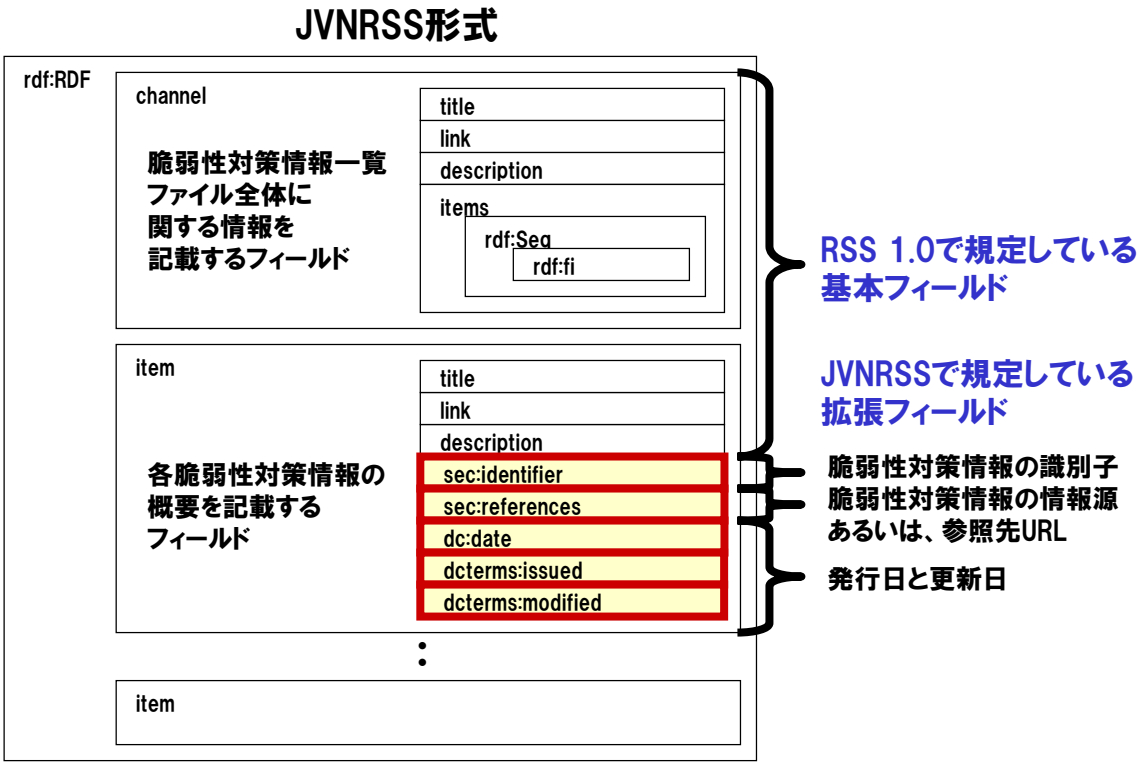
2.1 JVNRSSの概要

- JVNRSS: Japan Vulnerability Notes RSS
  - 脆弱性対策情報の概要記述用 XML フォーマットで、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 をベースとした仕様です。情報の再活用を考慮した配信、製品開発者からの情報収集の効率化や脆弱性対策情報のグループ化 (sec:identifier、sec:references) など、脆弱性対策情報の利活用を促進することを目的としています。

- JVNRSS形式では、次の3項目を記載する仕様となっています。
  - 脆弱性対策情報の識別子
    (製品開発者が脆弱性対策情報に識別子を付与している場合)
  - 脆弱性対策情報の情報源あるいは参照先URL
  - 発行日と更新日



JVNRSS形式では、RSS (RDF Site Summary) 1.0で規定している基本フィールドに加えて、識別子、情報源、発行日と更新日フィールドを利用します。



2.2 JVNRSSの構成 (a) rdf:RDF部

□ rdf:RDF部には、JVNRSS形式に関する基本情報として、名前空間接頭辞（dc、dcterms、secなど）とXMLスキーマファイルを記載します。

```
<?xml version="1.0" encoding="UTF-8" ?>

<rdf:RDF
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"
  xmlns="http://purl.org/rss/1.0/"
  xmlns:dc="http://purl.org/dc/elements/1.1/"
  xmlns:dcterms="http://purl.org/dc/terms/"
  xmlns:sec="http://jvn.jp/rss/mod_sec/"
  xsi:schemaLocation="http://purl.org/rss/1.0/   http://jvndb.jvn.jp/schema/jvnrss_2.0.xsd"
  xml:lang="ja">

  <channel>
  </channel>      ⇒ (b) channel部
  <item>
  </item>         ⇒ (c) item部

</rdf:RDF>
```

ここからは、JVN iPedia に掲載されている、年別情報 2008年のJVNRSS形式ファイル（http://jvndb.jvn.jp/ja/rss/years/jvndb_2008.rdf）を用いてJVNRSS形式のフィールド構成について解説します。
なお、事例では、脆弱性対策情報一覧に、「JVNDB-2008-001495：複数の DNS 実装にキャッシュポイズニングの脆弱性」のみが登録されているものとします。

JVNRSS形式は、(a) rdf:RDF部、(b) channel部、(c) item部の3つから構成されています。先頭部分はJVNRSS形式に関する基本情報を記載するフィールドで、名前空間接頭辞とXMLスキーマファイルを記載します。xml:langを除いて、rdf:RDF部のフィールドは固定です。

2.2 JVNRSSの構成 (b) channel部

- channel部には、JVNRSS形式ファイルに格納された脆弱性対策情報一覧に関する基本情報として、タイトル、概要、一覧された脆弱性対策情報への URLなどを記載します。

```
<channel rdf:about="http://jvndb.jvn.jp/ja/rss/jvndb_new.rdf">
 <title>JVNDB RSS Feed - 2008 Years Entry</title>
 <link>http://jvndb.jvn.jp/</link>
 <description>JVN iPedia 2008年情報</description>
 <dc:publisher></dc:publisher>
 <dc:creator></dc:creator>
 <dc:date>2009-04-19T09:00:01+09:00</dc:date>
 <dcterms:modified>2009-04-19T09:00:01+09:00</dcterms:modified>
 <items>
  <rdf:Seq>
   <rdf:li rdf:resource="http://jvndb.jvn.jp/ja/contents/2008/JVNDB-2008-001495.html" />
  </rdf:Seq>
 </items>
</channel>
```

channel部のフィールドには、脆弱性対策情報一覧ファイル全体に関する情報を次のように記載します。

```
<channel rdf:about="http://jvndb.jvn.jp/ja/rss/jvndb_new.rdf">  …JVNRSS形式ファイルを掲載するURLを記載します。
 <title>JVNDB RSS Feed - 2008 Years Entry</title>  …JVNRSS形式ファイルのタイトルを記載します。
 <link>http://jvndb.jvn.jp/</link>  …サイトのURL(ホームページや新着情報などのHTMLページ URL)を記載します。
 <description>JVN iPedia 2008年情報</description>  …JVNRSS形式ファイルの内容や概要の説明を記載します。
 <dc:publisher></dc:publisher>  …JVNRSS情報を発信する組織名(製品開発者名)を記載します。
 <dc:creator></dc:creator>  … JVNRSS情報を発信する組織(製品開発者)の問合せ先を記載します。
 <dc:date>2009-04-19T09:00:01+09:00</dc:date>  …JVNRSS形式ファイルを更新した日付を記載します。
 <dcterms:modified>2009-04-19T09:00:01+09:00</dcterms:modified>
                                                …JVNRSS形式ファイルを更新した日付を記載します。
 <items>
  <rdf:Seq>
   <rdf:li rdf:resource="http://jvndb.jvn.jp/ja/contents/2008/JVNDB-2008-001495.html" />
                                                …掲載する脆弱性対策情報自身のURLを記載します。
  </rdf:Seq>
 </items>
</channel>
```

2.2 JVNRSSの構成 (c) item部

□ item部には、各脆弱性対策情報に関する基本情報として、タイトル、概要、脆弱性対策情報に付与された識別子、脆弱性対策情報の情報源あるいは、参照先URLなどを記載します。

```
<item rdf:about="http://jvndb.jvn.jp/ja/contents/2008/JVNDB-2008-001495.html">
 <title>複数の DNS 実装にキャッシュポイズニングの脆弱性</title>
 <link>http://jvndb.jvn.jp/ja/contents/2008/JVNDB-2008-001495.html</link>
 <description>複数の DNS 実装にキャッシュポイズニング攻撃が容易になる脆弱性があります。
 </description>
 <dc:publisher></dc:publisher>
 <sec:identifier>JVNDB-2008-001495</sec:identifier>
 <sec:references>http://jvn.jp/cert/JVNVU800113/index.html</sec:references>
 <sec:references>http://jvn.jp/cert/JVNTA08-190A/</sec:references>
 <sec:references>http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1447
 </sec:references>
 <dc:date>2009-02-24T12:18+09:00</dc:date>
 <dcterms:issued>2008-07-23T15:31+09:00</dcterms:issued>
 <dcterms:modified>2009-02-24T12:18+09:00</dcterms:modified>
</item>
```

item部のフィールドは、各脆弱性対策情報に関する情報を次のように記載します。

```
<item rdf:about="http://jvndb.jvn.jp/ja/contents/2008/JVNDB-2008-001495.html">
                                  …該当する脆弱性対策情報を掲載しているページのURLを記載します。

 <title>複数の DNS 実装にキャッシュポイズニングの脆弱性</title>
                                  …該当する脆弱性対策情報のタイトルを記載します。

 <link>http://jvndb.jvn.jp/ja/contents/2008/JVNDB-2008-001495.html</link>
                                  …該当する脆弱性対策情報を掲載しているページのURLを記載します。

 <description>複数の DNS 実装にキャッシュポイズニング攻撃が容易になる脆弱性があります。</description>
                                  …該当する脆弱性対策情報の概要を記載します。

 <dc:publisher></dc:publisher>  …該当する脆弱性対策情報を発信する組織名(製品開発者名)を記載します。
<sec:identifier>JVNDB-2008-001495</sec:identifier>  …脆弱性対策情報の識別子を記載します。

 <sec:references>http://jvn.jp/cert/JVNVU800113/index.html</sec:references>
 <sec:references>http://jvn.jp/cert/JVNTA08-190A/</sec:references>
 <sec:references>http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1447</sec:references>
                                  …脆弱性対策情報の情報源あるいは、参照先URLを記載します。

 <dc:date>2009-02-24T12:18+09:00</dc:date>  …脆弱性対策情報の更新日を記載します。
 <dcterms:issued>2008-07-23T15:31+09:00</dcterms:issued>  …脆弱性対策情報の発行日を記載します。
 <dcterms:modified>2009-02-24T12:18+09:00</dcterms:modified>  …脆弱性対策情報の更新日を記載します。

</item>
```

IPA®
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

3. JVNRSSによる情報発信のポイント

3.1 脆弱性対策情報の公表例
3.2 JVNRSSによる脆弱性対策情報の公表例
3.3 FAQ:よくある質問と答え

本章では、「ソフトウェア製品開発者による脆弱性対策情報の公表マニュアル」に記載されている、脆弱性対策情報の公表例(望ましい公表の例)を取り上げ、JVNRSS形式の各項目に記載すべき内容について解説します。

- ソフトウェア製品開発者による脆弱性対策情報の公表マニュアル (2008-04-04)
  http://www.ipa.go.jp/security/ciadr/vuln_announce_manual.pdf

3.1 脆弱性対策情報の公表例

ロ ソフトウエア製品開発者による脆弱性対策情報の公表マニュアル 3.1.12. 脆弱性対策情報の公表例（望ましい公表の例）

☆☆☆☆株式会社 > セキュリティ脆弱性情報 > ○○○○製品 ・・・①

IPASA2007-001: ○○○○製品における××××の脆弱性 ・・・②

公開日 2007 年1 月4 日 ・・・③
最終更新日 2007 年1 月9 日 ・・・④

■概要

○○○○のバージョン△△以前に××××の脆弱性が存在することが判明しました。この脆弱性を悪用された場合、悪意ある第三者の攻撃により、○○○○が動作しているコンピュータ上で□□□□が実行されてしまう危険性があります。この問題の影響を受ける○○○○のバージョンを以下に示しますので、以下の修正プログラムを適用してください。 ・・・⑤

■該当製品の確認方法

影響を受ける製品は以下の製品です。
製品名称 ○○○○
該当バージョン
1.5.4（Windows XP SP2 版）以前の全てのバージョン
1.5.4（Linux 版）以前の全てのバージョン
使用しているバージョン番号の確認方法は以下の通りです。
1, ○○○○を起動し、「ヘルプ」メニューから「バージョン情報」を選択する。
2. 現れたウィンドウの下記の部分が起動している○○○○のバージョン番号です。

バージョン表示ウィンドウの図（省略）

■脆弱性の説明

○○○○製品は、ファイルの■■■■のために▽▽▽▽の機能を搭載しています。◎◎◎◎データの一部として提供され▲▲▲▲で配布された▽▽▽▽の機能に、××××の脆弱性が存在するため、外部の第三者からインターネット越しに□□□□を実行される脆弱性が存在します。

ここでは、脆弱性対策情報に記載すべき項目について紹介します。

■タイトル ・・・② ⇒ (b) item部の<title>へ

製品の名称で検索して情報に辿り着く利用者のために、ページタイトルに製品名を記載します。また、過去および将来において同じ製品に複数の脆弱性が生ずる場合があることから、それらを区別可能なように、タイトルに脆弱性名称を記し、脆弱性情報のシリアル番号等を含めます。

■概要 ・・・⑤ ⇒ (b) item部の<description>へ

利用者が脆弱性の要点を迅速に把握できるよう、内容を簡潔にまとめた概要を冒頭に示します。

■該当製品の確認方法

脆弱性のある製品のバージョン情報と、利用者が使用している製品のバージョン情報を確認する方法を説明します。

■脆弱性の説明

利用者が同じ製品に存在した他の脆弱性と混同するなどの混乱が生じないよう、脆弱性の名称やその原因箇所などを記載して、その脆弱性の存在を説明します。

3.1 脆弱性対策情報の公表例

■脆弱性がもたらす脅威
システム管理者権限でログインして本ソフトウエアを利用している場合、攻撃が成功すると、悪意のある第三者によってコンピュータを完全に制御されてしまう可能性があります。これにより、悪意のある第三者は、不正プログラムのインストール、データの変更や削除など、システム管理者の権限でコンピュータを任意に操作する可能性があります。
・IPASA2007-001 技術詳細情報

■対策方法
○○○○バージョン1.0.0 より前の製品を利用されているお客様は、一度製品をアンインストールしてから対策版製品をインストールしてください。
○○○○1.0.0 以降の製品を利用されているお客様は、修正プログラムをインストールしてください。
各プログラムのインストール方法に関しては同梱のreadme.txt を参照してください。
対象製品名称 ○○○○
修正プログラムのダウンロード
1.5.5 patch.zip (WindowsXP SP2 版) 2007.1.4
1.5.5 patch.tgz (Linux 版) 2007.1.4
・修正プログラムによって置き換えられる設定ファイル
xxxxx.cfg、yyyyy.dif

■回避策
この脆弱性は、次に示す手順で影響を緩和できる場合があります。
・回避策
○○○で使用する管理用ポート番号宛ての通信を信頼できるIP アドレスのみに限定するよう、IP フィルタリング機能またはルータ等にてフィルタリング設定を行うことで、影響を緩和することができます。

■関連情報
JVN#12345678 ○○○○製品における××××の脆弱性 ・・・⑥

■謝辞
□□□の□□□氏よりこの問題をご報告いただき(略)

■更新履歴 ・・・③
2007.01.4 この脆弱性情報ページを公開しました。
2007.01.9 脆弱性がもたらす脅威に、権限の低い設定のアカウントで利用している場合についての技術詳細情報を追加しました。 ・・・④

■連絡先
脆弱性連絡窓口
電話 :03-xxxxx-xxxx (平日10:00 – 17:00)
メール:example@example.co.jp ・・・⑦

■脆弱性がもたらす脅威
脆弱性を悪用された場合に生じ得る被害の内容、危険の度合い、攻撃が成功する可能性の大きさ等、脆弱性の深刻度を評価するために必要な情報を記載します。

■対策方法
対策を施した製品のインストール方法やバージョンアップ方法、修正プログラムの適用方法を記載します。

■回避策
修正プログラムを適用しないままで、製品の利用方法を制限することや、運用を工夫すること等によって被害を防止できる場合には、その方法を回避策として記載します。

■関連情報 ・・・⑥ ⇒ (b) item部の<sec:references>へ
製品開発者による情報以外に、その脆弱性について公表されている情報がある場合には、利用者に有益な参考情報として、当該情報へのリンク等を記載します。

■謝辞
製品開発者によっては、脆弱性発見者への謝辞を記載することがあります。

■更新履歴 ・・・③④ ⇒ (b) item部の<dc:date><dcterms:issued><dctermd:modified>へ
当該脆弱性対策情報を最初に公表した日時を明示します。後に記載内容を改変した場合は、更新日を示すとともに、更新内容の説明を記載します。

■連絡先 ・・・⑦ ⇒ (b) item部の<dc:creator>へ
公表した脆弱性対策情報に疑問が生じたり、修正プログラムに不具合が生じたりする場合に備えて、問い合わせ先を明記します。

3.2 JVNRSSによる脆弱性対策情報の公表例 (b) channel部

□ channel部のフィールドには、「☆☆☆☆株式会社 セキュリティ脆弱性情報 ○○○○製品」の脆弱性対策情報発信についての情報を記載します。

```
<channel rdf:about="http://info.example.co.jp/rss/jvnrss.rdf">
 <title>☆☆☆☆株式会社 セキュリティ脆弱性情報 ○○○○製品</title>  •••①
 <link>http://info.example.co.jp/</link>
 <description>JVNRSS形式を用いた脆弱性対策情報の発信</description>
 <dc:publisher>☆☆☆☆株式会社</dc:publisher>
 <dc:creator>example@example.co.jp</dc:creator>  •••⑦ 連絡先
 <dc:date>2007-01-09T11:11+09:00</dc:date>
 <dcterms:issued />
 <dcterms:modified>2007-01-09T11:11+09:00</dcterms:modified>
 <items>
  <rdf:Seq>
   <rdf:li rdf:resource="http://info.example.co.jp/IPASA2007-001.html" />
  </rdf:Seq>
 </items>
</channel>
```

脆弱性対策情報の公表例（望ましい公表の例）に対応した記載を示します。
なお、(a) rdf:RDF部については説明を省略します（2.2節参照）。

```
<channel rdf:about="http://info.example.co.jp/rss/jvnrss.rdf">
 <title>☆☆☆☆株式会社 セキュリティ脆弱性情報 ○○○○製品</title>
 <link>http://info.example.co.jp/</link>
 <description>JVNRSS形式を用いた脆弱性対策情報の発信</description>
 <dc:publisher>☆☆☆☆株式会社</dc:publisher>
 <dc:creator>example@example.co.jp</dc:creator>
                …JVNRSS情報を発信する組織（製品開発者）の問合せ先としては、メールアドレスを推奨します。
 <dc:date>2007-01-09T11:11+09:00</dc:date>
                …多くのRSSリーダが日付情報の参照先として、dc:dateを利用していることから記載します。
 <dcterms:issued />
                …発行日を特定できない場合には記載は不要です。
 <dcterms:modified>2007-01-09T11:11+09:00</dcterms:modified>
                …日付は、YYYY-MM-DDThh:mmTZD（例 1997-07-16T19:20+01:00）形式を推奨します。
 <items>
  <rdf:Seq>
   <rdf:li rdf:resource="http://info.example.co.jp/IPASA2007-001.html" />
  </rdf:Seq>
 </items>
</channel>
```

3.2 JVNRSSによる脆弱性対策情報の公表例 (c) item部

□ item部のフィールドには、「脆弱性対策情報の公表例(望ましい公表の例)」に示された脆弱性対策情報についての情報を記載します。

```
<item rdf:about="http://info.example.co.jp/IPASA2007-001.html">
 <title>IPASA2007-001: ○○○○製品における××××の脆弱性</title>    ・・・② タイトル
 <link>http://info.example.co.jp/IPASA2007-001.html</link>
 <description>○○○○のバージョン△△以前に××××の脆弱性が存在することが
   判明しました。この脆弱性を悪用された場合、悪意ある第三者の攻撃により、○○○○が
   動作しているコンピュータ上で□□□□が実行されてしまう危険性があります。    ・・・⑤ 概要
 </description>
 <dc:publisher>☆☆☆☆株式会社</dc:publisher>
 <dc:creator>example@example.co.jp</dc:creator>    ・・・⑦ 連絡先
 <sec:identifier>IPASA2007-001</sec:identifier>    ・・・② タイトル
 <sec:references>http://jvn.jp/jp/jvn12345678</sec:references>    ・・・⑥ 関連情報
 <dc:date>2007-01-09T11:11+09:00</dc:date>    ・・・④ 更新履歴
 <dcterms:issued>2007-01-04T10:10+09:00</dcterms:issued>    ・・・③ 更新履歴
 <dcterms:modified>2007-01-09T11:11+09:00</dcterms:modified>    ・・・④ 更新履歴
</item>
```

```
<item rdf:about="http://info.example.co.jp/IPASA2007-001.html">
 <title>IPASA2007-001: ○○○○製品における××××の脆弱性</title>
 <link>http://info.example.co.jp/IPASA2007-001.html</link>
 <description>○○○○のバージョン△△以前に××××の脆弱性が存在することが
   判明しました。この脆弱性を悪用された場合、悪意ある第三者の攻撃により、○○○○が
   動作しているコンピュータ上で□□□□が実行されてしまう危険性があります。
 </description>
 <dc:publisher>☆☆☆☆株式会社</dc:publisher>
 <dc:creator>example@example.co.jp</dc:creator>
 <sec:identifier>IPASA2007-001</sec:identifier>
                ...製品開発者が脆弱性対策情報に識別子を付与している場合には、その識別子を記載します。
 <sec:references>http://jvn.jp/jp/jvn12345678</sec:references>
                ...脆弱性対策情報の情報源あるいは、参照先として記載するURLは、
                   普及しているセキュリティ情報を推奨します。
                   自らが情報源の場合など、該当する情報源や参照先がない場合には記載は不要です。
 <dc:date>2007-01-09T11:11+09:00</dc:date>
                ...多くのRSSリーダが日付情報の参照先として、dc:dateを利用していることから記載します。
                ...日付は、YYYY-MM-DDThh:mmTZD (例 1997-07-16T19:20+01:00)形式を推奨します。

 <dcterms:issued>2007-01-04T10:10+09:00</dcterms:issued>
 <dcterms:modified>2007-01-09T11:11+09:00</dcterms:modified>
</item>
```

3.3 FAQ：よくある質問と答え

Q 脆弱性対策情報の情報源あるいは、参照先URLには、どのようなサイトのURLを記載すればよいのですか？

A <sec:references>には、脆弱性対策情報の情報源あるいは、参照先URLとして普及しているセキュリティ情報を参照します。参照先として普及しているセキュリティ情報として、次のようなサイトがあります。

- JPCERT 緊急報告 http://www.jpcert.or.jp/at/
- JVN http://jvn.jp/
- JVN iPedia http://jvndb.jvn.jp/
- マイクロソフト セキュリティ アドバイザリ http://www.microsoft.com/japan/technet/security/advisory/
- マイクロソフトセキュリティ情報 http://www.microsoft.com/japan/technet/security/current.aspx
- 共通脆弱性識別子CVE http://cve.mitre.org/cve/
- IBM Internet Security Systems: X-FORCE DATABASE http://xforce.iss.net/
- Secunia Advisories http://secunia.com/advisories/
- SecurityFocus: Vulnerabilities http://www.securityfocus.com/bid/
- US-CERT Technical Cyber Security Alerts http://www.us-cert.gov/cas/techalerts/
- US-CERT Vulnerability Notes http://www.kb.cert.org/vuls/

脆弱性対策情報の情報源あるいは参照先URLを複数記載したい場合には、列挙してください。

```
<item rdf:about="http://info.example.co.jp/IPASA2007-001.html">
                    :
<sec:identifier>IPASA2007-001</sec:identifier>
 <sec:references>http://jvn.jp/jp/jvn12345678</sec:references>
 <sec:references>http://www.kb.cert.org/vuls/id/123456</sec:references>
                              :
 <sec:references>http://nvd.nist.gov/nvd.cfm?cvename=CVE-2009-0000</sec:references>
 <dc:date>2007-01-09T11:11+09:00</dc:date>
 <dcterms:issued>2007-01-04T10:10+09:00</dcterms:issued>
 <dcterms:modified>2007-01-09T11:11+09:00</dcterms:modified>
</item>
```

3.3 FAQ：よくある質問と答え

Q JVNRSS形式の項目の出現順序を気にする必要はありますか？

A XMLスキーマファイルhttp://jvndb.jvn.jp/schema/jvnrss_2.0.xsd) では、(b) channel部、(c) item部に対して、次のような順序で項目を記述する仕様としています。JVNRSS形式で脆弱性対策情報を作成する際には、XMLスキーマファイルに沿った記述を推奨します。

```
<xs:element name="channel">
- <xs:complexType>
  - <xs:sequence>
      <xs:element ref="rss:title" minOccurs="1"
      <xs:element ref="rss:link" minOccurs="1" r
      <xs:element ref="rss:description" minOcc
      <xs:element ref="dc:language" minOccurs
      <xs:element ref="dc:publisher" minOccurs
      <xs:element ref="dc:rights" minOccurs="0"
      <xs:element ref="dc:creator" minOccurs="
      <xs:element ref="dc:subject" minOccurs="
      <xs:element ref="dc:identifier" minOccurs
      <xs:element ref="sec:identifier" minOccur
      <xs:element ref="dc:date" minOccurs="0"
      <xs:element ref="dcterms:issued" minOcc
      <xs:element ref="dcterms:modified" minO
      <xs:element ref="rss:items" minOccurs="1
    </xs:sequence>
    <xs:attribute ref="rdf:about" use="required
  </xs:complexType>
</xs:element>
```

```
<xs:element name="item">
- <xs:complexType>
  - <xs:sequence>
      <xs:element ref="rss:title" minOccurs="1" maxOccurs="1" />
      <xs:element ref="rss:link" minOccurs="1" maxOccurs="1" />
      <xs:element ref="rss:description" minOccurs="0" maxOccurs="1" />
      <xs:element ref="dc:language" minOccurs="0" maxOccurs="1" />
      <xs:element ref="dc:publisher" minOccurs="0" maxOccurs="1" />
      <xs:element ref="dc:rights" minOccurs="0" maxOccurs="1" />
      <xs:element ref="dc:creator" minOccurs="0" maxOccurs="1" />
      <xs:element ref="dc:subject" minOccurs="0" maxOccurs="1" />
      <xs:element ref="dc:identifier" minOccurs="0" maxOccurs="1" />
      <xs:element ref="dc:relation" minOccurs="0" maxOccurs="unbounded" />
      <xs:element ref="sec:identifier" minOccurs="0" maxOccurs="1" />
      <xs:element ref="sec:references" minOccurs="0" maxOccurs="unbounded" />
      <xs:element ref="sec:cpe-item" minOccurs="0" maxOccurs="unbounded" />
      <xs:element ref="sec:cvss" minOccurs="0" maxOccurs="1" />
      <xs:element ref="dc:date" minOccurs="0" maxOccurs="1" />
      <xs:element ref="dcterms:issued" minOccurs="0" maxOccurs="1" />
      <xs:element ref="dcterms:modified" minOccurs="0" maxOccurs="1" />
    </xs:sequence>
    <xs:attribute ref="rdf:about" use="required" />
  </xs:complexType>
</xs:element>
```

JVNRSS形式で脆弱性対策情報を作成する際には、XMLスキーマファイルに沿った記述を推奨しますが、脆弱性対策情報の自動収集の試行においては、項目の出現順序がXMLスキーマファイルと異なっていても問題ありません。

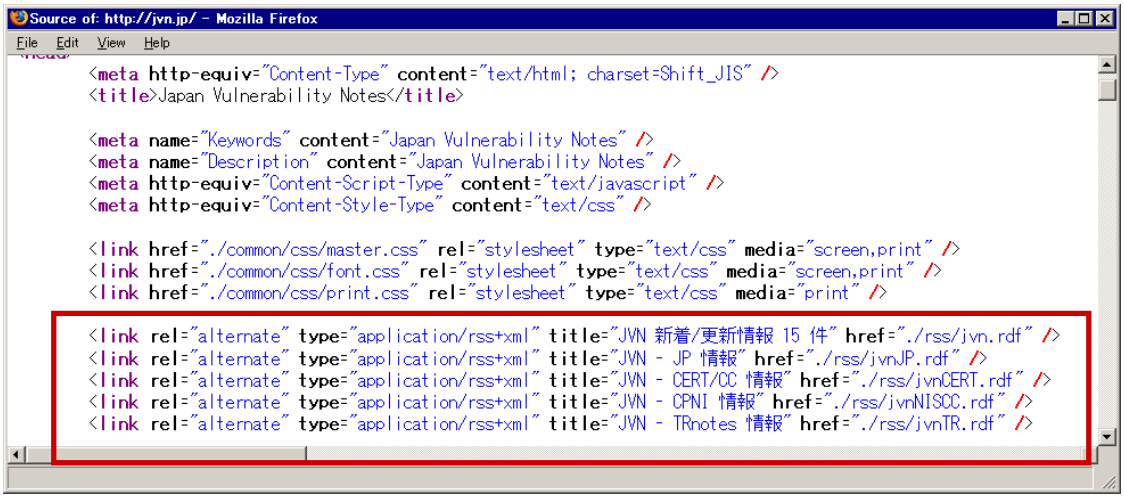
3.3 FAQ：よくある質問と答え

Q RSSファイルの存在を自動検出する仕組み（RSS Autodiscovery）とは何ですか？

A RSS Autodiscovery は、RSSへのリンクをHTMLページ中に明記することで、ブラウザ、RSSリーダーやWebサービスなどのプログラムが、RSSファイルの存在を自動検出できるようにするための仕組みです。

<link rel="alternate" type="MIMEタイプ" title="タイトル" href="RSSファイルのURL" />

記載事例（ http://jvn.jp/ ）



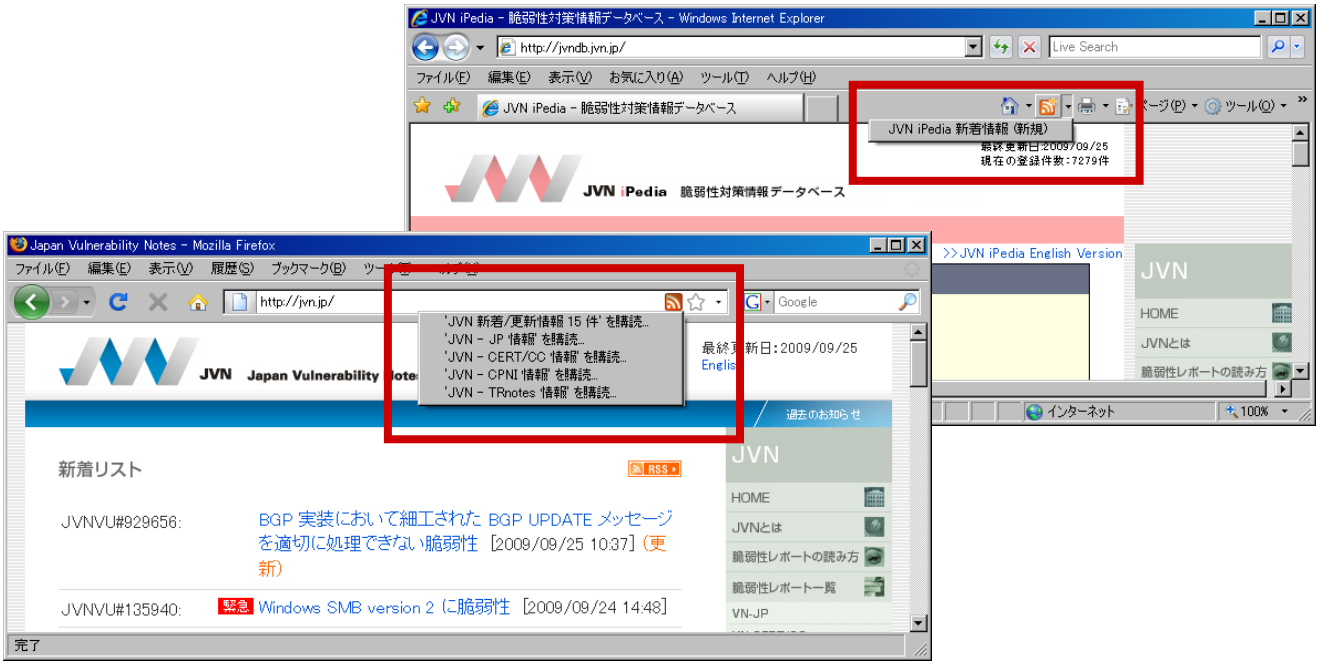
RSS Autodiscovery は、次のようなRSSへのリンクをHTMLページ中に明記することで、ブラウザ、RSSリーダーやWebサービスなどのプログラムが、RSSファイルの存在を自動検出できるようにするための仕組みです。Firefox、IE7では、RSS Autodiscovery に対応しており、RSSファイルを掲載している多くのWebサイトで RSS Autodiscovery を活用しています。

RSS 1.0、2.0、JVNRSSの場合

<link rel="alternate" type="application/rss+xml" title="JVN RSS Feed" href="index.rdf" />

Atomの場合

<link rel="alternate" type="application/atom+xml" title="JVN Atom Feed" href="index.atom" />



INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

参考情報

A. 脆弱性対策関連の情報
B. JVNRSS関連の仕様
C. JVNRSSのXMLスキーマファイル

A. 脆弱性対策関連の情報

- 脆弱性対策情報の自動収集の試行について（2009-04-28）
  http://www.ipa.go.jp/security/vuln/jvnrss.html
- ソフトウェア製品開発者による脆弱性対策情報の公表マニュアル（2008-04-04）
  http://www.ipa.go.jp/security/ciadr/vuln_announce_manual.pdf

B. JVNRSS関連の仕様

- RDF Site Summary (RSS) 1.0
  http://web.resource.org/rss/1.0/
- RDF Site Summary 1.0 Modules: Dublin Core
  http://purl.org/rss/1.0/modules/dc/
- RDF Site Summary 1.0 Modules: Qualified Dublin Core
  http://web.resource.org/rss/1.0/modules/dcterms/
- W3CDTF: Date and Time Formats
  http://www.w3.org/TR/NOTE-datetime
- JVNRSS - Japan Vulnerability Notes RDF Site Summary 2.2
  http://jvndb.jvn.jp/schema/jvnrss.html
- Qualified Security Advisory Reference (mod_sec)
  http://jvndb.jvn.jp/schema/mod_sec.html

C. JVNRSSのXMLスキーマファイル

- Resource Description Framework (RDF)
  namespace="http://www.w3.org/1999/02/22-rdf-syntax-ns#"
  schemaLocation="http://jvndb.jvn.jp/schema/jvnrss_rdf.xsd"
- RDF Site Summary (RSS) 1.0
  namespace="http://purl.org/rss/1.0/"
  schemaLocation="http://jvndb.jvn.jp/schema/jvnrss_2.0.xsd"
- RDF Site Summary 1.0 Modules: Dublin Core
  namespace="http://purl.org/dc/elements/1.1/"
  schemaLocation="http://jvndb.jvn.jp/schema/jvnrss_dc.xsd"
- RDF Site Summary 1.0 Modules: Qualified Dublin Core
  namespace="http://purl.org/dc/terms/"
  schemaLocation="http://jvndb.jvn.jp/schema/jvnrss_dcterms.xsd"
- Qualified Security Advisory Reference (mod_sec)
  namespace="http://jvn.jp/rss/mod_sec/"
  schemaLocation="http://jvndb.jvn.jp/schema/mod_sec_2.0.xsd"

謝辞
発信ガイド作成にあたり、「製品開発者によるJVNRSS情報発信検討WG」に参画頂いた各位に感謝いたします。

製品開発者によるJVNRSS情報発信検討WG（2007年）
富士通株式会社：草間正
株式会社日立製作所：田山晴康
日本電気株式会社：道城謙治
JPCERTコーディネーションセンター：古田洋久、戸田洋三
株式会社三菱総合研究所：川口修司、井上信吾

事務局
独立行政法人情報処理推進機構：小林偉昭、山岸正、相馬基邦、寺田真敏

［発行］　2009年4月28日　　第1版
2009年10月15日　　第2版：FAQにRSS Autodiscoveryの解説を追記（P18）
IPA（独立行政法人情報処理推進機構）セキュリティセンター

情報セキュリティに関する届出について

IPA セキュリティセンターでは、経済産業省の告示に基づき、コンピュータウイルス・不正アクセス・脆弱性関連情報に関する発見・被害の届出を受け付けています。

ウェブフォームやメールで届出ができます。詳しくは下記のサイトを御覧ください。
URL: http://www.ipa.go.jp/security/todoke/

コンピュータウイルス情報

コンピュータウイルスを発見、またはコンピュータウイルスに感染した場合に届け出てください。

不正アクセス情報

ネットワーク(インターネット、LAN、WAN、パソコン通信など)に接続されたコンピュータへの不正アクセスによる被害を受けた場合に届け出てください。

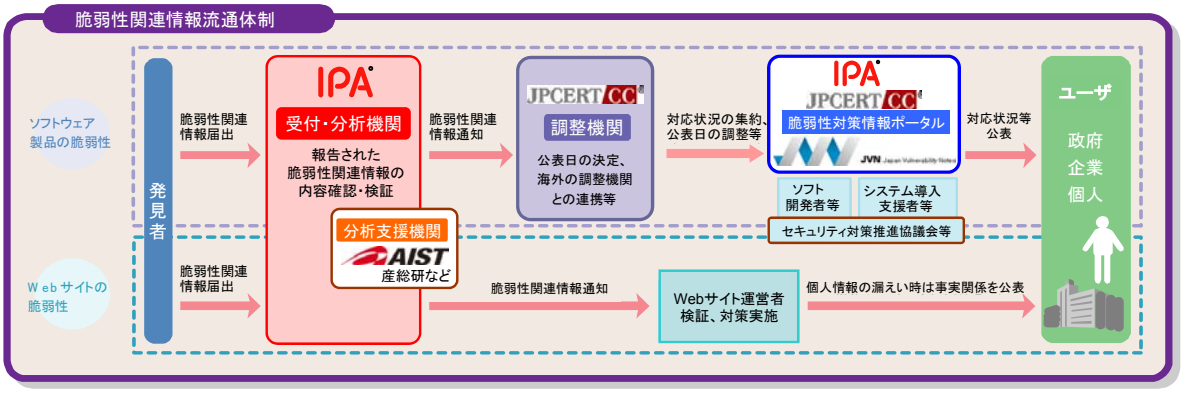
ソフトウエア製品脆弱性関連情報

OSやブラウザ等のクライアント上のソフトウエア、ウェブサーバ等のサーバ上のソフトウエア、プリンタやICカード等のソフトウエアを組み込んだハードウエア等に対する脆弱性を発見した場合に届け出てください。

ウェブアプリケーション脆弱性関連情報

インターネットのウェブサイトなどで、公衆に向けて提供するそのサイト固有のサービスを構成するシステムに対する脆弱性を発見した場合に届け出てください。

脆弱性関連情報流通の基本枠組み「情報セキュリティ早期警戒パートナーシップ」



※IPA:独立行政法人 情報処理推進機構、JPCERT/CC:一般社団法人 JPCERT コーディネーションセンター、産総研:独立行政法人 産業技術総合研究所

独立行政法人 情報処理推進機構
〒113-6591
東京都文京区本駒込二丁目28番8号
文京グリーンコートセンターオフィス16階
http://www.ipa.go.jp

セキュリティセンター
TEL: 03-5978-7527 FAX 03-5978-7518
http://www.ipa.go.jp/security/