

脆弱性対策情報データベース JVN iPedia の登録状況[2010年第4四半期(10月～12月)]

～ウェブブラウザ製品に関する脆弱性対策情報を拡充しました～

IPA（独立行政法人情報処理推進機構、理事長：藤江 一正）セキュリティセンターは、2010年第4四半期（10月～12月）の脆弱性対策情報データベース「JVN iPedia」（ジェイブイエヌ アイ・ペディア）の登録状況をまとめました。

(1) 脆弱性対策情報の登録件数が累計9,600件を突破（別紙1 1.参照）

2010年第4四半期に、脆弱性対策情報データベース「JVN iPedia（<http://jvndb.jvn.jp/>）」日本語版に登録した脆弱性対策情報は600件で、2007年4月25日の公開開始からの登録件数の累計が9,627件となりました。内訳は、国内製品開発者から収集したものが6件（累計116件）、脆弱性対策情報ポータルサイトJVN¹から収集したものが156件（累計995件）。また米国国立標準技術研究所NIST²の脆弱性データベース「NVD³」から、日本国内の個人や企業などで利用が多い製品に影響があると判断し、収集・翻訳したものが438件（累計8,516件）です。

2010年第4四半期は、個人や企業などで利用が多い製品としてウェブブラウザ製品の Google Chrome や、JVN から公表されている「任意の DLL/実行ファイル読み込みに関する脆弱性」についての脆弱性対策情報の登録を新たに開始しました。

(2) ウェブブラウザ製品に関する脆弱性対策情報を拡充しました（別紙1 2.参照）

(1)に記載したとおり、Google Chrome に関する情報の登録を新たに開始し、ウェブブラウザ製品に関する脆弱性対策情報を拡充しました。2010年12月末時点で、JVN iPedia 日本語版に登録済みの脆弱性対策情報9,627件のうち、約12.5%にあたる1,204件がウェブブラウザに関するものです。内訳は、Internet Explorer が308件、Mozilla Firefox が481件、Google Chrome が110件、Apple Safari が233件、Opera が90件です。なお、登録件数が多いことは、その製品自体が脆弱であることを示すのではなく、むしろ既知の脆弱性に対して適切な対策を実施している件数が多いと言えます。

ウェブブラウザに関する脆弱性対策情報の登録は年々増加しています。製品利用者は情報を日々収集し、製品のバージョンアップなどを遅滞なく行うことが重要です。

(3) MyJVN バージョンチェッカを利用して脆弱性対策を（別紙2 2.参照）

JVN iPediaのアクセス数を分析した結果、Lhaplusの脆弱性情報が1位と5位、Flash Playerの情報が9位になるなど、一般に広く利用されているソフトウェアに関する情報へのアクセスが多く、注目されています。IPAでは、ウェブブラウザをはじめ、このようなソフトウェアが最新のバージョンかどうかを簡単に確認できるツール「MyJVNバージョンチェッカ⁴」を無償で提供しています。「MyJVNバージョンチェッカ」などを活用し、ソフトウェアは常に脆弱性が解消された最新の状態で使用してください。

■ 本件に関するお問い合わせ先

IPA セキュリティセンター 渡辺／大森

Tel: 03-5978-7527 Fax: 03-5978-7518 E-mail: vuln-inq@ipa.go.jp

■ 報道関係からのお問い合わせ先

IPA 戦略企画部広報グループ 横山／大海

Tel: 03-5978-7503 Fax: 03-5978-7510 E-mail: pr-inq@ipa.go.jp

¹ Japan Vulnerability Notes. 脆弱性対策情報ポータルサイト。製品開発者の脆弱性への対応状況を公開し、システムのセキュリティ対策を支援しています。IPA、JPCERT/CC が共同で運営しています。 <http://jvn.jp/>

² National Institute of Standards and Technology. 米国国立標準技術研究所。米国の科学技術分野における計測と標準に関する研究を行う機関。 <http://www.nist.gov/>

³ National Vulnerability Database. NIST が運営する脆弱性データベース。 <http://nvd.nist.gov/home.cfm>

⁴ MyJVN バージョンチェッカ。 <http://jvndb.jvn.jp/apis/myjvn/>

2010年 第4四半期 脆弱性対策情報データベース JVN iPedia の登録状況（総括）

脆弱性対策情報データベース「JVN iPedia（<http://jvndb.jvn.jp/>）」は、日本国内で使用されているソフトウェア製品の脆弱性対策情報を収集することにより、脆弱性関連情報を容易に利用可能とすることを目指しています。1) 国内のソフトウェア製品開発者が公開した脆弱性対策情報、2) 脆弱性対策情報ポータルサイトJVN¹で公表した脆弱性対策情報、3) 米国国立標準技術研究所NIST²の脆弱性データベース「NVD³」が公開した脆弱性対策情報、の中から情報を収集、翻訳し、2007年4月25日から公開しています。

1. 脆弱性対策情報の登録状況

～ 脆弱性対策情報の登録件数が累計 9,600 件を突破～

2010年第4四半期（2010年10月1日から12月31日まで）にJVN iPedia日本語版へ登録した脆弱性対策情報は、国内製品開発者から収集したもの6件（公開開始からの累計は116件）、JVNから収集したもの156件（累計995件）、NVDから収集したもの438件（累計8,516件）、合計600件（累計9,627件）でした。脆弱性対策情報の登録件数が、累計9,600件を突破しました。（表1、図1）。

表 1. 2010年第4四半期の登録件数

	情報の収集元	登録件数	累計件数
日本語版	国内製品開発者	6件	116件
	JVN	156件	995件
	NVD	438件	8,516件
	計	600件	9,627件
英語版	国内製品開発者	6件	116件
	JVN	31件	481件
	計	37件	597件

JVN iPedia日本語版では、脆弱性対策情報を登録する対象製品を拡充しています。2010年第4四半期（2010年10月1日から12月31日まで）においては、個人や企業などで利用が多い製品として、ウェブブラウザのGoogle Chrome、バックアップ管理ソフトウェアのCA ARCserve Backupといった製品の脆弱性対策情報の登録を開始しています。また、「任意のDLL／実行ファイル読み込みに関する脆弱性の注意喚起⁴」に関してJVNから公表された脆弱性対策情報も14件登録しています。

JVN iPedia英語版は、国内製品開発者から収集したもの6件（累計116件）、JVNから収集したもの31件（累計481件）、合計37件（累計597件）でした。

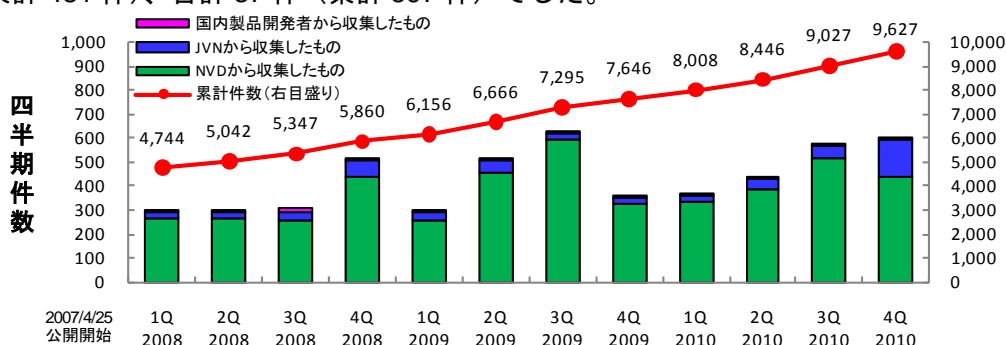


図1. JVN iPediaの登録件数の四半期別推移

¹ Japan Vulnerability Notes。脆弱性対策情報ポータルサイト。製品開発者の脆弱性への対応状況を公開し、システムのセキュリティ対策を支援しています。IPA、JPCERT/CC が共同で運営しています。 <http://jvn.jp/>

² National Institute of Standards and Technology。米国国立標準技術研究所。米国の科学技術分野における計測と標準に関する研究を行う機関。 <http://www.nist.gov/>

³ National Vulnerability Database。NIST が運営する脆弱性データベース。 <http://nvd.nist.gov/home.cfm>

⁴ 任意の DLL／実行ファイル読み込みに関する脆弱性の注意喚起。
<http://www.ipa.go.jp/about/press/20101111.html>

2. 登録している脆弱性対策情報に関する注目情報

～ウェブブラウザに関連する脆弱性対策情報を多数登録、速やかなバージョンアップを～

2010年12月末までに登録されたJVN iPedia日本語版の脆弱性対策情報9,627件のうち、約12.5%にあたる1,204件がウェブブラウザに関するものになっています。

JVN iPediaでは、共通脆弱性評価システムCVSS⁵により、それぞれの脆弱性の深刻度⁶を公開しています。図2のグラフは、JVN iPediaに登録済みのウェブブラウザ製品に関する脆弱性対策情報について、製品開発者やセキュリティポータルサイト等が脆弱性の対策情報を公開した日を基にした、深刻度別割合の公開年別推移を示したものです。図3はウェブブラウザ製品別の深刻度割合です。

図2のグラフを見ると、年々ウェブブラウザの脆弱性に関する件数は増えており、深刻度の高い脆弱性が増加傾向にあることがわかります。深刻度別の割合を集計すると、レベルIII（危険、CVSS基本値=7.0～10.0）が54%、レベルII（警告、CVSS基本値=4.0～6.9）が42%、レベルI（注意、CVSS基本値=0.0～3.9）が4%となっています。

図3のグラフを見ると、深刻度の高い脆弱性が特定の製品に限らないことがわかります。ウェブブラウザ製品別の登録件数は、Internet Explorerが308件、Mozilla Firefoxが481件、Google Chromeが110件、Apple Safariが233件、Operaが90件、となっています。

ウェブブラウザに関する脆弱性を多数登録しています。製品利用者は情報を日々収集し、製品のバージョンアップなどを遅滞なく行うことが重要です。

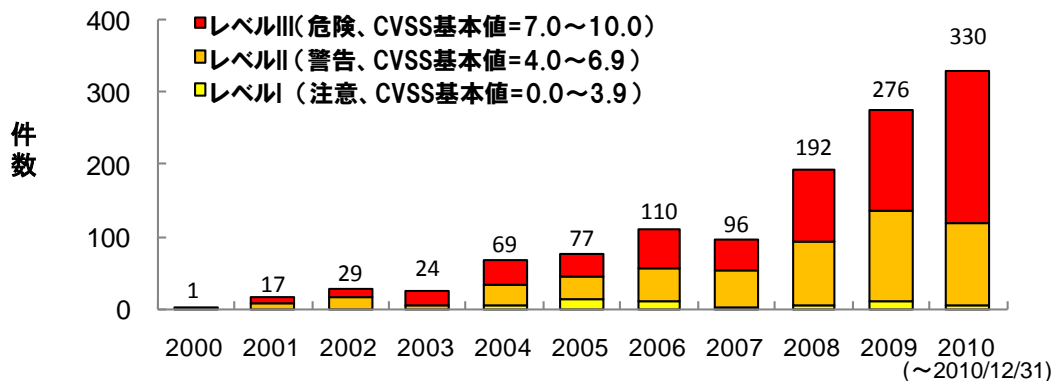


図2.ウェブブラウザの脆弱性に関する年別の深刻度割合

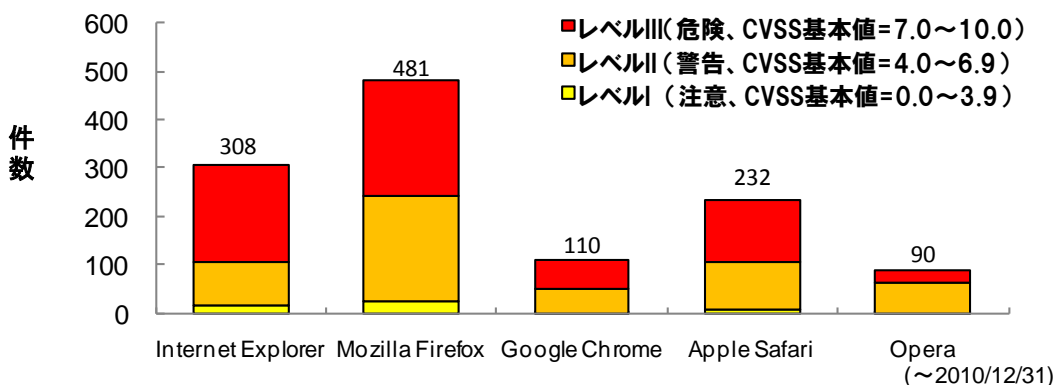


図3.ウェブブラウザ製品の脆弱性に関するブラウザ別の深刻度割合

⁵ Common Vulnerability Scoring System、共通脆弱性評価システム。
<http://www.ipa.go.jp/security/vuln/CVSS.html>

⁶ 脆弱性の深刻度評価の新バージョン CVSS v2 について。
<http://www.ipa.go.jp/security/vuln/SeverityLevel2.html>

2010年 第4四半期 脆弱性対策情報データベース JVN iPedia の登録状況（詳細）

1.脆弱性対策情報の登録状況

1.1 今四半期に登録した脆弱性の種類別件数

共通脆弱性タイプ一覧CWE⁷は、脆弱性の種類を識別するための共通の脆弱性タイプの一覧です。CWE を用いると、ソフトウェアの多種多様にわたる脆弱性に関して、脆弱性の種類（脆弱性タイプ）の識別や分析、国内外での比較などが可能になります。図4のグラフは、JVN iPediaへ今四半期に登録した脆弱性対策情報を、CWEで分類した、脆弱性の種類ごとの件数を示したものです。

件数が多い脆弱性は、CWE-119（バッファエラー）が116件、CWE-20（不適切な入力確認）が62件、CWE-399（リソース管理の問題）が44件、CWE-264（認可・権限・アクセス制御の問題）が40件、CWE-79（クロスサイト・スクリプティング）が34件、などとなっています。

これらは広く認知されている脆弱性の種類です。製品開発者は、これらの脆弱性に関してIPAが公開している「安全なウェブサイトの作り方⁸」、「安全なSQLの呼び出し方」、「セキュア・プログラミング講座⁹」などを参考に、ソフトウェア製品の企画・設計段階からセキュリティ実装を考慮する必要があります。

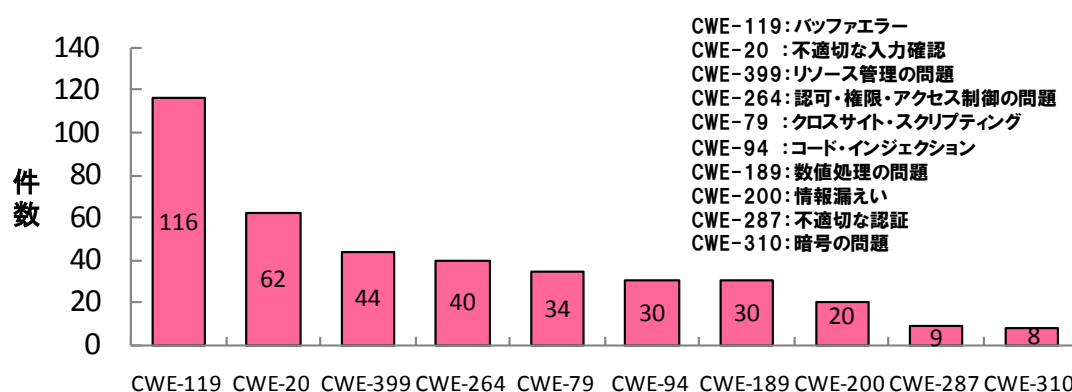


図4. 2010年第4四半期に登録した脆弱性の種類別件数

1.2 脆弱性に関する年別の深刻度別割合

図5のグラフはJVN iPediaに登録済みの脆弱性対策情報について、製品開発者やセキュリティポータルサイト等が脆弱性の対策情報を公開した日を基にした、脆弱性の深刻度別の件数の公開年別推移を示したものです。2008年までは増加傾向でしたが、2008年以降は横ばい状態となっており、深刻度の高い脆弱性の件数が大きな割合を占めています。

2010年12月31日までは、レベルIII（危険、CVSS基本値=7.0~10.0）が46%、レベルII（警告、CVSS基本値=4.0~6.9）が45%、レベルI（注意、CVSS基本値=0.0~3.9）が9%となっています。

深刻度の高い脆弱性が多数公開されていることから、製品利用者は情報を日々収集し、製品のバージョンアップやセキュリティ対策パッチの適用などを遅滞なく行うことが必要です。

⁷ Common Weakness Enumeration。概要は次を参照下さい。 <http://www.ipa.go.jp/security/vuln/CWE.html>

⁸ <http://www.ipa.go.jp/security/vuln/websecurity.html>

⁹ <http://www.ipa.go.jp/security/awareness/vendor/programmingv2/index.html>

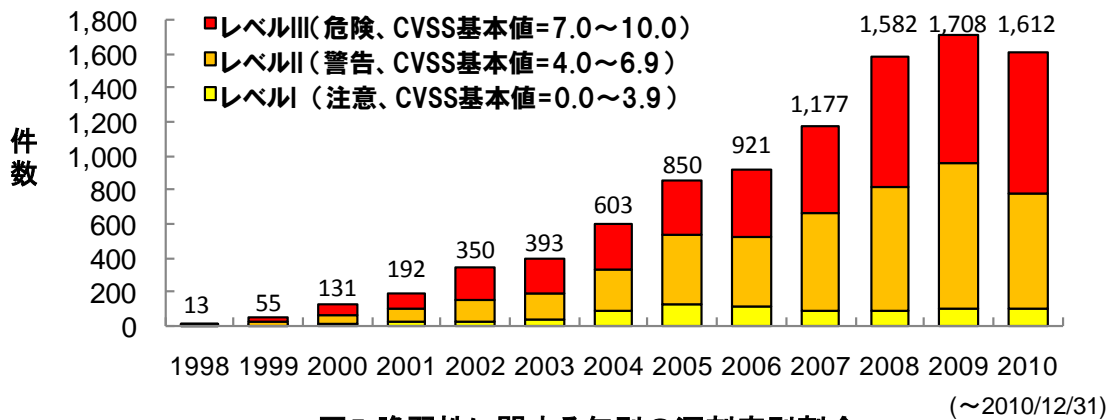


図5.脆弱性に関する年別の深刻度別割合

1.3 脆弱性対策情報を公表した製品の種別別件数

図6のグラフはJVN iPediaに登録済みの脆弱性対策情報について、その製品の種別別件数の公開年別推移を示したものです。Adobe Reader、Adobe Flash Player、Safari、Internet Explorer、Firefoxなどのデスクトップアプリケーションや、Webサーバ、アプリケーションサーバ、データベースなどのミドルウェア、また、PHP、Javaなど、アプリケーション・ソフトウェアの脆弱性対策情報の公開が年々増加しています。毎年、数多くのアプリケーションが新しく開発され、それらにおいて脆弱性が発見されており、**アプリケーション・ソフトウェアのセキュリティ対策は重要度を増しています。**

2008年頃からは、重要インフラなどで利用される、監視制御システム(SCADA: Supervisory Control And Data Acquisition)についても脆弱性の対策情報が公開されています。2008年分として8件、2009年分は9件、2010年分は6件、合計23件のSCADAに関する脆弱性対策情報を公開しています。

最近ではSCADAを攻撃対象とした、Windows シェルの脆弱性(MS10-046)を悪用して感染を拡げるウイルスStuxnet¹⁰も発見されています。**製品利用者は脆弱性対策情報を日々収集し、バージョンアップやセキュリティ対策パッチの適用などを遅滞なく行うことが必要です。**

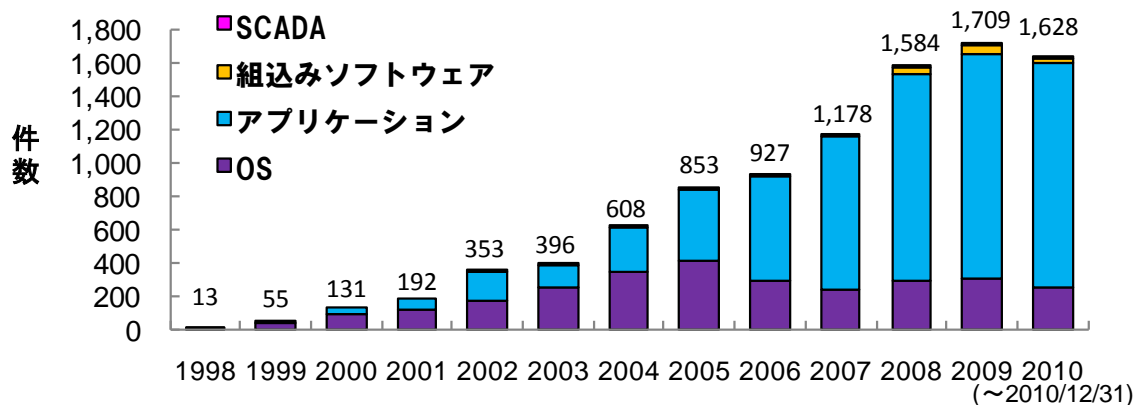


図6.脆弱性対策情報を公表した製品の種別別件数の公開年別推移

¹⁰ 原子力発電所の制御システムに影響を及ぼすウイルス。
 詳細は、IPA テクニカルウォッチ『新しいタイプの攻撃』に関するレポートも参照ください。
<http://www.ipa.go.jp/about/technicalwatch/20101217.html>

1.4 オープンソースソフトウェアの割合

図7のグラフはJVN iPediaに登録済みの脆弱性対策情報について、オープンソースソフトウェア(OSS)とOSS以外のソフトウェアの公開年別推移を示したものです。OSSの割合の年別推移を見ると、近年では2008年以降のOSSの割合が減少傾向となっており、2010年では20%の割合になっています。全体件数から見た割合は、OSSが33%、OSS以外が67%となっています。

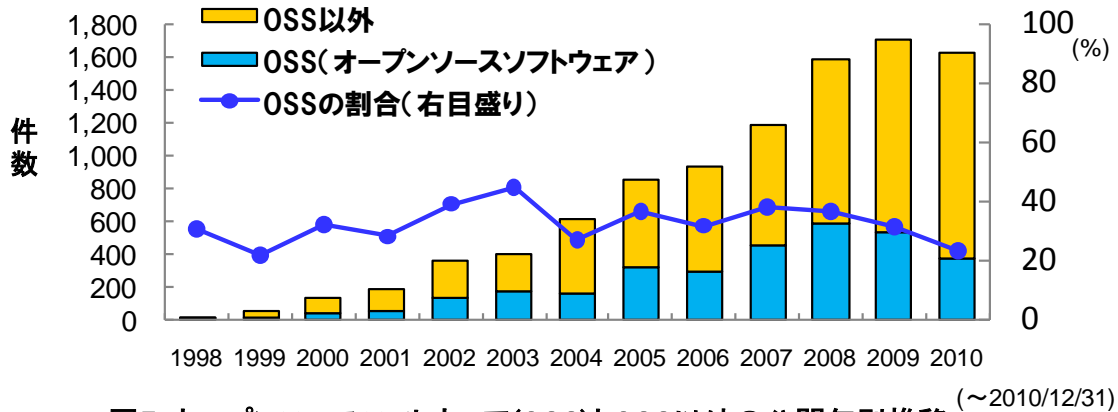


図7. オープンソースソフトウェア(OSS)とOSS以外の公開年別推移

1.5 ソフトウェア製品の開発者(ベンダー)の内訳

図8、図9のグラフは、JVN iPediaに登録済みのソフトウェア製品の開発者(ベンダー)に関して、OSSのベンダーの内訳とOSS以外のベンダーの内訳をそれぞれ示したものです。

OSSは、国内ベンダーが64、海外ベンダー(日本法人有り)が24、海外ベンダー(日本法人無し)が226、合計314ベンダーとなっています。OSS以外は、国内ベンダーが118、海外ベンダー(日本法人有り)が64、海外ベンダー(日本法人無し)が51、合計233ベンダーとなっています。

OSSに関しては、日本法人の無い海外ベンダーの脆弱性対策情報が数多く登録されています。**OSS**を利用する場合、製品のバージョンアップやセキュリティパッチの適用などのノウハウを持たない製品利用者は、製品のサポートサービスの活用、保守契約上の取り決め等の考慮が必要です。

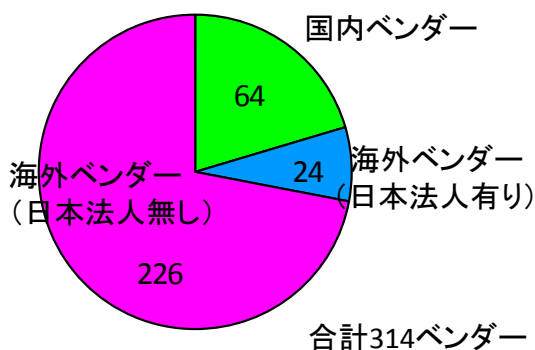


図8. OSSのベンダーの内訳

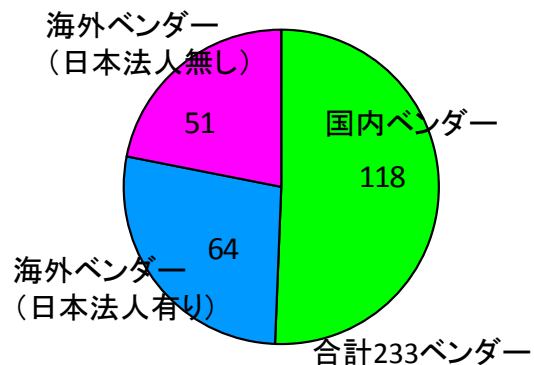


図9. OSS以外のベンダーの内訳

2.脆弱性対策情報の活用状況

～任意のDLL／実行ファイル読み込みに関する脆弱性が注目されています～

JVN iPedia のアクセス数は、2010 年 1 月～2010 年 12 月の 1 年間で 1,973 万件となっており、月平均で 160 万件を超えるアクセスがあります。

表 2 は 2010 年第 4 四半期(10 月～12 月)にアクセスの多かった JVN iPedia の脆弱性対策情報を、アクセス数の多い順に上位 20 件まで示しています。上位 20 件の内 9 件は IPA が「任意の DLL／実行ファイル読み込みに関する脆弱性の注意喚起」として注意喚起を行っている脆弱性です。この、任意の DLL／実行ファイル読み込みに関する脆弱性は、Microsoft Windows で動作する多数のソフトウェア製品が影響を受けます。また 20 件中 14 件が JVN から公表された脆弱性対策情報です。

なお、DNS 実装や SSL などは、脆弱性対策情報の公開から時間が経過しても多数のアクセスがあり、利用者が注目している情報となっています。

一般に広く利用されているソフトウェアに関する情報に着目すると、Lhaplusが 1 位と 5 位、Flash Playerが 9 位となっており、利用者からの注目を集めています。IPAでは、ウェブブラウザをはじめ、このようなソフトウェアが最新のバージョンかどうかを簡単に確認できるツール「MyJVNバージョンチェッカ¹¹」を無償で提供しています。「MyJVNバージョンチェッカ」などを活用し、ソフトウェアは常に脆弱性が解消された最新の状態で使用してください。

表 3 は国内の製品開発者から収集した脆弱性対策情報のアクセス数上位 5 件を示しています。

¹¹ MyJVN バージョンチェッカ。 <http://jvndb.jvn.jp/apis/myjvn/>

表 2.JVN iPediaの脆弱性対策情報のアクセス数上位 20 件 [2010 年 10 月～2010 年 12 月]

#	ID	タイトル	アクセス数	CVSS基本値	公開日
1	JVNDB-2010-000037	Lhaplus における DLL 読み込みに関する脆弱性	2892	6.8	2010/10/12
2	JVNDB-2010-000038	Lhasa における実行ファイル読み込みに関する脆弱性	2036	6.8	2010/10/12
3	JVNDB-2009-002319	SSL および TLS プロトコルに脆弱性	1147	6.4	2009/12/14
4	JVNDB-2010-000045	TeraPad における DLL 読み込みに関する脆弱性	1060	6.8	2010/10/21
5	JVNDB-2010-000039	Lhaplus における実行ファイル読み込みに関する脆弱性	744	6.8	2010/10/15
6	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	650	6.4	2008/7/23
7	JVNDB-2010-000047	Sleipnir および Grani における DLL 読み込みに関する脆弱性	596	6.8	2010/10/22
8	JVNDB-2010-000061	Movable Type における SQL インジェクションの脆弱性	565	6.8	2010/12/8
9	JVNDB-2010-000054	Flash Player におけるアクセス制限回避の脆弱性	565	2.6	2010/11/9
10	JVNDB-2010-001740	Apache Tomcat における重要な情報を取得される脆弱性	559	6.4	2010/7/29
11	JVNDB-2010-000066	アタッシュケースにおける実行ファイル読み込みに関する脆弱性	546	6.8	2010/12/17
12	JVNDB-2010-000052	一太郎シリーズにおける任意のコードが実行される脆弱性	533	9.3	2010/11/4
13	JVNDB-2010-000049	複数の Yokka 提供製品における実行ファイル読み込みに関する脆弱性	530	5.1	2010/10/22
14	JVNDB-2010-001174	Apache HTTP Server の ap_read_request 関数における重要な情報を取得される脆弱性	527	4.3	2010/3/23
15	JVNDB-2010-001229	OpenSSL における複数の関数に関する脆弱性	526	10.0	2010/4/9
16	JVNDB-2010-002118	64-bit プラットフォーム上で稼働している Linux kernel の compat_alloc_user_space 関数における権限昇格の脆弱性	525	7.2	2010/10/8
17	JVNDB-2010-000041	K2Editor における実行ファイル読み込みに関する脆弱性	514	5.1	2010/10/15
18	JVNDB-2010-000050	Active! mail 6 における HTTP ヘッダインジェクションの脆弱性	502	4.3	2010/10/29
19	JVNDB-2010-000051	GVim における DLL 読み込みに関する脆弱性	495	6.8	2010/11/1
20	JVNDB-2008-000084	PHP におけるクロスサイトスクリプティングの脆弱性	478	2.6	2008/12/19

表 3.国内の製品開発者から収集した脆弱性対策情報のアクセス数上位 5 件 [2010 年 10 月～2010 年 12 月]

#	ID	タイトル	アクセス数	CVSS 基本値	公開日
1	JVNDB-2008-001313	JP1/Cm2/Network Node Manager におけるサービス運用妨害 (DoS) の脆弱性	332	5.0	2008/5/9
2	JVNDB-2010-002077	Accela BizSearch の文書参照画面におけるフィッシング脅威の脆弱性	263	5.8	2010/10/1
3	JVNDB-2010-002078	Groupmax Scheduler Server における複数の脆弱性	248	9.0	2010/10/1
4	JVNDB-2008-001150	JP1/秘文の暗号化/復号機能および持ち出し制御機能における正しく動作が行われない問題	232	3.6	2008/3/14
5	JVNDB-2008-001895	JP1/VERITAS NetBackup の JAVA Administration GUI における特権昇格の脆弱性	225	6.5	2008/11/26

注 1) CVSS 基本値の深刻度による色分け

CVSS 基本値=0.0～3.9 深刻度=レベル I (注意)	CVSS 基本値=4.0～6.9 深刻度=レベル II (警告)	CVSS 基本値=7.0～10.0 深刻度=レベル III (危険)
------------------------------------	-------------------------------------	---------------------------------------

注 2) 公開日の年による色分け

2008 年以前の公開	2009 年の公開	2010 年の公開
-------------	-----------	-----------