脆弱性対策情報データベース JVN iPedia に関する活動報告レポート

[2013 年第 1 四半期（1 月～3 月)]

脆弱性対策情報データベース JVN iPedia に関する活動報告レポートについて

本レポートでは、2013 年 1 月 1 日から 2013 年 3 月 31 日までの間に JVN iPedia で登録をした脆弱性対策情報の統計について紹介しています。

独立行政法人情報処理推進機構 技術本部 セキュリティセンター

2013 年 4 月 18 日

目次

1. 2013 年第 1 四半期 脆弱性対策情報データベース JVN iPedia の登録状況

脆弱性対策情報データベース「JVN iPedia（ http://jvndb.jvn.jp/ ）」は、国内外で使用されているソフトウェアの脆弱性対策情報を収集・公開することにより、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 JVN (*1) で公表した脆弱性対策情報、3）米国国立標準技術研究所 NIST (*2) の脆弱性データベース「NVD (*3)」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。

1-1. 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 39,000 件を超過～

2013 年第 1 四半期（2013 年 1 月 1 日から 3 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 3 件（公開開始からの累計は 142 件）、JVN から収集したもの 85 件（累計 2,497 件）、NVD から収集したもの 1,149 件（累計 36,697 件）、合計 1,237 件（累計 39,336 件）となりました。**脆弱性対策情報の登録件数が、累計 39,000 件を超過しました**（表 1-1、図 1-1）。

表 1-1. 2013 年第 1 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	3 件	142 件
	JVN	85 件	2,497 件
	NVD	1,149 件	36,697 件
	計	1,237 件	39,336 件
英語版	国内製品開発者	3 件	142 件
	JVN	30 件	737 件
	計	33 件	879 件

JVN iPedia 英語版は、国内製品開発者から収集したものが 3 件（累計 142 件）、JVN から収集したものが 30 件（累計 737 件）、合計 33 件（累計 879 件）でした。

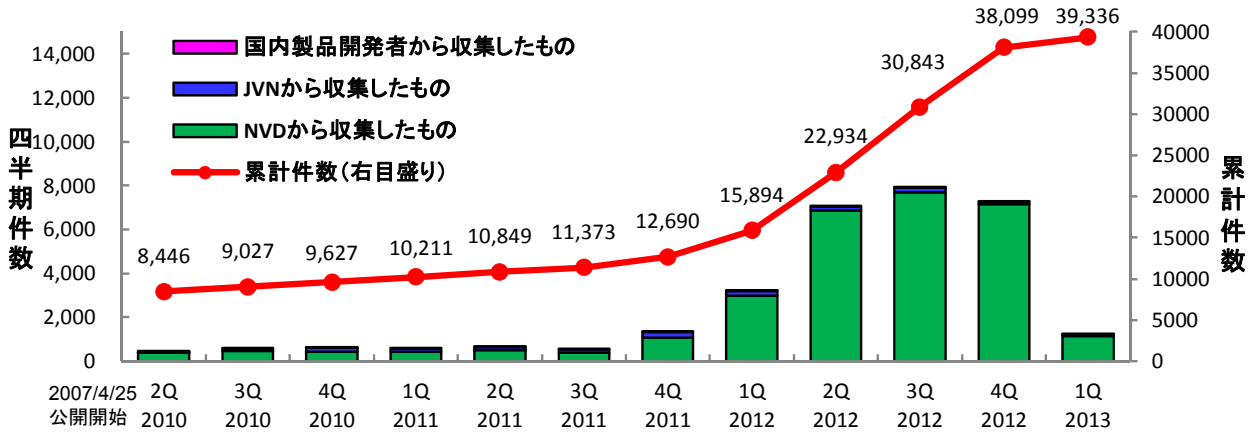

図1−1. JVN iPediaの登録件数の四半期別推移

IPA では、システム管理者が脆弱性対策に活用できるように、JVN iPedia に登録されている脆弱性対策情報の拡充を図っています。現在、2007 年以降に NVD に登録された脆弱性対策情報の全件が日本語に翻訳されて、JVN iPedia に登録されています。システム管理者は、幅広いソフトウェア製品に関する脆弱性対策情報を日本語で取得し、脆弱性対策に役立てることが可能です。

(*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

1-2. 脆弱性の種類別件数

図 1-2 のグラフは、JVN iPedia へ 2013 年第 1 四半期に登録した脆弱性対策情報を、CWE のタイプ別に分類した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 158 件、CWE-264（認可・権限・アクセス制御の問題）が 128 件、CWE-79（クロスサイト・スクリプティング）が 114 件、CWE-20（不適切な入力確認）が 98 件、CWE-399（リソース管理の問題）が 94 件、CWE-200（情報漏えい）が 74 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**ソフトウェアの企画・設計段階から、セキュリティ対策を講じる必要**があります。なお、IPA では、参考資料として**「セキュア・プログラミング講座 (*4)」**、実習形式による脆弱性体験学習ツール**「AppGoat (*5)」**を公開し、セキュアなプログラム開発の促進に努めています。

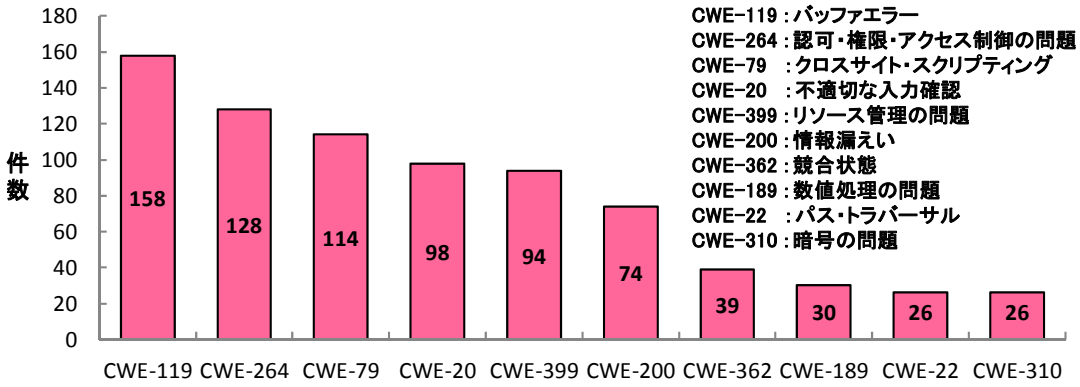

図1-2. 2013年第1四半期に登録した脆弱性の種類別件数

1-3. 脆弱性に関する深刻度別割合

図 1-3 のグラフは JVN iPedia に登録済みの脆弱性対策情報について、脆弱性の深刻度別の件数の公表年別推移を示したものです。

2013 年 3 月 31 日までに JVN iPedia に登録済みの脆弱性対策情報の深刻度別割合は、レベル III（危険、CVSS 基本値=7.0～10.0）が 45%、レベル II（警告、CVSS 基本値=4.0～6.9）が 49%、レベル I（注意、CVSS 基本値=0.0～3.9）が 6%となっています。

深刻度の高い脆弱性が多数登録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**などを速やかに行うことが重要です。

(*4) http://www.ipa.go.jp/security/awareness/vendor/programmingv2/index.html
(*5) 脆弱性体験学習ツール「AppGoat」。http://www.ipa.go.jp/security/vuln/appgoat/index.html

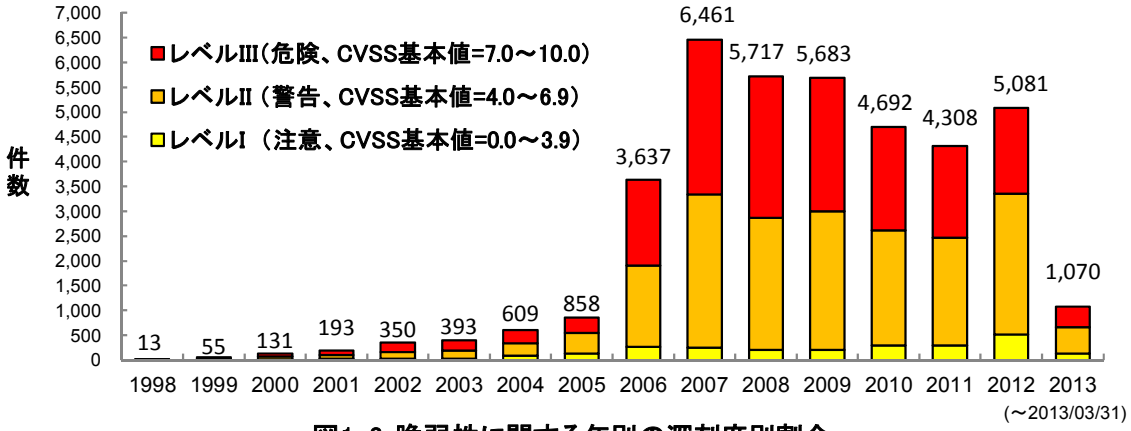

図1-3. 脆弱性に関する年別の深刻度別割合

1-4. 脆弱性対策情報を公表した製品の種類別件数

図 1-4 のグラフは JVN iPedia に登録済みの脆弱性対策情報について、その製品の種類別件数の公表年別推移を示したものです。2007 年以降の脆弱性対策情報を公表年別で見ると、アプリケーションに関する脆弱性対策情報の割合が 9 割前後を占めており、2013 年も同じ傾向になっています。

2008 年頃からは、重要インフラなどで利用される、産業用制御システムの脆弱性対策情報が登録されており、今四半期までに合計 340 件登録しています。

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、アプリケーションのセキュリティ対策は重要度を増しています。**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**などを速やかに行うことが重要です。

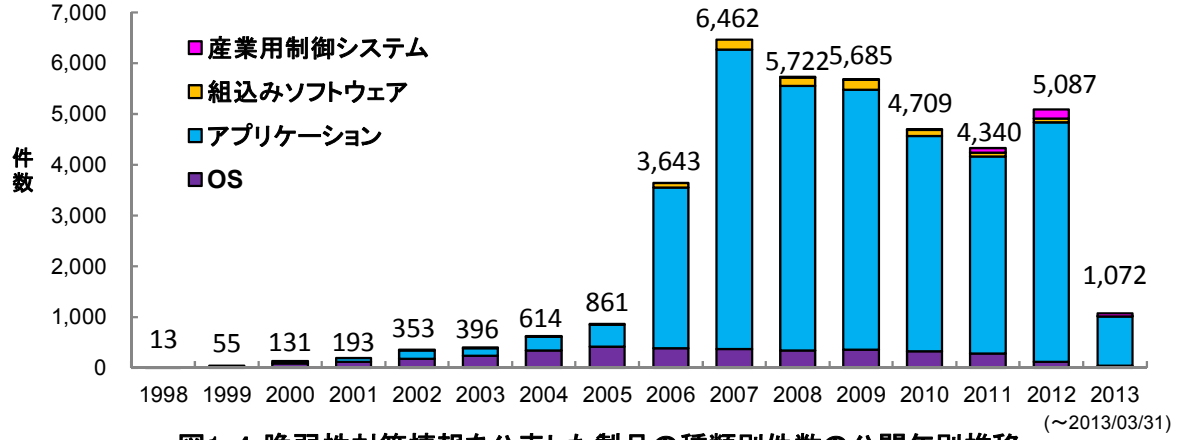

図1-4. 脆弱性対策情報を公表した製品の種類別件数の公開年別推移

1-5. オープンソースソフトウェアの割合

図 1-5 のグラフは JVN iPedia に登録済みの脆弱性対策情報について、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表年別推移を示したものです。累計で 15,937 件の OSS に関する情報を登録しており、全体の公開件数から見た割合は、OSS が 41%、OSS 以外が 59%となっています。

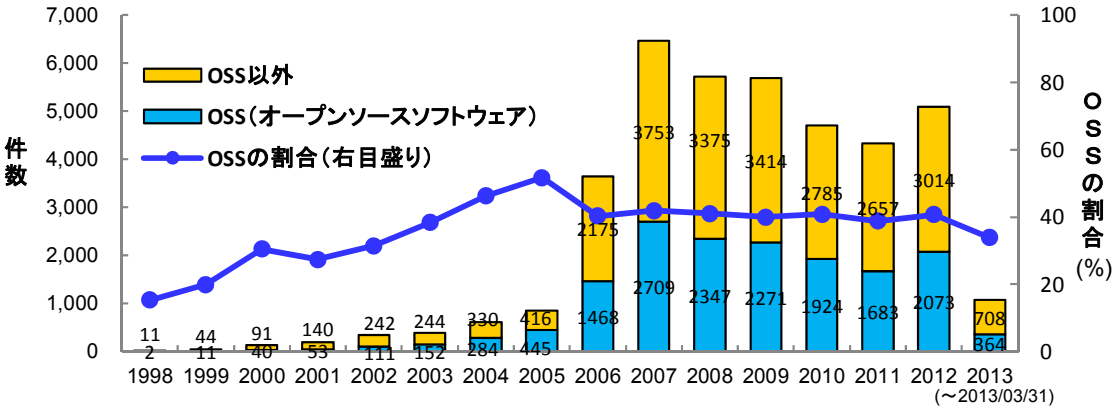

図1-5. オープンソースソフトウェア(OSS)とOSS以外の公開年別推移

1-6. 製品開発者（ベンダー）の内訳

図 1-6-1、図 1-6-2 のグラフは、JVN iPedia に登録済みの製品開発者（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 ベンダーの内訳は、国内ベンダーが 87、海外ベンダー（日本法人有り）が 68、海外ベンダー（日本法人無し）が 4,088、合計 4,243 ベンダーとなっています。OSS 以外は、国内ベンダーが 180、海外ベンダー（日本法人有り）が 209、海外ベンダー（日本法人無し）が 4,132、合計 4,521 ベンダーとなっています。

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。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**等の考慮を実施する必要があります。

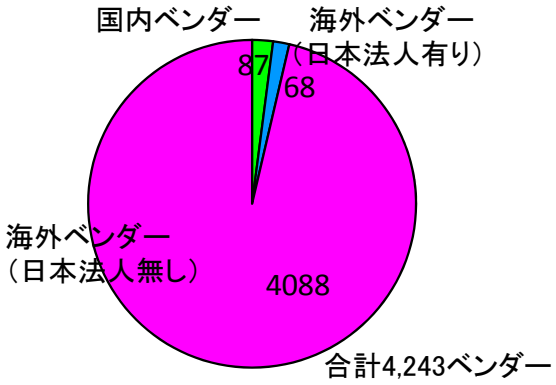

図1-6-1. OSSのベンダーの内訳

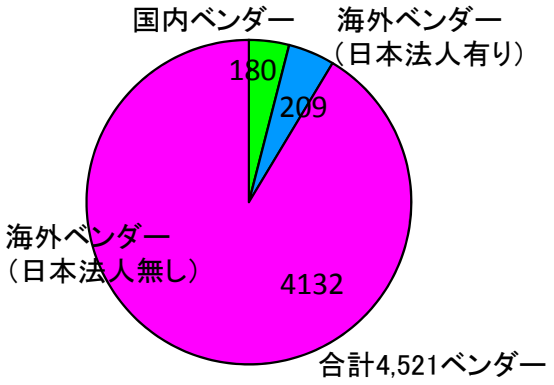

図1-6-2. OSS以外のベンダーの内訳

2. 2013 年第 1 四半期の注目すべき情報

2-1. 一般に広く利用されているソフトウェアの脆弱性について

～PC で広く利用されているソフトウェアの深刻な脆弱性対策情報が多数登録。速やかなバージョンアップを～

昨今の機密情報や個人情報の窃取を目的としたサイバー攻撃は、標的型メール攻撃に代表されるようにメールに添付したファイル等を経由し、ソフトウェアの脆弱性を悪用するウイルス感染手口が主流になっています。2013 年版 10 大脅威 (*6) でも、クライアントソフトを悪用した攻撃は、社会的な影響が大きかったセキュリティ上の脅威の 1 位となっています。

特に、ブラウザソフト、文書ソフト、実行環境などの一般に広く利用されているソフトウェアの脆弱性が悪用されています。図 2-1-1 は、PC で広く利用されているソフトウェア 8 製品の登録件数の年別推移です。2013 年第 1 四半期の登録件数は 292 件となっており、2012 年の 531 件と比較すると 3 ヶ月間だけで半数以上の件数になっています。

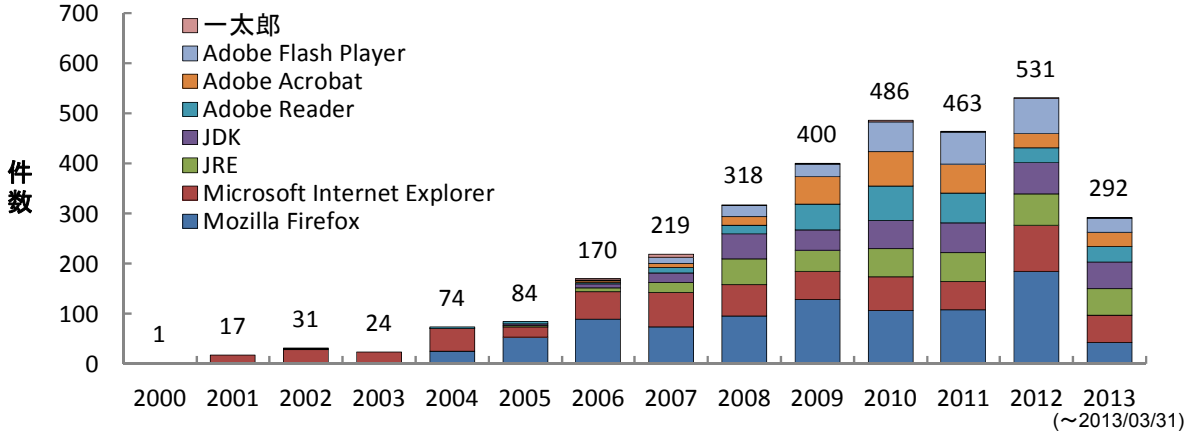

図2-1-1. PCで広く利用されているソフトウェアの脆弱性対策情報の登録件数の年別推移

JVN iPedia では、共通脆弱性評価システム CVSS (*7) により、それぞれの脆弱性の深刻度 (*8) を公開しています。図 2-1-2 は、PC で広く利用されているソフトウェア 8 製品における深刻度割合を集計したものです。内訳は Mozilla Firefox に関するものが 909 件、Microsoft Internet Explorer が 646 件、Adobe 3 製品（Reader、Acrobat、Flash Player）が 827 件です。これらの脆弱性の深刻度別の割合は、レベル III（危険、CVSS 基本値=7.0～10.0）が 65%、レベル II（警告、CVSS 基本値=4.0～6.9）が 32%、レベル I（注意、CVSS 基本値=0.0～3.9）が 3%となっており、レベル III の危険な脆弱性が約 2/3 を占めています。

(*6) プレス発表「『2013 年版 10 大脅威 身近に忍び寄る脅威』を公開」も参照。
http://www.ipa.go.jp/security/vuln/10threats2013.html

(*7) Common Vulnerability Scoring System、共通脆弱性評価システム。
http://www.ipa.go.jp/security/vuln/CVSS.html
脆弱性の基本評価基準の数値を基にⅠ,Ⅱ,Ⅲの 3 段階とし、数値が大きいほど深刻度が高い。
・レベルⅢ:リモートからシステムを完全に制御されるような場合や大部分の情報が漏えいするような脅威。
・レベルⅡ:一部の情報が漏えいするような場合やサービス停止につながるような脅威。
・レベルⅠ:攻撃する為の条件が複雑な場合や、レベルⅡに該当するが再現性が低い脅威。

(*8) 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

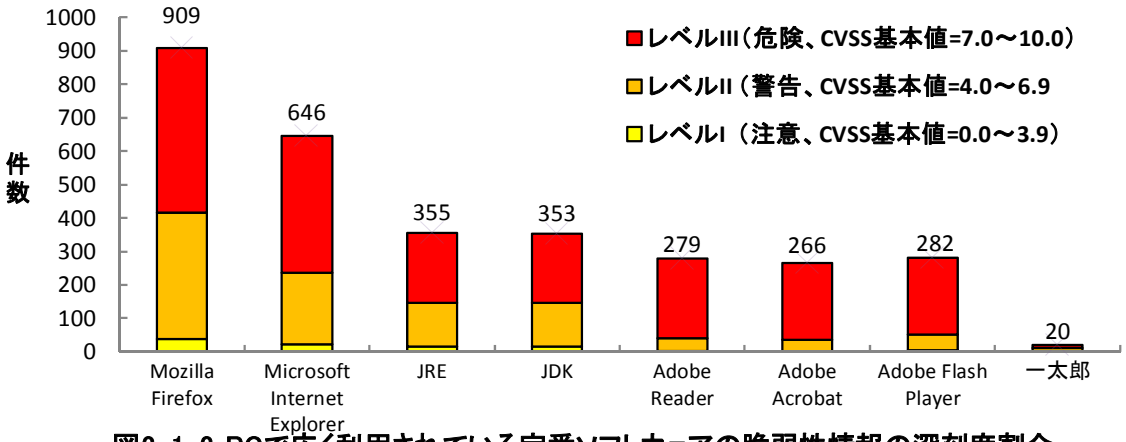

図2-1-2. PCで広く利用されている定番ソフトウェアの脆弱性情報の深刻度割合

深刻度の高い脆弱性が多数登録されています。**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速やかに**行ってください。

IPA では、使用しているソフトウェアのバージョンが最新であるか容易に確認できる **MyJVN バージョンチェッカ** (*9) を公開しています。また、**システム管理者向けに複数台の PC を自動的にチェックできるコマンドライン版** (*10) の提供もおこなっています。

2-2. 重要なセキュリティ情報の発信について

～重要なセキュリティ情報を毎日チェックしましょう！～

IPA では、多くの利用者が影響を受けるセキュリティ対策情報を対象に、「重要なセキュリティ情報」(*11) として、セキュリティ上の問題と対策についての情報発信を行っています。表 2-2 は、今四半期における重要なセキュリティ情報の発信一覧です。2013 年 1 月からの 3 ヶ月間では、既に攻撃が行われている等の「緊急」レベルの情報が 8 件、攻撃の情報は確認されていないが今後攻撃が行われる可能性がある「注意」レベルの情報が 9 件、計 17 件が公開されています。これは、2012 年第 4 四半期（10 月～12 月）の発信件数が 4 件であったことと比較をすると 4 倍以上に急増しています。

表 2-2. 2013 年第 1 四半期の「重要なセキュリティ情報」の発信一覧

発信日	レベル	タイトル
2013/1/9	注意	Adobe Reader および Acrobat の脆弱性対策について (APSB13-02)(CVE-2012-1530 等)
2013/1/9	注意	Adobe Flash Player の脆弱性対策について(APSB13-01)(CVE-2013-0630)
2013/1/15	緊急	Oracle Java の脆弱性対策について(CVE-2013-0422)
2013/1/15	緊急	Internet Explorer の脆弱性対策について(MS13-008)(CVE-2012-4792)
2013/2/4	緊急	Oracle Java の脆弱性対策について(CVE-2013-0437 等)
2013/2/8	緊急	Adobe Flash Player の脆弱性対策について(APSB13-04)(CVE-2013-0633 等)

(*9) MyJVN バージョンチェッカ。 http://jvndb.jvn.jp/apis/myjvn/
(*10) プレス発表「オフライン環境でもチェックが可能となった MyJVN バージョンチェッカ」も参照。
(*11) 重要なセキュリティ情報とは。
https://www.ipa.go.jp/security/announce/about.html

発信日	レベル	タイトル
2013/2/13	緊急	Internet Explorer の脆弱性対策について(MS13-010)(CVE-2013-0030)
2013/2/13	注意	Adobe Flash Player の脆弱性対策について(APSB13-05)(CVE-2013-1372 等)
2013/2/20	注意	Oracle Java の脆弱性対策について(CVE-2013-1487 等)
2013/2/21	緊急	Adobe Reader および Acrobat の脆弱性対策について (APSB13-07)(CVE-2013-0640 等
2013/2/21	注意	日本電気製「Universal RAID Utility」の脆弱性対策について
2013/2/26	注意	複数のジャストシステム製品の脆弱性対策について
2013/2/27	緊急	Adobe Flash Player の脆弱性対策について(APSB13-08)(CVE-2013-0643 等)
2013/3/5	緊急	Oracle Java の脆弱性対策について(CVE-2013-1493)
2013/3/7	注意	複数の Cisco 製スイッチの脆弱性対策について
2013/3/13	注意	Adobe Flash Player の脆弱性対策について(APSB13-09)(CVE-2013-0646 等)
2013/3/28	注意	DNS サーバ BIND の脆弱性対策について(CVE-2013-2266)
2013/3/28	注意	Adobe Reader および Acrobat の脆弱性対策について (APSB13-02)(CVE-2012-1530 等)

発信している情報の内訳を見ると、Adobe Flash Player に関する情報が 5 件、Oracle 社が提供する JDK（Java Development Kit）や JRE（Java Runtime Environment）といった Java プログラムに関する情報が 4 件となっており、公開した情報の半数以上を占めています。

また、Adobe Flash Player、JDK および JRE の脆弱性の公開件数が年々増加しています。図 2-2 は、JVNiPedia における Adobe Flash Player、JDK および JRE の脆弱性対策情報の登録件数の推移になります。Adobe Flash Player、JDK および JRE の脆弱性対策情報の 2013 年第 1 四半期の登録件数は 134 件となっており、3 ヶ月間だけで前年比の 2/3 以上の件数になっており、脆弱性の公開が増加する傾向にあります。

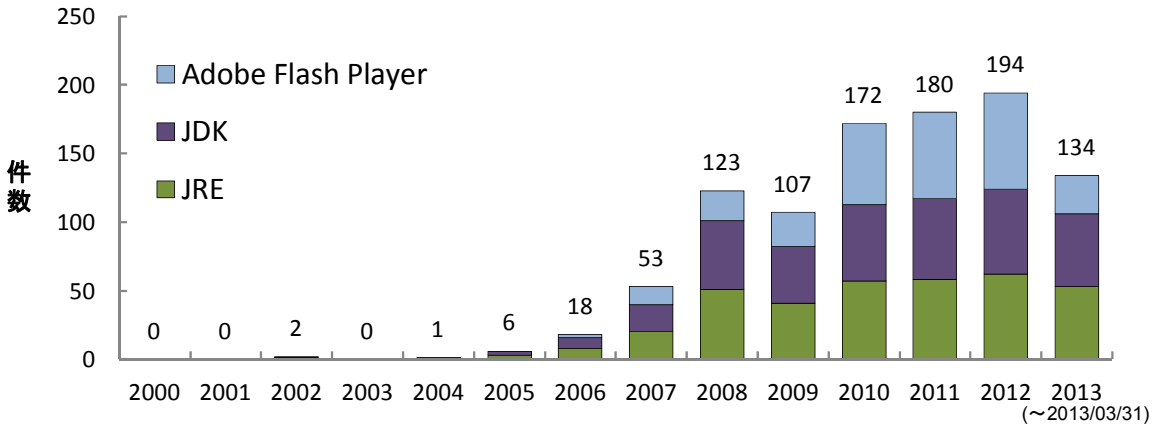

図2-2. Adobe Flash Player、JDKおよびJREのJVN iPediaへの登録件数の推移

Adobe Flash Player や JDK、JRE などのソフトウェアに関しては、**脆弱性対策情報の増加を見るだけでなく**、利用が不要な場合、該当ソフトウェアの**アンインストールを含めたセキュリティ対策**を実施してください。

2-3. 産業用制御システムの脆弱性について

～ 産業用制御システムに関する脆弱性対策情報が年々増加 ～

近年、工場の生産設備等で使用される監視モニタ等の産業用制御システム（ICS：Industrial Control Systems）に関するソフトウェアの脆弱性対策情報が増加しています。

図 2-3-1 は、JVN iPedia における産業用制御システムに関するソフトウェアの脆弱性対策情報の、登録件数と深刻度の割合を示しています。**2013 年も深刻度の高いレベル III の脆弱性が 46 件の登録のうち 24 件、と半数以上**を占めており、前年までの傾向が引き継がれています。

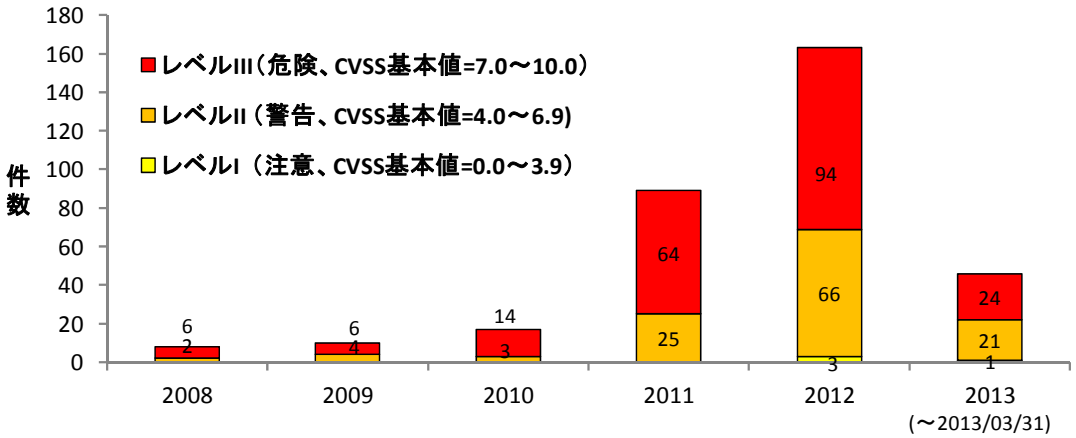

図2-3-1. 産業用制御システムに関するソフトウェアの脆弱性件数と深刻度割合の年別推移

図 2-3-2、図 2-3-3 のグラフは、JVN iPedia に登録済みの脆弱性対策情報に関して、産業用制御システムに関するソフトウェアと全体の深刻度の割合をそれぞれ示したものです。産業用制御システムに関するソフトウェアの深刻度の割合は、レベル III（危険、CVSS 基本値=7.0～10.0）が 63%、レベル II（警告、CVSS 基本値=4.0～6.9）が 36%、レベル I（注意、CVSS 基本値=0.0～3.9）が 1%となっており、ソフトウェア全体と比較して、深刻度の高い脆弱性対策情報が多く登録されています。

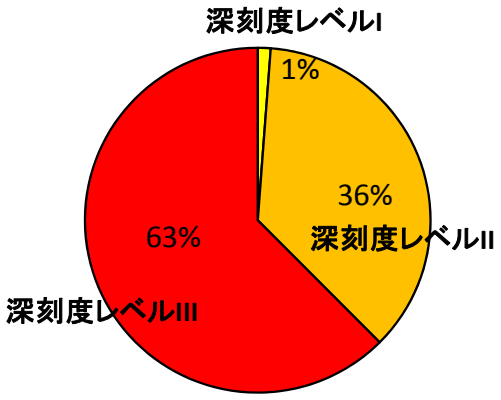

図2-3-2. 深刻度の割合（産業用制御システム）

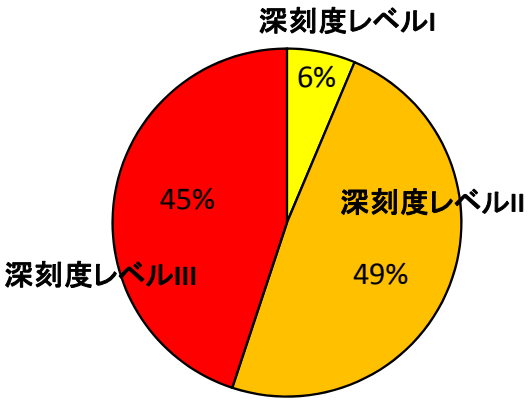

図2-3-3. 深刻度の割合（全体）

図 2-3-4 は、産業用制御システムに関するソフトウェアの脆弱性対策情報を、CWE [(*12)] のタイプ

(*12) Common Weakness Enumeration。概要は次を参照ください。
http://www.ipa.go.jp/security/vuln/CWE.html

別に分類した件数を示したものです。任意コードの実行などの重大な脅威につながる CWE-119（バッファーエラー）の件数が 102 件となっており、CWE-22(パス・トラバーサル)などの件数と比較をすると 3 倍以上の件数になっています。

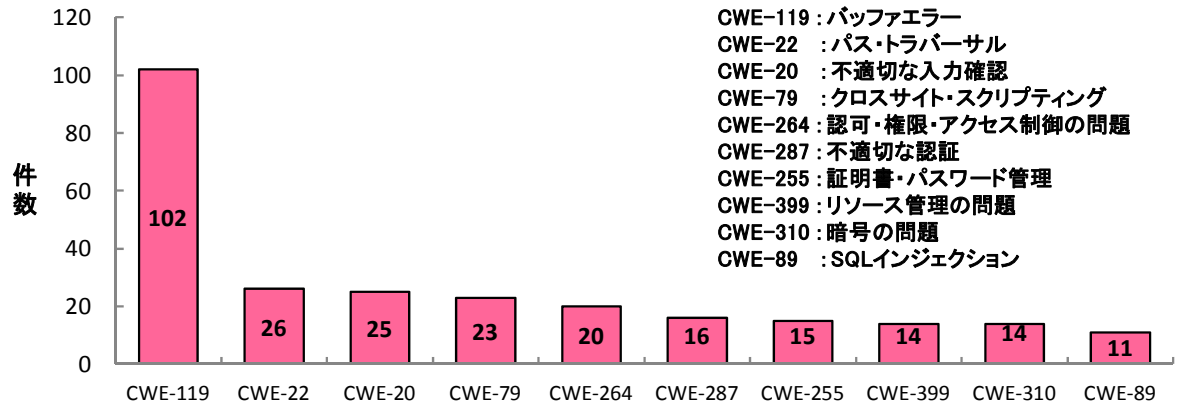

図2-3-4. 産業用制御システムを構成するソフトウェアの脆弱性の種類別件数

産業用制御システムの利用者は、**脆弱性対策情報を定期的に収集**し、利用している製品に**脆弱性が存在**する場合、開発元や販売元に**バージョンアップ等の対策方法の有無を確認**し、対策が存在する場合は**速やかな対応を検討**してください。直ちに対策することが**困難な場合**は、産業用制御システムが設置されている**ネットワーク等の利用環境やリスクを評価**し、その**改善や対策を図る**などの対応を検討してください。(*13)

(*13) 制御機器の脆弱性に関する注意喚起 http://www.ipa.go.jp/about/press/20120229.html

3. 脆弱性対策情報の活用状況

表 3-1 は 2013 年第 1 四半期（1 月～3 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。

表 3-2 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。

表 3-1.JVN iPedia の脆弱性対策情報のアクセス数上位 20 件 [2013 年 1 月～2013 年 3 月]

#	ID	タイトル	アクセス数	CVSS 基本値	公開日
1	JVNDB-2013-001027	Oracle Java 7 に脆弱性	5081	10.0	2013/1/11
2	JVNDB-2013-001912	Perl のハッシュ値の再計算メカニズムにおけるサービス運用妨害 (DoS) の脆弱性	2411	7.5	2013/3/21
3	JVNDB-2012-001258	Apache HTTP Server の protocol.c における HTTPOnly cookies の値を取得される脆弱性	1867	4.3	2012/2/1
4	JVNDB-2013-000012	NEC Universal RAID Utility におけるアクセス制限不備の脆弱性	1668	9.0	2013/2/21
5	JVNDB-2013-001019	Ruby on Rails に複数の脆弱性	1568	7.5	2013/1/10
6	JVNDB-2013-000017	複数の Cisco 製品におけるサービス運用妨害 (DoS) の脆弱性	1464	7.8	2013/3/7
7	JVNDB-2013-001237	Movable Type の mt-upgrade.cgi における eval インジェクションおよび SQL インジェクションの脆弱性	1290	7.5	2013/1/24
8	JVNDB-2012-005828	Internet Explorer に任意のコードが実行される脆弱性	1210	9.3	2013/1/4
9	JVNDB-2013-001460	TLS プロトコルおよび DTLS プロトコルにおける識別攻撃およびプレーンテキストリカバリ攻撃を誘発される脆弱性	1071	2.6	2013/2/13
10	JVNDB-2011-002172	Apache HTTPD サーバにサービス運用妨害 (DoS) の脆弱性	1046	7.8	2011/9/1
11	JVNDB-2011-002110	Samba Web Administration Tool におけるクロスサイトリクエストフォージェリの脆弱性	1006	4.0	2011/8/18
12	JVNDB-2013-000015	複数のジャストシステム製品において任意のコードが実行される脆弱性	971	6.8	2013/2/26
13	JVNDB-2013-000005	Android 版 ウェザーニュースタッチにおいて位置情報をログに出力する脆弱性	915	2.6	2013/1/31
14	JVNDB-2011-002305	SSL と TLS の CBC モードに選択平文攻撃の脆弱性	898	4.3	2011/10/4
15	JVNDB-2013-000008	サイボウズ ガルーンにおけるクロスサイトスクリプティングの脆弱性	855	2.6	2013/2/8
16	JVNDB-2013-001056	Oracle Java SE における任意のコードを実行される脆弱性	846	10.0	2013/1/15
17	JVNDB-2013-000007	サイボウズ ガルーンにおける SQL インジェクションの脆弱性	803	6.5	2013/2/8

#	ID	タイトル	アクセス数	CVSS 基本値	公開日
18	JVNDB-2012-000113	concrete5 におけるクロスサイトスクリプティングの脆弱性	802	2.6	2012/12/21
19	JVNDB-2009-002319	SSL および TLS プロトコルに脆弱性	792	6.4	2009/12/14
20	JVNDB-2012-000115	Android 版 ロケタッチにおける情報管理不備の脆弱性	789	2.6	2012/12/21

表 3-2.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 [2013 年 1 月～2013 年 3 月]

#	ID	タイトル	アクセス数	CVSS 基本値	公開日
1	JVNDB-2012-005827	複数の日立製品に含まれる Collaboration - Bulletin board におけるクロスサイトスクリプティングの脆弱性	768	4.3	2012/12/28
2	JVNDB-2013-001605	Hitachi Tuning Manager および JP1/Performance Management における複数の脆弱性	515	9.0	2013/2/20
3	JVNDB-2013-001321	日立 Cosminexus の運用管理機能におけるユーザ認証の脆弱性	457	6.8	2013/1/31
4	JVNDB-2013-001470	Accela BizSearch におけるユーザになりすまされる脆弱性	388	6.8	2013/2/13
5	JVNDB-2012-005486	JP1/Automatic Job Management System 3 および JP1/Automatic Job Management System 2 におけるサービス運用妨害 (DoS) の脆弱性	321	5.0	2012/11/22

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

2011 年以前の公開	2012 年の公開	2013 年の公開