

# 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

[2018 年第 4 四半期（10 月～12 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、2018 年 10 月 1 日から 2018 年 12 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及び事例について紹介しています。

## 目次

1. 2018 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 .....	- 3 -
1-1. 脆弱性対策情報の登録状況 .....	- 3 -
1-2. 【注目情報 1】Java SE の脆弱性について .....	- 4 -
1-3. 【注目情報 2】JVN iPedia に登録された脆弱性の種類別件数 .....	- 5 -
2. JVN iPedia の登録データ分類 .....	- 6 -
2-1. 脆弱性の種類別件数 .....	- 6 -
2-2. 脆弱性に関する深刻度別割合 .....	- 7 -
2-3. 脆弱性対策情報を公開した製品の種類別件数 .....	- 9 -
3. 脆弱性対策情報の製品別登録状況 .....	- 10 -
4. 脆弱性対策情報の活用状況 .....	- 11 -

# 1. 2018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

脆弱性対策情報データベース「JVN iPedia ( <https://jvndb.jvn.jp/> )」は、ソフトウェア製品に関する脆弱性対策情報を2007年4月25日から日本語で公開しています。システム管理者が迅速に脆弱性対策を行えるよう、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<sup>(1)</sup> 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<sup>(2)</sup> の脆弱性データベース「NVD<sup>(3)</sup>」が公開した脆弱性対策情報を集約、翻訳しています。

## 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の累計は92,674件～

2018年第4四半期(2018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右表の通りとなり、**脆弱性対策情報の登録件数の累計は、92,674件**でした(表1-1、図1-1)。

また、JVN iPedia英語版へ登録した脆弱性対策情報は右表の通り、累計で1,997件になりました。

表 1-1. 2018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	210件
	JVN	66件	8,271件
	NVD	3,488件	84,193件
	計	3,560件	92,674件
英語版	国内製品開発者	6件	210件
	JVN	36件	1,787件
	計	42件	1,997件

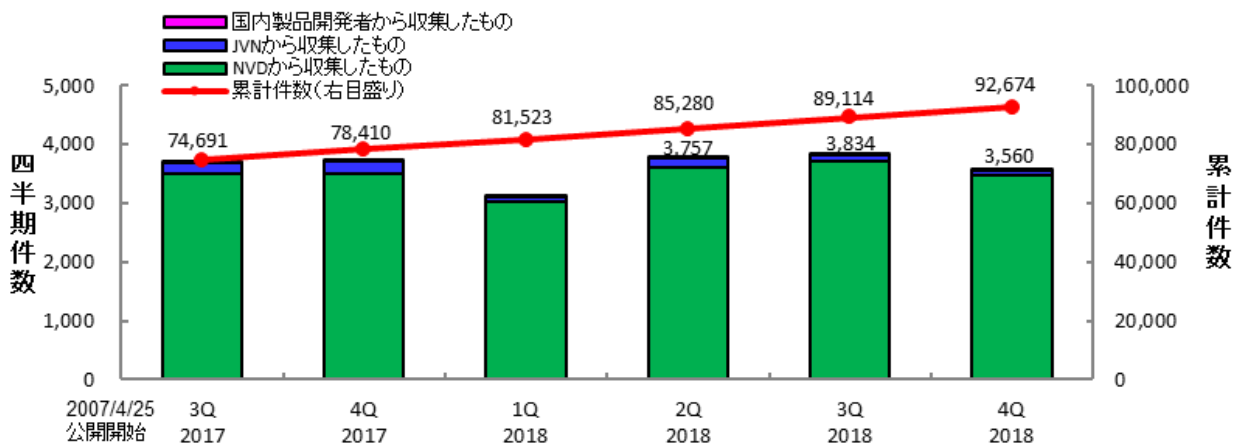


図1-1. JVN iPediaの登録件数の四半期別推移

(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。 <https://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 : <https://www.nist.gov>

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

## 1-2. 【注目情報 1】 Java SE の脆弱性について

～比較的高い深刻度レベルの脆弱性が多数確認されている Java SE 8 の無償サポートが終了～

Java SE の開発元であるオラクルコーポレーションより、商用ユーザーに向けた「Java SE 8 (Java Platform, Standard Edition8)」の無償のアップデート・リリースを 2019 年 1 月をもって終了すると案内<sup>(4)</sup>がされました。サポートを受けられない状態でソフトウェアを利用し続けた場合、新たな脆弱性が発見されても、修正パッチが開発元から提供されないため、脆弱性を悪用した攻撃による情報漏えいや意図しないサービス停止などの被害を受ける可能性があります。Java SE は多くの組織で利用されているソフトウェアであり、被害が発生した場合の影響が大きいことから、IPA では注意喚起情報<sup>(5)</sup>を公開しています。

図 1-2 は、1 年間(2018 年 1 月 1 日～2018 年 12 月 31 日)に JVN iPedia へ登録された、Java SE 8 に関する脆弱性対策情報の深刻度別割合です。脆弱性の深刻度が最も高いレベル III (CVSS 基本値=7.0～10.0) の脆弱性対策情報は登録されていませんが、深刻度が次に高いレベル II (CVSS 基本値=4.0～6.9) の脆弱性対策情報が 48 件中 38 件と全体の 8 割近くを占めています。今後も同等の脆弱性が公表される可能性があるため、脆弱性を悪用した攻撃から自組織のシステムを守るために、Java SE 8 を継続利用する場合は有償サポート契約の検討等の対応が必要となります。

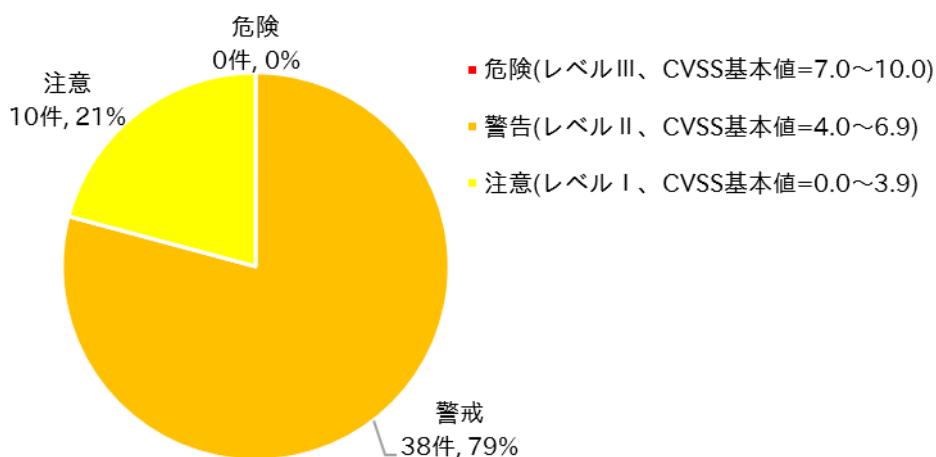


図1-2. 2018年(1/1～12/31)に登録されたJava SE 8の深刻度別割合 (CVSSv2)

<sup>(4)</sup> サポート・ロードマップ

<https://www.oracle.com/technetwork/jp/java/eol-135779-ja.html>

<sup>(5)</sup> 公式アップデートの提供方法の変更に伴う Java SE の商用ユーザーに向けた注意喚起

[https://www.ipa.go.jp/security/announce/java8\\_eol.html](https://www.ipa.go.jp/security/announce/java8_eol.html)

### 1-3. 【注目情報 2】 JVN iPedia に登録された脆弱性の種類別件数 ～昨年に引き続きクロスサイト・スクリプティングとバッファエラーが上位を占める。 複数のトークンに確認された整数オーバーフローも急増～

図 1-3 は、2018 年に JVN iPedia へ登録した脆弱性対策情報を共通脆弱性タイプ一覧(CWE)によって分類し、件数の多い 10 個の CWE について、2017 年の登録件数と比較したものです。

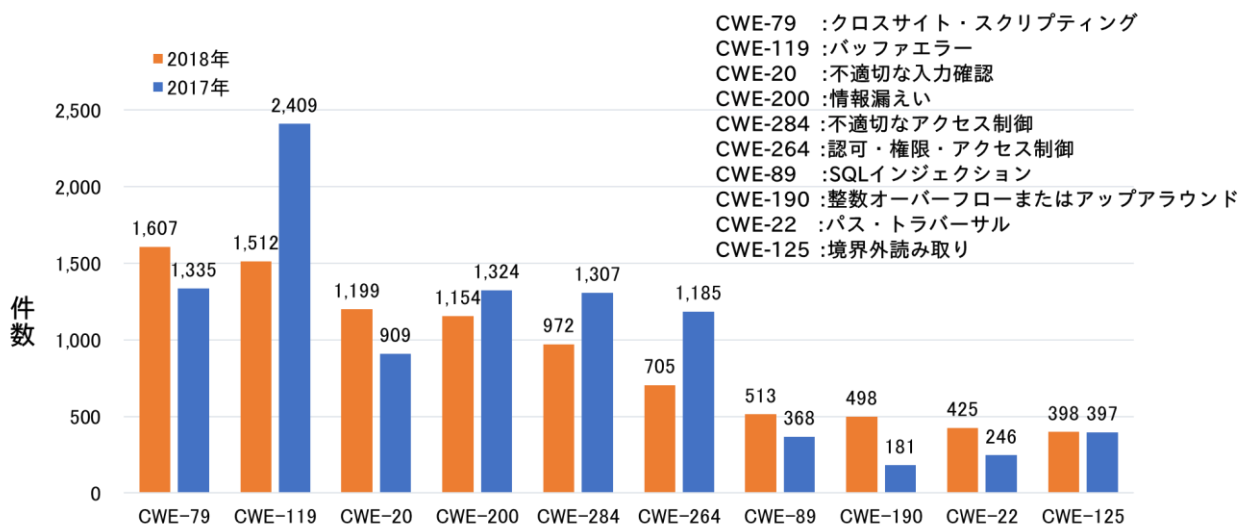


図1-3. 2017年と2018年に登録された脆弱性の種類別件数

2018 年に登録された CWE を多い順に見ていくと、1 位は CWE-79（クロスサイト・スクリプティング）で、2 位に CWE-119（バッファエラー）が続いています。上位 2 つは前年 2017 年と同じ CWE となっています。なお、CWE-119 は 2017 年と比較して大きく減り、2 位となっていますが、これは JVN iPedia の収集元の 1 つである NVD において CWE-119 に該当する脆弱性の公開が大きく減ったためです。また、3 位に CWE-20（不適切な入力確認）、4 位に CWE-200（情報漏えい）、5 位に CWE-284（不適切なアクセス制御）が続いています。これらの上位 5 位までの CWE で 2018 年に公開した脆弱性対策情報の約半分の件数を占めています。

また、2018 年の特徴的な脆弱性として、8 位の CWE-190（整数オーバーフローまたはアップアラウンド）が挙げられます。2017 年には 181 件だった登録件数が、2018 年には 498 件と 2 倍以上に増加しています。これは、イーサリアム<sup>(6)</sup>が提供するトークン規格の ERC20<sup>(7)</sup>に準拠した数 100 個のトークンにおいて、CWE-190 に該当する脆弱性があったことが一因として挙げられます。この脆弱性が悪用された場合、攻撃者は生成した不正なトークンと仮想通貨を交換し、結果として価格操作されてしまう可能性があります。このため、複数の仮想通貨取引所において ERC20 に準拠したトークンの取引を停止する等の対応が取られました。<sup>(8)</sup>

<sup>(6)</sup> イーサリアム、

<https://www.ethereum.org/>

<sup>(7)</sup> ERC20 Token（トークン）

<https://github.com/ethereum/EIPs/blob/master/EIPS/eip-20.md>

<sup>(8)</sup> New batchOverflow Bug in Multiple ERC20 Smart Contracts (CVE-2018-10299)

<https://medium.com/@peckshield/alert-new-batchoverflow-bug-in-multiple-erc20-smart-contracts-cve-2018-10299-511067db6536>

## 2. JVN iPedia の登録データ分類

### 2-1. 脆弱性の種類別件数

図 2-1 は、2018 年第 4 四半期（10 月～12 月）に JVN iPedia へ登録した脆弱性対策情報を、共通脆弱性タイプ一覧(CWE)によって分類し、件数を集計したものです。

集計結果は件数が多い順に、CWE-79（クロスサイトスクリプティング）が 490 件、CWE-119（バッファエラー）が 390 件、CWE-20（不適切な入力確認）が 292 件、CWE-284（不適切なアクセス制御）が 270 件、CWE-200（情報漏えい）が 249 件でした。

最も件数の多かった CWE-79（クロスサイトスクリプティング）は、悪用されると偽のウェブページが表示されたり、情報が漏えいしたりする可能性があります。

製品開発者は、ソフトウェアの企画・設計段階から、脆弱性の低減に努めることが求められます。なお、IPA ではそのための資料やツールとして、開発者や運営者がセキュリティを考慮したウェブサイトを作成するための資料「[安全なウェブサイトの作り方](#)<sup>(9)</sup>」や「[IPA セキュア・プログラミング講座](#)<sup>(10)</sup>」、脆弱性の仕組みを実習形式や演習機能で学ぶことができる脆弱性体験学習ツール「[AppGoat](#)<sup>(11)</sup>」などを公開しています。

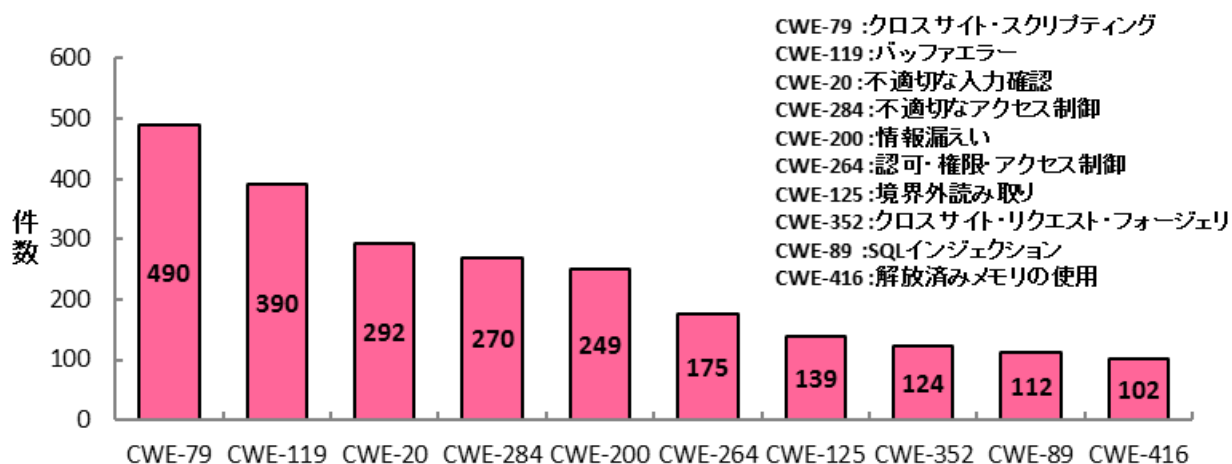


図2-1. 2018年第4四半期に登録された脆弱性の種類別件数

<sup>(9)</sup> IPA：「安全なウェブサイトの作り方」  
<https://www.ipa.go.jp/security/vuln/websecurity.html>

<sup>(10)</sup> IPA：「IPA セキュア・プログラミング講座」  
<https://www.ipa.go.jp/security/awareness/vendor/programming/>

<sup>(11)</sup> IPA：脆弱性体験学習ツール「AppGoat」  
<https://www.ipa.go.jp/security/vuln/appgoat/>

## 2-2. 脆弱性に関する深刻度別割合

図 2-2 は JVN iPedia に登録済みの脆弱性対策情報を CVSSv2 の値に基づいて深刻度別に分類し、登録年別にその推移を示したものです。

2018 年に JVN iPedia に登録した脆弱性対策情報は深刻度別に、レベル III が全体の 26.5%、レベル II が 63.0%、レベル I が 10.5% となっており、情報の漏えいや改ざんされるような危険度が高い脅威であるレベル II 以上が 89.5% を占めています。

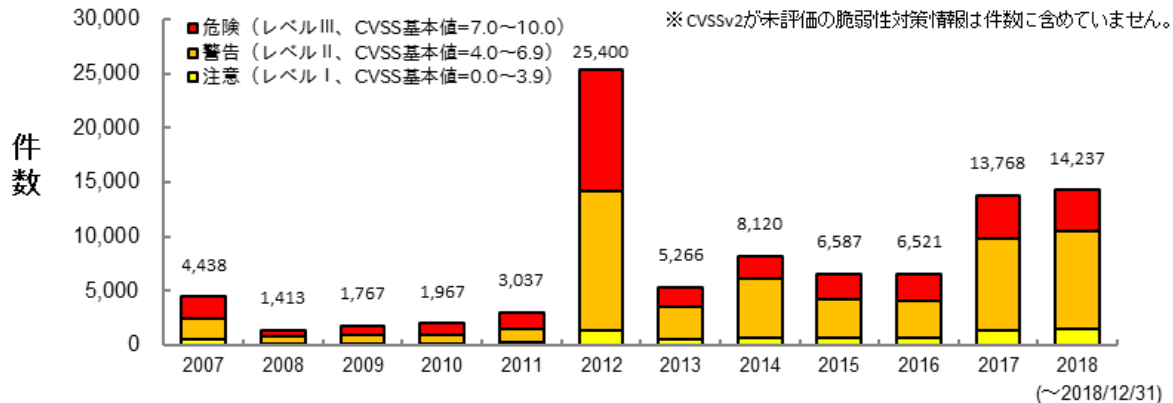


図2-2. 脆弱性の深刻度別件数(CVSSv2)

図 2-3 は JVN iPedia に登録済みの脆弱性対策情報を CVSSv3 の値に基づいて深刻度別に分類し、登録年別にその推移を示したものです。

2018 年に JVN iPedia に登録した脆弱性対策情報は深刻度別に、「緊急」が全体の 16.0%、「重要」が 46.3%、「警告」が 36.6%、「注意」が 1.1% となっています。

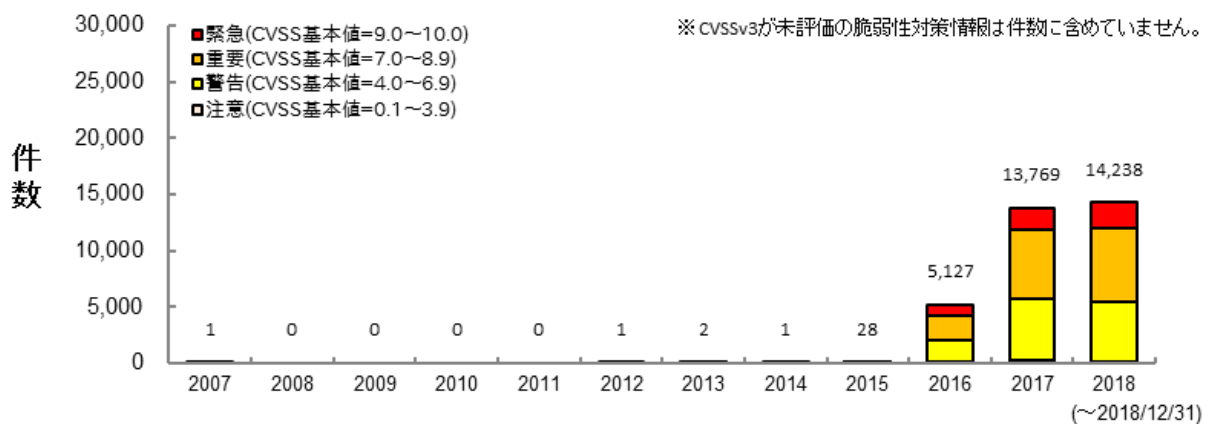


図2-3. 脆弱性の深刻度別件数(CVSSv3)

既知の脆弱性による脅威を回避するため、製品開発者は常日頃から新たに報告される脆弱性対策情報に注意を払うと共に、脆弱性が解消されている製品へのバージョンアップやアップデートなどを速やかに行ってください。

なお、新たに登録した JVN iPedia の情報を、RSS 形式や XML 形式<sup>([\\*12](#))</sup> で公開しています。

---

<sup>([\\*12](#))</sup> IPA : データフィード  
<https://jvndb.jvn.jp/ja/feed/>



### 2-3. 脆弱性対策情報を公開した製品の種別別件数

図 2-4 は JVN iPedia に登録済みの脆弱性対策情報を、ソフトウェア製品の種別別に件数を集計し、年次でその推移を示したものです。2018 年で最も多い種別はアプリケーションに関する脆弱性対策情報で、2018 年の件数全件の約 78.3% (11,164 件 / 全 14,264 件) を占めています。

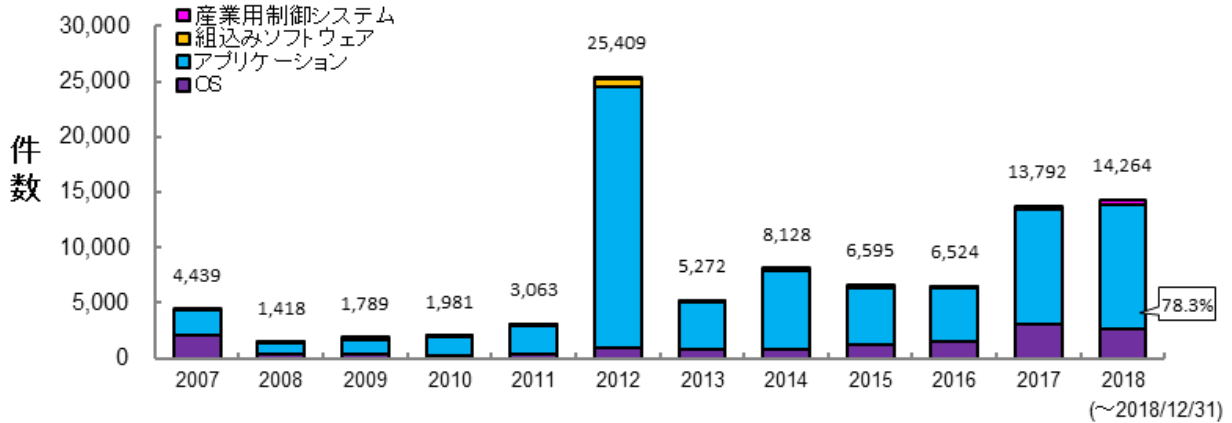


図2-4. 脆弱性対策情報を公表した製品の種別別件数の公開年別推移

図 2-5 は重要インフラなどで利用される、産業用制御システムに関する脆弱性対策情報の件数を集計し、年次でその推移を示したものです。これまでに累計で 1,635 件を登録しています (図 2-5)。

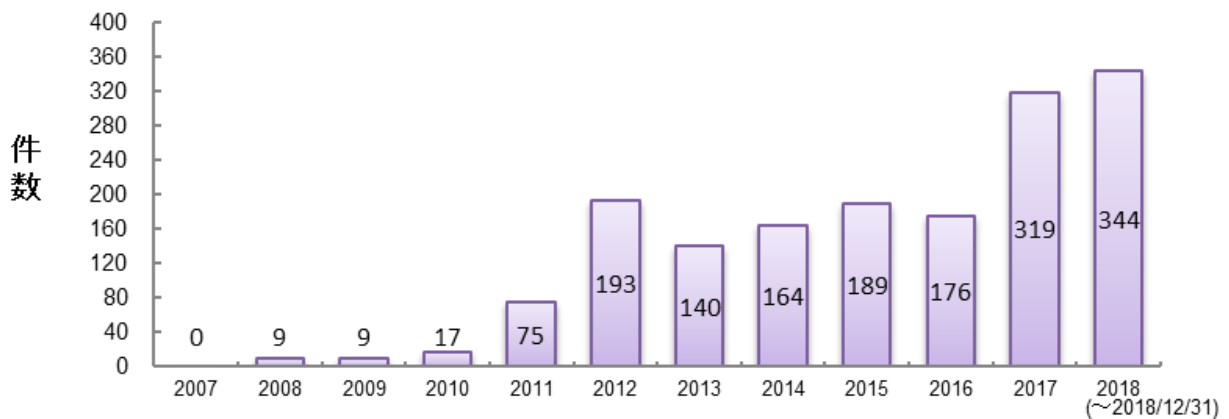


図2-5. JVN iPedia 登録件数(産業用制御システムのみ抽出)

### 3. 脆弱性対策情報の製品別登録状況

表 2-1 は 2018 年第 4 四半期（10 月～12 月）に JVN iPedia へ登録された脆弱性対策情報の中で登録件数が多かった製品の上位 20 件を示したものです。

今四半期において最も登録件数が多かったのは、LinuxOS である Debian 製品の Debian GNU/Linux でした。Debian GNU/Linux は、2018 年第 1 四半期においても 1 位（登録件数：117 件）にランクインしており、第 2 四半期は 3 位（登録件数：171 件）、第 3 四半期は 2 位（登録件数：212 件）と、継続して脆弱性対策情報が多く登録されています。また、今四半期は Debian GNU/Linux を含めた OS 製品がランキングの大半を占めており、レッドハットやマイクロソフトといった一般に広く利用されているベンダ製品に関する脆弱性対策情報が多数登録されました。

JVN iPedia は、表に記載されている製品以外にも幅広い脆弱性対策情報を登録公開しています。製品の利用者や開発者は、自組織などで使用しているソフトウェアの脆弱性対策情報を迅速に入手し、効率的な対策に役立ててください<sup>(\*)</sup>。

表 2-1. 製品別 JVN iPedia の脆弱性対策情報登録件数 上位 20 件 [2018 年 10 月～2018 年 12 月]

順位	カテゴリ	製品名（ベンダ名）	登録件数
1	OS	Debian GNU/Linux (Debian)	177
2	PDF 閲覧	Foxit Reader (Foxit Software Inc)	122
3	PDF 閲覧・編集	Foxit PhantomPDF (Foxit Software Inc)	121
4	OS	Ubuntu (Canonical)	108
5	PDF 閲覧・編集	Adobe Acrobat (アドビシステムズ)	95
5	PDF 閲覧	Adobe Acrobat Reader DC (アドビシステムズ)	95
5	PDF 閲覧・編集	Adobe Acrobat DC (アドビシステムズ)	95
8	OS	Microsoft Windows 10 (マイクロソフト)	90
9	OS	Microsoft Windows Server (マイクロソフト)	86
10	OS	Microsoft Windows Server 2016 (マイクロソフト)	75
10	OS	Android (Google)	75
12	OS	Red Hat Enterprise Linux Server (レッドハット)	68
13	OS	Red Hat Enterprise Linux Desktop (レッドハット)	59
13	OS	Microsoft Windows Server 2012 (マイクロソフト)	59
13	OS	Red Hat Enterprise Linux Workstation (レッドハット)	59
16	OS	Microsoft Windows 8.1 (マイクロソフト)	57
17	OS	Microsoft Windows RT 8.1 (マイクロソフト)	56
18	OS	Microsoft Windows Server 2008 (マイクロソフト)	55
19	OS	Microsoft Windows 7 (マイクロソフト)	53
20	OS	Microsoft Edge (マイクロソフト)	50

<sup>(\*)</sup> 脆弱性情報の収集や集めた情報の活用方法についての手引きをまとめたレポート「脆弱性対策の効果的な進め方（実践編）」を公開。  
<https://www.ipa.go.jp/security/technicalwatch/20150331.html>

#### 4. 脆弱性対策情報の活用状況

表 3-1 は 2018 年第 4 四半期（10 月～12 月）にアクセスの多かった JVN iPedia の脆弱性対策情報の上位 20 件を示したものです。

今四半期の 1 位は FileZen に関する脆弱性対策情報です。2 位以降と比較して非常に多いアクセス数となっておりますが、これは、特定の組織から短期間に非常に多くの機械的なアクセスがあったためです。また、上位 20 件中 17 位と 19 位以外の 18 件が、脆弱性対策情報ポータルサイト JVN で公表した脆弱性対策情報でした。JVN から公表した情報の中には、「情報セキュリティ早期警戒パートナーシップ<sup>(14)</sup>」に基づいて公表された情報も含まれています。これらの情報は注目度が高く、ニュースサイトやブログ記事等でも取り上げられたことからアクセス数が増加したものと考えられます。

表 3-1.JVN iPedia の脆弱性対策情報へのアクセス 上位 20 件 [2018 年 10 月～2018 年 12 月]

順位	ID	タイトル	CVSSv2 基本値	CVSSv3 基本値	公開日	アクセス 数
1	JVNDB-2018-000104	FileZen における複数の脆弱性	10.0	10.0	2018/10/15	514,239
2	JVNDB-2018-000102	Denbun における複数の脆弱性	7.5	9.8	2018/10/4	6,294
3	JVNDB-2018-000101	Baidu Browser のインストーラにおける DLL 読み込みに関する脆弱性	6.8	7.8	2018/10/3	6,239
4	JVNDB-2018-000100	スマートフォンアプリ「+メッセージ（プラスメッセージ）」における SSL サーバ証明書の検証不備の脆弱性	4.0	4.8	2018/9/27	5,843
5	JVNDB-2018-000092	INplc における複数の脆弱性	7.5	9.8	2018/9/7	5,643
6	JVNDB-2018-000110	Symantec Web Isolation におけるクロスサイトスクリプティングの脆弱性	4.3	6.1	2018/10/19	5,397
7	JVNDB-2018-000103	Music Center for PC にソフトウェアアップデート時のダウンロードファイル検証不備の脆弱性	5.1	7.5	2018/10/9	5,337
8	JVNDB-2018-000106	User-friendly SVN におけるクロスサイトスクリプティングの脆弱性	2.6	6.1	2018/10/9	5,284
9	JVNDB-2018-000107	OpenAM (オープンソース版) におけるセッション管理不備の脆弱性	4.0	5.0	2018/10/12	5,235
10	JVNDB-2018-000105	Metabase におけるクロスサイトスクリプティングの脆弱性	4.3	6.1	2018/10/11	5,104
11	JVNDB-2018-000129	i-FILTER における複数の脆弱性	4.3	6.1	2018/12/7	5,100
12	JVNDB-2018-000111	BlueStacks App Player におけるアクセス制限不備の脆弱性	5.8	6.3	2018/10/24	5,045
13	JVNDB-2018-000109	YukiWiki における複数の脆弱性	4.3	6.1	2018/10/19	4,969

<sup>(14)</sup> 情報セキュリティ早期警戒パートナーシップ

[https://www.ipa.go.jp/security/ciadr/partnership\\_guide.html](https://www.ipa.go.jp/security/ciadr/partnership_guide.html)

順位	ID	タイトル	CVSSv2 基本値	CVSSv3 基本値	公開日	アクセス 数
14	JVNDB-2018-000113	OpenDolphin における複数の脆弱性	6.5	8.8	2018/10/26	4,956
15	JVNDB-2018-000116	iOS メール App におけるサービス運用妨害 (DoS) の脆弱性	5.0	7.5	2018/11/2	4,895
16	JVNDB-2018-000112	SecureCore Standard Edition における認証不備の脆弱性	2.1	2.4	2018/10/24	4,758
17	JVNDB-2018-008547	Hitachi Device Manager におけるクリックジャッキングの脆弱性	4.3	4.3	2018/10/22	4,699
18	JVNDB-2018-000099	サイボウズ Garoon におけるディレクトリトラバースの脆弱性	5.5	6.4	2018/9/10	4,617
19	JVNDB-2018-009328	JP1/VERITAS 製品における複数の脆弱性	10.0	9.8	2018/11/15	4,586
20	JVNDB-2018-000117	WordPress 用プラグイン LearnPress における複数の脆弱性	6.5	7.2	2018/11/9	4,576

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でアクセスの多かった上位 5 件を示しています。

表 3-2.国内の製品開発者から収集した脆弱性対策情報へのアクセス 上位 5 件 [2018 年 10 月～2018 年 12 月]

順位	ID	タイトル	CVSSv2 基本値	CVSSv3 基本値	公開日	アクセス 数
1	JVNDB-2018-008547	Hitachi Device Manager におけるクリックジャッキングの脆弱性	4.3	4.3	2018/10/22	4,699
2	JVNDB-2018-009328	JP1/VERITAS 製品における複数の脆弱性	10.0	9.8	2018/11/15	4,586
3	JVNDB-2018-002257	JP1/ServerConductor/Deployment Manager および Hitachi Compute Systems Manager におけるサービス運用妨害 (DoS) の脆弱性	7.8	7.5	2018/4/4	4,090
4	JVNDB-2018-001389	Hitachi Device Manager における XXE 脆弱性	7.8	7.4	2018/2/14	4,076
5	JVNDB-2018-001388	Hitachi Command Suite 製品における複数の脆弱性	5.8	6.1	2018/2/14	4,040

注 1) CVSSv2 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) CVSSv3 基本値の深刻度による色分け

CVSS 基本値=0.1～3.9 深刻度=注意	CVSS 基本値=4.0～6.9 深刻度=警告	CVSS 基本値=7.0～8.9 深刻度=重要	CVSS 基本値=9.0～10.0 深刻度=緊急
----------------------------	----------------------------	----------------------------	-----------------------------

注 3) 公開日の年による色分け

2016 年以前の公開	2017 年の公開	2018 年の公開
-------------	-----------	-----------