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

[2017 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、2017 年 10 月 1 日から 2017 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。

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

2018 年 1 月 24 日

目次

1. 2017 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（ http://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 [*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 78,410 件～

2017 年第 4 四半期（2017 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、78,410 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 1,836 件になりました。

表 1-1. 2017 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	10 件	196 件
	JVN	213 件	7,864 件
	NVD	3,496 件	70,350 件
	計	3,719 件	78,410 件
英語版	国内製品開発者	8 件	194 件
	JVN	31 件	1,642 件
	計	39 件	1,836 件

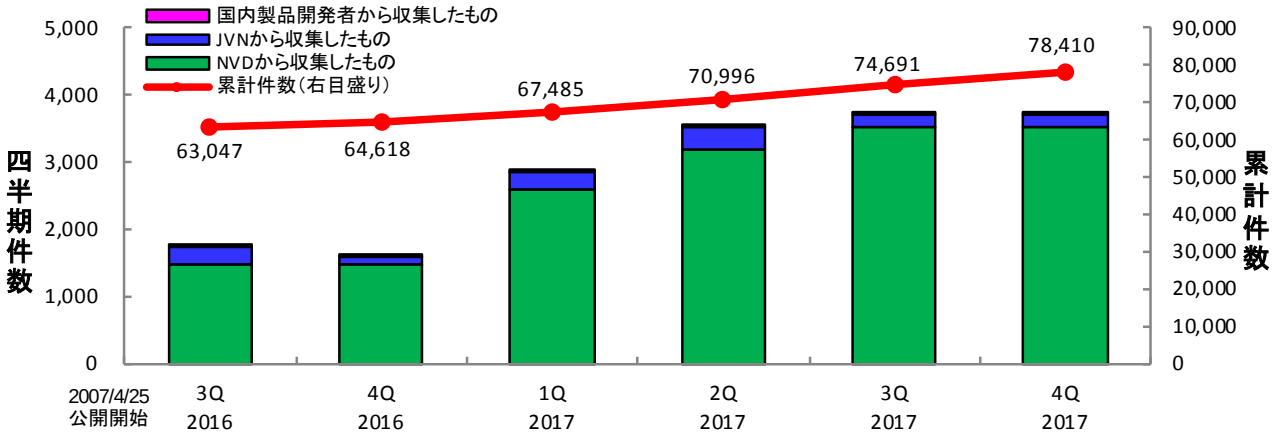

図1−1. JVN iPediaの登録件数の四半期別推移

[*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】JVN iPedia に登録された年間の脆弱性対策情報の推移
～JVN iPedia へ登録された脆弱性対策情報の年間の登録件数は、2017 年の 13,792 件が過去最多、2016 年と比べて 2 倍以上～

IPA では 2007 年 4 月から脆弱性対策情報データベース「JVN iPedia」を運用しています。図 1-2 は 2013 年から 2017 年までの直近 5 年間に JVN iPedia へ登録した脆弱性対策情報の推移です。

2013 年には 1 年間で 5,272 件だった登録件数が、3 年後の 2016 年には 6,524 件と増加しています。さらに翌年の 2017 年には 13,792 件の登録件数となっており、2016 年と比較すると 2 倍以上の登録件数で過去最多となっています。また、2017 年の登録件数の内訳を見ると、NVD から収集した件数が 12,804 件と全体の約 92%を占めており、NVD から公開される脆弱性情報が大幅に増加しています。

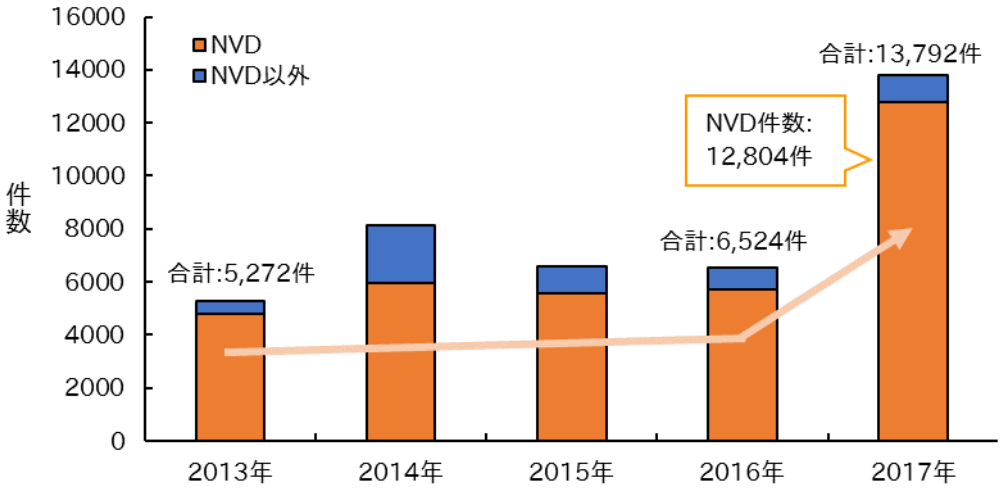

図 1-2.　2013 年から 2017 年までに JVN iPedia へ登録した脆弱性対策情報の推移

これは、発見される脆弱性の増加に加え、CVE の採番機関（CNA:CVE Numbering Authority）[*4] になるための認定基準が緩和され、CVE 採番機関の数が増加したことが一因として挙げられます[*5]。2016 年 12 月に 47 社[*6]だった CVE 採番機関が、2017 年 11 月には 81 社[*7]と約 1.7 倍となっています。これにより、多くの脆弱性情報に CVE が紐づけられ、NVD の公開件数増加につながった可能性があります。

(*4) CVE Numbering Authorities：CVE 採番機関（CNA）。製品に影響を与える脆弱性に CVE を割り当てる権限を与えられた組織。
https://cve.mitre.org/cve/cna.html

(*5) CVE Numbering Authorities (CNA) Rules, Version 2.0：CVE 採番機関（CNA）ルール。
https://cve.mitre.org/cve/cna/CNA_Rules_v2.0.pdf

(*6) CVE Adds 7 New CVE Numbering Authorities (CNAs)：7 つの新しい CVE 採番機関（CNA）を追加（2016 年 12 月 23 日時点）。
https://cve.mitre.org/news/archives/2016/news.html

(*7) SAP Added as CVE Numbering Authority (CNA)：SAP を CVE 採番機関（CNA）として追加（2017 年 11 月 09 日時点）。
https://cve.mitre.org/news/archives/2017/news.html

組織においてソフトウェアの利用が広まっていく一方で、脆弱性を悪用した攻撃による被害が後を絶ちません。ソフトウェア製品の利用者およびシステム管理者は、被害に遭わないために脆弱性に対して適切な対応が求められます。JVN iPedia では日々公表されている脆弱性情報をデータベースとして蓄積し続けており、目的の製品に関する脆弱性対策情報を容易に利用できるよう、様々な検索機能を用意しています。JVN iPedia を活用し、脆弱性対策に役立ててください。

1-3. 【注目情報 2】2020 年に終了する主要な製品の公式サポート終了について
～2017 年 1 年間の「危険」とされる脆弱性対策情報は 60 件以上、サポート終了までにベンダがサポートするバージョンや代替製品への移行などの検討を～

IPA では 2018 年 1 月 22 日に「安心相談窓口だより[*8]」でも、2020 年初頭にマイクロソフト社が提供している Windows7 と Windows Server 2008 の延長サポート終了について触れています。

図 1-3 は 2017 年 1 月から 12 月までに JVN iPedia へ登録された Windows7 と Windows Server 2008 の深刻度別脆弱性対策情報の割合です。Windows7 では 231 件中 26%の 60 件、Windows Server 2008 では 242 件中 26%の 63 件が、深刻度が最も高い「危険」になっています。そのため、今後も深刻度が「危険」と分類される脆弱性対策情報が複数公開される可能性があります。

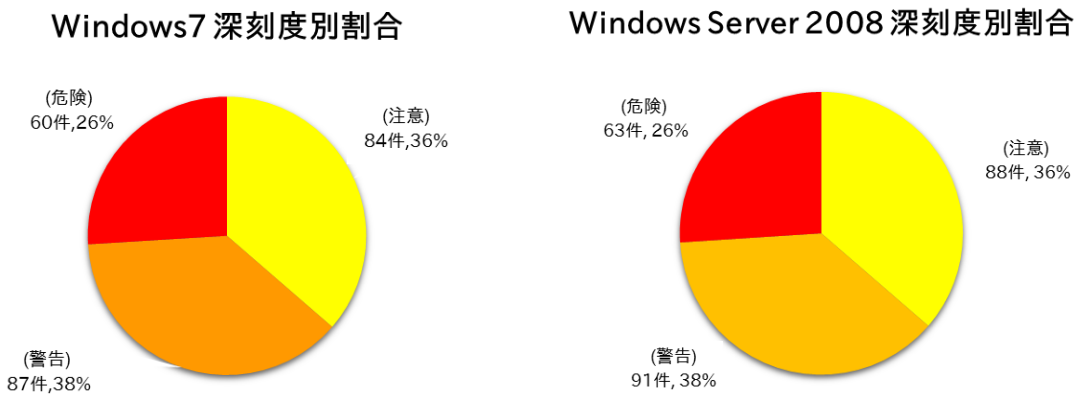

図 1-3. Windows7 および Windows Server 2008 の深刻度別割合

仮に製品のサポートが終了した後に、新たな脆弱性が発見され、さらに発見された脆弱性を悪用した攻撃が確認されたとしても、修正プログラムがベンダから提供されず、利用者は対策を行うことができない可能性があります。そのため、サポートが終了した製品を継続利用した場合、常にセキュリティリスクを抱えた状態となります。システム管理者は自組織で利用している製品のサポートが終了していないか、あるいは終了の予定がないかを確認してください。また、終了が既に公表されている場合は、製品ベンダがサポートするバージョンや代替製品への移行などを速やかに検討してください。

なお、2020 年には Windows7 と Windows Server 2008 の他にも、マイクロソフト社の Office 2010[*9]やアドビシステムズ社が提供している Adobe Flash Player[*10] もサポートが終了する予定です。これらの製品についても移行の計画等を検討する必要があります。

[*8] 「安心相談窓口だより」2020 年 1 月に Windows 7、Windows Server 2008 の延長サポートが終了　～　システム環境や業務内容に合わせた移行計画を　～： https://www.ipa.go.jp/security/anshin/mgdayori20180122.html

[*9] Windows 7 & Office 2010 2020 年 サポート終了：
https://www.microsoft.com/ja-jp/business/windows/endofsupport.aspx

[*10] Flash & The Future of Interactive Content – Adobe：
https://theblog.adobe.com/adobe-flash-update/

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、2017 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-119（バッファエラー）が 715 件、CWE-79（クロスサイト・スクリプティング）が 398 件、CWE-200（情報漏えい）が 371 件、CWE-264（認可・権限・アクセス制御不備）が 299 件、CWE-284（不適切なアクセス制御）が 253 件でした。最も件数の多かった CWE-119（バッファエラー）は、悪用されるとサーバや PC 上で悪意のあるコードが実行され、データを盗み見られたり、改ざんされたりなどの被害が発生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 (*11)」や「IPA セキュア・プログラミング講座 (*12)」、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 (*13)」などを公開しています。

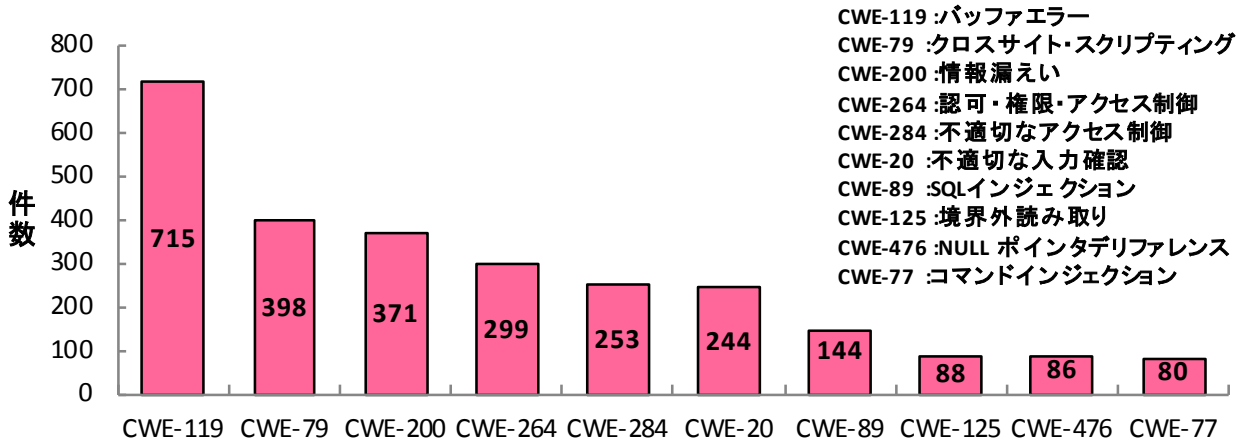

図2−1. 2017年第4四半期に登録された脆弱性の種類別件数

(*11) IPA：「安全なウェブサイトの作り方」
https://www.ipa.go.jp/security/vuln/websecurity.html
(*12) IPA：「IPA セキュア・プログラミング講座」
https://www.ipa.go.jp/security/awareness/vendor/programming/
(*13) 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、公表年別にその推移を示したものです。

脆弱性対策情報の登録開始から 2017 年 12 月 31 日までに 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 29.3%、レベルⅡが 61.6%、レベルⅠが 9.1%となっており、情報の漏えいや改ざんされるような高い脅威であるレベルⅡ以上が、90.9%を占めています。

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。IPA では新たに登録された深刻な脆弱性情報や既知の脆弱性を狙った攻撃に対する情報を即時に入手できるサービス「サイバーセキュリティ注意喚起サービス icat for JSON [*14] 」や、新たに公表した JVN iPedia の情報を RSS で公開しています。

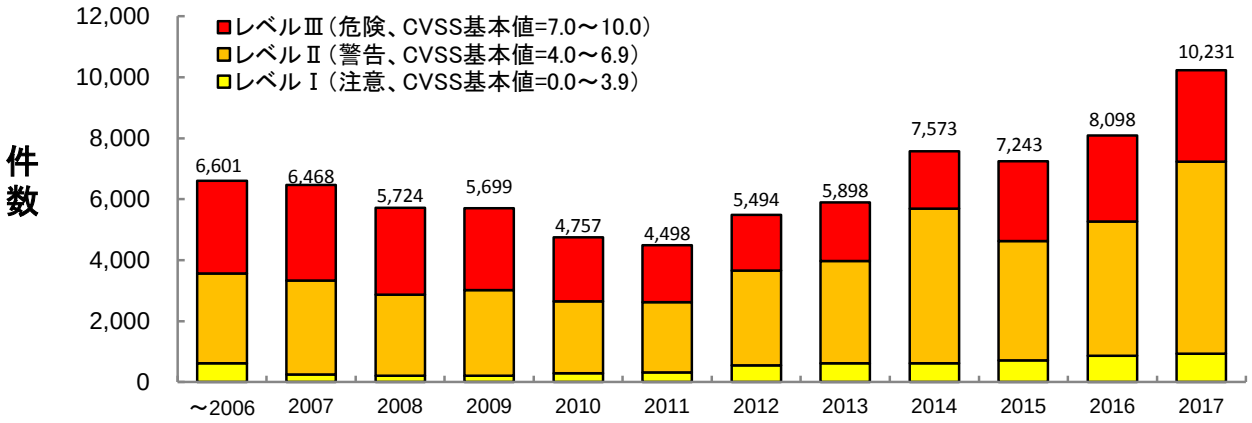

図2-2. 脆弱性の深刻度別件数

[*14] サイバーセキュリティ注意喚起サービス「icat for JSON」
https://www.ipa.go.jp/security/vuln/icat.html

2-3. 脆弱性対策情報を公表した製品の種類別件数

図 2-3 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類別に件数を集計し、年次でその推移を示したものです。2017 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、2017 年の件数全件の約 74.0%（7,580 件／全 10,250 件）を占めています。

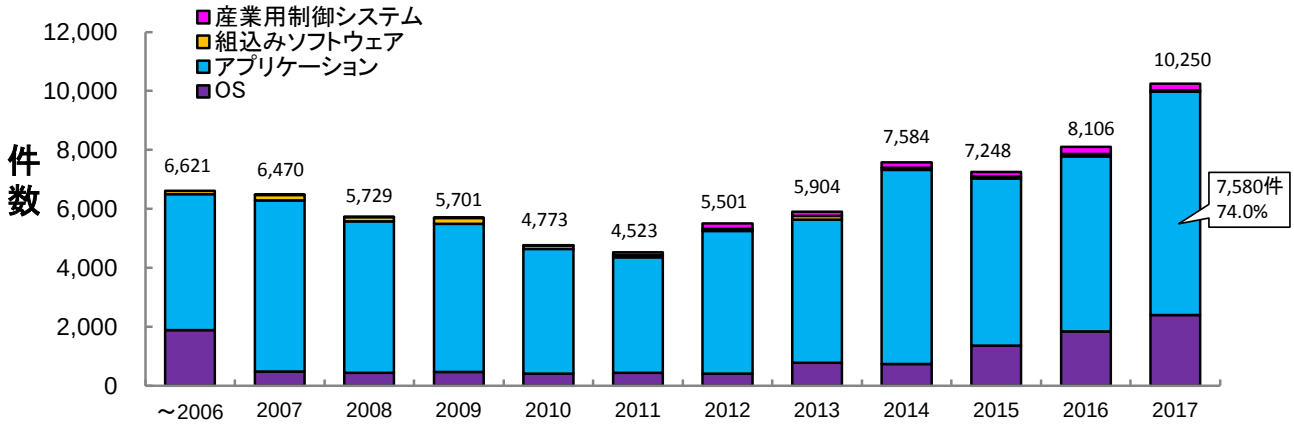

図2-3. 脆弱性対策情報を公表した製品の種類別件数の公開年別推移

また 2007 年以降、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を登録しています。これまでに累計で 1,263 件を登録しています（図 2-4）。1 年間の登録件数は 2012 年以降 100 件を越えており、2016 年以降は 200 件を超えています。

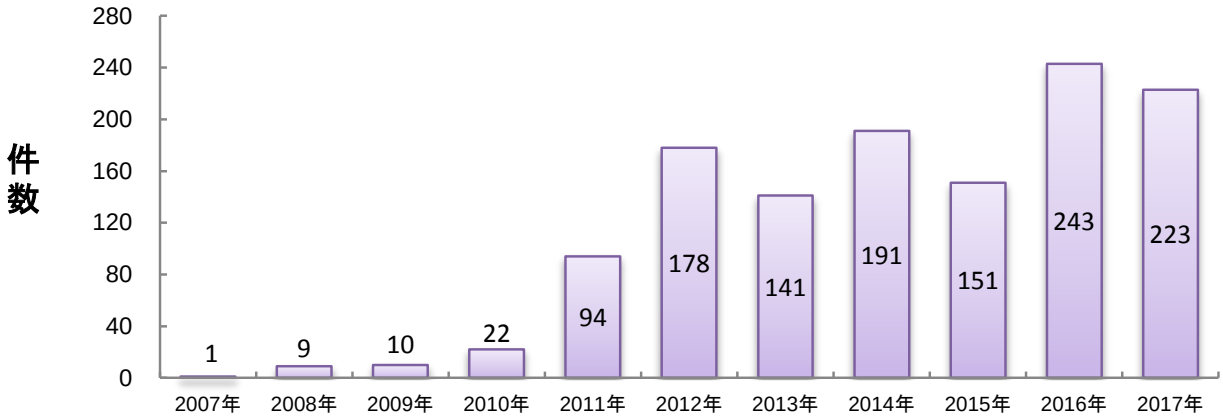

図2-4. JVN iPedia 登録件数（産業用制御システムのみ抽出）

2-4. 脆弱性対策情報の製品別登録状況

表 2-1 は 2017 年第 4 四半期（10 月～12 月）に JVN iPedia へ脆弱性対策情報の登録件数が多かった製品の上位 20 件を示したものです。1 位の Android OS の登録件数は 254 件、5 位の iOS の登録件数は 74 件と、多くの方が利用されているスマートフォンの OS の脆弱性が多数公開されています。そのため、脆弱性を悪用されないためにもスマートフォンに OS のアップデート通知が来た場合、速やかなアップデートを行うことが重要です。

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 [*15]。

表 2-1. 製品別 JVN iPedia の脆弱性対策情報登録件数　上位 20 件 [2017 年 10 月～2017 年 12 月]

順位	カテゴリ	製品名（ベンダ名）	登録件数
1	OS	Android(Google)	254
2	OS	Debian GNU/Linux(Debian)	95
3	パケットキャプチャ	tcpdump(The Tcpdump Group)	88
4	画像ビューア	IrfanView(Irfan Skiljan)	74
4	OS	iOS(アップル)	74
6	ブラウザ	Google Chrome(Google)	71
7	電子文書リーダー	STDU Viewer(STDUtility)	67
7	OS	Apple Mac OS X(アップル)	67
9	PDF 閲覧	Adobe Reader(アドビシステムズ)	62
9	PDF 閲覧・編集	Adobe Acrobat DC(アドビシステムズ)	62
9	PDF 閲覧	Adobe Acrobat Reader DC(アドビシステムズ)	62
9	PDF 閲覧・編集	Adobe Acrobat(アドビシステムズ)	62
13	OS	tvOS(アップル)	55
14	OS	Linux Kernel(kernel.org)	54
15	画像処理ソフト	XnView(XnSoft)	40
15	ブラウザ	Safari(アップル)	40
15	OS	Microsoft Windows 10(マイクロソフト)	40
15	ブラウザ	Microsoft Edge(マイクロソフト)	40
19	OS	Microsoft Windows Server 2016(マイクロソフト)	38
20	クラウドサービス	iCloud(アップル)	36

[*15] 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

3. 脆弱性対策情報の活用状況

表 3-1 は 2017 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。1 位、2 位、4 位、7 位、10 位、13 位、15 位の脆弱性は日立製作所の製品に関する脆弱性で、上位 20 件中、7 件が同ベンダの脆弱性対策情報となります。これらの脆弱性は JVN iPedia の情報収集元のうち、国内の製品開発者から収集した情報となっているため、国内の利用者が多く、注目されたのではないかと考えられます。

表 3-1.JVN iPedia の脆弱性対策情報へのアクセス　上位 20 件 [2017 年 10 月～2017 年 12 月]

順位	ID	タイトル	CVSSv2 基本値	公開日	アクセス数
1	JVNDB-2017-007767	JP1/秘文で作成した自己復号型機密ファイルの DLL 読み込みに関する脆弱性	6.8	2017/10/2	4,354
2	JVNDB-2017-008411	Hitachi Command Suite 製品における XXE 脆弱性	7.5	2017/10/18	4,219
3	JVNDB-2017-000229	ホームユニット KX-HJB1000 における複数の脆弱性	6.5	2017/10/17	3,886
4	JVNDB-2017-008369	Hitachi Infrastructure Analytics Advisor における複数の脆弱性	7.5	2017/10/17	3,825
5	JVNDB-2017-000228	秘文 機密ファイルビューアのインストーラにおける DLL 読み込みおよび実行ファイル呼び出しに関する脆弱性	6.8	2017/10/11	3,821
6	JVNDB-2017-000232	Wi-Fi STATION L-02F にバッファオーバーフローの脆弱性	10.0	2017/11/6	3,765
7	JVNDB-2017-008364	Hitachi Tuning Manager における RMI に関する脆弱性	10.0	2017/10/17	3,704
8	JVNDB-2017-008629	「楽々はがき」および「楽々はがき セレクト for 一太郎」にメモリ破壊の脆弱性	7.5	2017/10/25	3,689
9	JVNDB-2017-000225	サイボウズ Office におけるアクセス制限不備の脆弱性	4.0	2017/10/11	3,570
10	JVNDB-2017-008370	Hitachi Automation Director における情報露出の脆弱性	3.5	2017/10/17	3,553
11	JVNDB-2017-000226	秘文 機密ファイル復号プログラムにおける DLL 読み込みに関する脆弱性	6.8	2017/10/11	3,532
12	JVNDB-2017-000244	バッファロー製の複数の有線ブロードバンドルータに複数の脆弱性	4.3	2017/12/1	3,529
13	JVNDB-2017-008363	Hitachi Global Link Manager における情報露出の脆弱性	3.5	2017/10/17	3,483
14	JVNDB-2017-000231	OpenAM (オープンソース版) における認証回避の脆弱性	6.0	2017/11/1	3,440
15	JVNDB-2017-010043	JP1/Operations Analytics におけるクロスサイトスクリプティングの脆弱性	3.5	2017/12/1	3,254

順位	ID	タイトル	CVSSv2 基本値	公開日	アクセス数
16	JVNDB-2017-002923	Intel Active Management Technology (AMT) にアクセス制限不備の脆弱性	10.0	2017/5/9	3,186
17	JVNDB-2017-000213	フレッツ簡単セットアップツール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	2017/11/2	3,148
18	JVNDB-2017-008412	Wi-Fi Protected Access における Pairwise Transient Key Temporal Key を再インストールされる脆弱性	5.4	2017/10/18	3,078
19	JVNDB-2017-000238	ロボット家電 COCOROBO におけるセッション管理不備の脆弱性	4.3	2017/11/16	3,077
20	JVNDB-2017-000233	LAN DISK コネクトにおけるサービス運用妨害 (DoS) の脆弱性	3.3	2017/11/6	3,039

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 [2017 年 10 月～2017 年 12 月]

順位	ID	タイトル	CVSSv2 基本値	公開日	アクセス数
1	JVNDB-2017-007767	JP1/秘文で作成した自己復号型機密ファイルの DLL 読み込みに関する脆弱性	6.8	2017/10/2	4,354
2	JVNDB-2017-008411	Hitachi Command Suite 製品における XXE 脆弱性	7.5	2017/10/18	4,219
3	JVNDB-2017-008369	Hitachi Infrastructure Analytics Advisor における複数の脆弱性	7.5	2017/10/17	3,825
4	JVNDB-2017-008364	Hitachi Tuning Manager における RMI に関する脆弱性	10.0	2017/10/17	3,704
5	JVNDB-2017-008370	Hitachi Automation Director における情報露出の脆弱性	3.5	2017/10/17	3,553

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）公開日の年による色分け

2015 年以前の公開	2016 年の公開	2017 年の公開