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 2 四半期（4 月～6 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 4 月 1 日から 2018 年 6 月 30 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　セキュリティセンター

2018 年 7 月 24 日

目次

1. 2018 年第 2 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 [(*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 85,280 件～

2018 年第 2 四半期（2018 年 4 月 1 日から 6 月 30 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、85,280 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 1,922 件になりました。

表 1-1. 2018 年第 2 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	201 件
	JVN	146 件	8,099 件
	NVD	3,608 件	76,980 件
	計	3,757 件	85,280 件
英語版	国内製品開発者	3 件	201 件
	JVN	38 件	1,721 件
	計	41 件	1,922 件

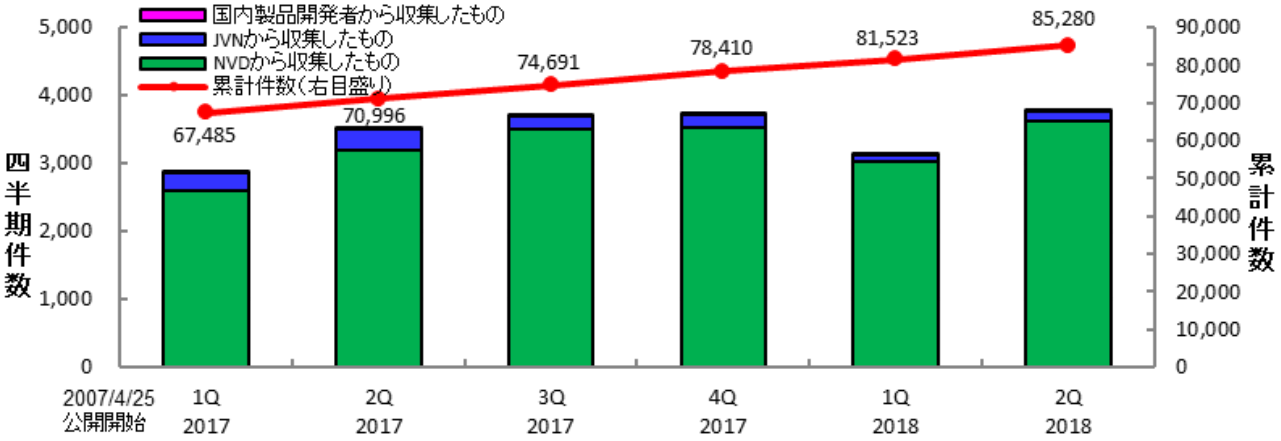

図1−1. JVN iPediaの登録件数の四半期別推移

(*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

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 2 四半期（4 月～6 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 514 件、CWE-79（クロスサイト・スクリプティング）が 422 件、CWE-200（情報漏えい）が 373 件、CWE-20（不適切な入力確認）が 365 件、CWE-264（認可・権限・アクセス制御）が 276 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 (*4) 」や「IPA セキュア・プログラミング講座 (*5) 」、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 (*6) 」などを公開しています。

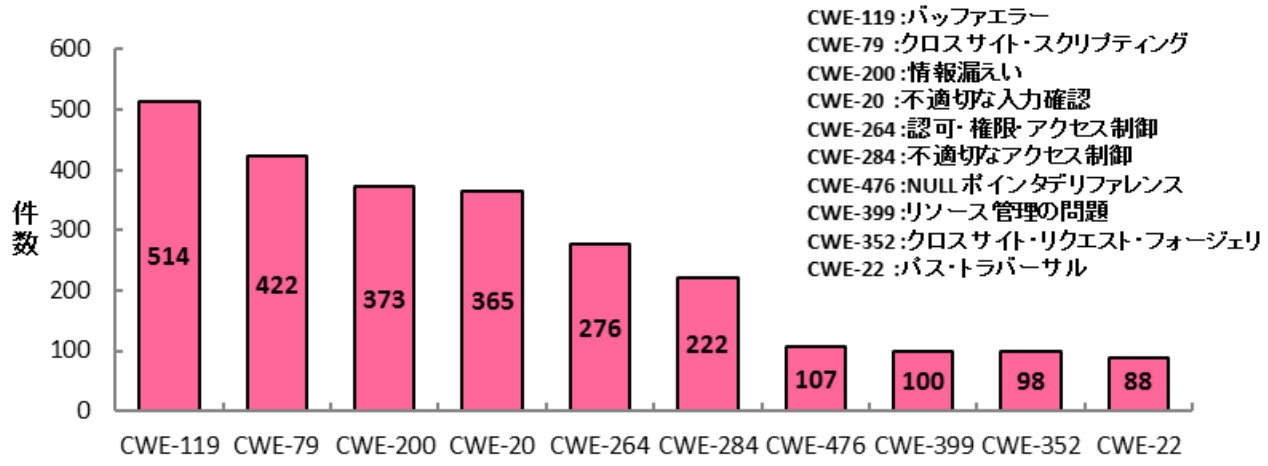

図2−1. 2018年第2四半期に登録された脆弱性の種類別件数

(*4) IPA：「安全なウェブサイトの作り方」
https://www.ipa.go.jp/security/vuln/websecurity.html
(*5) IPA：「IPA セキュア・プログラミング講座」
https://www.ipa.go.jp/security/awareness/vendor/programming/
(*6) 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 30.0%、レベルⅡが 58.7%、レベルⅠが 11.3%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 88.7%を占めています。

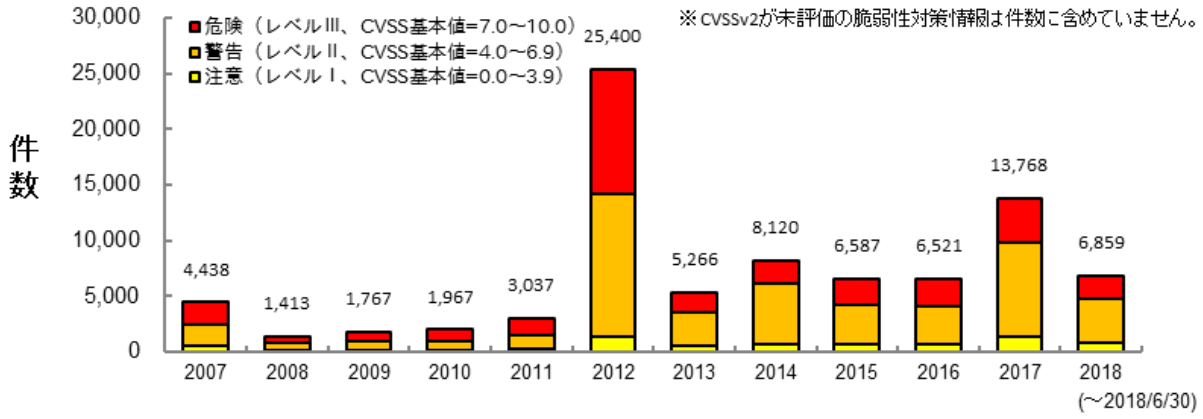

図2-2. 脆弱性の深刻度別件数(CVSSv2)

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 18.4%、「重要」が 43.5%、「警告」が 36.8%、「注意」が 1.3%となっています。

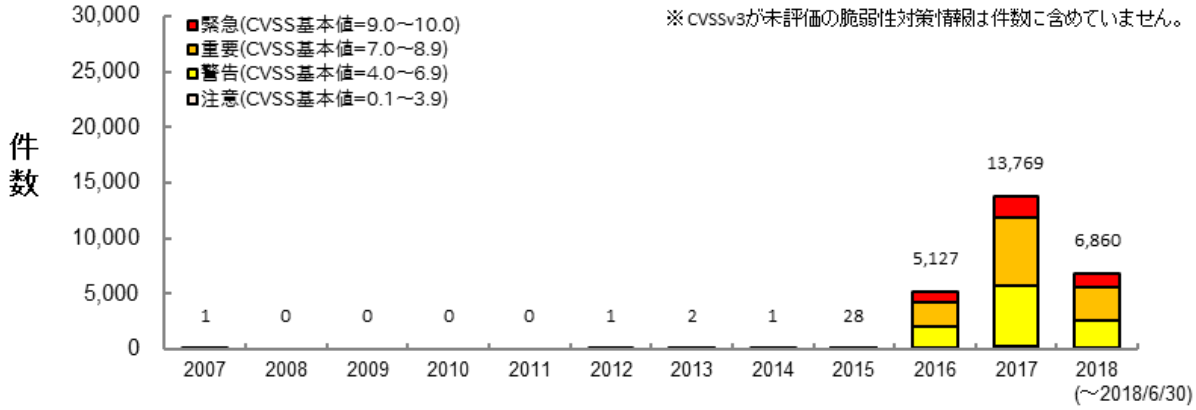

図2-3. 脆弱性の深刻度別件数(CVSSv3)

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 [*7] で公開しています。

[*7] 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類別件数

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類別に件数を集計し、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 73.7%（5,065 件／全 6,870 件）を占めています。

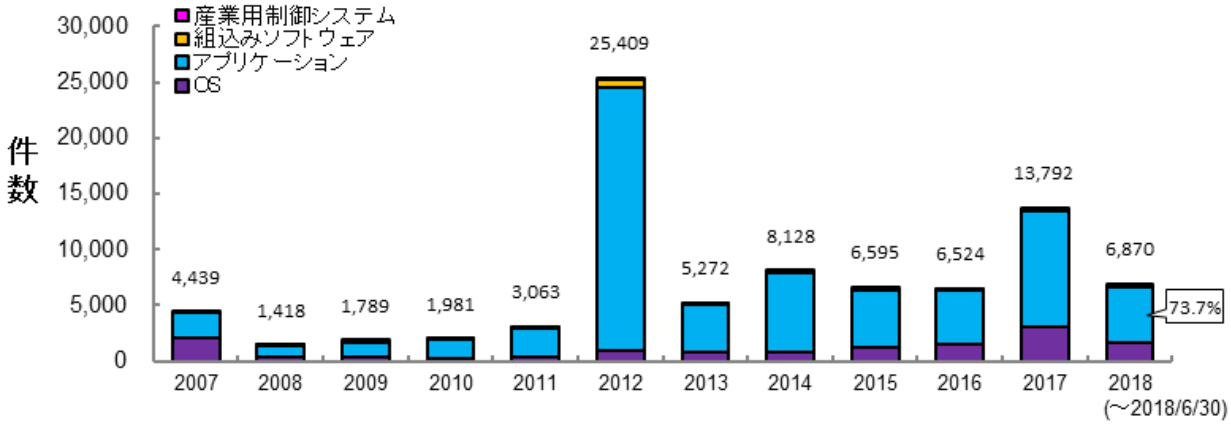

図2−4. 脆弱性対策情報を公表した製品の種類別件数の公開年別推移

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 1,460 件を登録しています（図 2-5）。

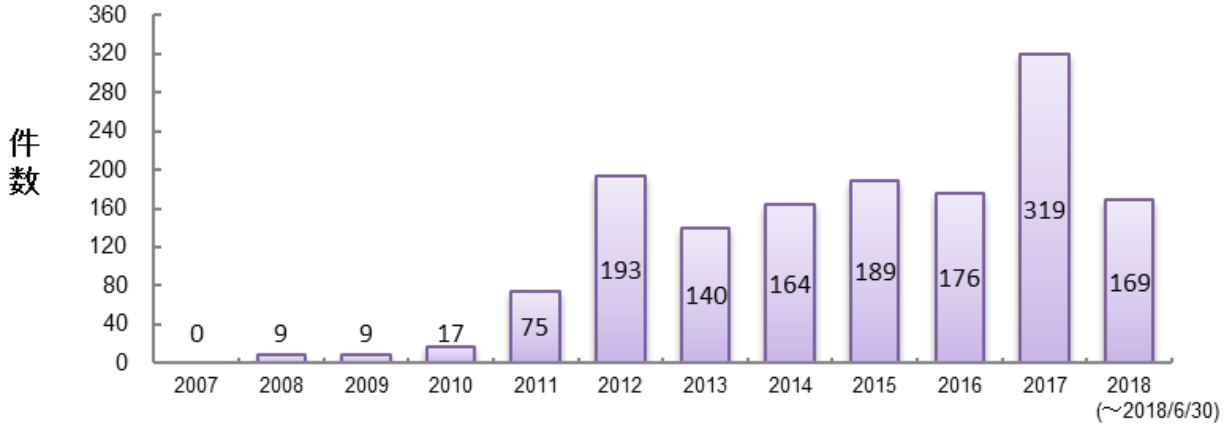

図2−5. JVN iPedia 登録件数(産業用制御システムのみ抽出)

2-4. 脆弱性対策情報の製品別登録状況

表 2-1 は 2018 年第 2 四半期（4 月～6 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。

今四半期は Android 製品に多く組み込まれている、クアルコム製プロセッサのファームウェアに関する登録件数が 268 件(※ SD 系や MSM 系などのクアルコム製プロセッサのファームウェアを 1 つのファームウェアとして取扱い、集計)、Android OS が 207 件と、Android 製品に関連する脆弱性が多数公開されています。また、2 位以降は OS 製品がランキングの大部分を占めており、マイクロソフトやアップルなどといった広く利用されているベンダーの製品に関する脆弱性対策情報を多く登録しています。

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 [(*8)] 。

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 4 月～2018 年 6 月]

順位	カテゴリ	製品名（ベンダ名）	登録件数
1	ファームウェア	Qualcomm firmware (クアルコム)	268
2	OS	Android (Google)	207
3	OS	Debian GNU/Linux (Debian)	171
4	PDF 閲覧	Foxit Reader (Foxit Software Inc)	94
5	PDF 閲覧・編集	Foxit PhantomPDF(Foxit Software Inc)	89
6	OS	iOS(アップル)	87
7	OS	Ubuntu(Canonical)	79
8	OS	Microsoft Windows 10 (マイクロソフト)	78
9	OS	Microsoft Windows Server 2016(マイクロソフト)	73
9	OS	Apple Mac OS X(アップル)	73
11	OS	tvOS(アップル)	58
12	OS	Microsoft Windows 8.1(マイクロソフト)	56
13	OS	Microsoft Windows 7(マイクロソフト)	55
14	OS	Microsoft Windows Server 2012(マイクロソフト)	54
15	OS	Microsoft Windows Server 2008(マイクロソフト)	53
16	OS	Microsoft Windows RT 8.1(マイクロソフト)	52
16	バックアップソフト	Disk Backup(Quest Software Inc.)	52
18	OS	Microsoft Windows Server バージョン 1709 (マイクロソフト)	49
19	OS	Linux Kernel(Kernel.org)	47
20	OS	watchOS(アップル)	45

[(*8)] 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 2018 年第 2 四半期（4 月～6 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 位は Pivotal Software, Inc. が提供する Spring Security と Spring Framework に関する脆弱性です。当該製品の対象バージョンがシステムに組み込まれている場合、遠隔の第 3 者に認証を回避され、情報漏えいする可能性があります。2 位は iPhone や Mac に搭載されている safari の脆弱性で、細工されたドメイン名のサイトに誘導されたユーザのウェブブラウザ上で、任意のスクリプトを実行される可能性があります。3 位はサイボウズ株式会社が提供するサイボウズ Garoon における複数の脆弱性で、ログイン認証の設定における操作制限回避などの様々な影響を受ける可能性があります。

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 4 月～2018 年 6 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-2018-000008	Spring Security と Spring Framework に認証回避の脆弱性	5.0	5.3	2018/2/2	7,870
2	JVNDB-2018-000029	Safari におけるスクリプトインジェクションの脆弱性	5.8	5.4	2018/3/30	6,629
3	JVNDB-2018-000031	サイボウズ Garoon における複数の脆弱性	5.5	5.4	2018/4/9	6,451
4	JVNDB-2018-000030	SoundEngine Free 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	2018/4/13	6,399
5	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	6,382
6	JVNDB-2018-000027	WZR-1750DHP2 における複数の脆弱性	8.3	8.8	2018/3/29	6,199
7	JVNDB-2018-000034	Tenable Appliance におけるクロスサイトスクリプティングの脆弱性	4.0	5.4	2018/4/12	6,016
8	JVNDB-2018-000028	LXR における OS コマンドインジェクションの脆弱性	7.5	9.8	2018/3/29	5,962
9	JVNDB-2018-000001	Lhaplus の ZIP64 形式のファイル展開における検証不備の脆弱性	4.3	3.3	2018/1/11	5,949
10	JVNDB-2018-000040	WordPress 用プラグイン Open Graph for Facebook, Google+ and Twitter Card Tags 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	2018/4/27	5,642
11	JVNDB-2018-000033	PhishWall クライアント Internet Explorer 版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	2018/4/12	5,634
12	JVNDB-2018-000013	トレンドマイクロ株式会社製の複数の製品における DLL 読み込みに関する脆弱性	6.8	7.8	2018/2/15	5,595
13	JVNDB-2018-000035	EC-CUBE におけるセッション固定の脆弱性	5.8	4.2	2018/4/17	5,559

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-2018-000041	株式会社セルシス製の複数の製品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	2018/4/27	5,509
15	JVNDB-2018-000026	Android アプリ「iRemoconWiFi」における SSL サーバ証明書の検証不備の脆弱性	4.0	4.8	2018/3/27	5,453
16	JVNDB-2018-000037	WordPress 用プラグイン Events Manager におけるクロスサイトスクリプティングの脆弱性	3.5	5.4	2018/4/27	5,416
17	JVNDB-2018-000038	WordPress 用プラグイン WP Google Map Plugin 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	2018/4/27	5,398
18	JVNDB-2018-000032	iOS アプリ「はてなブックマーク」におけるアドレスバー偽装の脆弱性	2.6	3.1	2018/4/10	5,366
19	JVNDB-2018-000908	WebProxy におけるディレクトリトラバーサルの脆弱性	7.5	7.3	2018/3/13	5,358
20	JVNDB-2018-000039	WordPress 用プラグイン PixelYourSite 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	2018/4/27	5,333

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 4 月～2018 年 6 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-2018-002257	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	6,382
2	JVNDB-2016-008607	Cosminexus HTTP Server および Hitachi Web Server における脆弱性	4.3	4.0	2017/6/26	4,891
3	JVNDB-2018-001389	Hitachi Device Manager における XXE 脆弱性	7.8	7.4	2018/2/14	4,310
4	JVNDB-2017-004687	富士通 Interstage List Works 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	2017/7/5	4,181
5	JVNDB-2017-002225	複数の日立製品におけるクロスサイトスクリプティングの脆弱性	4.3	4.7	2017/4/5	4,177

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