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 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、2018 年 1 月 1 日から 2018 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 4 月 24 日

目次

1. 2018 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（ 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 81,523 件～

2018 年第 1 四半期（2018 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右表の通りとなり、**脆弱性対策情報の登録件数の累計は、81,523 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 1,881 件になりました。

表 1-1. 2018 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	2 件	198 件
	JVN	89 件	7,953 件
	NVD	3,022 件	73,372 件
	計	3,113 件	81,523 件
英語版	国内製品開発者	4 件	198 件
	JVN	41 件	1,683 件
	計	45 件	1,881 件

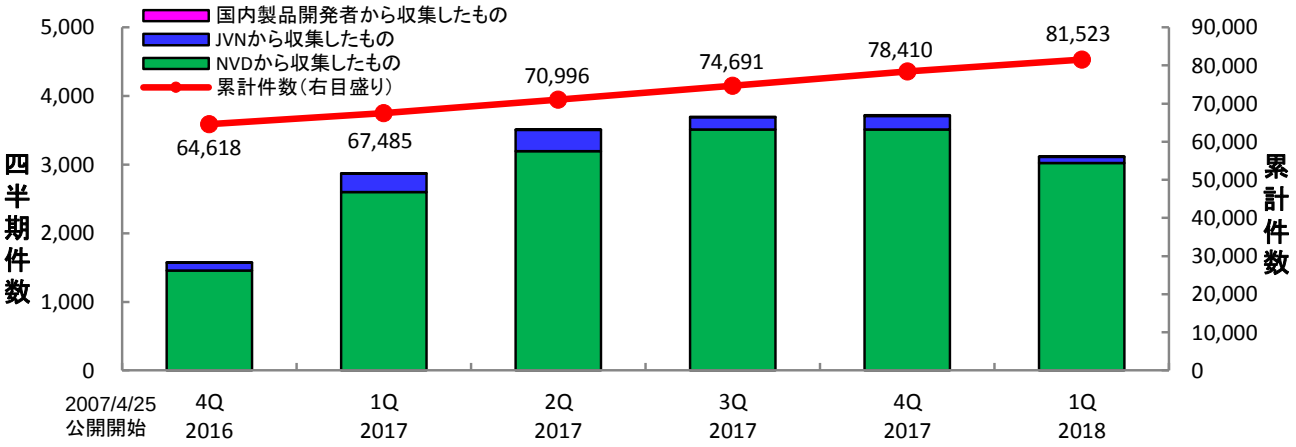

図1-1. JVN iPediaの登録件数の四半期別推移

(*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 1 四半期（1 月～3 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 414 件、CWE-119（バッファエラー）が 326 件、CWE-20（不適切な入力確認）が 326 件、CWE-200（情報漏えい）が 274 件、CWE-89（SQL インジェクション）が 255 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 (*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。

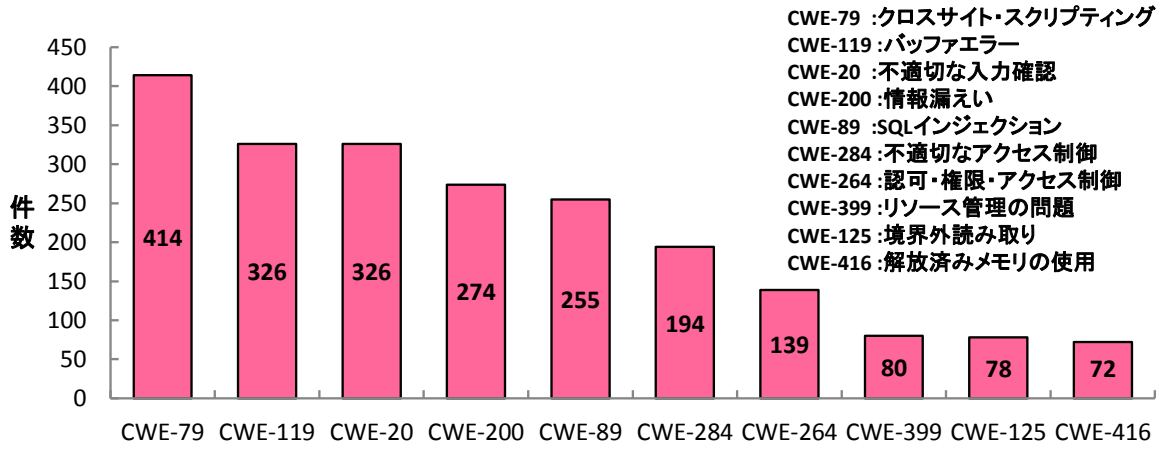

図2-1. 2018年第1四半期に登録された脆弱性の種類別件数

(*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 30.6%、レベルⅡが 57.9%、レベルⅠが 11.5%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 88.5%を占めています。

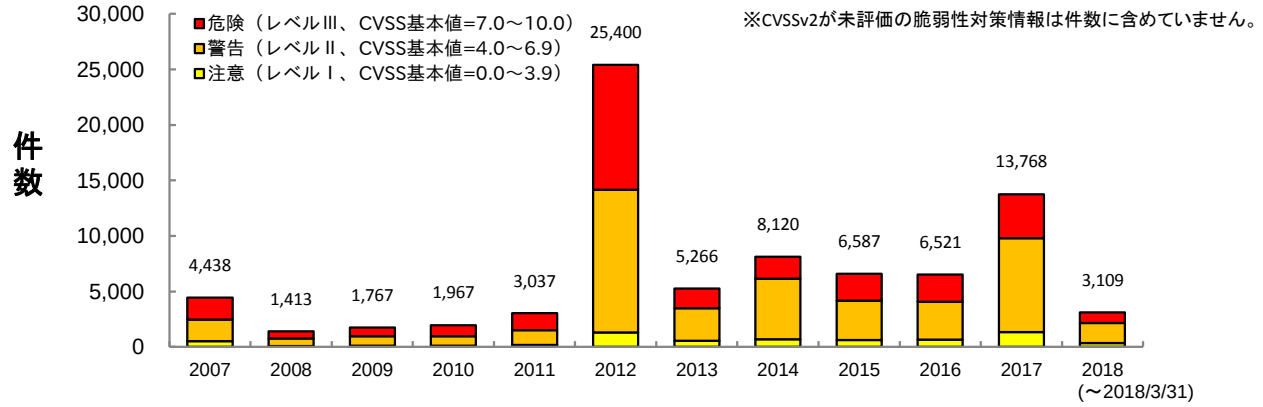

図2-2. 脆弱性の深刻度別件数(CVSSv2)

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 17.0%、「重要」が 45.1%、「警告」が 36.6%、「注意」が 1.3%となっております。

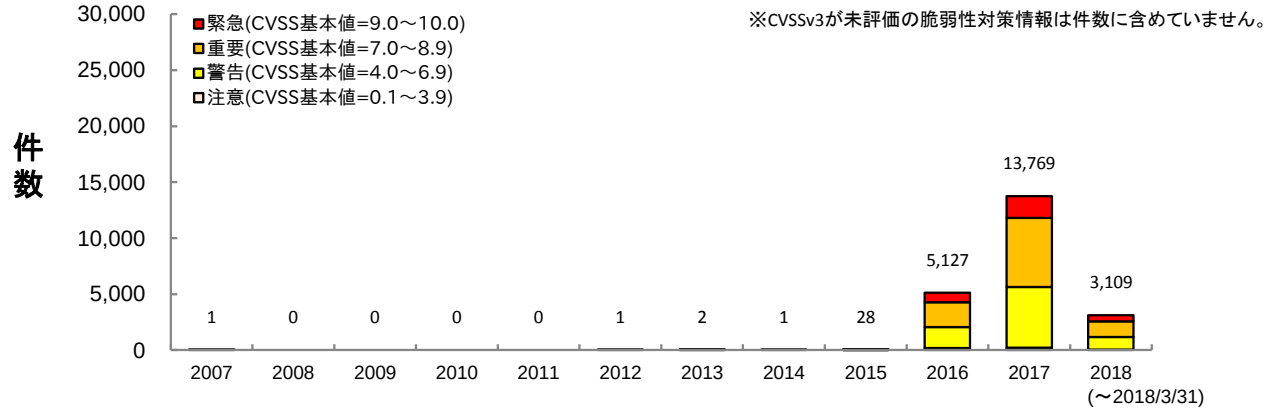

図2-3. 脆弱性の深刻度別件数(CVSSv3)

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、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 [*7] 」や新たに登録した JVN iPedia の情報を、RSS で公開しています。

[*7] 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 81.0%（2,520 件／全 3,113 件）を占めています。

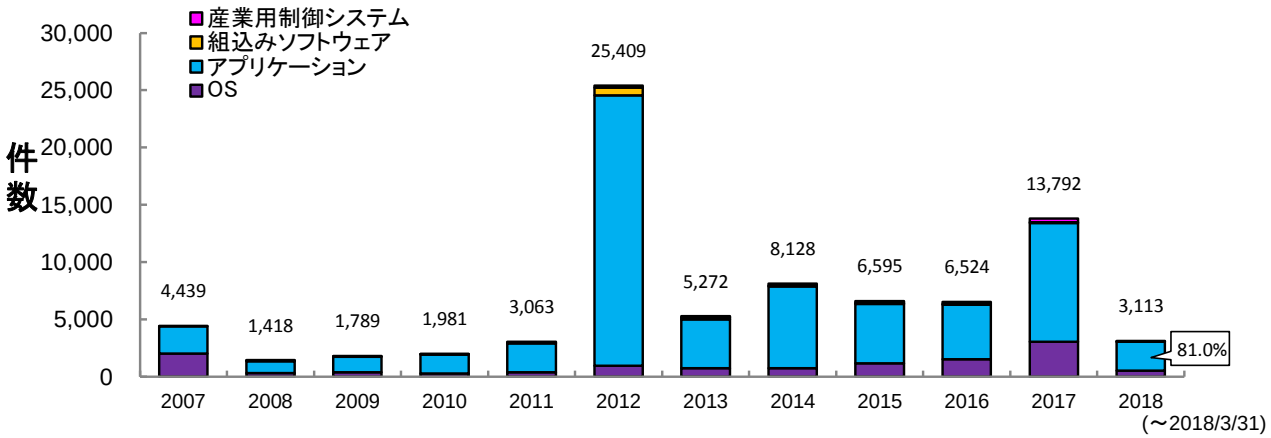

図2-4. 脆弱性対策情報を公表した製品の種類別件数の公開年別推移

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 1,318 件を登録しています（図 2-5）。

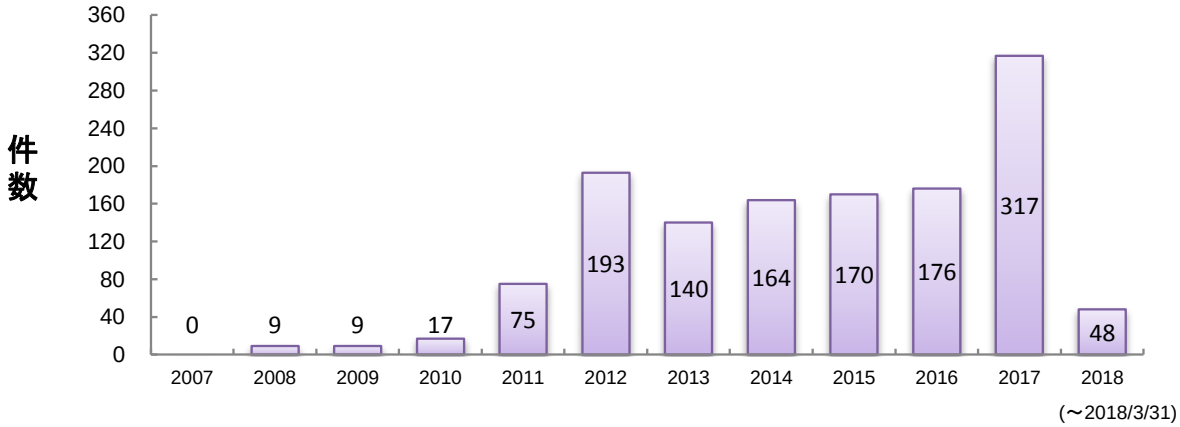

図2-5. JVN iPedia 登録件数（産業用制御システムのみ抽出）

2-4. 脆弱性対策情報の製品別登録状況

表 2-1 は 2018 年第 1 四半期（1 月～3 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 Debian GNU/Linux の登録件数は 117 件、4 位の Linux Kernel の登録件数は 50 件と、Linux の OS に関連する脆弱性が多数公開されています。

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 1 月～2018 年 3 月]

順位	カテゴリ	製品名（ベンダ名）	登録件数
1	OS	Debian GNU/Linux (Debian)	117
2	OS	Android (Google)	104
3	統合業務パッケージ	HPE Intelligent Management Center (ヒューレット・パッカード・エンタープライズ)	96
4	OS	Linux Kernel (Linux)	50
5	ブラウザ	Microsoft Edge (マイクロソフト)	46
6	PDF 閲覧	Foxit Reader (Foxit Software Inc)	43
6	実行環境	ChakraCore (マイクロソフト)	43
8	PDF 閲覧	Adobe Reader (アドビシステムズ)	39
8	PDF 閲覧・編集	Adobe Acrobat DC (アドビシステムズ)	39
8	PDF 閲覧	Adobe Acrobat Reader DC (アドビシステムズ)	39
8	PDF 閲覧・編集	Adobe Acrobat (アドビシステムズ)	39
12	ファームウェア	DP300 ファームウェア (Huawei)	36
13	OS	Microsoft Windows 10 (マイクロソフト)	35
14	OS	Microsoft Windows Server バージョン 1709 (マイクロソフト)	32
14	ファームウェア	TE30 ファームウェア (Huawei)	32
16	ファームウェア	RP200 ファームウェア (Huawei)	31
16	画像処理ソフト	ImageMagick (ImageMagick)	31
18	セキュリティソフト	K7 AntiVirus (K7 Computing)	29
18	OS	Microsoft Windows Server 2016 (マイクロソフト)	29
18	ネットワーク解析	Wireshark (Wireshark)	29

[(*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 1 四半期（1 月～3 月）にアクセスの多かった JVN iPedia の脆弱性対策情報の上位 20 件を示したものです。1 位の脆弱性「CPU に対するサイドチャネル攻撃」は影響を受ける製品が多く、ニュースでは「Meltdown (メルトダウン)」「Spectre (スペクター)」などと呼ばれ注目されました。また、4 位の「Oracle WebLogic Server」の脆弱性は前四半期の 2017 年 10 月に公開された脆弱性でしたが、本四半期において上位にランクインしました。本脆弱性は、2017 年 12 月下旬に脆弱性を悪用する攻撃事例が確認されたことから 2018 年 1 月に IPA から緊急対策情報を発信[(*9)]するなど、本四半期に入っても引き続き注目されました。

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 1 月～2018 年 3 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-2018-001001	CPU に対するサイドチャネル攻撃	4.4	4.7	2018/1/4	18,016
2	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	8,171
3	JVNDB-2018-000008	Spring Security と Spring Framework に認証回避の脆弱性	5.0	5.3	2018/2/2	7,070
4	JVNDB-2017-008734	Oracle Fusion Middleware の Oracle WebLogic Server における WLS Security に関する脆弱性	7.5	9.8	2017/10/26	6,137
5	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	6,111
6	JVNDB-2018-001570	Apache Tomcat の複数の脆弱性に対するアップデート	N/A	N/A	2018/2/26	5,286
7	JVNDB-2018-000003	GroupSession におけるオープンリダイレクトの脆弱性	2.6	4.7	2018/1/19	4,735
7	JVNDB-2018-000002	Android アプリ「Nootka」における OS コマンドインジェクションの脆弱性	5.1	7.5	2018/1/19	4,735
9	JVNDB-2018-001389	Hitachi Device Manager における XXE 脆弱性	7.8	7.4	2018/2/14	4,676
10	JVNDB-2018-000009	安心ネットセキュリティ (Windows 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	2018/2/6	4,475
11	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	4,444
12	JVNDB-2017-000247	Qt for Android における環境変数を改ざん可能な脆弱性	5.1	5.3	2017/12/11	4,437
13	JVNDB-2017-000241	ワイヤレスモバイルストレージ「デジ蔵 ShAirDisk」PTW-WMS1 における複数の脆弱性	10.0	9.8	2017/11/30	4,415
14	JVNDB-2018-000014	「フレッツ v4/v6 アドレス選択ツール」のアプリケーションおよびアプリケーションを含む自己解凍書庫における DLL 読み込みに関する脆弱性	6.8	7.8	2018/2/13	4,398

[(*9)] Oracle WebLogic Server の脆弱性（CVE-2017-10271）を悪用する攻撃事例について
https://www.ipa.go.jp/security/ciadr/vul/20180115_WebLogicServer.html

順位	ID	タイトル	CVSSv2 基本値	CVSSv3 基本値	公開日	アクセス数
15	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	4.6	2017/11/16	4,384
16	JVNDB-2018-000017	WXR-1900DHP2 における複数の脆弱性	8.3	8.8	2018/2/26	4372
17	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	6.1	2017/12/1	4,336
18	JVNDB-2018-000004	「フレッツ・ウイルスクリア 申込・設定ツール」および「フレッツ・ウイルスクリア v6 申込・設定ツール」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	7.8	2018/1/22	4,322
19	JVNDB-2017-000245	Windows 版 公的個人認証サービス 利用者クライアントソフト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	2017/12/6	4,297
20	JVNDB-2017-009884	QND Advance/Standard におけるディレクトリトラバーサルの脆弱性	9.4	9.1	2017/11/28	4,277

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 1 月～2018 年 3 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-2017-010236	富士通 NetCOBOL におけるクロスサイトスクリプティングの脆弱性	3.5	4.8	2017/12/8	3,987
2	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	3,785
3	JVNDB-2017-010275	JP1/Service Support および JP1/Integrated Management - Service Support におけるクロスサイトスクリプティングの脆弱性	3.5	4.1	2017/12/11	3,402
4	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	4.1	2017/12/1	3,294
5	JVNDB-2017-008411	Hitachi Command Suite 製品における XXE 脆弱性	7.5	8.1	2017/10/18	3,247

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