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

[2019 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、2019 年 1 月 1 日から 2019 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　セキュリティセンター

2019 年 4 月 24 日

目次

1. 2019 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 97,444 件～

2019 年第 1 四半期（2019 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、2007 年 4 月 25 日に JVN iPedia の公開を開始してから本四半期までの、**脆弱性対策情報の登録件数の累計は 97,444 件になりました**（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 2,018 件になりました。

表 1-1. 2019 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	213 件
	JVN	76 件	8,347 件
	NVD	4,691 件	88,884 件
	計	4,770 件	97,444 件
英語版	国内製品開発者	3 件	213 件
	JVN	18 件	1,805 件
	計	21 件	2,018 件

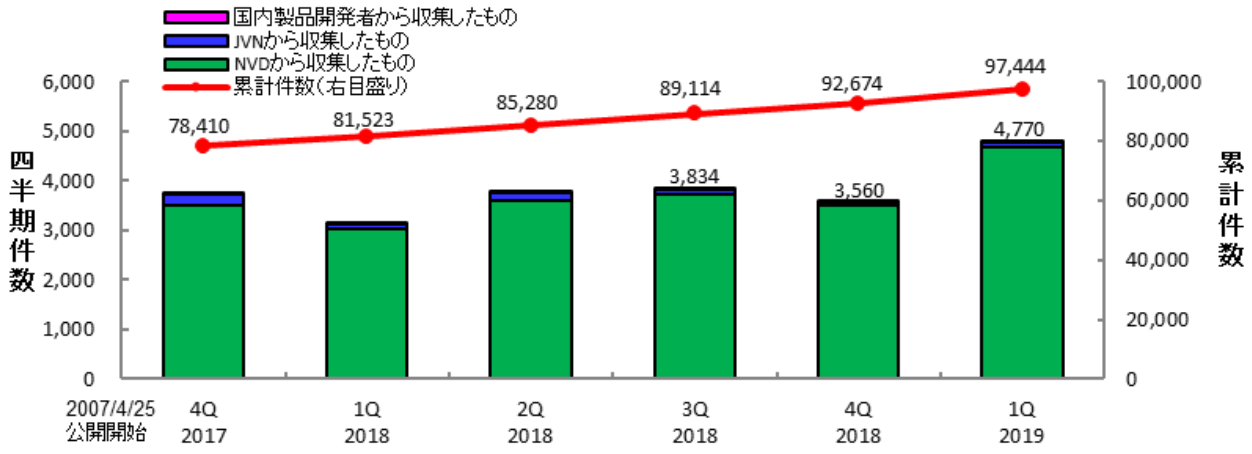

図1−1. JVN iPediaの登録件数の四半期別推移

(*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、2019 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 617 件、CWE-20（不適切な入力確認）が 430 件、CWE-119（バッファエラー）が 407 件、CWE-200（情報漏えい）が 317 件、CWE-284（不適切なアクセス制御）が 311 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。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。

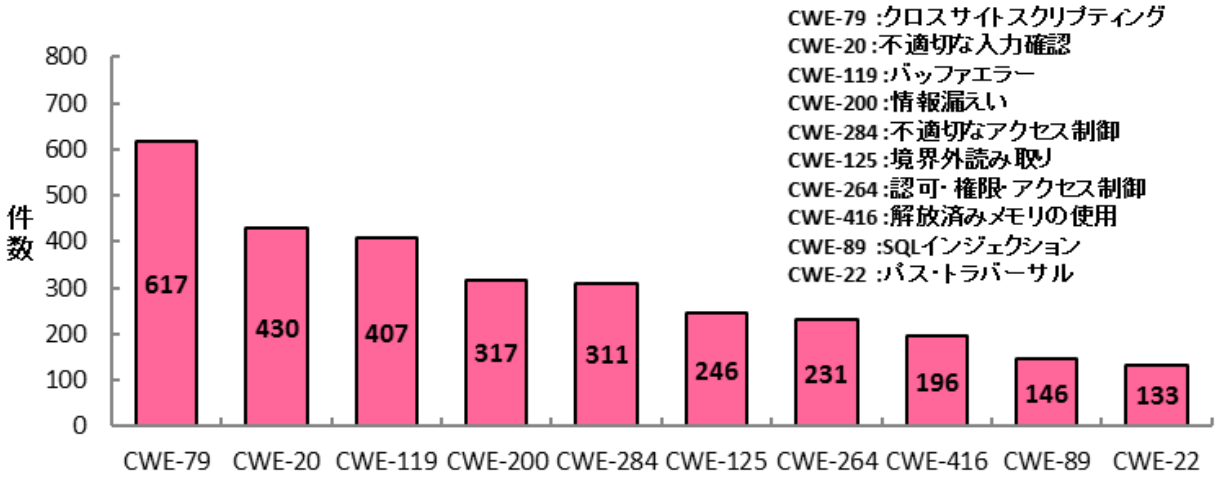

図2−1. 2019年第1四半期に登録された脆弱性の種類別件数

(*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。

2019 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 24.2%、レベルⅡが 64.3%、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。

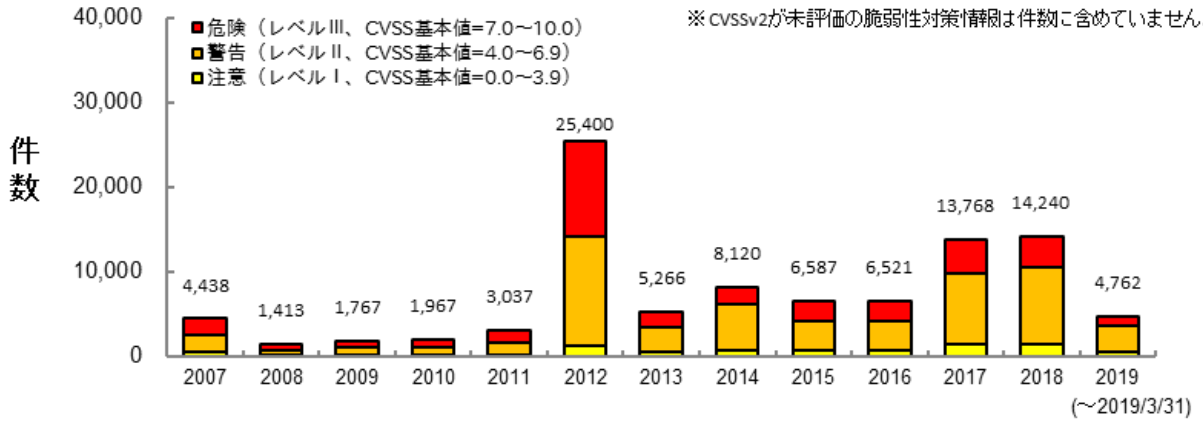

図2-2. 脆弱性の深刻度別件数(CVSSv2)

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。

2019 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 15.3%、「重要」が 42.3%、「警告」が 41.5%、「注意」が 0.9%となっています。

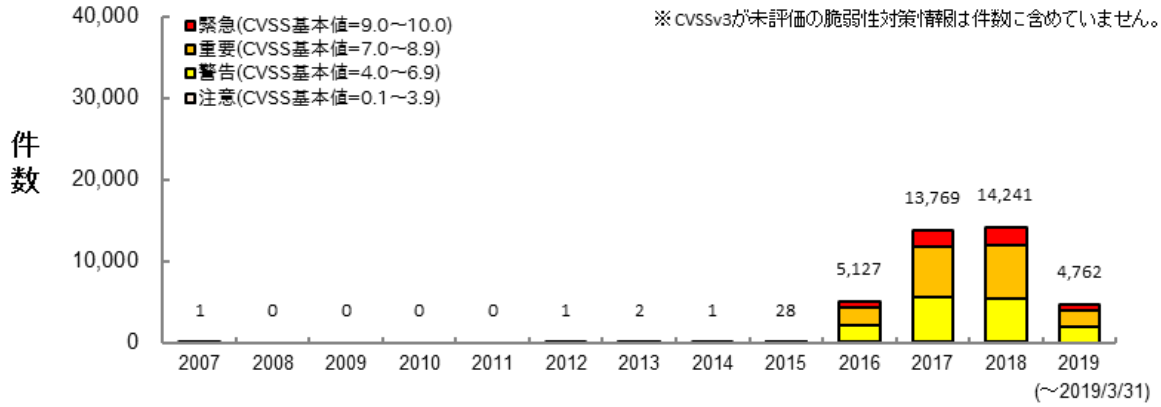

図2-3. 脆弱性の深刻度別件数(CVSSv3)

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。2019 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、2019 年の件数全件の約 75.9%（3,621 件／全 4,770 件）を占めています。

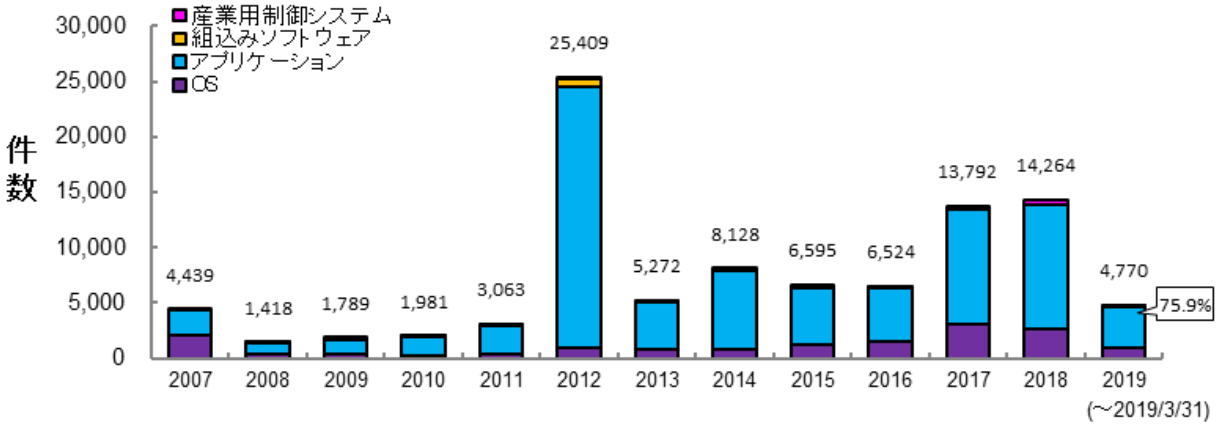

図2-4. 脆弱性対策情報を公表した製品の種類別件数の公開年別推移

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 1,831 件を登録しています。

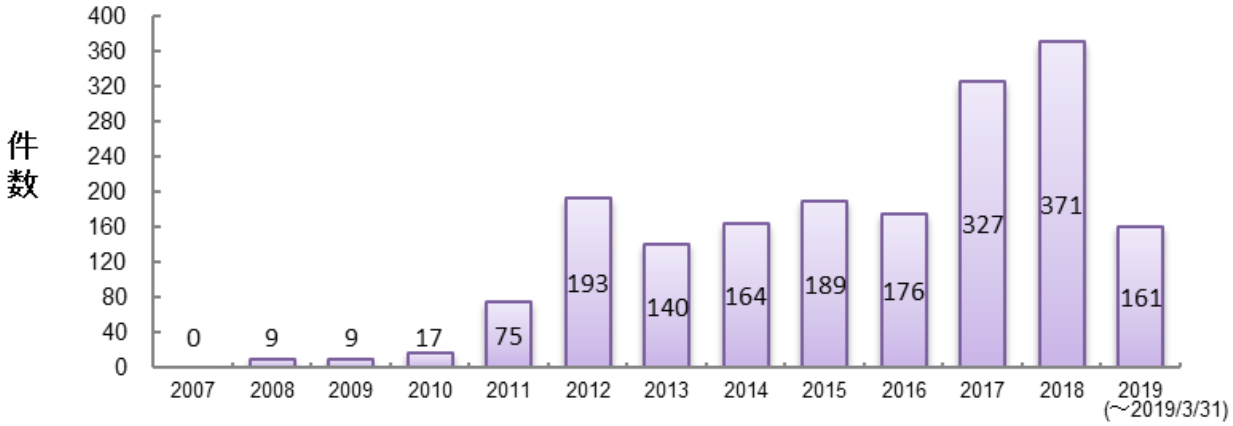

図2-5. JVN iPedia 登録件数(産業用制御システムのみ抽出)

2-4. 脆弱性対策情報の製品別登録状況

表 2-1 は 2019 年第 1 四半期（1 月～3 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。

本四半期において最も登録件数が多かった製品は、前四半期（2018 年第 4 四半期）から引き続き、Debian GNU/Linux となりました。なお、Debian GNU/Linux の登録件数が継続して多い要因として、Debian GNU/Linux が、OS と 5 万件以上のソフトウェアパッケージを統合して提供しており、そのパッケージに発見された脆弱性の修正にあわせて、Debian GNU/Linux 側も修正を行うためと考えられます [(*8)]。

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 [(*9)]。

表 2-1. 製品別 JVN iPedia の脆弱性対策情報登録件数　上位 20 件 [2019 年 1 月～2019 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)	401
2	OS	Red Hat Enterprise Linux Server (レッドハット)	246
3	OS	Red Hat Enterprise Linux Workstation (レッドハット)	237
4	OS	Red Hat Enterprise Linux Desktop (レッドハット)	236
5	ブラウザ	Google Chrome (Google)	203
6	OS	Ubuntu (Canonical)	186
7	OS	Android (Google)	167
8	ファームウェア	Qualcomm firmware (クアルコム) [(*10)]	113
9	PDF 閲覧	Foxit Reader (Foxit Software Inc)	108
10	PDF 閲覧・編集	Foxit PhantomPDF (Foxit Software Inc)	94
11	PDF 閲覧・編集	Adobe Acrobat (アドビシステムズ)	92
11	PDF 閲覧	Adobe Acrobat Reader DC (アドビシステムズ)	92
11	PDF 閲覧・編集	Adobe Acrobat DC (アドビシステムズ)	92
14	OS	Microsoft Windows 10 (マイクロソフト)	44
14	OS	Microsoft Windows Server (マイクロソフト)	44
16	ビデオ監視ソフトウェア	ZoneMinder (ZoneMinder)	41
17	OS	Microsoft Windows Server 2019 (マイクロソフト)	39

[(*8)] Debian について
https://www.debian.org/intro/about.ja.html
[(*9)] 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
[(*10)] 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。

順位	カテゴリ	製品名（ベンダ名）	登録件数
18	OS	Microsoft Windows Server 2016 (マイクロソフト)	38
19	ブラウザ	Mozilla Firefox (Mozilla Foundation)	36
20	OS	Linux Kernel (Kernel.org)	33

3. 脆弱性対策情報の活用状況

表 3-1 は 2019 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。

本四半期で上位にランクインした脆弱性対策情報の内、4 件（3 位、6 位、9 位、13 位）が国内製品開発者から収集した脆弱性対策情報で、それら 4 件と 5 位を除いた 15 件が脆弱性対策情報ポータルサイト JVN で公開した脆弱性対策情報です。こうした脆弱性対策情報に登録される製品は、国内での利用者が多く、注目を集めるため、該当するページへのアクセス数が増加する傾向にあります。

表 3-1.JVN iPedia の脆弱性対策情報へのアクセス　上位 20 件 [2019 年 1 月～2019 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-2019-000001	WordPress 用プラグイン spam-byebye 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	2019/1/10	6,672
2	JVNDB-2018-000137	GROWI 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	2018/12/26	6,548
3	JVNDB-2018-010851	Hitachi Automation Director におけるクリックジャッキングの脆弱性	4.3	4.3	2018/12/26	6,379
4	JVNDB-2019-000003	iOS アプリ「HOUSE GATE」におけるディレクトリトラバーサルの脆弱性	4.3	4.7	2019/1/24	6,354
5	JVNDB-2014-007972	OpenKM におけるクロスサイトスクリプティングの脆弱性	3.5	なし	2015/3/13	5,978
6	JVNDB-2019-001095	Hitachi Device Manager におけるクロスサイトスクリプティングの脆弱性	4.0	4.7	2019/1/22	5,717
7	JVNDB-2018-000135	WordPress 用プラグイン Google XML Sitemaps におけるクロスサイトスクリプティングの脆弱性	4.0	4.8	2018/12/25	5,495
8	JVNDB-2018-000134	PgpoolAdmin におけるアクセス制限不備の脆弱性	7.5	9.8	2018/12/21	5,448
9	JVNDB-2019-001094	Hitachi Command Suite 製品および Hitachi Infrastructure Analytics Advisor における情報露出の脆弱性	5.0	5.3	2019/1/22	5,420
10	JVNDB-2018-000136	マッピング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	2018/12/25	5,237
11	JVNDB-2018-000133	cordova-plugin-ionic-webview におけるパストラバーサルの脆弱性	4.3	4.7	2018/12/21	5,199
12	JVNDB-2019-000006	POWER EGG において任意の EL 式を実行される脆弱性	7.5	7.3	2019/2/5	5,041
13	JVNDB-2018-010027	JP1/Operations Analytics におけるディレクトリパーミッションの問題	3.5	4.9	2018/12/4	5,009
14	JVNDB-2018-000129	i-FILTER における複数の脆弱性	4.3	6.1	2018/12/7	4,992
15	JVNDB-2018-000132	東芝ライテック製ホームゲートウェイにおける複数の脆弱性	8.3	8.8	2018/12/19	4,890

順位	ID	タイトル	CVSSv2 基本値	CVSSv3 基本値	公開日	アクセス数
16	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	4,801
17	JVNDB-2019-000010	azure-umqtt-c におけるサービス運用妨害 (DoS) の脆弱性	5.0	7.5	2019/2/20	4,759
18	JVNDB-2019-000004	UNLHA32.DLL、 UNARJ32.DLL、 LHMelting および LMLzh32.DLL における DLL 読み込みに関する脆弱性	6.8	7.8	2019/1/31	4,699
19	JVNDB-2018-000124	RICOH Interactive Whiteboard における複数の脆弱性	10.0	9.8	2018/11/27	4,666
20	JVNDB-2018-000131	Aterm WF1200CR および Aterm WG1200CR における複数の脆弱性	5.8	8.8	2018/12/14	4,662

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 [2019 年 1 月～2019 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-2018-010851	Hitachi Automation Director におけるクリックジャッキングの脆弱性	4.3	4.3	2018/12/26	6,379
2	JVNDB-2019-001095	Hitachi Device Manager におけるクロスサイトスクリプティングの脆弱性	4.0	4.7	2019/1/22	5,717
3	JVNDB-2019-001094	Hitachi Command Suite 製品および Hitachi Infrastructure Analytics Advisor における情報露出の脆弱性	5.0	5.3	2019/1/22	5,420
4	JVNDB-2018-010027	JP1/Operations Analytics におけるディレクトリパーミッションの問題	3.5	4.9	2018/12/4	5,009
5	JVNDB-2018-009328	JP1/VERITAS 製品における複数の脆弱性	10.0	9.8	2018/11/15	4,521

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

2017 年以前の公開	2018 年の公開	2019 年の公開