

# 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 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、2019 年 4 月 1 日から 2019 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。

## 目次

1. 2019 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 .....	- 3 -
1-1. 脆弱性対策情報の登録状況 .....	- 3 -
2. JVN iPedia の登録データ分類.....	- 4 -
2-1. 脆弱性の種類別件数 .....	- 4 -
2-2. 脆弱性に関する深刻度別割合 .....	- 5 -
2-3. 脆弱性対策情報を公開した製品の種類別件数 .....	- 7 -
2-4. 脆弱性対策情報の製品別登録状況 .....	- 8 -
3. 脆弱性対策情報の活用状況 .....	- 9 -

# 1. 2019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<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 102,651 件～

2019年第2四半期(2019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、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 102,651 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 2,048 件になりました。

表 1-1. 2019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	5件	218件
	JVN	325件	8,672件
	NVD	4,877件	93,761件
	計	5,207件	102,651件
英語版	国内製品開発者	4件	217件
	JVN	25件	1,831件
	計	29件	2,048件

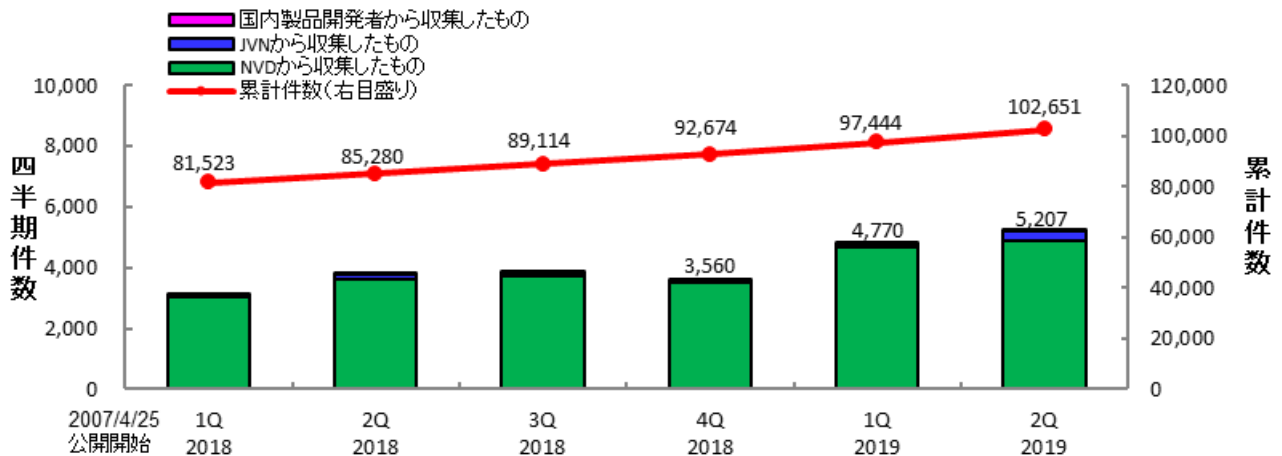


図 1-1. JVN iPedia の登録件数の四半期別推移

(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 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 579 件、CWE-79（クロスサイトスクリプティング）が 561 件、CWE-20（不適切な入力確認）が 518 件、CWE-200（情報漏えい）が 378 件、CWE-264（認可・権限・アクセス制御）が 306 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おそれがあります。

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](#)」<sup>(4)</sup>や「[IPA セキュア・プログラミング講座](#)」<sup>(5)</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>(6)</sup>などを公開しています。

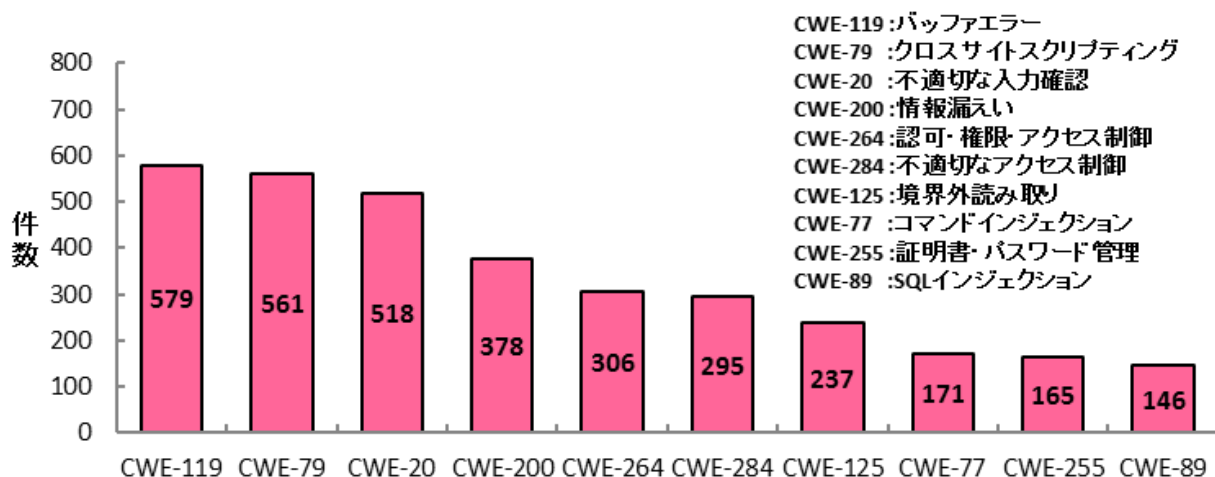


図 2-1. 2019 年第 2 四半期に登録された脆弱性の種類別件数

<sup>(4)</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>(5)</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>(6)</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。

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 27.4%、レベル II が 61.9%、レベル I が 10.7% 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 89.3% を占めています。

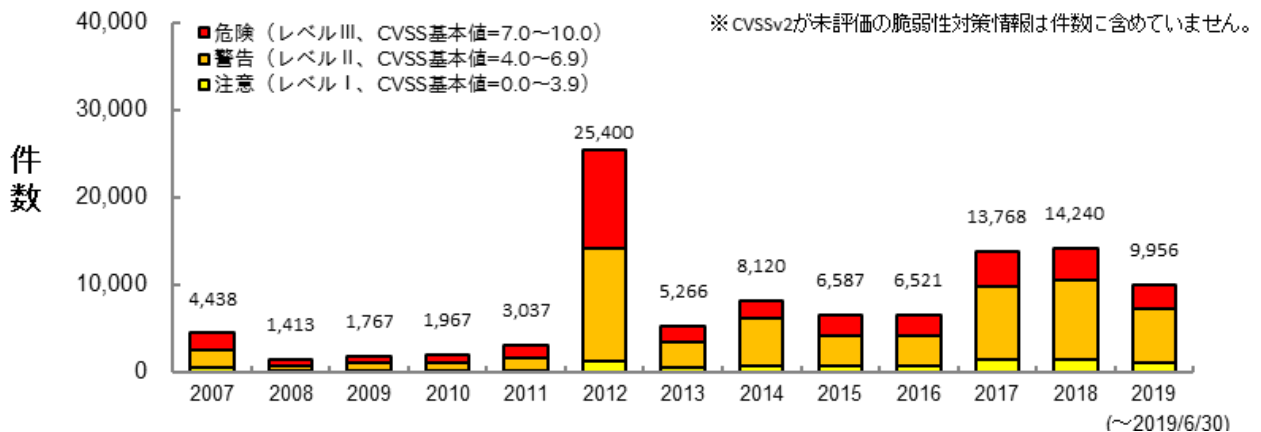


図 2-2. 脆弱性の深刻度別件数(CVSSv2)

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 16.0%、「重要」が 44.0%、「警告」が 39.1%、「注意」が 0.9% となっています。

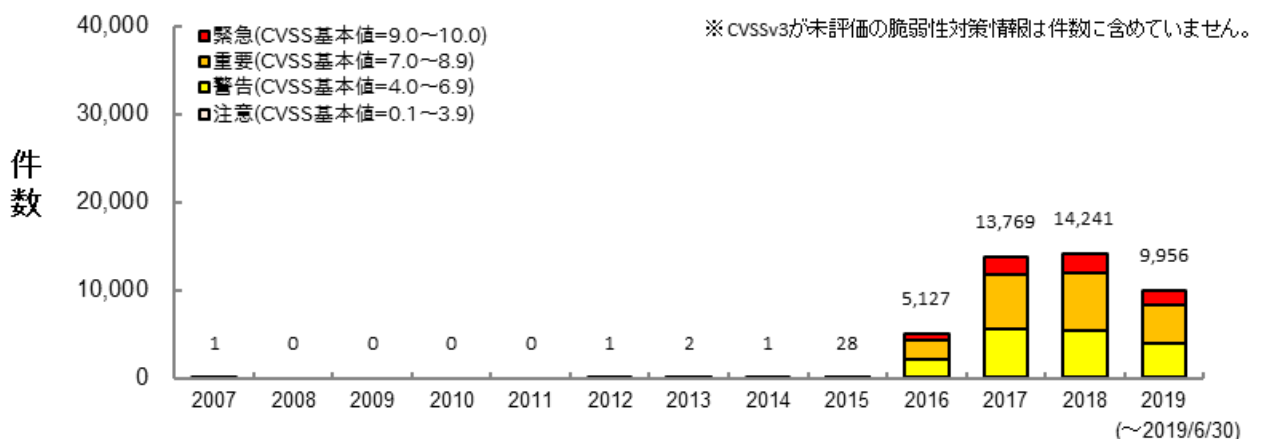


図 2-3. 脆弱性の深刻度別件数(CVSSv3)

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<sup>(\*)</sup> で公開しています。

---

<sup>(\*)</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。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 74.6%（7,445 件／全 9,977 件）を占めています。

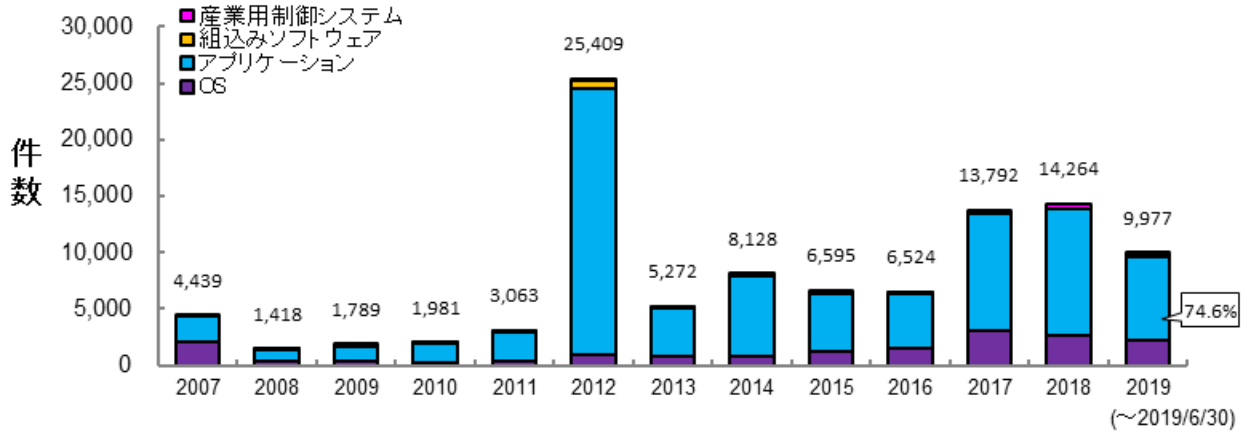


図 2-4. 脆弱性対策情報を公表した製品の種別別件数の公開年別推移

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 1,969 件を登録しています。

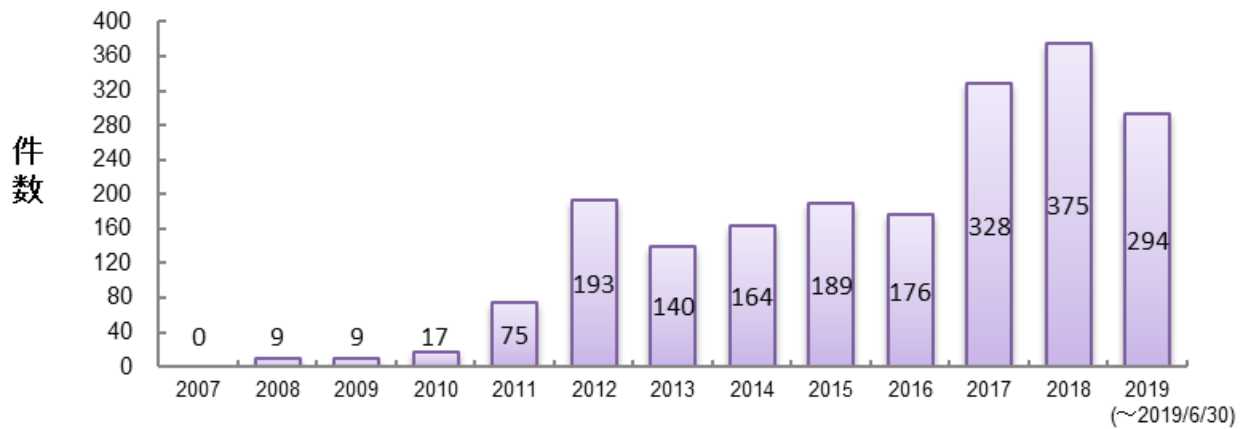


図 2-5. JVN iPedia 登録件数（産業用制御システムのみ抽出）

## 2-4. 脆弱性対策情報の製品別登録状況

表 2-1 は 2019 年第 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。

本四半期は OS 製品に関する脆弱性対策情報を多数登録しており、上位 20 件中 9 件がマイクロソフト、4 件がアップル、2 件が Linux 系 OS と OS 製品が全体の 7 割以上を占めました。

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>(\*)8)</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 [2019 年 4 月～2019 年 6 月]

順位	カテゴリ	製品名（ベンダ名）	登録件数
1	OS	Microsoft Windows 10 (マイクロソフト)	178
2	OS	Microsoft Windows Server (マイクロソフト)	176
3	PDF 閲覧	Adobe Acrobat Reader DC (アドビシステムズ)	175
3	PDF 閲覧・編集	Adobe Acrobat DC (アドビシステムズ)	175
3	PDF 閲覧・編集	Adobe Acrobat (アドビシステムズ)	175
6	OS	Microsoft Windows Server 2019 (マイクロソフト)	167
7	OS	iOS (アップル)	157
8	OS	Microsoft Windows Server 2016 (マイクロソフト)	152
9	OS	Microsoft Windows Server 2008 (マイクロソフト)	141
10	OS	Microsoft Windows 7 (マイクロソフト)	140
11	OS	Microsoft Windows Server 2012 (マイクロソフト)	136
12	OS	Microsoft Windows 8.1 (マイクロソフト)	133
13	OS	Microsoft Windows RT 8.1 (マイクロソフト)	130
14	OS	tvOS (アップル)	110
15	OS	Apple Mac OS X (アップル)	108
16	ネットワーク管理 ソフトウェア	HPE Intelligent Management Center (ヒューレット・パカード・エンタープライズ)	104
17	OS	Debian GNU/Linux (Debian)	100
18	OS	watchOS (アップル)	95
19	ファームウェア	Qualcomm component (クアルコム) <sup>(*)9)</sup>	91
20	OS	Ubuntu (Canonical)	86

<sup>(\*)8)</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>

<sup>(\*)9)</sup> 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。



### 3. 脆弱性対策情報の活用状況

表 3-1 は 2019 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。

本四半期で上位にランクインした脆弱性対策情報の内、2 件（3 位、19 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 2 件と 4 位を除いた 17 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。JVN 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 4 月～2019 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-2019-000022	GNU Wget におけるバッファオーバーフローの脆弱性	6.8	8.8	2019/4/3	10,020
2	JVNDB-2019-000021	Android アプリ「JR 東日本 列車運行情報 プッシュ通知アプリ」が使用する API サーバにアクセス制限不備の脆弱性	6.4	6.5	2019/4/1	8,754
3	JVNDB-2019-002892	Cosminexus における複数の脆弱性	なし	なし	2019/4/25	8,750
4	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	7,915
5	JVNDB-2019-000014	Microsoft Teams 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	2019/2/28	7,419
6	JVNDB-2019-000020	PowerActPro Master Agent Windows 版におけるアクセス制限不備の脆弱性	1.7	3.3	2019/3/27	7,320
7	JVNDB-2019-000023	サイボウズ Garoon における複数の脆弱性	6.5	6.0	2019/4/25	7,292
8	JVNDB-2019-000018	iOS アプリ「an」におけるディレクトリトラバーサル脆弱性の脆弱性	4.3	4.7	2019/3/19	7,157
9	JVNDB-2019-000019	簡易 CMS 紀永における複数のクロスサイトスクリプティングの脆弱性	4.3	6.1	2019/3/15	6,774
10	JVNDB-2019-000015	iOS アプリ「iChain 保険ウォレット」におけるディレクトリトラバーサル脆弱性の脆弱性	4.3	4.7	2019/3/12	6,622
11	JVNDB-2018-000099	サイボウズ Garoon におけるディレクトリトラバーサル脆弱性の脆弱性	5.5	6.4	2018/9/10	6,238
12	JVNDB-2018-000130	サイボウズ Garoon におけるアクセス制限回避の脆弱性	5.0	7.5	2018/12/10	6,081
13	JVNDB-2019-000017	Dradis Community Edition および Dradis Professional Edition 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	2019/3/5	6,072
14	JVNDB-2019-000012	ナブラックにおける複数の脆弱性	8.5	8.2	2019/2/27	6,067
15	JVNDB-2019-000013	Windows 7 における DLL 読み込みに関する脆弱性	6.8	7.8	2019/2/28	6,024

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-2019-000016	WordPress 用プラグイン Smart Forms におけるクロスサイトリクエストフォージェリの脆弱性	2.6	4.3	2019/2/28	5,933
17	JVNDB-2019-000011	WordPress 用プラグイン FormCraft におけるクロスサイトリクエストフォージェリの脆弱性	2.6	4.3	2019/2/26	5,840
18	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	5,724
19	JVNDB-2019-001285	JP1/Base における DoS 脆弱性	なし	なし	2019/2/25	5,709
20	JVNDB-2019-000009	Creative Cloud Desktop Application 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	2019/2/18	5,665

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 4 月～2019 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-2019-002892	Cosminexus における複数の脆弱性	なし	なし	2019/4/25	8,750
2	JVNDB-2019-001285	JP1/Base における DoS 脆弱性	なし	なし	2019/2/25	5,709
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	5,376
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	5,255
5	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	5,101

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
-------------	-----------	-----------