

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 [2023 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、2023 年 4 月 1 日から 2023 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および事例について紹介しています。

目次

1. 2023 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	- 2 -
1-1. 脆弱性対策情報の登録状況	- 2 -
2. JVN iPedia の登録データ分類.....	- 3 -
2-1. 脆弱性の種類別件数	- 3 -
2-2. 脆弱性に関する深刻度別割合	- 4 -
2-3. 脆弱性対策情報を公開した製品の種類別件数	- 6 -
2-4. 脆弱性対策情報の製品別登録状況	- 7 -
3. 脆弱性対策情報の活用状況	- 8 -

1. 2023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 158,560 件～

2023年第2四半期(2023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表1-1の通りとなり⁽⁴⁾、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158,560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表1-1の通り、累計で2,629件になりました。

表 1-1. 2023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	2件	265件
	JVN	254件	12,435件
	NVD	3,362件	145,860件
	計	3,618件	158,560件
英語版	国内製品開発者	3件	269件
	JVN	54件	2,360件
	計	57件	2,629件

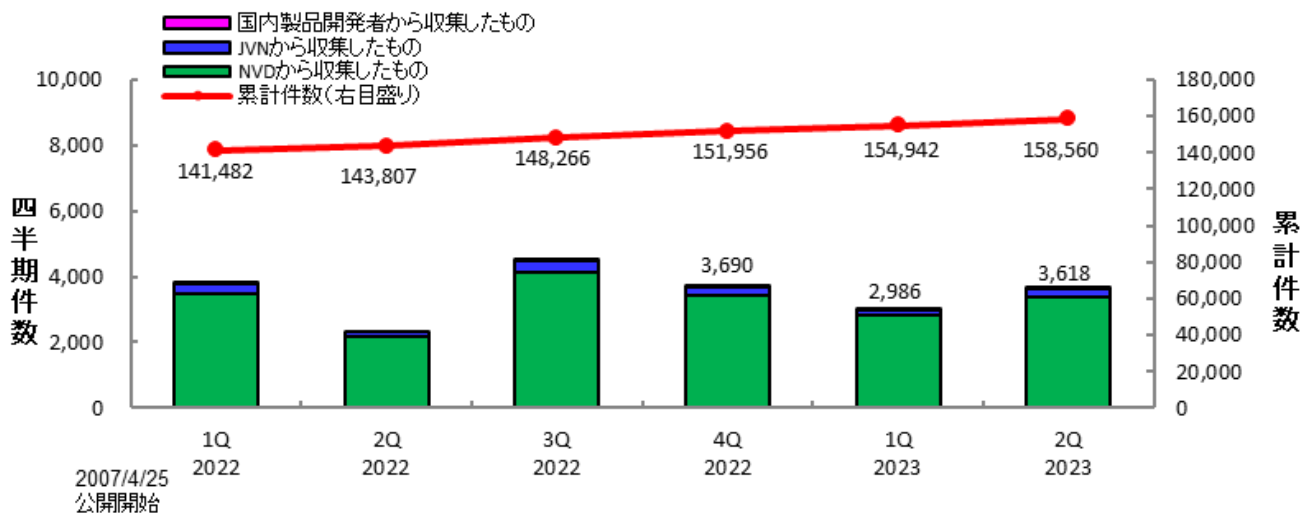


図 1-1. JVN iPedia の登録件数の四半期別推移

⁽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>

⁽⁴⁾ JVN iPedia の情報の収集元である NVD は本四半期で 7,160 件の公開件数となっている。そのため世の中で公開されている脆弱性の件数は JVN iPedia の登録件数より多い状況となっている。世の中の脆弱性の件数については NVD の公開件数等を参考にすることを推奨する。

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、2023 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-79（クロスサイトスクリプティング）が 460 件、CWE-89（SQL インジェクション）が 262 件、CWE-787（境界外書き込み）が 249 件、CWE-20（不適切な入力確認）が 178 件、CWE-125（境界外読み取り）が 140 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、開発者が実施すべき脆弱性対処をまとめた資料「[脆弱性対処に向けた製品開発者向けガイド](#)⁽⁵⁾」、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](#)⁽⁶⁾」、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](#)⁽⁷⁾」などを公開しています。

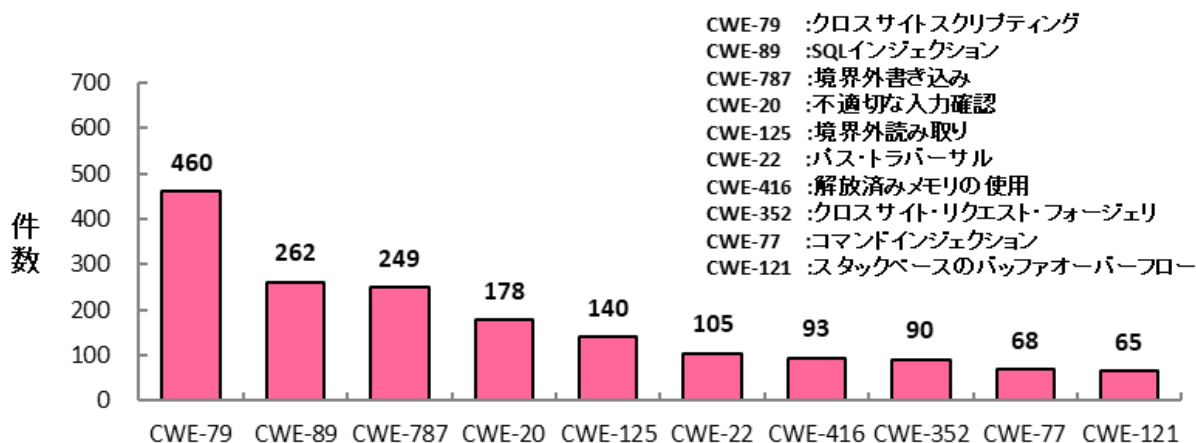


図 2-1. 2023 年第 2 四半期に登録された脆弱性の種類別件数

⁽⁵⁾ IPA：「脆弱性対処に向けた製品開発者向けガイド」
<https://www.ipa.go.jp/security/guide/vuln/forvendor.html>

⁽⁶⁾ IPA：「安全なウェブサイトの作り方」
<https://www.ipa.go.jp/security/vuln/websecurity/about.html>

⁽⁷⁾ IPA：「脆弱性体験学習ツール AppGoat」
<https://www.ipa.go.jp/security/vuln/appgoat/index.html>

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。

2023 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 3 が全体の 20.2%、レベル 2 が 65.7%、レベル 1 が 14.0% 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 2 以上が 85.9% を占めています。

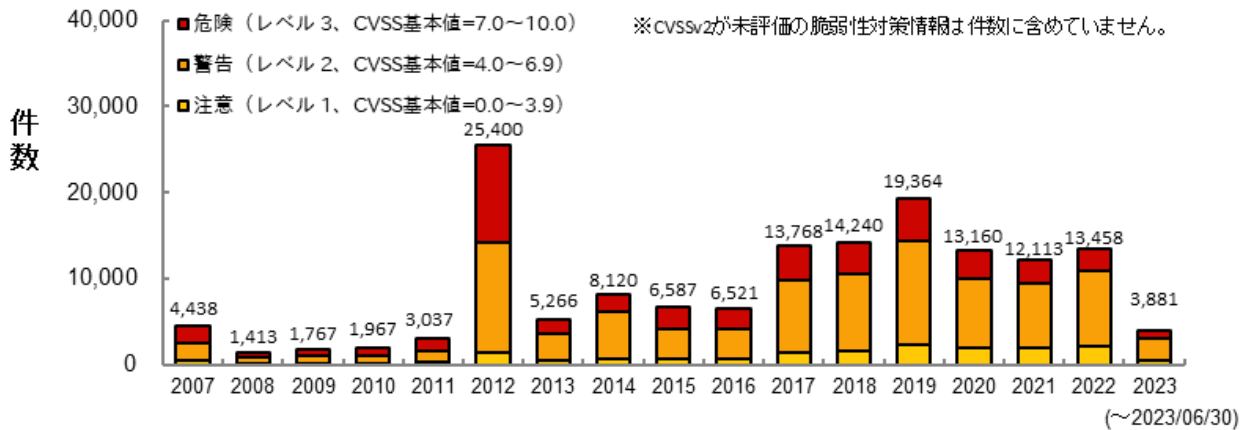


図 2-2. 脆弱性の深刻度別件数(CVSSv2)

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。

2023 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 16.8%、「重要」が 40.5%、「警告」が 40.9%、「注意」が 1.8% となっています。

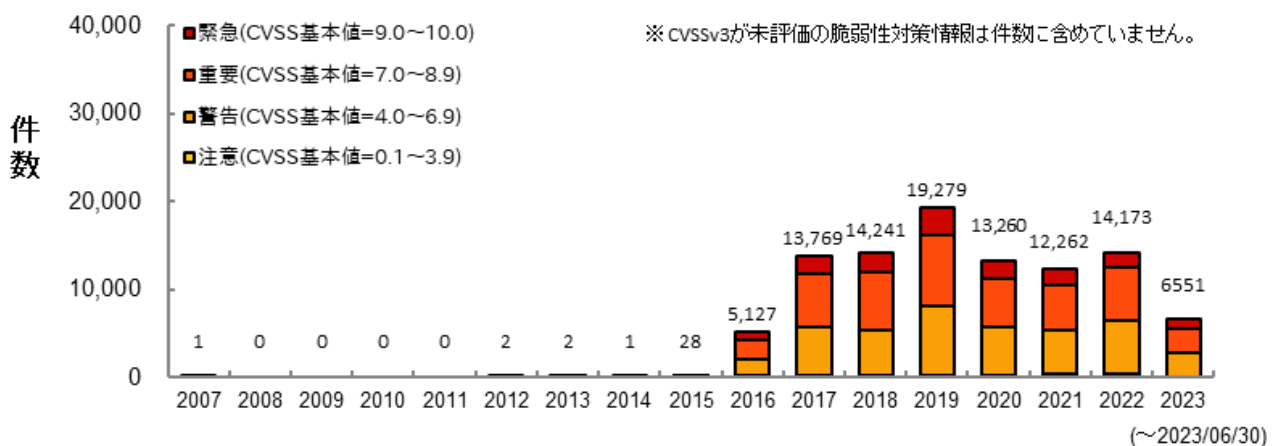


図 2-3. 脆弱性の深刻度別件数(CVSSv3)

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^(*)で公開しています。

^(*) IPA : 「JVN iPedia 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。2023 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、2023 年の件数全件の 71.5%（4,722 件／全 6,604 件）を占めています。

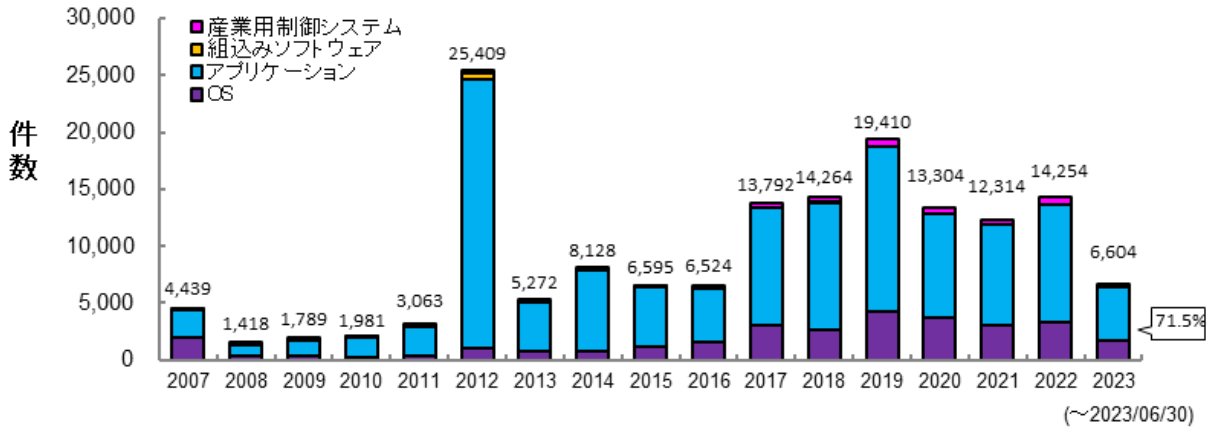


図 2-4. 脆弱性対策情報を公表した製品の種別別件数の公開年別推移

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 4,075 件を登録しています。

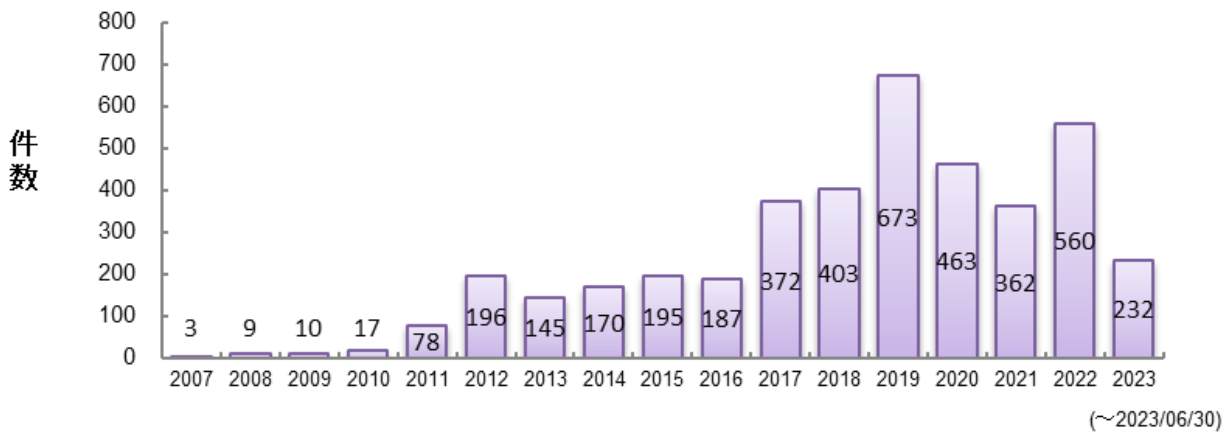


図 2-5. JVN iPedia 登録件数（産業用制御システムのみ抽出）

2-4. 脆弱性対策情報の製品別登録状況

表 2-1 は 2023 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上位 20 件を示したものです。

本四半期においてはクアルコムが提供する Qualcomm component が 1 位となりました。2 位以降はマイクロソフトが提供する Windows、Fedora Project が提供する Fedora、Google が提供する Android などの OS 製品が上位にランクインしています。

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^(*)。

表 2-1. 製品別 JVN iPedia の脆弱性対策情報登録件数 上位 20 件 [2023 年 4 月～2023 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 component (クアルコム)	420
2	OS	Microsoft Windows Server 2022 (マイクロソフト)	138
3	OS	Microsoft Windows Server 2019 (マイクロソフト)	135
4	OS	Fedora (Fedora Project)	134
5	OS	Microsoft Windows Server 2016 (マイクロソフト)	126
6	OS	Microsoft Windows 11 (マイクロソフト)	124
7	OS	Microsoft Windows 10 (マイクロソフト)	119
8	OS	Android (Google)	116
9	OS	Microsoft Windows Server 2012 (マイクロソフト)	115
10	OS	Debian GNU/Linux (Debian)	109
11	OS	Microsoft Windows Server 2008 (マイクロソフト)	85
12	その他	Insteon Hub (Insteon)	81
13	その他	Bentley View (Bentley Systems)	80
14	ファームウェア	RLC-410w ファームウェア (Reolink Digital Technology)	78
14	その他	MicroStation (Bentley Systems)	78
16	その他	MicroStation Connect (Bentley Systems)	71
17	ブラウザ	Google Chrome (Google)	64
18	その他	Google TensorFlow (Google)	56
19	OS	Linux Kernel (Linux)	44
20	PDF 閲覧・編集	PDF-XChange Editor (Tracker Software Products)	37

^(*) IPA：「脆弱性対策の効果的な進め方（実践編）」

<https://www.ipa.go.jp/security/reports/technicalwatch/20150331.html>

3. 脆弱性対策情報の活用状況

表 3-1 は 2023 年第 2 四半期（4 月～6 月）にアクセスが多かった JVN iPedia の脆弱性対策情報の上位 20 件を示したものです。

本四半期は、前四半期に続いて WordPress 用のプラグインの脆弱性が多くランクインしました。また上位に 2022 年公開のものがランクインしていますが、これは特定の組織より機械的なアクセスを受けたことによるものです。

表 3-1. JVN iPedia の脆弱性対策情報へのアクセス 上位 20 件 [2023 年 4 月～2023 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-2021-015177 Sharetribe Go 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	2022/11/11	10,944
2	JVNDB-2021-015181 iPack SCADA Automation ソフトウェアにおける SQL インジェクションの脆弱性	7.5	9.8	2022/11/11	10,700
3	JVNDB-2021-015197 Apache ShenYu Admin における認証に関する脆弱性	7.5	9.8	2022/11/11	10,288
4	JVNDB-2021-015198 MedData HBYS ソフトウェアにおける SQL インジェクションの脆弱性	7.5	9.8	2022/11/11	9,594
5	JVNDB-2022-002693 CLUSTERPRO X および EXPRESSCLUSTER X における制御されていない検索パスの要素に関する脆弱性	-	9.8	2022/11/11	8,815
6	JVNDB-2022-002694 CLUSTERPRO X および EXPRESSCLUSTER X における不適切なデフォルトパーミッションに関する脆弱性	-	9.8	2022/11/11	7,934
7	JVNDB-2023-000039 WordPress 用プラグイン LIQUID SPEECH BALLOON 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	2023/4/19	7,875
8	JVNDB-2022-002695 CLUSTERPRO X および EXPRESSCLUSTER X における古典的バッファオーバーフローの脆弱性	-	9.8	2022/11/11	7,400
9	JVNDB-2022-000091 WordPress 用プラグイン WordPress Popular Posts における外部入力の不適切な使用に関する脆弱性	5.0	5.3	2022/11/18	7,378

順位	ID/タイトル	CVSSv2 基本値	CVSSv3 基本値	公開日	アクセス 数
10	JVNDB-2023-000007 WordPress 用プラグイン Welcart e-Commerce におけるディレクトリトラバーサルの脆弱性	5.0	7.5	2023/1/17	7,316
11	JVNDB-2023-000040 WordPress 用プラグイン Appointment and Event Booking Calendar for WordPress - Amelia 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	2023/4/24	7,233
12	JVNDB-2022-000087 WordPress における複数の脆弱性	5.0	5.3	2022/11/8	7,128
13	JVNDB-2022-000085 WordPress 用プラグイン Salon booking system 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	2022/11/8	6,851
14	JVNDB-2022-000038 WordPress 用プラグイン WP Statistics 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	2022/5/24	6,791
15	JVNDB-2022-000041 WordPress 用プラグイン Modern Events Calen- dar Lite 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	2022/6/1	6,790
16	JVNDB-2023-000050 WordPress 用プラグイン MW WP Form および Snow Monkey Forms における複数の脆弱性	7.5	8.3	2023/5/15	6,760
17	JVNDB-2023-000042 WordPress 用プラグイン Newsletter 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	2023/5/9	6,405
18	JVNDB-2022-002696 CLUSTERPRO X および EXPRESSCLUSTER X に おけるパストラバーサルの脆弱性	-	9.8	2022/11/11	6,379
19	JVNDB-2022-000057 WordPress 用プラグイン Newsletter 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	2022/7/25	6,253
20	JVNDB-2022-000026 WordPress 用プラグイン「MicroPayments - Paid Author Subscriptions, Content, Downloads, Membership」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	2022/4/15	6,163

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 [2023 年 4 月～2023 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-2023-001492 JP1/VERITAS 製品における脆弱性	-	7.1	2023/4/12	4,685
2	JVNDB-2023-001926 Hitachi Ops Center Analyzer におけるクロスサイトスクリプティングの脆弱性	-	7.6	2023/5/23	3,359
3	JVNDB-2023-001008 Hitachi Tuning Manager におけるファイルおよびディレクトリパーミッションの脆弱性	-	6.6	2023/1/18	2,814
4	JVNDB-2023-001269 Hitachi Automation Director, Hitachi Infrastructure Analytics Advisor および Hitachi Ops Center 製品におけるファイルおよびディレクトリパーミッションの脆弱性	-	6.6	2023/3/1	2,787
5	JVNDB-2022-002771 JP1/Automatic Operation におけるユーザ認証に関わる情報露出の脆弱性	-	3.3	2022/12/7	2,721