

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 [2020 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、2020 年 4 月 1 日から 2020 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. 2020 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. 2020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 120,883 件～

2020年第2四半期(2020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120,883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2,159件になりました。

表 1-1. 2020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	7件	239件
	JVN	172件	9,271件
	NVD	4,100件	111,373件
	計	4,279件	120,883件
英語版	国内製品開発者	7件	237件
	JVN	20件	1,922件
	計	27件	2,159件

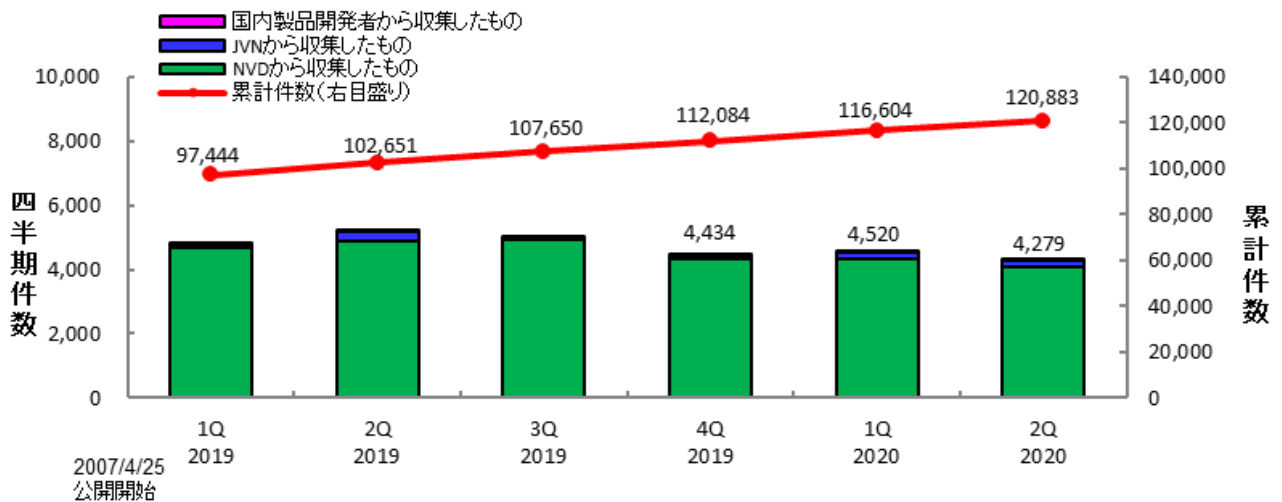


図 1-1. JVN iPedia の登録件数の四半期別推移

(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、2020 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 463 件、CWE-200（情報漏えい）が 352 件、CWE-20（不適切な入力確認）が 271 件、CWE-269（不適切な権限管理）が 257 件、CWE-787（境界外書き込み）が 246 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。

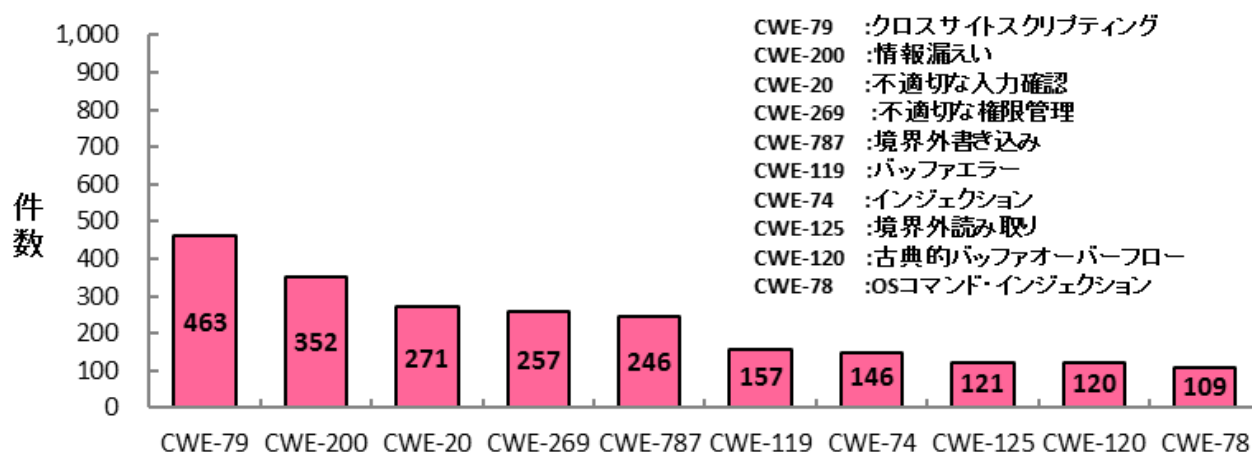


図 2-1. 2020 年第 2 四半期に登録された脆弱性の種類別件数

⁽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。

2020 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 23.8%、レベル II が 61.7%、レベル I が 14.5% 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 85.5% を占めています。

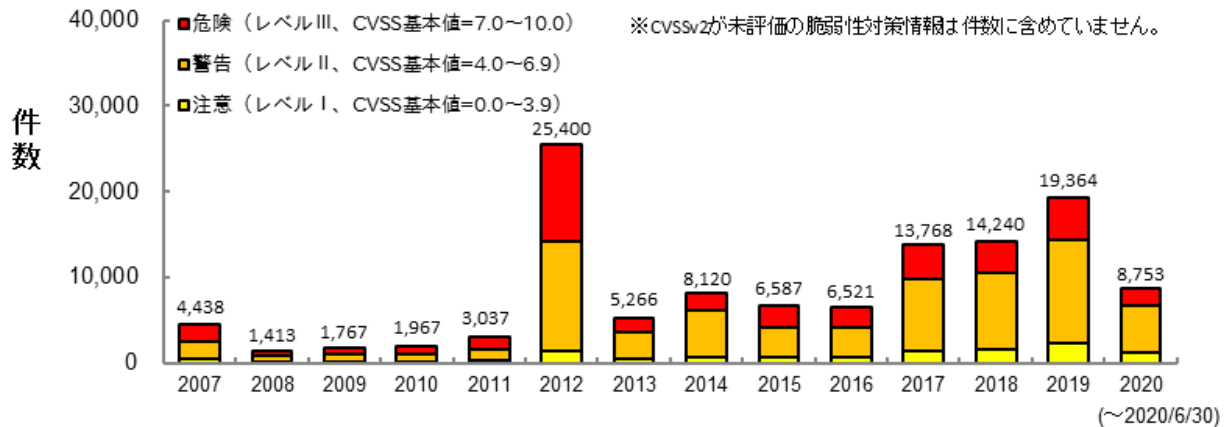


図 2-2. 脆弱性の深刻度別件数(CVSSv2)

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。

2020 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 41.5%、「警告」が 40.4%、「注意」が 2.1% となっています。

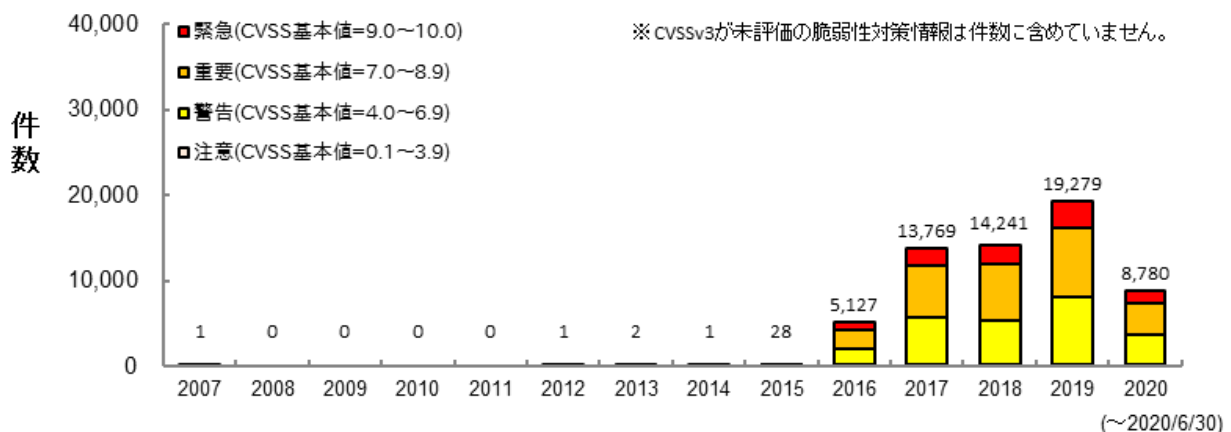


図 2-3. 脆弱性の深刻度別件数(CVSSv3)

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 : 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。2020 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、2020 年の件数全件の約 68.4% (6,022 / 全 8,798 件) を占めています。

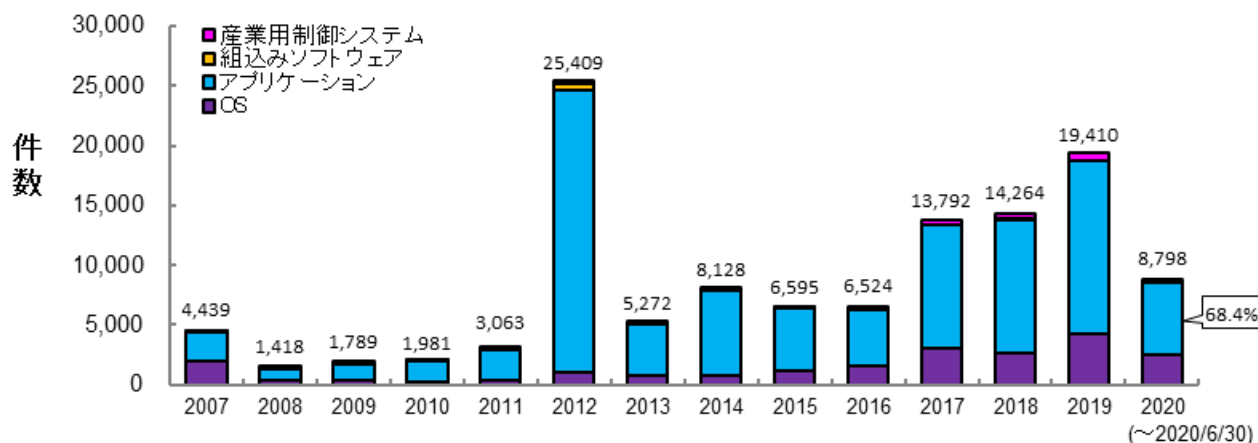


図 2-4. 脆弱性対策情報を公表した製品の種別別件数の公開年別推移

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 2,627 件を登録しています。

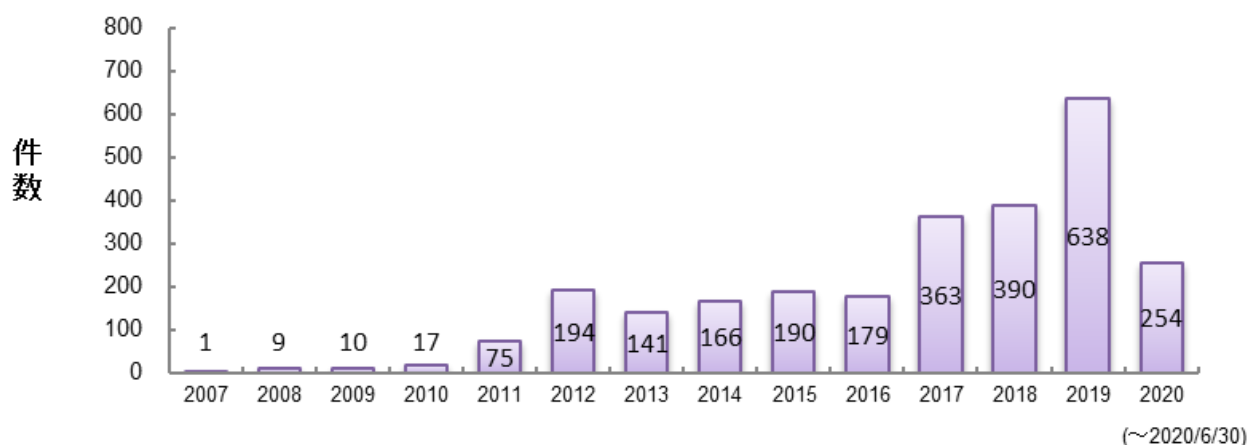


図 2-5. JVN iPedia 登録件数 (産業用制御システムのみ抽出)

2-4. 脆弱性対策情報の製品別登録状況

表 2-1 は 2020 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。

本四半期において最も登録件数が多かった製品は前四半期から引き続き、Microsoft Windows 10 となりました。2 位以降も同社製品である Windows OS が多くランクインされています。他にも Google が提供する Android やアップルが提供する iOS 等、OS 製品に関する脆弱性対策情報が多く登録されました。

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^(*)。

表 2-1. 製品別 JVN iPedia の脆弱性対策情報登録件数 上位 20 件 [2020 年 4 月～2020 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)	333
2	OS	Microsoft Windows Server (マイクロソフト)	327
3	OS	Android (Google)	319
4	OS	Microsoft Windows Server 2019 (マイクロソフト)	310
5	OS	Microsoft Windows Server 2016 (マイクロソフト)	278
6	ファームウェア	Qualcomm component (クアルコム)	210
7	OS	Microsoft Windows Server 2012 (マイクロソフト)	198
8	OS	Microsoft Windows 8.1 (マイクロソフト)	196
9	OS	Microsoft Windows RT 8.1 (マイクロソフト)	192
10	OS	Microsoft Windows Server 2008 (マイクロソフト)	167
11	OS	Microsoft Windows 7 (マイクロソフト)	166
12	開発環境	GitLab (GitLab.org)	139
13	ブラウザ	Google Chrome (Google)	133
14	ナレッジベースソフトウェア	PHPKB (Chadha Software Technologies)	119
15	統合業務パッケージ	Oracle E-Business Suite (オラクル)	97
16	OS	iOS (アップル)	83
16	OS	Debian GNU/Linux (Debian)	83
18	OS	Apple Mac OS X (アップル)	75
19	ブラウザ	Mozilla Firefox (Mozilla Foundation)	71
20	PDF 閲覧・編集	Foxit PhantomPDF (Foxit Software Inc)	69

^(*) 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 2020 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。

本四半期は、上位 20 件の内 15 位と 17 位以外の 18 件が、脆弱性対策情報ポータルサイト JVN で公表した脆弱性対策情報でした。JVN から公表した情報の中には、「情報セキュリティ早期警戒パートナーシップ⁽⁹⁾」に基づいて公表された情報も含まれています。これらの情報は注目度が高く、ニュースサイト等でも取り上げられたことからアクセス数が増加したものと考えられます。

表 3-1. JVN iPedia の脆弱性対策情報へのアクセス 上位 20 件 [2020 年 4 月～2020 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-2020-000021	ヤマハ製の複数のネットワーク機器におけるサービス運用妨害 (DoS) の脆弱性	7.1	5.9	2020/3/31	7,940
2	JVNDB-2020-000022	EasyBlocks IPv6 における複数の脆弱性	4.0	4.2	2020/4/8	7,094
3	JVNDB-2020-000024	Joomla! 用プラグイン「AcyMailing」における任意のファイルをアップロードされる脆弱性	5.0	5.3	2020/4/7	6,761
4	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	6,541
5	JVNDB-2020-000025	東芝デバイス&ストレージ株式会社製品によって登録される Windows サービスの実行ファイルパスが引用符で囲まれていない脆弱性	4.6	8.4	2020/4/20	6,148
6	JVNDB-2020-002958	三菱電機製 MELSEC シリーズの MELSOFT 交信ポートにおけるリソース枯渇の脆弱性	5.0	5.3	2020/3/31	5,901
7	JVNDB-2020-000026	複数のシャープ製 Android 端末における情報漏えいの脆弱性	2.6	3.3	2020/4/23	5,575
8	JVNDB-2020-000907	WL-Enq (WEB アンケート) における OS コマンドインジェクションの脆弱性	6.8	8.8	2020/3/24	5,282
9	JVNDB-2020-000908	掲示板 積木における OS コマンドインジェクションの脆弱性	7.5	7.3	2020/3/24	5,163
10	JVNDB-2020-000906	WL-Enq (WEB アンケート) 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	2020/3/24	5,070
11	JVNDB-2020-000027	サイボウズ Garoon における複数の脆弱性	5.0	5.3	2020/4/27	4,910
12	JVNDB-2020-000029	PALLET CONTROL において任意のコードが実行可能な脆弱性	6.8	7.8	2020/5/11	4,814
13	JVNDB-2020-000900	メールフォームにおけるクロスサイトスクリプティングの脆弱性	5.0	6.1	2020/3/24	4,767
14	JVNDB-2020-000901	メールフォームにおいて任意の PHP コードが実行可能な脆弱性	7.5	7.3	2020/3/24	4,719

⁽⁹⁾ 情報セキュリティ早期警戒パートナーシップ

https://www.ipa.go.jp/security/ciadr/partnership_guide.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-2020-005570	Nintendo 64 デバイス用 Morita Shogi 64 における境界外書き込みに関する脆弱性	7.5	9.8	2020/6/17	4,711
16	JVNDB-2020-000028	Sales Force Assistant 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	2020/4/28	4,636
17	JVNDB-2020-003896	Hitachi Infrastructure Analytics Advisor および Hitachi Ops Center Analyzer におけるディレトリパーミッションの脆弱性	なし	なし	2020/4/28	4,595
18	JVNDB-2019-000056	パナソニック Video Insight VMS における SQL インジェクションの脆弱性	6.5	8.8	2019/9/2	4,534
19	JVNDB-2020-000030	Movable Type における複数の脆弱性	6.5	6.3	2020/5/13	4,435
20	JVNDB-2020-000902	私本管理 Plus GOOUT における複数の脆弱性	7.5	7.3	2020/3/24	4,412

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 [2020 年 4 月～2020 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-2020-003896	Hitachi Infrastructure Analytics Advisor および Hitachi Ops Center Analyzer におけるディレトリパーミッションの脆弱性	なし	なし	2020/4/28	4,595
2	JVNDB-2018-010027	JP1/Operations Analytics におけるディレトリパーミッションの問題	3.5	4.9	2018/12/4	4,252
3	JVNDB-2020-002278	JP1/Performance Management - Manager [Web Console] におけるクロスサイトスクリプティングの脆弱性	なし	なし	2020/3/11	4,179
4	JVNDB-2020-002219	Hitachi Infrastructure Analytics Advisor および Hitachi Ops Center 製品における複数の脆弱性	なし	なし	2020/3/9	4,120
5	JVNDB-2020-002220	Hitachi Ops Center Common Services における LDAPS の証明書検証に関する脆弱性	なし	なし	2020/3/9	4,104

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

2018 年以前の公開	2019 年の公開	2020 年の公開
-------------	-----------	-----------