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 3 四半期（7 月～9 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 7 月 1 日から 2020 年 9 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。

独立行政法人情報処理推進機構　セキュリティセンター

2020 年 10 月 21 日

目次

1. 2020 年第 3 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 123,965 件～

2020 年第 3 四半期（2020 年 7 月 1 日から 9 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 123,965 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 2,188 件になりました。

表 1-1. 2020 年第 3 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	4 件	243 件
	JVN	232 件	9,524 件
	NVD	2,846 件	114,198 件
	計	3,082 件	123,965 件
英語版	国内製品開発者	4 件	241 件
	JVN	25 件	1,947 件
	計	29 件	2,188 件

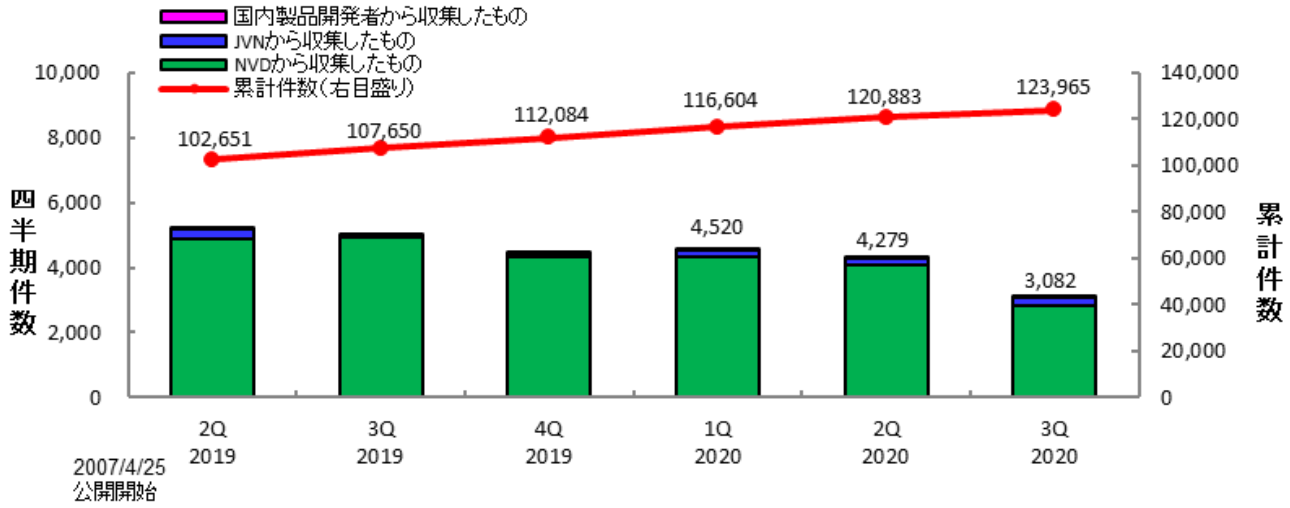

図 1-1. JVN iPedia の登録件数の四半期別推移

(*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 3 四半期（7 月～9 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 303 件、CWE-269（不適切な権限管理）が 268 件、CWE-200（情報漏えい）が 212 件、CWE-20（不適切な入力確認）が 176 件、CWE-119（バッファエラー）が 166 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**[*4]」、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**[*5]」や「**IPA セキュア・プログラミング講座**[*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。

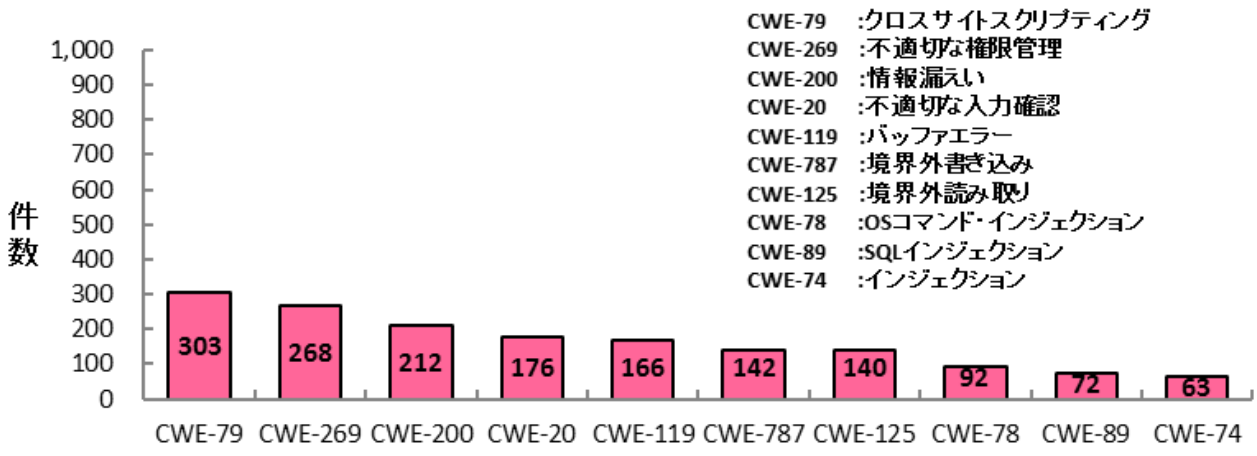

図 2-1. 2020 年第 3 四半期に登録された脆弱性の種類別件数

[*4] 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/vuln/report/notice/guideforvendor.html

[*5] IPA：「安全なウェブサイトの作り方」
https://www.ipa.go.jp/security/vuln/websecurity.html

[*6] IPA：「IPA セキュア・プログラミング講座」
https://www.ipa.go.jp/security/awareness/vendor/programming/

[*7] 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 24.0%、レベルⅡが 61.7%、レベルⅠが 14.3%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 85.7%を占めています。

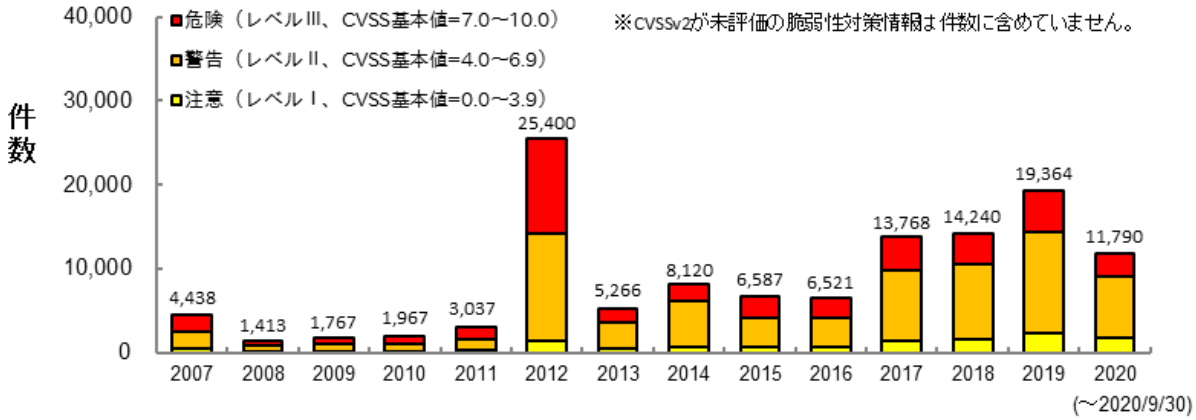

図 2-2. 脆弱性の深刻度別件数(CVSSv2)

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 15.5%、「重要」が 42.1%、「警告」が 40.4%、「注意」が 2.0%となっています。

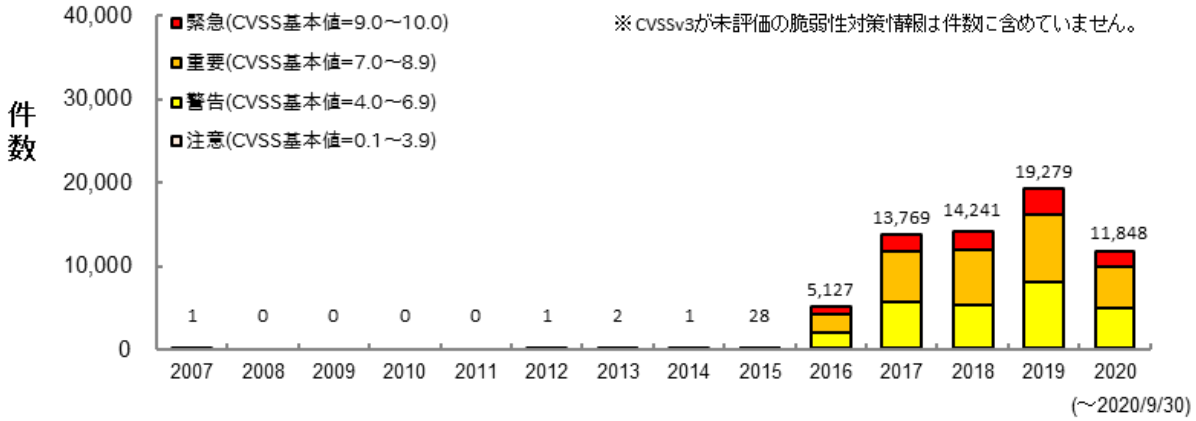

図 2-3. 脆弱性の深刻度別件数(CVSSv3)

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 [*8] で公開しています。

[*8] 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。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%（8,126 件／全 11,879 件）を占めています。

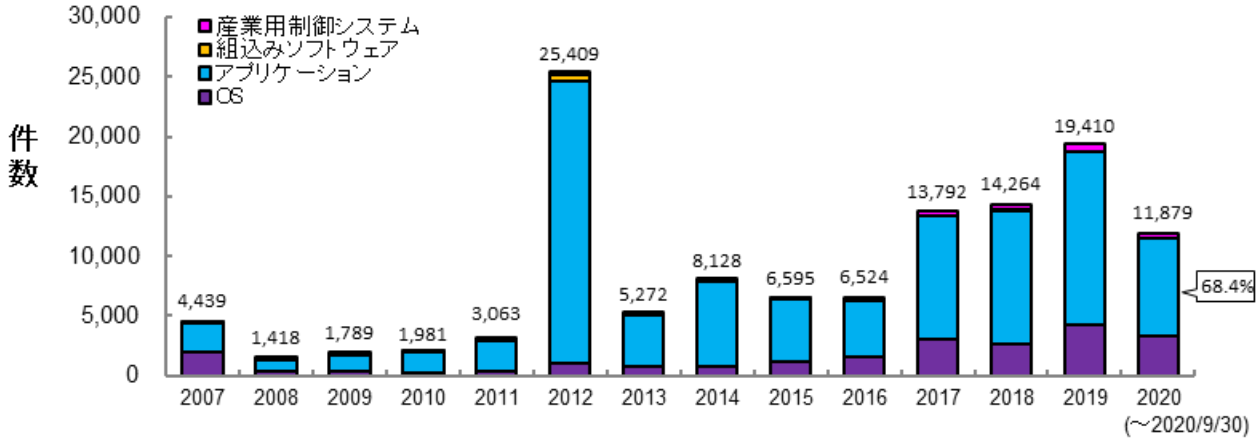

図 2-4. 脆弱性対策情報を公表した製品の種類別件数の公開年別推移

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 2,758 件を登録しています。

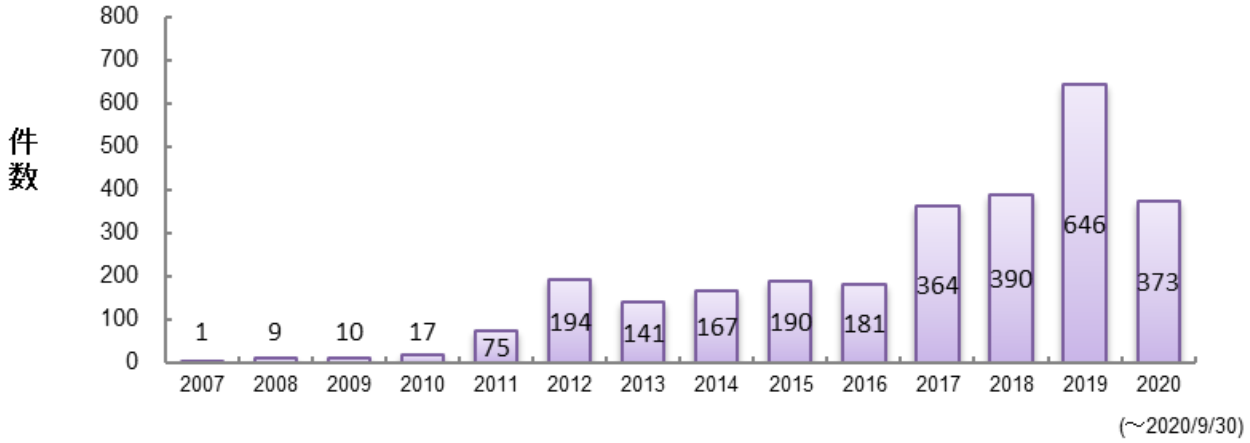

図 2-5. JVN iPedia 登録件数（産業用制御システムのみ抽出）

2-4. 脆弱性対策情報の製品別登録状況

表 2-1 は 2020 年第 3 四半期（7 月～9 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。

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 [2020 年 7 月～2020 年 9 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)	261
2	OS	Microsoft Windows Server (マイクロソフト)	243
3	OS	Microsoft Windows Server 2019 (マイクロソフト)	224
4	OS	Microsoft Windows Server 2016 (マイクロソフト)	187
5	OS	Android (Google)	140
6	OS	Microsoft Windows 8.1 (マイクロソフト)	129
6	OS	Microsoft Windows RT 8.1 (マイクロソフト)	129
8	OS	Microsoft Windows Server 2012 (マイクロソフト)	126
9	OS	Microsoft Windows 7 (マイクロソフト)	113
10	OS	Microsoft Windows Server 2008 (マイクロソフト)	108
11	PDF 閲覧・編集	Adobe Acrobat (アドビシステムズ)	50
11	PDF 閲覧・編集	Adobe Acrobat DC (アドビシステムズ)	50
11	PDF 閲覧	Adobe Acrobat Reader DC (アドビシステムズ)	50
14	ファームウェア	Qualcomm component (クアルコム)	49
15	OS	iOS (アップル)	42
15	OS	iPadOS (アップル)	42
17	OS	Apple Mac OS X (アップル)	41
18	サーバ管理ソフトウェア	CentOS Web Panel (CentOS Web Panel)	39
19	ファイル・情報共有ソフトウェア	Microsoft SharePoint Server (マイクロソフト)	35
20	ファイル・情報共有ソフトウェア	Microsoft SharePoint Enterprise Server (マイクロソフト)	34

[(*9)] IPA：「脆弱性対策の効果的な進め方（実践編）」
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 3 四半期（7 月～9 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。本四半期の 1 位は 2014 年に公開した phpMyAdmin に関する脆弱性対策情報でした。なお、これは特定の組織から機械的と思われる多くのアクセスがあったためです。また、上位 20 件のうち、6 件（8 位、12 位、13 位、15 位、18 位、19 位）が日立製品に関する脆弱性対策情報でした。こうした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 [2020 年 7 月～2020 年 9 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-2014-003893	phpMyAdmin 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	2014/8/25	7,058
2	JVNDB-2020-000043	Android アプリ「メルカリ」 (日本版) において Java オブジェクトの任意のメソッドが実行可能な脆弱性	5.1	5.0	2020/7/8	6,778
3	JVNDB-2020-000046	WordPress 用プラグイン Social Sharing Plugin 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	2020/7/22	6,741
4	JVNDB-2020-006469	三菱電機製 GOT2000 シリーズの TCP/IP 機能における複数の脆弱性	なし	9.8	2020/7/9	6,651
5	JVNDB-2020-000049	トヨタ自動車製 Global TechStream (GTS) におけるバッファオーバーフローの脆弱性	4.4	4.1	2020/7/29	6,613
6	JVNDB-2020-000052	SKYSEA Client View に権限昇格の脆弱性	6.8	7.8	2020/8/3	6,594
7	JVNDB-2020-000045	SHIRASAGI におけるオープンリダイレクトの脆弱性	4.3	4.7	2020/7/9	6,476
8	JVNDB-2020-006586	Hitachi Ops Center Analyzer viewpoint における Server Side Request Forgery の脆弱性	なし	なし	2020/7/13	6,072
9	JVNDB-2020-000051	複数の PHP 工房製品における複数の脆弱性	4.0	4.8	2020/7/31	5,910
10	JVNDB-2020-000050	Fanuc i Series CNC におけるサービス運用妨害 (DoS) の脆弱性	3.3	4.3	2020/7/31	5,904
11	JVNDB-2020-000047	JavaFX の WebEngine コンポーネントに任意の Java メソッド実行が可能になる脆弱性	6.8	8.8	2020/7/28	5,833
12	JVNDB-2020-006617	Hitachi Infrastructure Analytics Advisor および 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	なし	なし	2020/7/14	5,741
13	JVNDB-2020-006031	Hitachi Device Manager における DoS 脆弱性	なし	なし	2020/6/29	5,637
14	JVNDB-2020-000040	Chrome 拡張機能 e-Tax 受付システム AP において任意のコマンドが実行可能な脆弱性	5.1	5.0	2020/6/24	5,359
15	JVNDB-2020-007128	HiRDB における DoS 脆弱性	なし	なし	2020/8/3	5,239
16	JVNDB-2020-000042	サイボウズ Garoon に複数の脆弱性	5.5	8.5	2020/6/29	5,235

順位	ID	タイトル	CVSSv2 基本値	CVSSv3 基本値	公開日	アクセス数
17	JVNDB-2020-005854	三菱電機製 MELSEC iQ-R、iQ-F、Q、L、FX シリーズの CPU ユニットと GX Works3 および GX Works2 間の通信が平文で行われている脆弱性	なし	10.0	2020/6/24	5,126
18	JVNDB-2020-007127	Hitachi Command Suite 製品、Hitachi Automation Director、Hitachi Configuration Manager、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	2020/8/3	5,105
19	JVNDB-2020-005743	Cosminexus HTTP Server における脆弱性	なし	なし	2020/6/22	5,063
20	JVNDB-2020-000057	スマートフォンアプリ「ニトリアプリ」におけるアクセス制限不備の脆弱性	4.3	4.3	2020/8/26	5,019

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 7 月～2020 年 9 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-2020-006586	Hitachi Ops Center Analyzer viewpoint における Server Side Request Forgery の脆弱性	なし	なし	2020/7/13	6,072
2	JVNDB-2020-006617	Hitachi Infrastructure Analytics Advisor および 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	なし	なし	2020/7/14	5,741
3	JVNDB-2020-006031	Hitachi Device Manager における DoS 脆弱性	なし	なし	2020/6/29	5,637
4	JVNDB-2020-007128	HiRDB における DoS 脆弱性	なし	なし	2020/8/3	5,239
5	JVNDB-2020-007127	Hitachi Command Suite 製品、Hitachi Automation Director、Hitachi Configuration Manager、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	2020/8/3	5,105

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