

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 [2018 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、2018 年 7 月 1 日から 2018 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。

目次

1. 2018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	- 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. 2018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 89,114 件～

2018年第3四半期(2018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、**脆弱性対策情報の登録件数の累計は、89,114 件でした**(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1,955件になりました。

表 1-1. 2018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	3件	204件
	JVN	106件	8,205件
	NVD	3,725件	80,705件
	計	3,834件	89,114件
英語版	国内製品開発者	3件	204件
	JVN	30件	1,751件
	計	33件	1,955件

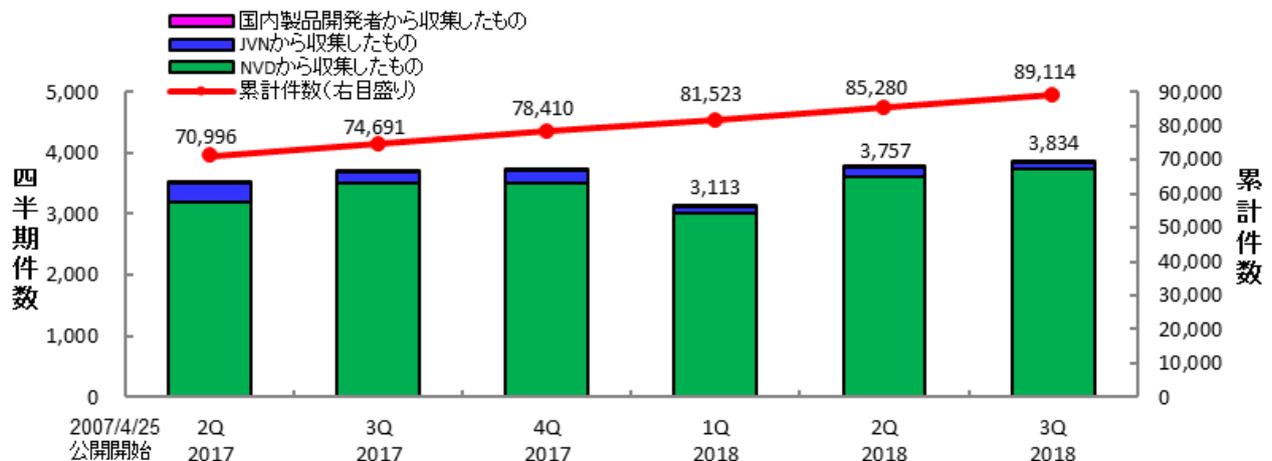


図1-1. JVN iPediaの登録件数の四半期別推移

⁽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、2018 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-190(整数オーバーフローまたはラップアラウンド)が 340 件、CWE-284（不適切なアクセス制御）が 286 件、CWE-119（バッファエラー）が 282 件、CWE-79（クロスサイト・スクリプティング）が 281 件、CWE-200（情報漏えい）が 258 件でした。

最も件数の多かった CWE-190（整数オーバーフローまたはラップアラウンド）は、悪用されバッファオーバーフローが発生すると、メモリ上の本来アクセスできないデータを上書きされてしまい、プログラムを異常終了されたり、外部から任意のコードを実行されたりなどの被害が発生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。なお、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。

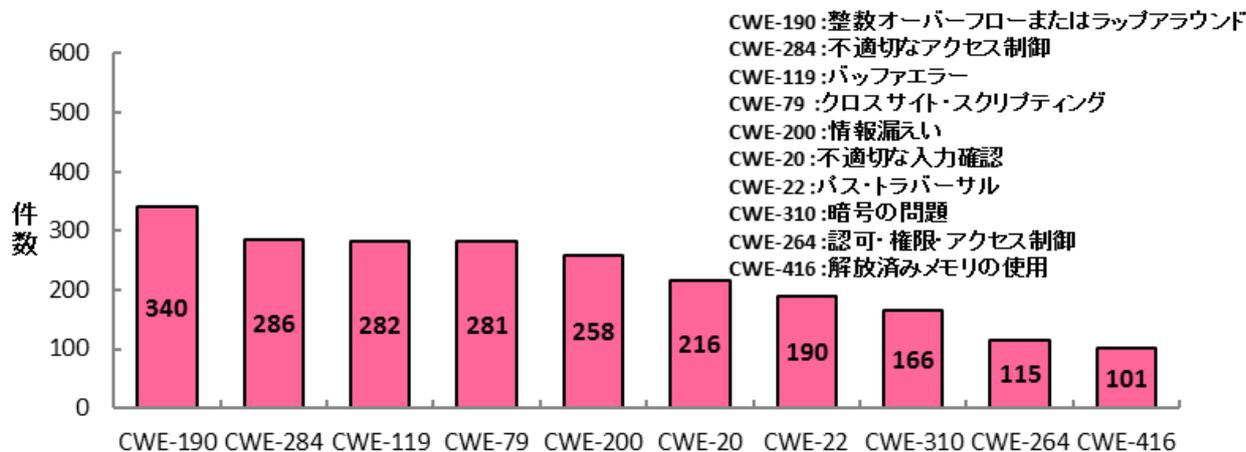


図2-1. 2018年第3四半期に登録された脆弱性の種類別件数

⁽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。

2018 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 27.1%、レベル II が 62.7%、レベル I が 10.2% 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 89.8% を占めています。

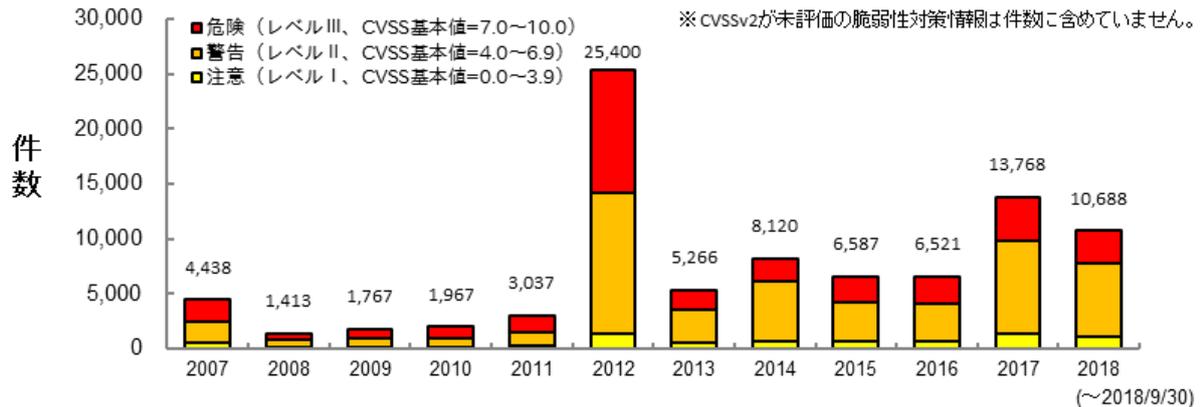


図2-2. 脆弱性の深刻度別件数(CVSSv2)

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。

2018 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 16.7%、「重要」が 47.0%、「警告」が 35.1%、「注意」が 1.2% となっています。

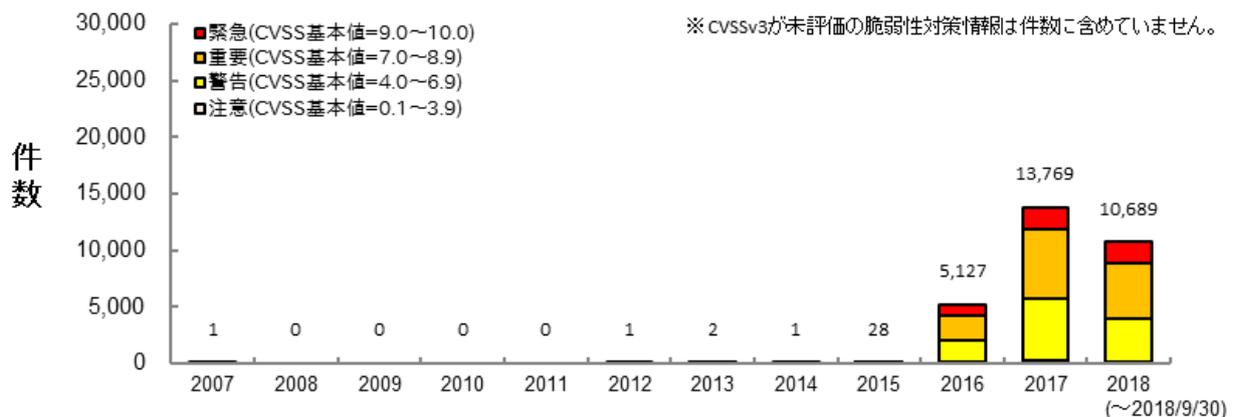


図2-3. 脆弱性の深刻度別件数(CVSSv3)

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。2018 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、2018 年の件数全件の約 78.0% (8,353 件 / 全 10,704 件) を占めています。

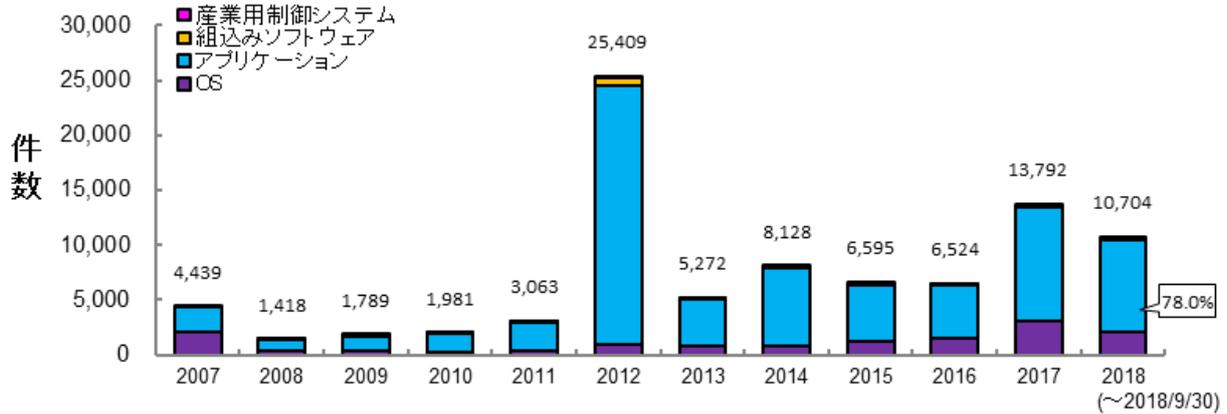


図2-4. 脆弱性対策情報を公表した製品の種別別件数の公開年別推移

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 1,539 件を登録しています (図 2-5)。

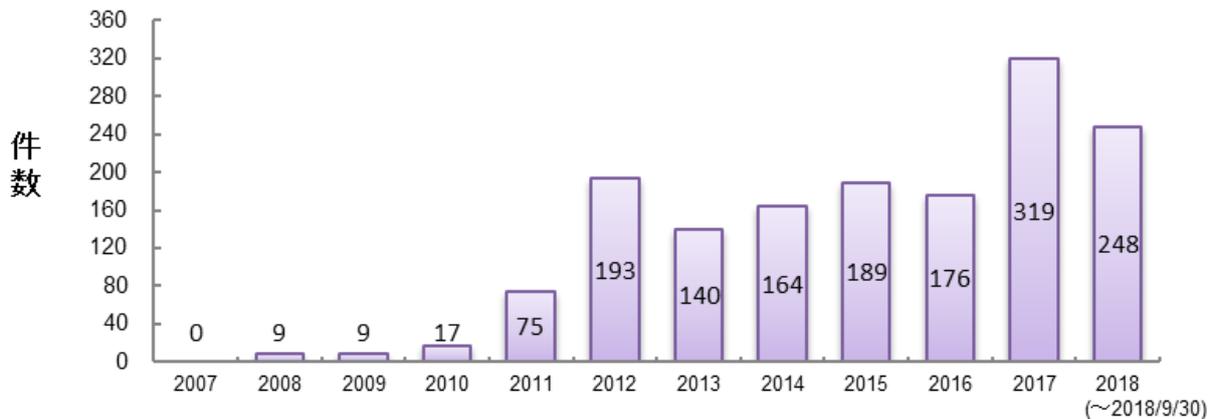


図2-5. JVN iPedia 登録件数(産業用制御システムのみ抽出)

2-4. 脆弱性対策情報の製品別登録状況

表 2-1 は 2018 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の上位 20 件を示したものです。

今四半期において最も登録件数が多かったのは、Mozilla Foundation が提供する Mozilla Firefox でした。さらに同社製品である Mozilla Thunderbird と Mozilla Firefox ESR もそれぞれ 8 位、10 位にランクインしています。また、2 位以降は Debian の LinuxOS をはじめ、レッドハットやマイクロソフトなどが提供する OS 製品関連の脆弱性対策情報が多数登録されました。

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 [2018 年 7 月～2018 年 9 月]

順位	カテゴリ	製品名（ベンダ名）	登録件数
1	ブラウザ	Mozilla Firefox (Mozilla Foundation)	301
2	OS	Debian GNU/Linux (Debian)	212
3	PDF 閲覧	Adobe Acrobat Reader DC (アドビシステムズ)	155
3	PDF 閲覧・編集	Adobe Acrobat (アドビシステムズ)	155
3	PDF 閲覧・編集	Adobe Acrobat DC (アドビシステムズ)	155
6	OS	Red Hat Enterprise Linux Server (レッドハット)	153
7	OS	Red Hat Enterprise Linux Workstation (レッドハット)	152
8	OS	Red Hat Enterprise Linux Desktop (レッドハット)	150
8	メールソフト	Mozilla Thunderbird (Mozilla Foundation)	150
10	ブラウザ	Mozilla Firefox ESR (Mozilla Foundation)	149
11	OS	Ubuntu (Canonical)	144
12	OS	Red Hat Enterprise Linux (レッドハット)	89
13	OS	Android (Google)	87
14	品質管理ソフト	Rational Quality Manager (IBM)	48
15	開発管理ソフト	Rational Collaborative Lifecycle Management (IBM)	40
15	OS	Microsoft Windows 10 (マイクロソフト)	40
17	OS	Microsoft Windows Server (マイクロソフト)	38
17	OS	Linux Kernel (Kernel.org)	38
19	OS	iOS (アップル)	37
20	OS	Microsoft Windows Server 2016 (マイクロソフト)	34

^(*) 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 2018 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。

今四半期の上位 20 件は全て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^(*)」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、ニュースサイトやブログ記事など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 [2018 年 7 月～2018 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-2018-000072	複数のロジクール製ソフトウェア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	2018/7/6	5,875
2	JVNDB-2018-000069	サイボウズ Garoon における SQL インジェクションの脆弱性	6.5	6.3	2018/7/2	5,795
3	JVNDB-2018-000075	Aterm WG1200HP における複数の OS コマンドインジェクションの脆弱性	5.2	6.8	2018/7/12	5,617
4	JVNDB-2018-000071	Android アプリ「DHC オンラインショップ」における SSL サーバ証明書の検証不備の脆弱性	4.0	4.8	2018/7/6	5,596
5	JVNDB-2018-000068	コルソス CSDX および CSDJ シリーズ製品における複数の脆弱性	6.5	8.8	2018/7/2	5,585
6	JVNDB-2018-000070	Glary Utilities 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	2018/7/3	5,570
7	JVNDB-2018-000079	Explzh におけるディレクトリトラバーサル脆弱性	4.3	3.3	2018/7/13	5,473
8	JVNDB-2018-000077	Aterm HC100RC における複数の脆弱性	5.2	6.8	2018/7/12	5,412
9	JVNDB-2018-000076	Aterm W300P における複数の脆弱性	5.2	6.8	2018/7/12	5,238
10	JVNDB-2018-000080	Movable Type 用プラグイン MTAppjQuery において任意の PHP コードが実行可能な脆弱性	7.5	7.3	2018/7/18	5,166
11	JVNDB-2018-000081	日医標準レセプトソフトにおける複数の脆弱性	5.2	5.5	2018/7/18	5,164
12	JVNDB-2018-000067	Mailman 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	2018/6/28	5,139
13	JVNDB-2018-000090	アタッシェケースにおける複数のディレクトリトラバーサル脆弱性	4.3	3.3	2018/8/6	5,092
14	JVNDB-2018-000078	WordPress 用プラグイン FV Flowplayer Video Player 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	2018/7/17	5,060

(*) 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-2018-000083	キヤノン IT ソリューションズ株式会社製の複数製品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	2018/7/24	4,981
16	JVNDB-2018-000066	めも CGI におけるディレクトリトラバーサル脆弱性	5.0	5.8	2018/6/27	4,980
17	JVNDB-2018-000035	EC-CUBE におけるセッション固定脆弱性	5.8	4.2	2018/4/17	4,826
18	JVNDB-2018-000074	弥生 17 シリーズの複数の製品における DLL 読み込みに関する脆弱性	6.8	7.8	2018/7/20	4,817
19	JVNDB-2018-000084	Android 版 LINE MUSIC における SSL サーバ証明書の検証不備脆弱性	4.0	4.8	2018/7/26	4,807
20	JVNDB-2018-000082	WL-330NUL 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	2018/7/20	4,727

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 [2018 年 7 月～2018 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-2018-003030	Hitachi Infrastructure Analytics Advisor におけるアクセス制御に関する脆弱性	7.5	7.3	2018/5/10	4,224
2	JVNDB-2017-004687	富士通 Interstage List Works におけるクロスサイトスクリプティング脆弱性	4.3	6.1	2017/7/5	3,928
3	JVNDB-2018-001389	Hitachi Device Manager における XXE 脆弱性	7.8	7.4	2018/2/14	3,919
4	JVNDB-2018-002257	JP1/ServerConductor/Deployment Manager および Hitachi Compute Systems Manager におけるサービス運用妨害 (DoS) の脆弱性	7.8	7.5	2018/4/4	3,914
5	JVNDB-2017-010236	富士通 NetCOBOL におけるクロスサイトスクリプティング脆弱性	3.5	4.8	2017/12/8	3,871

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

2016 年以前の公開	2017 年の公開	2018 年の公開
-------------	-----------	-----------