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 4 四半期（10 月～12 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 10 月 1 日から 2019 年 12 月 31 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 1 月 22 日

目次

1. 2019 年第 4 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 -
1-2.【注目情報 1】Adobe Flash Player の脆弱性について ..... - 3 -
1-3.【注目情報 2】リモートデスクトップサービスに関連する脆弱性について ..... - 3 -
2. JVN iPedia の登録データ分類 ..... - 6 -
2-1. 脆弱性の種類別件数 ..... - 9 -
2-2. 脆弱性に関する深刻度別割合 ..... - 10 -
2-3. 脆弱性対策情報を公開した製品の種類別件数 ..... - 12 -
2-4. 脆弱性対策情報の製品別登録状況 ..... - 13 -
3. 脆弱性対策情報の活用状況 ..... - 14 -

1. 2019 年第 4 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 112,084 件～

2019 年第 4 四半期（2019 年 10 月 1 日から 12 月 31 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 112,084 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 2,093 件になりました。

表 1-1. 2019 年第 4 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	8 件	226 件
	JVN	113 件	8,875 件
	NVD	4,313 件	102,983 件
	計	4,434 件	112,084 件
英語版	国内製品開発者	8 件	226 件
	JVN	19 件	1,867 件
	計	27 件	2,093 件

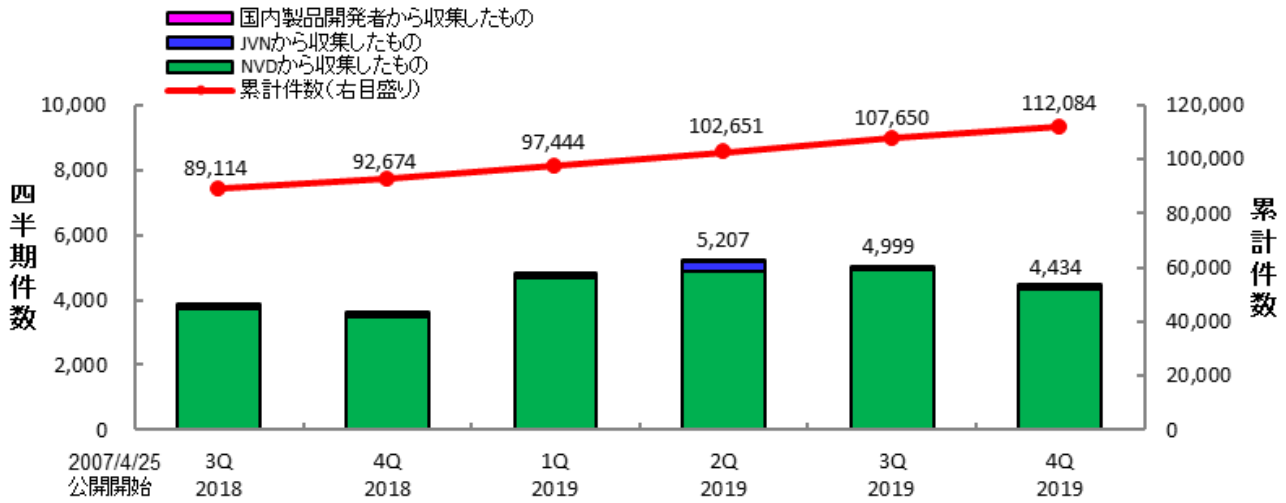

図 1-1. JVN iPedia の登録件数の四半期別推移

(*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

1-2. 【注目情報 1】Adobe Flash Player の脆弱性について
～2019 年は深刻度レベルが高い脆弱性対策情報を 10 件登録、サポート終了までに代替製品への移行検討を～

Adobe Flash Player の開発元であるアドビシステムズ社より、2020 年末に Adobe Flash Player の更新と配布を停止し、サポートを終了することが告知[*4]されています。

図 1-2 は、2017 年～2019 年に JVN iPedia へ登録された、Adobe Flash Player に関する脆弱性対策情報の深刻度別割合です。過去 3 年間に登録された脆弱性の全てが、脆弱性の深刻度が最も高い「危険」（CVSS 基本値=7.0～10.0）または、次に高い「警告」（CVSS 基本値=4.0～6.9）に分類されており、危険度が高い脆弱性が占めていることが分かります。

また、登録件数については、2017 年に 70 件、2018 年に 25 件、2019 年に 10 件と減少傾向となっています。しかし、「危険」に分類される深刻度の割合で見てみると、2017 年は 90%、2018 年は 44%、2019 年は 50%と変動しており、2017 年が突出しているものの、2019 年も依然として危険度が高い脆弱性の占める割合が多くなっています。今後も登録される件数の減少が予想されますが、引き続き深刻度が高い脆弱性対策情報が公開されるおそれがあります。

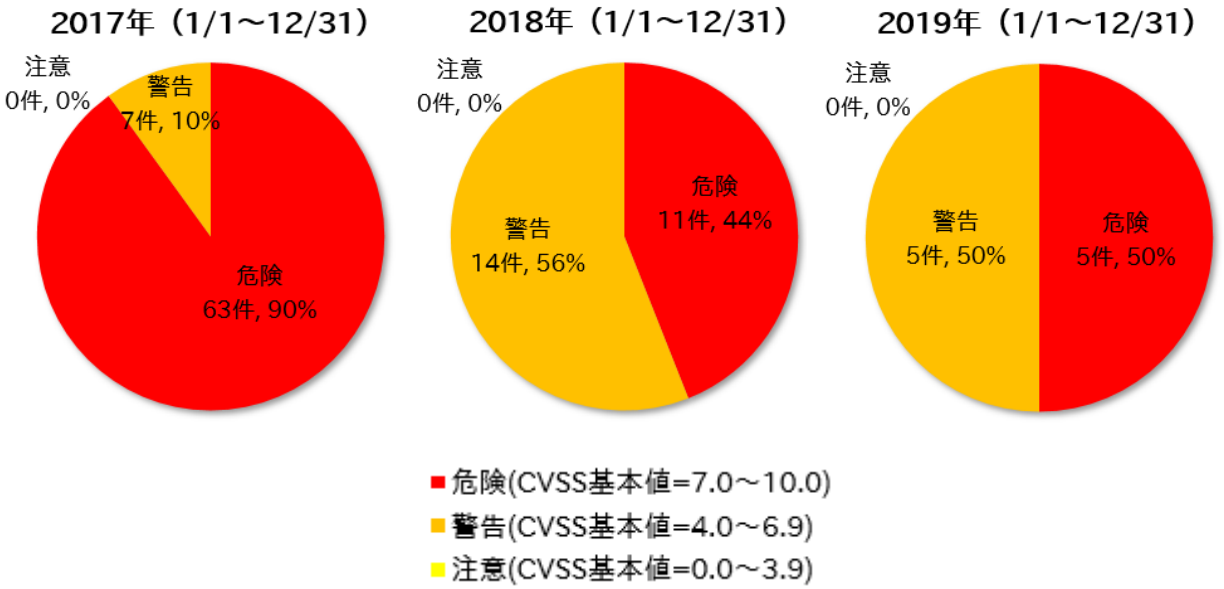

図 1-2.　2017 年～2019 年に登録された Adobe Flash Player の深刻度別割合（CVSSv2）

一般的にサポート終了後は新たな脆弱性が発見された場合でも製品ベンダによる修正が行われないため、サポートが終了した製品を継続利用していると、脆弱性を悪用した攻撃により被害を受けるリスクが増大します。Adobe Flash Player を利用するコンテンツを公開している組織においては HTML5 等の代替手段へ移行する等の対応をとることを推奨します。また、Adobe Flash Player を利用するコンテンツの利用者に対して移行方法等の案内を行ってください。移行および利用者への案内は 2020 年末のサポート終了までに対応することが求められます。

[*4] Flash & The Future of Interactive Content – Adobe
https://theblog.adobe.com/adobe-flash-update/

なお、IPA でも、現在 Adobe Flash Player を利用したサイバーセキュリティ注意喚起サービス「icat（Flash 版）」を運用していますが、サポートが終了する 2020 年末より前にサービスの提供を終了し、Adobe Flash Player を利用しない「icat for JSON」に一本化する予定です[*5]。「icat（Flash 版）」の利用者は、サービス紹介ページでも案内しているとおり、「icat for JSON」への移行をお願いいたします。

[*5] サイバーセキュリティ注意喚起サービス「icat for JSON」
https://www.ipa.go.jp/security/vuln/icat.html

1-3. 【注目情報 2】リモートデスクトップサービスに関連する脆弱性について
～リモートデスクトップサービスに関連する脆弱性は 深刻度が最も高い「危険」が 63%を占める～

2019 年 5 月、「BlueKeep」と呼ばれる Windows のリモートデスクトップサービスの脆弱性（CVE-2019-0708）がマイクロソフト社より公開[*6]されました。また、本脆弱性は、認証されていない遠隔の攻撃者が標的となるシステム側の操作を介さずリモートデスクトッププロトコル（RDP）経由で攻撃可能といった特性があることから、2017 年に猛威を振るった「WannaCry」のような自己増殖機能を有しネットワーク上に感染を拡大するワームに感染するおそれがありました。それを受け、マイクロソフト社は、当該脆弱性について注意を促す情報を発信し、サポートが終了している Windows XP と Windows Server 2003 のパッチを提供する等の異例の措置を行いました[*7]。また、2019 年 11 月には本脆弱性を悪用して仮想通貨の採掘を行わせる攻撃が確認されており、今後も注意が必要です[*8]。

2019 年には、「BlueKeep」以外にも、リモートデスクトップサービスやその接続に使われる RDP に関連する脆弱性がマイクロソフト社より公開されています。図 1-3 は 2019 年（1/1～12/31）に JVN iPedia へ登録されたリモートデスクトップサービスや RDP に関連すると思われる脆弱性対策情報の深刻度別割合です。また、表 1-2 はその一覧表です。公開された 19 件の脆弱性対策情報の内 12 件が、深刻度が最も高い「危険」（CVSS 基本値=7.0～10.0）に分類されており、全体の 63%を占めています。また、残りの 7 件は深刻度が次に高い「警告」（CVSS 基本値=4.0～6.9）に分類されており、「注意」（CVSS 基本値=0.0～3.9）は 0 件となりました。なお、「BlueKeep」（JVNDB-2019-003551）は、CVSS 基本値が最大の 10.0 となっており、「危険」に含まれます。

2019 年において、リモートデスクトップサービスや RDP に関連する脆弱性は、CVSS 基本値 10.0 を含む危険度が高い脆弱性が登録されている傾向が見えます。

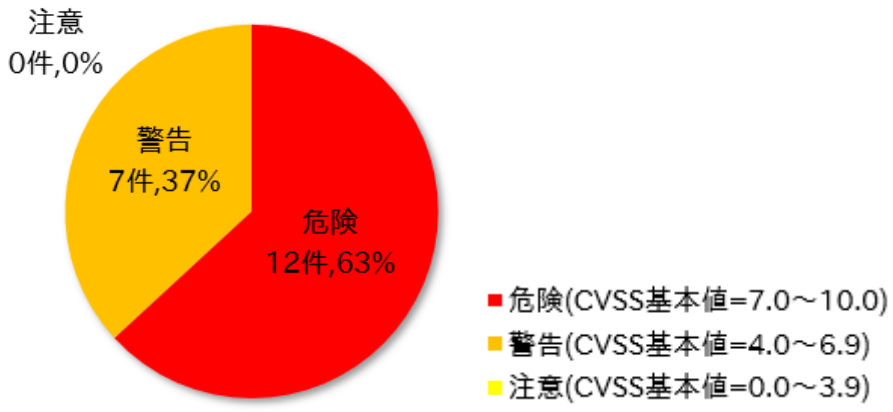

図 1-3.　2019 年（1/1～12/31）に登録されたリモートデスクトップサービスおよび RDP に関連する脆弱性対策情報の深刻度別割合（CVSSv2）

[*6] CVE-2019-0708 | リモート デスクトップ サービスのリモートでコードが実行される脆弱性
https://portal.msrc.microsoft.com/ja-jp/security-guidance/advisory/CVE-2019-0708
[*7] 新たな「WannaCryptor」になるかもしれない脆弱性「BlueKeep」とは？
https://ascii.jp/elem/000/001/890/1890827/
[*8] マイクロソフト、「BlueKeep」脆弱性を悪用するさらなる攻撃の可能性について注意喚起
https://japan.zdnet.com/article/35145189/

表 1-2.　2019 年（1/1～12/31）に登録されたリモートデスクトップサービスおよび RDP に関連する脆弱性対策情報

No	ID	タイトル	CVSSv2 基本値
1	JVNDB-2019-012975	複数の Microsoft Windows 製品のリモートデスクトッププロトコルにおけるサービス運用妨害 (DoS) の脆弱性	5.0
2	JVNDB-2019-012905	Microsoft Windows XP における情報を公開される脆弱性	5.0
3	JVNDB-2019-010491	複数の Microsoft Windows 製品の Windows リモートデスクトップクライアントにおけるリモートでコードを実行される脆弱性	9.3
4	JVNDB-2019-010476	複数の Microsoft Windows 製品のリモートデスクトッププロトコルにおけるサービス運用妨害 (DoS) の脆弱性	7.8
5	JVNDB-2019-009253	複数の Microsoft Windows 製品の Windows リモートデスクトップクライアントにおけるリモートでコードを実行される脆弱性	9.3
6	JVNDB-2019-009252	複数の Microsoft Windows 製品の Windows リモートデスクトップクライアントにおけるリモートでコードを実行される脆弱性	9.3
7	JVNDB-2019-009209	複数の Microsoft Windows 製品の Windows リモートデスクトップクライアントにおけるリモートでコードを実行される脆弱性	9.3
8	JVNDB-2019-009208	複数の Microsoft Windows 製品の Windows リモートデスクトップクライアントにおけるリモートでコードを実行される脆弱性	9.3
9	JVNDB-2019-008030	複数の Microsoft Windows 製品 における情報を公開される脆弱性	5.0
10	JVNDB-2019-008029	複数の Microsoft Windows 製品 における情報を公開される脆弱性	5.0
11	JVNDB-2019-008028	複数の Microsoft Windows 製品のリモートデスクトッププロトコルにおけるサービス運用妨害 (DoS) の脆弱性	5.0
12	JVNDB-2019-007743	複数の Microsoft Windows 製品のリモートデスクトップサービスにおけるリモートでコードを実行される脆弱性	10.0
13	JVNDB-2019-007742	複数の Microsoft Windows 製品のリモートデスクトップサービスにおけるリモートでコードを実行される脆弱性	9.3
14	JVNDB-2019-007739	複数の Microsoft Windows 製品のリモートデスクトップサービスにおけるリモートでコードを実行される脆弱性	10.0
15	JVNDB-2019-007738	複数の Microsoft Windows 製品のリモートデスクトップサービスにおけるリモートでコードを実行される脆弱性	10.0
16	JVNDB-2019-006521	複数の Microsoft Windows 製品のリモートデスクトップサービスにおけるリモートでコードを実行される脆弱性	8.5
17	JVNDB-2019-006364	複数の Microsoft Windows 製品 における情報を公開される脆弱性	4.0
18	JVNDB-2019-004672	Microsoft Windows リモートデスクトップのネットワークレベル認証に Windows ロックスクリーンをバイパスされる問題	4.6
19	JVNDB-2019-003551	複数の Microsoft Windows 製品のリモートデスクトップサービスにおけるリモートでコードを実行される脆弱性	10.0

組織に所属されている方は、業務を行う中で別の端末に接続するためにリモートデスクトップサービスを利用するケースがあります。また、リモートデスクトップサービスは Windows 標準で搭載されている機能であるため、端末を共同で利用している場合、意図せず有効になっていることもあります。

リモートデスクトップサービスは便利な機能ではありますが、悪用されてしまった場合、大きな被害につながるおそれがあります。マイクロソフト社よりセキュリティパッチが公開された場合、早急な適用を推奨します。

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 4 四半期（10 月～12 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 535 件、CWE-20（不適切な入力確認）が 516 件、CWE-200（情報漏えい）が 302 件、CWE-125（境界外読み取り）が 226 件、CWE-787（境界外書き込み）が 187 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[*9]」や「IPA セキュア・プログラミング講座[*10]」、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[*11]」などを公開しています。

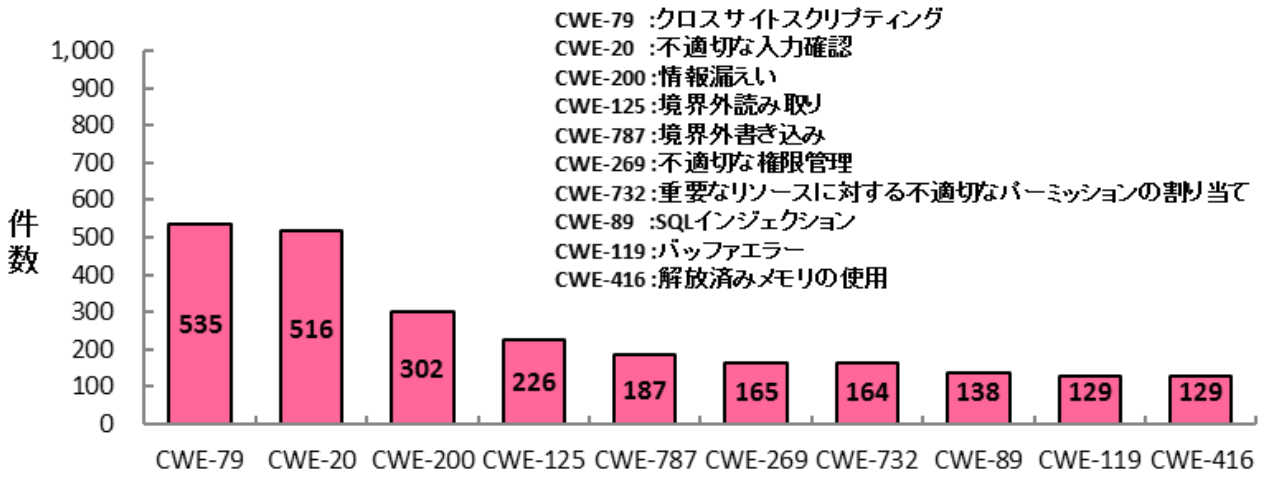

図 2-1. 2019 年第 4 四半期に登録された脆弱性の種類別件数

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

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

[*11] 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 25.8%、レベルⅡが 62.7%、レベルⅠが 11.5%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 88.5%を占めています。

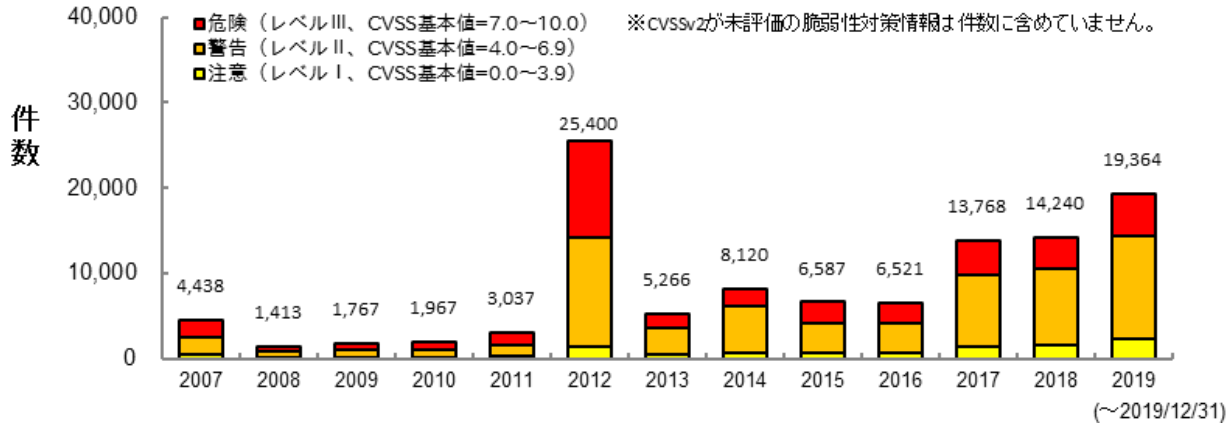

図 2-2. 脆弱性の深刻度別件数(CVSSv2)

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。

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 15.8%、「重要」が 41.9%、「警告」が 40.7%、「注意」が 1.6%となっています。

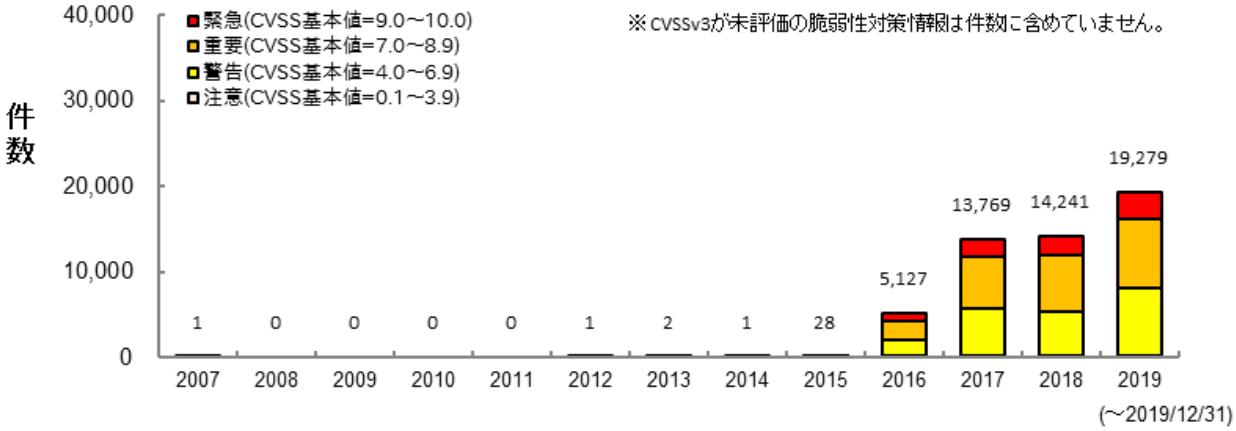

図 2-3. 脆弱性の深刻度別件数(CVSSv3)

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 [*12] で公開しています。

[*12] 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。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 74.5%（14,470／全 19,410 件）を占めています。

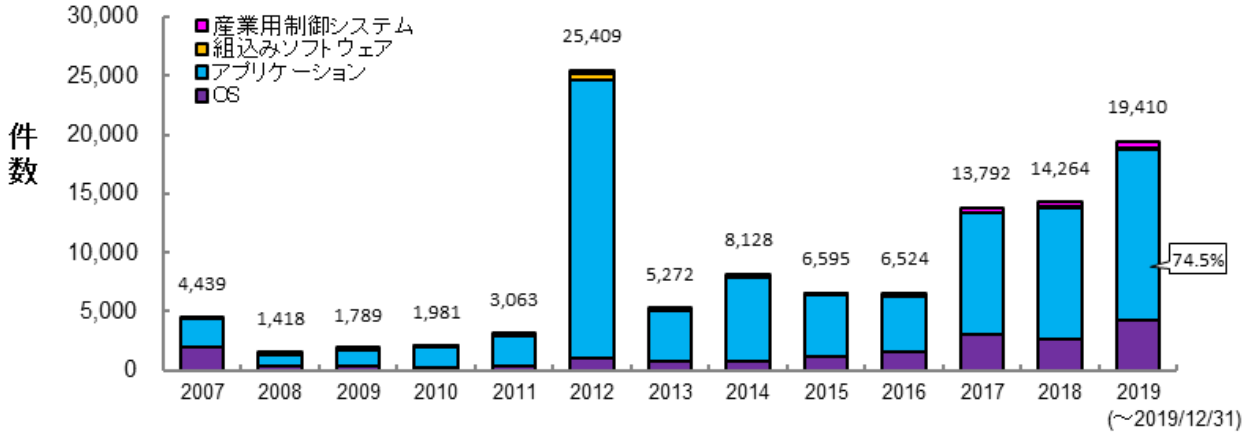

図 2-4. 脆弱性対策情報を公表した製品の種類別件数の公開年別推移

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 2,333 件を登録しています。

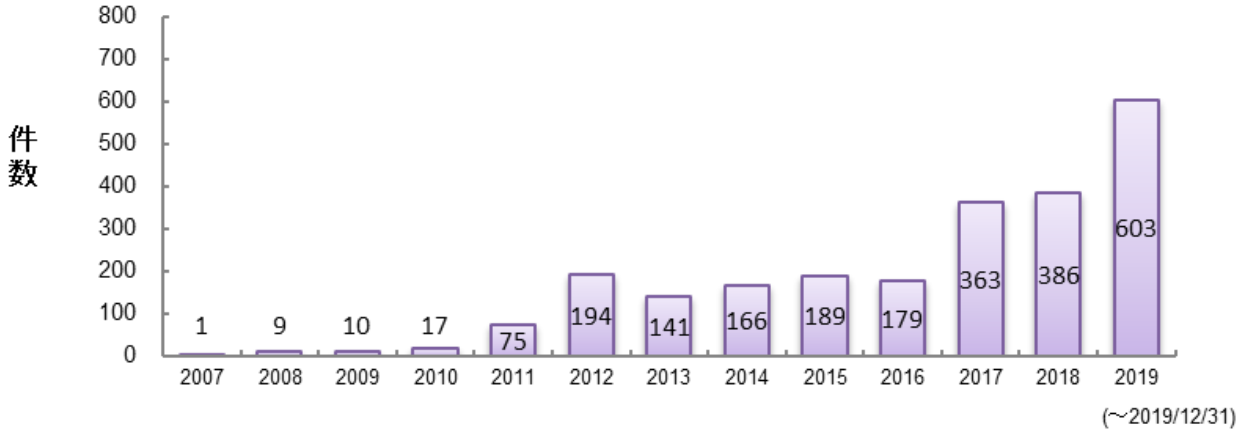

図 2-5. JVN iPedia 登録件数（産業用制御システムのみ抽出）

2-4. 脆弱性対策情報の製品別登録状況

表 2-1 は 2019 年第 4 四半期（10 月～12 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登録件数 315 件の Android OS が 1 位となりました。2 位以降はマイクロソフトの Windows 製品や Linux OS の Debian GNU/Linux や Linux Kernel 等、OS 製品に関する脆弱性対策情報が多く登録される結果となっています。

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 [(*13)] 。

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 10 月～2019 年 12 月]

順位	カテゴリ	製品名（ベンダ名）	登録件数
1	OS	Android (Google)	315
2	OS	Debian GNU/Linux (Debian)	225
3	ブラウザ	Google Chrome (Google)	154
4	OS	Linux Kernel (Kernel.org)	118
5	OS	Fedora (Fedora Project)	99
6	OS	Microsoft Windows 10 (マイクロソフト)	97
7	OS	Microsoft Windows Server (マイクロソフト)	92
7	ファームウェア	Qualcomm compornent (クアルコム)	92
9	OS	Microsoft Windows Server 2019 (マイクロソフト)	88
10	OS	Microsoft Windows Server 2016 (マイクロソフト)	72
11	PDF 閲覧	Adobe Acrobat Reader DC (アドビシステムズ)	70
11	PDF 閲覧・編集	Adobe Acrobat DC (アドビシステムズ)	70
13	CMS	Magento (Magento, Inc.)	65
13	OS	Microsoft Windows 7　(マイクロソフト)	65
15	OS	Microsoft Windows 8.1 (マイクロソフト)	64
15	OS	Microsoft Windows Server 2012 (マイクロソフト)	64
17	OS	Microsoft Windows Server 2008 (マイクロソフト)	63
18	OS	Microsoft Windows RT 8.1 (マイクロソフト)	60
19	OS	Red Hat Enterprise Linux (レッドハット)	53
20	OS	Ubuntu (Canonical)	38

[(*13)] 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 2019 年第 4 四半期（10 月～12 月）にアクセスの多かった JVN iPedia の脆弱性対策情報の 20 件を示したものです。

本四半期は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や国内の製品開発者から収集した脆弱性対策情報が上位 20 件を占めました。

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 10 月～2019 年 12 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-2019-000060	LINE (Android 版) における複数の整数オーバーフローの脆弱性	6.8	6.3	2019/9/19	9,135
2	JVNDB-2019-000068	スマートフォンアプリ「ラクマ」における認証情報漏えいの脆弱性	2.6	4.7	2019/11/7	8,875
3	JVNDB-2019-010374	Cosminexus HTTP Server および Hitachi Web Server における脆弱性	なし	なし	2019/10/11	8,116
4	JVNDB-2019-000064	WordPress 用プラグイン wpDataTables Lite における複数の脆弱性	6.5	7.2	2019/10/11	8,097
5	JVNDB-2019-000063	EC-CUBE 用モジュール「ルミーズ決済モジュール (2.11 系・2.12 系・2.13 系)」における複数の脆弱性	5.0	5.3	2019/10/7	7,200
6	JVNDB-2019-009884	FON がオープンリゾルバとして機能してしまう問題	5.0	5.8	2019/10/2	7,164
7	JVNDB-2019-000062	DBA-1510P における複数の OS コマンドインジェクションの脆弱性	5.8	8.8	2019/10/7	7,117
8	JVNDB-2019-011088	ウイルスバスターコーポレートエディションにおけるディレクトリトラバーサルの脆弱性	5.2	8.2	2019/10/29	7,059
9	JVNDB-2019-000065	NetCommons3 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	2019/10/15	6,921
10	JVNDB-2019-000059	apng-drawable における整数オーバーフローの脆弱性	6.8	5.3	2019/9/12	6,866
11	JVNDB-2019-000054	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	7.6	2019/8/26	6,853
12	JVNDB-2019-000066	PowerCMS におけるオープンリダイレクトの脆弱性	2.6	4.7	2019/10/23	6,779
13	JVNDB-2019-000053	Smart TV Box におけるアクセス制限不備の脆弱性	6.8	7.3	2019/8/23	6,580
14	JVNDB-2019-000043	ひかり電話ルータ/ホームゲートウェイにおける複数の脆弱性	4.3	6.1	2019/6/27	6,575
15	JVNDB-2019-000040	VAIO Update における複数の脆弱性	6.8	7.8	2019/6/21	6,505
16	JVNDB-2019-000049	WordPress 用プラグイン Category Specific RSS feed Subscription 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	2019/7/18	6,447

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-2019-000048	WordPress 用プラグイン WordPress Ultra Simple Paypal Shopping Cart 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	2019/7/16	6,415
18	JVNDB-2019-007404	WonderCMS におけるディレクトリトラバーサルの脆弱性	5.5	6.4	2019/8/9	6,402
19	JVNDB-2019-010375	Hitachi Global Link Manager における複数の脆弱性	なし	なし	2019/10/11	6,277
20	JVNDB-2019-000036	WordPress 用プラグイン Contest Gallery 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	2019/6/12	6,094

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 10 月～2019 年 12 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-2019-010374	Cosminexus HTTP Server および Hitachi Web Server における脆弱性	なし	なし	2019/10/11	8,116
2	JVNDB-2019-010375	Hitachi Global Link Manager における複数の脆弱性	なし	なし	2019/10/11	6,277
3	JVNDB-2019-008917	Hitachi Command Suite 製品および Hitachi Infrastructure Analytics Advisor における複数の脆弱性	なし	なし	2019/9/9	5,867
4	JVNDB-2019-011488	Hitachi Command Suite 製品における情報露出の脆弱性	なし	なし	2019/11/11	5,084
5	JVNDB-2019-011487	Hitachi Command Suite 製品および Hitachi Infrastructure Analytics Advisor における DoS 脆弱性	なし	なし	2019/11/11	5,014

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