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

[2022 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、2022 年 10 月 1 日から 2022 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

2023 年 1 月 18 日

目次

1. 2022 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 151,956 件～

2022 年第 4 四半期（2022 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 151,956 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 2,527 件になりました。

表 1-1. 2022 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	2 件	268 件
	JVN	270 件	11,939 件
	NVD	3,418 件	139,749 件
	計	3,690 件	151,956 件
英語版	国内製品開発者	2 件	263 件
	JVN	42 件	2,264 件
	計	44 件	2,527 件

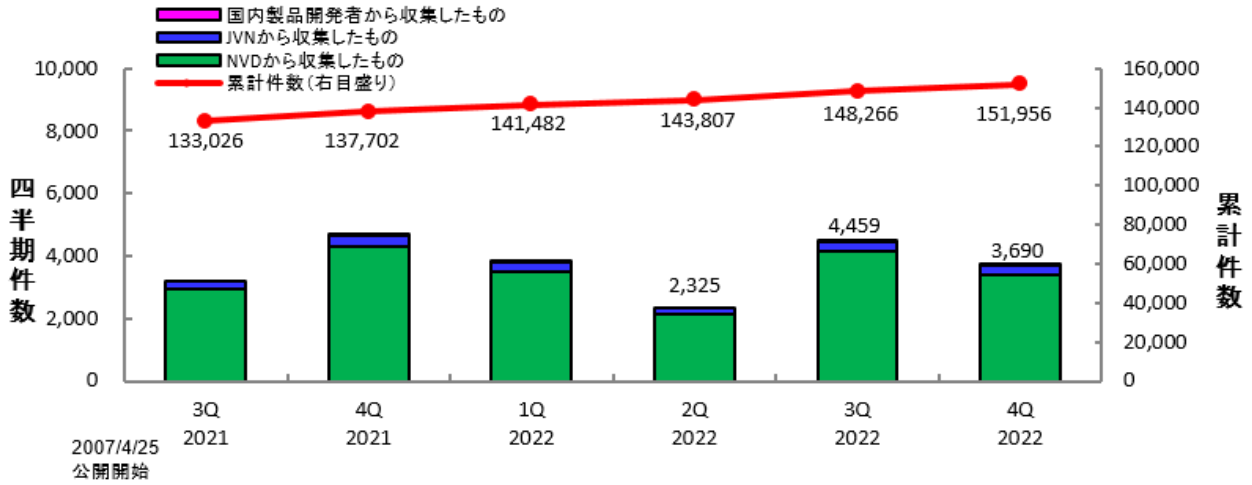

図 1-1. JVN iPedia の登録件数の四半期別推移

(*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】「Internet Explorer」のサポート終了について
～「Internet Explorer」のサポート終了に伴い、「Microsoft Edge」に切り替えを～

2022 年 6 月 16 日（日本時間）にマイクロソフトより提供されていたブラウザである Internet Explorer のサポートが終了しました。[*4] サポート終了後 Internet Explorer を利用しようとすると、マイクロソフトが提供する Microsoft Edge が起動するようになっています。

JVN iPedia には Internet Explorer に関する脆弱性が 2022 年 12 月末時点で 2,045 件登録されています。全体の深刻度（CVSSv2）の割合は最も高い「危険」（CVSS 基本値=7.0～10.0）が 1,570 件で 76.8%、次に高い「警告」（CVSS 基本値=4.0～6.9）が 424 件で 20.7%、「注意」（CVSS 基本値=0.1～3.9）が 51 件で 2.5%でした。（図 1-2）

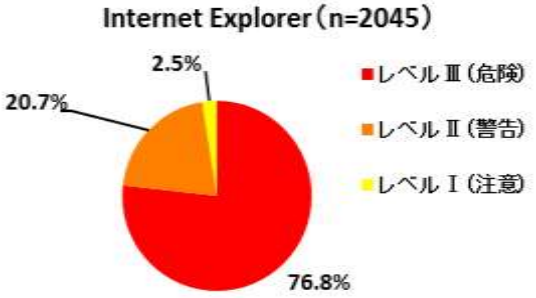

図 1-2.　2022 年までに JVN iPedia へ登録された Internet Explorer の脆弱性の深刻度別割合（CVSSv2）

一方、今回の Internet Explorer のサポート終了を契機に別のブラウザを利用していたのにも関わらず、意図せず Internet Explorer に関連する脆弱性が悪用される被害事例がありました。2022 年 11 月にマイクロソフトより Internet Explorer の JScript エンジン「jscript9.dll」に対するリモートでコードを実行される脆弱性「CVE-2022-41128」が公表されましたが、セキュリティ更新プログラムが公開される前の 10 月末時点でハッカー集団によるゼロデイ攻撃への悪用が行われていました。[*5]脆弱性を悪用する word ファイルがオンライン上にアップロードされており、閲覧者が word ファイルを開いた後にマクロの実行許可を与えた場合、Internet Explorer を介してリモートでコードが実行されるおそれがありました。なお、この脆弱性はマイクロソフトの 11 月のセキュリティ更新プログラムにより Windows OS を修正したため、解消されています。

今回の被害事例のように、使っていないからとアンインストールをせず PC 内に残しておくと、脆弱性をきっかけに悪用されてしまう場合があります。サポートが切れたソフトウェアについては、インストールしたままで放置せず、アンインストール等の適切な対応が求められます。また、脆弱性が発見され、マイクロソフトからそれに対応したセキュリティ更新プログラムを配信された場合には、利用者は即座にアップデートを行うことも大切です。しかし、セキュリティ更新プログラムの配信は基本的に「サポート期限内」のソフトウェアに限られることに注意が必要です。そのため、2022 年 6 月に Internet Explorer がサポート終了したことにより、今後脆弱性が発見されてもセキュリティ更新プログラムが公開されず、利用者は脆弱性に対応できないことが考えられるため即時のブラウザの切り替えが求められます。なお、今回の脆弱性「CVE-2022-41128」を受けてマイクロソフトから

[*4] Internet Explorer は Microsoft Edge へ - Windows 10 の Internet Explorer 11 デスクトップアプリは 2022 年 6 月 15 日にサポート終了
https://blogs.windows.com/japan/2021/05/19/the-future-of-internet-explorer-on-windows-10-is-in-microsoft-edge/

[*5] Google が IE のゼロデイ脆弱性を突いて韓国のユーザーを狙った北朝鮮発の攻撃を解説
https://forest.watch.impress.co.jp/docs/news/1462309.html

セキュリティ更新プログラムが公開されましたが、これは Windows OS の脆弱性への対応として公開されており、サポートが終了していた Internet Explorer に対してのものではありませんでした。

Internet Explorer のサポート終了に伴いマイクロソフトは Microsoft Edge にブラウザを切り替えるようアナウンスしています。Microsoft Edge は Internet Explorer の後継としてマイクロソフトでサポートされるブラウザで、Windows10 から標準搭載されています。2029 年までの期間限定ではありますが、Internet Explorer と互換性があり同じように閲覧できる機能を持った「IE モード」が搭載されており、Internet Explorer でしか動作しないウェブサイト等を閲覧されている場合は、モードを切り替えて利用することができます。

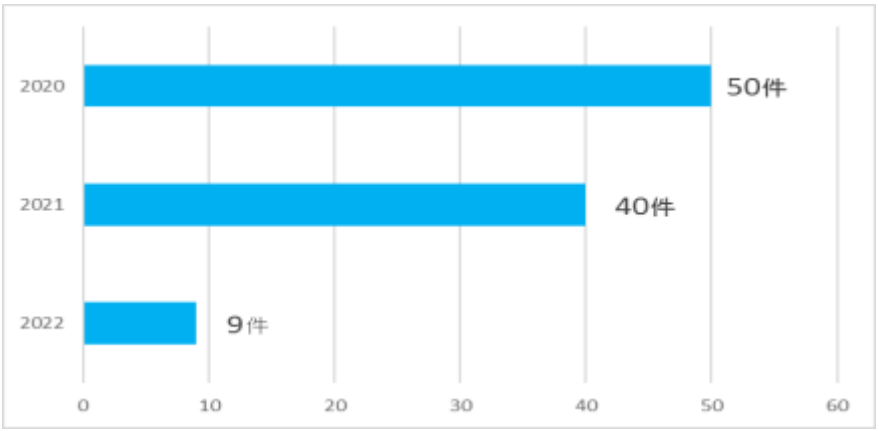

図 1-3.　JVN iPedia へ登録された Microsoft Edge の脆弱性件数（2020～2022 年）

Microsoft Edge についても、2015 年のリリース以降多くの脆弱性が公開されています。図 1-3 は直近 3 年間（2020～2022 年）に JVN iPedia へ登録された Microsoft Edge の脆弱性の年別の件数です。JVN iPedia における脆弱性の登録数は減少傾向にありますが、脆弱性はいつ発見されるか予測がつかないため、マイクロソフトが公開するセキュリティ更新プログラムを定期的にアップデートすることを推奨します。

IPA では深刻な脆弱性攻撃の発生に対して緊急対策情報を公開しています。また、その情報をいち早く受け取れる「icat for JSON[*6]」というサービスを提供しています。こちらもご活用ください。

[*6] IPA：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】Microsoft Exchange Server に関する既知の脆弱性を使った攻撃について
～定期アップデートが正しく行われているか注意。アップデートの見落としがないか十分確認を～

2022 年 11 月のマイクロソフトのセキュリティ更新プログラムにて、標的型攻撃に悪用が確認された脆弱性が公表されました。標的型攻撃は、IPA が毎年公表している「情報セキュリティ 10 大脅威」でも近年毎年上位にランクインしている脅威（情報セキュリティ 10 大脅威 2022 では、組織 2 位「標的型攻撃による機密情報の窃取」）です。今回の標的型攻撃で悪用されたのはマイクロソフトが提供するメールシステムである Microsoft Exchange Server の脆弱性 CVE-2022-41040 および CVE-2022-41082 で、その 2 つを組み合わせることで権限を不正に奪い、リモートから任意のコードを実行させることが可能でした。その攻撃は「ProxyNotShell」と呼ばれていました。悪用された CVE-2022-41040[(*7)]は権限管理に関する脆弱性で、CVE-2022-41082[(*8)]はリモートでコードが実行される脆弱性です。どちらも CVSSv3 は 8.8 とされており深刻度が 2 番目に高い「重要」（CVSSv3 基本値 7.0～8.9）となる脆弱性でした。

セキュリティ更新プログラムの公開後、「ProxyNotShell」は下火になりましたが、2022 年 11 月後半より CVE-2022-41080 および CVE-2022-41082 の 2 つを組み合わせて悪用する、「ProxyNotShell」の緩和策を回避する新たな攻撃が行われていることが確認されました。CVE-2022-41080[(*9)]は CVE-2022-41040 に似た権限昇格の脆弱性です。今回は Exchange Server に付随する「Outlook Web Access（OWA）」というシステムを介し、権限を不正に奪い、リモートでコードを実施する攻撃でした。この攻撃は「OWASSRF」と呼ばれています。CVE-2022-41080 は CVE-2022-41040 および CVE-2022-41082 と同じく 2022 年 11 月のセキュリティ更新プログラムで修正された脆弱性でしたが、攻撃者はアップデートを行っていないユーザを標的として攻撃を仕掛けていました。

以下は 2022 年に JVN iPedia に登録された Exchange Server に関する脆弱性の深刻度の割合となります。

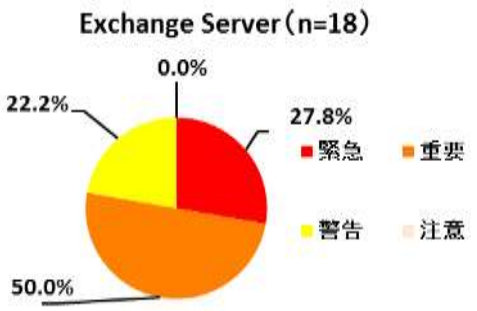

図 1-4.　2022 年に JVN iPedia へ登録された Exchange Server の深刻度割合（CVSSv3）

2022 年に登録された Exchange Server の件数は 18 件であり、そのうち深刻度は最も高い「緊急」（CVSSv3 基本値 9.0～10.0）が 27.8%、次に高い「重要」（CVSSv3 基本値 7.0～8.9）が 50.0%となっており、脆弱性が発生した場合の対応を早急に行わなければならない傾向にあるといえます。

今回解説した「ProxyNotShell」はセキュリティ更新プログラムが公開される前のゼロデイの脆弱

(*7) Microsoft Exchange Server における権限管理に関する脆弱性
https://jvndb.jvn.jp/ja/contents/2022/JVNDB-2022-002439.html
(*8) Microsoft Exchange Server における脆弱性
https://jvndb.jvn.jp/ja/contents/2022/JVNDB-2022-002438.html
(*9) Microsoft Exchange Server における権限を昇格される脆弱性
https://jvndb.jvn.jp/ja/contents/2022/JVNDB-2022-002733.html

性を悪用したものであるため、組織としては事前の対策は難しいものでした。しかし、公開後にアップデートすることでその後の被害を防ぐことができました。一方、「OWASSRF」は定期的にアップデートを行っていれば防ぐことができるものでした。ゼロデイ攻撃の有無に関わらず、被害に遭わないためにマイクロソフトなどのベンダから提供されるセキュリティ更新プログラムや修正パッチが公開されたら早急にアップデートすることを推奨します。なお、何らかの理由にアップデートできない場合は回避策など別の代替策で対応することも検討してください。今一度自組織のシステムに関するルールを確認しておきましょう。

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、2022 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 507 件、CWE-787（境界外書き込み）が 204 件、CWE-89（SQL インジェクション）が 183 件、CWE-20（不適切な入力確認）が 123 件、CWE-22（パス・トラバーサル）が 115 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**[(*10)]」、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**[(*11)]」や「**IPA セキュア・プログラミング講座**[(*12)]」、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**[(*13)]」などを公開しています。

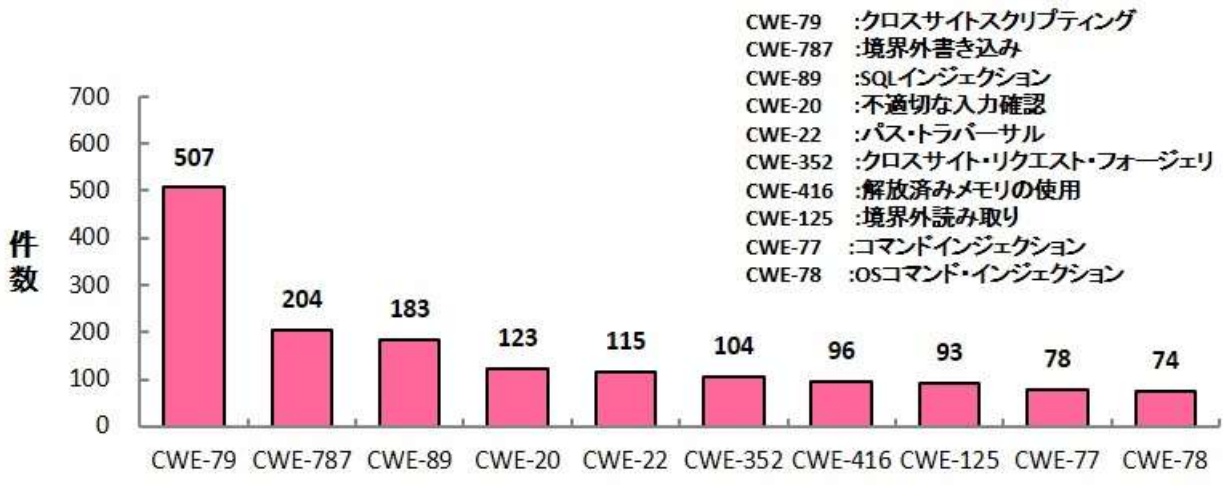

図 2-1. 2022 年第 4 四半期に登録された脆弱性の種類別件数

(*10) 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
(*11) IPA：「安全なウェブサイトの作り方」
https://www.ipa.go.jp/security/vuln/websecurity.html
(*12) IPA：「IPA セキュア・プログラミング講座」
https://www.ipa.go.jp/security/awareness/vendor/programming/
(*13) 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。

2022 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 19.8%、レベルⅡが 64.0%、レベルⅠが 16.2%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 83.8%を占めています。

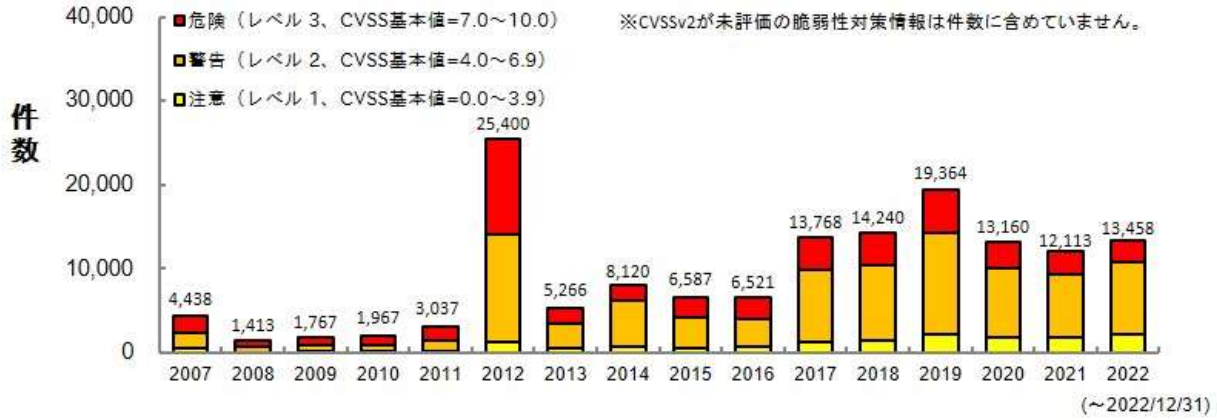

図 2-2. 脆弱性の深刻度別件数(CVSSv2)

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。

2022 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 12.3%、「重要」が 42.2%、「警告」が 43.3%、「注意」が 2.3%となっています。

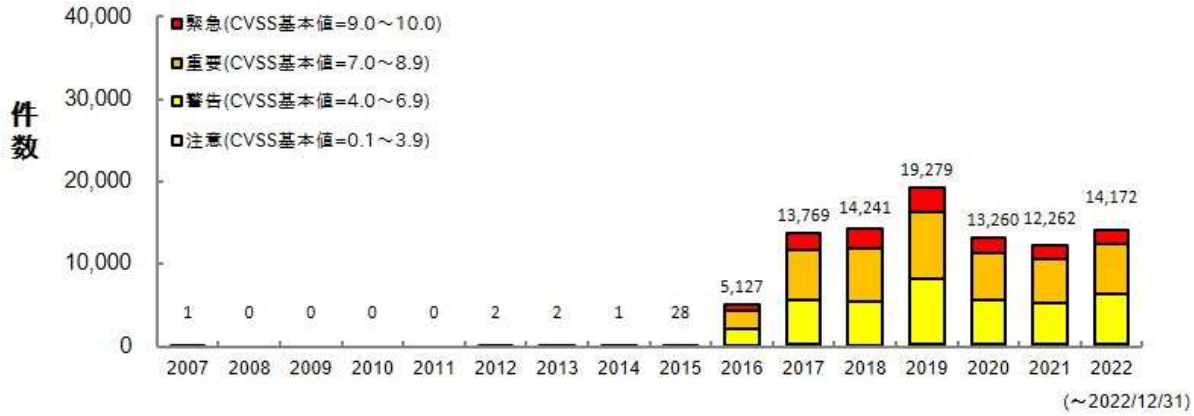

図 2-3. 脆弱性の深刻度別件数(CVSSv3)

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 [*14] で公開しています。

[*14] 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。2022 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、2022 年の件数全件の約 73.7%（117,951 件／全 151,801 件）を占めています。

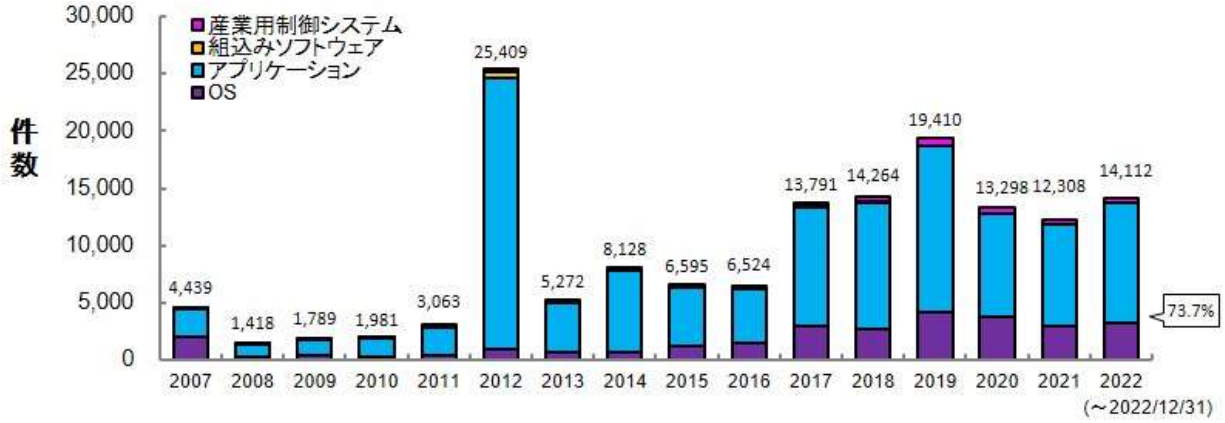

図 2-4. 脆弱性対策情報を公表した製品の種類別件数の公開年別推移

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 3,747 件を登録しています。

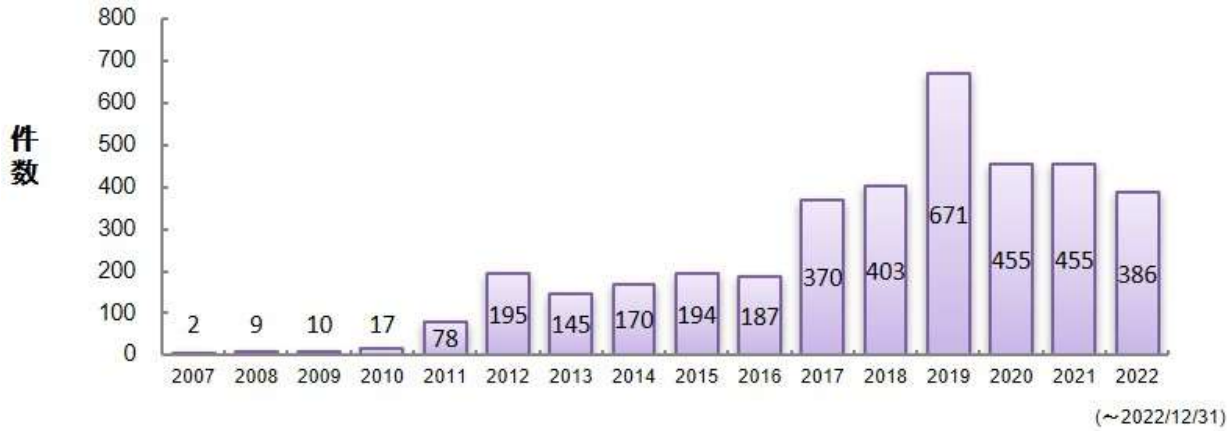

図 2-5. JVN iPedia 登録件数（産業用制御システムのみ抽出）

2-4. 脆弱性対策情報の製品別登録状況

表 2-1 は 2022 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。

本四半期において最も登録件数が多かったのは、Google が提供する Android でした。2 位以降は前四半期ランクインしていたクアルコム製品や 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 [*15] 。

表 2-1. 製品別 JVN iPedia の脆弱性対策情報登録件数　上位 20 件 [2022 年 10 月～2022 年 12 月]

順位	カテゴリ	製品名（ベンダ名）	登録件数
1	OS	Android (Google)	186
2	ファームウェア	Qualcomm component (クアルコム)	180
3	OS	Debian GNU/Linux (Debian)	164
4	OS	Fedora (Fedora Project)	163
5	OS	Microsoft Windows Server 2022 (マイクロソフト)	129
5	OS	Microsoft Windows 11 (マイクロソフト)	129
7	OS	Microsoft Windows 10 (マイクロソフト)	128
8	OS	Microsoft Windows Server 2019 (マイクロソフト)	123
9	OS	Microsoft Windows Server 2016 (マイクロソフト)	107
10	OS	HarmonyOS (Huawei)	102
11	OS	Microsoft Windows Server 2012 (マイクロソフト)	94
12	OS	Microsoft Windows 8.1 (マイクロソフト)	91
13	OS	Microsoft Windows RT 8.1 (マイクロソフト)	88
14	OS	Microsoft Windows Server 2008 (マイクロソフト)	82
15	OS	Microsoft Windows 7　(マイクロソフト)	78
16	その他	Magic UI (Huawei)	72
16	その他	EMUI (Huawei)	72
18	ブラウザ	Google Chrome (Google)	67
19	ファームウェア	RBR850 ファームウェア (ネットギア)	49
19	ファームウェア	RBK852 ファームウェア (ネットギア)	49

[*15] 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 2022 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上位 20 件を示したものです。

本四半期は、20 件中 11 件が WordPress また WordPress 用のプラグインの脆弱性がランクインしました。前四半期に比べ、OS 製品の脆弱性のランクインは減少しています。

表 3-1. JVN iPedia の脆弱性対策情報へのアクセス　上位 20 件 [2022 年 10 月～2022 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-2021-012563	XMP Toolkit SDK における古典的バッファオーバーフローの脆弱性	6.8	7.8	2022/9/2	9,419
2	JVNDB-2021-013508	複数の Apple 製品における解放済みメモリの使用に関する脆弱性	7.5	9.8	2022/9/14	8,100
3	JVNDB-2021-012173	WordPress 用 Shopp プラグインにおける危険なタイプのファイルの無制限アップロードに関する脆弱性	7.5	9.8	2022/8/25	6,638
4	JVNDB-2021-012490	Rancher におけるアクセス制御に関する脆弱性	4.0	9.9	2022/9/1	6,135
5	JVNDB-2022-002444	バッファロー製ネットワーク機器における複数の脆弱性	-	8.8	2022/10/5	5,569
6	JVNDB-2022-000076	GROWI におけるアクセス制限不備の脆弱性	4.0	4.3	2022/10/7	5,485
7	JVNDB-2022-000082	日本語プログラミング言語「なでしこ 3」における複数の脆弱性	7.5	9.8	2022/10/20	5,481
8	JVNDB-2022-000087	WordPress における複数の脆弱性	5.0	5.3	2022/11/8	5,330
9	JVNDB-2022-000023	WordPress 用プラグイン Advanced Custom Fields における認証欠如の脆弱性	4.0	6.5	2022/3/30	4,906
10	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	4,862
11	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	4,795
12	JVNDB-2022-000041	WordPress 用プラグイン Modern Events Calendar 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	4,756
12	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	4,752
14	JVNDB-2022-002436	Apache Tomcat に Http11Processor インスタンスにおける競合状態による情報漏えいの脆弱性	-	5.3	2022/10/3	4,659
15	JVNDB-2022-002639	Apache Tomcat における無効な HTTP ヘッダの取り扱いに関する問題	-	7.5	2022/11/4	4,640
16	JVNDB-2022-000002	WordPress 用プラグイン Quiz And Survey Master における複数の脆弱性	4.0	5.4	2022/1/12	4,634

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-2021-000109	WordPress 用プラグイン Advanced Custom Fields における複数の認証欠如の脆弱性	4.0	4.3	2021/12/2	4,600
18	JVNDB-2022-000075	IPFire の WebUI におけるクロスサイトスクリプティングの脆弱性	3.5	4.8	2022/10/6	4,592
19	JVNDB-2021-000103	WordPress 用プラグイン Push Notifications for WordPress (Lite) 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	2021/11/16	4,574
19	JVNDB-2021-000086	WordPress 用プラグイン OG Tags 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	2021/9/28	4,574

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 [2022 年 10 月～2022 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-2022-002443	Hitachi Storage Plug-in for VMware vCenter における権限昇格の脆弱性	-	5.4	2022/10/5	4,372
2	JVNDB-2022-002364	uCosminexus TP1/Client/J および Cosminexus Service Coordinator における DoS 脆弱性	-	-	2022/9/14	3,190
3	JVNDB-2022-002143	Hitachi Automation Director および Hitachi Ops Center Automator における情報露出の脆弱性	-	-	2022/8/1	2,698
4	JVNDB-2022-001382	Hitachi Command Suite 製品におけるファイルパーミッションの脆弱性	-	-	2022/3/7	2,639
5	JVNDB-2022-001299	JP1/IT Desktop Management 2 におけるクロスサイトスクリプティングの脆弱性	-	-	2022/2/8	2,625

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

2020 年以前の公開	2021 年の公開	2022 年の公開