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

[2023 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、2023 年 10 月 1 日から 2023 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

2024 年 1 月 17 日

目次

1. 2023 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 ..... - 2 -
1-1. 脆弱性対策情報の登録状況 ..... - 2 -
1-2. 【注目情報 1】MOVEit Transfer のゼロデイ脆弱性について ..... - 3 -
1-3. 【注目情報 2】Citrix Bleed に関する新しい製品の脆弱性を使った攻撃について ..... - 5 -
2. JVN iPedia の登録データ分類 ..... - 7 -
2-1. 脆弱性の種類別件数 ..... - 7 -
2-2. 脆弱性に関する深刻度別割合 ..... - 8 -
2-3. 脆弱性対策情報を公開した製品の種類別件数 ..... - 10 -
2-4. 脆弱性対策情報の製品別登録状況 ..... - 11 -
3. 脆弱性対策情報の活用状況 ..... - 12 -

1. 2023 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 193,872 件～

2023 年第 4 四半期（2023 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表 1-1 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 193,872 件になりました**（表 1-1、図 1-1）。なお、2023 年第 3 四半期に引き続き JVN iPedia の登録件数が大幅に増えている理由は、当該期間中に脆弱性が世の中に多く発見されたということを意味するものではなく、公開が遅れていた主に昨年の脆弱性が JVN iPedia の運用方法の変更に伴い多数公開されたためです。

また、JVN iPedia 英語版へ登録した脆弱性対策情報は表 1-1 の通り、累計で 2,724 件になりました。

表 1-1. 2023 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	5 件	275 件
	JVN	1,151 件	14,236 件
	NVD	20,728 件	179,361 件
	計	21,884 件	193,872 件
英語版	国内製品開発者	5 件	279 件
	JVN	44 件	2,445 件
	計	49 件	2,724 件

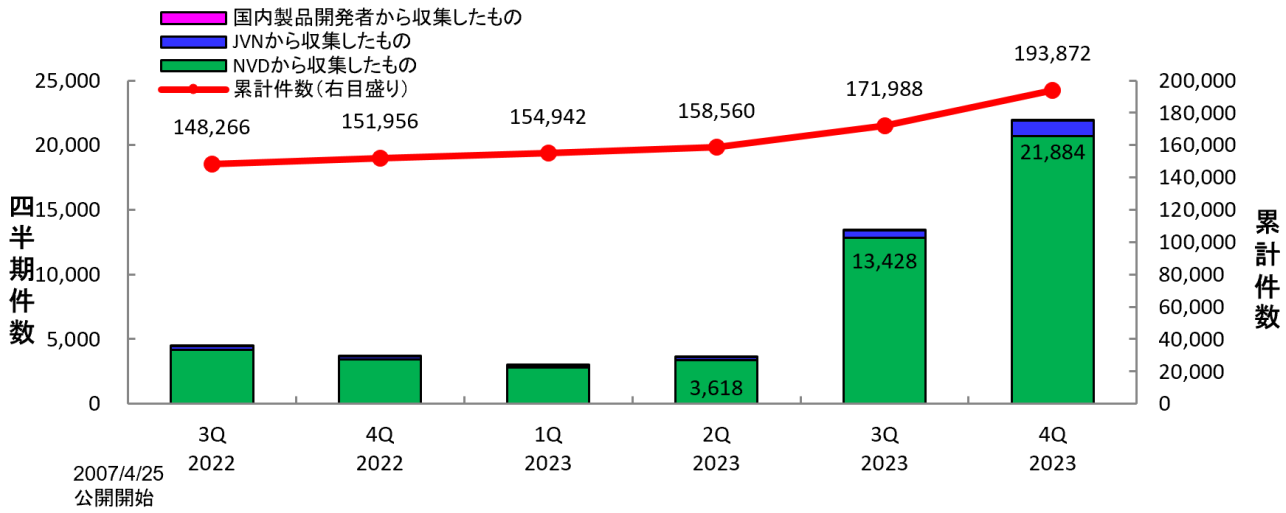

図 1-1. JVN iPedia の登録件数の四半期別推移

(*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】MOVEit Transfer のゼロデイ脆弱性について
～サイバー攻撃グループによる大規模な攻撃への悪用が確認される～

2023 年 5 月、Progress Software が提供するデータ転送ソリューション MOVEit Transfer の脆弱性 CVE-2023-34362 が公開されました(*4)。本脆弱性はデータベースを不正に操作されるおそれのある SQL インジェクションの脆弱性で、これを悪用されると認証されていないリモートの攻撃者に MOVEit Transfer データベースに不正アクセスされ、データの窃取や改ざん、権限の昇格を実行されるおそれがあります。脆弱性の深刻度を示す CVSSv3.1 基本値は 9.8 で、最も深刻度が高い「緊急」（CVSSv3 基本値=9.0～10.0）と評価されています(*5)。

本脆弱性は、脆弱性対策情報が公開される前から攻撃に悪用されていたことが確認されました。このような脆弱性はゼロデイ脆弱性と呼ばれています。攻撃は当該製品が広く使われている欧米を中心に脆弱性対策情報が公開された後、米国の複数の政府機関も被害を受けました。特に多くの被害が確認されたのが、ランサムウェアによるデータの暗号化や情報窃取により、身代金を要求する手口で知られるサイバー攻撃グループ「Clop」による攻撃によるものでした。国外拠点を持つ日本の企業も攻撃を受け、従業員情報が漏えいする等の被害が確認されました。2024 年 1 月時点で、全世界で 2,730 組織および約 9,334 万人の個人が被害を受けたことが明らかとなっています(*6)(*7)(*8)(*9)。

2023 年は他にも MOVEit Transfer の脆弱性が複数公開されました。特に、6 月に立て続けに公開された CVE-2023-35036 および CVE-2023-35708 は、悪用が確認された CVE-2023-34362 と同様に SQL インジェクションの脆弱性であったことや、CVSSv3.1 基本値がそれぞれ 9.1、9.8 と最も深刻度が高い「緊急」に分類される脆弱性であったことでネット記事等にも掲載され、広く注目されました(*10)(*11)(*12)。

また、JVN iPedia には 2024 年 1 月時点で累計 29 件の MOVEit 関連製品の脆弱性が登録されています。図 1-2 はその深刻度別割合を示したものです。脆弱性の深刻度が高い順に「緊急」（CVSSv3 基本値=9.0～10.0）が 31.0%、「重要」（CVSSv3 基本値=7.0～8.9）が 31.0%、「警告」（CVSSv3 基本値=4.0～6.9）が 20.7%、「注意」（CVSSv3 基本値=0.1～3.9）が 0.0%となっており、過半数が脆弱性を悪用された場合の影響が大きい「緊急」および「重要」に分類されています。

(*4)MOVEit Transfer Critical Vulnerability (May 2023) (CVE-2023-34362)
https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023
(*5)CVE-2023-34362
https://nvd.nist.gov/vuln/detail/CVE-2023-34362
(*6)「MOVEit Transfer」にゼロデイ脆弱性 - 侵害状況も確認を
https://www.security-next.com/146673
(*7)US energy department, other agencies hit in global hacking spree
https://www.reuters.com/world/us/us-government-agencies-hit-global-cyber-attack-cnn-2023-06-15/?_gl=1
(*8)Sony confirms data breach impacting thousands in the U.S.
https://www.bleepingcomputer.com/news/security/sony-confirms-data-breach-impacting-thousands-in-the-us/
(*9)Unpacking the MOVEit Breach: Statistics and Analysis
https://www.emsisoft.com/en/blog/44123/unpacking-the-moveit-breach-statistics-and-analysis/
(*10)CVE-2023-35036
https://nvd.nist.gov/vuln/detail/CVE-2023-35036
(*11)CVE-2023-35708
https://nvd.nist.gov/vuln/detail/CVE-2023-35708
(*12)「MOVEit Transfer」にあらたな脆弱性 - 5 月末以降、3 度目の更新
https://www.security-next.com/147099

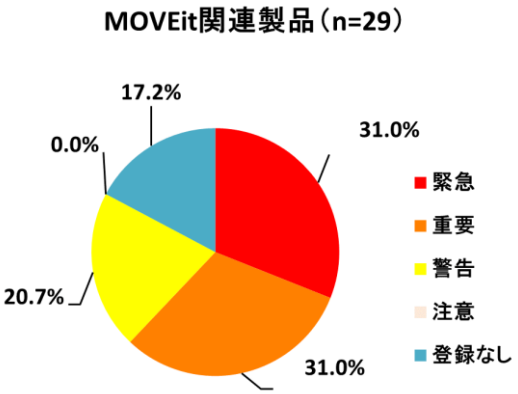

図 1-2.　2024 年 1 月までに JVN iPedia へ登録された MOVEit 関連製品の深刻度割合（CVSSv3）

MOVEit Transfer のように利用者の多い製品は、脆弱性情報が公開されると攻撃者の注目も集め、攻撃に悪用されるおそれがあります。MOVEit Transfer は主に海外の組織での利用が多いためか、日本における被害は限定的でしたが、仮に国内でも広く使われている製品に MOVEit Transfer と同等の脆弱性が発見されたのであれば、国内の被害もより多くなることが考えられます。利用者においては、継続的に脆弱性情報を収集し、セキュリティパッチが公開された場合は速やかに対応することが求められます。また、本事例のように脆弱性を悪用した攻撃が既に確認されている場合は、攻撃情報も収集し被害の有無を確認することを推奨します。

1-3. 【注目情報 2】Citrix Bleed に関する新しい製品の脆弱性を使った攻撃について
～ランサムウェア攻撃に悪用され、被害が拡大する場合も～

2023 年にも数々の脆弱性が発見されましたが、10 月に公表された CVE-2023-4966[*13]は「Citrix Bleed」と名付けられ話題になりました。Citrix Bleed は NetScaler ADC および NetScaler Gateway に存在する脆弱性で、特定の条件下で機器を動作させると、バッファオーバーフローが引き起こされ、情報漏えいが発生するおそれがあります。また、本脆弱性を悪用して窃取したセッション情報や多要素認証に必要な情報を使い、認証を回避してシステムに侵入することが可能となります。本脆弱性は 2023 年の 8 月から悪用が確認されており、その時点では脆弱性対策情報が公開される前のゼロデイ脆弱性でした。その後、LockBit3.0[*14]等のランサムウェアへの悪用が確認され、被害が拡大しました。

この脆弱性を受け、開発元であるシトリックス・システムズは、脆弱性への対策としてソフトウェアのアップデートだけではなく、追加でコマンドを実行してアクティブなセッションや永続的なセッションを削除することを推奨しました。また、同社は CVSSv3.1 基本値を 9.4 とし、最も深刻度が高い「緊急」（CVSSv3 基本値=9.0～10.0）と評価しました。

2021 年から 2023 年に公表され、JVN iPedia に登録されたシトリックス・システムズ製品の脆弱性対策情報件数の推移および深刻度別割合を以下のグラフに記載します。

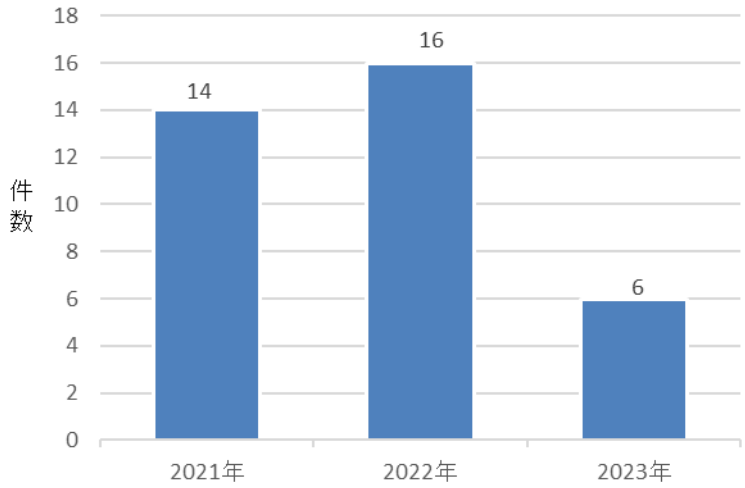

図 1-3.　2021 年～2023 年に公表されたシトリックス・システムズ社製品の脆弱性対策情報件数

[*13]CVE-2023-4966
https://nvd.nist.gov/vuln/detail/CVE-2023-4966
[*14]「Citrix Bleed」に対する攻撃増加 - 著名ランサムグループも悪用
https://www.security-next.com/151349

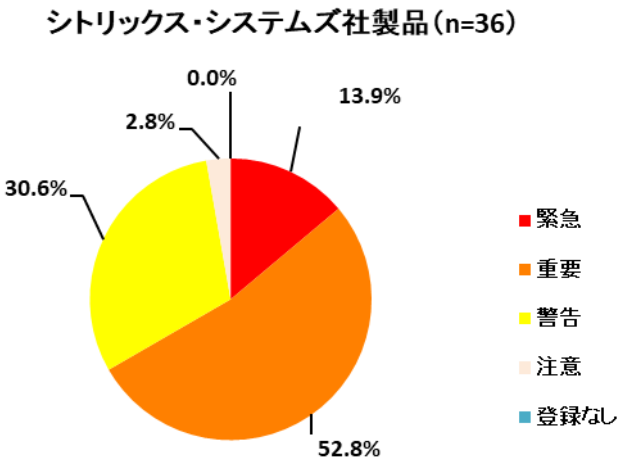

図 1-4.　2021 年～2023 年に公表されたシトリックス・システムズ社製品の深刻度割合（CVSSv3）

毎年度脆弱性が公表されており、深刻度別割合を見ると脆弱性の深刻度が高い順に「緊急」（CVSSv3 基本値=9.0～10.0）が 13.9%、「重要」（CVSSv3 基本値=7.0～8.9）が 52.8%、「警告」（CVSSv3 基本値=4.0～6.9）が 30.6%、「注意」（CVSSv3 基本値=0.1～3.9）が 2.8%となっており、全体の 66.7%が脆弱性を悪用された場合の影響が大きい「緊急」および「重要」に分類されています。

ソフトウェアやハードウェアは、導入当初に既存の脆弱性に対応した最新バージョンを利用していても、時間が経過するとともに新しく脆弱性が発見される可能性があります。また、脆弱性に対応した最新バージョンへのアップデートだけではなく、今回の Citrix Bleed のようにアクティブなセッションや永続的なセッションを削除する等の追加の対応が必要になる場合もあります。自組織で利用している製品の脆弱性情報を収集し、開発元等から最新バージョンへのアップデート以外に追加の対応が要求されている場合は速やかに実施する必要があります。

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、2023 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 3,526 件、CWE-787（境界外書き込み）が 1,669 件、CWE-89（SQL インジェクション）が 1,571 件、CWE-352（クロスサイト・リクエスト・フォージェリ）が 846 件、CWE-125（境界外読み取り）が 771 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**[*15]」、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**[*16]」、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**[*17]」などを公開しています。

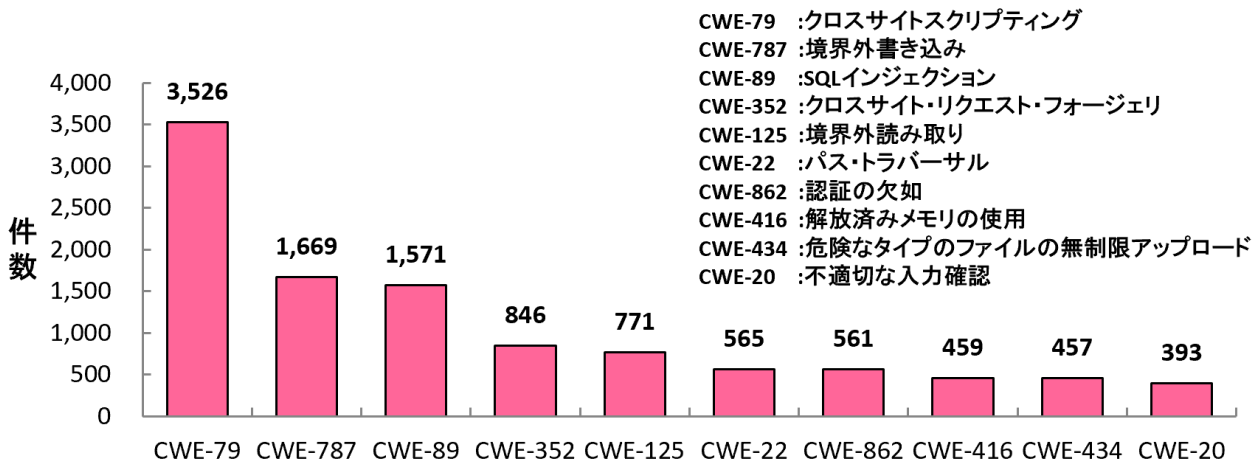

図 2-1. 2023 年第 4 四半期に登録された脆弱性の種類別件数

[*15] 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/guide/vuln/forvendor.html
[*16] IPA：「安全なウェブサイトの作り方」
https://www.ipa.go.jp/security/vuln/websecurity/about.html
[*17] IPA：「脆弱性体験学習ツール AppGoat」
https://www.ipa.go.jp/security/vuln/appgoat/index.html

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。

2023 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 3 が全体の 24.1%、レベル 2 が 60.6%、レベル 1 が 15.3%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 2 以上が 84.7%を占めています。

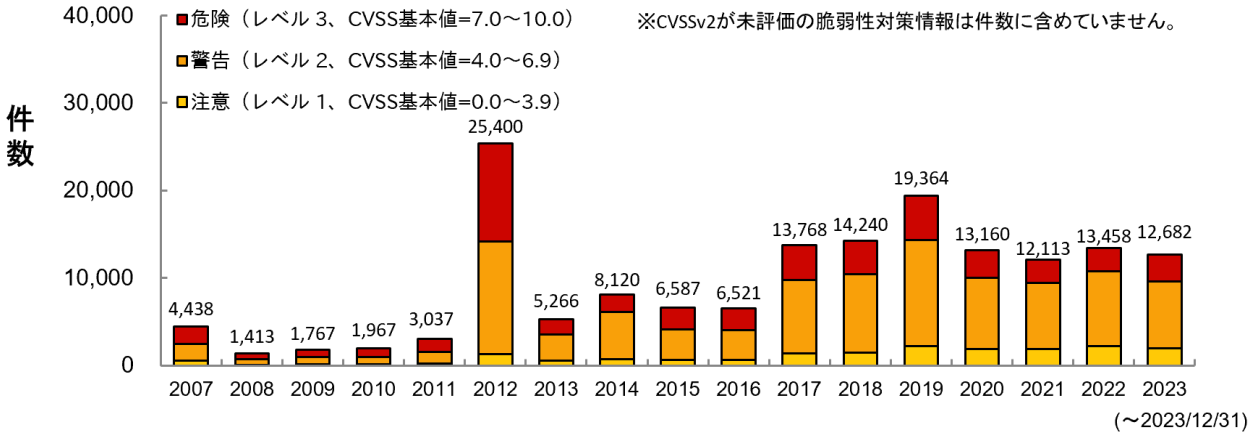

図 2-2. 脆弱性の深刻度別件数(CVSSv2)

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。

2023 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 17.5%、「重要」が 39.1%、「警告」が 41.7%、「注意」が 1.7%となっています。

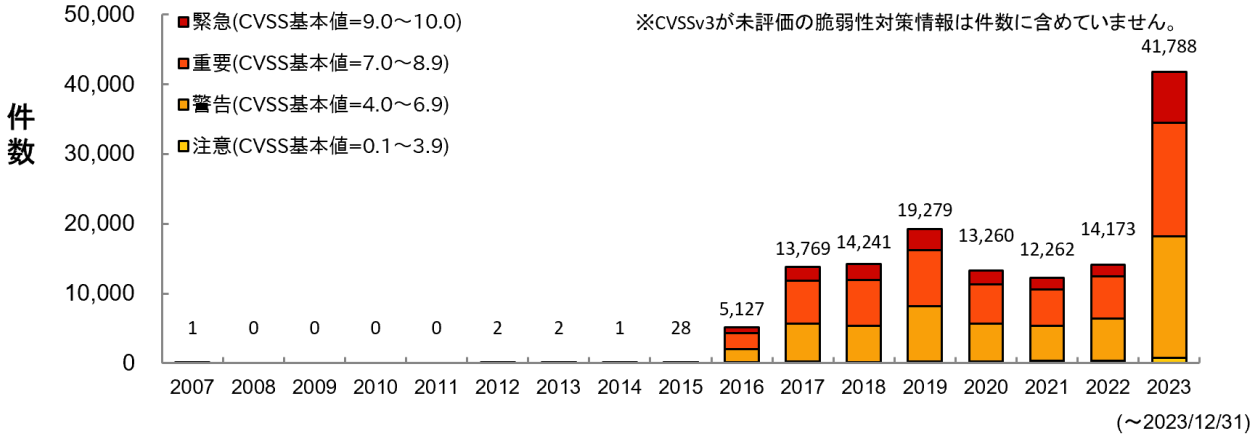

図 2-3. 脆弱性の深刻度別件数(CVSSv3)

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 [*18] で公開しています。

[*18] 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。2023 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、2023 年の件数全件の約 72.6%（30,415 件／全 41,916 件）を占めています。

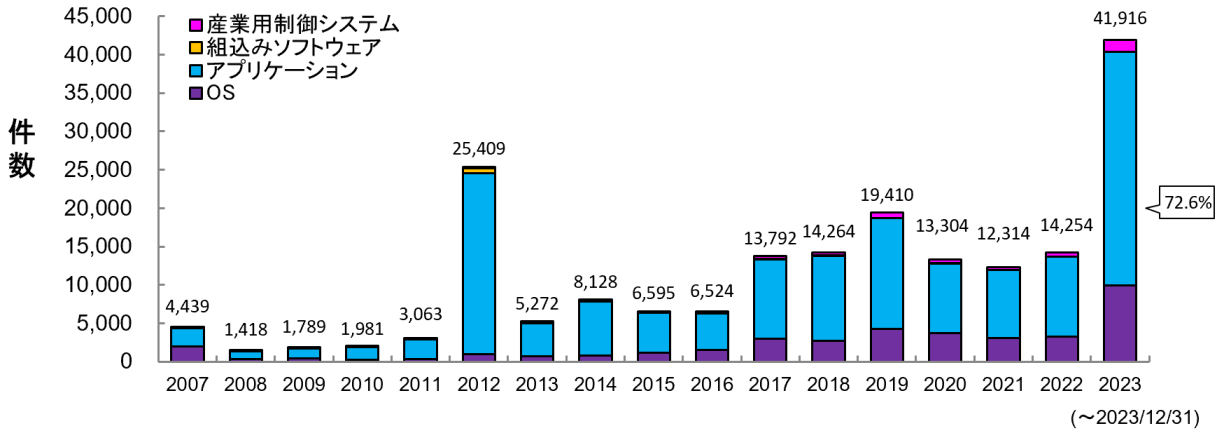

図 2-4. 脆弱性対策情報を公表した製品の種類別件数の公開年別推移

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 5,402 件を登録しています。

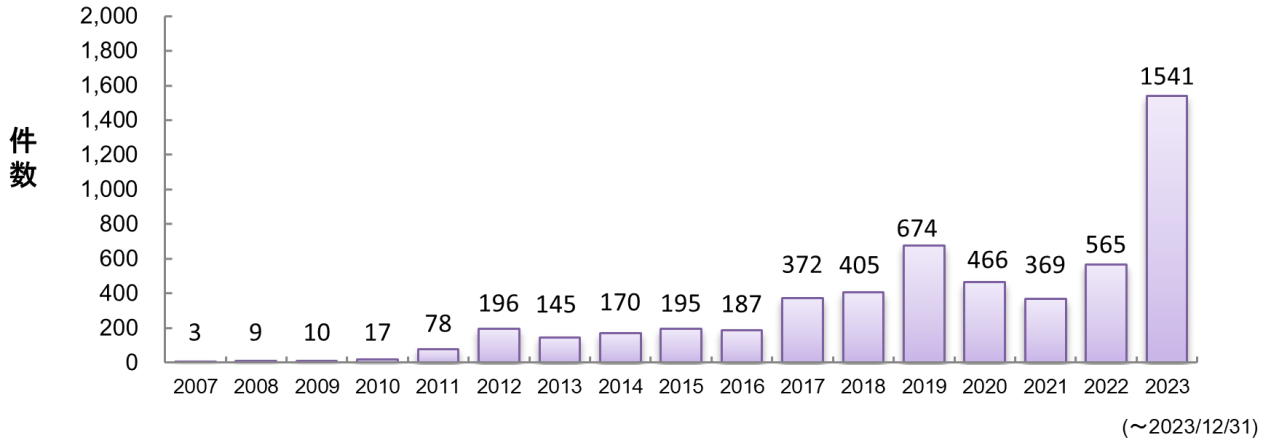

図 2-5. JVN iPedia 登録件数（産業用制御システムのみ抽出）

2-4. 脆弱性対策情報の製品別登録状況

表 2-1 は 2023 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クアルコムが提供する Qualcomm component が 1 位となりました。2 位以降は Google、アップル、マイクロソフトなど、幅広いベンダの OS がランクインをしました。

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 [(*19)] 。

表 2-1. 製品別 JVN iPedia の脆弱性対策情報登録件数　上位 20 件 [2023 年 10 月～2023 年 12 月]

順位	カテゴリ	製品名（ベンダ名）	登録件数
1	ファームウェア	Qualcomm component (クアルコム)	4,965
2	OS	Android (Google)	1,406
3	OS	Fedora (Fedora Project)	524
4	OS	Debian GNU/Linux (Debian)	476
5	OS	macOS (アップル)	406
6	OS	Linux Kernel (Linux)	335
7	OS	iOS (アップル)	311
8	OS	iPadOS (アップル)	285
9	ブラウザ	Google Chrome (Google)	269
10	OS	EMUI (Huawei)	206
11	OS	watchOS (アップル)	180
11	OS	HarmonyOS (Huawei)	180
13	OS	tvOS (アップル)	164
14	その他	GitLab (GitLab.org)	144
15	OS	Red Hat Enterprise Linux (レッドハット)	138
16	OS	Microsoft Windows Server 2022 (マイクロソフト)	134
17	OS	Microsoft Windows Server 2019 (マイクロソフト)	129
18	OS	Microsoft Windows 11 (マイクロソフト)	128
19	OS	Microsoft Windows 10 (マイクロソフト)	122
20	OS	Microsoft Windows Server 2016 (マイクロソフト)	116

[(*19)] IPA：「脆弱性対策の効果的な進め方（実践編）」
https://www.ipa.go.jp/security/reports/technicalwatch/20150331.html

3. 脆弱性対策情報の活用状況

表 3-1 は 2023 年第 4 四半期（10 月～12 月）にアクセスが多かった 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、前四半期から引き続き WordPress 用のプラグインの脆弱性が多くランクインしました。これは特定の組織より機械的なアクセスを受けたことによるものです。

表 3-1. JVN iPedia の脆弱性対策情報へのアクセス　上位 20 件 [2023 年 10 月～2023 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-2023-000040 WordPress 用プラグイン Appointment and Event Booking Calendar for WordPress - Amelia 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	2023/4/24	10,153
2	JVNDB-2023-000050 WordPress 用プラグイン MW WP Form および Snow Monkey Forms における複数の脆弱性	7.5	8.3	2023/5/15	9,878
3	JVNDB-2022-000087 WordPress における複数の脆弱性	5.0	5.3	2022/11/8	9,586
4	JVNDB-2023-000007 WordPress 用プラグイン Welcart e-Commerce におけるディレクトリトラバーサルの脆弱性	5.0	7.5	2023/1/17	9,509
5	JVNDB-2023-000042 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	2023/5/9	9,480
6	JVNDB-2023-000045 WordPress 用プラグイン VK Blocks および VK All in One Expansion Unit 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	2023/5/9	9,472
7	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	9,447
8	JVNDB-2023-000039 WordPress 用プラグイン LIQUID SPEECH BALLOON 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	2023/4/19	9,446
9	JVNDB-2022-000091 WordPress 用プラグイン WordPress Popular Posts における外部入力の不適切な使用に関する脆弱性	5.0	5.3	2022/11/18	9,435
10	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	9,415
11	JVNDB-2022-000085 WordPress 用プラグイン Salon booking system 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	2022/11/8	9,402

順位	ID/タイトル	CVSSv2 基本値	CVSSv3 基本値	公開日	アクセス数
12	JVNDB-2023-000094 WordPress 用プラグイン Welcart e-Commerce における複数の脆弱性	5.5	5.4	2023/9/22	7,480
13	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	7,262
14	JVNDB-2023-000084 WordPress 用プラグイン Advanced Custom Fields 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	2023/8/21	7,220
15	JVNDB-2022-012258 The JForum Team の Jforum 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	6.8	8.8	2023/8/28	6,808
16	JVNDB-2023-000070 WordPress 用プラグイン TS Webfonts for さくらのレンタルサーバにおける複数の脆弱性	2.6	6.1	2023/7/20	6,781
17	JVNDB-2023-000067 WordPress 用プラグイン Snow Monkey Forms におけるディレクトリトラバーサルの脆弱性	5.0	5.8	2023/6/27	6,778
18	JVNDB-2023-000100 Cisco Secure Email Gateway におけるスキャン回避の問題	-	-	2023/10/16	6,628
19	JVNDB-2023-000048 ASUS ルーター RT-AX3000 における Secure 属性なしの Cookie 使用の脆弱性	2.6	3.7	2023/6/9	6,326
20	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	6,037

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 [2023 年 10 月～2023 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-2023-001926 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	-	7.6	2023/5/23	5,269
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	5,231
3	JVNDB-2023-001008 Hitachi Tuning Manager におけるファイルおよびディレクトリパーミッションの脆弱性	-	6.6	2023/1/18	5,217
4	JVNDB-2023-001269 Hitachi Automation Director, Hitachi Infrastructure Analytics Advisor および Hitachi Ops Center 製品におけるファイルおよびディレクトリパーミッションの脆弱性	-	6.6	2023/3/1	5,207
5	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	5,127