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 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、2020 年 10 月 1 日から 2020 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

2021 年 1 月 20 日

目次

1. 2020 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 125,388 件～

2020 年第 4 四半期（2020 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 125,388 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 2,217 件になりました。

表 1-1. 2020 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	3 件	246 件
	JVN	179 件	9,705 件
	NVD	1,241 件	115,437 件
	計	1,423 件	125,388 件
英語版	国内製品開発者	3 件	244 件
	JVN	26 件	1,973 件
	計	29 件	2,217 件

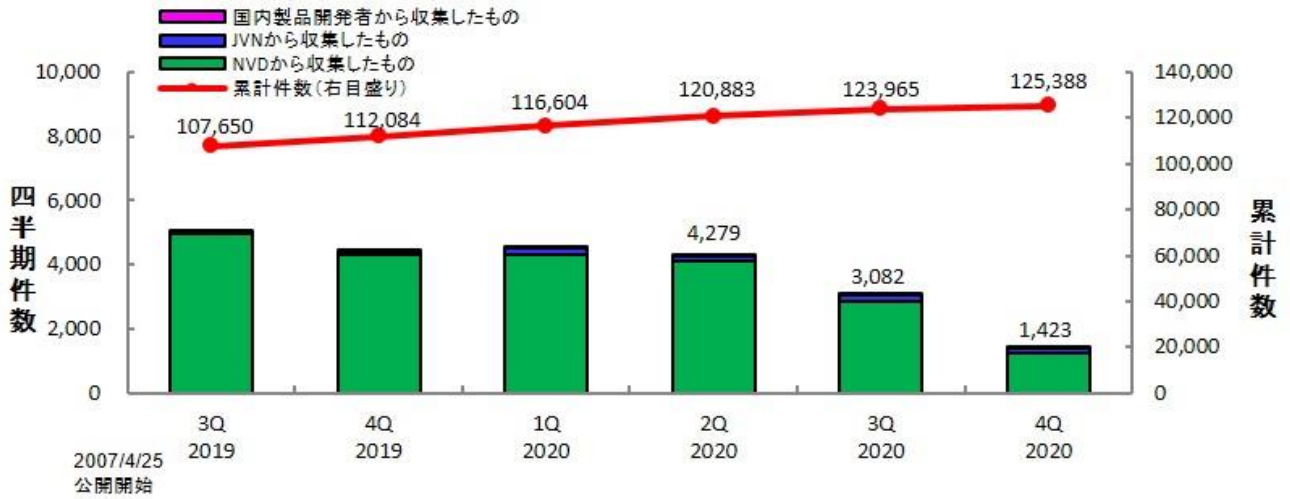

図 1-1. JVN iPedia の登録件数の四半期別推移

(*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】「Zerologon」と呼ばれる Microsoft Server 製品の脆弱性について
～「Zerologon（CVE-2020-1472)」の脆弱性は最も深刻度の高い「危険」に分類。その他の Microsoft Server 製品の脆弱性も多数「危険」に分類される～

「Zerologon」と呼ばれる脆弱性（CVE-2020-1472）は、Windows Server 製品のドメインコントローラ機能で使われる「Netlogon Remote Protocol（MS-NRPC)」に発見された特権昇格の脆弱性です。本脆弱性を悪用され、攻撃者にドメインの管理者権限を奪われてしまうと、組織の重要な機密情報が窃取される、ドメインに参加している PC が攻撃者に乗っ取られる等の被害につながるおそれがあり、多くのセキュリティ機関で注意が呼びかけられました。本脆弱性は 2020 年 8 月に Microsoft 社から脆弱性対策情報(*4)が提供された際、CVSSv3 基本値は深刻度が最も高い 10.0 に評価されており、後に Microsoft 社から本脆弱性を悪用する攻撃を確認したとの情報も公開(*5)されたため、利用者は早急に対応を行う必要がありました。

また、「Zerologon」の脆弱性（CVE-2020-1472）に対する修正プログラムは 2020 年 8 月にリリースされましたが、「Netlogon Remote Protocol」が Windows 以外の製品にも実装されていることから、Microsoft 社はそれらの製品との互換性を考慮し、本脆弱性への対処を 2 段階に分けて実施すると発表(*6)しました。ソフトウェア製品の利用者およびシステム管理者は、Microsoft 社が案内している専用のガイダンスページを参照の上、自組織で必要となる作業を把握し、2 段階目のリリース（2021 年 2 月 9 日公開予定）時には早急に対応できるよう準備を行ってください。

一方、「Zerologon」以外にも 2020 年は Microsoft Server 製品の脆弱性が多数公開されています。図 1-2 は、2020 年の 1 年間（1 月 1 日～12 月 31 日）と第 4 四半期（10 月 1 日～12 月 31 日）に JVN iPedia へ登録された Microsoft Server 製品に関する脆弱性対策情報の深刻度別割合です。1 年間に登録された脆弱性のうち、深刻度が最も高い「危険」（CVSS 基本値=7.0～10.0）に分類された脆弱性が 78%、その次に高い「警告」（CVSS 基本値=4.0～6.9）が 21%、「注意」（CVSS 基本値=0.1～3.9）が 1%となっており、重大な被害につながる「危険」の脆弱性が 7 割を占めています。また、直近の第 4 四半期（10 月 1 日～12 月 31 日）においても、その「危険」の脆弱性が 7 割を占めていることから、2021 年も引き続き同様の傾向が続くおそれがあります。

(*4) Netlogon の特権の昇格の脆弱性
https://msrc.microsoft.com/update-guide/ja-JP/vulnerability/CVE-2020-1472
(*5) Attacks exploiting Netlogon vulnerability (CVE-2020-1472)
https://msrc-blog.microsoft.com/2020/10/29/attacks-exploiting-netlogon-vulnerability-cve-2020-1472/
(*6) [AD 管理者向け] CVE-2020-1472 Netlogon の対応ガイダンスの概要
https://msrc-blog.microsoft.com/2020/09/14/20200915_netlogon/

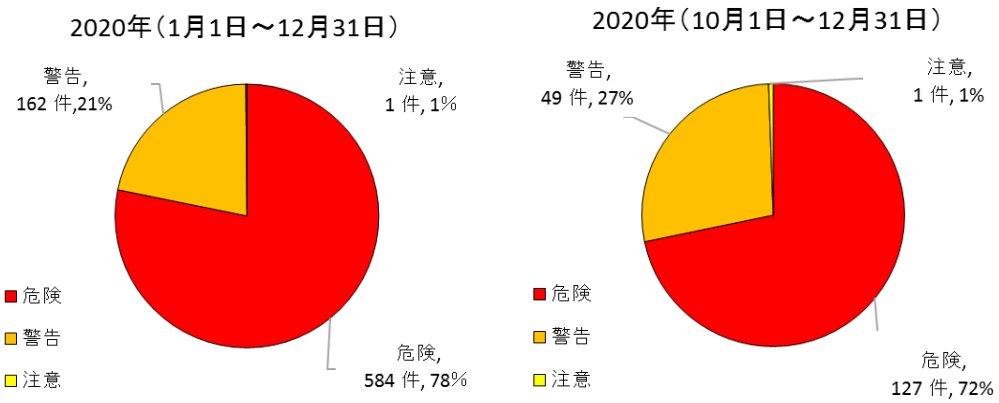

図 1-2.　2020 年の 1 年間（1 月 1 日～12 月 31 日）と第 4 四半期（10 月 1 日～12 月 31 日）に JVN iPedia へ登録された Microsoft Server 製品の深刻度別割合（CVSSv2）

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[*7]」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。なお、「icat」(Flash 版) に関しては、2020 年 12 月 31 日の Adobe Flash Player の廃止[*8]に伴い、2021 年 1 月 4 日に提供を終了しておりますので、「icat」(Flash 版)をご利用いただいていたウェブサイトの管理者は早期に「icat for JSON」への移行をお願いします。

[*7] 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
[*8] Adobe Flash Player サポート終了情報ページ
https://www.adobe.com/jp/products/flashplayer/end-of-life.html

1-3. 【注目情報 2】テレワーク等で使われるソフトウェアの脆弱性について

～VPN 製品や Web 会議サービス等の脆弱性を標的とするサイバー攻撃が発生。テレワークを継続的に行うために組織全体でセキュリティ対策の見直しを～

新型コロナウイルス感染症（COVID-19）の影響により、テレワークの普及が急速に進んだ一方で、テレワーク環境で使われる VPN 製品や Web 会議サービス等の脆弱性を狙ったサイバー攻撃が行われ、IPA を含むセキュリティ機関からテレワーク実施に関して注意が呼びかけられました。テレワークで利用する VPN 製品や Web 会議サービスのソフトウェアは、利用者が初めて使うものや緊急時用に導入したまま使われていなかったソフトウェアも多く、情報の収集先やアップデートの適用方法を知らないまま利用を続けているケースが少なからずあると考えられます。しかし、脆弱性対策が不十分なまま利用を続けてしまうと、攻撃者に脆弱性を悪用され、ソフトウェアの認証情報や組織の機密情報が外部に流出する等の被害に遭ってしまうおそれがあります。実際に、攻撃者がそうした重要な情報を窃取するため、テレワーク環境を標的とした攻撃を行っているとの情報も公開[*9]されており、テレワーク実施の際は十分注意する必要があります。

2019 年および 2020 年に JPCERT/CC より、悪用される可能性がある複数の VPN 製品について注意喚起等[*10][*11][*12][*13]が公開されました。図 1-3 は、2020 年に JVN iPedia へ登録された、それらの注意喚起等に記載されている VPN 製品、左から Palo Alto Networks 社製の VPN（PAN-OS）、Fortinet 社製の VPN（FortiOS）、Pulse Secure 社製の VPN（Pulse Policy Secure と Pulse Connect Secure を含む）に関する脆弱性対策情報の深刻度別割合です。いずれも「危険」と「警告」に分類される脆弱性を合わせると 95%以上を占めており、ベンダから修正プログラムがリリースされた際には早急に対応を行うことが求められます。特に注意喚起等が行われている脆弱性については、悪用される可能性が高いため、アップデートの見落としがないか十分に確認するようにしてください。

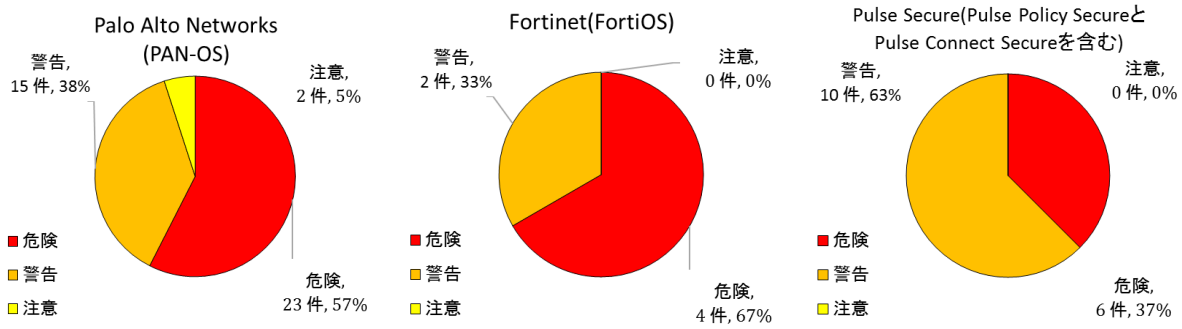

図 1-3.　2020 年に登録された VPN 製品の深刻度別割合（CVSSv2）

[*9] リモート接続ねらうサイバー攻撃が急増 テレワーク増加で
https://www3.nhk.or.jp/news/html/20201112/k10012708711000.html

[*10] 複数の SSL VPN 製品の脆弱性に関する注意喚起
https://www.jpcert.or.jp/at/2019/at190033.html

[*11] Palo Alto Networks 製品の脆弱性（CVE-2020-2021）について
https://www.jpcert.or.jp/newsflash/2020063001.html

[*12] Fortinet 社製 FortiOS の SSL VPN 機能の脆弱性（CVE-2018-13379）の影響を受けるホストに関する情報の公開について
https://www.jpcert.or.jp/newsflash/2020112701.html

[*13] Pulse Connect Secure の脆弱性への対策や侵害有無などの確認を
https://www.jpcert.or.jp/newsflash/2020041701.html

図 1-4 は、2020 年に JVN iPedia へ登録された Web 会議サービス、左から Microsoft 社製の Microsoft Teams、Cisco System 社製の Cisco Webex Meetings（Desktop と Online を含む）、Zoom Video Communications 社製の Zoom（Client と Meetings を含む）に関する脆弱性対策情報の深刻度別割合です。件数としては少ないですが、図 1-3 の VPN 製品の深刻度別割合と同様に、「危険」や「警告」が占める割合が多く注意が必要です。この内、Zoom に関しては、2020 年 4 月 3 日に IPA より、注意喚起[*14]をしています。

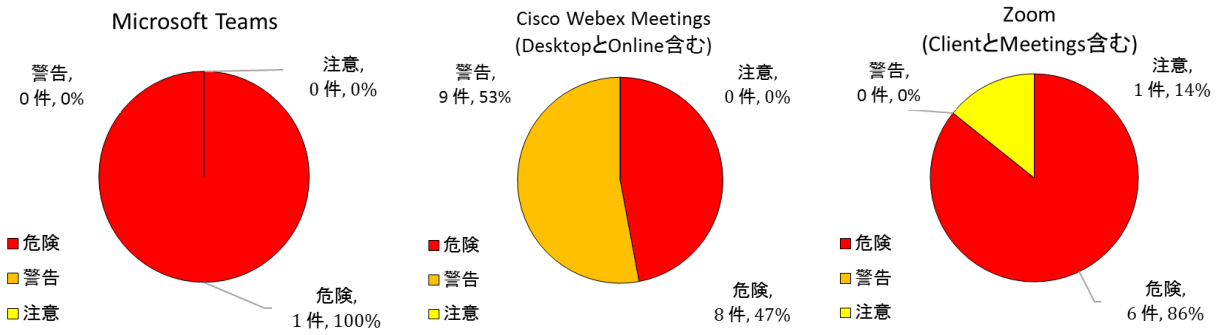

図 1-4.　2020 年に登録された Web 会議サービスの深刻度別割合（CVSSv2）

VPN 製品や Web 会議サービス等の脆弱性を悪用しようとする攻撃を未然に防ぐためには、利用しているソフトウェアの脆弱性対策情報を日ごろから収集するようにし、ベンダから修正プログラムがリリースされた際には速やかに適用する等の対策実施を行うことが求められます。また、クライアント側のソフトウェアだけではなく、自組織でサーバを構築している場合は、サーバ側のソフトウェアについても同様の対応が必要です。さらに、システム管理者は外部からサイバー攻撃を受けた形跡がないか等の確認を行い、適宜、組織内の手続きや対策の見直しを行うことが重要となります。

IPA では、テレワーク環境で働く勤務者を対象とした「テレワークを行う際のセキュリティ上の注意事項[*15]」や、Web 会議サービスの利用において留意すべきセキュリティ上のポイントをまとめた「Web 会議サービスを使用する際のセキュリティ上の注意事項[*16]」を公開しています。テレワークや Web 会議を実施する際は事前にこれらの資料を参照し、安全な状態で実施できるよう準備を行ってください。また、テレワークを継続的に行う場合には、NISC（内閣サイバーセキュリティセンター）から案内[*17]されているように、情報セキュリティリスクの再評価や情報セキュリティ関連規程の確認と必要に応じた改定等を行うことも重要です。

[*14] Zoom の脆弱性対策について
https://www.ipa.go.jp/security/ciadr/vul/alert20200403.html
[*15] テレワークを行う際のセキュリティ上の注意事項
https://www.ipa.go.jp/security/announce/telework.html
[*16] Web 会議サービスを使用する際のセキュリティ上の注意事項
https://www.ipa.go.jp/security/announce/webmeeting.html
[*17] テレワーク等への継続的な取組に際しての留意事項(注意喚起)
https://www.nisc.go.jp/active/general/pdf/telework20200611.pdf

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 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-269（不適切な権限管理）が 138 件、CWE-79（クロスサイトスクリプティング）が 136 件、CWE-20（不適切な入力確認）が 84 件、CWE-200（情報漏えい）が 75 件、CWE-787（境界外書き込み）が 46 件でした。最も件数の多かった CWE-269（不適切な権限管理）は、悪用されると管理者権限を取得され、システムが変更され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**[*18]」、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**[*19]」や「**IPA セキュア・プログラミング講座**[*20]」、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**[*21]」などを公開しています。

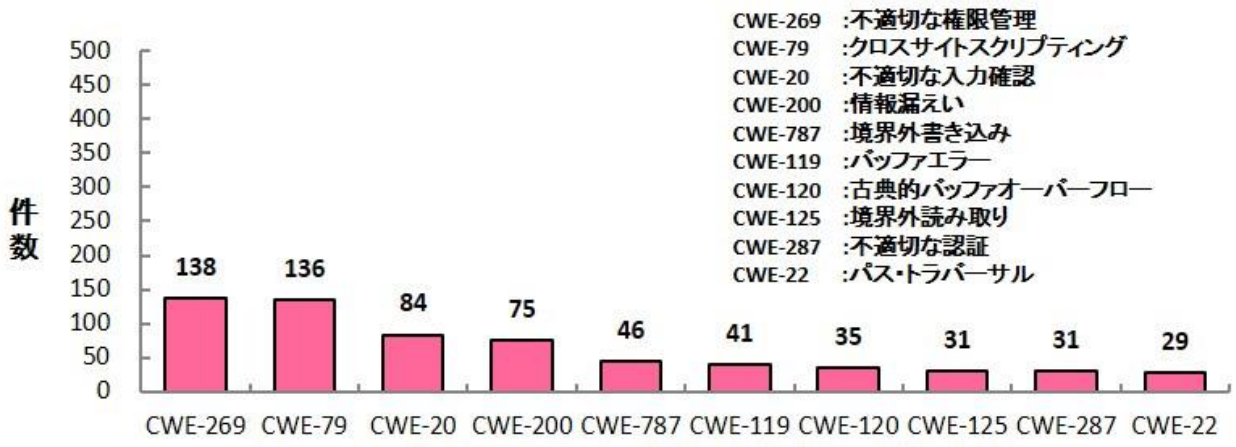

図 2-1. 2020 年第 4 四半期に登録された脆弱性の種類別件数

[*18] 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

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

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

[*21] 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 23.7%、レベルⅡが 61.9%、レベルⅠが 14.4%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 85.6%を占めています。

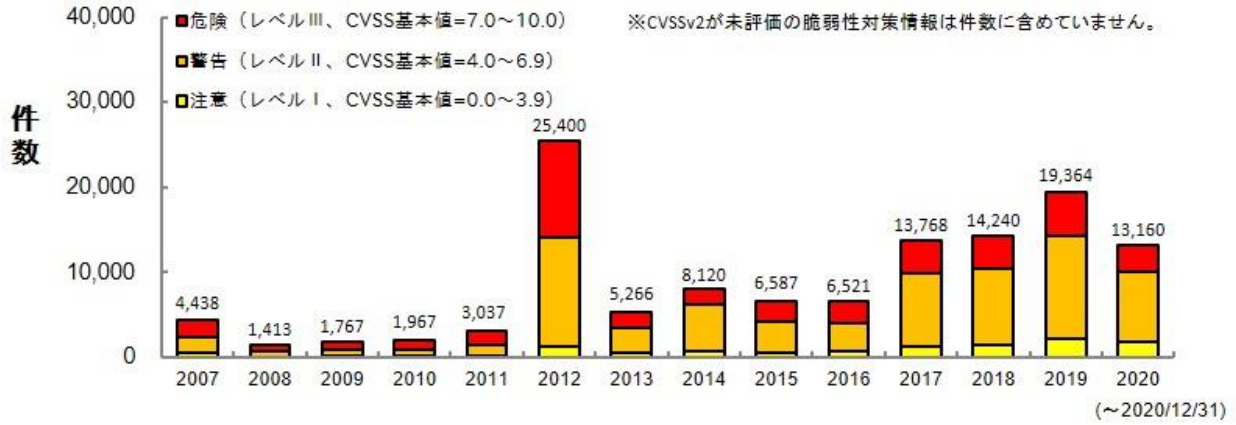

図 2-2. 脆弱性の深刻度別件数(CVSSv2)

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 14.8%、「重要」が 42.5%、「警告」が 40.6%、「注意」が 2.1%となっています。

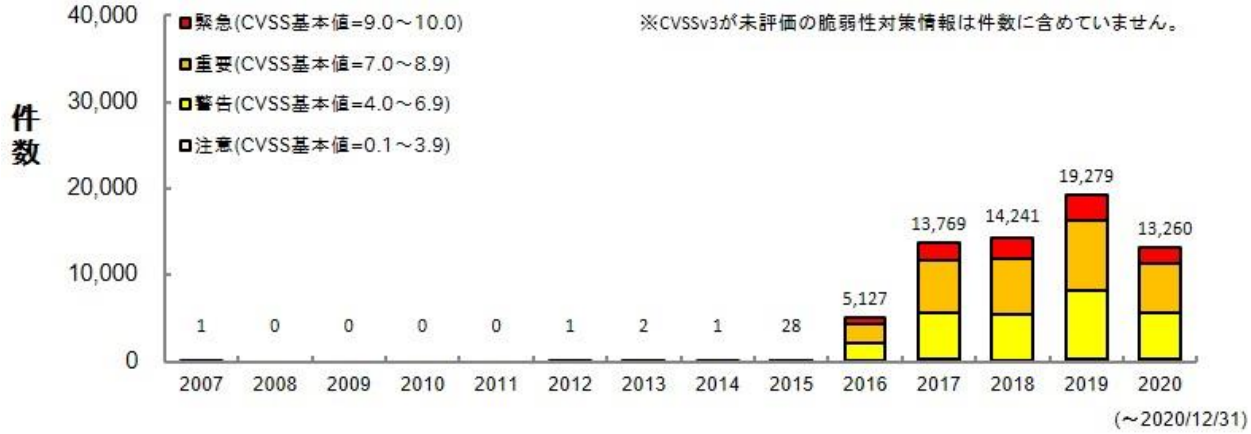

図 2-3. 脆弱性の深刻度別件数(CVSSv3)

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 [*22] で公開しています。

[*22] 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%（9,104 件／全 13,304 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 2,815 件を登録しています。

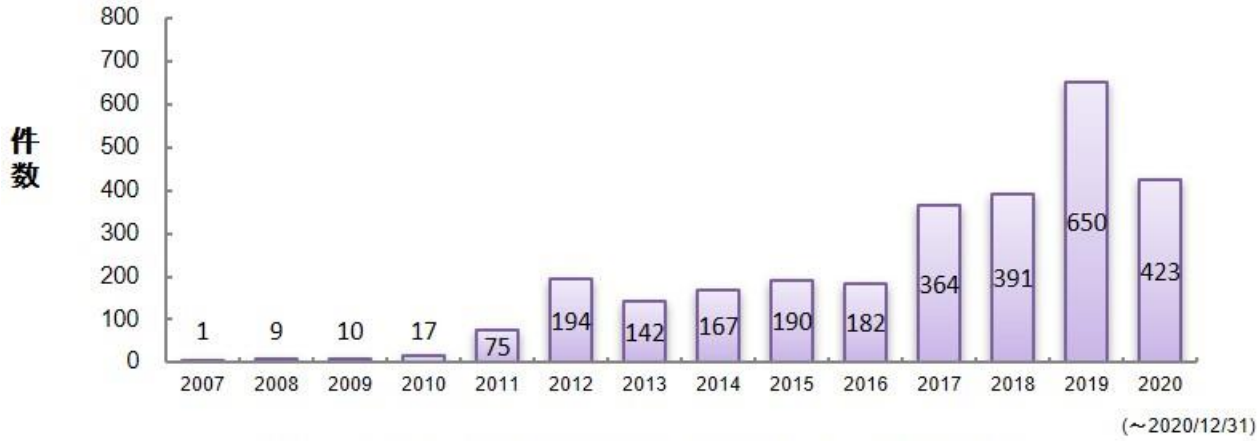

図 2-5. JVN iPedia 登録件数（産業用制御システムのみ抽出）

2-4. 脆弱性対策情報の製品別登録状況

表 2-1 は 2020 年第 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 [*23] 。

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 10 月～2020 年 12 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)	184
2	OS	Microsoft Windows Server (マイクロソフト)	177
3	OS	Microsoft Windows Server 2019 (マイクロソフト)	165
4	OS	Microsoft Windows Server 2016 (マイクロソフト)	143
5	OS	Microsoft Windows Server 2012 (マイクロソフト)	96
6	OS	Microsoft Windows 8.1 (マイクロソフト)	86
6	OS	Microsoft Windows Server 2008 (マイクロソフト)	86
8	OS	Microsoft Windows RT 8.1 (マイクロソフト)	83
9	OS	Microsoft Windows 7 (マイクロソフト)	78
10	ファームウェア	Qualcomm component (クアルコム)	69
11	ミドルウェア	MySQL (オラクル)	48
12	OS	iOS (アップル)	46
12	OS	iPadOS (アップル)	46
14	ファイル・情報共有ソフトウェア	Microsoft SharePoint Server (マイクロソフト)	36
15	OS	Apple Mac OS X　(アップル)	35
16	OS	watchOS (アップル)	34
17	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)	33
18	OS	tvOS (アップル)	32
19	業務用ソフトウェア	Microsoft Office (マイクロソフト)	29
19	業務用ソフトウェア	Microsoft 365 Apps (マイクロソフト)	29

[*23] 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 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。

本四半期の 1 位、2 位、3 位、4 位、9 位は 2020 年 7 月に公開した WordPress 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。

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 10 月～2020 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-2020-006830	WordPress 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	2020/7/20	10,787
2	JVNDB-2020-006831	WordPress におけるクロスサイトスクリプティングの脆弱性	3.5	6.8	2020/7/20	10,646
3	JVNDB-2020-006893	WordPress における代替パスまたはチャネルを使用した認証回避に関する脆弱性	6.0	3.1	2020/7/22	10,636
4	JVNDB-2020-006788	WordPress におけるクロスサイトスクリプティングの脆弱性	3.5	2.4	2020/7/17	10,620
5	JVNDB-2020-009481	Firefox および Thunderbird における境界外書き込みに関する脆弱性	9.3	8.8	2020/11/9	9,504
6	JVNDB-2020-000074	Hibernate ORM における SQL インジェクションの脆弱性	4.0	7.4	2020/11/19	9,393
7	JVNDB-2020-009073	KDE Ark におけるパストラバーサルの脆弱性	4.3	3.3	2020/10/16	9,226
8	JVNDB-2020-000067	複数のエレコム製 LAN ルーターにおける OS コマンドインジェクションの脆弱性	5.8	8.8	2020/10/5	9,136
9	JVNDB-2020-006832	WordPress におけるオープンリダイレクトの脆弱性	4.9	5.7	2020/7/20	8,938
10	JVNDB-2020-000066	InfoCage SiteShell においてサービス実行ファイルが書き換え可能な脆弱性	6.8	7.8	2020/9/30	8,852
11	JVNDB-2020-008942	Kubernetes ingress-nginx コンポーネントにおける別領域リソースに対する外部からの制御可能な参照に関する脆弱性	4.9	5.9	2020/10/8	8,849
12	JVNDB-2018-016161	Cloudera CDH における不適切なデフォルトパーミッションに関する脆弱性	6.5	7.2	2019/12/16	8,594
13	JVNDB-2020-008931	トレンドマイクロ株式会社製ウイルスバスター for Mac に権限昇格の脆弱性	なし	7.8	2020/10/7	8,321
14	JVNDB-2020-008821	CMONOS.JP におけるクロスサイトスクリプティングの脆弱性	なし	6.1	2020/9/28	8,010
15	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	7,933
16	JVNDB-2020-009467	XOOPS 用モジュール XooNIps における複数の脆弱性	なし	6.3	2020/11/9	7,796

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-2020-006469	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	7,695
18	JVNDB-2020-000068	WordPress 用プラグイン Live Chat - Live support 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	2020/10/14	7,663
19	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	7,661
20	JVNDB-2020-000055	Apache Struts 2 にサービス運用妨害 (DoS) の脆弱性	4.3	5.9	2020/8/25	7,629

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 10 月～2020 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-2020-007128	HiRDB における DoS 脆弱性	なし	なし	2020/8/3	4,474
2	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	4,467
3	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	4,327
4	JVNDB-2020-005743	Cosminexus HTTP Server における脆弱性	なし	なし	2020/6/22	4,270
5	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	4,266

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