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

[2021 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、2021 年 10 月 1 日から 2021 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

2022 年 1 月 19 日

目次

1. 2021 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】Microsoft Windows 製品の脆弱性について ..... - 3 -
1-3. 【注目情報 2】Apache HTTP Server の脆弱性について ..... - 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. 2021 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 137,702 件～

2021 年第 4 四半期（2021 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 137,702 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 2,375 件になりました。

表 1-1. 2021 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	261 件
	JVN	358 件	10,814 件
	NVD	4,313 件	126,627 件
	計	4,676 件	137,702 件
英語版	国内製品開発者	5 件	256 件
	JVN	33 件	2,119 件
	計	38 件	2,375 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】Microsoft Windows 製品の脆弱性について
～2021 年 10 月にリリースされた Microsoft Windows 11 にも深刻度の高い脆弱性。引き続き脆弱性対策を～

マイクロソフト社より、Windows 11 が 2021 年 10 月 5 日（日本時間）にリリースされました。本製品は Windows 10 の後継バージョンとして注目を集め、無償でアップグレードすることができるため、徐々に利用者が増えている状況です。同社は、Windows 11 は様々な新機能に加え、セキュリティ面もゼロトラストの考え方を取り入れるなど強化しているとしています。[*4]

一方、Windows 11 において既に多くの脆弱性が公開されています。リリースされてから 2021 年 12 月末までに、89 件の Windows 11 の脆弱性対策情報が JVN iPedia に登録されました。その中には、深刻度の高い脆弱性も含まれています。図 1-2 は、2021 年第 4 四半期（10 月 1 日～12 月 31 日）に JVN iPedia へ登録された、現在マイクロソフト社でサポートされている Windows 8.1、Windows 10、Windows 11 の脆弱性対策情報の深刻度別割合です。Windows 11 においては、脆弱性の深刻度が最も高い「危険」（CVSS 基本値=7.0～10.0）が 12.4%、次に高い「警告」（CVSS 基本値=4.0～6.9）が 70.8%、「注意」（CVSS 基本値=0.1～3.9）が 16.9%となっており、「危険」および「警告」にあたる脆弱性が全体の 8 割以上を占めています。また、Windows 8.1、Windows 10 と比較してみても深刻度別割合に大きな差はみられませんでした。このことから、2022 年以降も Windows 11 は、これまでの Windows OS と同様の傾向で脆弱性対策情報が公開されると見られます。

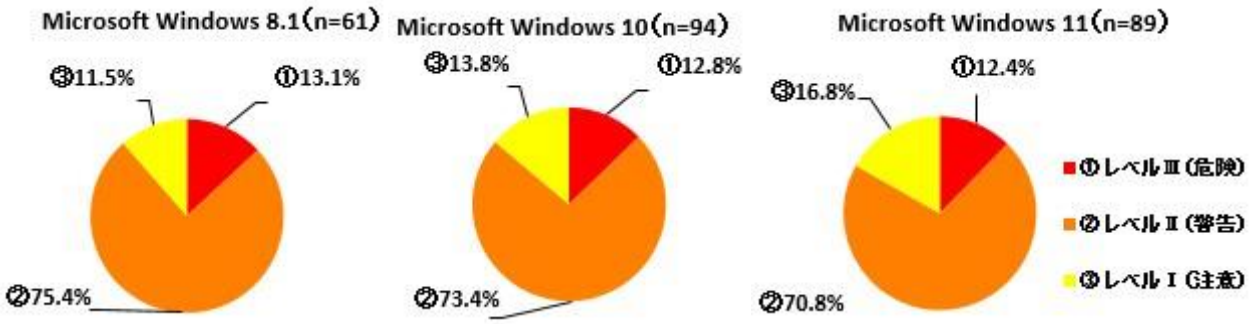

図 1-2. 2021 年第 4 四半期（10 月 1 日～12 月 31 日）に JVN iPedia へ登録された Microsoft Windows 8.1、Windows 10、Windows 11 の深刻度別割合（CVSSv2）

これらの脆弱性を解消し安全に Windows 11 を利用するためには、利用者は従来の Windows 製品と同様にマイクロソフト社から公開されるセキュリティパッチを速やかに適用することが推奨されます。IPA においても、同社から月例のセキュリティパッチが公開された場合、重要なセキュリティ情報として注意喚起情報を公開しており、特に脆弱性攻撃が確認されている場合は緊急対策情報として発信しています。また、その情報を組織に所属する従業員や公開しているサービスの利用者等にい

[*4] Windows 11: ハイブリッド ワークと学習のためのオペレーティング システム
https://blogs.windows.com/japan/2021/06/25/windows-11-the-operating-system-for-hybrid-work-and-learning/

ち早く情報を発信する「icat for JSON[*5]」というサービスも提供していますので、こちらもご活用ください。

[*5] 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】Apache HTTP Server の脆弱性について
～パストラバーサルの脆弱性(CVE-2021-41773)を悪用する攻撃が国内で確認される～

2021 年 10 月に、Apache Software Foundation から Apache HTTP Server の脆弱性 CVE-2021-41773 の情報が公開され、IPA をはじめ複数の公的機関から脆弱性の悪用が確認されたとして注意喚起が発信されました。[(*6)(*7)]本脆弱性はドキュメントルート外のファイルにアクセスされるおそれのあるパストラバーサルの脆弱性で、これを悪用されるとリモートの攻撃者に不正にファイルを操作されるおそれがありました。脆弱性の深刻度を示す CVSSv2 基本値は 4.3[(*8)]で二番目に深刻度が高い「警告」（CVSS 基本値=4.0～6.9）にあたりますが、特別高い数値ではありませんでした。しかし、複数の実証コードが公開され、国内での攻撃が確認されたこともあり、脆弱性の影響を受けるバージョンを利用している組織は対策が求められました。

また、CVE-2021-41773 の修正版としてリリースされたバージョンの Apache HTTP Server にも、数日で別のパストラバーサルの脆弱性 CVE-2021-42013 が存在することが明らかになりました。本脆弱性は、CVSSv2 基本値は 7.5[(*9)]で深刻度が最も高い「危険」（CVSS 基本値=7.0～10.0）に分類されました。CVE-2021-41773 と同様本脆弱性も実証コードの公開が確認され、また、CVE-2021-41773 の修正版のリリース直後に発見された脆弱性ということもあり、ネット記事等にも掲載され[(*10)]、広く注目されました。

Apache HTTP Server は、Apache Software Foundation がオープンソースソフトウェアとして提供しているウェブサーバ用のプログラムです。本製品の脆弱性対策情報は、JVN iPedia に 2021 年末までの累計で 194 件登録されています。図 1-3 はその深刻度別割合を示したものです。脆弱性の深刻度が最も高い「危険」（CVSS 基本値=7.0～10.0）が 12.4%、次に高い「警告」（CVSS 基本値=4.0～6.9）が 82.0%、「注意」（CVSS 基本値=0.1～3.9）が 4.1%となっており、ほとんどが「危険」および「警告」にあたり、脆弱性を悪用された場合の影響が大きいものが大半を占めています。

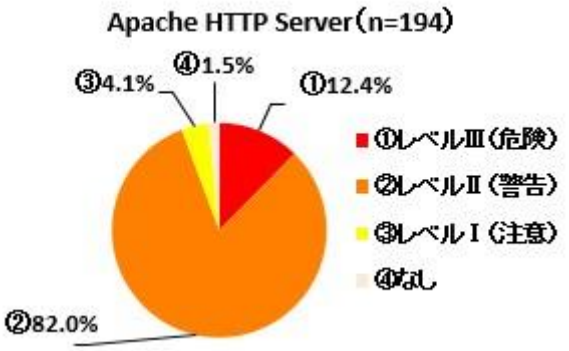

図 1-3. JVN iPedia に登録された Apache HTTP Server の深刻度別割合（CVSSv2）

(*6) 更新：Apache HTTP Server の脆弱性対策について(CVE-2021-41773, CVE-2021-42013)
https://www.ipa.go.jp/security/ciadr/vul/alert20211006.html

(*7) Apache HTTP Server のパストラバーサルの脆弱性（CVE-2021-41773）に関する注意喚起
https://www.jpcert.or.jp/at/2021/at210043.html

(*8) CVE-2021-41773
https://nvd.nist.gov/vuln/detail/CVE-2021-41773

(*9) CVE-2021-42013
https://nvd.nist.gov/vuln/detail/CVE-2021-42013

(*10) わずか 3 日、「Apache HTTPD」が再修正 - 前回修正は不十分、RCE のおそれも
https://www.security-next.com/130520

Apache HTTP Server のように広く利用されているソフトウェアは、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。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、2021 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 501 件、CWE-787（境界外書き込み）が 274 件、CWE-269（不適切な権限管理）が 172 件、CWE-89（SQL インジェクション）が 165 件、CWE-125（境界外読み取り）が 145 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**[(*11)]」、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**[(*12)]」や「**IPA セキュア・プログラミング講座**[(*13)]」、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**[(*14)]」などを公開しています。

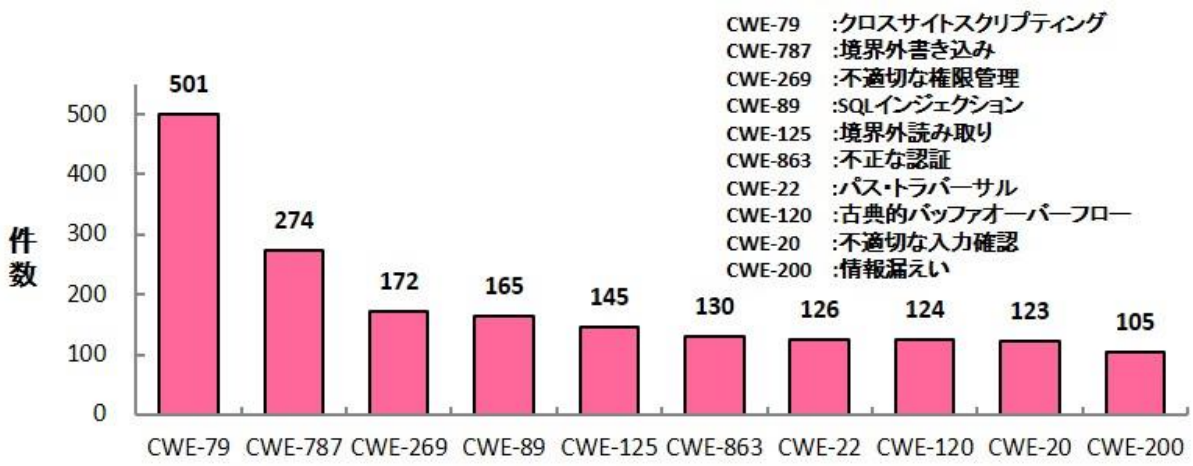

図 2-1. 2021 年第 4 四半期に登録された脆弱性の種類別件数

(*11) 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
(*12) IPA：「安全なウェブサイトの作り方」
https://www.ipa.go.jp/security/vuln/websecurity.html
(*13) IPA：「IPA セキュア・プログラミング講座」
https://www.ipa.go.jp/security/awareness/vendor/programming/
(*14) 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。

2021 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 22.2%、レベルⅡが 62.2%、レベルⅠが 15.6%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 84.4%を占めています。

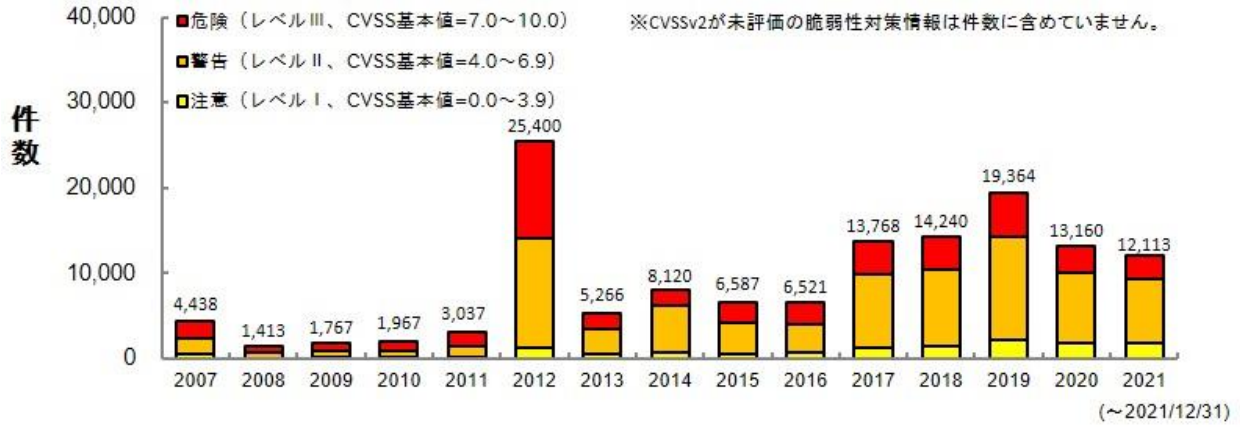

図 2-2. 脆弱性の深刻度別件数(CVSSv2)

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。

2021 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 14.1%、「重要」が 42.3%、「警告」が 41.0%、「注意」が 2.5%となっています。

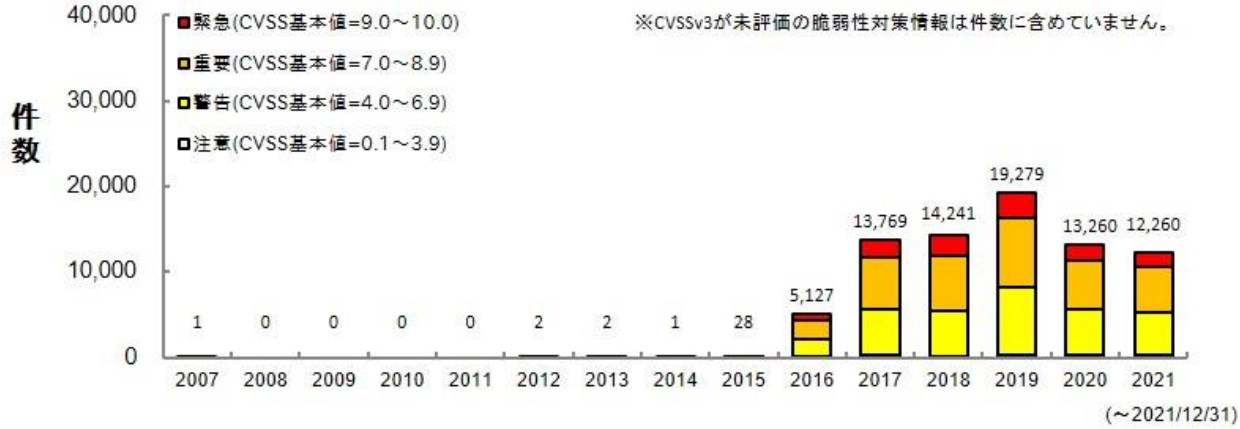

図 2-3. 脆弱性の深刻度別件数(CVSSv3)

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 [*15] で公開しています。

[*15] 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。2021 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、2021 年の件数全件の約 72.1%（8,884 件／全 12,314 件）を占めています。

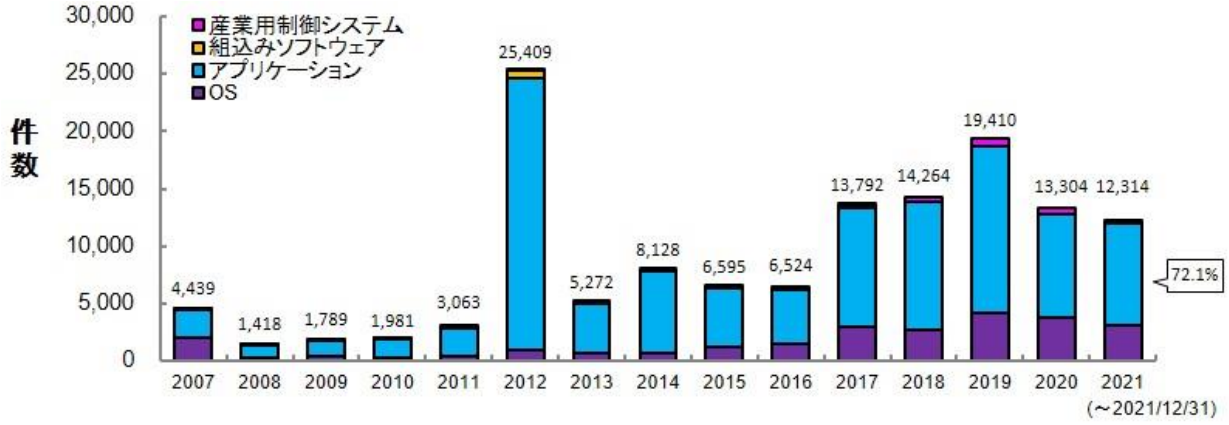

図 2-4. 脆弱性対策情報を公表した製品の種類別件数の公開年別推移

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 3,198 件を登録しています。

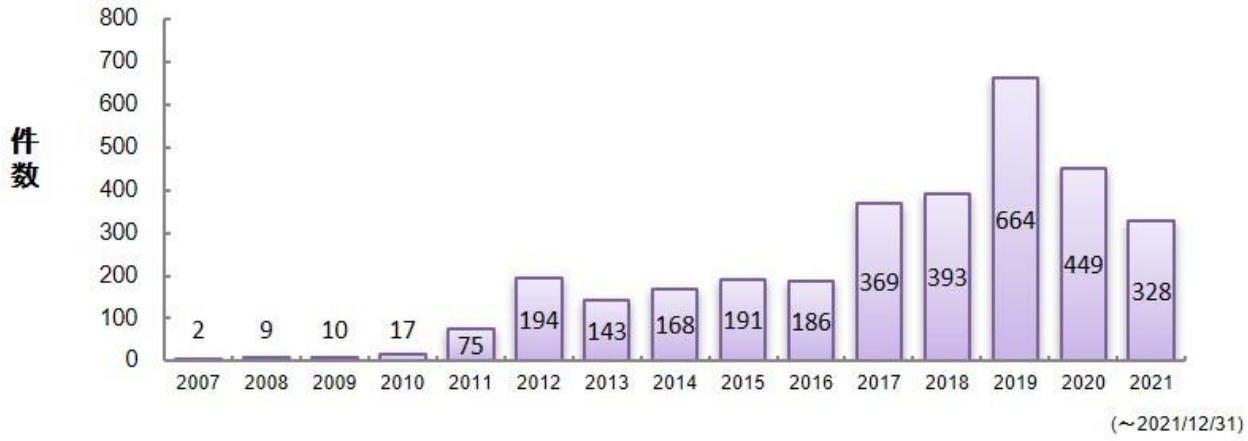

図 2-5. JVN iPedia 登録件数（産業用制御システムのみ抽出）

2-4. 脆弱性対策情報の製品別登録状況

表 2-1 は 2021 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クアルコム製品でした。2021 年は第 1 四半期、第 2 四半期、第 4 四半期においてクアルコム製品が四半期中に最も登録された製品となりました。

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 [(*16)] 。

表 2-1. 製品別 JVN iPedia の脆弱性対策情報登録件数　上位 20 件 [2021 年 10 月～2021 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)	979
2	OS	Fedora (Fedora Project)	292
3	OS	Debian GNU/Linux (Debian)	186
4	OS	Android (Google)	155
5	ブラウザ	Google Chrome (Google)	110
6	OS	Microsoft Windows Server (マイクロソフト)	102
7	OS	Microsoft Windows Server 2022 (マイクロソフト)	98
8	OS	Microsoft Windows 10 (マイクロソフト)	96
9	OS	Microsoft Windows Server 2019 (マイクロソフト)	95
10	OS	Microsoft Windows 11 (マイクロソフト)	89
11	OS	Microsoft Windows Server 2016 (マイクロソフト)	81
12	その他	OnCommand Insight (NetApp)	68
12	OS	Microsoft Windows Server 2012 (マイクロソフト)	68
14	OS	Microsoft Windows 8.1 (マイクロソフト)	63
15	OS	Microsoft Windows RT 8.1 (マイクロソフト)	62
16	OS	Linux Kernel (Kernel.org)	56
17	その他	SnapCenter (NetApp)	55
17	OS	Red Hat Enterprise Linux (レッドハット)	55
17	OS	Microsoft Windows Server 2008 (マイクロソフト)	55
20	OS	Microsoft Windows 7　(マイクロソフト)	51

[(*16)] 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 2021 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 位はいずれも国内で脆弱性を悪用した攻撃が確認され、話題になったものです。特に 2 位の Apache Log4j の脆弱性は 2021 年 12 月 14 日の公開であったにもかかわらず、12 月末時点でアクセス数が 10,000 件を超えました。

表 3-1. JVN iPedia の脆弱性対策情報へのアクセス　上位 20 件 [2021 年 10 月～2021 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-2021-000093	Movable Type の XMLRPC API における OS コマンドインジェクションの脆弱性	7.5	9.8	2021/10/20	10,265
2	JVNDB-2021-005429	Apache Log4j における任意のコードが実行可能な脆弱性	9.3	10.0	2021/12/14	10,196
3	JVNDB-2021-000090	Apache HTTP Server におけるディレクトリトラバーサルの脆弱性	5.0	7.5	2021/10/8	7,671
4	JVNDB-2019-013606	Log4j における信頼性のないデータのデシリアライゼーションに関する脆弱性	7.5	9.8	2020/1/10	6,567
5	JVNDB-2021-000088	サイボウズ リモートサービスにおける複数の脆弱性	6.3	5.3	2021/9/30	6,411
6	JVNDB-2021-002774	トレンドマイクロ製 ServerProtect における認証回避の脆弱性	-	-	2021/10/1	6,264
7	JVNDB-2021-000089	スマートフォンアプリ「Nike」における Custom URL Scheme の処理にアクセス制限不備の脆弱性	4.3	4.3	2021/10/8	5,971
8	JVNDB-2021-000097	CLUSTERPRO X および EXPRESSCLUSTER X における複数の脆弱性	10.0	9.8	2021/10/29	5,763
9	JVNDB-2021-000022	サイボウズ Office に複数の脆弱性	4.0	4.3	2021/3/15	5,675
10	JVNDB-2021-002810	Hitachi Tuning Manager、Hitachi Infrastructure Analytics Advisor および Hitachi Ops Center Analyzer における情報露出の脆弱性	-	-	2021/10/5	5,610
11	JVNDB-2021-002752	トレンドマイクロ製スマートホームスキャナー (Windows 版) における権限昇格の脆弱性	-	-	2021/9/30	5,521
12	JVNDB-2021-000085	iOS アプリ「スニーカーダンク スニーカーフリマアプリ」におけるサーバ証明書の検証不備の脆弱性	4.0	4.8	2021/9/28	5,395
13	JVNDB-2021-000091	128 Technology Session Smart Router における認証不備の脆弱性	7.5	9.8	2021/10/18	5,297
14	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	5,162
15	JVNDB-2021-003080	オムロン製 CX-Supervisor における領域外のメモリ参照の脆弱性	-	6.5	2021/10/18	5,142
16	JVNDB-2021-000084	スマートフォンアプリ「InBody」における情報漏え	2.9	3.5	2021/9/28	5,141

順位	ID	タイトル	CVSSv2 基本値	CVSSv3 基本値	公開日	アクセス数
		いの脆弱性				
17	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	5,116
18	JVNDB-2020-005296	Apache log4net における XML 外部エンティティの脆弱性	7.5	9.8	2020/6/11	5,029
19	JVNDB-2021-000081	シャープ NEC ディスプレイソリューションズ製パブリックディスプレイにおける複数の脆弱性	10.0	9.8	2021/9/17	5,023
20	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	4,993

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 [2021 年 10 月～2021 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-2021-002810	Hitachi Tuning Manager、Hitachi Infrastructure Analytics Advisor および Hitachi Ops Center Analyzer における情報露出の脆弱性	-	-	2021/10/5	5,610
2	JVNDB-2021-003660	Hitachi Device Manager における認証バイパスの脆弱性	-	-	2021/11/1	4,230
3	JVNDB-2021-003811	Hitachi Automation Director、Hitachi Infrastructure Analytics Advisor および Hitachi Ops Center 製品におけるファイルパーミッションの脆弱性	-	-	2021/11/5	4,223
4	JVNDB-2021-001021	JP1/IT Desktop Management 2 - Manager、JP1/NETM/Asset Information Manager におけるアクセス制御不備による脆弱性	-	-	2021/2/8	4,034
5	JVNDB-2021-001345	Cosminexus 運用管理機能における情報露出の脆弱性	-	-	2021/4/13	4,023

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

2019 年以前の公開	2020 年の公開	2021 年の公開