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

[2017 年第 2 四半期（4 月～6 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、2017 年 4 月 1 日から 2017 年 6 月 30 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 技術本部 セキュリティセンター

2017 年 7 月 25 日

目次

1. 2017 年第 2 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】WordPress 用プラグインのソフトウェアに関する脆弱性対策情報について ..... - 3 -
1-3. 【注目情報 2】IPA に報告された DLL 読み込みに関する脆弱性について ..... - 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表した製品の種類別件数 ..... - 9 -
2-4. 脆弱性対策情報の製品別登録状況 ..... - 10 -
3. 脆弱性対策情報の活用状況 ..... - 11 -

1. 2017 年第 2 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（ http://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 70,996 件～

2017 年第 2 四半期（2017 年 4 月 1 日から 6 月 30 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、**脆弱性対策情報の登録件数の累計は、70,996 件でした**（表 1-1、図 1-1）。2017 年から NVD の公開件数が増加傾向となっており、今四半期の登録件数は 3,511 件と、前四半期の登録件数の 2,867 件を上回りました。

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 1,728 件になりました。

表 1-1. 2017 年第 2 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	183 件
	JVN	310 件	7,470 件
	NVD	3,198 件	63,343 件
	計	3,511 件	70,996 件
英語版	国内製品開発者	3 件	183 件
	JVN	89 件	1,545 件
	計	92 件	1,728 件

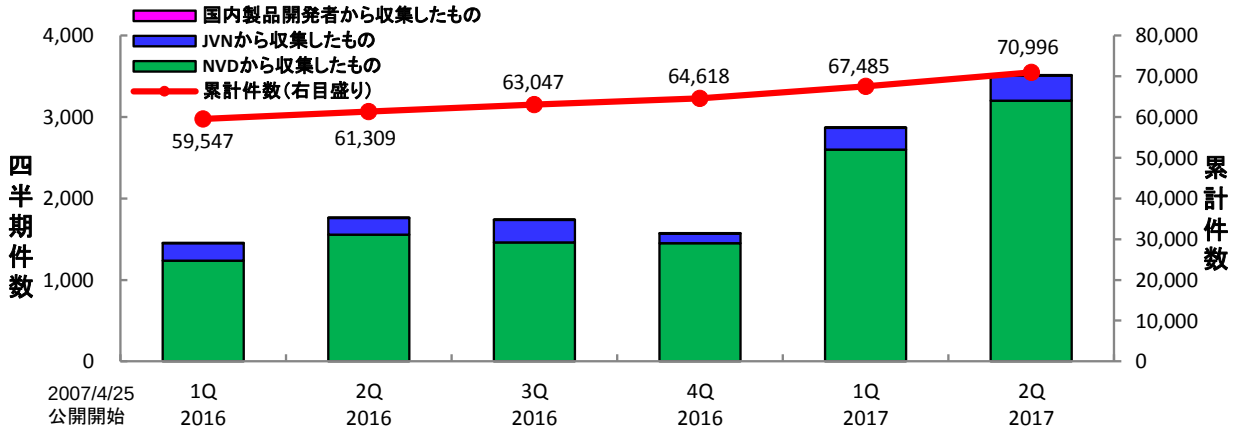

図1−1. JVN iPediaの登録件数の四半期別推移

[*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://nvd.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】WordPress 用プラグインのソフトウェアに関する脆弱性対策情報について

～8 割以上の脆弱性対策情報がサービス停止につながる高い脅威である深刻度レベル II 以上～

2017 年 6 月、WordPress 用プラグイン[*4]「WP Job Manager」を使用した国内の複数のウェブサイトにおいて、本プラグインの脆弱性を悪用した攻撃による被害が発生しました。本脆弱性が悪用された場合、ウェブサイトにログインしていない遠隔の第三者によって、画像ファイルをアップロードされ、ウェブサイトが改ざんされるなどの被害が発生します。IPA では同様の被害が拡大する可能性が非常に高い状況であることから、当該ソフトウェアの利用者に対して緊急対策情報を発信しました[*5]。

表 1-2 は今四半期（2017 年 4 月 1 日～2017 年 6 月 30 日までの 3 ヶ月間）に JVN iPedia で登録した WordPress 用プラグインのソフトウェア全般に関する脆弱性対策情報の一覧です。

表 1-2. WordPress 用プラグインのソフトウェアに関する脆弱性対策情報
(2017 年 4 月～2017 年 6 月)

No.	JVNDB-ID	タイトル	CVSSv2 基本値	CWE
1	JVNDB-2015-007553	WordPress 用 Aviary Image Editor Add-on For Gravity Forms プラグインにおける任意のコードを実行される脆弱性	7.5	CWE-434
2	JVNDB-2017-002629	WordPress 用 Spider Event Calendar プラグインにおける SQL インジェクションの脆弱性	7.5	CWE-89
3	JVNDB-2017-000115	WordPress 用プラグイン Multi Feed Reader における SQL インジェクションの脆弱性	6.5	CWE-89
4	JVNDB-2017-004276	WordPress 用 WP-Testimonials プラグインにおける SQL インジェクションの脆弱性	6.5	CWE-89
5	JVNDB-2017-004277	WordPress 用 Event List プラグインにおける SQL インジェクションの脆弱性	6.5	CWE-89
6	JVNDB-2017-004278	WordPress 用 WP Jobs プラグインにおける SQL インジェクションの脆弱性	6.5	CWE-89
7	JVNDB-2015-007554	WordPress 用 Image Export プラグインにおける絶対パストラバーサルの脆弱性	6.4	CWE-22
8	JVNDB-2015-007539	WordPress 用 Wow Moodboard Lite プラグインの wowproxy.php の proxyimages 関数におけるオープンリダイレクトの脆弱性	5.8	CWE-601
9	JVNDB-2017-002812	WordPress 用 WHIZZ プラグイン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	5.8	CWE-352
10	JVNDB-2015-007548	WordPress 用 Zip Attachments プラグインにおけるディレクトリトラバーサルの脆弱性	5.0	CWE-22
11	JVNDB-2015-007549	WordPress 用 WP e-Commerce Shop Styling プラグインにおけるディレクトリトラバーサルの脆弱性	5.0	CWE-22
12	JVNDB-2015-007550	WordPress 用 MDC YouTube Downloader プラグインにおける絶対パストラバーサルの脆弱性	5.0	CWE-22
13	JVNDB-2015-007555	WordPress 用 Powerplay Gallery プラグインの upload.php における任意のディレクトリを作成される脆	5.0	CWE-264
14	JVNDB-2017-000067	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	5.0	CWE-79
15	JVNDB-2017-000068	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	5.0	CWE-79
16	JVNDB-2017-000073	WordPress 用プラグイン Booking Calendar におけるディレクトリトラバーサルの脆弱性	5.0	CWE-22
17	JVNDB-2017-000074	WordPress 用プラグイン Booking Calendar におけるクロスサイトスクリプティングの脆弱性	5.0	CWE-79
18	JVNDB-2017-000092	WordPress 用プラグイン WP Booking System におけるクロスサイトスクリプティングの脆弱性	5.0	CWE-79
19	JVNDB-2017-000139	WordPress 用プラグイン WP Job Manager におけるアクセス制限不備の問題	5.0	CWE-264
20	JVNDB-2014-008308	WordPress Backup to Dropbox プラグインにおけるクロスサイトスクリプティングの脆弱性	4.3	CWE-79
21	JVNDB-2015-007538	WordPress 用 AdSense Click Fraud Monitoring プラグインで使用される phpWhois におけるクロスサイトスクリプティングの脆弱性	4.3	CWE-79
22	JVNDB-2016-008453	WordPress 用 Clean Login プラグイン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	4.3	CWE-352
23	JVNDB-2017-000127	WordPress 用プラグイン WordPress Download Manager におけるクロスサイトスクリプティングの脆弱	4.3	CWE-79
24	JVNDB-2017-002813	WordPress 用 CopySafe Web Protection プラグインにおけるクロスサイトリクエストフォージェリの脆弱	4.3	CWE-352
25	JVNDB-2017-003315	WordPress 用 Easy WP SMTP プラグインにおけるクロスサイトスクリプティングの脆弱性	4.3	CWE-79
26	JVNDB-2017-003980	WordPress 用 Spiffy Calendar プラグインにおけるクロスサイトスクリプティングの脆弱性	4.3	CWE-79
27	JVNDB-2017-004500	WordPress 用 Raygun4WP プラグインの sendtesterror.php における反射型クロスサイトスクリプティングの脆弱性	4.3	CWE-79
28	JVNDB-2017-004557	WordPress 用 Webhammer WP Custom Fields Search プラグインにおけるクロスサイトスクリプティングの脆弱性	4.3	CWE-79
29	JVNDB-2017-004589	WordPress 用 WP Editor.MD プラグインにおける格納型クロスサイトスクリプティングの脆弱性	4.3	CWE-79
30	JVNDB-2017-004590	WordPress 用 Markdown on Save Improved プラグインにおける格納型クロスサイトスクリプティングの脆弱性	4.3	CWE-79
31	JVNDB-2017-000062	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	CWE-79
32	JVNDB-2017-000093	WordPress 用プラグイン MaxButtons におけるクロスサイトスクリプティングの脆弱性	2.6	CWE-79
33	JVNDB-2017-000094	複数の BestWebSoft 製 WordPress 用プラグインにおけるクロスサイトスクリプティングの脆弱性	2.6	CWE-79
34	JVNDB-2017-000103	WordPress 用プラグイン WP Live Chat Support におけるクロスサイトスクリプティングの脆弱性	2.6	CWE-79
35	JVNDB-2017-000128	WordPress 用プラグイン WordPress Download Manager におけるオープンリダイレクトの脆弱性	2.6	CWE-20
36	JVNDB-2017-000132	WordPress 用プラグイン WP-Members におけるクロスサイトスクリプティングの脆弱性	2.6	CWE-79
37	JVNDB-2017-000140	WordPress 用プラグイン Event Calendar WD におけるクロスサイトスクリプティングの脆弱性	2.6	CWE-79

今四半期は、上記の緊急対策情報で攻撃対象となった脆弱性対策情報 JVNDB-2017-000139 を含

[*4] プラグイン：ソフトウェアの機能を拡張するために追加できるプログラム

[*5] WordPress 用プラグイン「WP Job Manager」におけるアクセス制限不備の問題について(JVN#56787058)
https://www.ipa.go.jp/security/ciadr/vul/20170615-jvn.html

めて、合計 37 件の脆弱性対策情報を登録し、そのうちの 8 割以上（30 件）が、サービス停止につながるような高い脅威である深刻度レベル II（CVSSv2 基本値 4.0～6.9）以上となっています。

図 1-2 は、表 1-2 を元にした、セキュリティ上の弱点（脆弱性）の種類を識別するための識別子である共通脆弱性タイプ一覧 CWE の割合です。

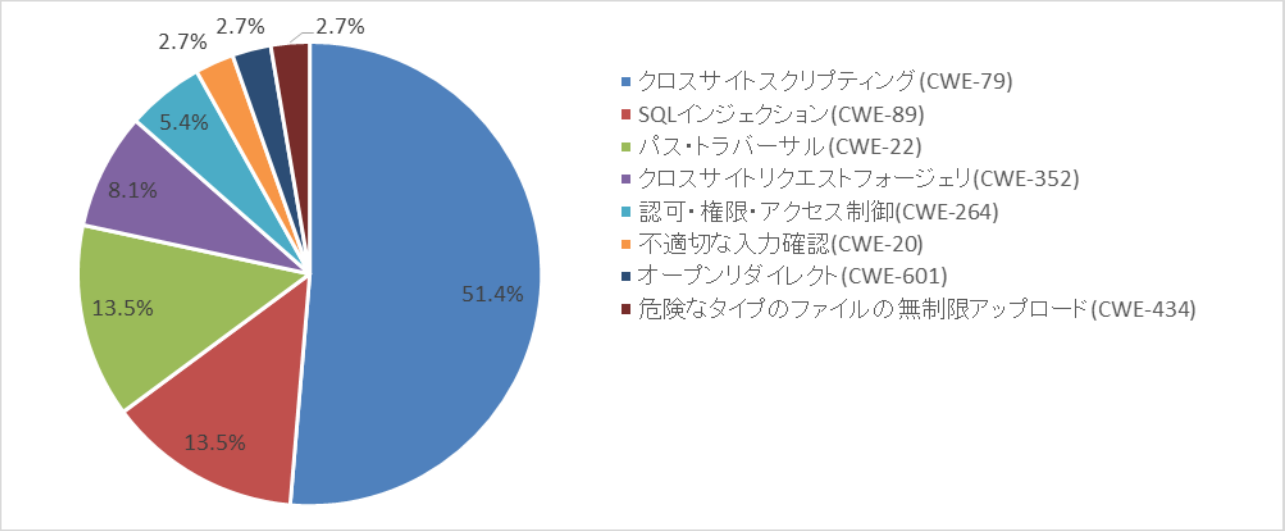

図 1-2.　表 1-2 の WordPress プラグインに関する脆弱性対策情報　CWE 割合

上述の CWE の割合に着目をすると、クロスサイトスクリプティング(CWE-79)が 51.4%と多くを占めており、続いて SQL インジェクション(CWE-89)、パス・トラバーサル(CWE-22)が 13.5%となっています。一例として、SQL インジェクション(CWE-89)の被害事例に注目すると、データベースの情報を改ざんされたり、窃取されたりすることにより、重要な情報が漏えいする、などの重大なインシデントが発生します。

このように、WordPress に関する脆弱性は本体だけでなく、そのプラグインのソフトウェアにも存在しており、SQL インジェクションの脆弱性を悪用されるといった重大なインシデントが発生する可能性があります。WordPress などの CMS（Contents Management System）のソフトウェアを利用しているシステムの運用・管理者は、本体だけでなく、そのプラグインのソフトウェアについても最新の更新情報を随時確認し、すみやかに最新パッチを適用することが重要です。

なお、IPA では多くの利用者が影響を受けるソフトウェアを対象に、必要に応じて緊急対策情報を公開しており、またその緊急対策情報をいち早く受け取るための「icat for JSON [*6] 」サービスもあわせて提供しています。システムの運用・管理者は、このようなサービス活用も検討するなどして迅速な脆弱性対策を実施してください。

[*6] IPA から発信している重要なセキュリティ情報をリアルタイムに配信するサービス。1,000 組織以上がサービス活用中。
https://www.ipa.go.jp/security/vuln/icat.html

1-3. 【注目情報 2】IPA に報告された DLL 読み込みに関する脆弱性について

～今四半期の登録件数は 29 件、直近 3 年間において最大の登録件数～

今四半期は、情報セキュリティ早期警戒パートナーシップ [*7] に基づき IPA に報告された、DLL [*8] 読み込みに関する脆弱性を JVN iPedia に多数登録しました。本脆弱性は、インストーラや自己解凍書庫ファイル等のアプリケーション実行時、DLL ファイルの読み込みにおいて、Windows のシステムディレクトリなどに配置されている正規の DLL ファイルではなく、アプリケーションと同じディレクトリに配置されている DLL ファイルが優先して読まれる問題です。ウイルスの中には、この挙動を悪用して感染拡大するものも確認されています [*9] 。

図 1-3 は 2014 年第 3 四半期から今四半期までの本脆弱性の登録件数の推移です。今四半期の登録件数は 29 件となっており、直近 3 年間において最大の登録件数となっています。本脆弱性は、容易に発見できるため、登録が急激に増加したと考えられます。

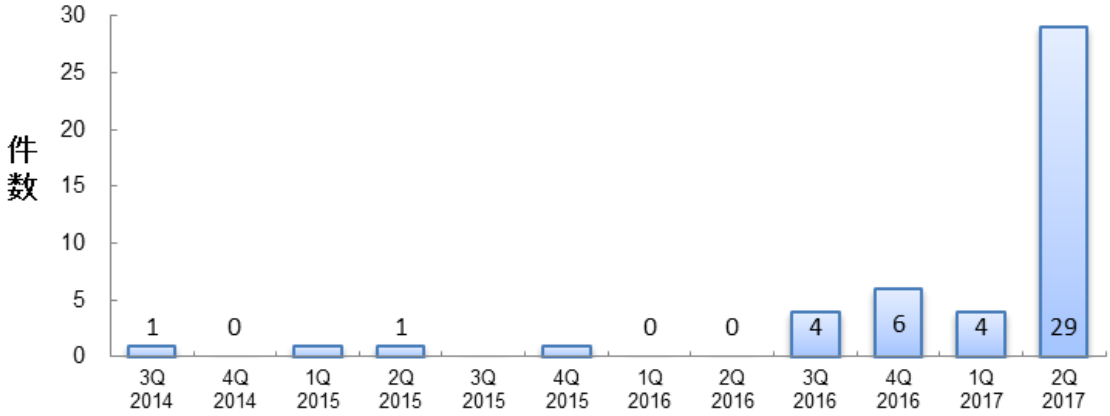

図1−3.IPAに報告されたDLL読み込みに関する脆弱性対策情報の登録件数

表 1-3 は、今四半期に登録した本脆弱性の脆弱性対策情報を一部抜粋したものです。脆弱性の深刻度がレベル II (CVSSv2 基本値：6.8)と比較的高く、脆弱性を悪用した攻撃を受けた際に影響が大きいことがわかります。

表 1-3.IPA に報告された DLL 読み込みに関する脆弱性対策情報(一部抜粋)

No	JVNDB-ID	タイトル	CVSSv2 基本値	JVN iPedia 公開日
1	JVNDB-2017-000153 (CVE-2017-2233)	法務省が提供する PDF 署名プラグインのインストーラにおける任意の DLL 読み込みに関する脆弱性	6.8	2017/6/30
2	JVNDB-2017-000145 (CVE-2017-2226)	e-Tax ソフト (WEB 版) 事前準備セットアップのインストーラにおける DLL 読み込みに関する脆弱性	6.8	2017/6/28
3	JVNDB-2017-000102 (CVE-2017-2177)	商業登記電子認証ソフトのインストーラにおける DLL 読み込みに関する脆弱性	6.8	2017/5/26
4	JVNDB-2017-000101	航空自衛隊が提供するスクリーンセーバーのインストーラ	6.8	2017/5/25

[*7] 情報セキュリティ早期警戒パートナーシップガイドライン
https://www.ipa.go.jp/security/ciadr/partnership_guide.html
[*8] DLL：ソフトウェアで使用する汎用的な機能をモジュール化したファイル
[*9] オープンソースの RAT を改良したマルウエア RedLeaves(2017-04-03)
https://www.jpcert.or.jp/magazine/acreport-redleaves.html

No	JVNDB-ID	タイトル	CVSSv2 基本値	JVN iPedia 公開日
	(CVE-2017-2176)	における DLL 読み込みに関する脆弱性		
5	JVNDB-2017-000076 (CVE-2017-2154)	花子を含む複数の製品における任意の DLL 読み込みに関する脆弱性	6.8	2017/4/20
6	JVNDB-2017-000069 (CVE-2017-2149)	東芝製メモリカード関連ソフトウェアの複数のインストーラにおける DLL 読み込みに関する脆弱性	6.8	2017/4/14

インストーラ作成ソフトウェアや圧縮解凍ツールの開発者およびインストーラや自己解凍書庫ファイルの開発者は、利用者が被害に遭わないために、以下のような対策 [*10] が求められます。

■インストーラ作成ソフトウェアや圧縮解凍ツールの開発者

本脆弱性の問題がインストーラ作成ソフトウェアや圧縮解凍ツールに存在しないことを確認し、適切な対策を実施してください。

■インストーラや自己解凍書庫ファイルの開発者

JVN iPedia 等でアプリケーションに脆弱性を確認した場合、対策済みバージョンのインストーラ作成ソフトウェアや圧縮解凍ツールを使用してください。また、コマンド実行などの改修を行う場合には、意図したディレクトリにあるコマンドを実行するよう、適切に改修を行ってください。

また、アプリケーション利用者においても、インストーラや自己解凍書庫ファイルの実行時に以下の点を注意する必要があります。

■アプリケーション利用者

インストーラや自己解凍書庫ファイルを実行する際、同一ディレクトリ内に不審なファイルがないことを確認してから実行するか、新たに作成したディレクトリにファイルをコピーしてから実行してください。また、インターネット経由でダウンロードしたアプリケーションをダウンロードディレクトリに置いたまま実行しないことを推奨します。例えば、細工された DLL ファイルをダウンロードディレクトリにダウンロードしている状態で、インストーラをそのまま実行すると、細工された DLL ファイルが読み込まれてインストーラを実行する可能性があります。

[*10] Windows アプリケーションによる DLL 読み込みやコマンド実行に関する問題　JVNTA#91240916
https://jvn.jp/ta/JVNTA91240916/

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、2017 年第 2 四半期（4 月～6 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-119（バッファエラー）が 559 件、CWE-284（不適切なアクセス制御）が 364 件、CWE-264（認可・権限・アクセス制御不備）が 316 件、CWE-200（情報漏えい）が 302 件、CWE-79（クロスサイト・スクリプティング）が 289 件でした。最も件数の多かった CWE-119（バッファエラー）は、悪用されるとサーバや PC 上で悪意のあるコードが実行され、データを盗み見られたり、改ざんされる、などの被害が発生する可能性があります。

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。なお、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 (*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。

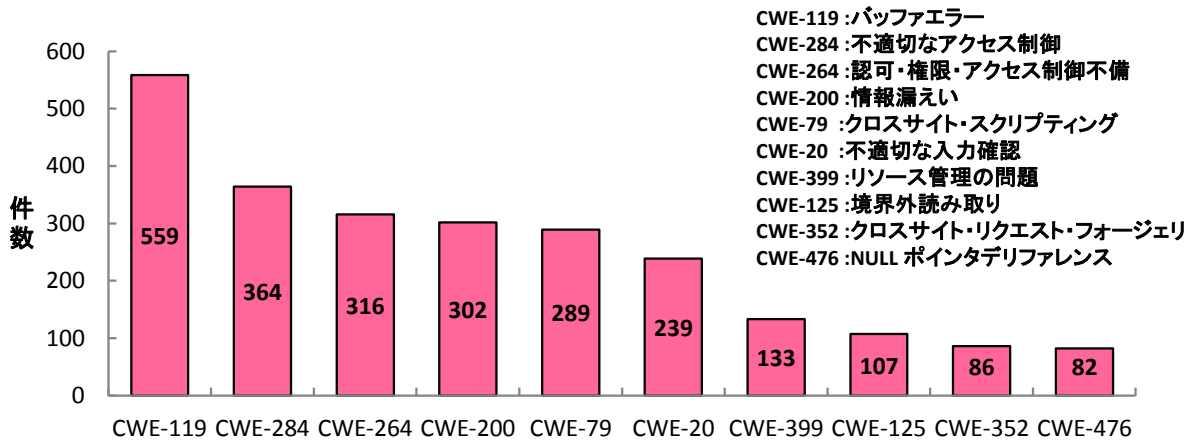

図2-1. 2017年第2四半期に登録された脆弱性の種類別件数

(*11) 「安全なウェブサイトの作り方」 https://www.ipa.go.jp/security/vuln/websecurity.html
(*12) 「IPA セキュア・プログラミング講座」 https://www.ipa.go.jp/security/awareness/vendor/programming/
(*13) 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、公表年別にその推移を示したものです。

脆弱性対策情報の登録開始から 2017 年 6 月 30 日までに 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 39.1%、レベルⅡが 53.2%、レベルⅠが 7.7%となっており、情報の漏えいや改ざんされるような高い脅威であるレベルⅡ以上が、92.3%を占めています。

既知の脆弱性による脅威を回避するため、**製品利用者は日頃から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、JVN iPedia では、CVSSv2 によるこれまでの評価方法に加えて、2015 年 12 月 1 日より CVSSv3 (*14) による評価方法も試行運用しています (*15) 。

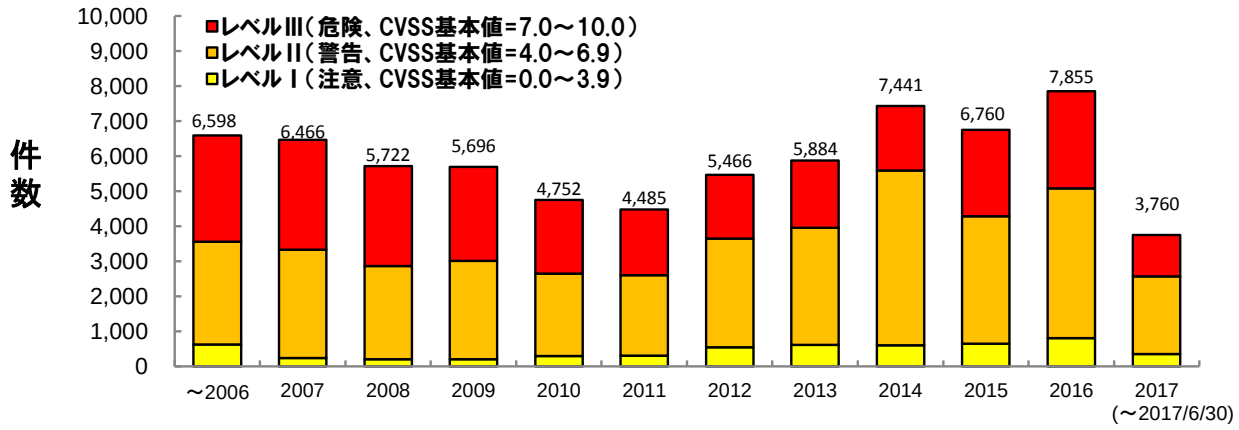

図2-2. 脆弱性の深刻度別件数

(*14) CVSSv3：脆弱性の深刻度を評価するための指標。仮想化やサンドボックス化などが進んできていることから、利用状況の変化を取り込んだ仕様
https://www.ipa.go.jp/security/vuln/CVSSv3.html

(*15) 共通脆弱性評価システム CVSS v3 (新バージョン)での評価の開始について
https://www.ipa.go.jp/security/vuln/SeverityLevel3.html

2-3. 脆弱性対策情報を公表した製品の種類別件数

図 2-3 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。2017 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、2017 年の件数全件の 73.3%を占めています。

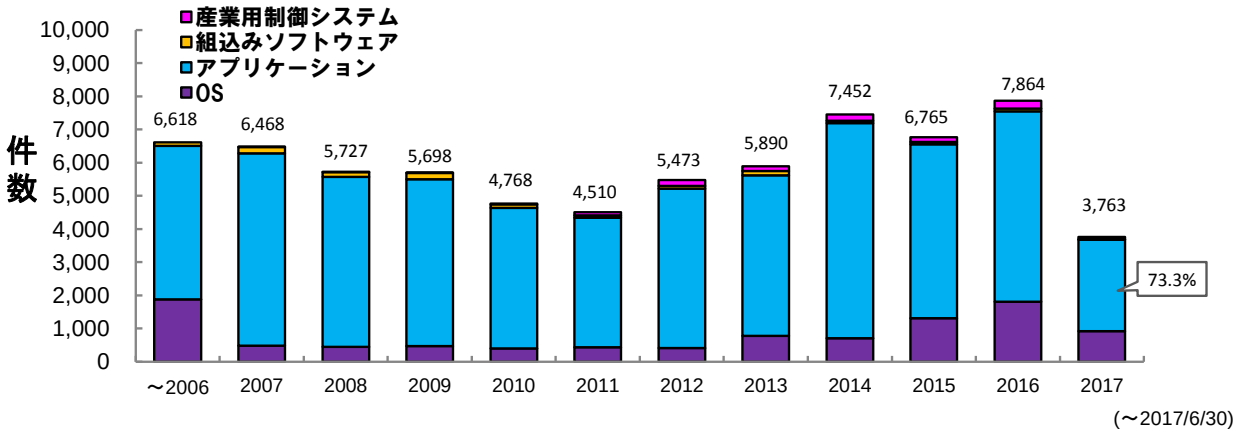

図2-3. 脆弱性対策情報を公表した製品の種類別件数の公開年別推移

また 2007 年以降、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を登録しています。これまでに累計で 1,091 件を登録しています（図 2-4）。

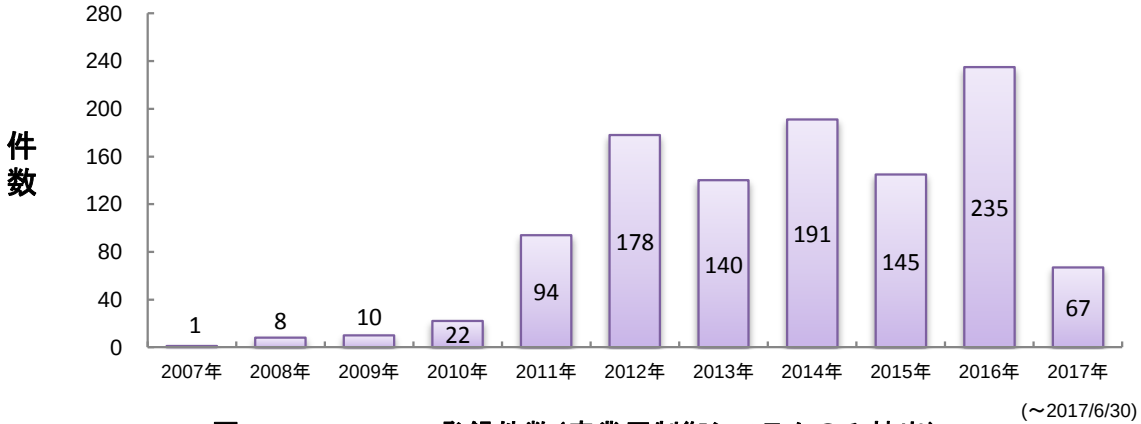

図2-4. JVN iPedia 登録件数（産業用制御システムのみ抽出）

2-4. 脆弱性対策情報の製品別登録状況

表 2-1 は 2017 年第 2 四半期（4 月～6 月）に JVN iPedia へ脆弱性対策情報の登録件数が多かった製品の上位 20 件を示したものであり、1 位の画像処理ソフトである ImageMagick の登録件数は 151 件でした。なお、ImageMagick の登録が多かった理由は、NVD が 2017 年より前に発見された脆弱性情報をまとめて公開したためであり、今四半期に脆弱性が多く発見されたわけではありません。2 位以降は OS 製品が上位にランクインしており、マイクロソフトやアップルなど、一般に広く利用されているベンダーの製品に関する脆弱性対策情報が多く登録されました。

JVN iPedia は、表にある製品だけではなく、国内の企業や家庭で使われている製品に関する脆弱性対策情報を登録しています。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 [2017 年 4 月～2017 年 6 月]

順位	カテゴリ	製品名（ベンダー）	登録件数
1	画像処理ソフト	ImageMagick(ImageMagick)	151
2	OS	iOS(アップル)	136
3	OS	Linux Kernel(kernel.org)	135
4	OS	Android(Google)	118
4	OS	Microsoft Windows 10(マイクロソフト)	103
6	OS	Microsoft Windows Server 2016(マイクロソフト)	103
7	OS	Microsoft Windows Server 2012(マイクロソフト)	102
8	OS	Apple Mac OS X(アップル)	101
9	OS	Microsoft Windows 8.1(マイクロソフト)	96
10	OS	Microsoft Windows Server 2008(マイクロソフト)	90
11	OS	tvOS(アップル)	89
12	OS	Microsoft Windows 7(マイクロソフト)	82
13	OS	Microsoft Windows RT 8.1(マイクロソフト)	78
13	ブラウザ	Safari(アップル)	70
13	OS	watchOS(アップル)	53
13	画像処理ソフト	AutoTrace(AutoTrace project)	50
17	PDF 閲覧	Adobe Reader(アドビシステムズ)	49
17	PDF 閲覧・編集	Adobe Acrobat(アドビシステムズ)	49
19	OS	openSUSE Leap(openSUSE project)	43
20	ブラウザ	Microsoft Edge(マイクロソフト)	38

[(*16)] 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 2017 年第 2 四半期（4 月～6 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。

1 位の Intel Active Management Technology に関する脆弱性は、当該製品がサーバなどに搭載されている場合、影響を受ける可能性があり、影響範囲が広いことから企業などでも注意が呼びかけられ注目を集めました。

表 3-1.JVN iPedia の脆弱性対策情報へのアクセス　上位 20 件 [2017 年 4 月～2017 年 6 月]

順位	ID	タイトル	CVSSv2 基本値	公開日	アクセス数
1	JVNDB-2017-002923	Intel Active Management Technology (AMT) にアクセス制限不備の脆弱性	10.0	2017/5/9	7,767
2	JVNDB-2017-000069	東芝製メモリカード関連ソフトウェアの複数のインストーラにおける DLL 読み込みに関する脆弱性	6.8	2017/4/14	4,299
3	JVNDB-2017-000054	ASSETBASE におけるクロスサイトスクリプティングの脆弱性	2.6	2017/4/11	4,095
4	JVNDB-2017-000070	WN-AC1167GR におけるクロスサイトスクリプティングの脆弱性	1.4	2017/4/14	3,980
5	JVNDB-2016-004511	TLS プロトコルなどの製品で使用される DES および Triple DES 暗号における平文のデータを取得される脆弱性	5.0	2016/9/2	3,977
6	JVNDB-2017-000058	Tablacus Explorer におけるスクリプトインジェクションの脆弱性	6.8	2017/4/7	3,961
7	JVNDB-2017-000072	WNC01WH における OS コマンドインジェクションの脆弱性	5.2	2017/4/21	3,893
8	JVNDB-2017-002402	Microsoft OLE URL Moniker における遠隔の HTA データに対する不適切な処理	9.3	2017/4/13	3,811
9	JVNDB-2017-000068	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	5.0	2017/4/13	3,520
10	JVNDB-2017-000055	NETGEAR ProSAFE Plus Configuration Utility におけるアクセス制限不備の脆弱性	2.9	2017/4/18	3,408
11	JVNDB-2017-000074	WordPress 用プラグイン Booking Calendar におけるクロスサイトスクリプティングの脆弱性	5.0	2017/4/20	3,398
12	JVNDB-2017-000044	CentreCOM AR260S V2 における権限昇格の脆弱性	5.2	2017/3/30	3,355
13	JVNDB-2017-000076	花子を含む複数の製品における任意の DLL 読み込みに関する脆弱性	6.8	2017/4/20	3,338
14	JVNDB-2017-000060	WN-G300R3 におけるバッファオーバーフローの脆弱性	5.8	2017/4/10	3,276

順位	ID	タイトル	CVSSv2 基本値	公開日	アクセス数
15	JVNDB-2017-000077	Windows 版 Vivaldi のインストーラにおける実行ファイル読み込みの脆弱性	6.8	2017/4/25	3,258
16	JVNDB-2017-000059	WN-G300R3 における OS コマンドインジェクションの脆弱性	5.2	2017/4/10	3,254
17	JVNDB-2017-000066	サイボウズ Office の API に関するサービス運用妨害 (DoS)の脆弱性	7.8	2017/4/11	3,224
18	JVNDB-2017-000065	サイボウズ Office のカスタムアプリのテンプレート削除機能におけるアクセス制限不備の脆弱性	5.5	2017/4/11	3,200
19	JVNDB-2017-000075	風神ビュアーにおけるバッファオーバーフローの脆弱性	5.1	2017/4/20	3,187
20	JVNDB-2017-000050	WordPress 用プラグイン YOP Poll におけるクロスサイトスクリプティングの脆弱性	4.0	2017/3/23	3,179

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。対象製品を利用している場合、システム管理者は、ベンダーが提供する対策パッチなどを早期に自システムに適用し、攻撃による被害を未然に防ぐことが重要です。

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 [2017 年 4 月～2017 年 6 月]

順位	ID	タイトル	CVSSv2 基本値	公開日	アクセス数
1	JVNDB-2016-006450	JP1/Cm2/Network Node Manager i における脆弱性	4.3	2017/1/4	2,731
2	JVNDB-2017-002225	複数の日立製品におけるクロスサイトスクリプティングの脆弱性	4.3	2017/4/5	788
3	JVNDB-2017-003108	Hitachi IT Operations Director および JP1/IT Desktop Management における複数の脆弱性	7.5	2017/5/16	657
4	JVNDB-2011-001632	Hitachi Web Server の SSL および TLS プロトコルにおける任意のデータが挿入される脆弱性	4.3	2011/5/26	254
5	JVNDB-2007-001022	Apache の mod_autoindex.c における UTF-7 エンコードに関するクロスサイトスクリプティングの脆弱性	4.3	2007/12/25	245

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）公開日の年による色分け

2015 年以前の公開	2016 年の公開	2017 年の公開