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

[2016 年第 3 四半期（7 月～9 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、2016 年 7 月 1 日から 2016 年 9 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

2016 年 10 月 25 日

目次

1. 2016 年第 3 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 63,047 件～

2016 年第 3 四半期（2016 年 7 月 1 日から 9 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、63,047 件でした**（表 1-1、図 1-1）。

JVN iPedia 英語版へ登録した脆弱性対策情報も右表の通り、累計で 1,516 件になりました。

表 1-1. 2016 年第 3 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	178 件
	JVN	278 件	6,776 件
	NVD	1,458 件	56,093 件
	計	1,738 件	63,047 件
英語版	国内製品開発者	2 件	178 件
	JVN	56 件	1,338 件
	計	58 件	1,516 件

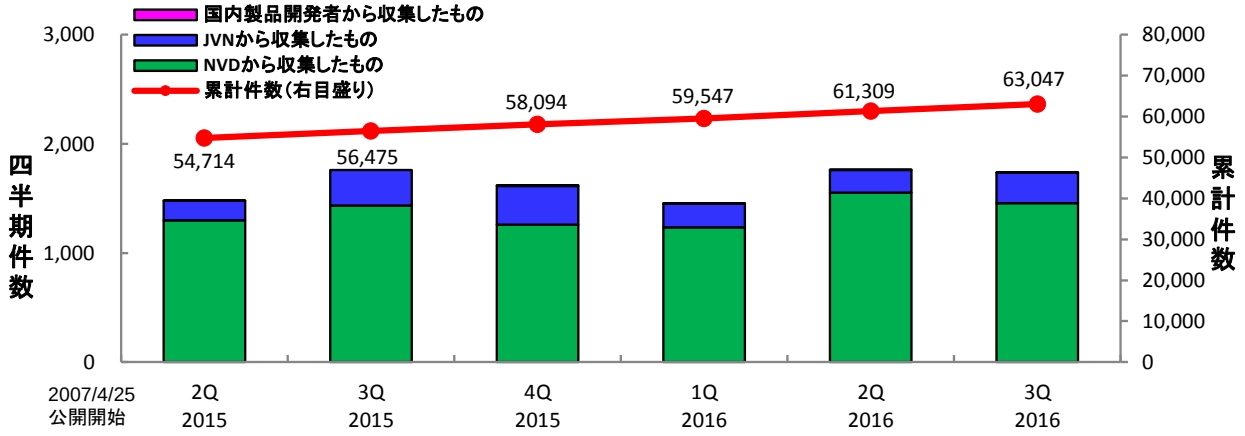

図1-1. JVN iPediaの登録件数の四半期別推移

(*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。 http://www.nist.gov/

(*3) National Vulnerability Database。NIST が運営する脆弱性データベース。http://nvd.nist.gov/home.cfm

1-2. 【注目情報 1】スマートフォンの OS に関する脆弱性対策情報について

～Apple iOS の 3 つの脆弱性を悪用した攻撃を確認、OS のアップデートは迅速な実施を～

2016 年 8 月にアップル社の iPhone や iPad の OS である iOS に関する脆弱性対策情報が当該ベンダーから公開されました。本情報が公開された時点で、セキュリティベンダーより本脆弱性を悪用した攻撃を確認済みであり [*4]、今後被害が拡大する可能性があることから IPA では緊急対策情報の発信を行いました [*5]。なお、この攻撃は iOS に存在する 3 つの脆弱性を悪用しており、攻撃者が用意したページに脆弱性の対策がされていないスマートフォンでアクセスすると、通話履歴や SMS などの情報が漏えいする可能性があります。

表 1-2 は攻撃に悪用された脆弱性対策情報を示したものです。項番 3 の脆弱性 CVE-2016-4657 は深刻度が「レベル II (警告)」と評価されていますが、当該脆弱性への攻撃を踏み台とされることで CVE-2016-4655、CVE-2016-4656 である「レベル III (危険)」の脆弱性を悪用され、より深刻な被害に繋がります。なお、脆弱性の影響を受けウイルスに感染をしている場合は、OS のアップデートだけでは対策ができないため、セキュリティソフトなどによる対処が必要 [*6] となります。

表 1-2. 攻撃に悪用された脆弱性対策情報

No	ID（CVE）	タイトル	深刻度（CVSSv2）
1	JVNDB-2016-004455 (CVE-2016-4655)	Apple iOS のカーネルにおけるメモリから重要な情報を取得される脆弱性	7.1
2	JVNDB-2016-004456 (CVE-2016-4656)	Apple iOS のカーネルにおける特権付きコンテキスト内で任意のコードを実行される脆弱性	9.3
3	JVNDB-2016-004457 (CVE-2016-4657)	Apple iOS などで使用される WebKit における任意のコードを実行される脆弱性	6.8

iPhone などのスマートフォンは電話やインターネットの閲覧、GPS による現在地の確認など様々な用途で用いられており、それに伴い電話番号や通信記録、位置情報などの多くの重要な情報を取り扱っています。このため攻撃により、情報の漏えいやスマートフォンが制御されると、深刻な被害となる可能性があります。

スマートフォンを安全に利用するためにも、利用者は OS の脆弱性が確認されたら早急にアップデートを行う必要があります。OS の脆弱性対策以外にも、スマートフォンで使用するアプリケーションは公式のマーケットからインストールし、インストール後も最新バージョンが公開されたらアップデートする等の脆弱性対策を実施する。さらに、ウイルス感染の危険性を下げるためにセキュリティソフトを導入するなどの対策を実施することも重要です。

[*4] 3 things CISOs need to know about the Trident iOS vulnerabilities
https://blog.lookout.com/blog/2016/08/25/lookout-trident-pegasus-enterprise-discovery/

[*5] Apple iOS および OS X の脆弱性対策について(CVE-2016-4655 等)
https://www.ipa.go.jp/security/ciadr/vul/20160829-ios.html

[*6] まとめ：iOS の脆弱性を狙う脅威「ペガサス」概要と、対策方法
https://blog.lookout.com/jp/2016/09/08/pegasussummary/

1-3. 【注目情報 2】セキュリティソフトの脆弱性対策情報について

～Symantec 製品に最も深刻度の高い「レベルⅢ(危険)」の脆弱性、早急な対応が必要～

2016 年 6 月下旬にノートンなどのセキュリティソフトを提供している Symantec 社の製品に関する脆弱性情報が公開されました。本脆弱性を悪用した攻撃コードが一般に公開されており、誰でも容易に攻撃が可能な状況となっていたため、IPA では悪用される可能性が極めて高いと判断し、2016 年 7 月に緊急対策情報を発信しています。[(*7)]。

表 1-3 は当該脆弱性に関してベンダーから発信された情報を基に JVN iPedia で公開をした、深刻度が「レベルⅢ(危険)」と評価された脆弱性対策情報の一覧です。これらの脆弱性を悪用された場合、アプリケーションプログラムが異常終了する、攻撃者によってパソコンを制御されるなど、様々な被害が発生する可能性があります。なお、一部の企業向け製品においては LiveUpdate などの自動更新だけではなく、最新版の製品をインストールする必要があることに注意をしてください。アップデート方法についての詳細は、ベンダー情報 [(*8)] などを確認し実施をする必要があります。

表 1-3. Symantec 製品に関する脆弱性対策情報

No	ID（CVE）	タイトル	深刻度（CVSSv2）
1	JVNDB-2016-003441 (CVE-2016-2207)	複数の Symantec 製品の圧縮解凍エンジンにおける任意のコードを実行される脆弱性	10.0
2	JVNDB-2016-003442 (CVE-2016-2209)	複数の Symantec 製品の圧縮解凍エンジンの Dec2SS.dll におけるバッファオーバーフローの脆弱性	9.0
3	JVNDB-2016-003443 (CVE-2016-2210)	複数の Symantec 製品の圧縮解凍エンジンの Dec2LHA.dll におけるバッファオーバーフローの脆弱性	9.0
4	JVNDB-2016-003444 (CVE-2016-2211)	複数の Symantec 製品の圧縮解凍エンジンにおける任意のコードを実行される脆弱性	9.3
5	JVNDB-2016-003445 (CVE-2016-3644)	複数の Symantec 製品の圧縮解凍エンジンにおける任意のコードを実行される脆弱性	10.0
6	JVNDB-2016-003446 (CVE-2016-3645)	複数の Symantec 製品の圧縮解凍エンジンの TNEF アンパッカーにおける整数オーバーフローの脆弱性	10.0
7	JVNDB-2016-003447 (CVE-2016-3646)	複数の Symantec 製品の圧縮解凍エンジンにおける任意のコードを実行される脆弱性	10.0

一般的なセキュリティソフトはスパイウェアやマルウェアなどの脅威から PC を守る役割を持っています。しかし今回公開された脆弱性のようにセキュリティソフト自体に脆弱性が確認され、悪用される原因になってしまうケースも存在します。

そのため利用者は、セキュリティソフト製品も脆弱性の影響を受ける可能性のあるソフトウェアの一つと認識する必要があり、ベンダーから製品のアップデート情報などが公開された場合は、脆弱性を悪用される前に、公開された情報をもとに早急にアップデートなどの対策実施を行うことが重要です。

(*7) Symantec 製品の脆弱性対策について(CVE-2016-3647 等)
https://www.ipa.go.jp/security/ciadr/vul/20160705-symantec.html

(*8) セキュリティアドバイザリー - シマンテックの圧縮解除エンジンの解析に複数の脆弱性
https://www.symantec.com/content/ja/jp/enterprise/other_resources/sym16-010.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、2016 年第 3 四半期（7 月～9 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、件数を集計した示したものです。

集計結果は件数が多い順に、CWE-119（バッファエラー）が 327 件、CWE-200（情報漏えい）が 189 件、CWE-264（認可・権限・アクセス制御不備）が 187 件、CWE-20（不適切な入力確認）が 133 件、CWE-79（クロスサイト・スクリプティング）が 113 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、開発者や運営者が適切な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 (*9) 」、脆弱性の仕組みを演習で実践的に学ぶことができる脆弱性体験学習ツール「AppGoat (*10) 」を公開しています。

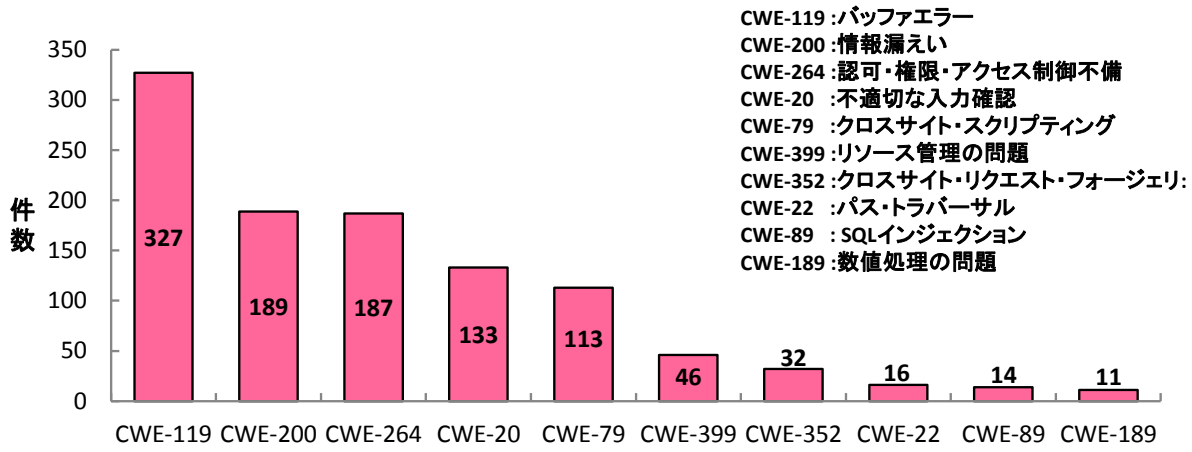

図2-1. 2016年第3四半期に登録された脆弱性の種類別件数

(*9) 「安全なウェブサイトの作り方」 https://www.ipa.go.jp/security/vuln/websecurity.html
(*10) 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、公表年別にその推移を示したものです。

脆弱性対策情報の公開開始から 2016 年 9 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 40.1%、レベルⅡが 52.5%、レベルⅠが 7.4%となっています。

これら既知の脆弱性の深刻度は、92.6%が情報の漏えい、改ざんされるような高い脅威であるレベルⅡ以上となっています。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 による評価方法も試行運用しています。

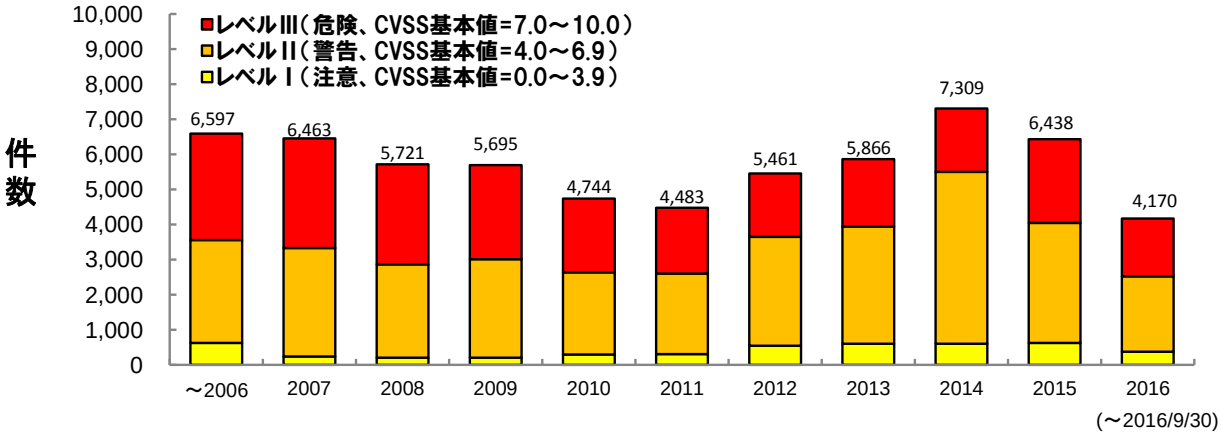

図2-2. 脆弱性の深刻度別件数

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。最も多いのはアプリケーションに関する脆弱性対策情報で、2016 年の件数全件の 70.4%を占めています。

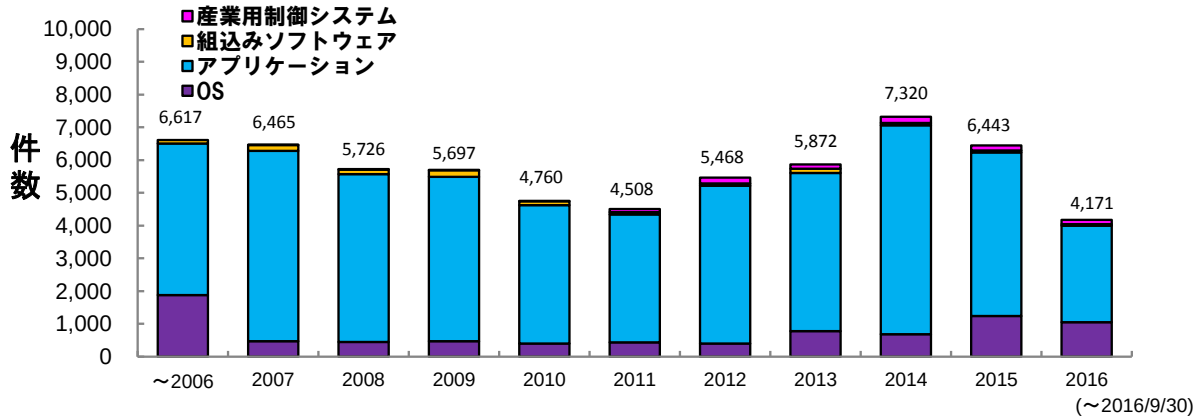

図2-3. 脆弱性対策情報を公表した製品の種類別件数の公開年別推移

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918件が登録しています（図2-4）。

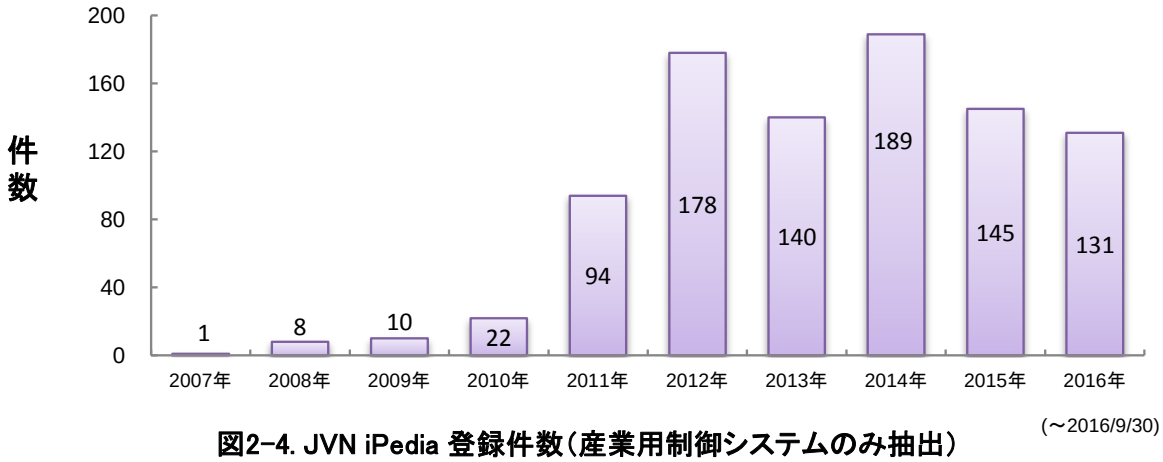

図2-4. JVN iPedia 登録件数（産業用制御システムのみ抽出）

2-4. 脆弱性対策情報の製品別登録状況

表 2-4 は 2016 年第 3 四半期（7 月～9 月）に JVN iPedia へ脆弱性対策情報の登録が多かった製品の上位 20 件を示したものです。1 位の Android の登録件数は 231 件で、月例パッチで公開された脆弱性対策情報を登録しました。Android の他には Microsoft Windows10 などのマイクロソフトの OS 製品に関する脆弱性対策情報も多く登録しています。

JVN iPedia は、表にある OS 製品やブラウザ製品などの脆弱性対策情報だけではなく、国内の企業や家庭で使われているソフトウェアに関する脆弱性対策情報を網羅的に登録しています。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 [(*11)]。

表 2-4. 製品別 JVN iPedia の脆弱性対策情報登録件数　上位 20 件 [2016 年 7 月～2016 年 9 月]

順位	カテゴリ	製品名（ベンダー）	登録件数
1	OS	Android（Google）	231
2	ブラウザ	Google Chrome（Google）	138
2	OS	Microsoft Windows 10（マイクロソフト）	119
4	OS	Microsoft Windows Server 2012（マイクロソフト）	113
4	OS	Microsoft Windows 8.1（マイクロソフト）	113
6	OS	Microsoft Windows RT 8.1（マイクロソフト）	97
7	OS	Apple Mac OS X（アップル）	91
8	OS	iOS（アップル）	89
9	動画再生ソフト	Adobe Flash Player（アドビシステムズ）	78
10	OS	tvOS（アップル）	59
11	スクリプト言語	PHP（The PHP Group）	48
12	ブラウザ	Mozilla Firefox（Mozilla Foundation）	44
13	PDF 閲覧	Adobe Reader（アドビシステムズ）	39
13	PDF 閲覧・編集	Adobe Acrobat（アドビシステムズ）	39
13	PDF 閲覧・編集	Adobe Acrobat DC（アドビシステムズ）	39
13	PDF 閲覧	Adobe Acrobat Reader DC（アドビシステムズ）	39
17	OS	watchOS（アップル）	38
17	ブラウザ	Safari（アップル）	38
19	ブラウザ	Microsoft Internet Explorer（マイクロソフト）	37
20	OS	Linux Kernel（kernel.org）	35

[(*11)] 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 2016 年第 3 四半期（7 月～9 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 位は Apache Commons FileUpload に関する脆弱性で Apache Struts や Apache Tomcat も本製品を使用しており、多くのソフトウェアが影響を受ける可能性があります。また、Apache Struts にも着目すると 3 位、5 位、13 位、14 位と複数ランクインしており、ウェブアプリケーションを作成する上で利用されているソフトウェアの脆弱性にも注目が集まりました。4 位、10 位は LINE に関する脆弱性で、最新のバージョンをインストールしていない場合、中間者攻撃により不正なファイルをダウンロードさせられたり、不正なプログラムを実行させられたりする可能性があります。

表 3-1.JVN iPedia の脆弱性対策情報へのアクセス　上位 20 件 [2016 年 7 月～2016 年 9 月]

順位	ID	タイトル	CVSSv2 基本値	公開日
1	JVNDB-2016-000121	Apache Commons FileUpload におけるサービス運用妨害 (DoS) の脆弱性	5.0	2016/6/30
2	JVNDB-2016-000154	有限会社 AKABEi SOFT2 製の複数のゲーム製品における OS コマンドインジェクションの脆弱性	6.8	2016/8/31
3	JVNDB-2016-000112	Apache Struts の Getter メソッドにおける検証回避の脆弱性	6.8	2016/6/20
4	JVNDB-2016-000123	LINE PC 版（Windows 版）における DLL 読み込みに関する脆弱性	6.8	2016/7/8
5	JVNDB-2016-000096	Apache Struts 1 におけるメモリ上にあるコンポーネントを操作可能な脆弱性	6.8	2016/6/7
6	JVNDB-2016-000125	WordPress プラグイン「Nofollow Links」におけるクロスサイトスクリプティングの脆弱性	2.6	2016/7/20
7	JVNDB-2016-000126	Vtiger CRM におけるアクセス制限不備の脆弱性	5.5	2016/7/20
8	JVNDB-2016-002475	OpenSSL の ASN.1 の実装における任意のコードを実行される脆弱性	10.0	2016/5/10
9	JVNDB-2016-004375	Linux Kernel の net/ipv4/tcp_input.c における TCP セッションをハイジャックされる脆弱性	4.3	2016/8/18
10	JVNDB-2016-000153	LINE PC 版（Windows 版）におけるダウンロードファイル検証不備の脆弱性	5.1	2016/8/25
11	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
12	JVNDB-2016-000130	EC-CUBE 用プラグイン「割引クーポンプラグイン」における SQL インジェクションの脆弱性	6.4	2016/7/22
13	JVNDB-2016-000097	Apache Struts 1 における入力値検証機能に関する脆弱性	5.8	2016/6/7
14	JVNDB-2016-000110	Apache Struts において任意のコードを実行可能な脆弱性	6.8	2016/6/20

順位	ID	タイトル	CVSSv2 基本値	公開日
15	JVNDB-2016-003304	OpenSSL におけるサービス運用妨害 (DoS) の脆弱性	4.3	2016/6/22
16	JVNDB-2016-002474	OpenSSL の AES-NI の実装における重要な平文情報を取得される脆弱性	2.6	2016/5/10
17	JVNDB-2016-003802	Apache HTTP Server における任意のプロキシサーバにアプリケーションのアウトバウンド HTTP トラフィックをリダイレクトされる脆弱性	5.1	2016/7/25
18	JVNDB-2016-000105	複数のひかり電話ルータおよびひかり電話対応機器における OS コマンドインジェクションの脆弱性	5.2	2016/6/27
19	JVNDB-2016-000106	複数のひかり電話ルータおよびひかり電話対応機器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	4.0	2016/6/27
20	JVNDB-2016-000152	シンプルチャットにおけるクロスサイトスクリプティングの脆弱性	4.3	2016/8/23

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 [2016 年 7 月～2016 年 9 月]

順位	ID	タイトル	CVSSv2 基本値	公開日
1	JVNDB-2016-004496	Hitachi Tuning Manager におけるクロスサイトスクリプティングの脆弱性	3.5	2016/9/2
2	JVNDB-2016-003527	Hitachi Compute Systems Manager における情報漏えいに関する脆弱性	3.5	2016/7/13
3	JVNDB-2011-001632	Hitachi Command Suite 製品における情報漏えいに関する脆弱性	4.3	2011/5/26
4	JVNDB-2016-002716	Hitachi Command Suite 製品における外部のファイルをブラウザにロードできる脆弱性	4.3	2016/5/18
5	JVNDB-2016-002715	uCosminexus Portal Framework および Groupmax Collaboration におけるクロスサイトスクリプティングの脆弱性	3.5	2016/5/18

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

2014 年以前の公開	2015 年の公開	2016 年の公開