# 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

## [2024 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、2024 年 10 月 1 日から 2024 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

2025 年 01 月 22 日

**目次**

1. 2024 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 -
2. JVN iPedia の登録データ分類 ..... - 3 -
2-1. 脆弱性の種類別件数 ..... - 3 -
2-2. 脆弱性に関する深刻度別割合 ..... - 4 -
2-3. 脆弱性対策情報を公開した製品の種類別件数 ..... - 6 -
2-4. 脆弱性対策情報の製品別登録状況 ..... - 7 -
3. 脆弱性対策情報の活用状況 ..... - 8 -

## 1. 2024 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 223,690 件～**

2024 年第 4 四半期（2024 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 223,690 件になりました**（表 1-1、図 1-1）。なお、2024 年第 4 四半期に JVN iPedia の登録件数が減少した理由は、当該期間中に JVN iPedia での脆弱性情報の公開が遅延しているのではなく、NVD における脆弱性情報の公開が遅延しているためです。

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 2,942 件になりました。

表 1-1. 2024 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 | 2 件 | 290 件 |
| | JVN | 301 件 | 16,061 件 |
| | NVD | 6,591 件 | 207,339 件 |
| | 計 | 6,894 件 | 223,690 件 |
| 英語版 | 国内製品開発者 | 2 件 | 293 件 |
| | JVN | 38 件 | 2,649 件 |
| | 計 | 40 件 | 2,942 件 |

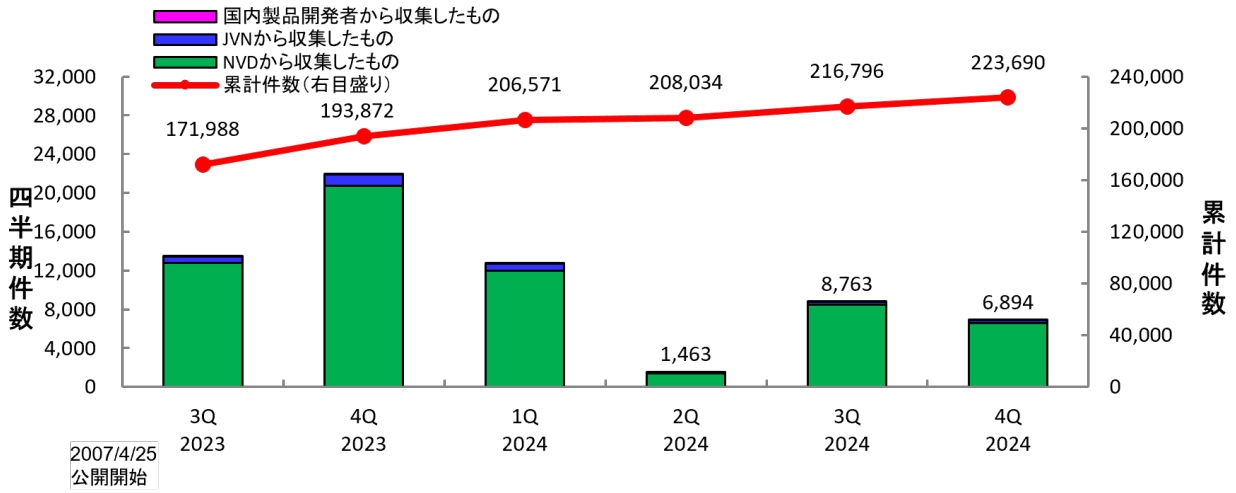


図 1-1. JVN iPedia の登録件数の四半期別推移

(*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

## 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、2024 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 979 件、CWE-89（SQL インジェクション）が 431 件、CWE-787（境界外書き込み）が 369 件、CWE-416（解放済みメモリの使用）が 320 件、CWE-125（境界外読み込み）が 300 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** (*4) 」、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** (*5) 」、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 (*6) 」などを公開しています。

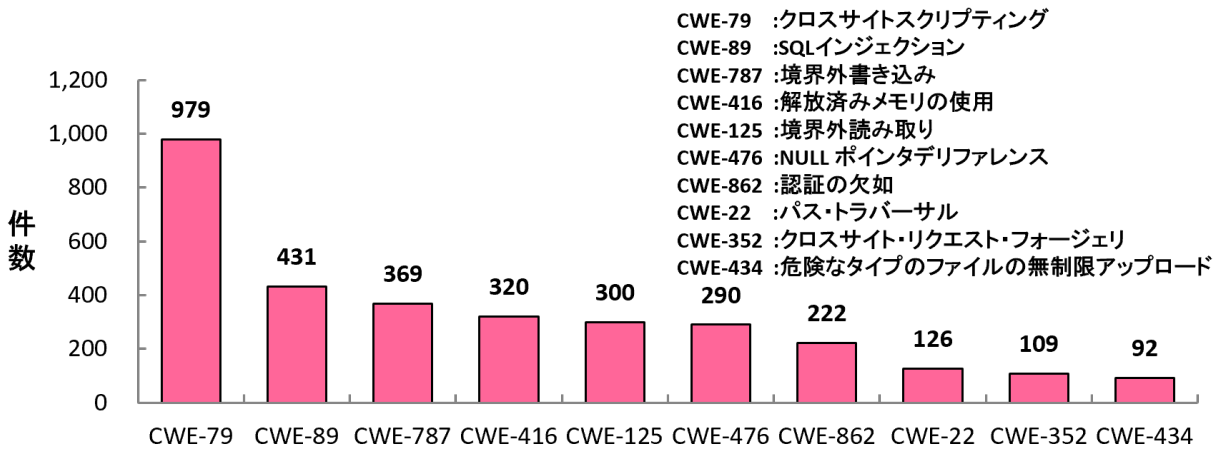


**図 2-1. 2024 年第 4 四半期に登録された脆弱性の種類別件数**

(*4) 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
(*5) IPA：「安全なウェブサイトの作り方」
https://www.ipa.go.jp/security/vuln/websecurity/about.html
(*6) 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。

2024 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 30.2%、レベル 2 が 61.4%、レベル 1 が 8.5%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 91.5%を占めています。

なお、2024 年に JVN iPedia における CVSSv2 の登録件数が大幅に減少した理由は、JVN iPedia の情報収集元である NVD において CVSSv2 の評価が積極的には行われていない [*7] ためです。

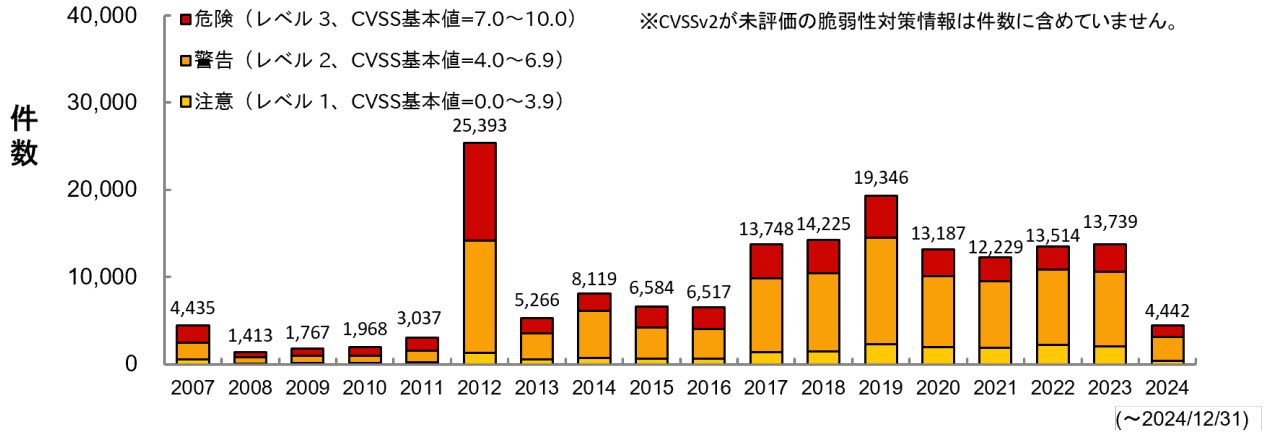


**図 2-2. 脆弱性の深刻度別件数(CVSSv2)**

[*7] NIST：「Retirement of CVSS v2」
https://nvd.nist.gov/general/news/retire-cvss-v2

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。

2024 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 13.9%、「重要」が 37.1%、「警告」が 47.3%、「注意」が 1.7%となっています。

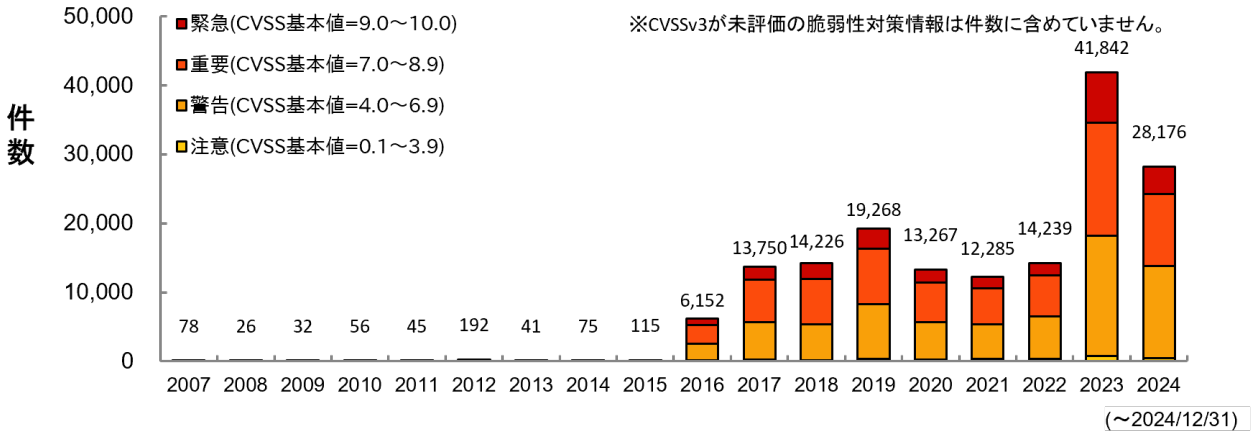


**図 2-3. 脆弱性の深刻度別件数(CVSSv3)**

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 [*8] で公開しています。

[*8] 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。2024 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、2024 年の件数全件の約 70.5%（21,013 件／全 29,818 件）を占めています。

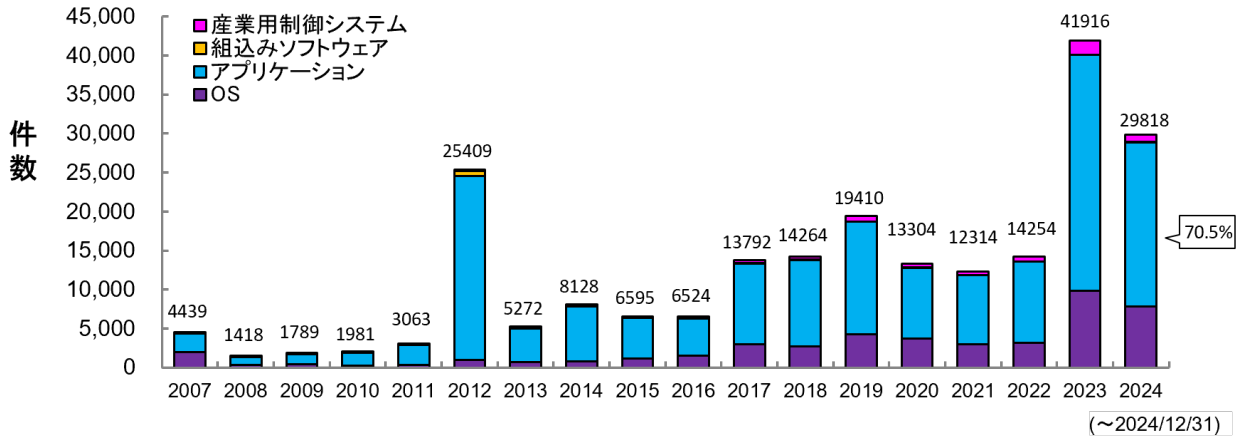


**図 2-4. 脆弱性対策情報を公表した製品の種類別件数の公開年別推移**

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 6,737 件を登録しています。

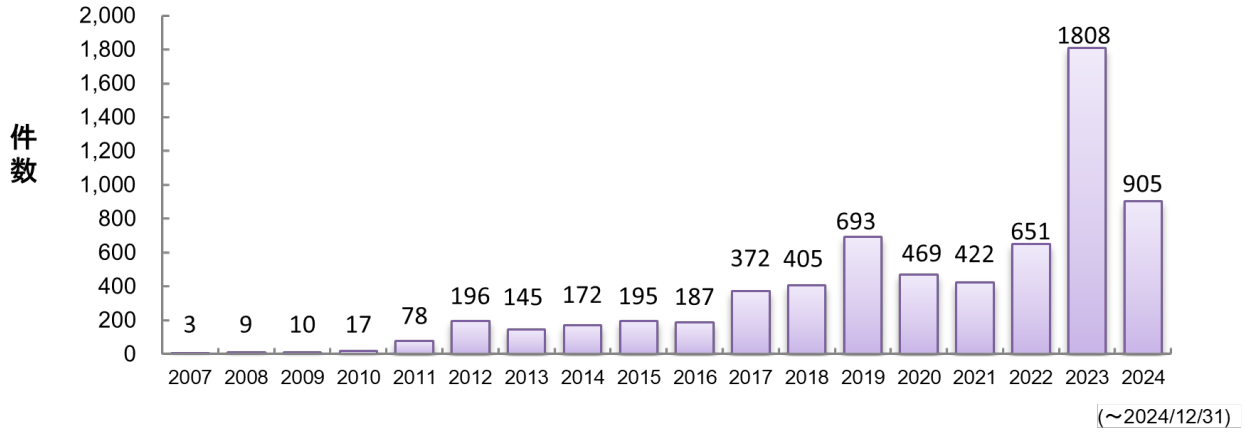


**図 2-5. JVN iPedia 登録件数（産業用制御システムのみ抽出）**

### 2-4. 脆弱性対策情報の製品別登録状況

表 2-1 は 2024 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製品が 1 位となりました。2 位以降は Linux Kernel や、Google、アップル、マイクロソフトなどの幅広いベンダの 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 [(*9)]。

**表 2-1. 製品別 JVN iPedia の脆弱性対策情報登録件数　上位 20 件 [2024 年 10 月～2024 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) | 1685 |
| 2 | OS | Linux Kernel (Linux) | 1157 |
| 3 | OS | Android (Google) | 315 |
| 4 | OS | macOS (アップル) | 248 |
| 5 | OS | iOS (アップル) | 164 |
| 5 | OS | iPadOS (アップル) | 164 |
| 7 | OS | Microsoft Windows Server 2022 (マイクロソフト) | 156 |
| 8 | CMS | Adobe Experience Manager (アドビ) | 151 |
| 9 | OS | Microsoft Windows Server 2019 (マイクロソフト) | 135 |
| 10 | OS | Microsoft Windows 11 (マイクロソフト) | 126 |
| 11 | OS | Microsoft Windows 10 (マイクロソフト) | 116 |
| 12 | OS | Microsoft Windows Server 2016 (マイクロソフト) | 109 |
| 13 | OS | Microsoft Windows Server 2012 (マイクロソフト) | 98 |
| 14 | OS | watchOS (アップル) | 86 |
| 14 | OS | Fedora (Fedora Project) | 86 |
| 16 | 画像ビューア | IrfanView (Irfan Skiljan) | 83 |
| 17 | ブラウザ | Google Chrome (Google) | 82 |
| 18 | OS | Microsoft Windows Server 2008 (マイクロソフト) | 79 |
| 19 | OS | tvOS (アップル) | 78 |
| 20 | OS | HarmonyOS (Huawei) | 77 |

[(*9)] 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 2024 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、上位 20 件中 17 件が脆弱性対策情報ポータルサイト JVN で公開された脆弱性対策情報でした。

**表 3-1. JVN iPedia の脆弱性対策情報へのアクセス　上位 20 件 [2024 年 10 月～2024 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-2024-002050<br>キヤノン製スモールオフィス向け複合機およびレーザービームプリンターにおける複数の境界外書き込みの脆弱性 | - | 9.8 | 2024/2/7 | 3,002 |
| 2 | JVNDB-2024-002832<br>Hitachi Global Link Manager における EL インジェクションの脆弱性 | - | 7.6 | 2024/2/21 | 2,310 |
| 3 | JVNDB-2020-013805<br>Zeroshell 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 | 2021/7/13 | 2,268 |
| 4 | JVNDB-2024-002560<br>Android アプリ「Mopria Print Service」における Intent の取り扱い不備の脆弱性 | - | 5.5 | 2024/2/15 | 2,255 |
| 5 | JVNDB-2024-000019<br>a-blog cms における URL 偽装の脆弱性 | 4.3 | 4.7 | 2024/2/15 | 2,246 |
| 6 | JVNDB-2024-002831<br>エレコム製無線 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 | 5.2 | 6.8 | 2024/2/21 | 2,190 |
| 7 | JVNDB-2024-000020<br>エレコム製無線 LAN ルーターおよび無線 LAN 中継器における複数の脆弱性 | 3.5 | 4.8 | 2024/2/20 | 2,092 |
| 8 | JVNDB-2024-001882<br>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ローカルファイルインクルードの脆弱性 | - | 9.8 | 2024/2/7 | 2,005 |
| 9 | JVNDB-2024-002578<br>シーメンスの Tecnomatix Plant Simulation における境界外書き込みに関する脆弱性 | - | 7.8 | 2024/2/15 | 1,994 |
| 10 | JVNDB-2024-002577<br>シーメンスの Tecnomatix Plant Simulation における境界外書き込みに関する脆弱性 | - | 7.8 | 2024/2/15 | 1,985 |
| 11 | JVNDB-2024-002580<br>シーメンスの Tecnomatix Plant Simulation における NULL ポインタデリファレンスに関する脆弱性 | - | 5.5 | 2024/2/15 | 1,980 |

| 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-2024-002579<br>シーメンスの Tecnomatix Plant Simulation における NULL ポインタデリファレンスに関する脆弱性 | - | 5.5 | 2024/2/15 | 1,978 |
| 13 | JVNDB-2024-001985<br>トレンドマイクロの Trend Micro Deep Security および Deep Security Agent におけるリンク解釈に関する脆弱性 | - | 7.8 | 2024/2/7 | 1,870 |
| 14 | JVNDB-2024-001984<br>トレンドマイクロの Trend Micro Deep Security および Deep Security Agent における脆弱性 | - | 7.8 | 2024/2/7 | 1,839 |
| 15 | JVNDB-2023-025682<br>レッドハットの shim および Red Hat Enterprise Linux における境界外書き込みに関する脆弱性 | - | 8.3 | 2024/2/7 | 1,825 |
| 16 | JVNDB-2024-002582<br>シーメンスの Tecnomatix Plant Simulation における境界外読み取りに関する脆弱性 | - | 7.8 | 2024/2/15 | 1,822 |
| 17 | JVNDB-2024-001804<br>HOME SPOT CUBE2 における複数のバッファオーバーフローの脆弱性 | - | 8.8 | 2024/2/6 | 1,780 |
| 18 | JVNDB-2024-002837<br>マイクロソフトの複数の Microsoft Windows 製品における権限を昇格される脆弱性 | - | 7.8 | 2024/2/22 | 1,776 |
| 19 | JVNDB-2024-002576<br>シーメンスの Tecnomatix Plant Simulation における境界外書き込みに関する脆弱性 | - | 7.8 | 2024/2/15 | 1,751 |
| 20 | JVNDB-2024-001785<br>トレンドマイクロ製 Air サポートにおける不適切なアクセス権の割り当ての脆弱性 | - | 7.8 | 2024/2/6 | 1,731 |

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 [2024 年 10 月～2024 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-2024-002832<br>Hitachi Global Link Manager における EL インジェクションの脆弱性 | - | 7.6 | 2024/2/21 | 2,310 |
| 2 | JVNDB-2024-001462<br>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 | 2024/2/5 | 1,555 |
| 3 | JVNDB-2024-001160<br>Hitachi Storage Plug-in for VMware vCenter 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 | - | 7.9 | 2024/1/31 | 1,419 |
| 4 | JVNDB-2023-003771<br>JP1/Performance Management 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 | - | 8.4 | 2023/10/4 | 878 |
| 5 | JVNDB-2023-003335<br>JP1/VERITAS 製品における脆弱性 | - | 9.8 | 2023/9/6 | 817 |