

2024.02.16  
Vuls祭り#9

JPCERT **CC**®

# CVEはこうしてやってくる

- EPSSとCVSS v4もチラ見してみよう

一般社団法人JPCERTコーディネーションセンター  
早期警戒グループ

シニアテクニカルリード 戸田 洋三  
脆弱性コーディネーター 戸塚 紀子

# 話者紹介



戸田洋三 ([yozo.toda@jpcert.or.jp](mailto:yozo.toda@jpcert.or.jp))

JPCERT/CC 早期警戒グループ

2001年10月からJPCERT/CCにてインシデント対応、定点観測、脆弱性調整、セキュアコーディングの啓発活動など。



戸塚紀子 ([noriko.totsuka@jpcert.or.jp](mailto:noriko.totsuka@jpcert.or.jp))

JPCERT/CC 早期警戒グループ

2021年4月からJPCERT/CCにて脆弱性コーディネーション業務担当。  
前職は、ベンダーPSIRTのメンバーとして15年ほど勤務。

## ■ 一般社団法人JPCERTコーディネーションセンター

### Japan Computer Emergency Response Team / Coordination Center

- コンピュータセキュリティインシデントへの対応、国内外にセンサーをおいたインターネット定点観測、ソフトウェアや情報システム・制御システム機器などの脆弱性への対応など国内の「セキュリティ向上を推進する活動」を実施
- サービス対象: 国内のインターネット利用者やセキュリティ管理担当者、ソフトウェア製品開発者等のセキュリティに関わる担当者
- インシデント対応をはじめとする、国際連携が必要なオペレーションや情報連携に関する**日本の窓口となる「CSIRT」**

※各国に同様の窓口CSIRTが存在する（米国のCISA、CERT/CC、中国のCNCERT/CC、韓国のKrcERT/CC等）

- 経済産業省からの委託事業としてサイバー攻撃等国際連携対応調整事業を実施
- サイバーセキュリティ基本法上の「サイバーセキュリティに関する事象が発生した場合における国内外の関係者との連絡調整を行う関係機関」
- サイバーセキュリティ協議会（2019年発足）の事務局をNISCとともに実施（事案対応の相談や情報共有活用の運用面を担当）

# お伝えする内容

---

- CVEはこうしてやってくる
- EPSSとCVSS v4もチラ見してみよう（簡単な紹介）

# CVEはこうしてやってくる



# 「Vuls祭り#1」でお話ししました

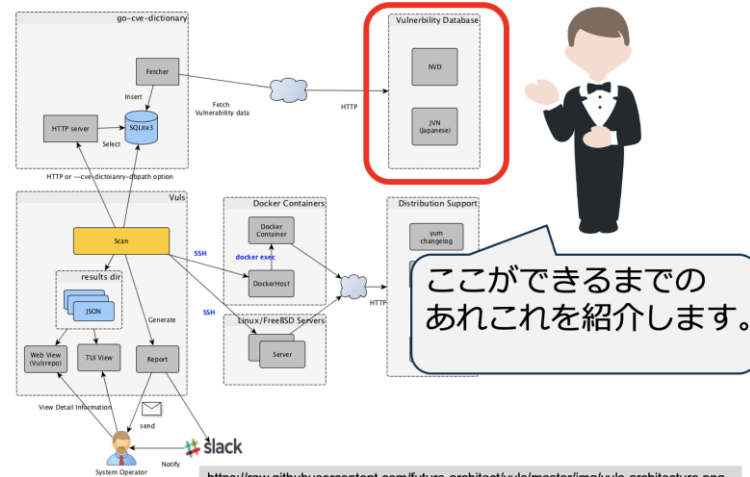
20th Anniversary  
JPCERT/CC

2016.09.26  
Vuls 祭り#1

脆弱性情報はこうして  
やってくる

JPCERT/CC 情報流通対策グループ  
戸田洋三

## お話の内容

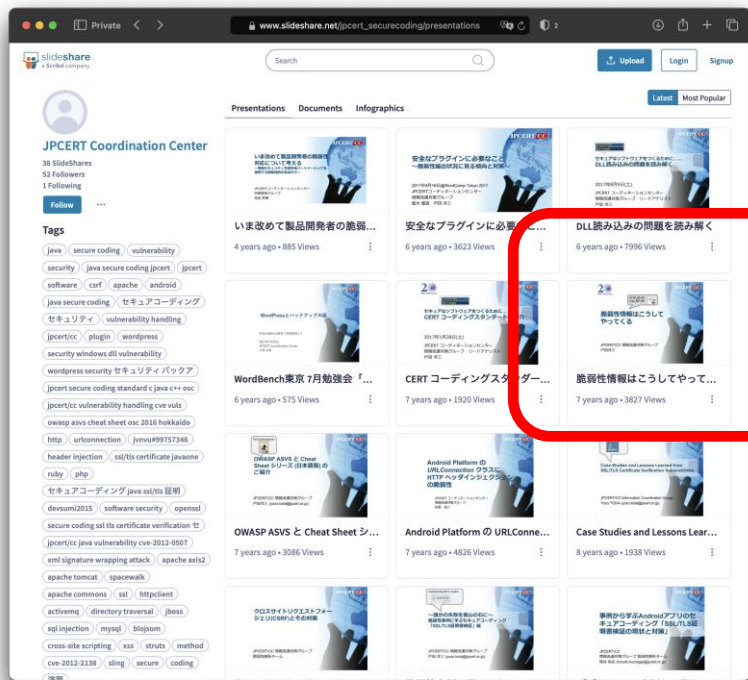


5

Copyright ©2016 JPCERT/CC All rights reserved.

JPCERT/CC

# 「Vuls祭り#1」でお話しました



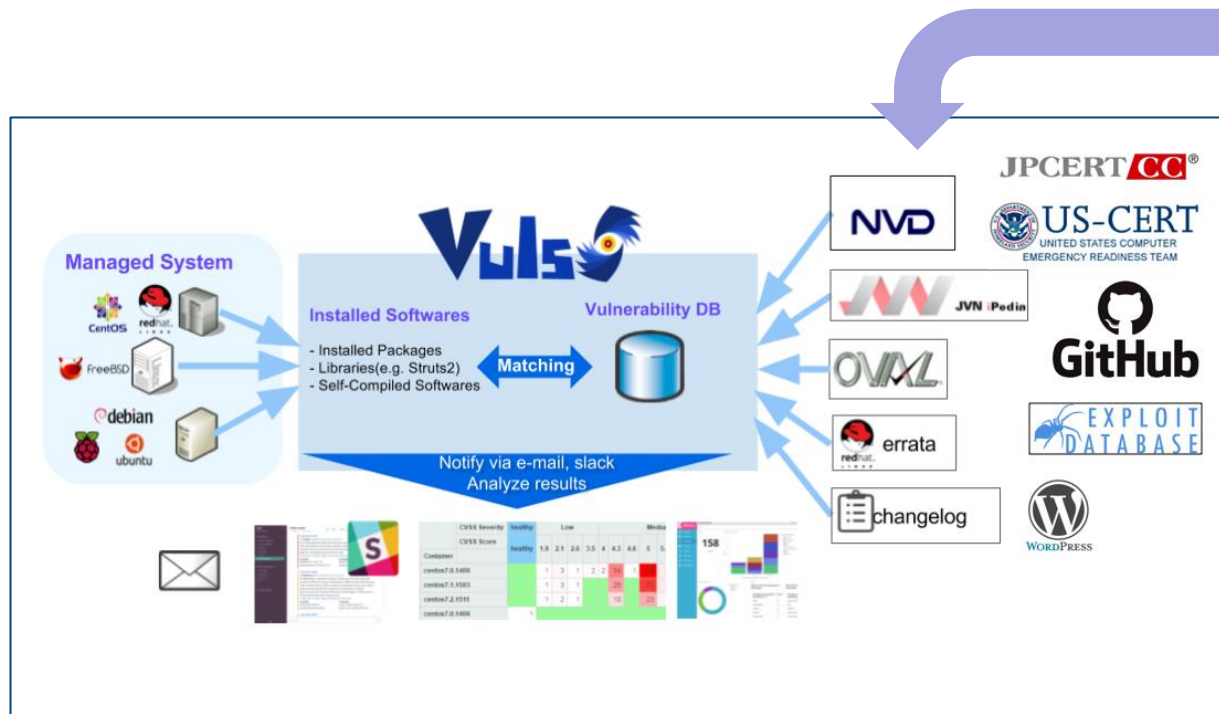
当時の資料は slideshare で見てね！

これ！

[https://www.slideshare.net/jpcert\\_securecoding/presentations](https://www.slideshare.net/jpcert_securecoding/presentations)



# CVEはこうしてやってくる



CVE®

今回はCVE情報が  
ここにやってくる  
までのあれこれをお  
しゃべりします。

<https://vuls.io/img/docs/vuls-abstract.png>



# 脆弱性の識別, 分類, 評価

脆弱性対応を適切に行うために...

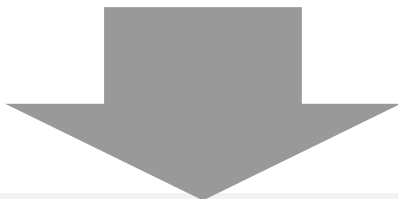


- 識別： **CVE**を使って対象の脆弱性を明確にする
  - 複数の脆弱性を扱う場面で誤解なく迅速に情報共有
- 分類： **CWE**を使って脆弱性の種類を簡潔に示す
  - 問題の性質を明確にし, 対応方法の迅速な理解につなげる
- 評価： **CVSS**を使って脆弱性による影響を測る
  - 多数の脆弱性に対応する際の優先度付け

# 脆弱性情報を識別する



脆弱性対応や他組織との情報交換のため、  
対象とする脆弱性を特定する方法が欲しい



CVE  
**C**ommon **V**ulnerabilities and **E**xposures

# CVE情報の例 : CVE-2023-29160

<https://www.cve.org/CVERecord?id=CVE-2023-29160>

**CVE-2023-29160** PUBLISHED View JSON

**Important CVE JSON 5 Information** +

**Assigner:** JPCERT/CC  
**Published:** 2023-06-13 **Updated:** 2023-06-13

Stack-based buffer overflow vulnerability exists in FRENIC RHC Loader v1.1.0.3. If a user opens a specially crafted FNE file, sensitive information on the system where the affected product is installed may be disclosed or arbitrary code may be executed.

**Product Status**

**Learn About the Versions Section** +

Vendor	Versions
FUJI ELECTRIC CO., LTD.	<i>Default Status: unknown</i>
<b>Product</b> FRENIC RHC Loader	<ul style="list-style-type: none"><li>affected at v1.1.0.3 and earlier</li></ul>

**References**

- <https://felib.fujielectric.co.jp/download/details.htm?dataid=45829407&site=global&lang=en>
- <https://jvn.jp/en/vu/JVNVU97809354/>

View additional information about [CVE-2023-29160](#) on NVD.  
(Note: The NVD is not operated by the CVE Program)



Assigner : このCVEを作成したCNA

このCVEレコードが示す脆弱性の説明

この脆弱性が指摘されている製品  
(提供者, 製品名称, バージョン)

この脆弱性情報の裏付けとなる情報源  
(「参考情報」ではないことに注意)

# CVE Program

<https://www.cve.org/>

The screenshot shows the CVE Program website homepage. At the top, there's a navigation bar with links like 'About', 'Partner Information', 'Program Organization', 'Downloads', 'Resources & Support', and 'Report/Request'. Below this is a search bar with a 'Find' button. A banner message welcomes users to the new CVE Beta website, mentioning the new format and the temporary hosting of CVE List keyword search on the legacy cve.mitre.org website. The main content area features the 'CVE® Program Mission' section, which states the goal is to identify, define, and catalog publicly disclosed cybersecurity vulnerabilities. It also mentions that there are 205,935 CVE Records accessible via Download or Search. Below this is a 'Learn More' button and a 'Become a Partner' button. The 'Access' section lists links for List of Partners, CNA Rules, CVE Record Lifecycle, and CVEProject on GitHub for Development. The 'Learn' section includes links for About CVE, Process, Program Organization, Related Efforts, Terminology, and CVE Services for CNAs. The 'Report/Request' section provides links for Report vulnerability/Request CVE ID, Request CVE Record be published/updated, and Report the use of a reserved CVE ID. The 'Access Resources Based on Role' section has three icons: CNA, Workflows, and Vulnerability Manager. A feedback link is provided. The footer contains links for Policies (Terms of Use, Privacy Policy, Website Security Policy), Media (News, Sign up for e-newsletter), Social Media (Facebook, LinkedIn, YouTube, Twitter), and Contact (CVE Program Support, CNA, CVE Website Support). A small disclaimer at the bottom states that the CVE List and associated references are subject to the terms of use, and that CVE is sponsored by the U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA).



- 1999年とあるワークショップでの提案が発祥
  - 複数の脆弱性データベース間の情報を関連付ける  
試み
- 米国政府の資金のもと、米国MITRE社のプロジェクトとして開始
- やがて脆弱性研究の興隆で業務逼迫
- 2016年あたりからは製品開発者（社）をCNAとする戦略へ

CNA ... CVE Numbering Authority

# trivia : CVE と NVD

<https://www.cve.org/About/RelatedEfforts#NVD>

**Related Efforts**

Links that redirect to external websites will open a new window or tab depending on the web browser used.

### National Vulnerability Database (NVD)

CVE and NVD are separate programs. The U.S. National Vulnerability Database (NVD) was launched by the National Institute of Standards and Technology (NIST) in 2005, while the CVE List was launched by The MITRE Corporation as a community effort in 1999.

NVD is a vulnerability database built upon — and fully synchronized with — the CVE List so that any updates to CVE appear immediately in NVD.

The CVE List feeds NVD, which then builds upon the information included in CVE Records to provide enhanced information for each CVE Record such as:

- Severity scores and impact ratings
- Common Platform Enumeration (CPE) information
- Fix information
- Searching by OS; by vendor name, product name, and/or version number; and by vulnerability type, severity, related exploit range, and impact
- CVE API for content updates

While separate, both CVE and NVD are sponsored by the U.S. Department of Homeland Security(DHS) Cybersecurity and Infrastructure Security Agency(CISA), and output from both programs are free for public use.

### Common Vulnerability Scoring System (CVSS)

The CVSS standard operated by the Forum of Incident Response and Security Teams (FIRST), which is a separate program from CVE, can be used to score the severity of software vulnerabilities identified by CVE Records. In general, severity scores for CVE Records are provided by NVD, but some CVE Records on the CVE List include severity ratings if the CNA publishing the record decides to include them.

CVSS Version 3.0 provides “a way to capture the principal characteristics of a vulnerability, and produce a numerical score reflecting its severity, as well as a textual representation of that score. The numerical score can then be translated into a qualitative representation (such as low, medium, high, and critical) to help organizations properly assess and prioritize their vulnerability management processes.”

**About**

- Overview +
- History +
- Process +
- Related Efforts -

- National Vulnerability Database (NVD)
- Common Vulnerability Scoring System (CVSS)
- Known Exploited Vulnerabilities (KEV) Catalog
- Common Weakness Enumeration (CWE™)
- Common Attack Pattern Enumeration And Classification (CAPEC™)
- ATT&CK®
- Metrics +

CVEとNVDは別の活動  
(ただしどちらもCISAがスポンサー)

NVDはCVE Programが公開しているデータにCVSSやCPE情報などを追加して公開している



脆弱性が発見されてからCVEレコードが公開されるまで

# CVE Record Life Cycle

<https://www.cve.org/About/Process>



脆弱性を  
発見

脆弱性を  
(CNAに)  
報告

(CNAが)  
CVE IDを予約

(CNAが)  
CVEレコードを  
アップロード

CVEレコードが  
公開される



# CVEと脆弱性調整

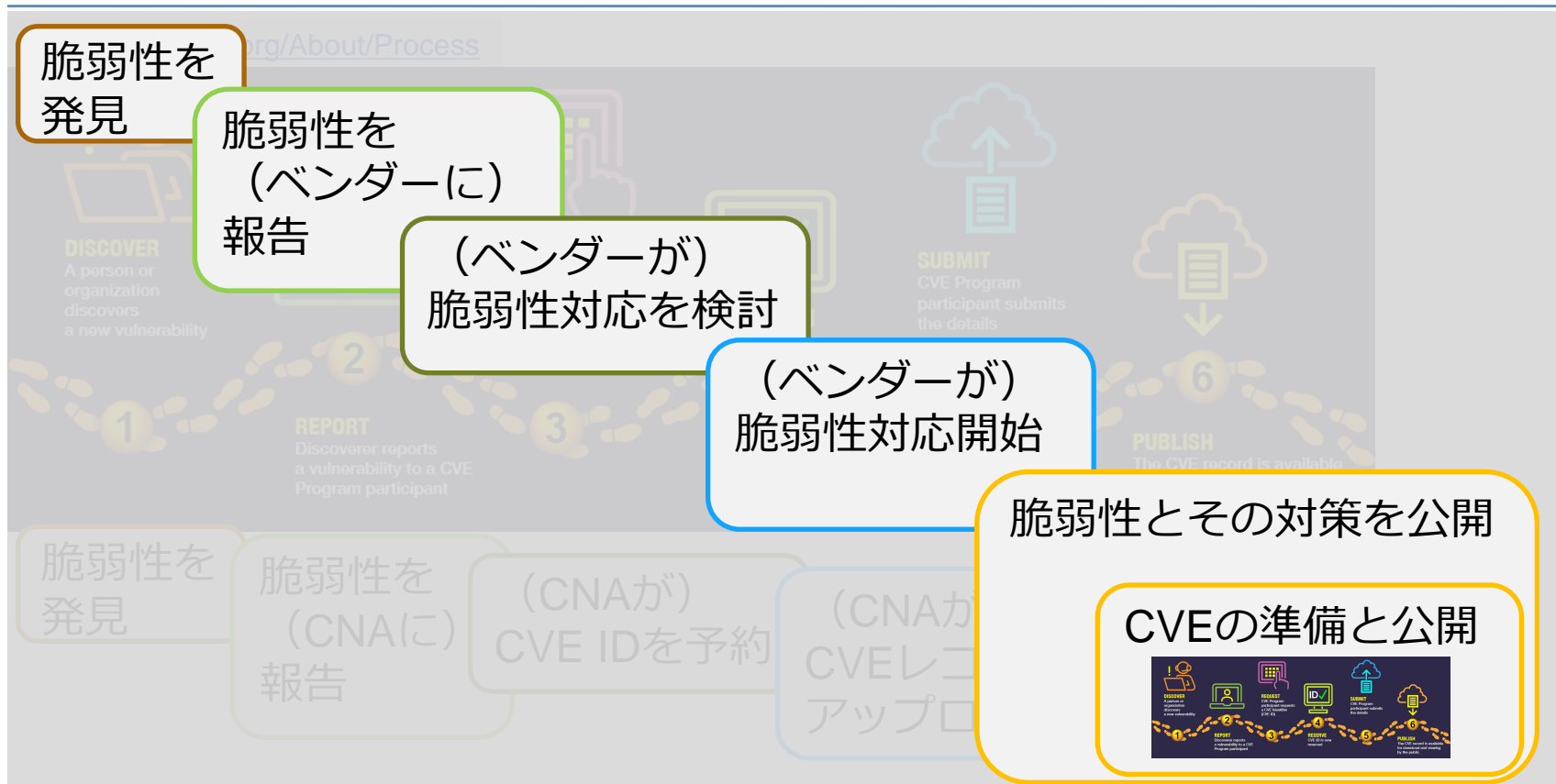
もともとのCVEは  
複数の公開情報の関連付け

製品を修正するベンダーとの連携は  
意識されていなかったのかな？

しかし, 脆弱性修正には  
ベンダーの対応が必要

関係者との脆弱性調整って  
重要だよね！

# CVE Record Life Cycle



# trivia : CNAの情報知りたい (1)

<https://www.cve.org/PartnerInformation/ListofPartners>

The screenshot shows the CVE.org website's 'List of Partners' page. The page has a dark blue header with the CVE logo and navigation links: About, Partner Information, Program Organization, Downloads, Resources & Support, and Report/Req. The main content area is titled 'List of Partners' and includes a note about external links, contact information for Top-Level Roots, Roots, CNAs, and CNA-LRs, and a search bar. Below the search bar, there are buttons for 'Request a CVE ID / Update a CVE Record' and 'Program Roles / Organization Types'. A sidebar on the right contains a 'Partner Information' section with a '+' icon and a 'List Of Partners' button. The main content area shows a search bar with the text 'Enter search terms' and a 'Search Tips' button. Below the search bar, it says '362 partners' and provides options to 'Show: 10' and 'Sort by: Partner (A to Z)'. A table lists the first four partners: 1E Limited, 42Gears Mobility Systems Pvt Ltd, Absolute Software, and Acronis International GmbH.

Partner	Scope	Program Role	Organization Type	Country*
1E Limited	All 1E products (including end-of-life/end-of-service products), as well as vulnerabilities in third-party software discovered by 1E that are not in another CNA's scope	CNA	Vendor, Researcher	UK
42Gears Mobility Systems Pvt Ltd	42Gears branded products and technologies only	CNA	Vendor	India
Absolute Software	Absolute issues only	CNA	Vendor	USA
Acronis International GmbH	All Acronis products, including Acronis Cyber Protect, Acronis Cyber Protect Home Office	CNA	Vendor	Switzerland

CNA一覧から検索しよう

各CNAの情報を公開している

- 脆弱性取り扱いポリシー
- 連絡先
- 対象製品
- アドバイザー一覧ページ

# trivia : CNAの情報知りたい (2)

<https://www.cve.org/PartnerInformation/ListofPartners/partner/Zyxel>

The screenshot shows the CVE.org partner page for Zyxel Corporation. The page includes a header with the CVE logo, a title 'Zyxel Corporation', and a subtitle 'Links that redirect to external websites will open a new window or tab depending on your browser settings'. Below this is a section titled 'Steps to Report a Vulnerability or Request a CVE ID' with two steps: 'Step 1: Read disclosure policy' (with a 'View Policy' link) and 'Step 2: Contact' (with an 'Email' link). A table lists details about Zyxel's participation: Scope (Zyxel products issues only), Program Role (CNA), Top-Level Root (MITRE Corporation), Security Advisories (View Advisories), Organization Type (Vendor), and Country\* (Taiwan). A footnote states '\* Self-identified by CNA'. At the bottom, there are four columns of links: Policies & Cookies (Terms of Use, Website Security Policy, Privacy Policy, Cookie Notice, Manage Cookies), Media (News, Blogs, Podcasts, Email newsletter sign up), Social Media (Twitter, LinkedIn, YouTube, Facebook, GitHub, New CVE Records, CVE Announce), and Contact (CVE Program Support, CNA Partners, CVE Website Support, CVE Program Idea Tracker). A footer contains legal disclaimers and copyright information.

**Zyxel Corporation**

Links that redirect to external websites will open a new window or tab depending on your browser settings

**Steps to Report a Vulnerability or Request a CVE ID**

Step 1: Read disclosure policy [View Policy](#)

Step 2: Contact [Email](#)

Scope	Zyxel products issues only
Program Role	CNA
Top-Level Root	<a href="#">MITRE Corporation</a>
Security Advisories	<a href="#">View Advisories</a>
Organization Type	Vendor
Country*	Taiwan

\* Self-identified by CNA

**Policies & Cookies**

- [Terms of Use](#)
- [Website Security Policy](#)
- [Privacy Policy](#)
- [Cookie Notice](#)
- [Manage Cookies](#)

**Media**

- [News](#)
- [Blogs](#)
- [Podcasts](#)
- [Email newsletter sign up](#)

**Social Media**

- [Twitter](#)
- [LinkedIn](#)
- [YouTube](#)
- [Facebook](#)
- [GitHub](#)
- [New CVE Records](#)
- [CVE Announce](#)

**Contact**

- [CVE Program Support](#)
- [CNA Partners](#)
- [CVE Website Support](#)
- [CVE Program Idea Tracker](#)

Use of the CVE® List and the associated references from this website are subject to the [terms of use](#). CVE is sponsored by the U.S. Department of Homeland Security (DHS) [Cybersecurity and Infrastructure Security Agency \(CISA\)](#). Copyright © 1999-2024, [The MITRE Corporation](#). CVE and the CVE logo are registered trademarks of The MITRE Corporation.

例えばアルファベット順末尾の  
Zyxel

脆弱性取り扱いポリシー

連絡先

対象製品

アドバイザリー一覧ページ



CVEレコードが公開されるパターンいろいろ

# パターン1：報告者からMITREへ

報告者がMITRE CNAにリクエスト, CVEレコード公開  
CVEレコードの References には報告者が公開している  
情報のみ



ベンダーには全く連絡せずにCVE公開？

ベンダーに連絡つかなかった？

それともベンダーは知ってるけど何も  
情報を出してない？

なんかモヤモヤ...

## パターン2：報告者からJPCERT/CCへ

報告者がJPCERT/CCに連絡, JPCERT/CCとベンダーとの調整を経てCVEレコード公開

CVEレコードの References にはベンダーの情報とJVNが掲載



ベンダーによる対策準備済み

このパターンのバリエーションとして、報告を受けたベンダーからJPCERT/CCへの調整依頼の場合もあり

MITREからJPCERT/CCにふってくることもあり



# パターン3：報告者からベンダーへ

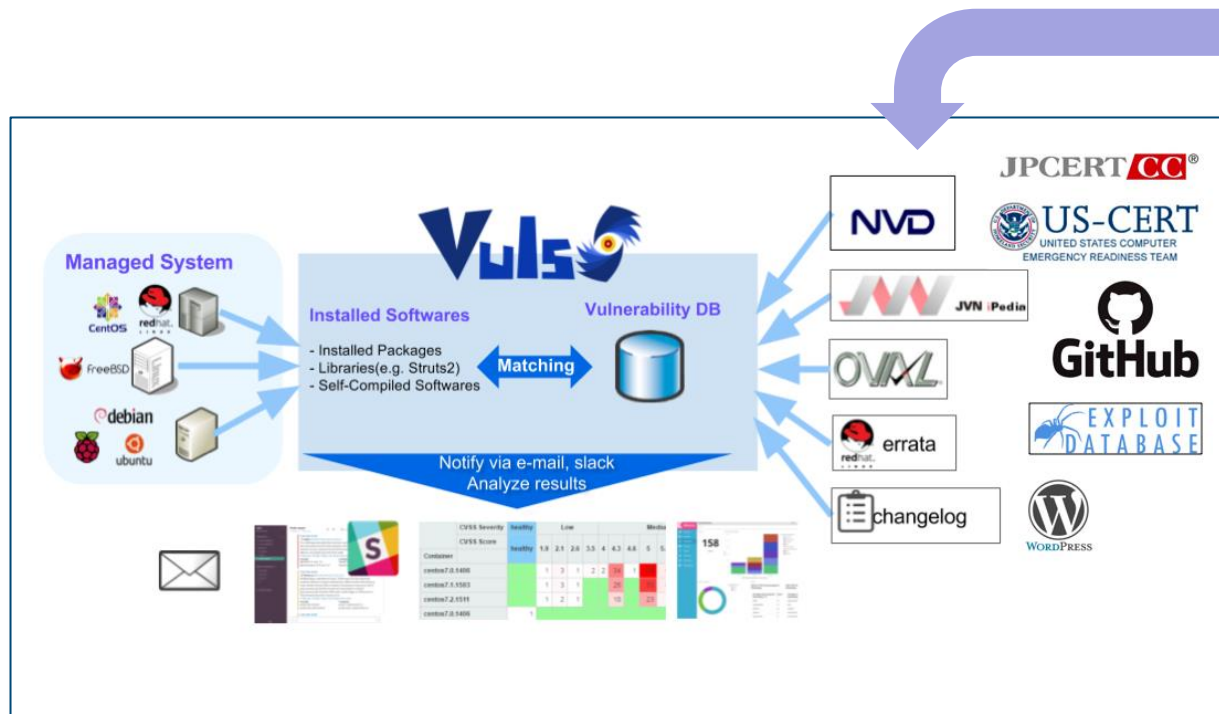
報告者がベンダーに連絡, ベンダーの準備を経てCVEレコード公開  
CVEレコードの References にはベンダーの情報が掲載



ベンダーによる対策準備済み

ベンダーがCNAの場合や, ベンダーが他のCNAにCVEをリクエストする場合など

# CVEはこうしてやってくる



CVE

というわけでCVE情報  
がここにやってく  
るまでのあれこれ  
をお話しました。

<https://vuls.io/img/docs/vuls-abstract.png>

# EPSSとCVSS v4もチラ見してみよう

# EPSS (Exploit Prediction Scoring System) とは

## ■ 概要

- FIRST epss-sigによる脆弱性対応の優先順位設定支援のための取り組み
- CVEごとに、今後30日間で悪用される確率（スコア）を0～100%の範囲で算出
- CVE Programが公開しているCVEが対象
- 機械学習を利用しており、計算式、モデル、ソースコード非公開
- ユーザーは、公開スコアを利用する（入手用APIあり）
- 現在、EPSS v3（2023年3月7日 アップデート）

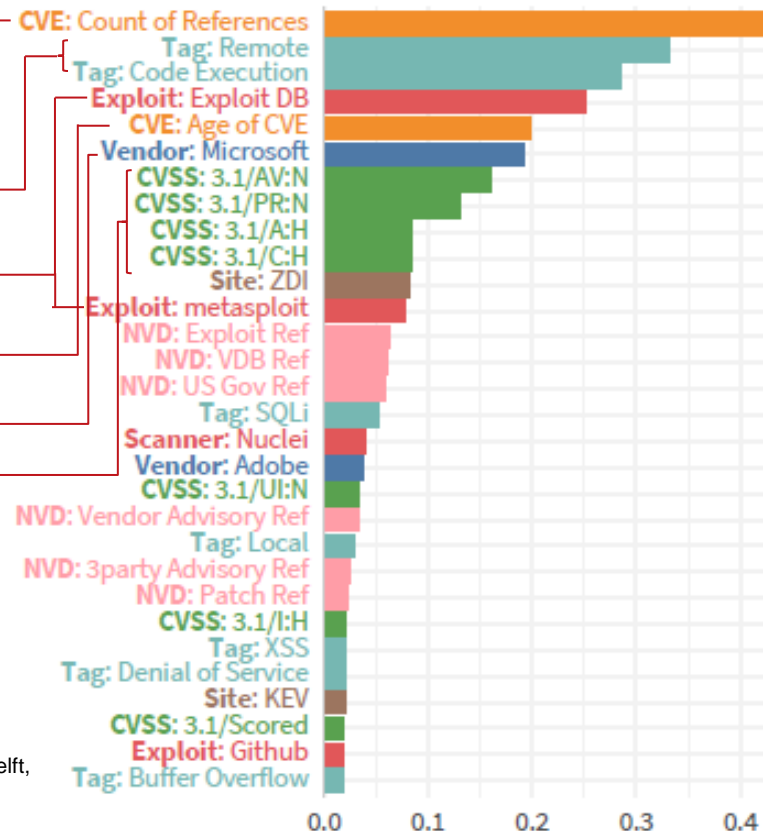
## ■ 注意点

- 悪用可能性に特化、深刻度は加味されていない
  - EPSSは低いですが、悪用された場合のリスクが高い脆弱性などもある
  - 適用判断には、CVSSなど他の指標との併用がお勧め
- CVE公開からの日数やエクスプロイトコードの有無などさまざまな情報源から算出
  - 日々情報が変化するので、スコアも変化する

# EPSSの情報源と重み

## ■ 計算で使用する情報源 (変数は1000以上)

- CVEに掲載のリファレンス数
- 観測している悪用実態 (Fortinet 等)
- 公開されたエクスプロイトコード有無  
(Exploit-DB, GitHub, Metasploit)
- CVEが公開されてからの経過日数
- 製品ベンダー
- CVSS評価 (NVD)
- セキュリティツールやスキャナーの  
情報  
など



参照元: Jay Jacobs, Sasha Romanosky, Octavian Suci, Ben Edwards and Armin Sarabi, Enhancing Vulnerability Prioritization: Data-Driven Exploit Predictions with Community-Driven Insights, 2023 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Delft, Netherlands, 2023, pp. 194-206, doi: 10.1109/EuroSPW59978.2023.00027

# EPSSのパフォーマンス

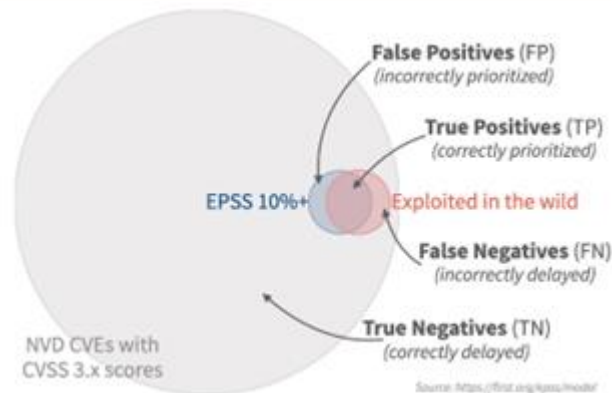
## ■ 2023年10月1日時点の予測

- CVE総数：139,000（以下概数）
- EPSS 10%以上：3,700
- 対応率：2.7%（3700/139000）

## ■ 10月末（30日間）悪用実績：3,800

- EPSS 10%以上：2,400
- 以外：1,400
- ヒット率：65%（2400/3700）

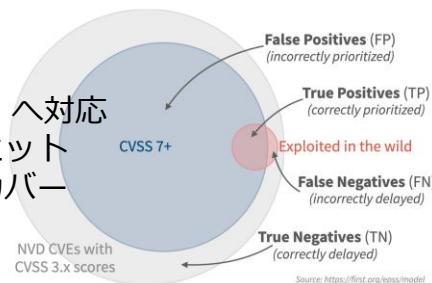
2.7%対応／65%有効／64%カバー



[参考]

CVSS v3.1：7以上へ対応

- ・ 57%（80,000/139,000）へ対応
- ・ 4%（3100/80000）のヒット
- ・ 84%（3100/3800）のカバー



参照元：FIRST「The EPSS Model」<https://www.first.org/epss/model>

# EPSS データソース例

## ■ EPSSスコア Top10 (2024/01/30)

データダウンロード元：First「EPSS Data」 [https://www.first.org/epss/data\\_stats](https://www.first.org/epss/data_stats)

#	CVE ID	EPSS	脆弱性の概要
1	CVE-2019-2725	0.97572	Oracle WebLogic Serverにおける リモートから任意のコード実行が可能な脆弱性
2	CVE-2018-7600	0.97571	Drupal における リモートから任意のコード実行が可能な脆弱性
3	CVE-2015-7297	0.97564	Joomla! における SQL インジェクションの脆弱性
4	CVE-2014-6271	0.97559	GNU Bashの脆弱性 (ShellShock)
5	CVE-2017-8917	0.97555	Joomla! における SQL インジェクションの脆弱性
6	CVE-2019-1653	0.97555	Cisco RV320およびRV325デュアルギガビットWAN VPNルーターにおける情報流出の脆弱性
7	CVE-2020-5902	0.97555	BIG-IP における リモートから任意のコード実行 が可能な脆弱性
8	CVE-2017-5753	0.97551	CPUの脆弱性 「Spectre」
9	CVE-2015-1635	0.97544	Windows OS における リモートから任意のコード実行が可能な脆弱性
10	CVE-2020-14750	0.97544	Oracle WebLogic Serverにおける リモートから任意のコード実行が可能な脆弱性

有名な名前付きの脆弱性やスコア値寄与度が高い「リモート」「コード実行」を含んだ脆弱性が多い  
同じ製品の脆弱性が複数ランクインしている



# CVSS v4.0 CVSS-Bにおける主な変更点

- 新規：AT（Attack Requirements：攻撃の要件）
  - AC（Attack Complexity：攻撃の複雑さ）の定義を2つ（AC, AT）に分割
- 更新：UI（User Interaction）
  - 不要（N）、Passive（P）、Active（A）の3択に
- 廃止：S（Scope）
  - C, I, A 評価の一部として、SC, SI, SA に置き換え

※ v4.0には、OTシステム（産業制御システム等）の考慮など、興味深い変更が多くあります。本日は、Base Metrics の部分だけ簡単に見てみます。概要をお伝えするため、かなり大胆に簡素化しています。詳細は、「参考情報」に掲載したサイトなどご覧ください。

# CVSS v4 AC を AT と AC に分離

■ AT：攻撃には、初期設定からの変更など特別な条件や環境が必要か？

None (N)	不要。初期設定のままで攻撃可能。
Present (P)	必要。特定の設定やモジュールの有効化などが必要。

■ AC：攻撃には、攻撃防御のための技術の回避が必要か？

Low (L)	不要。攻撃者は、脆弱なシステムに対して繰り返し攻撃できる。
High (H)	必要。例えば、推測などによりASLR（アドレス空間配置のランダム化）を突破するなど。

# CVSS v4 User Interaction の更新

## ■ 攻撃者以外のユーザー（人）が必要か？

None (N)	不要。 <ul style="list-style-type: none"><li>- リモートから標的にパケットを送信する</li><li>- 認証済ユーザー（攻撃者）がコードを実行して権限昇格する 等</li></ul>
Passive (P)	脆弱なシステムや攻撃者の誘いに対し、受動的に関わるユーザーが必要。 <ul style="list-style-type: none"><li>- 悪意あるサイトの閲覧（XSS、CSRF）</li><li>- 悪意あるバイナリを呼び出すアプリケーションの実行 等</li></ul> ユーザーによる、脆弱なシステムの保護機能の意識的回避はない。
Active (A)	脆弱なシステムや攻撃者の誘いに対し、意識的な操作をするユーザーが必要。 <ul style="list-style-type: none"><li>- ファイルを特定の方法でインポートする、特定のディレクトリに配置する</li><li>- ウェブアプリケーションに特定の文字列を送信する（Self-XSS）</li><li>- ファイルを開くなどの操作前のセキュリティ警告を無視する、受け入れる</li></ul>

※ 意識的な操作か、否かの判断が難しそうですね。

ユーザーが自身の操作の直接的な意味を意識しているかどうかのポイント？

# CVSS v4 Scope の廃止と SC, SI, SA の採用

- 理解が難しいScopeを廃止
- 影響度メトリクス（C, I, A）を2つに拡張
  - Vulnerable System：脆弱なシステム
    - 脆弱性が悪用されセキュリティポリシーが侵害される、その脆弱性があるシステム
      - 機密性：VC、完全性：VI、可用性：VA
  - Subsequent System：後続のシステム
    - 脆弱性が悪用された結果、セキュリティポリシーが侵害されるシステムだが、脆弱性のあるシステムではない
      - 機密性：SC、完全性：SI、可用性：SA

脆弱なWebサイト（XSS）



ユーザーのブラウザ  
（Script実行、CI侵害）

# CVSS v4 脆弱なシステム・後続のシステム

## ■ 脆弱なサービスやモジュールが大きなユニット（アプリケーション）の一部

- 分離できない（単独で機能しない）場合は、脆弱なシステムはユニット全体
- 分離できれば、脆弱なシステムはサービスやモジュールのみ



参考：CVSS v4 資料

- FAQ : <https://www.first.org/cvss/v4.0/faq>
- Specification : <https://www.first.org/cvss/v4.0/specification-document>
- Example : <https://www.first.org/cvss/v4.0/examples>

# CVSS v4.0 と v3.1 のベーススコア比較例

## ■ CVE-2022-41741 NGINXの脆弱性（問題のコードはngx\_http\_mp4\_module）

- 細工されたファイルを使用し、ローカル攻撃者が NGINX ワーカーのメモリを破壊し、NGINX ワーカーの終了またはその他の影響を引き起こす
- ngx\_http\_mp4\_module を使用してビルドされた NGINX 製品のみ影響を受ける
  - AT:P 特定の設定やモジュールの有効化などが必要。

CVSS v3.1 AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H 7.0

CVSS v4.0 AV:L/AC:L/AT:P/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N 7.3

## ■ CVE-2022-21830 (Rocket.chat Livechat の Self-XSSの脆弱性)

- 攻撃者は、ユーザーがチャットに悪意のあるスクリプトを入力するよう促す
  - UI:A ユーザーは意識的な操作をする
- 影響を受けるシステムは、スクリプトが実行されるユーザーのブラウザー
  - SC:L/SI:L/SA:N ブラウザーが侵害されるシステムだが、脆弱性のあるシステムではない

CVSS v3.1 AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N 6.1

CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:L/SI:L/SA:N 5.1

## ■ EPSS

FIRST epss-sig 公開サイト

<https://www.first.org/epss/>

IEEE : EPSS 関連論文

Jay Jacobs, Sasha Romanosky, Octavian Suci, Ben Edwards and Armin Sarabi, *Enhancing Vulnerability Prioritization: Data-Driven Exploit Predictions with Community-Driven Insights*, 2023 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Delft, Netherlands, 2023, pp. 194-206, doi: 10.1109/EuroSPW59978.2023.00027.

<https://ieeexplore.ieee.org/document/10190703>

Future VulsBlog : EPSS入門 : 脆弱性管理を変革する新指標の理解と活用方法

<https://vuls.biz/blog/articles/20240115a/>

## ■ CVSS v4.0

FIRST 公開サイト

<https://www.first.org/cvss/v4-0/>

FIRST 説明資料 : Announcing CVSS v4.0 (PDF)

<https://www.first.org/cvss/v4-0/cvss-v40-presentation.pdf>

CVSS v4.0 スコア値の例 : Common Vulnerability Scoring System v4.0: Examples

<https://www.first.org/cvss/v4.0/examples>



# JPCERT/CCへのご連絡は

## 本資料に関するお問い合わせ

- Email : [vultures@jpcert.or.jp](mailto:vultures@jpcert.or.jp)
- <https://jvn.jp/>

## JPCERTコーディネーションセンター

- Email : [pr@jpcert.or.jp](mailto:pr@jpcert.or.jp)
- <https://www.jpcert.or.jp/reference.html>



※資料に記載の社名、製品名は各社の商標または登録商標です。

ご清聴ありがとうございました

