Engineer

CVE

公表された脆弱性一件ごとに共通のIDを付ける公開一覧

どのようなものか

CVEはCommon Vulnerabilities and Exposuresの略で、公表されたサイバーセキュリティー上の脆弱性を、一件につき一つのCVE Recordにまとめる公開カタログです。CVE Programは、その使命を、脆弱性の識別、定義、登録と説明しています。二人の人や二つのツールが、同じ不具合を指していると分かるようにするためです。CVEという語は、プログラムにも、一覧にも使います。「そのライブラリーには未解決のCVEが二件ある」のように、一つの項目を緩く指すこともあります。

各記録にはCVE IDが付きます。形式は、接頭辞の `CVE` 、四桁の年、四桁以上の連番です。そのため、 `CVE-1999-0067` 、 `CVE-2019-12345` 、 `CVE-2021-7654321` は、いずれも有効です。連番の桁数に上限はありません。年は、IDを予約した年か、脆弱性が公表された年です。プログラム自身も、「年の部分は、脆弱性が発見された時期を示すためには使わない」と述べています。

一つの中央窓口が、すべてのIDを配るわけではありません。CVE Numbering Authorities、略してCNAは、プログラムから、各自の担当範囲でIDを割り当て、記録を公開する権限を得た組織です。ベンダー、研究者、オープンソースプロジェクト、緊急対応チーム、オンラインサービスの運営者、バグ報奨金制度の提供者、コンソーシアムなどが含まれます。すべてのCVE RecordはCNAが追加します。CNAになるための料金や契約はなく、プログラムは2016年以降、積極的に参加組織を増やしています。

記録には、変化の過程に応じて三つの状態があります。最初はReserved、予約済みです。CNAが確保したIDを、関係者が、公表前の初期対応を調整するために使います。CNAが、少なくともID、短い説明、影響を受ける製品とバージョン、公開された参照先を記入すると、Published、公開済みになります。IDを使うべきでなくなれば、Rejected、却下済みになります。その場合も、IDを持つ人が無効だと確認できるよう、記録は一覧に残ります。

発想は1999年にさかのぼります。MITREの技術者David E. MannとSteven M. Christeyが、1999年1月にPurdue Universityのワークショップで、ホワイトペーパーとして構想を発表しました。1999年9月に一覧を公開し、当初の記録は321件でした。

概念を判断に生かす

「CVEとは？」を実際の判断に生かしましょう。その概念を、開発または購入するシステムに結び付けて考えるお手伝いをします。 アカウント、パスワード、権限を整理し、業務に必要なアクセスだけを付与し、退職者の権限は当日に解除します。

サービスを見る お問い合わせ →

用語の背後にある前提を検証する

解説とリンク先の実績を参考に、プロジェクトについての質問を整理してください。ツールを選ぶ前に、前提を一緒に検討できます。 Linuxサーバーを守る1,000件のRBACルールを作成 — 1,000 セキュリティ上の穴を塞ぐアクセスルール

Linuxサーバーを守る1,000件のRBACルールを作成 お問い合わせ →

なぜ重要なのか

脆弱性の報告が役立つには、別の報告と同じ問題を扱っているか、読んだ人が判断できる必要があります。CVE IDが、それを解決します。同じIDを持つ二つの勧告、スキャナーの検出結果、対応チケットは、同じ不具合についてのものです。多くの主要OSベンダーが、問題を告知した時点から全員が同じIDを持てるよう、勧告にCVE IDを記載します。世界中のセキュリティー製品やサービスも、報告にCVE Recordを組み込んでいます。

ほかのサービスは、一覧と並立するのではなく、その上に構築されています。NISTが2005年に開始した米国のNational Vulnerability Databaseは、別のプログラムですが、CVE Recordを基礎に、各記録へ独自の分析を加えます。CISAのKnown Exploited Vulnerabilities、KEVカタログは、攻撃者が実際に利用したと確認された不具合を列挙します。各項目にCVE IDを示し、対応する記録へリンクします。

CVEについて特に役立つのは、何を表さないかを知ることです。深刻度の測定には、別の標準であるCommon Vulnerability Scoring System、CVSSを使います。運営するFIRSTは、世界のコンピューターセキュリティー対応チームを支援することを使命とする、米国拠点の非営利団体です。CVSSバージョン4.0は、Base、Threat、Environmental、Supplementalという評価項目のグループを使い、脆弱性を0から10で評価します。基礎、脅威、環境、補足の各項目で、数値をNone、Low、Medium、High、Criticalという深刻度、すなわち、なし、低、中、高、緊急に対応させます。Criticalの範囲は9.0から10.0です。CVE Record Formatは、

CNAが記録へCVSSスコアを含めることを認めています。ただし、スコアはCVSSのもので、ID自体の性質ではありません。同じ不具合に、発行元の異なる複数のスコアが付くことも、一つも付かないこともあります。

CVEは、弱点の種類でもありません。Common Weakness Enumeration、CWEは、コミュニティーが作る弱点の一覧です。ソフトウェア、ファームウェア、ハードウェア、サービスにある、条件次第で脆弱性を生む状態を扱います。CVE Programは、CWEをCVE Recordの根本原因と説明しています。CVEが特定の製品の一つの不具合を示すのに対し、CWEは、その背後にある誤りの種類を示します。たとえば、SQLインジェクションはCWE-89という弱点で、その誤りが見つかった製品には、それぞれ個別のCVE IDが付きます。

実際の活用例

Bashの2014年の不具合、Shellshockを見ると、三つの仕組みを並べて確認できます。cve.orgは、JSON形式のCVE Record Formatで記録を表示します。この記録の先頭部分は、次のとおりです。一部のフィールドを省き、並べ替えています。

```
{
  "dataType": "CVE_RECORD",
  "dataVersion": "5.1",
  "cveMetadata": {
    "cveId": "CVE-2014-6271",
    "assignerShortName": "debian",
    "state": "PUBLISHED",
    "dateReserved": "2014-09-09T00:00:00.000Z",
    "datePublished": "2014-09-24T18:00:00.000Z",
    "dateUpdated": "2025-10-22T00:05:36.342Z"
  }
}
```

CNAとしてのDebianは、2014年9月9日にIDを予約し、十五日後に記録を公開しました。説明によると、バージョン4.3までのBashは、環境変数の値にある関数定義の後に続くテキストを処理します。そのため、細工した環境を通して、遠隔の攻撃者が任意のコードを実行できます。最初の修正が不完全で、残った問題に、CVE-2014-7169という別のIDが付いたことも記録しています。一度だけパッチを適用して止めたチームは、なお危険にさらされていました。

記録には、続いて、三つの異なる出所のコンテナーがあります。CNAコンテナーには、Debianの説明と参照先が入っています。CVE Program Containerは、独自の参照先を加えます。三つ目は認定データ発行者（Authorized Data Publisher）

による、CISA ADP Vulnrichmentというコンテナーで、CVE IDだけでは分からない情報を加えています。

```
{
  "cvssV3_1": {
    "version": "3.1",
    "vectorString": "CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H",
    "baseScore": 9.8,
    "baseSeverity": "CRITICAL"
  }
}
```

ベクター文字列は、9.8という値の根拠を示します。ネットワーク経由の攻撃で、複雑さは低く、権限も利用者の操作も不要で、機密性、完全性、可用性への影響はいずれも大きいという評価です。同じコンテナーは、OSコマンドインジェクションの弱点分類であるCWE-78に不具合を対応付け、CISAが2022年1月28日にKEVカタログへ追加したことも記録しています。つまり、一つの記録に、CVE ProgramのID、FIRSTが公開するCVSSのあるバージョンによるスコア、CWEの弱点分類が入っています。それぞれ、出所も、答える問いも異なります。

日常の運用では、CVE IDは、読み物というより照合のキーとして重要です。当社のセキュリティーページは、通常の手順を説明しています。各システムを構成する部品を一覧にし、以前は動いたからと信用せず、公開された勧告と照合します。その検査で得た問題を、勧告までさかのぼり、解消するアップグレードまで追うために使えるのが、CVE IDです。

問題が起きるところ

スコアを、そのままリスクと読んでしまいます。 ThreatやEnvironmentalの値を誰も与えない場合、CVSS 4.0の仕様は、最悪を想定する既定値で補います。NVDや製品の保守担当者は、通常Baseスコアだけを公開するとも記しています。外部から到達できないコンポーネントの9.8は、自分の環境のリスクが9.8という意味ではありません。仕様に従い、BaseだけならCVSS-B、ThreatとEnvironmentalも適用したならCVSS-BTEと明記します。作業の優先順位を決める前に、自分たちのシステムのEnvironmental値を加えます。

CVE、CVSS、CWEを混同します。 「9.8のCVE」は、識別子とスコアを混ぜています。「SQLインジェクションのCVE」は、個別の不具合と、不具合の分類を混ぜています。チケットや報告では、CVEのID、バージョンを添えたCVSSのスコア、CWEの根本原因を分けて記します。

ベクターなしに、数値だけを引用します。 FIRSTは、CVSSデータを公開する人に、数値とともにベクターも公開するよう求めています。評価の前提を調べられるようにするためです。数値だけでは、検証も、CVSSのバージョン間の比較も、自分の環境に合わせた調整もできません。バージョンを示す `CVSS:3.1/` や `CVSS:4.0/` の接頭辞も含め、ベクター全体を保存します。

IDの年を、発見日と読んでしまいます。 年が示すのは、IDを予約した時期か、不具合が公表された時期です。2014年のIDが、1990年代に出荷したコードを説明することも、十二月に見つかった不具合に翌年の番号が付くこともあります。日付には、IDではなく、記録の `dateReserved` と `datePublished` フィールドを使います。

四桁だと思い込みます。 連番は四桁以上で、上限がありません。そのため、`CVE-\d{4}-\d{4}` のようなパターンは、長いIDを気付かないまま途中で切ります。代わりに `^CVE-[0-9]{4}-[0-9]{4,}$` で照合します。先頭のゼロを失わないよう、IDは数値ではなく文字列として扱います。

Rejectedの記録を、存在しないものとして扱います。 却下したIDを一覧に残すのは、無効だと利用者へ伝えるためです。無視するツールも、未解決の問題として数えるツールも、それぞれ逆の方向へ誤らせます。 `state` フィールドを読み、`REJECTED` を明示的に扱います。

記録を、完成したものと考えます。 Shellshockの記録が最後に変わったのは、公開から十一年後の2025年10月です。KEVへの登録も2022年1月でした。CVSSの仕様は、Threatグループで、時間とともに変わる脆弱性の状況を扱います。修正せず受け入れた問題については、その根拠となる記録を、決めた周期で読み直します。

最初の修正で止めてしまいます。 Shellshockに二つ目のIDが必要だったのは、最初のパッチで、不具合の一部が残ったためです。記録ごとの説明と参照先を読み、関連して後から付いたIDも調べます。コンポーネントを指すすべてのIDが解消するまでは、問題を完了にしません。

CVEがないことを、脆弱性がないことと考えます。 CVEが扱うのは、公表され、担当範囲内のCNAからIDが付いた脆弱性です。自社コードの不具合には、誰かが報告し、公開するまではCVEがありません。依存先を一覧と照合して分かるのは、ほかの人が見つけた問題です。自分たちのコードには、別に静的解析、レビュー、テストが必要です。

参考資料

- CVE Program：概要 — 使命、CVE Record、IDを割り当て記録を公開する参加組織を説明します。
- CVE Program：手順 — IDの形式、記録に必要な最低限の内容、三つの状態を説明します。
- CVE Program：関連する取り組み — NVD、CVSS、KEVカタログ、CWEとCVEの関係、それぞれの違いを説明します。
- Common Vulnerability Scoring System v4.0：仕様書 — FIRSTの評価項目のグループ、スコアの表記、深刻度の段階を説明します。
- CVE Record Format — CVE Servicesが使うバージョンで、記録の構造を定めるJSON定義です。
- CVE Program：よくある質問（アーカイブ）

用語集

実際の制約に合わせて選ぶ

デプロイの流れ、運用上のリスク、緊急対応の担当者をお知らせください。検査、復旧手段、明確な責任の所在を伴う変更の範囲を定められます。

料金を見る お問い合わせ →

用語を実務に結び付ける

「CVEとは？」がお客様の組織にどう当てはまるかをご相談ください。現在のシステムの具体例が一つあれば、話を始められます。

サービスを見る

welcome@engineer.company +45 50 10 61 84 デンマーク、コペンハーゲン

このページを持ち歩く

連絡先カード

心を込めて丁寧に制作： D.

CVR 45969703 · Tagensvej 105C, 3. th, 2200 København N

著作権 © 2025 – 現在 · Engineer ApS · すべての権利を留保します。

印刷元： https://engineer.company/ja/glossary/cve/