地政学的変動下における米国外脆弱性情報の評価と課題、示唆：持続可能なエコシステムへの提言

井上 圭[1]

概要：近年の米国国家脆弱性データベース（NVD）の更新遅延や CVE Foundation の発足は、世界が米国資金に依存した脆弱性情報基盤に大きなリスクを抱えていることを示している。本稿では、日本（JVN）、シンガポール（SingCERT）、オーストラリア（ACSC）、欧州（EUVD）、さらには Vulnrichment、中国（CNNVD）、ロシア（FSTEC/BDU）などの代替・補完情報源を取り上げ、その特性・利点・限界を比較検討する。その結果、現状では NVD を完全に代替することは困難であるが、複数の情報源を組み合わせることでリスクを低減できることを示す。さらに、将来的には国際的な共同体による多国間のデータガバナンスが不可欠であり、日本がこの分野で主導的役割を果たし得ることを提言する。

キーワード：CSS 2025，NVD, Vulnerability Management

Assessment of vulnerability information outside the United States under geopolitical changes, and its challenges and implications: Recommendations for a sustainable ecosystem

Kei INOUE [*1]

Abstract: Recent delays in updating the U.S. National Vulnerability Database (NVD) and the launch of the CVE Foundation indicate significant risks to the world's vulnerability information infrastructure, which relies heavily on U.S. funding. This paper examines alternative and complementary information sources, including Japan (JVN), Singapore (SingCERT), Australia (ACSC), Europe (EUVD), as well as Vulnrichment, China (CNNVD), and Russia (FSTEC/BDU), and compares their characteristics, advantages, and limitations. The results show that while it is currently difficult to completely replace the NVD, combining multiple information sources can mitigate risks. Furthermore, we argue that multinational data governance by an international community is essential in the future and suggest that Japan can play a leading role in this field.

Keywords: CSS 2025, NVD, Vulnerability Management

1. はじめに

サイバーセキュリティの脅威が日々増大する現代において、脆弱性情報は組織の継続性を維持するための基盤である。しかし、現在の脆弱性情報は米国主導のシステムに過度に依存しており、地政学的リスクを内包している。近年の NVD[*2]遅延やトランプ政権化における資金削減は、米国の政策や予算編成プロセスが世界的な脆弱性管理に直接影響を与える構造的課題を露呈した。本稿はこうした課題を踏まえ、米国外の情報源の有効性と限界を分析し、より分散的かつ強靭なエコシステム構築への示唆を与えることを目的とする。

2. 現在の脆弱性情報を取り巻く状況の変化

今日のサイバー脅威環境は絶えず変化しており、脆弱性情報源を単一に依存することは、リスクを伴う状況となっている。例えば、米国国立脆弱性データベース（NVD）における最近の分析遅延は、NVD の運営主体である米国国立標準技術研究所（National Institute of Standards and Technology：NIST）や国土安全保障省[*3]（Department of Homeland Security：DHS）の政府予算編成プロセスや NVD の運営を行う外部委託契約の更新プロセスにおける課題に直面したことにより発生した。この事態は、単なる技術的な問題ではなく、米国の国内政策や行政手続きが、脆弱性管理というグローバルな公共サービスに直接的な影響及ぼすという構造的な脆弱性を全世界に知らしめた。これは、グローバルで NVD の情報を参照するという、集中型アプ

1 株式会社ラック
サイバー・グリッド・ジャパン
次世代セキュリティ技術研究所
兼　ナショナルセキュリティ研究所
kei.inoue@lac.co.jp
2 https://nvd.nist.gov/vuln/
3 https://www.nist.gov/

ローチの脆弱性を浮き彫りにした。この状況から、CVE プログラムに関しては、MITRE 社[*4]ではなく財団化した CVE Foundation[*5]により管理されるようになるなど、政府の影響を受けないものに移管される事象が発生している。

欧州連合サイバーセキュリティ機関[*6]（ENISA）では、NIS2 指令[*7]の義務付けにより、欧州脆弱性データベース[*8]（EUVD）を最近立ち上げた。EUVD は、EU 内で販売または使用される製品やサービスに影響を与える脆弱性に関する、集中化された信頼性の高い実用的な情報源となることを目指している。これには、各国の CSIRT（Computer Security Incident Response Team）、ベンダー、CISA の既知の悪用された脆弱性カタログ[*9]（Known Exploited Vulnerability Catalog：KEV Catalog）や CVE Foundation の CVE プログラムなどの既存のデータベースからのデータが統合されている。また、EUVD は、CVE ID と並行して独自の EUVD 識別子を割り当て、自動化のために Common Security Advisory Framework[*10]（CSAF）をサポートする。

NVD の運用上の問題、特に CVE エンリッチメントの遅延やバックログは、EUVD のようなイニシアチブを直接的に促進した。これは、サイバーセキュリティにおける地域的なデジタル主権への世界的な動きを示している。NVD の課題が、他の地域が独自の堅牢で独立した脆弱性データベースを開発するきっかけとなり、グローバルなサイバーセキュリティガバナンスの転換と地域的な自給自足への推進が示唆されている。また、EUVD の目標に見られるように、「実用的な」および「文脈化された」脆弱性情報への重点の増大は、脆弱性管理が単に欠陥をリストアップする段階から、実際の脅威状況に基づいて積極的に優先順位付けし、緩和する段階へと成熟していることを示している。

3. 脆弱性管理における基礎概念

脆弱性管理においては、CVE-ID や CVSS Base Score などのフレームワークを基にした判断を行う。以下に代表的なフレームワークを示す。

3.1 Common Vulnerabilities and Exposures (CVE)

CVE は、既知のセキュリティ脆弱性を識別し、カタログ化するための公開データベースであり、それぞれに一意の ID（CVE-[年]-[番号]）を割り当てる。MITRE Corporation によって管理されている CVE プログラムは、サイバーセキュリティコミュニティ全体で一貫した追跡とコミュニケーションに不可欠な標準化された命名規則を提供する。脆弱性が CVE として認定されるには、独立して修正可能であること、単一のコードベースに影響を与えること、およびベンダーによって文書化された負のセキュリティ影響が認められていること、という特定の基準を満たす必要がある。

CVE プログラムの管理は長年米 MITRE Corporation が運営してきたが、運営体制をより自足可能で透明性の高いものにするために CVE Foundation が設立され、段階的に移行が始まっている。

3.2 Common Vulnerability Scoring System (CVSS)

CVSS[*11]は、SCAP（Security Content Automation Protocol）で定義された標準仕様の一つであり、脆弱性それ自体の影響度を示すフレームワークである。FIRST が管理している。Base Score は脆弱性の深刻度を数値（0-10）で評価し、Vector 値により詳細を示している。脆弱性それ自体の評価であるため、CVSS Base Score だけでは実際の悪用可能性やビジネスへの影響を反映しておらず、リスクの全体像を把握することはできない。

3.3 Common Weakness Enumeration (CWE) & Common Platform Enumeration (CPE)

CWE[*12]は、CVSS 同様に SCAP の標準仕様の一つであり、セキュリティ上の脆弱性の種類を識別するための共通基準である。MITRE 社により管理・運営がされている。SQL インジェクションやバッファオーバーフローなどの脆弱性の種類を体系化したものである。

CPE[*13]も、CVSS 同様に SCAP の標準仕様の一つであり、IT システム、ソフトウェア、およびハードウェアコンポーネントの標準化された命名スキームである。NIST が管理している。cpe:/a:apache:http_server:2.4.54 のような表記を行い、ベンダーやソフトウェア名、バージョンなどを特定することができる。NVD のエンリッチメントでは、CPE は製品特定のために重要な役割を占める。脆弱性情報においては、これをキーとして情報を付与していくことになる。

3.4 Known Exploited Vulnerabilities (KEV) & Exploit Prediction Scoring System (EPSS)

KEV カタログは、CISA によって維持されている、実際に悪用されている脆弱性の公式リストである。米国において、連邦政府機関は KEV カタログに登録された脆弱性を 2 週間以内に対応することが義務付けられている（拘束力のある運用指令 BOD 22-01[*14]）。すべての組織にとって、KEV

4 https://www.mitre.org/
5 https://www.thecvefoundation.org/
6 https://www.enisa.europa.eu/
7 https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng
8 https://euvd.enisa.europa.eu/
9 https://www.cisa.gov/known-exploited-vulnerabilities-catalog
10 https://www.csaf.io/
11 https://www.first.org/cvss/
12 https://cwe.mitre.org/
13 https://nvd.nist.gov/products/cpe
14 https://www.cisa.gov/news-events/directives/bod-22-01-reducing-significant-risk-known-exploited-vulnerabilities

にリストされている脆弱性の修復を優先することが強く推奨されている。また、悪用の有無は、CISA が管理していることもあり米国においての発生や認知を基準としている。

EPSS[*15]は、FIRST によって管理されている、脆弱性が 30 日以内に悪用される確率を機械学習を用いて 0.0 から 10.0 で推定したデータである。これは動的であり、「脅威前の情報」を提供することで、これから悪用が多くなる可能性が高くなるという「天気予報」のような役割を担う。

3.5 Stakeholder-Specific Vulnerability Categorization (SSVC)

SSVC[*16]は、脆弱性優先度を意思決定するためのフレームワークであり、米国 CISA 及び Carnegie Mellon University[*17] によって策定された。CVSS が脆弱性そのものの深刻度を数値化して示すのに対し、SSVC は組織や関係者（Stakeholder）の視点を反映しており、「今、対応すべきか」を判断することを目的としている。評価はスコアではなく、複数の意思決定ポイント（Decision Points）で分岐し、最終的に推奨する対応を出力する。

複数のステークホルダーに対応するために判断決定木（Decision Tree）が用意されているが、基本的には、脆弱性の悪用状況（Exploit Status）・影響範囲（System Exposure）・組織へのミッション影響（Mission Impact）・安全性や人命リスク（Safety Impact）などの要素を組み合わせて評価を行う。その為、数値では表せないリスク許容度などの文脈を示せることが特徴であり、これに CVSS Base Score や EPSS などを併用することで、より現実的な脆弱性対応の意思決定が可能になる。

3.6 Framework と脆弱性管理

近年のコンピュータやソフトウェアの普及により、発見される脆弱性が増加した。それにより、対処すべき脆弱性の数が増加し、ソフトウェア更新などの脆弱性対応をすべきソフトウェアやシステムが増加した。また、ソフトウェアを脆弱性修正版に更新するためにアップデートを行った場合、他の修正や機能変更により今までの機能が正しく動かず、更新によりシステムが停止することも発生している。同様にバグが含まれていることもあり、定期的な更新を行ったところシステムやホストが起動しなくなることもある。これらにより、「脆弱性が発見されたソフトウェアは、即座に最新の修正版ソフトウェに更新する」という戦略は、主にシステムの停止が事業の損害につながる企業においては実施しえないものとなった。

そのため、影響に対するリスクベースで適用や対応をすべき脆弱性を優先順位付けて対応する「脆弱性トリアージ」という対応方針へ変化してきている。それらを取り入れた脆弱性管理を Risk-Based Vulnerability Management（RBVM）と呼んでいる。従来は、脆弱性それ自体の危険度を示す CVSS Base Score だけで選別していたが、KEV Catalog により悪用が確認されている脆弱性を優先し、EPSS により今後の悪用可能性により優先順位をつけることが可能である。また、SSVC においては、公共への影響（Public Safety）なども考慮可能となっており、評判の影響（Reputation Risk）も考慮されている。これらの情報を活用して優先順位をつけることで、企業における脆弱性対応に対するリソース不足に対応し、必要な個所を優先して対応できるようになることが想定されている。

これらのフレームワークでは CVSS Base Score や EPSS などの情報を取り扱うが、各データ間は CVE-ID と CPE により結び付けられている。CVE-ID と CPE は脆弱性管理の根本部分で依存している情報であり、CVE-ID と紐づく CVSS Base Score も同様に基幹情報として扱われている。

本稿は、CVE-ID と CPE が適用された後の、脆弱性を細かく調査した後で付与される CVSS の情報、NVD で公開される情報について焦点を当てる。CVE-ID は CVE Foundation となったことで（形式的には）単一の国から独立し、中立性がある状態となっている。CPE に関しては NVD が管理しているが、完全に中央集権的ではない為、比較的中立と言えると考えられる。但し、公式な基準としては NVD の CPE Dictionary を参照することになる。比較的中立な CVE-ID や CPE に対し、NVD の情報は完全に特定の国家主体で生成されているため、単一障害点となりうると考えられる。

なお、脆弱性トリアージの手法については本稿から逸脱するため記載はとどめるが、ISOG-J[*18] WG1 が提供している「脆弱性トリアージガイドライン作成の手引き[*19]」が参考となる。

次項より NVD の代替や併用となりうる情報源について確認し、NVD の情報なしで脆弱性管理が可能かを検討する。

4. 主な地域別脆弱性情報源

4.1 日本：JPCERT/CC と Japan Vulnerability Notes(JVN)

JPCERT/CC[*20]は、日本および世界における脆弱性情報処理の主要なプレーヤーであり、MITRE によって認定された CVE 採番機関（CNA：CVE Numbering Authority）として機

15 https://www.first.org/epss/
16 https://www.cisa.gov/stakeholder-specific-vulnerability-categorization-ssvc
17 https://www.sei.cmu.edu/library/prioritizing-vulnerability-response-a-stakeholder-specific-vulnerability-categorization-version-20/
18 https://isog-j.org/
19 https://isog-j.org/output/2024/TriageGuidelines.html
20 https://www.jpcert.or.jp/

能している。CERT（Computer Emergency Response Team）ではあるが、「/CC」とあるように Coordination Center の役割である、国際的・組織間の調整機能を担っている。

JPCERT/CC と情報処理推進機構[*21]（IPA）は、Japan Vulnerability Notes（JVN）ポータルサイト[*22]（jvn.jp）と JVN iPedia[*23]（jvndb.jvn.jp）を共同で運営しており、これらは日本国内外の脆弱性対策情報のデータベースとなっている。国内で利用されている製品についての脆弱性情報のデータベースも担っており、グローバル展開されていないソフトウェについても、CVE-ID がない状態で掲示されることもある。その場合は「JVNDB-<年>-<6 桁の数字>」のデータベース登録番号と CPE で識別される。

JVN のデータは API[*24]でのアクセスができるようになっている。API のエンドポイントは複数あるが、個別の情報が取得できる getVulnDetailInfo[*25]（ver. HND）を確認する限り、対象の脆弱性は JVNDB 番号でしか検索できないようだ。CVE-ID や CPE による検索は不可能となっている。他のエンドポイントであれば CPE 検索は可能であるが、一度 JVNDB 番号を指定せずに全項目を取得し、自身でデータベースを構築したほうが再利用性は高い。
例えば JVNDB-2025-011400[*26]で登録されている「Adobe Experience Manager Forms における脆弱性」（CVE-2025-54253）の場合、JVNDB-2025-011400 をキーとして「https://jvndb.jvn.jp/myjvn?method=getVulnDetailInfo&feed=hnd&vulnId=JVNDB-2025-011400」のようなアクセスを行う。応答として CVSS Base Score・Vector 値・CPE・CWE・参考情報（URL）などの情報が記載されている。脆弱性管理で自動化に利用できるようなフォーマットとなっているが、例えば CPE についてバージョンの記載がないような状態となっており。情報の不足を感じられる。

JPCERT/CC が CNA としての役割を果たし、海外の CSIRT と積極的に連携していることは、JVN の信頼性が高く相互運用可能な情報源として位置づけられ、NVD の強力な代替となることを示唆している。JPCERT/CC は「日本および世界の脆弱性情報の要[*27]」「海外の CSIRT と連携している 27」と明記しており、これは JVN が単なるローカルデータベースではなく、グローバルな脆弱性エコシステムに積極的に統合されていることを意味する。これにより、データは国際標準（CVE）と整合性が保たれ、広範な連携努力の恩恵を受けていると考える。これは JVN データを既存の CVE に依存するツールに統合する際の障壁が少ないことを意味すると考える。

しかしながら、NVD の代替とするにはデータの粒度が荒く、また登録データ量も NVD には及ばない為、単独での代替はできない。しかしながら API でデータを取得することができる為、独立したでーばベースとして利用が可能である。他のデータベースの補助的に使用とし、また日本国内製品の脆弱性データベースとしては唯一として利用することが望ましいと考えられる。

4.2 シンガポール：Singapore Cyber Emergency Response Team(SingCERT)

SingCERT[*28]は、シンガポールサイバーセキュリティ庁（CSA）の下にあり、サイバーセキュリティインシデントの検出、解決、および防止を促進する国家 CERT である。CSA は、CVE 採番機関（CNA）としても機能している。

脆弱性やサイバー脅威の情報について、警告のリリースやアドバイザリ、セキュリティパッチの提供やインシデント対応チェックリスト、プレイブックなどを提供している。

ウェブサイトで「Alerts & Advisories[*29]」を提供しているが、その脆弱性データベースに対する直接的な API や専用の RSS フィードは提供されていない。

提供されるデータは、Background・Impact・Known Exploitation・Affected Products・Recommendations・References の項目が設定されている。全体として文字での説明がされている。Impact には CVE-ID が記載されているが、CVSS Base Score や Vector 値などの脆弱性管理で直接必要になる情報は書かれていない。Known Exploitation の項目もあるが、これは CISA の KEV Catalog への登録を示しているのか、シンガポール独自で判定したのか、前提条件が記載されていない。Affected Products の項目はあるが、CPE で記載されておらず、例えば”The vulnerabilities affect AEM Forms on JEE Versions 6.5.23.0 and earlier.[*30]”のような人間が判読する校正の文字列で書かれており、自動化は難しい記載となっている。

SingCERT は CNA であるにもかかわらず、その脆弱性データベースに容易に入手できないように見えることは、利用に際しては手動での作業やサードパーティの集約業者への依存が必要となる可能性が高い。

JVN 同様、シンガポールとしての脆弱性に対する反応を見ることはできるが、単独で脆弱性データベースとして利

21 https://www.ipa.go.jp/
22 https://jvn.jp/
23 https://jvndb.jvn.jp/
24 https://jvndb.jvn.jp/apis/index.html
25 https://jvndb.jvn.jp/apis/getVulnDetailInfo_api_hnd.html
26 https://jvndb.jvn.jp/ja/contents/2025/JVNDB-2025-011400.html
27 JPCERT/CC 事業概要
https://www.jpcert.or.jp/about/06_3.html
28 https://www.csa.gov.sg/resources/singcert
29 https://www.csa.gov.sg/alerts-and-advisories
30 https://www.csa.gov.sg/alerts-and-advisories/alerts/al-2025-078/

用することは難しく、あくまでアドバイザリのような情報源として利用する事が想定されていると考えられる。

4.3 オーストラリア：Australian Cyber Security Centre (ACSC)

ACSC[*31]は、オーストラリア政府の情報機関であるAustralian Signals Directorate[*32]（ASD）の一部で、オーストラリア政府のサイバーセキュリティに関する技術的権威として機能している。主要なオーストラリア企業に影響を与えるサイバーセキュリティ問題の単一連絡窓口として機能し、重要インフラストラクチャも対象とした活動をしている。組織構成から、ACSC はオーストラリアの諜報機関および法執行機関と密接に連携している。前述の JPCERT/CC・IPA や SingCERT とは異なり、CVE 採番機関（CAN）ではない。

ACSC は独自の脆弱性データベースを保有していない。活動として、Alerts and Advisories[*33]という仕組みでオーストラリア国内に影響を与える重大な脆弱性や脅威に関する情報を提供している。JNVDB のような検索可能な包括的データベースを提供するのではなく、細心の脆弱性や攻撃キャンペーンに関する速報性の高い情報提供に重点を置いている。

過去の Alerts は「All archived alerts and advisories[*34]」で確認ができるが、検索項目は Type・Status・Audience となっており、CVE-ID などでの検索を想定している物ではない。Alerts も例えば「Critical vulnerabilities in Citrix Gateway and Application Delivery Controller(ADC) devices」などを見る限り、Alert status（CVSS の Severity に該当）・Content complexity（コンテンツの複雑さ）・Background・Mitigation で表現されており、脆弱性管理に必要な情報ではなく、オーストラリア国内においての対応判断を示すものとなっている。CVE-ID は Background 項目に含まれているが、CPE や CVSS Vector 値などは記載されていない。

ACSC は脆弱性情報データベースという観点では、CVE 採番機関（CNA）ではなく独自の脆弱性情報を持ち得ていない為、速報性の高い情報提供やホワイトペーパーなどの提供を行う事に注力していると考えられる。NVD のようなデータベースを持つというよりは、その情報を早く伝え、ユーザが適切に扱えるような周辺情報を整理している役割と言える。

4.4 欧州連合：European union vulnerability database（EUVD）

EUVD[*35]は、欧州のサイバーセキュリティ戦略における中核機関である欧州サイバーセキュリティ庁[*36]（European Network and Information Security Agency：ENISA）が、特に NIS2 指令[*37]に基づき、域内のデジタルレジリエンスを強化数為に設立した、欧州脆弱性データベースである。ENISA 自体は CVE 採番機関（CNA）ではないが、複数の EU 加盟国の国家 CERT/CSIRT が CNA として機能しているため、CVE エコシステムと密接に連携している。

EUVD は、加盟国の CSIRT やベンダー、既存の脆弱性データベース（NVD や CISA KEV Catalog など）から脆弱性情報を集約する、中央集権的かつ信頼性の高いデータベースとして機能している。FAQ[*38]においても「情報源の高レベルの相互接続性を確保することを目的としている」胸が書かれている。EUVD の目的は、米国中心の脆弱性情報への依存を低減し、欧州独自のデジタル主権を確立することにある。このため、EUVD は独自に「EUVD ID」を脆弱性情報に割り当てているが、相互運用性を確保するために CVE-ID も併記されている。

例えば Adobe Experience Manager Forms における脆弱性（CVE-2025-54253）は EUVD-2025-23647 で登録[*39]されており、ENISA ID・CVE-ID・Vendor・Product・Version・CVSS Base Score（CVSS v3.1）・CVSS Vector 値、EPSS Score などが登録されている。当該項目には表示は無かったが、KEV Catalog に該当するかも記録されるようだ。残念ながら CPE によるバージョン記載はないが、CPE を作るための情報は記載されている。「相互接続性の確保」という目的があるため、脆弱性管理に必要な情報はほぼ集約されていると言ってよいと考えられる。

データへのアクセスも API[*40]が用意されており、取得時の選択自由度は高い。例えば単一の脆弱性情報を取得する場合、EUVD- ID さえ分かれば「 https://euvdservices.enisa.europa.eu/api/enisaid?id=EUVD-2025-23647」のような形で取得が可能である。CVE-ID での検索ができない事、CPE での検索ができないことを除けば、十分なデータベース公開と考えられる。

EUVD は、情報源の相互接続性の確保を強調したデータベースであり、データベース公開自体も脆弱性管理で利用可能なレベルで公開されている。また、FAQ によると JVN iPedia も含まれているとの事で、網羅性は NVD よりも広い

31 https://www.cyber.gov.au/
32 https://www.asd.gov.au/
33 https://www.cyber.gov.au/about-us/view-all-content/alerts-and-advisories
34 https://www.cyber.gov.au/about-us/view-all-content/alerts-and-advisories/archive
35 https://euvd.enisa.europa.eu/
36 https://www.enisa.europa.eu/
37 https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng
38 https://euvd.enisa.europa.eu/faq
39 https://euvd.enisa.europa.eu/vulnerability/EUVD-2025-23647
40 https://euvd.enisa.europa.eu/apidoc

可能性が高い。EUVD の母体である ENISA 自体は CVE 採番機関（CNA）ではないが、複数の EU 加盟国が CNA であることを考えると、脆弱性情報の信用性や質は高いと考えられる。

しかしながら CVE-ID や CPE での検索ができない、CVE-ID は NVD のデータに依存している、という点を考慮すると CVE エコシステムにおいては直ぐに置き換えが可能なものではない。CVE-ID から EUVD を検索するための中間作業が必要となる。これを考慮すると、既存の CVE エコシステムに直接組み込むことは難しく、あくまで CVE-ID で参照できるシステムへの補助データベースとなると考えられる。EUVD ID を中心とした、もしくは CVE-ID と同等に扱う脆弱性管理のエコシステムができれば、この点は解消されると考えられるが、現時点で CVE によるエコシステムは普及しているため、脆弱性管理での中心的データベースになることは難しいと考えられる。

4.5 Vulnrichment

Vulnrichment[*41]は、NVD における脆弱性エンリッチメントデータの停滞という近年の深刻な課題に対応するために生まれた、オープンソースのコミュニティ主導のプロジェクトである。NVD の運営主体である NIST が、政府の予算やリソース不足により CVD-ID に付随する CVSS 情報・CPE・CWE などのメタデータの提供を大幅に遅延させたことで、脆弱性管理エコシステム全体に大きな空白が生じた。この状況が続くと多くの脆弱性管理ツールやセキュリティ運用が機能不全に陥るため、その代替として Vulnrichment が注目を集めている。

Vulnrichment は NVD で不足している情報を補完するものとなっている。ボランティアの協力と自動化ツールを組み合わせ、CVE-ID に不足しているメタデータを付与する。提供されるデータは GitHub にて JSON 形式で公開されているため、自由に利用することができる状態となっている。CVE が登録/更新される度にデータが付与されるフロー[*42]となっているため、NVD に依存しない。これにより、NVD のデータが不完全な状況であっても、セキュリティ運用が中断なく継続できる設計といえる。また、GitHub で公開されているため、脆弱性管理ツールなどでも直接利用ができる。特定の組織により API が提供されているわけではないが、それにより、特定組織による影響を受けなくて済むと考えられ、利用上は問題ないと考えられる。

エンリッチメントされたデータは json の adp コンテナ（Authorized Data Publisher Container）以下に格納され、SSVC の選択肢（CISA Coordinator tree）・KEV Catalog のフラグ・CWE・NVD 以外が算出した SSVC Base Score と Vector・CPE などが含まれている。SSVC[*43]の Decision が登録されていることにより、ユーザ環境にかかわる「Mission&Well-being」以外は自動で SSVC の判定ができることになる。これは、中小企業などの脆弱性に対するインテリジェンスやインフォメーションが少ない企業にとっては重要であり、専門家やそれに類するコミュニティにより分析された情報が、脆弱性トリアージに直接使えることを意味している。

データとしては CVE-ID 毎に json ファイルが作成され、CVE-ID をキーに GitHub 上に配置されている。例えば CVE-2025-54153 の場合、”2025/54xxx/CVE-2025-54253.json”として配置される。CVE-ID から予測可能な配置であるため、API を使わず直接アクセスすることができる。SSVC データについては”PoC”・”yes”・”Total”のような記載で記録されているため、文字列として認識や処理が可能である。

Vulnrichment は、NVD の機能不全が顕在化したことで生まれた、コミュニティ主導の重要な試みである。NVD の代替として設計されたものではないが、NVD のエンリッチメントデータの保管という領域において、きわめて有効な役割を果たしている。GitHub にてオープンにデータが提供されているということは、自動化された脆弱性管理システムとの統合を容易にし、NVD への依存を軽減するうえで現実的な選択肢を提供する。

しかしながら、その持続可能性やデータの網羅性、信頼性はコミュニティの活動に依存するため、単独の情報源として全面的に信頼するのではなく、NVD や他の公的データベースと併用し、その信頼性を補完する形で利用することが望ましい。Vulnrichment は、特定の国の行政的な課題がグローバルなサイバーセキュリティ基盤に影響を与える状況に対する、コミュニティ主導のレジリエンスを示すよう事例と考えられる。

4.6 その他の注目すべき国家脆弱性データベース（概要）

4.6.1 中国 (CNNVD)

China National Vulnerability Database（CNNVD）[*44]は中国のサイバーセキュリティにおける主要な脆弱性情報データベースであり、中国国家情報技術安全評価センター[*45]（CNITSEC）によって運営されている。CNITSEC は、中国の対外情報機関である国家安全部（MSS）の傘下にあり、この組織的な関連性が CNNVD の運用とデータに大きな影響を与えていると、広く指摘されている。

CNNVD は、脆弱性情報に関して独自の CNNVD-ID を割

41 https://github.com/cisagov/vulnrichment
42 https://github.com/cisagov/vulnrichment/blob/develop/flowcharts.md
43 https://www.cisa.gov/stakeholder-specific-vulnerability-categorization-ssvc
44 https://www.cnnvd.org.cn/
45 https://www.itsec.gov.cn/

り当てている。しかし、その運営は NVD や JVN とは大きく異なり、データは単なる脆弱性情報ポータルとして機能するだけではなく、国家のサイバー安全保障及び情報活動を支援する目的で利用されていると考えられている。Recorded Future による分析[*46]では、高脅威の脆弱性が提供委の脆弱性よりも 21 日から 156 日遅れて公開された事例がある、同分析が公開された後に CNNVD のデータが不自然に書き換えられている（CNNVD が公開遅延していた脆弱性が、平均で 57 日さかのぼって公開日が変更されていた)、等の事象があり、意図的であると類推できる。これは国家の戦略的意図によって操作されるリスクがあることを示している。

CNNVD のデータは、サイトを確認する限りでは API や RSS によるアクセスは提供しておらず、WEB サイトでの情報提供のみと考えられる。記載されている情報は人間が読むような文章で書かれており、機械化は難しいと思われる。脆弱性の概要と CVE-ID、バージョンなどが提供されている。

CNNVD は、特定の中国製製品や中国の国家支援型脅威アクターが関心を持つ脆弱性に関する独自の早期情報を提供する場合があるため、補助的な情報源としては一定の価値を持つ。しかし、その運営主体が国家の情報機関と密接に関連しているという背景から、情報の操作や意図的な公開の遅延という、運用上許容しがたいリスクが存在する。

したがって、CNNVD は NVD の代替とはなりえない。一般的な脆弱性の意思決定に直接使用するべきではなく、脅威インテリジェンスアナリストによる手動分析と、他の信頼できる情報源との相互参照を通じてのみ利用されることが望ましい。CNNVD は、特定の国家の行政課題ではなく、その戦略的意図がグローバルなサイバーセキュリティの基盤に影響を与える事例であり、その情報には極めて慎重な取り扱いが求められる。

4.6.2 ロシア (FSTEC/BDU)

ロシアの脆弱性データベースである、FSTEC（Federal Service for Technical and Export Control：ロシア連邦技術輸出管理庁）の BDU[*47]（Data Security Threats Database：略語はロシア語頭文字をアルファベットに変換（音訳）したもの）は、運営主体がロシア連邦国防省傘下の軍事機関であるという、きわめて特殊な性質を持っている。この組織的な背景が、BDU が提供する脆弱性情報の品質や完全性、そして目的に決定的な影響を与えていると広く指摘されている。

FSTEC BDU は、独自の「BDU ID」を脆弱性に割り当てている。しかし、そのデータは NVD や他のグローバルデータベースと比べ、網羅性と公開のタイムリーさにおいて著しく劣る。FSTEC BDU は、NVD で見つかった脆弱性のわずか約 10%しかカバーしておらず、その公開速度も CNNVD よりも遅い。これは Recorded future 社の分析[*48]にも書かれており、NVD に対する遅延は平均 50 日、CCNVD に対する遅延も平均で 83 日遅く、全体的に脆弱性が公に開示されてから BDU に掲載されるまでの平均日数は 95 日となる。この遅延と不完全性は、BDU が公共の利益のためではなく、主にロシアの国家安全保障と、ロシアの国家情報システムへの脅威を分析するという極めて狭い目的に焦点を当てていることを示唆している。

FSTEC BDU のサイトの証明書は、CN：”Russian Trusted Root CA”、O：”The Ministry of Digital Development and Communications”で署名されており、一般的な日本国内の PC では信頼できるルート CA として登録されていない。またサイトの応答は、少なくとも日本国内からは遅く、ページを開くのに 10 秒程度応答しない。尚、CNNVD は GlobalSign で署名されており、問題なくアクセスが可能である。

脆弱性情報を見ると、例えば LibTIFF ライブラリの脆弱性（BDU：2025-09847）では、CWE や CVSS の Vector 値、CVE-ID などが公開されているが、NVD よりも詳細性はない。

このサイトの特徴的な点として、ScanOVAL[*49]という脆弱性検出ツールを提供していることがあげられる。OVAL 情報をもとに脆弱性をスキャンするスキャナのようだが、Windows 7-10、Windows Server 2008-2016 が対象となっていた。Linux 用[*50]も存在しており、Astra Linux や Alt9（ALT Linux version 9 と想定)、Rosa Cobalt（ROSA Linux のセキュリティ認証付きエディション）が対象となっていた。これらの OS は、軍や政府で利用しているものである。このような脆弱性検出ツールと脆弱性情報（OVAL）の提供は西側諸国の CERT では少なく、見習う点はあると感じる。また、トレーニングビデオも同サイト内で公開していた。ファジングや静的分析などが用意されている。このような

FSTEC BDU は、その運営主体が軍事機関であり、その目的が国家安全保障と情報統制に置かれていることから、信頼性と運用上のリスクが極めて高い情報源であるといえる。このデータは脆弱性情報の主要な基盤として利用することは望ましくなく、NVD や他の信頼できるデータベースの代替とはなりえない。

46 https://www.recordedfuture.com/blog/chinese-vulnerability-data-altered
47 https://bdu.fstec.ru/vul
48 https://www.recordedfuture.com/research/russian-vulnerability-analysis
49 https://bdu.fstec.ru/scanoval
50 https://bdu.fstec.ru/scanovalforlinux

しかしながら、その特殊な性質ゆえに、ロシアの国家アクターが関心を持つ脆弱性や、ロシア国内で利用される特定の技術に関するニッチな脅威インテリジェンスを提供する可能性がある。したがって、BDU から得られる情報は、脆弱性管理の意思決定に直接使用するのではなく、脅威インテリジェンスアナリストによる手動解析や、他の情報源との相互参照を通じてのみ、限定的な補助情報として利用されるべきと考える。

4.6.3 CNNVD と FSTEC/BDU の総括

中国やロシアのような国々における脆弱性情報に対する国家統制は、これらの地域で運用されている、またはこれらの地域の技術を扱う組織にとって、慎重で多角的な情報収集アプローチを必要とする。MSS が CNNVD に影響を与え潜在的に悪用している、FSTEC がロシアの BDU を管理する軍事機関でありデータベースが非常に不完全で遅いことが、先の Recorded Future 社の報告などで示されている。公開される情報が国家安全保障の観点でフィルタリングされており、攻撃的に使用される可能性のある重要なデータが意図的に隠されている可能性があると想定する必要があると考えられる。

5. 結論

本研究は、NVD の更新遅延とトランプ政権による一連の資金削減により顕在化した「一国依存の脆弱性情報基盤リスク」を起点とし、主要な非米国ソースの実態を比較分析した。その結果、以下を結論とする。

1 つ目として、NVD などの完全な代替は、現時点では困難である。JVN や EUVD などの地域的取り組み、Vulnrichment のようなコミュニティ主導の試みは有効ではあるが、データ量・粒度・信頼性の面で NVD に匹敵するものは現時点では存在しない。

2 つ目として、多層的・分散的な補完戦略が必要である。各国ソースを補完的に活用することで、米国依存によるリスクを低減できる。特に Vulnrichment によるエンリッチメントや EUVD の統合性、JVN の国内的要請は有効である。

3 つ目として、国際協調による新たなガバナンスモデルが必要と考えられる。将来的には国連や FIRST などの枠組みを活用した多国間の脆弱性情報基盤を確立すべきである。これは単なる冗長化ではなく、地政学的リスクを分散し、サイバーセキュリティの公共財としての性格を担保するために不可欠と考える。

4 つ目、最後に、日本の役割を明確化し、国際協調を主導する立場を担うべきである。JVN はすでに EUVD などの他国の参照先として利用されており、日本にはリーダーシップを発揮する下地はある。自国ソフトウェアにとどまらず、国際的な情報共有のハブとして機能を強化することで、日本国の国際的地位向上にもつながる。これは日本として情報源を持つというよりも、例えば国連や FIRST に対して 3 小梅で述べたような多国間脆弱性情報基盤を確立するよう主導的働きを行うことなどを想定している。

以上より、短期的には多様な情報源の活用によるレジリエンス強化を目指し、中期的には国際的連携の強化を行い、長期的には多国間のガバナンス確立を進めることが、持続可能な脆弱性管理エコシステムの実現につながると結論付ける。