関係各部署 御中

To departments concerned

Confidentiality classification	PROTECTED 関係者外秘	原紙保管 Storage of original	M/Y /
		コピー保管 Storage of copy	M/Y /

(別紙 1)

既製品の脆弱性分析ガイド

(Annex 1)
Guide for Off-the-shelf Vulnerability Analysis

制御電子プラットフォーム開発部
制御ネットワーク・アーキ開発室 4G
E/E Architecture Development Div
System network & architecture development dept 4G

No. SEC-ePF-VUL-ECU-REQ-SPEC-a00-07-b

承認 Approved	調査 Checked	作成 Created	/ /

目次

1. はじめに

1.1. 本書の目的

本脆弱性分析ガイドは、分析対象となるシステムおよび機器に対して悪用可能である明白な脆弱性の存在についての分析を実施する為のガイドである。本書に従い、分析対象となるシステム、及び、機器に対して脆弱性分析を実施する。

なお、脆弱性分析は、Common Criteria の「情報技術セキュリティ評価のための共通方法:通称 CEM」の付属書 B に記載されている脆弱性分析手法を参考にしている。

1.2. 引用規格

■ IPA 翻訳版

- 情報技術セキュリティ評価のためのコモンクライテリア（CC）
  - パート 1:概説と一般モデル バージョン 3.1 改訂第 4 版［翻訳第 1.0 版］
  - パート 2:セキュリティ機能コンポーネント バージョン 3.1 改訂第 4 版［翻訳第 1.0 版］
  - パート 3:セキュリティ保証コンポーネント バージョン 3.1 改訂第 4 版［翻訳第 1.0 版］
- 情報技術セキュリティ評価のための共通方法
  - 評価方法 バージョン 3.1 改訂第 4 版［翻訳第 1.0 版］（CEM）

■ 原文

- Common Criteria for Information Technology Security Evaluation
  - Part1: Introduction and general model Version 3.1 Revision 4 September 2012 CCMB-2012-09-001
  - Part2: Security functional components Version 3.1 Revision 4 September 2012 CCMB-2012-09-002
  - Part3: Security assurance components Version 3.1 Revision 4 September 2012 CCMB-2012-09-003
- Common Methodology for Information Technology Security Evaluation
  - Evaluation methodology Version 3.1 Revision 4 September 2012 CCMB-2012-09-004

2. 既知の脆弱性分析

2.1. 探索対象となる公開脆弱性 DB

公開脆弱性 DB として、情報セキュリティの脆弱性評価の探索対象とされるのは、表 2.1 に示す 3 種類がある。

これらの公開脆弱性 DB、はすべてソフトウェアに関するものであるが、一方、ファームウェアに関するものや、ソフトウェアの脆弱性に関連するハードウェア情報が含まれている場合など、ソフトウェア/ファームウェアとの関連性が強いハードウェアの脆弱性情報が含まれている場合もあるので、ハードウェアの場合でも、これらの公開脆弱性 DB の探索が参考になる場合がある。

表 2.1 公開脆弱性 DB

公開脆弱性探索範囲	対象：システム/ソフトウェア	対象：ハードウェア （IC チップ組込み製品など）
公開脆弱性 DB	S1) JVN iPedia: http://jvndb.jvn.jp/ ［日本語；英語もあり］ S2) CVE: http://cve.mitre.org/cve/ ［英語］ S3) US-CERT DB: http://www.kb.cert.org/vuls/ ［英語］	左記 DB に、含まれている場合もある （ソフトウェア/ファームウェアとの関連性が強いハードウェアの脆弱性情報）

2.2. 公開脆弱性 DB の探索手順・探索方法

公開脆弱性 DB の探索は、一般に以下の手順で実施することが想定されている。

Step1）探索に用いるキーワードの選出
Step2）選出したキーワードを用いて対象の公開脆弱性 DB を探索
Step3）探索結果を適切に絞り込みながら、評価対象の潜在的脆弱性に繋がる可能性のある脆弱性を分析対象候補として選別
Step4）評価対象となるシステム仕様に、選別された分析対象候補の潜在的脆弱性と同様の脆弱性が含まれていないかどうかを確認

このうち、Step4 に関しては、評価対象となるシステム仕様の確認のみのため、以降 Step1~3 の詳細に関して説明する。

2.2.1. Step1） 探索に用いるキーワードの選出

Step1 の探索用キーワードは、以下のような観点で、選出することが望ましいとされている。ただし、すべての種類のキーワード選出が要求されている訳ではなく、適宜、選択・選出を行う。

表 2.2 探索用キーワード選出の例

キーワード群	内容
1	評価対象の製品種別、同一タイプ製品・類似タイプ製品に関するキーワード
2	評価対象のセキュリティ機能に関するキーワード
3	評価対象が使用している製品・技術（ソフトウェア）に関するキーワード
4	評価対象が使用しているハードウェア・ハードウェアインタフェースに関するキーワード
5	その他、評価者が独自に設定したキーワード

なお、キーワードの選出にあたっては、探索対象の公開脆弱性 DB が、日本語版か英語版かも考慮して、日本語・英語の適切なキーワードの設定・併用が必要となることがあることを留意して選出し、キーワードにそれらの区別を含めておくことを推奨する。

また、探索対象の公開脆弱性 DB の検索機能は各々異なっており、あまり一般的な言葉や複合語を用いると適切な結果が得られない場合が多いため、検索しようとする製品・技術をできる限り短く表現できる固有の単語をキーワードとして選出することがポイントになる。

2.2.2. Step2 ～Step3） 公開脆弱性 DB の探索と候補の絞り込み

選出したキーワードを用いた公開脆弱性 DB の探索と候補の絞り込みについては、以下、表 2.1 に示した 3 つの公開脆弱性 DB それぞれに、その特徴と留意点を記述する。

S1) JVN iPedia（脆弱性対策情報データベース JVN iPedia）：http://jvndb.jvn.jp/

実際の検索は、JVN iPedia の先頭ページから「詳細検索」を選んだ下図（図 2.1）の画面を使って実施する。

図 2.1 JVN iPedia の詳細検索画面

この詳細検索画面から分かるように JVN iPedia では、いろいろな検索オプションが用意されており、選出したキーワードと検索目的に合わせた検索オプションを設定して検索する（詳細は、上記画面の「検索の使い方」を参照）。

JVN iPedia に登録されている脆弱性情報は、すべて「**JVNDB-YYYY-XXXXXX**」の形式の一意的な脆弱性識別子が割り振られており、脆弱性探索では、この JVNDB 識別子と、その識別子の下で記述されている「**概要**」、「**影響を受けるシステム**」、「**想定される影響**」、「**対策**」、「**ベンダ情報**」、「**参考情報**」を確認しながら、評価対象の潜在的脆弱性に繋がる可能性のある脆弱性かどうか、判断する。

1 件 1 件の分析判断も可能であるが、検索結果が多い場合など、通常は適切に絞り込んだ検索結果を手元 PC に取り込んだ後、じっくりと評価対象の潜在的脆弱性に繋がる可能性のある脆弱性かどうか、分析判断するのが一般的である。

なお、JVN iPedia では、その情報を Web を通じて利用するための API（MyJVN API）が用意され、その検索をプログラム化することも可能になっているので、検索作業を自動化/半自動化することも可能である（詳細は、URL： http://jvndb.jvn.jp/apis/ 参照）。

S2) CVE（Common Vulnerabilities and Exposures）：http://cve.mitre.org/cve/

CVE の公開脆弱性 DB の探索は、下図（図 2.2）の先頭ページから、「Search keywords or look-up CVE-IDS」のメニューを選択し、その検索画面（図 2.3）から行うのが通常である。

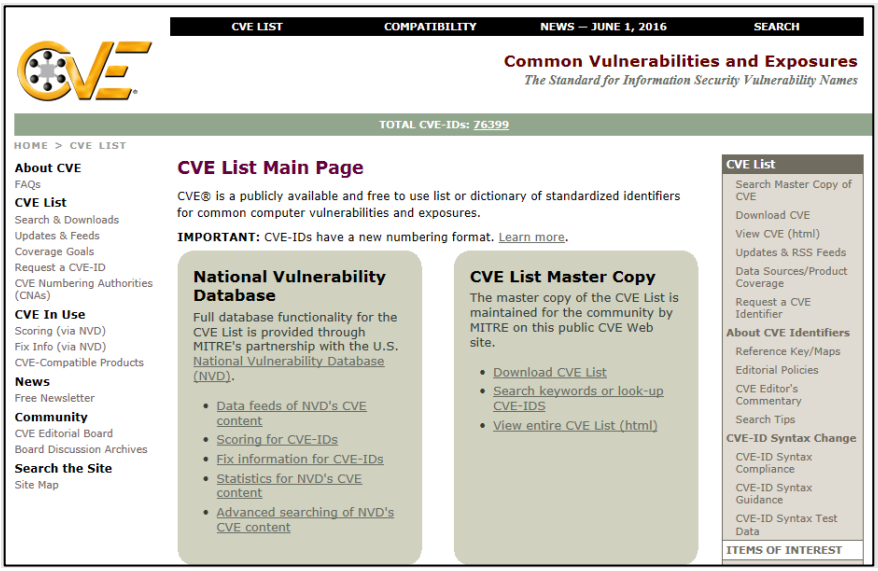

図 2.2　CVE の先頭ページ

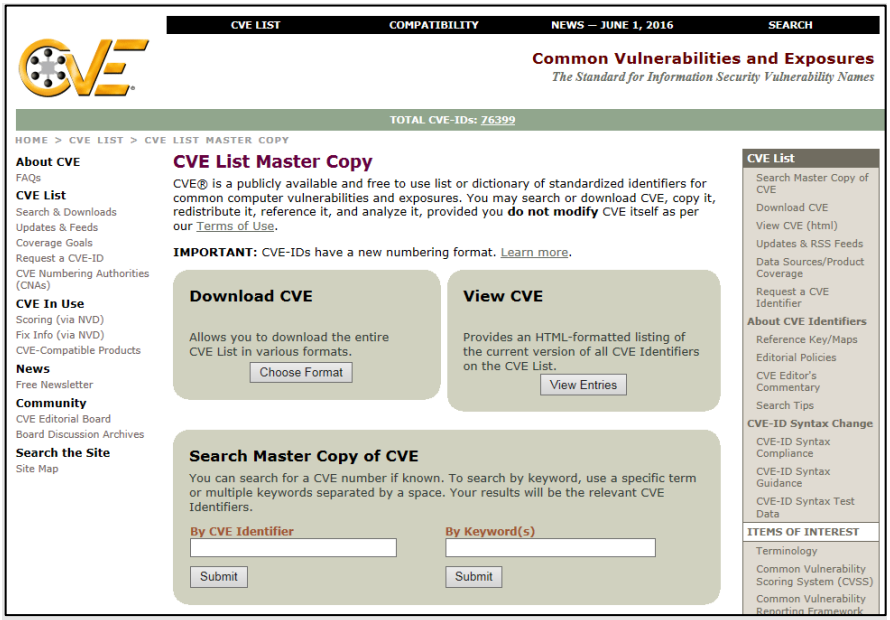

図 2.3　CVE の検索画面

また、CVE の先頭ページ（図 2.2）左に、「U.S. National Vulnerability Database (NVD).」に対する検索メニュー「Advanced searching of NVD's CVE content」が配置されているが、この NVD の取扱い等については、後述する。

検索画面（図 2.3）から分かるように、CVE では、特別な検索オプションは用意されておらず、検索画面中の説明文にあるとおり、以下の規則の下で検索が実施される。

- 複数のキーワードがある場合は、キーワードをスペースで分割する

  （スペースで区切られた複合語とは解釈されない）

従って、あまり複雑なキーワードや条件検索には不向きである。CVE の検索方法に関する補足説明は、URL： https://cve.mitre.org/find/search_tips.html を参照されたい。

一方、CVE の先頭ページ（図 2.2）左に登場する「National Vulnerability Database (NVD).」とその検索メニュー「Advanced searching of NVD's CVE content」は、以前米国政府機関（NIST）が独自に運用管理していた「ICAT（Internet Catalog of Attacks Toolkit.）脆弱性 DB」の後継として、その主要な機能を引き継ぎながら、CVE ベースの公開脆弱性 DB として機能強化を計った米国政府機関直轄（NIST 管理）の公開脆弱性 DB である。

従って、この NVD の検索は、以下のような場合に使用することが想定されている。

- CVE の検索方法では、うまく表現・実現できない「CVE の高度な検索」が必要な場合
- CVE としては提供されていない「個々の脆弱性に関する詳細情報（含：外部重要情報提供先へのリンク）」が必要な場合

なお、上記後者のケースでは、個々の CVE 脆弱性情報の先頭に、当該脆弱性に対する NVD へのリンク情報が提供されるので、何時でも CVE 脆弱性 DB 検索の中から、NVD 付加情報が参照できるようになっている。

また、高度な検索を外部の脆弱性 DB の機能に頼らず、自らの環境で自由に検索できるように CVE 脆弱性 DB をダウンロードできる機能も提供されている（図 2.3 の画面参照）。この機能を使って自らの PC 環境にダウンロードした DB ファイルを検索することも可能である。

いずれの場合（CVE、NVD）でも脆弱性 DB に登録されている脆弱性情報は、すべて「**CVE-YYYY-XXXX**」の形式の一意的な脆弱性識別子が割り振られており、脆弱性探索では、この CVE 識別子と、その識別子の下で、記述されている「**Description**」、「**References**」情報、場合によっては NVD 情報（「**Overview**」、「**Impact**」、「**References to Advisories, Solutions, and Tools**」など）を確認しながら、評価対象の潜在的脆弱性に繋がる可能性のある脆弱性かどうか、判断する。

S3) US-CERT DB（Vulnerability Notes Database）：http://www.kb.cert.org/vuls/

実際の検索は、US-CERT DB (Vulnerability Notes Database) の先頭ページから「Advanced Search」」を選んだ下図（図 2.4）の画面を使って実施する。

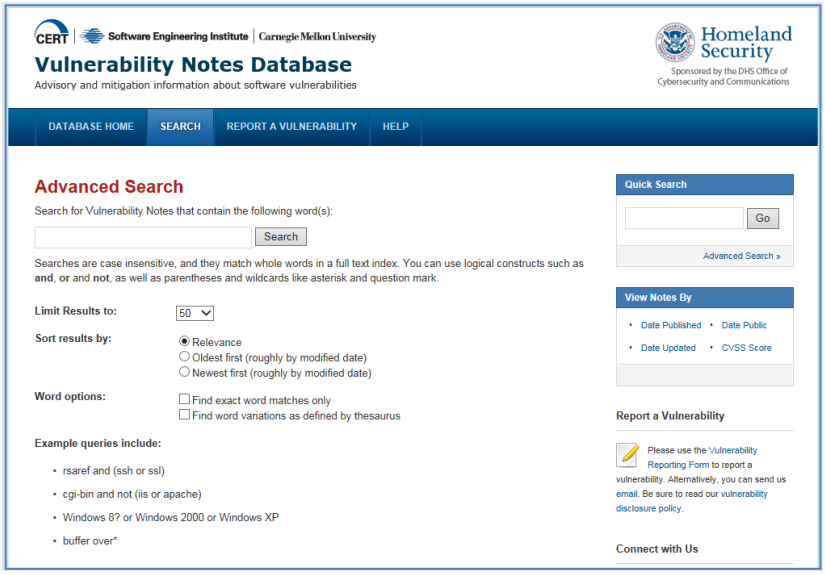

図 2.4 US-CERT DB の検索画面

この詳細検索画面から分かるように US-CERT DB では、いくつかの検索オプションが用意されており、選出したキーワードと検索目的に合わせた検索オプションを設定して検索する。

検索規則に関する基本的な情報は、この画面内のテキスト説明にあるように、以下のような規則が適用され、いろいろな条件検索、ワイルドカード検索も可能になっている。

- 予約語 「**and** 」、「**or**」、 「**not**」、予約記号「**()**」を使った条件指定
- 予約記号「**?**」、「*****」を使ったワイルドカード条件指定
- 大文字・小文字の区別なし

これらの検索オプション、検索方法に関する詳細説明は http://www.kb.cert.org/vuls/html/searchhelp に記載されている。

US-CERT DB に登録されている脆弱性情報は、全て「**VU#XXXXXX**」の形式の一意的な脆弱性識別子が割り振られており、脆弱性探索では、この US-CERT DB 識別子と、その識別子の下で、記述されている「**Overview**」、「**Description**」、「**Impact**」、「**Vendor Information**」、「**References**」を確認しながら、評価対象の潜在的脆弱性に繋がる可能性のある脆弱性かどうか、判断する。

なお、US-CERT DB では、CVE 同様にその脆弱性 DB をダウンロードできる機能も提供されているので（URL： http://www.cert.org/download/vul_data_archive/ 参照)、この機能を使って自らの PC 環境で検索することも可能である。

2.2.3. 公開脆弱性 DB 探索の効率化方法

Step2~3) 公開脆弱性 DB の探索における効率化の方法について説明する。

① 各 DB 間での重複部分を見つける方法

既知の脆弱性探索に使用する公開脆弱性 DB として、2.1 章にて 3 つの DB を示した。これらの DB には、各々独自の脆弱性情報も含まれているが、大半がいずれの DB にも含まれる重複した脆弱性情報である。

例えば JVN iPedia の場合、脆弱性情報に「参考情報」として、CVE 識別子が記載されているものがあるが、これは CVE でも同様の脆弱性情報が記載されていることを意味している。(図 2.5)。

ここで、JVN iPedia による脆弱性探索が完了し、その後 CVE を用いて同様のキーワードによる探索を行う場合を考える。CVE を用いた探索により、JVN iPedia を用いた探索と同じ CVE 識別子の脆弱性情報が見つかった場合は、JVN iPedia で探索した際に十分に脆弱性分析が完了していれば、改めて脆弱性分析を行う必要はなく、2.3 章に記載の分析まとめに他の DB と重複していることを記載すればよい。

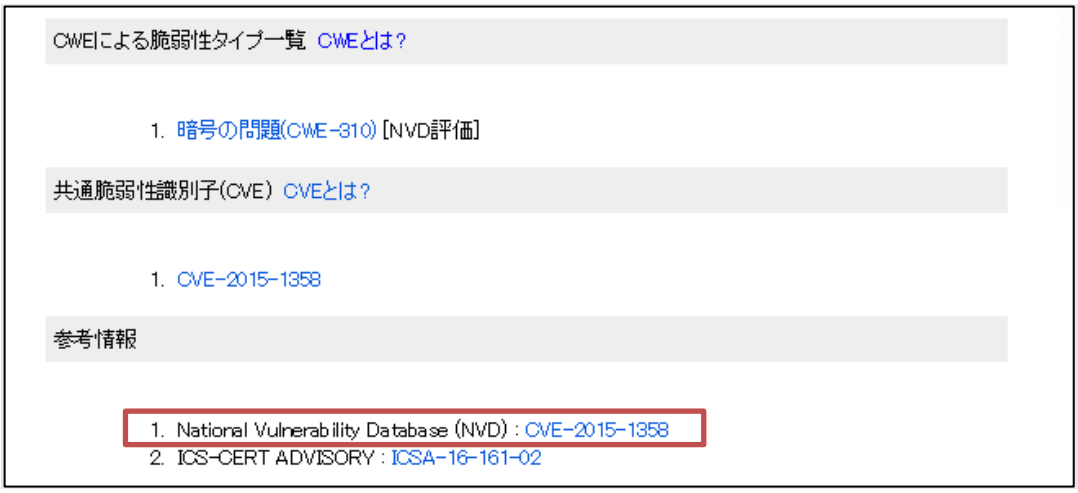

図 2.5 JVN iPedia の脆弱性情報

② 過去の探索との差分のみを探索する方法

公開脆弱性 DB の情報は日々更新されるため、定期的に DB の確認を行う必要がある。過去に同じキーワードで脆弱性探索を行っていた場合、過去の探索日と共に脆弱性情報をまとめておくことで、過去の探索日以前の脆弱性情報を改めて DB で探索する必要はない。

例えば JVN iPedia の場合、図 2.1 のように「公表日」と「最終更新日」を指定することが可能である。この機能を使用することで、過去に探索済みの情報を除く、差分のみの脆弱性探索が可能となる。

2.3. 既知の脆弱性分析結果のまとめ方

既知の脆弱性分析結果としては、公開脆弱性 DB を活用して脆弱性を確認し、関連する脆弱性に対しての対策結果をまとめる。分析結果まとめに含むべき内容を表 2.3 に示す。

表 2.3 既知の脆弱性分析まとめに含むべき内容

記載項目		記載内容
①	公開脆弱性 DB	探索に使用した公開脆弱性 DB を記載
②	ID	各 DB の脆弱性識別子を記載
③	他 DB との関連	他の DB に同様の脆弱性情報が記載されている場合に、その識別子を記載 (JVN iPedia の「参考情報」等)
④	重複	他の DB に重複する脆弱性情報が記載されており、脆弱性分析まで行っている場合、その番号を記載 (ここに番号が記載された場合、以降の記入は不要である)
⑤	タイトル	公開脆弱性 DB に記載されているタイトルを記載
⑥	深刻度(CVSSv2)※	CVSSv2 による深刻度を記載
⑦	深刻度(CVSSv3)※	CVSSv3 による深刻度を記載
⑧	公表日	脆弱性情報が公表された日を記載
⑨	最終更新日	脆弱性情報が最後に更新された日を記載
⑩	該当する機能の有無	評価対象に、探索した脆弱性情報が該当する機能を有しているかどうかを記載
⑪	該当しないと判断した理由	⑩で該当しないと判断した場合に理由を記載
⑫	対策実施の有無	⑩で該当すると判断した場合に、対策を実施するかどうかを記載
⑬	対策を実施していない理由	⑫で対策を実施しないと判断した場合に理由を記載
⑭	どのような対策を実施したか	⑫で対策を実施すると判断した場合、どのような対策を実施したかを記載
⑮	対策を実施していることの検証方法	⑭で実施した対策に関して、どのように検証するのかを記載

※JVN iPedia では、2015 年 12 月 1 日より、CVSSv2 と CVSSv3 を併記して記載している。それ以前のものは CVSSv2 の値のみが記載されている。どちらか一方の情報しかない場合は、そちらの情報のみ記載すればよい。

Table of Contents

1. Introduction

1.1. Purpose of this Document

This Vulnerability Analysis Guide is a guide for performing analysis on existence of obvious exploitable vulnerabilities for a system and device to be analyzed. In accordance with this document, vulnerability analysis is performed on a system and device to be analyzed.

Note that the vulnerability analysis uses the vulnerability analysis methodology described in Appendix B of Common Criteria “Common Methodology for Information Technology Security Evaluation (commonly known as CEM)” as a reference.

1.2. Normative references

- IPA translated version
  - 情報技術セキュリティ評価のためのコモンクライテリア（CC）
    - パート 1:概説と一般モデル バージョン 3.1 改訂第 4 版［翻訳第 1.0 版］
    - パート 2:セキュリティ機能コンポーネント バージョン 3.1 改訂第 4 版［翻訳第 1.0 版］
    - パート 3:セキュリティ保証コンポーネント バージョン 3.1 改訂第 4 版［翻訳第 1.0 版］
  - 情報技術セキュリティ評価のための共通方法
    - 評価方法 バージョン 3.1 改訂第 4 版［翻訳第 1.0 版］（CEM）
- Original texts
  - Common Criteria for Information Technology Security Evaluation
    - Part1: Introduction and general model Version 3.1 Revision 4
      September 2012 CCMB-2012-09-001
    - Part2: Security functional components Version 3.1 Revision 4
      September 2012 CCMB-2012-09-002
    - Part3: Security assurance components Version 3.1 Revision 4
      September 2012 CCMB-2012-09-003
  - Common Methodology for Information Technology Security Evaluation
    - Evaluation methodology Version 3.1 Revision 4
      September 2012 CCMB-2012-09-004

2. Analysis of Known Vulnerabilities

2.1. Public Vulnerability Database to be Searched

There are three types of public vulnerability databases to be searched for vulnerabilities in information security as shown in Table 2.1.

All these public vulnerability databases are related to software. But these may contain vulnerability information on hardware highly relevant to software or firmware such as vulnerability information related to firmware, information on hardware related to vulnerability on software and so on. Therefore, the search of these public vulnerability databases may be referenced even for hardware.

Table 2.1 Public vulnerability databases

Scope of search for public vulnerability	Target: System/Software	Target: Hardware (A product with built-in IC chip, etc.))
Public vulnerability databases	S1) JVN iPedia: http://jvndb.jvn.jp/ [Japanese; English ver. is also available.] S2) CVE: http://cve.mitre.org/cve/ [English] S3) US-CERT DB: http://www.kb.cert.org/vuls/ [English]http://www.kb.cert.org/vuls/	The databases listed on the left sometimes contain the information. (Vulnerability information on hardware highly relevant to software/firmware)

2.2. Public Vulnerability Database Search Procedures and Search Methods

In general, it is assumed that public vulnerability database search is performed in accordance with the following procedures.

Step1) Selection of keywords for the search
Step2) Search of the target public vulnerability database using selected keywords
Step3) Sorting out vulnerabilities which could lead to a potential vulnerability of the evaluation target system/device as analysis target candidates while narrowing down the search result appropriately
Step4) Confirm whether the system specifications to be evaluated doesn't include vulnerabilities similar to the potential vulnerabilities which is selected as analysis target candidates

Of these above steps, Step 4 is simply to confirm the system specifications to be evaluated. Therefore, details of Step 1 to 3 are explained hereafter.

2.2.1. Step1) Selection of Keywords for the Search

It is considered that keywords for search in step1 should be selected from the following perspectives. However, it is not required to select all types of keywords. The keywords are selected and sorted out appropriately.

Table 2.2 Example of Selection of Keywords for Search

Keyword group	Content
1	Keywords related to product types and same or similar kind of products with evaluation target
2	Keywords related to security function on the evaluation target
3	Keywords related to products and technologies (software) used by the evaluation target
4	Keyword related to the hardware and the hardware interface used by the evaluation target
5	Other keywords independently selected by the evaluator

When selecting keywords, consider whether the public vulnerability database to be searched is the Japanese or English version. Note that it is necessary to set appropriate keywords for the database, and that the use of both may be necessary. It is recommended to include those distinctions in the keywords.
In addition, search functions in public vulnerability databases to be searched are different, and use of an excessively general word and compound term often leads to failure to get appropriate results. Therefore, a key

point is to select, as a keyword, a unique word that can express the product/technology to be searched for as shortly as possible.

2.2.2. Step2 ～Step3) Search of the Public Vulnerability Database and Narrowing Down of the Candidates

Regarding the search of the public vulnerability database using the selected keyword and narrowing down of the candidates, the characteristics and the notes of the three public vulnerability databases indicated in Table 2.1 are described as follows.

S1) JVN iPedia (vulnerability countermeasure information database JVN iPedia): http://jvndb.jvn.jp/

Practically, search can be performed by using the screen shown in the figure below (Fig. 2.1) which appears by selecting “Advanced Search” from the top page of JVN iPedia.

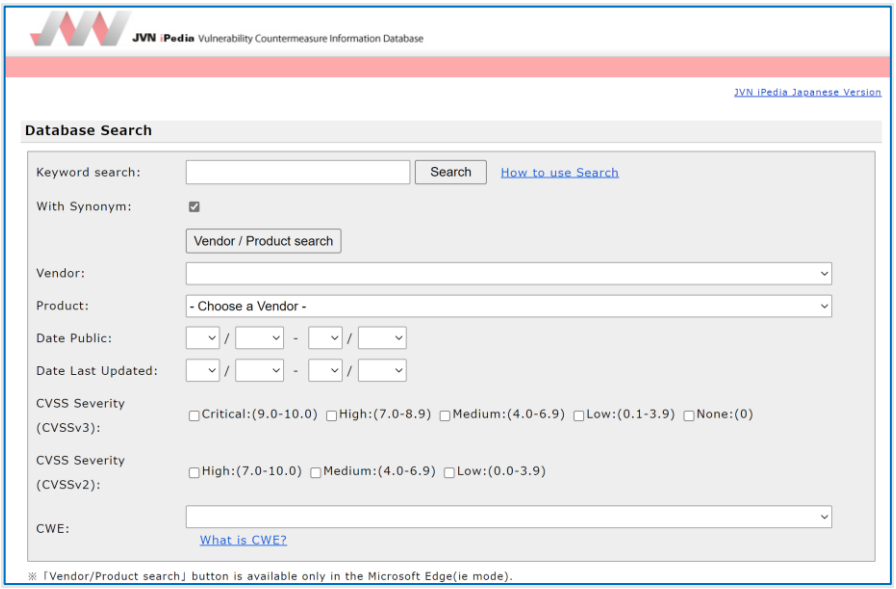

Fig. 2.1 Advanced Search Screen of JVN iPedia

As can been seen on this Advanced Search screen, JVN iPedia provides various search options. Search is performed by setting a search option that matches the selected keyword and the search objective. (For details, see “How to use Search” on the above screen.)

All vulnerability information registered in JVN iPedia is assigned with a unique vulnerability identifier in the “**JVNDB-YYYY-XXXXXX**” format. In vulnerability search, the evaluator judges whether the given vulnerabilities could lead to potential vulnerabilities of the evaluation target system/device by verifying this JVNDB identifier and “**Overview**”, “**Affected Products**”, “**Impact**”, “**Solution**”, “**Vendor Information**”, and “**References**” described for that identifier.

Although it is possible to make analysis and judgment for each case, evaluators generally import the appropriately

narrowed down search result to the local computer and then carefully make analysis and judgment on whether given vulnerabilities could lead to potential vulnerabilities of the evaluation target system/device in the case where there are many candidates in the search result.
Also note that, JVN iPedia provides API (MyJVN API) for using the information via Internet and the program can be created with it to perform the search. Therefore, it is possible to automate or semi-automate the search operation. (For details, see URL: http://jvndb.jvn.jp/apis/.)

S2) CVE (Common Vulnerabilities and Exposures): http://cve.mitre.org/cve/

In normal cases, search of CVE public vulnerability database is performed by selecting “Search keywords or look-up CVE-IDS” from the top page in the figure below (Fig. 2.2) and starting search on the search screen (Fig. 2.3).

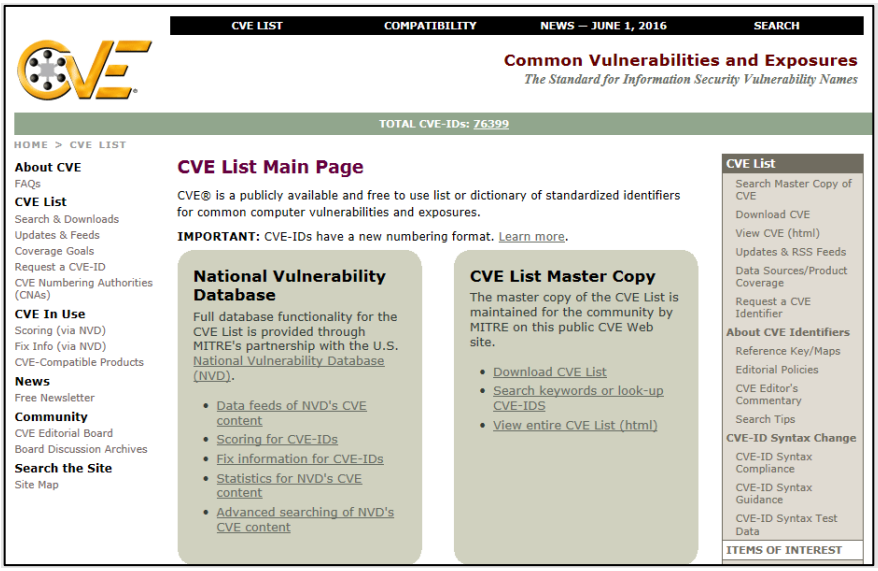

Fig. 2.2 Top Page of CVE

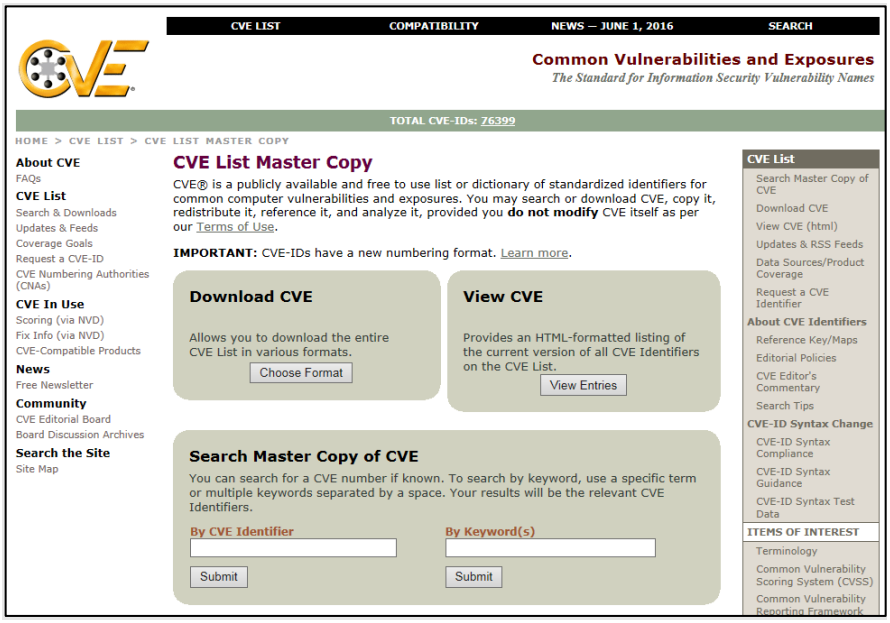

Fig. 2.3 Search Screen of CVE

The search menu “Advanced searching of NVD’s CVE content” for “U.S. National Vulnerability Database (NVD)” is laid out on the left side of the top page of CVE (Fig. 2.2). The handling of NVD is described later.
As can be seen on the search screen (Fig. 2.3), CVE does not provide a special search option. Search is performed according to the following rule as explained in the text on the search screen.

- Separate keywords by a space if there are multiple keywords

  (not interpreted as a compound word delimited by a space)

Therefore, CVE is not suitable for complex keywords or conditional. For additional instructions on how to find CVE, see URL: https://cve.mitre.org/find/search_tips.html.
On the other hand, “National Vulnerability Database (NVD)” that appears on the left side of the top page of CVE (Fig. 2.2) along with its search menu “Advanced searching of NVD’s CVE content” is a successor public vulnerability database to “Internet Catalog of Attacks Toolkit (ICAT) vulnerability Database” which is directly operated and managed independently by the US government (NIST). NVD is a CVE-based public database managed by the US government (NIST) and it has strengthened functions compared to CVE while taking over the major functions of ICAT vulnerability database.
Therefore, it is assumed that the search of this NVD is used in the following cases.

- In the case that an “advanced searching of CVE” is required, which cannot be expressed or realized well by the CVE search method is required
- In the case that “detailed information on individual vulnerability (including a link to external source of important information)” which is not provided by CVE is required

For the latter case above, link information to NVD for the vulnerability is provided at the top of each CVE vulnerability information, so that NVD additional information can be referenced from the search of CVE vulnerability database at any time.
In addition, the function to download CVE vulnerability database is also available so that the user can perform advanced searching with user's own computer without relying on functions of an external vulnerability database. (See the screen in Fig. 2.3.) It is also possible to search the database file downloaded locally to the user's computer using this function.

In either case (CVE, NVD), all vulnerability information registered in the vulnerability database is assigned a unique vulnerability identifier in the "**CVE-YYYY-XXXX**" format. In vulnerability search, the evaluator judges whether the given vulnerabilities could lead to potential vulnerabilities of the evaluation target system/device by verifying this CVE identifier and "**Description**", "**References**" information described for that identifier, and possibly NVD information (e.g., "**Overview**", "**Impact**", "**References to Advisories, Solutions, and Tools**").

S3) US-CERT Database (Vulnerability Notes Database): http://www.kb.cert.org/vuls/

Practically, search can be performed by using the screen shown in the figure blow (Fig. 2.4) which appears by selecting "Advanced Search" from the top page of US-CERT Database (Vulnerability Notes Database).

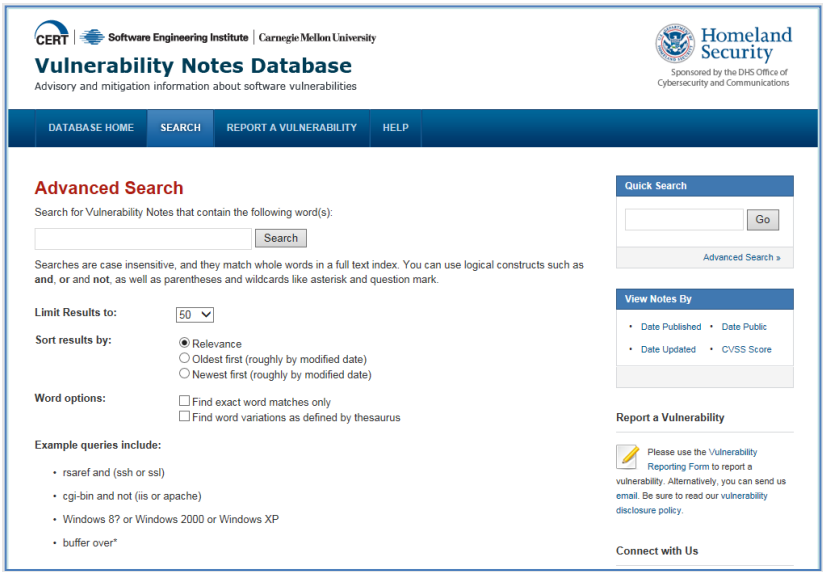

Fig. 2.4 Search Screen of US-CERT Database

As can been seen on this Advanced Search screen, US-CERT database provides various search options. Search is performed by setting a search option that matches the selected keyword and the search objective.
Basic information about the search rules is described in the text description on this screen. It is possible to apply the following rules and search by various criteria or by using wildcards.

- Setting search conditions using reserved words "and ", "or", "not", and reserved symbol "()"
- Setting wildcard search conditions using reserved symbol "?" or "*"
- Case insensitive

The detailed explanation on these search options and search method are described in http://www.kb.cert.org/vuls/html/searchhelp.

All vulnerability information registered in US-CERT database is assigned with a unique vulnerability identifier in the "**VU#XXXXXX**" format. In vulnerability search, the evaluator judges whether the given vulnerabilities could lead to potential vulnerabilities of the evaluation target system/device by verifying this US-CERT database identifier and "**Overview**", "**Description**", "**Impact**", "**Vendor Information**", and "**References**" described for that identifier.
In addition, US-CERT database provides the ability to download vulnerability database as well as CVE. (Refer to URL: http://www.cert.org/download/vul_data_archive/) Therefore, it is possible to search with the user's own computer using this function.

2.2.3. Method for Improving Efficiency of Search of Public Vulnerability Database

In this section, the method for improving efficiency of search of public vulnerability database in Step2~3 is described.

① Method for discovering duplicated contents between multiple databases

Three databases are introduced in chapter 2.1 as open vulnerability databases to use for known vulnerabilities searches. Although each of these databases contains some unique vulnerability information, but the majority of vulnerability information is duplicate information contained in each of these databases.2.1

For example, in the case of JVN iPedia, some vulnerability information includes CVE identifiers as "references", which means that same vulnerability information is included in CVE. (Fig. 2.5).

Here, we consider the case where the vulnerability search by JVN iPedia is completed, and then a similar keyword search is performed using CVE. If CVE searches reveal vulnerability information with the same CVE identifier as JVN iPedia searches, there is no need to perform a vulnerability analysis again if the vulnerability analysis has been thoroughly completed in search with JVN iPedia. Then the analysis summary described in Section 2.3 should indicate that the vulnerability analysis overlaps with other database.2.3

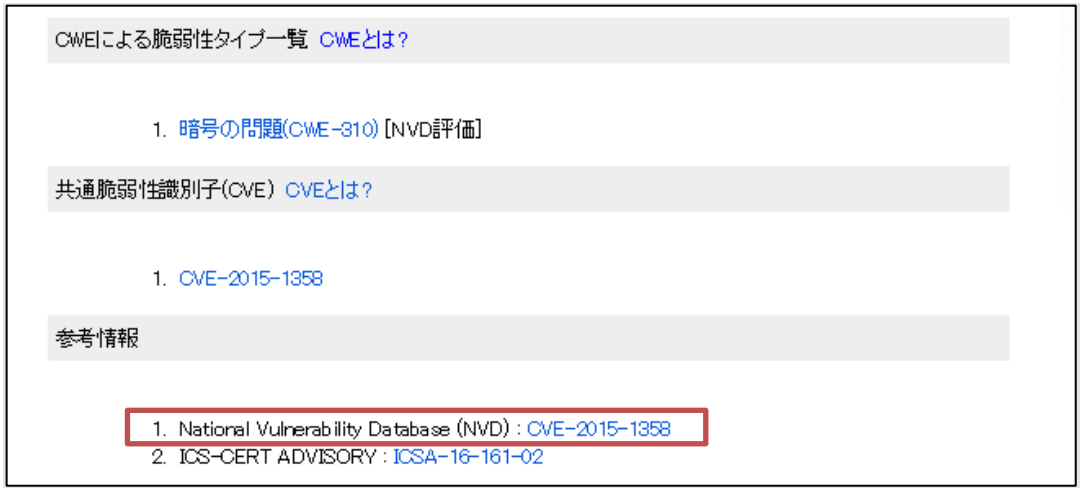

Fig. 2.5 Vulnerability Information of JVN iPedia

② Method for searching only for differences from searches in the past

Because the public vulnerability database is updated daily, database need to be checked regularly. If a vulnerability search has been conducted using the same keyword in the past, it is not necessary to search database for vulnerability information updated prior to the previous search date. So it is recommended to summarize the vulnerability information together with the previous search date.

For example, in the case of JVN iPedia, " Date Public" and " Date Last Updated" can be specified as shown in Fig. 2.1. By using this function, it is possible to search for vulnerabilities except for information that has been searched in the past.

2.3. Summary of Known Vulnerability Analysis Results

For the results of known vulnerability analyses, use public vulnerability database to identify vulnerabilities, and summarize the results of measures against relevant vulnerabilities. The content to be included in the analysis summary is shown in Table 2.3.

Table 2.3 Content to be included in Known Vulnerability Analysis summary

Items described		Description
(1)	Public vulnerability database	Describe the public vulnerability database used in the search.
(2)	ID	Describe the vulnerability identifier of database.
(3)	Relationship with other databases	Describe the identifiers if other databases contain similar vulnerabilities. (e.g., "References" in JVN iPedia)
(4)	Duplication	Describe the number if other databases contain duplicate vulnerabilities and the vulnerability analysis for them have been performed. (If the number is described here, no subsequent entry is required)
(5)	Title	Describe the titles listed in the Public Vulnerability database
(6)	Severity (CVSSv2) ※	Describe the severity of CVSSv2.
(7)	Severity (CVSSv3) ※	Describe the severity of CVSSv3.
(8)	Release date	Describe the date when the vulnerability information was released.
(9)	Final update date	Describe the date when vulnerability information was updated most recently.
(10)	Presence of applicable functions	Describe whether the evaluation target system/device has functions to which the searched vulnerability information is applicable.
(11)	Reason for judgement as “not applicable”	Describe the reason if the judgement result is “not applicable” in (10).
(12)	Whether to implement a countermeasure	Describe whether to implement a countermeasure if the

Items described		Description
		judgement result is “applicable” in (10).
(13)	Reason for not implementing a countermeasure	Describe the reason if the judgement result is “not to implement a countermeasure.” in (12).
(14)	What countermeasure is implemented	Describe what countermeasure is implemented if the judgement result is “to implement a countermeasure” in (12).
(15)	Method for verifying implementation of the countermeasure	Describe how to verify the countermeasure implemented in (14).

※In JVN iPedia, both CVSSv2 and CVSSv3 have been described since December 1, 2015. Prior to that date, only the values in CVSSv2 were described. If information is available only in either one of them, only that available information maybe described..