コンピュータセキュリティシンポジウム 2002
平成 14 年 10 月

JPCERT/CC Vendor Status Notes DB 構築に関する検討

寺田真敏†‡ 土居範久†
terada@doi.ics.keio.ac.jp doi@keio.ac.jp

†慶應義塾大学大学院理工学研究科
〒223-8522 神奈川県横浜市港北区日吉 3-14-1
‡(株)日立製作所 システム開発研究所
〒224-0817 神奈川県横浜市戸塚区吉田町 292

あらまし：インターネットの常時接続の普及に伴い、マルウェアの流布を含む不正アクセス活動は活発化しており、また、その被害も広範囲かつ多岐に渡るようになってきている。しかし、不正アクセス対策を行なうために必要となる、国内で利用されているソフトウェアや装置を対象とする脆弱性情報ならびに対策情報については、「情報が散々している」「影響範囲の把握が難しい」などの解決すべき課題がある。本稿では、このような課題を解決し、国内でのセキュリティ対策推進を支援するために、国内で利用されているソフトウェアや装置の脆弱性を対象とした対策情報データベース(JVN: JPCERT/CC Vendor Status Notes Data Base)の構築について述べる。
キーワード：ネットワークセキュリティ、脆弱性、セキュリティ情報、JPCERT/CC

Consideration on JPCERT/CC Vendor Status Notes DB: JVN

Masato Terada†‡ Norihisa Doi†
terada@doi.ics.keio.ac.jp doi@keio.ac.jp

† Keio University
3-14-1 Hiyoshi, Kouhoku-ku, Yokohama, 223-8522 Japan
‡ Systems Development Laboratory, Hitachi Ltd.
292 Yoshida-cho, Totsuka-ku, Yokoham, 244-0817 Japan

Abstract: Unauthorized access containing Malware propagation is activated and causes a lot of damage. In order to protect the unauthorized access and eliminate the vulnerability, it is necessary to improve the security information providing environment about the domestic software and the equipments. This paper described the overview of JVN(JPCERT/CC Vendor Status Notes Database) , which supports the security information about vulnerability of domestic software and equipments.
key words: Network Security, Vulnerability, Security Information, JPCERT/CC

1. はじめに

インターネットの常時接続の普及に伴い、マルウェアの流布を含む不正アクセス活動は活発化しており、また、その被害も広範囲かつ多岐に渡るようになってきている。特に、2001年7月中旬の「Code Red I/II の流布」、そして2001年9月中旬の「Nimda の流布」は、情報システムにおける不正アクセス対策をサーバだけではなくクライアントにも実施しなければならないことを教訓として残した。しかし、不正アクセス対策を行なうために必要となる、国内で利用されているソフトウェアや装置を対象とする脆弱性情報ならびに対策情報については、「情報が散々している」「影響範囲の把握が難しい」などの解決すべき課題がある。本稿では、このような課題を解決すると共に、国内でのセキュリティ対策推進を支援するために、国内製品や国内向けにポーティングされたオープンソフトウェアなど、国内で利用されているソフトウェアや装置の脆弱性を対象とした対策情報データベース(JVN: JPCERT/CC Vendor Status Notes Data Base)の構築について述べる。

2. 国内における情報提供環境の課題

インターネットをとりまくセキュリティ対策環境は日々改善しており、国内においても脆弱性対策のための情報を早期に入手できるようになってきた。しかし、国内で提供されている脆弱性対策の情報提供環境には以下のような課題がある。

(1) 国内で利用されているソフトウェアや装置を対象とする脆弱性情報ならびに対策情報が散々している

セキュリティインシデントに対する活動を早期から行なっている CERT/CC では、脆弱性情報の対策を喚起するために勧告として配信する CERT Advisory[1]と、脆弱性情報に関連する情報をまとめた CERT/CC Vulnerability Note[2]の2種類を提供している。とくに、後者の Vulnerability Note では、該当する脆弱性に関連するベンダの対策ステータスが一覧としてまとめられており、対策を推進するにあたっては有用なポインタとなる。残念ながら、国内で利用されているソフトウェアや装置を対象とするベンダの対策ステータスの一覧はなく、必要にあわせて散在した脆弱性対策の情報を探し回らなければならない[a]。

(2) 脆弱性の影響範囲の把握が難しい

上記の情報散在とも関係するが、現状の脆弱性情報提供環境では、報告された脆弱性が国内で利用されているソフトウェアや装置にどの程度の影響があるのかを把握しにくい。昨今の SNMP[3], Apache[4] , OpenSSH[5], DNS リゾルバ[6], OpenSSL[7]の脆弱性は、国内で利用されているソフトウェアや装置にも広範囲にわたって影響を与えているはずであるが、おおよその実態すらも把握することができない。

これは、現段階の国内での脆弱性情報提供が、国外で報告された脆弱性情報に対処するというレベルでとまってしまっていること、国内で利用されているソフトウェアや装置という地域に即した脆弱性対策情報提供環境が整備されていないことに起因すると思われる。

3. JVN の概要

JPCERT/CC の支援を得て構成したワーキンググループと共同で構想構築中の JVN では、地域に即した脆弱性対策情報提供環境、すなわち、国内で利用されているソフトウェアや装置を対象とした脆弱性対策情報提供環境を整備することで、上記の課題を解決する。

3.1 JVN 構築のポイント

(1) 勧告と脆弱性対策情報の分離

---

a) 国内製品が CERT Advisory, CERT/CC Vulnerability Notes に掲載されない理由のひとつとして、製品の海外展開状況などが関係していると思われる。

CERT/CC でのアプローチと同様に、注意喚起を促す勧告(Advisory)と、脆弱性に対する対策情報(Vulnerability Note)とを分離する。これにより、勧告として配信されない脆弱性ならびにその対策情報を提供することができる。JVN では、後者の脆弱性に対する対策情報を対象とした情報提供に主眼を置く。

(2) ベンダ主導の対策ステータスの提供ならびに更新

脆弱性そのものについての情報提供は、すでに数多くの組織やベンダによりセキュリティホール情報や脆弱性 DB としてサービス提供されている[8]。ここに、ベンダから提示された対策ステータスや更新情報を組み込むことができれば、情報はより有用なものとすることができる。JVN では、ベンダが提示する対策ステータスや更新情報をまとめあげていくことに主眼をおく。

3.2　JVN が提供する情報構成

図 3.1、図 3.2に JVN で想定している情報構成の概略とサンプル情報を示す。情報構成上の特徴は、以下の通りである。

(1) CERT/CC Vulnerability Note を踏襲する形態とする。

JVN の立ち上げフェーズでは、ベンダの提示する対策ステータスや更新情報を情報提供の対象とするが、今後、国内で利用されているソフトウェアや装置の脆弱性対策情報(Vulnerability Note)を取り扱うことも想定している。

(2) JVN 識別子として、CERT Advisory の文書番号を使用する。

脆弱性を一意に識別する識別子して、CVE (Common Vulnerabilities and Exposures)[9]がある。CVE は、脆弱性に対して一意の識別子を付与することにより、CERT Advisory やその他ベンダが提示する脆弱性情報ならびにセキュリティ情報の関連付けを行うことができるため有用であるが、注意喚起を促す勧告(Advisory)との関連性を考慮し、CERT Advisory の文書番号を使用する。

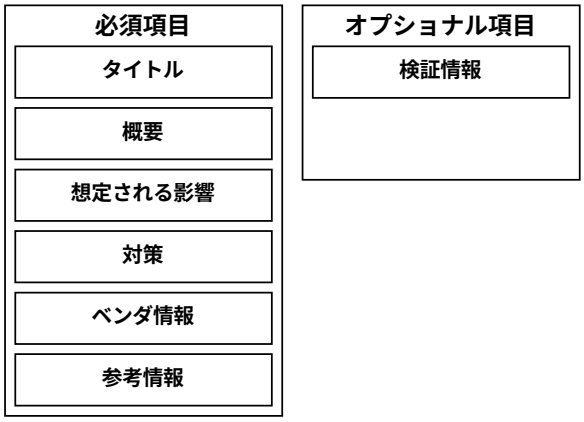

図 3.1　JVN の情報構成案

図 3.2　JVN のサンプル情報

4. JVN 環境構築推進のアプローチ

JVN 構築を推進するにあたっては、以下のような方針で推進していく。

- JPCERT/CC ならびに、JPCERT/CC の活動を支援しているベンダとの協力による推進

JVN 構築にあたっては、勧告を発行する組織、

そして、対策情報を提供するベンダとの協力が必要不可欠である。このため、JPCERT/CC ならびに、JPCERT/CC の活動を支援しているベンダの助言ならびに協力を得て推進していく。

- 中立的な立場での活動推進と広報活動

JVN 構築にあたっては、数多くのベンダからの協力を早期に取り付けることが成功の鍵となる。そのために、中立的な立場から推進していくことと、積極的な広報活動により進めていく。

5. JVN 構築のステップ

5.1 フェーズ分けによる段階的な構築

JVN 構築のステップとして、大きく 3 つのフェーズを考えている。ただし、ステップ 3 については、関連組織との事前調整や情報開示に関する契約などを考慮しなければならないため、本研究では、ステップ 1 と 2 を整備していくことで、ステップ 3 の実現性を問うに留める。

- ステップ 1：発行された勧告に追従した JVN (Vendor Status Notes)の提供

CERT/CC, JPCERT/CC などの IRT が既に発行した勧告に従い、国内の複数ベンダにまたがる脆弱性対策情報を取り纏めていく。

- ステップ 2：国内で報告された脆弱性に追従した JVN(Vulnerability Notes)の提供

国内で利用されているソフトウェアや装置の脆弱性を対象を絞り、報告された脆弱性に関する情報を取り纏めていく。

- ステップ 3：早期対策体制の整備

CERT/CC, JPCERT/CC などの IRT が発行する勧告に対して、ベンダは先行的に対策を準備し、勧告発行時には、国内で利用されているソフトウェアや装置に対しての対策を提示できるよう環境を整備する。

5.2 ステップ 1 における情報提供形態

(1) 既存情報提供形態との関連性

現在、JPCERT/CC では、インシデント報告などに基づき、同種のインシデントの発生を防止するために発行している「緊急報告」、JPCERT/CC が重要と判断したセキュリティ情報のサマリである「JPCERT/CC レポート」を発行している。JVN のステップ 1 では、既に JPCERT/CC が実施している既存情報提供形態との関連性ならびに整合性を保つために、「緊急報告」「JPCERT/CC レポート」に記載されたベンダ情報に基づき JVN データを作成する。これにより、スナップショット的に発行される情報である「緊急報告」「JPCERT/CC レポート」と、これら情報の計時的な集積となる情報「JVN」とが有機的に関連性を持つことができる(図 5.1)。

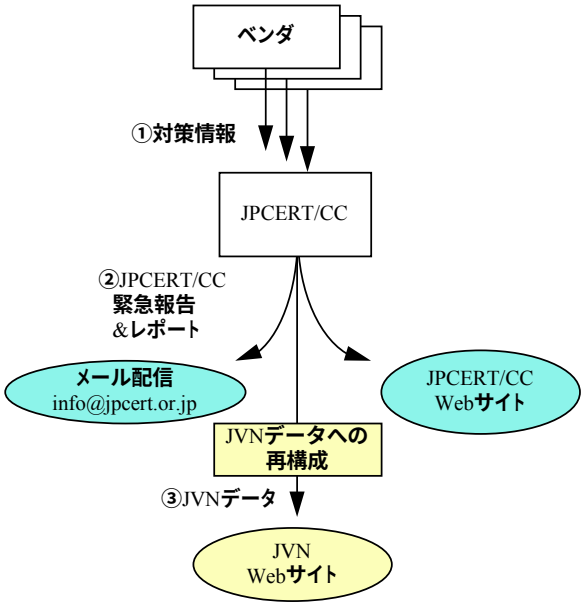

図 5.1 既存 JPCERT/CC 情報との関連性

(2) JVN データ作成ならびに掲載手順

「緊急報告」「JPCERT/CC レポート」に記載されたベンダ情報に基づき JVN データを作成ならびに掲載するまでのフローの一例を図 5.2に示す。フロー中に JVN データの確認作業を入れている目的のひとつに、「ベンダ情報掲載の承諾手順の確立」がある。

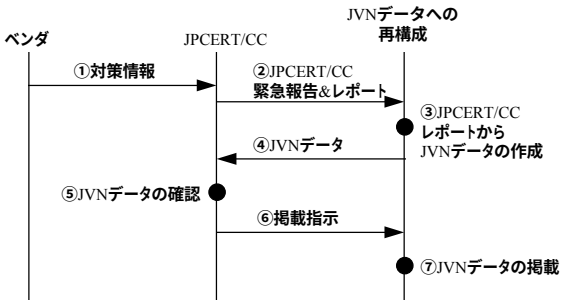

図 5.2 「緊急報告」「JPCERT/CC レポート」から JVN データの作成ならびに掲載フロー

6. 課題

JVN 構築を推進するにあたっては、以下に示すような課題が考えられ、さらに、これら課題については、各ステップ毎に明確にして解決していく必要がある。

- 対象範囲：対象とする脆弱性の範囲はどこまでとするのか。
- 提供情報の内容：どんな情報をどこまで整備するのか。
- 情報提供のタイミング：情報入手から提供までのタイムスパンや時期をどのように調整していくのか。
- 情報の更新：国内で利用されているソフトウェアや装置の対策情報の入手ならび、掲載手続き
- 提供情報に関する責任：公開した情報、およびその情報により発生した現象の責任所在、情報を出さなかったことに対する免責
- 対策情報の確認：ベンダから提供された対策情報に対する確認(脆弱性の除去有無など)

7. おわりに

本稿では、国内で利用されているソフトウェアや装置の脆弱性を対象とした対策情報データベース JVN の構想について述べた。このような環境を整えていくことにより、国内のセキュリティ対策の推進に貢献できるであろうと考えている。現在、JVN Web サイトを構築中であり、準備ができ次第試行公開していく予定である。

謝辞

本研究は、JPCERT/CC の支援を受け実施しているものである。本研究を進めるにあたって有益な助言と協力を頂いた、JPCERT/CC 関係者各位、JVN ワーキンググループに参加して頂いている株式会社インターネットイニシアティブ(IIJ)の齋藤衛氏、インターネットセキュリティシステムズ(株)の高橋正和氏、徳田敏文氏の皆様に深く感謝致します。

参考文献

1) CERT Advisory, http://www.cert.org/advisories/
2) CERT/CC Vulnerability Notes Database, http://www.kb.cert.org/vuls
3) CA-2002-03: Multiple Vulnerabilities in Many Implementations of the Simple Network Management Protocol (SNMP) http://www.cert.org/advisories/CA-2002-03.html
4) CA-2002-17: Apache Web Server Chunk Handling Vulnerability http://www.cert.org/advisories/CA-2002-17.html
5) CA-2002-18: OpenSSH Vulnerabilities in Challenge Response Handling http://www.cert.org/advisories/CA-2002-18.html
6) CA-2002-19: Buffer Overflows in Multiple DNS Resolver Libraries http://www.cert.org/advisories/CA-2002-19.html
7) CA-2002-23: Multiple Vulnerabilities In OpenSSL http://www.cert.org/advisories/CA-2002-23.html
8) V-STAF: http://www.v-staf.org/
LAC: http://www.lac.co.jp/
iDEFENCE JAPAN: http://www.idefense.co.jp/
SofTek: http://www.softek.co.jp/
JISAC: http://www.j-isac.jp/
9) CVE, http://cve.mitre.org/