脆弱性対策情報データベースJVNの提案

寺田真敏[†,††] 高田眞吾[††] 土居範久[††,†††]

インターネットの常時接続の普及にともない，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わたるようになってきている．しかし，不正アクセス対策を行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．本論文では，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（JP Vendor Status Notes）を提案する．さらに，提案に基づき構築したWeb試行サイトの運用を通して得られた利用状況から構築したシステムでの情報提供の有効性を確認した．

Proposal of JP Vendor Status Notes Database (JVN)

Masato Terada,[†,††] Shingo Takada[††] and Norihisa Doi[†††,††]

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 sharing environments about the Japanese domestic software and the equipments. When the new vulnerability is exposed or security advisory is released, the security administrators try to gather countermeasure information about that vulnerability. In this work, we have taken up this issue. We have examined — how we can provide a security information sharing service for the security administrators. We propose JVN (JP Vendor Status Notes) as the security information sharing system. JVN includes two service components, "Vendor Status Notes (VN)" and "Status Tracking Notes (TRnotes)". The former is the countermeasure information service of the vulnerability, and the latter is the event information service of the incidents. This paper discusses the requirements of these services and introduce our sharing framework.

1. はじめに

インターネットの常時接続の普及にともない，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，その被害も広範囲かつ多岐にわたるようになってきている．特に，2003年1月の「Slammerの流布」，2003年8月の「Blasterの流布」は，情報システムにおける不正アクセス対策を情報システムすべての機器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．

本論文では，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を提供する脆弱性対策情報データベースJVN（JP Vendor Status Notes）を提案し，試行運用を通してその有効性について述べる．

JVNは，セキュリティに関わるシステム管理者向けに対策情報を広く告知することを目的とした公開型データベースであり，CERT Advisory[1]ならびにCIAC Bulletin[2]など主要な対策勧告に対する製品開発ベンダの対策情報を集約して提供するとともに，対策勧告で取り上げられた脆弱性に関わる経過を時系列情報として提供することを特徴としている．また，JVNを公開型データベースとして具体化するために，2002年6月にJPCERT/CCの支援を受け慶

† 株式会社日立製作所システム開発研究所
Systems Development Laboratory, Hitachi Ltd.
†† 慶應義塾大学大学院理工学研究科
Graduate School of Science and Technology, Keio University
††† 中央大学大学院理工学研究科
Graduate School of Science and Engineering, Chuo University

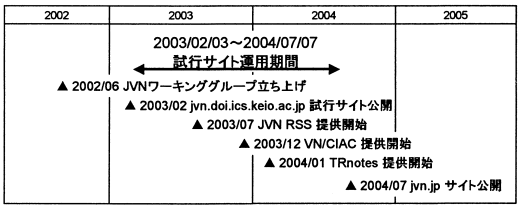

図 1 JVN 試行サイトの構築ならびに運用
Fig. 1 Construction and operation of JVN trial site.

應義塾大学に試行サイト構築ワーキンググループを立ち上げ，2003 年 2 月に JPCERT/CC の試行サイト（http://jvn.doi.ics.keio.ac.jp/）として運用を開始した[3]．

以降，2003 年 7 月に XML フォーマットに共通の書式でドキュメントの見出しや要約などをリスト化する JVN RSS（RDF Site Summary）を用いた情報提供[4]，2003 年 12 月に CIAC Bulletins 対応の Vendor Status Notes - CIAC の情報提供，2004 年 1 月には時系列で経過情報を共有する TRnotes（Status Tracking Notes）の情報提供を開始し[5]，試行サイトでの情報提供の有効性についての検証を行ってきた（**図 1**）．なお，JVN 試行サイトの構築運用にあたって考慮した事項は製品開発ベンダの協力を得た推進である．このために JPCERT/CC とともにいくつかの製品開発ベンダを訪問し，JVN の趣旨説明とともに試行サイトへの情報掲載を依頼することで試行運用へとつなげている．社会人学生という機会は，JVN をより実運用に近いレベル，すなわち JPCERT/CC の試行サイトという位置づけでの実現や特定の製品開発ベンダに偏ることなく中立的な立場でのフレームワーク推進を可能とし，また製品開発ベンダの協力可能範囲をふまえた試行運用の実現に活かすことができたと考えている．

本論文の構成について述べる．まず，2 章で国内における脆弱性対策情報の提供に関する課題を示す．次に，3 章で情報提供のフレームワークと Web 試行サイトでの実現方式を示す．4 章では試行サイトでの提供実績と利用状況を示す．5 章は結論である．

2. 国内における脆弱性対策情報の提供に関する課題

本章では，国内における脆弱性対策情報の提供に関する課題について述べる．

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されており，既存 CSIRT（Computer Security Incident Response Team）や商用サービスによる対策情報提供だけではなく，オープンソース型のコミュニティで脆弱性情報データベース構築を試みる OSVDB（Open Source Vulnerability Database）[6]，脆弱性自身の記述を目的とした仕様 AVDL（Application Vulnerability Description Language）[7] や脆弱性の存在有無確認を目的とした仕様 OVAL（Open Vulnerability Assessment Language）[8] の検討も進められている．また，国内においてもインターネット定点観測システム[9),10)] の観測データ公開提供も始まり，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情報の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対策情報の集約化

セキュリティインシデントに対する活動を早期から進めている CERT/CC では，脆弱性対策を喚起するために勧告として配信する CERT Advisory と，脆弱性に関連する情報をまとめた CERT/CC Vulnerability Note の 2 種類を対策情報として提供している．これら CERT/CC から提供される情報は，国内のセキュリティ教育において脆弱性対策の参照情報として紹介されることも多い．特に，後者の Vulnerability Note では，脆弱性に関連する製品開発ベンダの対応状況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．

ところが，国内マーケットを対象とする製品の対策情報が CERT/CC Advisory や Vulnerability Note に掲載されていることはほとんどない．これは掲載可能な国内の製品開発ベンダが少ないだけではなく，国内の製品開発ベンダにとって，海外展開していない製品の情報を掲載する利点は少ないという製品マーケットにも一部起因している．また，国内の商用サービスによる対策情報の多くは，英語圏の情報が翻訳され提供されているのが実情である．たとえば，国内製品の対策情報を英語版として公開すると，英語圏のセキュリティ情報収集ベンダが拾い上げ，商用サービスが英語を日本語に再翻訳して提供しているという事例もある．

このように，CERT Advisor や Vulnerability Note は国内のセキュリティ教育で紹介されていながらも，実際には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製品開発ベンダの対策情報は掲載されておらず，また商用サービスについても同様な状況となっ

☆ 2004 年 7 月 7 日経済産業省「ソフトウエア等脆弱性関連情報取扱基準」が公示され，以降，日本国内の製品開発ベンダの脆弱性対応状況については対策ポータルサイトである http://jvn.jp/ サイトから公開されている．

ている．このため，セキュリティに関わるシステム管理者は必要にあわせてインターネット上に散在している脆弱性対策情報を探し回らなければならないというのが実情である．

(2) 脆弱性の影響範囲の把握

項番 (1) の情報散在とも関係するが，現状の脆弱性対策情報の提供環境は，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影響を与えているのかを把握しにくい．たとえば，2002 年に報告された SNMP についてはインターネット全体で 90 社近くの製品開発ベンダに影響を与える脆弱性であった[11]．そのほかにも Apache[12]，OpenSSH[13]，DNS リゾルバ[14]，OpenSSL[15] 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く影響を与えているはずであるが，その実態すらも把握することができない状況にある．

このような状況を引き起こしてしまっている要因の 1 つとして，国内マーケットを対象とする製品にオープンソフトウェアがいろいろな形態で取り込まれ，販売されていることがあげられる．また，この課題は，国内での脆弱性対策情報の提供が海外で報告された脆弱性にシステム管理者が対処するというレベルにとどまってしまっており，国内の製品開発ベンダの対応状況を集約するための手順など，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対策情報の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) 脆弱性に関わる経過の共有

2003 年は，1 月末の SQL Slammer，8 月の Blaster，Nachi（Welchia），9 月の Sobig.E などワームの流布だけではなく，7 月には Cisco IOS☆のサービス運用妨害に関わる脆弱性の攻略活動など，インターネットインフラに多大な影響を与えるインシデントが数多く発生した．これらインシデントの発生を通して，国内においても「脆弱性はどのようなものなのか?」「脆弱性の影響を受ける製品は?」「製品開発ベンダの対策情報は?」という脆弱性対策情報に関する提供環境は整備されて始めている．

しかし，「いつ攻撃プログラム（exploit code と呼ばれている）が公開されたのか?」「脆弱性を悪用したインシデントとして何が発生したのか?」「インシデントにともない各組織でどのような対応がとられたのか?」など，インシデントの早期対応ならびに被害拡大を低減するために必要となる経過を共有情報として提供する環境は整備されるに至ってはいない．たとえば，ワームによるインシデント発生は，「脆弱性の発見ならびに公開」「攻撃プログラムの公開」「ワームの出現」という段階を経ることが多く，2003 年 8 月に流布した Blaster，Nachi ワームについても**図 2** に示すように同様な段階を経ている．この場合，「攻撃プログラムの公開」は，未対策システムへの対策促進ならびに，ワーム出現に備えた監視ならびに対応体制のエスカレーションを図るトリガとなる．このように，現在どのような段階にあるのかという経過を情報として共有することは，次に実施すべきインシデント対応施策を検討するうえで必要とされてきている．

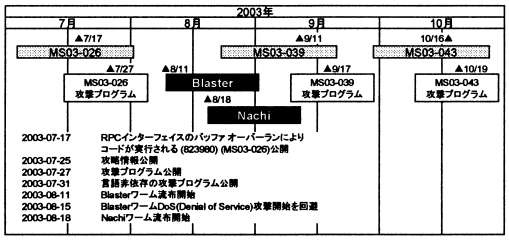

図 2 Blaster, Nachi ワーム出現までの経過
Fig. 2 The appearance process of the Blaster/Nachi worm.

本論文で提案する脆弱性対策情報データベース JVN 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製品開発ベンダの対策情報を集約して提供するとともに，「いつ攻撃プログラムが公開されたのか?」などの脆弱性に関わる経過を時系列情報として提供していくものであり，過去にこのような特徴を持つ研究を行っているものはない．

3. 脆弱性対策情報データベース

本章では，2 章で述べた課題を解決するための脆弱性対策情報データベース JVN（JP Vendor Status Notes）について述べる．

3.1 JVN

不正アクセス対策を行うにあたっては，セキュリティ上なんらかの問題を引き起こす脆弱性を除去するための「脆弱性対策活動」と，実際に発生している侵害活動の回避やセキュリティに関する問題事象を解決するための「インシデント対応活動」があり，これらの活動は**図 3** に示すような時間軸上でのつながりがある．

脆弱性対策情報の提供にあたっては，脆弱性対策活動とインシデント対応活動のつながりを考慮しなければ「脆弱性の発見ならびに公開」から「ワームの出現」のように一連の段階を経るインシデントに対して後手の対応を踏むことになってしまう．そこで，JVN では

☆ Cisco, Cisco IOS は，米国およびその他の地域における，Cisco Systems Inc. および関係会社の登録商標です．その他記載の会社名，製品名はそれぞれの会社の商標または登録商標です．

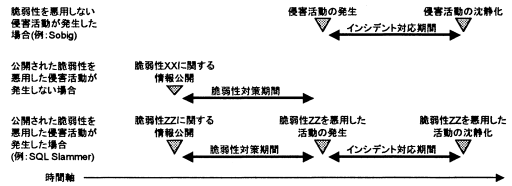

図 3 脆弱性対策とインシデント対応
Fig. 3 The vulnerability handling and incident response.

表 1 Vendor Status Notes における情報提供項目
Table 1 The items of Vendor Status Notes.

項目	説明
識別子	脆弱性対策情報 VN を一意に識別するための識別子
タイトル	脆弱性対策情報の題名
概要	脆弱性に関する情報ならびに脆弱性により影響を受けるバージョン，システムに関する情報
想定される影響	脆弱性により発生しうる影響
ベンダ情報	製品開発ベンダの対策情報
参考情報	官公庁系の注意喚起やインターネットで公開されている脆弱性対策情報などの参考情報と該当する Status Tracking Notes の情報

国内での脆弱性対策ならびにインシデント対応を支援するために，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て対策情報を提供する Vendor Status Notes と，脆弱性に関わる経過を時系列情報として提供する Status Tracking Notes から構成する方式を提案する．

3.1.1 VN — Vendor Status Notes

Vendor Status Notes の目的は脆弱性対策活動を支援するための情報提供であり，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て製品開発ベンダの対策情報を集約整理して提供することで課題 (1)，(2) の解決を図る．

Vendor Status Notes で提供する情報としては，脆弱性の概要，想定される影響，対策に必要となる製品開発ベンダの情報ならびに参考情報から構成する（**表 1**）．

3.1.2 TRnotes — Status Tracking Notes

Status Tracking Notes の目的は，実際に発生している侵害活動の回避やセキュリティに関する問題事象などを解決するインシデント対応活動のための情報提供である．具体的には，図 2 に示したワーム出現までの経過情報以外にも下記のような事例がある．

- 事例 1：短期間に発生する対策の更新を共有する．
  脆弱性対策活動に含まれる部分ではあるが，2003 年 9 月に報告された OpenSSH のバッファ管理機構の脆弱性（CA-2003-24）では，初版の対策版 openssh-3.7.tgz リリースからわずか 12 時間後に，影響を受けるバージョンが「OpenSSH 3.7 未満」から「OpenSSH 3.7.1 未満」となり改訂版 openssh-3.7.1.tgz がリリースされた．さらに 1 週間後に新たな脆弱性が確認され，openssh-3.7.1p2.tgz がリリースされている．製品開発ベンダの迅速な対応は，脆弱性を早期に除去する対策を推進することができる反面，対策状況を短期間に変更する可能性を高め，スナップショットとして発行される注意喚起だけでは状況を把握してきれなくなる場合もある．
- 事例 2：インシデント発生にともなう各組織の対応を共有する．
  2003 年 8 月に出現した Sobig.F は，8 月末にトロイの木馬機能が活性化し，DoS（Denial of Service）攻撃活動を開始するとの報告があり，ISP（Internet Service Provider）によっては「特定 IP アドレスへのパケット遮断」を実施するなどの施策をとっている．また，Blaster 以降，関連省庁が合同で注意喚起を促す機会も増えてきており，各組織の動きをトリガとして対策の加速化を図ることもインシデントを予防するという観点では重要となる．

特に，インシデント対応にあたっては，他の組織と連携して対処する場合もあり，状況把握のための情報共有は連携のための前提条件となる．そこで，Status Tracking Notes で提供する情報としては，**表 2** に示すとおり脆弱性またはインシデントに関する概要に加えて，攻撃プログラムの公開，インターネット定点観測システムの兆候変動，官公庁系の注意喚起発行など監視ならびに対応体制のエスカレーションのトリガとなるイベント，特定パケットの遮断や DNS の設定変更などインシデントの拡大防止のために実施された施策に関するイベントをインシデント対応に求められる時系列イベントとして加味することで，課題 (3) の解決を図る．

3.2 試行サイトでの実現方式

脆弱性対策情報データベースとして JVN を具体化するためには，情報提供に必要となる識別子の付与方法や時系列イベントの表記方法などを規定するとともに，国内で脆弱性対策ならびにインシデント対応を行っている既存 CSIRT が推進する活動との協調が必要となる．本節では，JPCERT/CC の試行サイトとして実施した情報提供について述べる．

表 2 Status Tracking Notes における情報提供項目
Table 2 Status Tracking Notes.

項目	説明
識別子	脆弱性に関して共有すべき状況情報 TRnotes を一意に識別するための識別子
タイトル	脆弱性に関して共有すべき状況情報の題名
概要	脆弱性やインシデントに関する情報
時系列イベント	脆弱性の発見日，各種勧告の発行日，攻撃プログラムの公開日，ワームやウイルスの発生日，官公庁系の注意喚起発行日などのイベント情報
参考情報	該当する Vendor Status Notes の情報

表 3 Vendor Status Notes の構築フェーズ
Table 3 Phase of construction for Vendor Status Notes.

構築フェーズ	説明
ステップ 1	主要な対策勧告に関する製品開発ベンダの対策情報を集約整理し提供
ステップ 2	国内で報告された脆弱性に関する製品開発ベンダの対策情報を集約整理し提供
ステップ 3	製品開発ベンダが勧告発行と同時に対策を提示できる早期対策体制の整備

3.2.1 VN — Vendor Status Notes 試行サイトの構築のアプローチ

Vendor Status Notes 試行サイト構築にあたっては，JPCERT/CC が実施している情報提供との関連を保つことに主眼を置き，下記に示す方針を設定した．

(1) 主要な対策勧告に追従した Vendor Status Notes の提供

試行サイトの構築にあたっては構築フェーズを 3 つに分けることとし（**表 3**），本論文で取り扱うステップ 1 においては，広く知られている対策勧告である CERT Advisory ならびに CIAC Bulletin に追従することにより，インターネット全体に影響を及ぼす可能性の高い脆弱性ならびにインシデントに関する対策情報を提供する．また，CERT Advisory については，国内のシステム管理者の注目度も高いことから，製品開発ベンダの対策情報を集約整理し同日公開することとした．

(2) 対策勧告の文書番号に基づく識別子の付与

脆弱性を一意に識別する識別子して，脆弱性情報ならびにセキュリティ情報の関連付けのために開発された CVE（Common Vulnerabilities and Exposures）[16] がある．しかし，Vendor Status Notes の場合には，システム管理者に対策勧告との関連性を明示的に示すことがより重要であると考え，CERT Advisory あるいは CIAC Bulletin の文書番号に JVN の文書であるプレフィックスを付与した形式を使用する．

(3) 既存情報提供活動との関連性の確保

表 4 メール通知フォーマット
Table 4 Notification mail format from vendor to JVN.

タグ	説明
X-JVN-cano:	CERT Advisory No（必須）
X-JVN-vendor:	ベンダ名称（必須）
X-JVN-id:	対策情報の ID（オプション）
X-JVN-title:	対策情報のタイトル（必須）
X-JVN-url:	対策情報の掲載された URL（必須）
X-JVN-update:	対策情報の更新日（オプション）

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発生の防止を目的とした「緊急報告」，最新のセキュリティ関連情報などを週刊でまとめた「JPCERT/CC レポート」を発行している．試行サイトでは,「緊急報告」「JPCERT/CC レポート」で取り上げる製品開発ベンダ情報との整合性をとり公開型データベースを作成する．これにより，スナップショットとして発行される「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 Vendor Status Notes との連携を図ることができる．

(4) 製品開発ベンダからの対策情報通知手順の確立

国内の製品開発ベンダの対応状況を集約するにあたっては，試行サイト側で一方的に対策情報を検索収集するのではなく，製品開発ベンダの協力を得た推進を実施する．すなわち，製品開発ベンダからの対策情報通知手順を整備することで課題 (2) で示した集約手順の改善を図っていく．ステップ 1 では，製品開発ベンダ側の業務形態と作業工数を考慮し，**表 4** に示すメールフォーマットと試行サイト更新に必要な情報をメールにより通知する手順とを準備することとした．

3.2.2 TRnotes — Status Tracking Notes 試行サイトの構築のアプローチ

2003 年 7 月に報告された Cisco IOS のサービス運用妨害に関わる脆弱性（CA-2003-15）については,「脆弱性の発見ならびに公開」から「攻撃プログラムの公開」までの時間が約 1 日強ときわめて短時間であった．さらに，2004 年 3 月に報告された ISS Protocol Analysis Module（PAM）コンポーネントの ICQ 向け解析ルーチンに関わる脆弱性に至っては，脆弱性対策情報の公開翌日に脆弱性を悪用する Witty ワームが出現している．

脆弱性対策情報公開直後からの経過を共有することは大規模インシデントの発生を未然に防ぐという観点からも有効かつ重要となる．Status Tracking Notes 試行サイト構築にあたっては経過情報を共有することに主眼を置き，下記に示す方針を設定した．

(1) 時単位レベルでの時系列イベント表示

脆弱性対策ならびにインシデント対応に関連する状

況変化は日単位というよりは時単位になりつつある．また，時差を加味したイベントの時系列化は，インターネット全体として状況変化を追いかけることができることから，時差を加味するとともに，可能な限り時単位レベルでのイベント表示を行う．現時点の時刻情報の収集方法として，メーリングリストの場合には投稿時間，Web サイトの場合には HTTP プロトコルのヘッダ情報として提供される Last-Modified を利用することとした．

(2) 公開情報に基づくイベントの時系列化

組織にまたがって経過を共有することを想定し，公開されている情報に基づき状況変化，すなわち時系列イベントをまとめる．これにより，組織間の情報共有でしばしば問題となる情報に対する守秘義務などの制約が発生せず，より多くのシステム管理間での経過情報を共有することが可能となる．

(3) イベントの特徴項目の抽出

脆弱性に関わる経過記述にあたっては，**表 5** に示すイベントを特徴付ける項目を抽出し併記する．これは，類似するイベントどうしの差分の明確化，対応体制のエスカレーションのトリガ，監視項目の対象となりうる項目を抽出している．たとえば，脆弱性が発見された場合には，脆弱性の深刻さや脆弱性により影響を受けるバージョン情報をイベントの特徴付け項目とし，攻撃プログラムの公開の場合には，攻撃プログラムの名前，動作確認の行われた環境，攻撃プログラムの動作として使用すると思われるポート番号を特徴付け項目とした．特に，攻撃プログラムの名前は，攻撃プログラムを掲載するサイトによって名前が異なることも多いことから，同一の攻撃プログラムを異なる名前で参照している場合などに利用する．また，使用すると思われるポート番号については，公開型のインターネット定点観測システム[17] のモニタリング情報を参照する形態をとることで簡易的な機能連携を実現している．

(4) Vendor Status Notes との連携

脆弱性対策活動とインシデント対応活動のつながりを考慮し，脆弱性に関する対策情報 Vendor Status Notes と脆弱性に関する経過情報 Status Tracking Notes を相互参照可能とする．

4. 試行サイトの有効性検証

本章では，試行サイトにおける利用実績ならびに利用状況と，時系列イベントからの特徴抽出を通して JVN の有効性を検証する．

表 5 イベントの特徴項目
Table 5 The characteristic items of the event.

項目	説明
Affected-Port	脆弱性により影響を受けるポート番号
Affected-Version	脆弱性により影響を受けるバージョン情報
Severity-Rating	脆弱性の深刻さ
Cid	攻撃プログラムに付与されていると思われるファイル名
Tested	攻撃プログラムの動作環境に関する情報
Binding-Port	攻撃プログラムやバックドアプログラムが使用すると思われるポート番号

例：攻撃プログラムの公開

日付（JST）	内容
2003-11-12 21:40	Full-Disclosure に “Proof of concept for Windows Workstation Service overflow” が投稿される #Cid: 11.12.MS03-049PoC.c #Tested: Windows 2000 [EN] + SP4 #Binding-Port: 5555 #Post-Date: Wed, 12 Nov 2003 15:40:38 +0300

4.1 利用実績ならびに利用状況

(1) 試行サイトでのサービス提供実績

2003 年 2 月から開始した試行サイトでの Vendor Status Notes 提供事例を**図 4** に示す．試行サイトでは，CERT Advisory ならびに CIAC Bulletin に追従した脆弱性対策情報として約 210 件を提供するとともに，国内製品開発ベンダの協力を得て対策情報通知手順を用いたベンダ情報の更新を実施した．また，概要，想定される影響，ベンダ情報に加え，脆弱性対策情報の Web ページごとに PGP による電子署名情報を準備することにより，対策情報の発信元を確認できる手段を提供した．

また，2004 年 1 月から開始した試行サイトでの Status Tracking Notes 提供事例を**図 5** に示す．試行サイトでは，CERT Advisory，CERT Vulnerability Note ならびに CIAC Bulletin のうち約 40 件を対象に経過情報を提供するとともに，国内 CSIRT 組織の協力を得てイベント情報の更新を実施した．

(2) サービスの利用状況と情報提供の有効性

試行サイト全体の利用状況を**図 6** に示す．試行サイト運用開始から半年が経過して以降は，立ち上げ当初の倍近くの利用頻度となっており，少しずつではあるが活用されていることが分かった．また，**図 7** の VN エントリごとのアクセス数の推移に示す通りアクセス数が山となっている部分は，新たな対策情報が公開されたときとほぼ合致していることと，1 日あたりのアクセス数は公開後おおよそ約 2 週間から 1 カ月まで

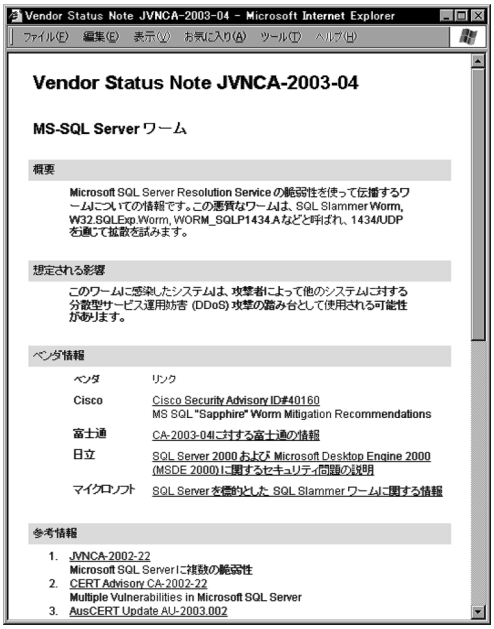

図 4 VN での情報提供事例（CA-2003-04）
Fig. 4 An example of VN about CA-2003-04.

図 5 TRnotes での提供情報事例
Fig. 5 An example of TRnotes about CA-2003-19.

間がそれ以降に比べ多くなっているという結果が得られた．

次に，脆弱性対策情報の提供にあたって考慮した脆弱性対策とインシデント対応活動支援の観点から利用状況について述べる．

(a) 脆弱性が報告されてから，その脆弱性を悪用したインシデントが発生した事例

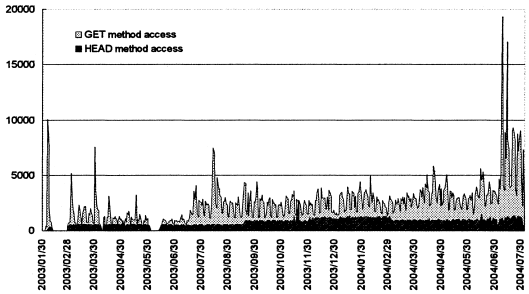

図 6 JVN 試行サイトのアクセス数状況
Fig. 6 Access counts of JVN Trial Site.

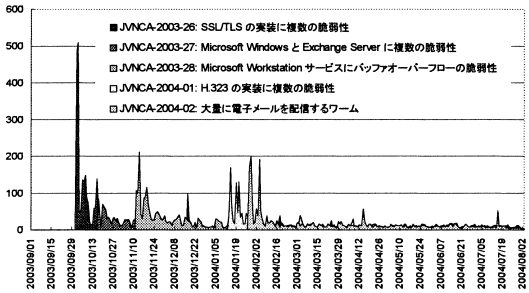

図 7 VN エントリごとのアクセス数の推移
Fig. 7 Access counts of each VN entry.

脆弱性が報告されてから，その脆弱性を悪用したインシデントが発生した事例として Microsoft Windows☆環境の脆弱性を悪用し流布した「Sasser ワーム」を取り上げる．Sasser ワームに関しては**表 6** に示す 3 件の Vendor Status Notes と Status Tracking Notes を提供しており，これら情報の利用状況を**図 8** に示す．当初は対策情報である JVNTA04-104A に比べ，経過情報を示す TRTA04-104A へのアクセスは少ないものの，Sasser ワームの発生にあわせアクセス数が増加している．また Sasser ワームに絞った経過情報のリリースにともない TRJVN04-2004-02 にアクセスが集まり，収束すると全体の経過情報である TRTA04-104A にアクセスが戻っている．この事例の場合，脆弱性対策とインシデント対応活動のつながりを対象とした情報提供が活用されたと判断できる．

(b) 脆弱性の公開をともなわずにインシデントが発生した事例

脆弱性の公開をともなわずにインシデントが発生した事例として「Netsky ワーム」を取り上げる．Netsky ワームに関しては**表 7** に示す 2 件の Status Tracking

☆ Microsoft, Windows は，米国およびその他の国における米国 Microsoft Corp. の登録商標です．

表 6 Sasser ワームに関する VN，TRnotes
Table 6 VN, TRnotes entries about Sasser worm.

名称	種別	提供情報の概要
JVNTA04-104A	VN	2004 年 4 月に Microsoft Windows 環境において確認された複数の脆弱性（MS04-011〜MS04-014）に関する対策情報である．
TRTA04-104A	TRnotes	上記 Microsoft Windows 環境において確認された複数の脆弱性に関する経過情報である．2004 年 4 月〜7 月の期間で約 130 件の経過記録があり，うち，攻撃プログラムの公開に関する記録が 12 件，ウイルスの発生に関する記録が約 30 件となっている．
TRJVN04-2004-02	TRnotes	Sasser ワームに絞った経過情報である．2004 年 4 月〜5 月の期間で約 30 件の経過記録がある．

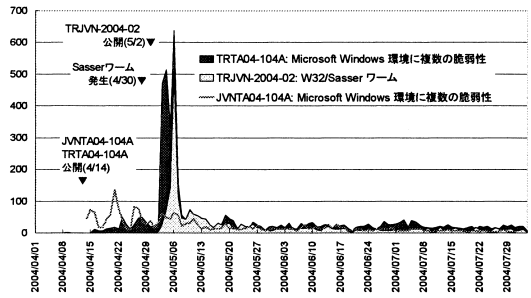

図 8 Sasser ワームに関連する VN，TRnotes のアクセス状況
Fig. 8 Access counts of VN, TRnotes entries about Sasser worm.

Notes を提供しており，これら情報の利用状況を**図 9** に示す．当初は Netsky ワームとその亜種の発生に関する経過情報を示す TRIN-2004-02 へのアクセスは少ないものの，DDoS（Distributed Denial of Service）機能を具備した亜種 Netsky.Q ワームの発生にあわせアクセス数が増加している．また Netsky.Q ワームに絞った経過情報の公開にともない TRJVN-2004-01 にアクセスが集まり，収束すると Netsky ワーム全体の経過情報である TRIN-2004-02 にアクセスが戻っている．この事例の場合，インシデント全体の情報とその中の特定のインシデントを対象とした情報提供の組合せが活用されたと判断できる．

いずれの事例においても，脆弱性対策情報である Vendor Status Notes とインシデント対応のための経過情報である Status Tracking Notes の双方が活用されているという利用状況を確認した．

4.2 ネットワークワーム出現と時系列イベントの関連性

本節では，ネットワークワーム出現に関する時系列イベントの特徴抽出を通して，提案方式が脆弱性対策とインシデント対応活動支援に有効であることを示す．

表 7 Netsky ワームに関する TRnotes
Table 7 TRnotes entries about Netsky worm.

名称	種別	提供情報の概要
TRIN-2004-02	TRnotes	Netsky ワームとその亜種の発生に関する経過情報であり，Netsky.Q ワーム以外の DDoS 機能を具備した亜種 Netsky.S〜Netsky.Z ワームなど，2004 年 3 月〜7 月の期間で約 110 件の経過記録がある．
TRJVN-2004-01	TRnotes	DDoS 機能を具備した亜種 Netsky.Q ワームに絞った経過情報である．2004 年 3 月〜4 月の期間で約 14 件の経過記録がある．

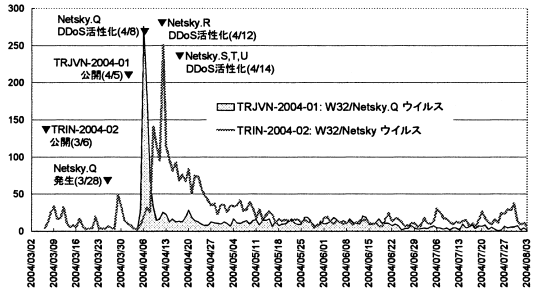

図 9 Netksy ワームに関連する TRnotes のアクセス状況
Fig. 9 Access counts of VN, TRnotes entries about Netsky worm.

2003 年〜2004 年にかけて報告された Windows 環境の脆弱性[18] のうち，その脆弱性を悪用して流布した代表的なマルウェアは**表 8** のとおりである．また，ネットワークワームの出現につながった「MS03-026（CA-2003-16）：Microsoft Windows RPC にバッファオーバフローの脆弱性」「MS04-011（TA04-104A）：Microsoft Windows 環境に複数の脆弱性」の脆弱性について，時系列イベントの抽出を行ったところ**表 9** のような結果が得られた．

この時系列イベントの抽出からは下記の特徴を導き出すことができ，特に，前者の「脆弱性を悪用するトロイの木馬の出現」は，脆弱性の攻略しやすさ，すなわちワームへの発展可能性の 1 つの指標となると思われる．

- ネットワークワームの出現につながった脆弱性は，ワームの出現前に脆弱性を悪用するトロイの木馬が発見されている．
- 脆弱性の悪用に使用するポート番号あるいは攻撃プログラムが使用するポート番号のトラフィックには，攻略活動の兆候が現れる．

このように脆弱性公開後の時系列イベントの提供は，

表 8 脆弱性を悪用したマルウェア
Table 8 Malware which exploits the vulnerability.

脆弱性	発生した代表的なマルウェア
MS03-001	Nachi.F
MS03-007	Nachi〜Nachi.F
MS03-014	Mimail
MS03-026	Blaster, Nachi〜Nachi.F, Raleka, Cirebot
MS03-049	Nachi.B〜Nachi.F
MS04-011	Sasser, Gaobot

表 9 ネットワークワーム出現までの代表的な時系列イベント
Table 9 Event involved in the network worm appearance.

項目	MS03-026 Blaster	MS04-011 Sasser
脆弱性公開日	2003-07-17	2004-04-14
公開された攻撃プログラムの数	4 種類以上	4 種類以上
攻撃プログラムの初出日	2003-07-21	2004-04-17
ワームに利用された攻撃プログラムの出現日	2003-07-27	2004-04-29
ワームの出現	2003-08-11	2004-04-30
脆弱性を悪用するトロイの木馬の出現日	2003-08-02 Cirebot	2004-04-27 Gaobot
脆弱性を悪用するトラフィックの兆候発生日	2003-08-05	2004-04-30
攻撃プログラムが使用するポート番号に関するトラフィックの兆候発生日	2003-08-11	—

インシデントの予兆に関する情報共有にもつながり，脆弱性対策とインシデント対応活動支援の観点からも有効であると判断できる．

5. おわりに

本論文では，国内でのセキュリティ対策推進を支援するための脆弱性対策情報データベース JVN（JP Vendor Status Notes）を提案した．まず，課題解決にあたっては，脆弱性対策活動とインシデント対応活動を考慮し，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て対策情報を提供する Vendor Status Notes と，脆弱性に関わる経過を時系列情報として提供する Status Tracking Notes から構成する方式を提示した．

さらに，提案に基づき構築した Web 試行サイトの運用を通して得られた利用状況から，立ち上げ当初の倍近くの利用頻度となっており，少しずつではあるが活用されていること，また,「脆弱性が報告されてから，その脆弱性を悪用したインシデントが発生した事例」「脆弱性の公開をともなわずにインシデントが発生した事例」のいずれにおいても，脆弱性対策情報である Vendor Status Notes とインシデント対応のための経過情報である Status Tracking Notes の双方が活用されているという利用状況を確認した．現在，JVN 試行サイトは，2004 年 7 月 7 日，経済産業省告示「ソフトウエア等脆弱性関連情報取扱基準」を受けて，日本国内の製品開発ベンダの脆弱性対応状況を公開する対策ポータルサイト（http://jvn.jp/）としてリニューアルされ発展的に活用されている．

今後の課題としては，脆弱性対策情報ならびにインシデント対応のための経過情報を収集し，再配信するための情報流通機構の検討や，インターネット定点観測システムなどの各種ネットワークモニタリングと連携したインシデント検出などがあげられる．

謝辞 本研究は JPCERT/CC の支援を受け実施したものである．本研究を進めるにあたって有益な助言と協力をいただいた JPCERT/CC 関係者各位，JVN ワーキンググループに参加していただいた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，製品開発ベンダの対策情報提供にご協力をいただいた富士通（株）ソフトウェア品質検証部の豊田和男氏の皆様に深く感謝いたします．

参 考 文 献

1) CERT/CC Advisories. http://www.cert.org/advisories/
2) CIAC Bulletins. http://www.ciac.org/cgi-bin/index/bulletins
3) 寺田真敏，土居範久：JPCERT/CC Vendor Status Notes DB 構築に関する検討，コンピュータセキュリティシンポジウム 2002 (2002.10).
4) 寺田真敏，土居範久：RDF Site Summary を用いたセキュリティ情報流通に関する検討，研究報告コンピュータセキュリティ No.021 (2003.07).
5) 寺田真敏，城戸博之，菊池大輔，高田眞吾，土居範久：Status Tracking Notes；時系列イベント情報の共有，研究報告コンピュータセキュリティ No.025 (2004.05).
6) OSVDB. http://www.osvdb.org/
7) AVDL. http://www.avdl.org/
8) OVAL. http://oval.mitre.org/
9) JPCERT/CC: Internet Scan Data Acquisition System (ISDAS). http://www.jpcert.or.jp/isdas/
10) 警察庁セキュリティポータルサイト@police — インターネット定点観測. http://www.cyberpolice.go.jp/detect/observation.html
11) CA-2002-03: Multiple Vulnerabilities in Many Implementations of the Simple Network Management Protocol (SNMP).

12) CA-2002-17: Apache Web Server Chunk Handling Vulnerability.
13) CA-2002-18: OpenSSH Vulnerabilities in Challenge Response Handling.
14) CA-2002-19: Buffer Overflows in Multiple DNS Resolver Libraries.
15) CA-2002-23: Multiple Vulnerabilities In OpenSSL.
16) CVE. http://cve.mitre.org/
17) Distributed Intrusion Detection System. http://www.dshield.org/
18) Microsoft TechNet：セキュリティセンター. http://www.microsoft.com/japan/technet/security/

(平成 16 年 9 月 2 日受付)
(平成 17 年 2 月 1 日採録)

寺田 真敏（正会員）

1986 年千葉大学大学院工学研究科写真工学専攻修士課程修了．同年（株）日立製作所入社．システム開発研究所にてネットワークセキュリティの研究に従事．2004 年 4 月から JPCERT コーディネーションセンター専門委員，2004 年 4 月から中央大学研究開発機構客員研究員，2004 年 8 月から情報処理推進機構セキュリティセンター研究員を兼務．

高田 眞吾（正会員）

1990 年慶應義塾大学理工学部卒業．1992 年同大学大学院理工学研究科修士課程修了．1995 年同博士課程修了．博士（工学）．同年奈良先端科学技術大学院大学情報科学研究科助手．1999 年より慶應義塾大学理工学部情報工学科専任講師．ソフトウェア工学，情報検索等の研究に従事．電子情報通信学会，日本ソフトウェア科学会，ACM，IEEE CS 各会員．

土居 範久（正会員）

1969 年慶應義塾大学大学院博士課程単位取得退学．慶應義塾大学理工学部教授を経て，2003 年より中央大学理工学部教授，慶應義塾大学名誉教授．工学博士．現在，文部科学省科学技術・学術審議会委員，総務省情報通信審議会委員，世界科学会議（International Council for Science（ICSU））Priority Area Assessment Panel of Scientific Data and Information メンバ，科学技術振興機構（JST）社会技術システムミッションプログラム II「情報セキュリティ」研究統括，特定非営利活動法人日本セキュリティ監査協会会長，国際計算機学会（ACM）日本支部長，など．専門はソフトウェアを中心とした計算機科学．