Status Tracking Notes；時系列イベント情報の共有

寺田真敏[†1,†4] 城戸博行[†2] 菊地大輔[†3] 高田眞吾[†1] 土居範久[†1†3]

[†1)] 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
[†2)] 奈良先端科学技術大学院大学 情報科学研究科
〒630-0192 奈良県生駒市高山町 8916-5
[†3)] 中央大学大学院 理工学研究科
〒112-8551 東京都文京区春日 1-13-27

概要：JVN (JPCERT/CC Vendor Status Notes) サイトを含め，国内における対策情報の提供環境は整備されてきているが，「脆弱性に関わる状況変化の情報共有」という観点での情報提供環境については整備されていない．本稿では，課題として取り上げる「脆弱性に関わる状況変化の情報共有」の具体的な事例を提示すると共に，解決の施策として「Status Tracking Notes；時系列イベント情報の共有」と呼ぶ情報流通と，これら情報流通を支援するための対策情報用の XML フォーマットを提案する．
キーワード：ネットワークセキュリティ，脆弱性

Status Tracking Notes; Event sharing based on time series

Masato Terada[†1†4] Hiroyuki Kido[†2] Daisuke Kikuchi[†3] Shingo Takada[†1] Norihisa Doi[†1†3]

[†1)] Graduate School of Science and Technology, Keio University
3-14-1 Hiyoshi, Kouhoku-ku, Yokohama, 223-8522 Japan.
[†2)] Graduate School of Information Science, Nara Institute of Science and Technology
8916-5 Takayamacho, Ikoma, Nara, 630-0192 Japan.
[†3)] Graduate School of Science and Engineering, Chuo University.
1-13-27 Kasuga, Bunkyo-ku, Tokyo 112-8551 Japan.

Abstract: The providing environment of the security information has been improved including the JVN. In order to protect the unauthorized access and eliminate the vulnerability, it is necessary to improve the follow‐up environment of the incidents and the vulnerability. This paper described the overview of TRnotes (Status Tracking Notes), which supports the follow‐up security events about vulnerability and incidents.
Key words: Network Security, Vulnerability

1. はじめに

国内のセキュリティ情報の流通を支援すべく，2003 年 2 月にJVN (JPCERT/CC Vendor Status Notes) サイトの試行運用を開始した[1]．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RSS (RDF Site Summary)を用いた情報提供を開始し[2]，2003 年 12 月にCIAC Bulletins [3]対応のVendor Status Notes / CIAC [4]を立ち上げた．これらのセキュリティ情報流通の支援を通して，脆弱性の対策情報の提供環境は整備されてきているが，「脆弱性に関わる状況変化の情報共有」という観点での情報提供環境については整備されていないことがわかった．

本稿では，課題として取り上げる「脆弱性に関わる状況変化の情報共有」の具体的な事例を提示すると共に，解決の施策として「Status Tracking Notes；時系列イベント情報の共有」と呼ぶ情報流

[†4)] (株)日立製作所 システム開発研究所 セキュリティシステム研究部
〒212-8567 神奈川県川崎市幸区鹿島田 890

通と，これら情報流通を支援するための対策情報用の XML フォーマットを提案する．

2. 関連研究

セキュリティ情報の流通支援については，これまでに様々な検討がなされている．本稿で議論する情報流通に関連する技術を次に示す．

(1) 時系列型の情報に関する流通支援

ある事柄に関して，意見や解説などを日記に近い形式で公開するブログ(web log)が時系列型の情報提供手段のひとつとして活用され始めている．例えば，W32/Netsky.QのDDoS機能活性化の際に，DDoS攻撃対象サイトのDNS設定やWebサイトの応答性に関する情報をブログにより提供するという事例がある[5].

(2) 脆弱性情報に関連する流通支援

アプリケーションの脆弱性に関する情報交換を目的としてAVDL (Application Vulnerability Description Language)[6]が提案されている．「Webアプリケーションを対象とした脆弱性の記述」から「より汎用的な脆弱性の記述」へと段階的な仕様検討が行われている．また，コミュニティーベースの脆弱性情報データベースとしてOSVDB (Open Source Vulnerability Database)[7]が立ち上がっており，データだけではなくデータベース構造も公開している．いずれも仕様を規定し公開していくことで脆弱性の情報流通を図ろうとしている．

(3) インシデント情報に関連する流通支援

JPCERT/CC では，インターネット定点観測システム(ISDAS)で収集したスキャン情報データを国別に解析し，海外 CSIRT に報告するインシデント情報交換システムの稼動を開始した．このインシデント情報交換システムでは，インシデント情報交換用の XML である IODEF(Incident Object Description and Exchange Format)を用いて情報交換を行っている．

本稿で提案する「時系列イベント情報の共有」は，ある脆弱性に関して発生した時系列イベントを共有していくものであり，過去にこのような研究を行っているものはない．

3. 対策情報共有における解決すべき課題

2003 年は，1 月末の SQL Slammer, 8 月の Blaster, Nachi(Welchia)，9 月の Sobig.F など悪質なコードの流布だけではなく，7 月の Cisco IOS のサービス運用妨害に関わる脆弱性など，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．これらのインシデントの発生を通して，「脆弱性の問題はどのようなものなのか?」「脆弱性の影響を受ける製品は?」「ベンダの対策情報は?」という脆弱性の対策情報の提供環境は整備されてきている．

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は何があったのか?」「インシデントに伴いどのような対応がとられたのか?」という脆弱性に関わる状況変化についての情報共有環境は整備されていない．

以下，状況変化による情報共有の必要性を具体的な事例と共に示す．

事例 1：脆弱性の公開ならびに脆弱性を攻略する活動の経過を共有する．

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い．2003 年 8 月に流布した Blaster, Nachi ワームについても同様な段階を経ており(図 3.1), 現在どのような段階にあるのかという情報を共有することは，次に実施すべき施策を検討する際にも有効である．

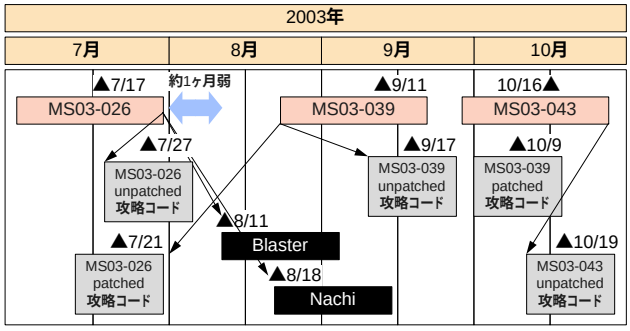


図 3.1 Blaster, Nachi ワーム出現までの経過

また，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(表 3.1), 「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 日強と極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．脆弱性公

開後の活動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．

事例 2：短期間に発生する対策の更新を共有する．

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．

表 3.1 Cisco IOS のサービス運用妨害に関わる脆弱性(CA-2003-15)[8]に関する経過

日時 (JST)	内容
2003-07-17 09:00	Cisco Systems, Inc. Cisco IOS Interface Blocked by IPv4 Packets の初版(Revision 1.0)を Web 公開
2003-07-17 11:40	Full-Disclosure に Cisco Security Advisory: Cisco IOS Interface Blocked by IPv4 Packet が投稿される
2003-07-17 AM	ISS AlertCON ① => ② SecurityFocus ThreatCON ① => ②
2003-07-17 13:58	CERT メーリングリスト経由で CA-2003-15 が届く
2003-07-17 16:10	ISSKK Cisco IOS におけるリモートからのサービス不能攻撃の脆弱点 を Web 公開
2003-07-18 23:35	@Police Cisco社製ネットワーク機器の脆弱性について を Web 公開
2003-07-18 08:00	Cisco Systems, Inc. 影響を受けるプロトコルフィールドを提示した Cisco IOS Interface Blocked by IPv4 Packets の第 3 版(Revision 1.3)を Web 公開
2003-07-18 10:29	Foundstone, Inc. SNScan v1.05 をリリース
2003-07-18 13:42	Full-Disclosure に攻略コードが投稿される #Cid: shadowchode.tar.gz #Cid: 07.18.shadowchode.c
2003-07-18 19:00	Cisco Systems, Inc. 攻略コードが公開されたことに伴い，Cisco IOS Interface Blocked by IPv4 Packets の第 4 版(Revision 1.4)を Web 公開
2003-07-18 PM	ISS AlertCON ② => ③
2003-07-18	OCN Cisco社製ルータの脆弱性に対するＯＣＮの対応について (該当パケットを遮断) を Web 公開 NTT西日本 Cisco社製ルータにおける脆弱性に対するNTT西日本の対応について (該当パケットを遮断) を Web 公開
2003-07-19 00:29	CERT メーリングリスト経由で CA-2003-17 が届く
2003-07-19 AM	SecurityFocus ThreatCON ② => ③
2003-07-21 07:54	Full-Disclosure に "FW: Cisco Vulnerability forensic protocol analysis results." が投稿される
2003-07-22 AM	ISS AlertCON ③ => ② SecurityFocus ThreatCON ③ => ②

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．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．

表 3.2 OpenSSH のバッファ管理機構の脆弱性(CA-2003-24)[9]に関する経過

日時 (JST)	内容
2003-09-16 01:02	Full-Disclosure に "new ssh exploit?" (ssh の新たな脆弱性の存在有無に関する問合せ) が投稿される
2003-09-16 08:31	Full-Disclosure に "openssh remote exploit" (openssh の脆弱性に関する指摘) が投稿される
2003-09-16 13:56	OpenSSH openssh-3.7.tgz, openssh-3.7p1.tgz をリリース
2003-09-16 21:32	OpenSSH OpenSSH Security Advisory: buffer.adv 第 1 版 (RCS file: buffer.c,v) を openbsd-announce に投稿 ならびに Web 公開 #Affected-Version: OpenSSH 3.7 未満
2003-09-17 01:25	OpenSSH openssh-3.7.1.tgz, openssh-3.7.1p1.tgz をリリース
2003-09-17 08:06	CERT メーリングリスト経由で CA-2003-24 が届く #Affected-Version: OpenSSH 3.7 未満
2003-09-17 08:13	OpenSSH OpenSSH Security Advisory: buffer.adv 第 2 版 (RCS file: buffer.c,v channels.c,v) を openbsd-announce に投稿 ならびに Web 公開 #Affected-Version: OpenSSH 3.7.1 未満
2003-09-17 13:37	ISSKK OpenSSH メモリ破損の脆弱性 を Web 公開
2003-09-17	CERT CA-2003-24 第 2 版 を Web 公開 #Affected-Version: OpenSSH 3.7.1 未満
2003-09-19 07:11	Full-Disclosure に "new openssh exploit in the wild!" (remote openssh buffer management sploit を装ったトロイの木馬 theosshucksass.c) に関する情報が投稿される
2003-09-23 14:49	OpenSSH openssh-3.7.1p2.tgz をリリース
2003-09-23 (米国日付)	CERT/CC OpenSSH の "Pluggable Authentication Modules (PAM)" の脆弱性に関する VU#209807, VU#602204 を Web 公開
2003-09-23 21:39	OpenSSH Portable OpenSSH 3.7.1p2 released を openbsd-announce に投稿 ならびに Web 公開
2003-09-30 08:08	CERT メーリングリスト経由で "CERT Advisory Notice: Clarifications regarding recent vulnerabilities in OpenSSH (OpenSSH に 3 つの脆弱性 VU#333628, VU#209807, VU#602204 が報告されていることに関する注意喚起)" が届く

事例 3：インシデント発生に伴う各組織の対応を共有する．

2003 年 8 月末は，Sobig.F の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 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取っている．また，Blaster ワーム以降，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，各組織の動きを踏まえて対策を推進することも効果的にインシデントを防ぐという観点で重要となってきている．

上記事例に示す通り，脆弱性の発見ならびに公開以降の状況変化を共有していくことは，脆弱性対策のフォローアップとして重要である．

表 3.3　Sobig.Fワームの流布(IN-2003-03)[10]に関する経過

日時 (JST)	内容
2003-08-19 08:46	W32.Sobig.F が NewsGroup に投稿される．
2003-08-18 (米国日付)	シマンテック W32.Sobig.F@mm を確認
2003-08-19 (米国日付)	ネットワークアソシエイツ W32/Sobig.f@MM を確認 トレンドマイクロ WORM_SOBIG.F を確認
2003-08-20 08:29	@Police Sobig.Fウィルスの蔓延について を Web 公開
2003-08-22	IPA/ISEC 「W32/Sobig」の亜種 (Sobig.F) に関する情報 を Web 公開
2003-08-22 (米国日付)	CERT/CC CERT Incident Note IN-2003-03 W32/Sobig.F Worm を Web 公開
2003-08-23 02:38	OCN SOBIG.F対策における特定IPアドレスへのパケット遮断を実施
2003-08-23 04:00-07:00	W32.Sobig.F トロイの木馬機能の活性化 (活動は不発)
2003-08-25 04:00-07:00	W32.Sobig.F トロイの木馬機能の活性化 (活動は不発)
2003-08-25 11:37	ISSKK 大量に電子メールを配信する Sobig.F ワーム - トロイの木馬機能 を Web 公開
2003-08-25	OCN SOBIG.F対策における特定IPアドレスへのパケット遮断について を Web 公開
2003-08-29 04:00-07:00	W32.Sobig.F トロイの木馬機能の活性化 (活動は不発)
2003-08-31 04:00-07:00	W32.Sobig.F トロイの木馬機能の活性化
2003-09-05 04:00-07:00	W32.Sobig.F トロイの木馬機能の活性化
2003-09-07 04:00-07:00	W32.Sobig.F トロイの木馬機能の活性化
2003-09-10	W32.Sobig.F 活動停止
2003-09-18	OCN SOBIG.F対策における特定IPアドレスへのパケット遮断の解除について を Web 公開

4.　時系列イベント情報の共有

本章では，上述の課題解決を図るために，報告された脆弱性に関して「いつ攻撃プログラムが公開されたのか?」「脆弱性を悪用したインシデントは何があったのか?」「インシデントに伴いどのような対応がとられたのか?」という視点から脆弱性に関わる状況変化を時系列にまとめていく TRnotes (Status Tracking Notes)について述べる．

4.1　TRnotes の概要

TRnotes は，脆弱性に関わる状況変化を時系列でまとめていくことから，図 4.1に示すような情報構成をとっている．図 4.2にその情報構成に沿ったサンプル情報を示す．また，情報構成にあたっては，以下に示すような特徴を持たせている．

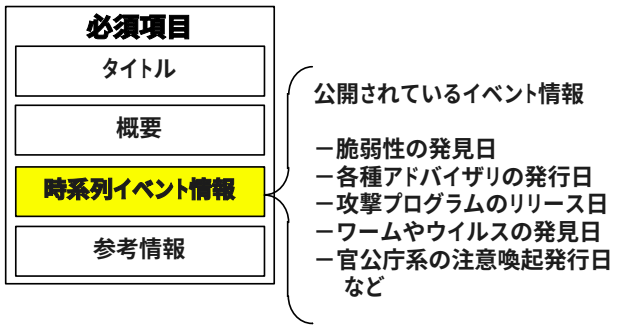


図 4.1　TRnotes の情報構成

図 4.2　TRnotes のサンプル情報

(1) 時単位レベルでのイベント表示

表 3.1～表 3.3の経過で示す通り，状況変化は日単位というよりは時単位になりつつある．このことを踏まえ，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 を利用している．

(2) 脆弱性に関する対策情報との連携

「脆弱性に関する対策情報」と「脆弱性に関する状況変化情報」との関連付けを行なう．この結果，対策情報をいろいろな側面から提供できることになる．ここでは，既に試行を行っている JVN: Vendor Status Notes との連携を図っている．

(3) 公開情報に基づくイベントの時系列化

組織にまたがって状況変化を共有することを想定し，公開されている情報をベースに時系列イベントをまとめている．これにより，情報に対する守秘義務などの制約が発生せず，より多くのセキュリティ担当者間での状況を共有することが可能となる．さらに，イベント記述にあたっては，表 4.1に示す項目を抽出していくことで，脆弱性に関わる状況変化の特徴付けを行っている．なお，特徴付けを行う項目の拡張については，今後の課題である．

表 4.1　特徴付けに使用している項目

項目	内容
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
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	攻撃プログラムが使用すると思われるポート番号

4.2.　時系列イベント情報の収集を想定した対策情報用 XML フォーマット

TRnotes による時系列イベント情報の共有を実現する上で，脆弱性に関連するイベント情報の収集と，そのイベントの発生時刻の抽出がポイントとなる．ところが，HTTP プロトコルのヘッダ Last-Modified に頼った現行の時刻抽出では，「Last-Modified が付加されていない場合がある」「その値が情報公開などのイベント時刻に合致しているとは限らない」などの課題を抱えている．そこで，TRnotes では，この課題を合わせて解決するために，時系列イベント情報の収集を想定した対策情報用 XML フォーマットとして，情報の記述粒度による使い分けを想定した，概要記述向けと詳細記述向けフォーマットを提案する(図 4.3).

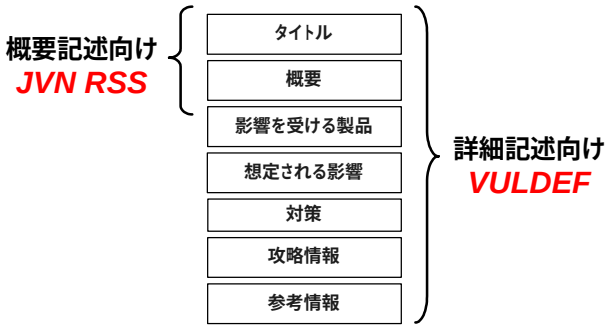


図 4.3　概要記述(JVN RSS)と詳細記述(VULDEF)

(1) 概要記述向け：JVN RSS

概要記述向けの XML フォーマットとしては，既に試行運用で使用している JVN の RSS を利用できる．JVN の RSS では，日付要素(dc:date)と関連付け要素(dc:relation)を備えており，「タイトル」「概要」を対象とした時系列イベント情報の収集に向いている．

(2) 詳細記述向け：VULDEF

VULDEF(Vulnerability Data Publication Format): Security Advisory Publication Format は，対策情報を詳細に記述するための XML フォーマットであり，以下の要件を前提に作成を行った．UML によるデータモデルは図 4.4の通りである．

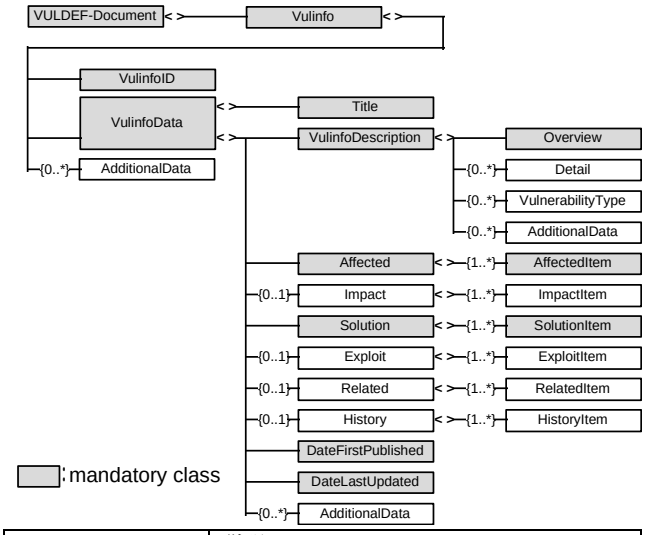
対策情報提供フォーマットとして

- 各々のベンダ・組織が作成する対策情報のコア・フォーマットと成り得ること．
- 各々のニーズを満たす為の例外的な詳細部について記述可能なマージンを取っておくこと．
- 将来的な予測不能な新たな記述に対して，拡張可能であること．

時系列イベント情報収集フォーマットとして

- 関連付けを行うために必要となる要素を持っていること．
- 時刻情報を抽出するために，登録日と更新日を要素として持っていること．
- 状況変化の特徴付け項目を取り込むことができること．

対策情報として最低限必要な項目として，「対策情報の題名(Title)」「脆弱性に関する概要(Detail)」「脆弱性により影響を受けるシステムに関する情報(AffectedItem)」「脆弱性により想定される影響(AffectedItem)」「脆弱性を回避するための施策(SolutionItem)」に絞り込みを行っている．また，特徴付け項目を取り込むために，「脆弱性の相対的な深刻度の指標」「NIST ICAT で規定している脆弱性のタイプ」「脆弱性を攻略するために必要となる環境」「影響を受ける製品のベンダ名／製品名／バージョン番号」などをクラスの属性として用意した．VULDEF については，現在，JPCERT/CC Alert, Bugtraq Vulnerability Archive, CERT Advisory, JVN, CERT/CC Vulnerability Note の 5 つのセキュリティ情報を対象にデータモデルの受容性確認を行っている．



クラス	説明
Title	対策情報の題名
VulinfoDescription	脆弱性に関する情報(概要，詳細，脆弱性のタイプなど)
Affected	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
Impact	脆弱性により想定される影響
Solution	脆弱性を回避するための施策
Exploit	脆弱性の攻略に関する情報
Related	脆弱性ならびに対策に関連する情報
History	改訂履歴など
DateFirstPublished	対策情報の初版公開日
DateLastUpdated	対策情報の最新更新日
AdditionalData	備考用

図 4.4　VULDEF のデータモデル

5. おわりに

本稿では，脆弱性に関わる状況変化に関する情報共有TRnotesと，時系列イベント情報の収集を想定した対策情報用XMLフォーマットについて述べた．状況変化に関する情報は，JPCERT/CCインターネット定点観測システムISDAS(Internet Scan Data Acquisition System) [11]などの各種ネットワークモニタリングと連携することにより相乗効果が得られると考えている．また，対策情報用XMLフォーマットについて時系列イベント情報の収集だけではなく，脆弱性検査ツール[12]での利用を検討していきたいと考えている．

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)寺田，土居: JPCERT/CC Vendor Status Notes DB 構築に関する検討, CSS2002
http://jvn.doi.ics.keio.ac.jp/
2) 寺田，土居: RDF Site Summary を用いたセキュリティ情報流通に関する検討，情処学会研究報告 2003-CSEC-21
3) http://www.ciac.org/cgi-bin/index/bulletins?all
4) JVN/CIAC, http://jvn.doi.ics.keio.ac.jp/
5) F-Secure : News from the Lab
http://www.f-secure.com/weblog/
6) AVDL, http://www.avdl.org/
7) OSVDB, http://www.osvdb.org/
8) CERT Advisory CA-2003-15: Cisco IOS Interface Blocked by IPv4 Packet
http://www.cert.org/advisories/CA-2003-15.html
9) CERT Advisory CA-2003-24: Buffer Management Vulnerability in OpenSSH
http://www.cert.org/advisories/CA-2003-24.html
10) CERT Incident Note IN-2003-03: W32/Sobig.F Worm
http://www.cert.org/incident_notes/IN-2003-03.html
11) JPCERT/CC インターネット定点観測システム
http://www.jpcert.or.jp/isdas/
12) 菊池他: バージョン情報を用いた脆弱性ソフトウェア検査システムの検討，情処学会研究報告 2004-CSEC-25