

Status Tracking Notes ; 時系列イベント情報の共有

寺田真敏 *1*a

terada@doi.ics.keio.ac.jp

高田 眞吾 *1

michigan@ics.keio.ac.jp

土居範久 *1,*2

doi@ise.chuo-u.ac.jp

*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) 中央大学 理工学部 情報工学科

〒112-8551 東京都文京区春日 1-13-27

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)サイトを立ち上げた[1]。以降、2003年07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、要約などをリスト化するRSS (RDF Site Summary) を用いたセキュリティ情報の提供試行[2]、2003年12月にCIAC Bulletins [3] 対応の Vendor Status Notes / CIAC の提供試行[4]を行ってきた。

これらの情報流通の支援活動を通して、解決すべき新たな課題のあることがわかった。本稿では、その課題と解決のための施策である「Status Tracking Notes ; 時系列イベント情報の共有」について述べる。

2. 脆弱性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.E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、現状のセキュリティ情報の共有は、報告された脆弱性に関して、「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?」「その製品ベンダの対策情報?」という脆弱性対策につ

いては整備されてきてはいるが、「いつ攻略コードが公開されたのか?」「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の情報共有は未整備であることがわかった。

以下、状況変化による情報共有の事例を示す。

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」「攻略コードの公開」「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についても同様な段階を経ており(図2.1)、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、次の施策を検討する際にも有効である。

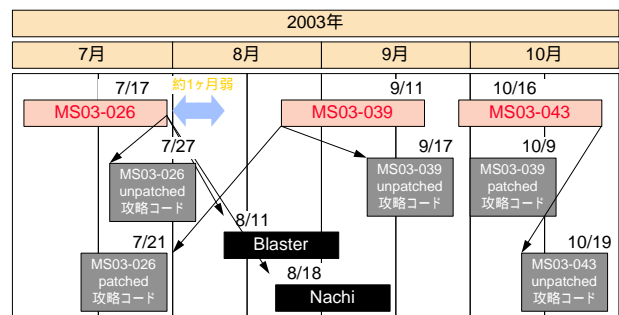


図 2.1 Blaster, Nachi 出現までの経過

また、2003年7月に報告されたCisco IOSのサ

*a) (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

ービス運用妨害に関わる脆弱性(CA-2003-15)については(表 2.1)、「脆弱性の発見ならびに公開」から「攻略コードの公開」までの時間が約 1 日強と極めて短時間であり、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となるであろう。

表 2.1 Cisco IOS のサービス運用妨害に関わる脆弱性(CA-2003-15)[5]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 => SecurityFocus ThreatCON =>
2003-07-17 13:18	First メーリングリスト経由で CA-2003-15 が届く
2003-07-17 13:37	JPCERT メーリングリスト経由で CA-2003-15 の FYI が届く
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 =>
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 (該当バケットを遮断) 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 (該当バケットを遮断) を Web 公開
2003-07-18 23:37	First メーリングリスト経由で CA-2003-17 が届く
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 09:12	JPCERT メーリングリスト経由で CA-2003-17 の FYI が届く
2003-07-19 AM	SecurityFocus ThreatCON =>
2003-07-21 07:54	R02 Full-Disclosure に "FW: Cisco Vulnerability forensic protocol analysis results." が投稿される
2003-07-22 AM	ISS AlertCON => SecurityFocus ThreatCON =>

事例 2 : 短期間に発生する脆弱性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、

表 2.2 OpenSSH のバッファ管理機構の脆弱性 (CA-2003-24)[6]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 より以前
2003-09-17 01:25	OpenSSH openssh-3.7.1.tgz , openssh-3.7.1p1.tgz をリリース
2003-09-17 06:53	First メーリングリスト経由で CA-2003-24 が届く #Affected-Version: OpenSSH 3.7 より以前
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 より以前
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 より以前
2003-09-17 09:15	JPCERT メーリングリスト経由で CA-2003-24 の FYI が届く
2003-09-17 13:37	ISSKK OpenSSH メモリ破壊の脆弱性 を Web 公開
2003-09-17	CERT CA-2003-24 第 2 版 を Web 公開 #Affected-Version: OpenSSH 3.7.1 より以前
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

影響を受けるバージョンが「OpenSSH 3.7 より以前」から「OpenSSH 3.7.1 より以前」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。

ベンダ側の早期対応は、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できなくなる場合もある。

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.E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

表 2.3 Sobig.Eワームの流布(IN-2003-03)[7]に関する経過

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)	日本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ウイ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

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た。

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になると考えられる。

3. TR notes の概要

TR notes (Status Tracking Notes)は、報告された脆弱性に関して、「いつ攻略コードが公開されたのか?」「脆弱性を悪用したインシデントは何かあったのか?」「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を取りまとめていくことにより、上記の課題を解決する。

図 3.1、図 3.2に TR notes 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。

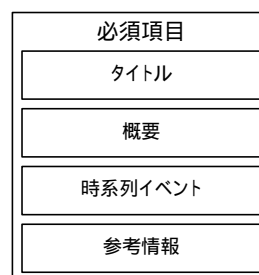


図 3.1 TR notes の情報構成案

(1) 時刻レベルでのイベント表示

表 2.1～表 2.3の経過で示す通り、状況変化は日単位というよりは時刻単位になりつつある。このことを踏まえ、可能な限り時刻レベルでのイベント表示を行う。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 を利用することができる。

(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」とを関連付けることにより、脆弱性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く。

(3) 公開情報に基づく情報共有

より多くの組織間で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、状況変化をまとめていく。



図 3.2 TR notes のサンプル情報

4. 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TR notesの構想について述べた。このような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) [8]などの各種ネットワークモニタリングの状況変動データ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。現在、TR notes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(IJ)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) JPCERT/CC Vendor Status Notes DB 構築に関する検討

<http://jvn.doi.ics.keio.ac.jp/nav/CSS02-P-97.pdf>
<http://jvn.doi.ics.keio.ac.jp/>

2) RDF Site Summary を用いたセキュリティ情報流通に関する検討

<http://jvn.doi.ics.keio.ac.jp/nav/2003-csec-21-40.pdf>
<http://jvn.doi.ics.keio.ac.jp/rss/>

3) <http://www.ciac.org/cgi-bin/index/bulletins?all>

4) Vendor Status Notes / CIAC

<http://jvn.doi.ics.keio.ac.jp/>

5) CERT Advisory CA-2003-15: Cisco IOS Interface Blocked by IPv4 Packet

<http://www.cert.org/advisories/CA-2003-15.html>

6) CERT Advisory CA-2003-24: Buffer Management Vulnerability in OpenSSH

<http://www.cert.org/advisories/CA-2003-24.html>

7) CERT Incident Note IN-2003-03: W32/Sobig.F Worm

http://www.cert.org/incident_notes/IN-2003-03.html

8) JPCERT/CCインターネット定点観測システム

<http://www.jpccert.or.jp/isdas/>