個人の社会生活に様々な影響を及ぼし始めた コンピュータセキュリティの今後

墨　岡　　学

はじめに

五島昌明先生から平成17年度の卒業式の場で「身内の組織内のコンピュータで管理している個人情報について，ちょっと相談に乗って欲しい」とのお話を聞いた。それをきっかけに，セキュリティについて，特にコンピュータセキュリティについて身近で発生した事件を中心にして現状をまとめた。情報流出，偽メール事件など世間的な話題からはじめる。つぎに，伝説のハッカーであるケビン・ミトニックがセキュリティの人間的な要素をコントロールする大切さを語った「The Art of Deception」の一部を紹介する。これは，情報セキュリティに関して2002年に話題となった本である。さらに日本国内で行政機関情報などをインターネットへ情報流出させた原因となったとして，Winnyそのものが悪であると批判された。そのWinnyの作者である金子勇氏によって平成18年3月11日土曜日にソフトウェア技術者連盟大阪セミナーで講演「Winnyの技術とその到達点」が行われた。これらのセキュリティ問題を中心にして本稿をまとめた。「体育人として勝負にこだわり続けた五島先生」に贈るため，本論はプログラマであることに，こだわり続ける筆者の立場での見解であることをはじめにお断りしておきたい。

政府機関の機密情報流出

朝日新聞2006年3月16日木曜日の朝刊に「ウィニー〈改行〉対策は「使わ

ぬこと」〈改行〉政府お手上げ」の見出しで政府が3月15日に発表した内容をもとにした記事が掲載されている。この記事には,いくつか特徴がある。まず,見出しの改行の入れ方が,凝っている。3行の見出しのうち,中の“対策は「使わぬこと」”は黒地に白字になっている。この中の行を飛ばすと,「ウィニー政府お手上げ」となってしまう。読者には,ウィニーに対する情報流出の防止策がないことを政府が認めてしまったと,はっきり印象付けてしまう。もうひとつ,政府が特定のソフトウェアの名前を記者会見の場であげたことである。安倍官房長官は記者会見で「最も確実な対策はパソコンでウィニーを使わないこと」であると,Winnyの使用自粛を国民に呼びかけた。このような具体的なソフトウェアの名称を政府が公の場で出したことは,過去に例がない。コンピュータ関連で,首相や閣僚が「IT」や「フロッピーディスク」などの抽象的な名詞を口にしたことはあったが,それ以上に具体的なものは何もなかった。このことからもWinnyが衝撃的なソフトウェアであることを示している。

同記事中のWinnyを介しての情報流出が起きた公的機関などの例を次にあげる。

05年7月　原子力安全保安院の原発検査報告書
11月　関西電力原発の安全管理体制表など
12月　日本航空の航空安全ダイヤ集中管理関連システム
東京電力のシステム設計ガイドライン
06年1月　神奈川県警の空き巣被害情報
2月　鹿児島刑務所・福岡拘置所の受刑者情報
宮崎地検に関係する容疑者情報
海上自衛隊護衛艦に関する暗号情報
東京地裁の取り扱った個人情報
3月　陸上自衛隊の業務情報
航空自衛隊の業務情報

岡山県警の捜査情報

愛媛県警の捜査情報

これらは，すべて政府機関の機密情報に属するものである。しかし，Winnyが政府機関の機密情報を主たるターゲットとし，それをインターネットに流出させているのでは，もちろんない。インターネットという大衆（the masses）民衆（the public）の利用可能なネットに誰かがこれらの政府の流出機密情報を置いたことが問題点である。それが，流出を意図して置かれたものか，そうでないのかは，この先の議論とする。

偽メール事件

さきほどの政府機関の機密情報の流出事件と直接の関係を示すものはなにもないが，この「ウィニーを使わないように」の政府発表のあった日付で，全国紙にある謝罪文が掲載された。それは〈「偽メール」に関する謝罪文〉との見出しで掲載された謝罪広告であった。その全文を引用する。

「偽メール」に関する謝罪文

武部勤氏の次男に3,000万円を送金するよう指示したメールは全くの偽物であり，送金された事実はなく，メールの内容も全くの事実無根でした。

心よりお詫び申し上げます。

衆議院議員永田寿康及び民主党は，予算委員会や党首討論における質疑，または報道を通じて，あたかも3,000万円がライブドアから武部勤氏の次男の金融機関の口座に送金され，ライブドアの資金が武部幹事長周辺に流れたと指摘しましたが，全くの事実無根の発言でありました。

武部勤氏の次男ならびに同氏が経営される会社関係者の皆様に対し，その名誉を著しく毀損しましたことを心からお詫び申し上げます。また，会社業務にも多大なご迷惑をおかけしましたことを衷心より陳謝いたします。

名誉毀損にかかる国会での発言部分は議事録の削除を申し出させていただきます。今後は国会議員の発言の影響力を十分に自覚し，事実関係を十分調査した上で国会の質疑等を行ってまいります。

2006年3月15日

民主党

衆議院議員　永田寿康

メールに偽物と本物の違いがどのようにあるのかどうか。これは，大衆民衆の中でその区別が自らの力でできるものは，おそらく非常に少数であると推測される。

民衆に広く利用され俗にフリーメールと呼ばれている，使用料金などが一切無料のメールがある。

その中の一つであるYahoo!メールで，実際に筆者のアドレスsumioka@yahoo.co.jpに届いたものを示す。もちろんこれは，迷惑メールに該当するものである[1)]。したがって，通常は受信メール一覧から消去，あるいは，プロバイダの迷惑メール防止機能により自動的に迷惑メールフォルダに分類され受信者が見ることは少ない。下記のメール情報は，Yahoo!メールでメールを開封したときの標準的なものである。

From : “菅　真愛”〈apprehend751@coo.net〉アドレスブックに追加

To : Suemitsu_dora2@

1）実際に，大学の筆者のメールアドレスには，類する迷惑メールが1日に300通近く届くこともある。メールユーザ・エージェント（MUA）の機能を利用して自動分別しなければ手に負えなくなってしまった。従って，常用の頻度の高い送信者からのメールを選別して読むようになってしまう。常用でないメールアドレスからのものは「その他のアーカイブ」にしまわれ，暇なときにしか開いて読むことはない。この傾向は筆者のメール相手でも同じようであり，筆者の新規のアドレスからのメールは無視され読まれていないことがわかった。

Subject : Re :

Date : Sat, 10 Jun 2006 06 : 19 : 20 ＋0500

はじめまして 32 歳主婦のかずみです。

私の親友を 2 人紹介したいと思っております。

高校からの友達で 3 人仲良しです。（以下省略）

このメールにはフラグがついていません。［フラグを付ける－未読にする］

迷惑メールであると報告

X-Apparently-To : sumioka@yahoo.co.jp via 203.216.226.187 ; Sat, 10 Jun 2006 10 : 19 : 31 ＋0900

Authentication-Results : mta93.mail.bbt.yahoo.co.jp from=coo.net ; domainkeys= neutral（no sig）

X-Originating-IP : ［220.175.94.209］

Return-Path : 〈apprehend751@coo.net〉

Received : from 220.175.94.209（HELO202.93.77.230）（220.175.94.209）by mta93.mail.bbt.yahoo.co.jp with SMTP ; Sat, 10 Jun 2006 10 : 19 : 30 ＋0900

X-Message-Info : 842nbATOitWF376RvfBWE6DYG60XZwPssMYEgnaRNtf66RCL

Received : from olive.freemail.ne.jp（128.2.213.190）by ipa95-lkb170.livedoor.com with Microsoft SMTPSVC（7.1.5131.6264）; Fri, 09 Jun 2006 18 : 18 : 20-0700

Received : from so-net.ne.jp（aol.com 220.120.2.236）by nifty.ne.jp（8.12.10/8.12.9） with ESMTP id ie80EFLZ947 for 〈suemitsu_dora2@yahoo.co.jp〉; Fri, 09 Jun 2006 19 : 17 : 20-0600（EST）（envelope-from apprehend751@coo.net）

Received : from GXI15865525427370（modemcable5.90597-604.k.hotmail.com169.176.130.41）（authenticated bits=9）by hotmail.com（8.12.10/8.12.9）with ESMTP id pzu8M7y926 for〈suemitsu_dora2@yahoo.co.jp〉; Fri, 09 Jun 2006 21 : 19 : 20-0400（EST）(envelope-from apprehend751@coo.net）

Message-ID : 〈12810nnh266t50$ps792u19zi457$0v08au327@F863543226618〉

From : “菅 真愛”〈apprehend751@coo.net〉アドレスブックに追加

To : Suemitsu_dora2@

Subject : Re :

Date : Sat, 10 Jun 2006 06 : 19 : 20 ＋0500

MIME-Version : 1.0

Content-Type : multipart/alternative ; boundary＝“－－232408029849567”

Content-Length : 1146

ここでは，これをコンピュータやネットについて特に知識はなく猜疑心も特に強くない人が受け取った場合を想定してみる。おそらく，その人は，From の項目が送信者であること，To が受信者であること，Subject がそのメールの件名であるくらいは判断できる。Date が日付と時間であることは明白だが，受信の日時であろうと推測する人と，発信日かもしれないと思う人たちに分かれるかもしれない。その判定は置いておくことにして，まず，From の発信者項目にある名前は見るだろう。2重の引用符で囲まれた文字列がおそらく本名あるいは発信者が名乗る姓名であることも推測するだろう。通常メールの送受信に慣れていれば，そこでそれが，まったく見知らぬ人の場合は無視することが多いが，郵便の場合は開封する習慣があれば，電子メールもクリックして開

封することになる。さらに，〈　〉で囲まれたものが電子メールアドレスであることがわかっても，@の右側がドメイン名であることを知って，ドメインに関するインターネットの規則をある程度知っている人はかなり少ない。ドメイン名がインターネットの住所に相当することも，漠然とわかっても，その住所の記述に関する規則を知っている人はさらに少ない。

初期の頃のインターネットユーザは，InterNIC の Whois データベース[2] を使うことを必ず教わったのだが，大学の IT スキルズのような入門科目で，それの使い方をしっかりと教えていないようである。これは，それが英語圏のものであることも原因となっているのかもしれない。

この Whois データベース検索により，次のように Cool.net ドメインの登録管理会社，その登録日などがわかる。これらが，さらにこのドメインについて詳細に調査をしなければならなくなったときの手がかりとなる。

Domain Name : COOL.NET
Registrar : GO DADDY SOFTWARE, INC.
Whois Server : whois.godaddy.com
Referral URL : http : //registrar.godaddy.com
Name Server : PARK15.SECURESERVER.NET
Name Server : PARK16.SECURESERVER.NET
Status : REGISTRAR-LOCK
Updated Date : 06-dec-2005
Creation Date : 02-nov-1994
Expiration Date : 01-nov-2007

2）http : //www.internic.net/whois.html
InterNIC は，次のようなトップレベルドメインを管理している。.aero, .arpa, .biz, .cat, .com, .coop, .edu, .info, .int, .jobs, .mobi, .museum, .name, .net, .org, .pro, and .travel。トップレベルドメインの中で国名のトップレベルドメイン，たとえば，.jp などのサブドメインはそれぞれの国のネット管理組織が行っている。日本の場合は，JPNIC。

また，Toの送信先項目は，@の右側のドメインがなく，不完全であることも，注意深く見ればあまり知識がなくとも分かる。さらに，Subject項目は，返信記号のRe:だけであって，これも不完全である。このように不完全なメール情報を持つことから，これが正体不明のものであることは，ネットの知識があまりなくとも明らかになる。もちろん，メールの本文は，読み始めて1秒もたたないうちにゴミ箱へ入れたくなるものである。

1982年8月13日に公開されたRFC822（STANDARD FOR THE FORMAT OF ARPA[3] INTERNET TEXT MESSAGES）は，インターネット上のメッセージ交換の形式を定めるが，このRFCを詳細に読み，メッセージ形式の細部を知ることで偽かそうでないか判断できるのであろうか。RFC822は知らなくとも，メールが中継されたメールサーバの日付，時刻とそのサーバの名前などは読み取り，もし犯罪に使われたような疑いがあるなら，警察の生活安全課あるいはハイテク犯罪対策室へ知らせることができる程度の証拠は確保しておくのは，これからの一般人でも常識としなくてはいけないのかも知れない。

メールに関する中国の政治的状況

2006年5月29日のインターネット・ウォッチに掲載された「中国から日本のメールサーバ内のメールが受信不能に－メール受信に用いられるPOP3のポートを遮断した可能性」の記事によれば，どうやら中国大陸全土でこの状況が発生しているようだ。この原稿を書いている6月はじめでも同じ状況が続いているらしい。もちろん，直接の被害を受けるのは中国に出張している日本人ビジネスマンや日本企業の中国支店である。中国国内のファイアウォールがメール受信用のTCPポート110番（POP3）を遮断している可能性が高い。Google

3）ARPAは，ARPANet（the Defense department's Advanced Research Projects Agency Network）を指す。インターネット（the Internet）は，これの後継者である。したがって，政府機関，研究所，大学の間で情報を自由に共有することが目的であり，ほとんどの教育機関で当初セキュリティについての配慮はなかった。

の規制[4] や Wikipedia も検閲版を立ち上げ[5] るなど中国政府はさまざまな情報管理を行っている事実は広く知られている。

松山大学においても中国大陸から経済学部教員として採用された H 先生が，1993 年頃に「中国国内のメールは不自由（検閲されているという意味と受け取った）なので，松山大学のドメインでのメールを発行して欲しい」と個人的に依頼があった。この当時は，まだ松山大学内教員の全員にメールアドレスを発行していないときであった。

追加情報として，大衆・民衆が匿名性を利用して書き込みを行っている掲示板 2 ちゃんねるでは，6 月 8 日以降回復してきているとの情報もあるが，実勢のところは不明確でわからないことが多い。

はじめの POP3 の中国プロバイダーによる遮断は，日本と中国間の外交的取り引きあるいは政治的な問題の発生と関連することは，ほぼ間違いない。

詐欺の芸術 （the Art of deception）

ケビン・ミトニック（KM）は伝説のハッカーとして知られている。この本のカバーの裏には，サイバー・デスペラード，命知らずのならず者としてサイバーネットの世界を荒らしまわったこと，FBI 大規模捜査陣により逮捕される前後の話が，数多くの新聞記事や本や映画やドキュメンタリーを生み出したとして紹介されている。2000 年に連邦刑務所を出所した後，彼はセキュリティ犯罪対策の専門家としてのビジネスをはじめた。古臭い言葉だが「泥棒を捕まえるには泥棒をつかえ」の最新の意味づけをサイバースペース，インターネットで詳しく解説したのが，詐欺あるいは，いかさまの芸術である。舞台はサイ

4）IT メディアの 2006 年 6 月 8 日の記事による。http : //www.itmedia.co.jp/news/articles/0606/08/news020.html
「中国が検閲強化，Google.com へのアクセス不能に」

5）IT メディアの 2006 年 5 月 15 日の記事による。http : //www.itmedia.co.jp/news/articles/0605/15/news020.html
「検閲付きの中国版 Wikipedia 立ち上げ」。中国では，政府により百科事典サイト Wikipedia の閲覧が禁止されている。

バースペースであるが，手口は現実社会で数千年前から行われてきたいかさまと基本は全くかわっていないことが，KM により明かされる。

この本の構成で興味深いのは，前書きをスティーヴ・ウォズニアック[6] が書いていることである。その要点は，次のような人間の本能にも触れるようなものである。

・我々人間には，まわりの環境を探索したいという内的衝動が，生まれたときから備わっている。
・しかし，自分のまわりを自由に探索しようとすると何らかの障害に阻まれる。
・その結果として，まわりの世の中が，行動の規則とでも言うべきものを教えてくれることになる。
・科学者や技術者あるいは KM のような人間は，新しいことを発見したり，難しい問題を解決したりすることで，報酬を得るが，実は，この内的欲求にしたがい行動の規則を発見することに無上のスリルを感じる種類の人々である。

もうひとつ，KM によるハッカー人種の分類も挙げておく。それは，新しい技術に関心を持つものとそうでないものに分かれる。常に新しい技術に関心を持つものでも，単にハッカーツール[7] と呼ばれる，プログラムをダウンロード

6）世界で最初の普通のマニアが買える値段のパーソナル・コンピュータのハードウェアを設計し，ROM に整数型 BASIC を組み込み，ユーザがプログラミングの能力と忍耐さえあれば，自分用にカスタマイズしてホビーにも小規模なビジネスにも使えるようにしたという意味で最初のパソコンの開発者。

7）2000 年に愛媛県庁の庁内 LAN 設備構築の準備に際して，テストシステムのチェックを依頼された筆者は，庁内 LAN のメールサーバにウィルスを仕掛けることに成功した。これは，ルートキットと呼ばれる管理者権限を奪取する単純なスクリプト・キディー的なものですんでしまった。スクリプト・キディーは，システムにダウンロードしたプログラムをインストールする程度の能力があれば，簡単である。準備段階とはいえ，簡単なスクリプト・キディーの侵入を許してしまうシステムはセキュリティに問題があった。

してシステム破りに使うものたちを，スクリプト・キディーと呼ぶ。

コンピュータ犯罪の実例

KM が最初に取り上げるのは古典的な銀行口座への振込み詐欺の例である。それは，だいぶん昔のことになるが，ロサンジェルスのある銀行でリフキンという名の若者が起こした巧妙な詐欺事件である。この事件に関して，リフキン本人が何も喋っていないため，KM は公表された事実から事件を再構成している。

リフキンは，1978 年のある日のこと，ぶらりとその銀行の部外者立ち入り禁止のオンライン電信振込み室に入っていった。その厳重に警備された部屋では，毎日スタッフが 10 億ドル相当の送金や入金処理を行っていた。彼は，その銀行のメインコンピュータがダウンしたときのためのバックアップシステム開発を請け負った会社に勤めていた。その仕事の関係から，彼はその銀行での送金入金の仕組みや手順を知ることができた。銀行では，安全のために毎朝違う暗号コードを使い送金処理を行うことになっていた。しかし，スタッフたちは，毎日変わる暗号を忘れないようにと付箋紙にメモを取っていたのだ。彼は，ある日，バックアップシステムの動作チェックをするふりをしながら部屋の中を歩いて，その秘密の暗号コードを盗み読み記憶した。さて，午後 3 時に部屋をでると銀行のロビーの公衆電話のところまで行った。頭をすっかり切り替え別人に成りすまし，銀行のあるコンサルタントになりきって，電信振り込み室に電話をかけ，電話に出た女性のオペレータに「やあ，私は，コンサルタントのマイク・ハンセンだが」と言った。

彼女は，オフィス番号を尋ねた。それは，標準的な手続きにもとづくものだったので，彼はあらかじめ調べておいた「286」と答えた。

彼女は，つぎに「それでは，暗証コードをお願いします」と言った。

リフキンは，ドキドキしていることをさとられないように自然な調子で「4789」と答え，振込みの指示をはじめた。「1 千万ドル，そして 20 万ドルを

ちょうど」を彼があらかじめ口座を作っておいたスイスのある銀行に送金するように伝えた。

そうすると彼女は「わかりました，そのようにします。それでは，国際間オフィスで取り決めたナンバーをおっしゃってください」と言った。

リフキンは，あせった。この質問は彼が予期しないものだった。事前調査の手落ちだった。しかし，あわてたそぶりを出さず「いや，ちょっと待ってくれたまえ。確認して直ぐに電話するから」と電話を切った。今度は，また頭を切り替え，電信振込みの客になりすまし，別の部署に電話をして，電信室のオペレータについて苦情を言い，まんまとそのナンバーを教えてもらって再び電話をかけなおした。

彼女は，ナンバーを告げられて「Thanks」と答えたのだった。なんとも皮肉な Thanks だが，数日してリフキンはスイス銀行で８百万ドルを引き出し，ロシアマフィアを通してダイヤモンドに換え，それを腹に巻いて税関をパスしアメリカ国内に戻ることに成功した。銀行強盗としては，全米史上最高額になったのだが，銃はおろかコンピュータも使っていない。しかし，KM はこの事件が奇妙なことにギネスブックの史上最悪のコンピュータ犯罪として記録されていると書いている。

リフキンが用いた詐欺の手口は，ソーシャル・エンジニアリングと呼ばれるものである。KM はこの『詐欺の芸術』でさまざまなソーシャル・エンジニアリングについて解説をしているのである。この古典的な成りすましによる，振込み詐欺が，未だに日本国内では素人のような詐欺師集団によって行われ，それにひっかかる人々が多いことからもいつまでも通用する詐欺の芸術的な手法であることがわかる。

松山大学の学生に見られるハッキングの技術

松山大学は，2006 年 4 月に薬学部を開設したが，それまでは，経済学部，経営学部，人文学部，法学部の人文系 4 学部の大学である。また，コンピュー

タ・プログラミングなどの技術的な教育もあまりシステムプログラミングにまでは踏み込んで行われない。したがって，ハッキングの技術を持つ学生は少ないと思われた。しかし，スクリプト・キディーはいる。正確な日時は省略するが，人文学部に所属する当時 4 年生の男子学生が，ハッキング・ツール「John the Ripper password cracker[8]」を利用して教員などのパスワードを手に入れた事件があった。教員と学生の認証は，NIS を用いて行われていたが，この学生は，NIS の認証サーバにあるコマンドを発行し，暗号化されたパスワードファイルを手に入れたあと，それを当該ツールを利用して教員や学生のそれぞれのパスワードを復元した。

これは，ツールを使うだけで特にシステムプログラミングの必要も無いが，学内ネットワークの認証が NIS で行われていること，その認証サーバからパスワードファイルを入手することなどは，学内 LAN を運用管理するコンピュータ室の職員あるいはそこでアルバイトしている学生などから必要な情報をソーシャルエンジニアリングのテクニックで聞き出すのは簡単である。スクリプト・キディー達もそのツールを有効に使うためには，そのシステムに関する知識が必要でそのためにはソーシャルエンジニアリングが有効であることを示すひとつの例であった。

スクリプト・キディーのようにネットワークやコンピュータに関する経験や知識が浅いものでも利用できるような本がたくさん出版されていることも問題である。しかし，ネットワークやコンピュータのセキュリティを監視するものたちにとってもこれらの本は，侵入の手口を知るために欠かせない。両刃の剣である。パスワード破りについては，「Hacking　Exposed」（参考文献 2）などが詳しい解説を載せている。この本も，めまぐるしい変化がある IT 技術に対応するために毎年のように改訂版を出版している。それは，それだけの需要があることを示している。

8）http : //www.openwall.com/john/ で公開されている。

オペレーティング・システム（OS）のツールなどを製作するシステム・プログラミングでは，セキュリティの穴として「バッファ・オーバーフロー」が広く知られている。これは，プログラムのメモリ管理のバグでもあり，プログラマーの責任でもあるが，効率だけを考えられた初期のシステム・プログラムにはこの脆弱性を持つものが少なくなかった。松山大学内の学生ではなかったが，1994 年に松山大学で SunOS 上の Web サーバをインターネットに公開した後は，国外の大学からおそらく学生と思われる者が SunOS のこのタイプのセキュリティ・ホールを狙ってくるようになった。CVE（Common Vulnerabilities and Exposures）[9] としてこのタイプの脆弱性が公開されるようになったのは，1999 年からでそのリストの管理は，米国政府機関である U. S. Department of Homeland Security[10]（米国国土安全保障省）が行っている。

1996 年 11 月 8 日発行の Phrack49 に，その数ヶ月前から多発し始めたバッフォ・オーバーフローの論文が掲載された。その論文は‘Smashing The Stack For Fun and Profit’と名付けられていたが，ふざけた題名とは裏腹に内容は少しシステム・プログラミングの知識とアセンブラの知識があれば，適切なスタック処理をしていないプログラムに対して，リモートからでもローカルでも攻撃することが可能であることをわかりやすく解説し，かつ実践的である。

9）http : //www.cve.mitre.org/

10）DHS（Department of Homeland Security）は，災害時の危機管理，違法な入国の取り締まり，旅行者の安全確保など広い意味でのセキュリティを管理している。入国時に指紋審査などでセキュリティチェックを行っているが，筆者の指紋は，ある治療により非常に読み取りにくくなっている。たとえば，Lenovo 製のノート PC に組み込まれた指紋認証システムでは自分の指紋がどうしても認識されないために指紋認証方式が採用できない。パスワードフレーズをキー入力しなければならない。しかし，米国に入国時のチェックでは係官が何度かやり直して，筆者の指紋登録が成功した。このことから，個人的には DHS が採用しているシステムは，Lenovo などの民生用 PC と比較して相当に精度が高いものと推測する。しかしながら，出国時に筆者は，出国ゲートにある装置がなかなか自分の指紋を認証してくれないために相当に焦ってしまった。出国時と入国時の端末の精度に違いがあるのかどうかは，結局わからない。http : //www.dhs.gov/dhspublic/index.jsp

金子勇氏の講演「Winny の技術とその到達点」
平成 18 年 3 月 11 日土曜日

この Winny 製作者である金子勇氏による講演は，NPO 法人ソフトウェア技術者連盟の大阪セミナーの一環として行われた。当日は，テレビ報道関係者や新聞記者などマスコミがこの講演を取材するために集まっていた。新大阪駅近くにある東淀川区東中島一丁目の新大阪丸ビル新館の中にある会議室は，報道関係者が多数を占め，あとは主催の NPO 法人のスタッフで一般の人はほとんど見かけなかった。当日配付された資料によると，主催は，NPO 法人ソフトウェア技術者連盟（LSE）理事長 新井俊一，事務局 大阪市中央区内平野町 1-2-9。パンフレットの紹介文には「学術組織とは異なり，技術者の Professional Life をサポートすることが主な目的です。」とある。あと協賛団体は，CPSR/Japan[11]（社会的責任を考えるコンピュータ専門家の会　日本支部），国際大学グローバルコミュニケーションセンター（GLOCOM），特定非営利活動法人市民コンピュータコミュニケーション研究会（JCAFE）であった。

はじめに Winny 弁護団団長の弁護士 桂充弘氏より，Winny についての話があった。当日配付された資料を紹介する。

ファイル共有ソフト Winny の作者である金子勇氏は，Winny を開発提供した行為が著作権侵害をしたものを幇助したとして現在，刑事被告人となっております。

しかしながら，Winny は世界的にも極めて効率性の高い優れたファイル共有ソフトであり，また，金子氏は Winny を新しい技術開発を生み出すことを目的として開発しております。我々は，優れた技術を生み出すことが著作権法

11）http : //www.cpsr.org/act/global/japan/

の幇助となることは明らかに不当であるとして，弁護活動を続けております。

この Winny でありますが，Winny ネットワークを通じてダウンロードされたウイルスに感染したパソコンからの情報漏洩事件が相次いでおります。中には，あたかも Winny 自身がウイルスであるかのような報道が為されてることもあり，我々としては非常に問題といわざるを得ません。

我々は，Winny について，以下の事実を指摘したいと思います。

① Winny は効率の高い情報流通を可能にするファイル共有ソフトであり，大学の授業でも取り上げられることもある技術であり，今後のデジタル時代の技術的中核となる可能性を秘めております。Winny は世間で誤って考えられているような，情報漏洩のためのソフトでも，ウイルスのような違法なものでもありません。「Winny に感染した」という表現は誤りであります。

② Winny に情報を漏洩させる機能はありません。これらはいずれもウイルスを原因とするものであります。最近では Winny ネットワークを介さずに情報を漏洩させるタイプのウイルスが主流となりつつあります。つまり，ウイルスの感染の手法はユーザー心理や Windows の脆弱性を悪用したものであり，「Winny により情報漏洩した」という理解は誤りであります。

③ Winny でウイルス問題が発生したのは，平成 15 年 11 月 27 日に，京都府警が被告人に「今後，Winny の開発・公開はしない」旨の文書を提出させてから，3 ヶ月以上後のことで，被告人としてはウイルスの存在を予見できない状況でした。また，被告人はウイルス対策のアイデアはあるものの，刑事事件では検察官がバグ修正だけのアップデートを繰り返したことを違法視して主張していることから，今回のウイルス対策を取ることがさらなる幇助として問われかねない状況であり，このような状況では保釈取り消しや新たな幇助とされることを懸念せざるをえません。Winny の製作・公開の何が違法であるかを明らかにし，ウイルス対策やバグの解消であるアップデート版の公開がなんら違法でないことを検察・裁判所が明らかにしない限りウイルス対策は不可能であります。

④情報漏洩の問題は，本質的には心ないウイルス作者が強く非難されるべきであると思われます。現在は，被告人がウイルス対策をとれないために，ウイルス作者がより感染しやすいウイルスの製作を競うかのような様相となっております。この問題を解決するには，被告人が適切なウイルス対策をすることが必須であると考えておりますが，上記のとおり不可能な状況となっております。

⑤現在流通しているウイルスのほとんどは，極めて安易な感染方法が原因であり，自らウイルスファイルを実行しているのが現状です。これはセキュリティの知識に不足しているといわざるを得ません。特に捜査情報などの流出が絶対に許されない重要データを私物であるパソコンに保存していること自体，セキュリティ対策に対する意識欠如と言わざるを得ません。

⑥情報漏洩をもたらしているウイルスの多くは，ユーザーが複雑な手順でポートを開放することにより初めて情報漏洩が可能になるものです。ポートの開放等は金子氏は一切指示しておりません。自らポートを開放することの意味すら分からない者が，重大な情報を杜撰な管理をしていたことが最近の情報漏洩問題につながっています。

そもそも，我が国は IT 立国を目指して開発を進めているはずであります。世界最高峰のデジタル流通のインフラとなる力を秘めたソフトを，悪用の可能性があるだけで，警察の偏見や誤った功名心により違法視して取締りすることは，到底許されるものではありません。

現在でも， Winny の開発提供が，なぜ違法なのかという問題すら明らかになっていません。現在，刑事事件の萎縮的効果により，多くの P2P 技術の開発が中止を余儀なくされております。

このような， Winny の現状を十分ご理解ください。

以上

この弁護士による「Winnyについての御理解と御願い」と題された文書は，マスコミによる誤解，あるいは意図してWinnyに罪を着せようとしているものがあることを示唆するような表現も含んではいるが，弁護団として現状の問題を①から⑥に整理し，要領よくまとめてあり，大衆・民衆に理解しやすいものを目指して書かれたと思われる。

この①から⑥の中の問題点に触れる前に，金子氏の当日の講演の内容をまとめてみる。

金子氏による講演内容

この「Winnyの技術と当時の技術的到達点」という講演名からは，かなり技術的な詳細を開発者本人が語るのかと期待していたが，内容は，さほど詳細な技術解説は行われなかった。聴衆の大半がマスコミ関係者であったからかもしれない。金子氏は，Winnyの概要から始めた。そこでは，ファイル共有ソフトとしてのWinny1と分散型BBSとしてのWinny2の違いの強調から始めた。ここで，Winnyという名前をマスコミでしか聞いたことのない人々は，Winnyにはふたつのバージョンがあることを知る。おそらく会場の大半はそうであったのではないだろうか。資料によれば，P2Pファイル共有ソフトとして開発されたWinny1は2002年5月6日から2003年4月7日まで開発が続いている。分散型BBSとして強調されたWinny2が，現在多くの利用者により使われているが，Winny2も実はP2Pファイル共有機能を持っている。このあたりの技術詳細については，金子勇『Winnyの技術』アスキーにある。Winny2は，2003年5月5日（v2.0 β1）から2003年11月27日（v2.0 β7.1）まで開発が続いた。

P2Pについても，クライアントサーバ型のネットワークとの違いを一般的な教科書的な説明でしか行っていない。このあたりは，マスコミ一般向けの退屈な説明であったが，金子氏の几帳面な性格からしかたがない。続いて，分散型ファイル共有の必要性とその技術進化に伴うWinnyの製作背景の説明となっ

た。ファイル共有ソフトの世代別の比較として，第1世代のナップスター[12]，第2世代のナテラ，第3世代のフリーネット，Winnyの特徴をあげ，簡単な説明を加えた。音楽著作権問題に大きな影響を与え，猫がヘッドフォンをかけているナップスターのロゴは，またたくまに世界中に有名となったため，ナップスターはインターネットで音楽ファイルを交換・共有する仕掛けを作ったことでコンピュータマニアでなくとも認知度は高い。おそらく，ナップスターがネットで欲しいものがタダで手に入ると，大衆・民衆が喜んだ最初のソフトではないだろうか。金子氏は，技術者としての性格から，このようなほとんどの国で違法なネットの利用法を促進した，ファイル共有ソフトの社会的な責任については，講演では触れていない。あくまで，P2P技術の進化に限定して話を進めた。筆者の大学においても，Gnutella（ナテラ）[13]をある学生のグループが使用し，著作権で保護されたファイルを大量にダウンロードしている例が発見された事実がある。これは，隣の大学の学生たちと筆者の大学で学生が利用できる共同研究室内で秘密裏にしばらくの間，行われていたが，2000年頃はまだ学内の学生によるネットワーク利用の管理が甘く，発覚まで時間がかかってしまった。[14]

このあと，2ちゃんねるに大学名が登場するような音楽ファイル交換についての事件までが発生し，本学のネット管理者は通常の大学ではありえないほどの厳重なセキュリティ管理を始めた。

金子氏は，P2P技術の進化を技術論的な視点で解説していたが，その技術を利用する大衆・民衆の心理はまったく解析されていない。その心理のほとんどは，タダで欲しいものを手に入れるという単純なものである。その単純な動機を，現実化するための利用者にとっての技術の進化は，なんらかの歯止めがな

12）Napsterは，はじめショーン・ファニングによって音楽ファイルの共有を目的に作られた。はじめて公開されたのは，1999年の6月であった。
13）Gnutellaは，Nullsoft社のサーバから2000年の3月中旬からダウンロード可能になった。
14）この事件の詳細は，公表されていないが，共同研究室内での禁止されている炊事などが原因となって発覚したとの情報もある。

ければ加速し続けるのであろうか。現在，世界的に見て，というかインターネットの世界でこの言葉はおかしいのだが，最も利用されているファイル共有のネットワークを具体的にその名前をあげてみる。ネットワークは，インターネットがTCP/IPのプロトコルによって定義されるように，プロトコルによって定義される。その中のプロトコルのひとつとして，主にmp3フォーマットの音楽ファイル共有に使われているFastTrackがある。これは，FastTrackネットワークと呼ばれる。音楽だけでなく，映画やソフトウェアを共有するために使われているのは，eDonkeyネットワークである。その次に利用者の多いネットワークがナテラである。Winnyは，P2Pネットワークであるが，主に日本国内で有名になった。Winnyの開発は，日本人により日本国内で行われたが，Winny開発の動機は技術的に匿名性を実現させたFreenetの出現であったと開発者の金子氏は語る。

その重要な動機「技術的に完全な匿名性の実現」について少しここで解説する。Freenetは，イアン・クラークがエディンバラ大学で1999年に書いた論文「A Distributed, Decentralised Information Storage and Retrieval System（分散自立型による情報格納と検索システム）[15]」のインプリメンテーション（実装）として作られたので，Freenetの目指した匿名性についてはこの論文にそのアルゴリズムが書かれている。既存のP2P型システムに対する長所として，クラークは次のようなものをあげている。

・いかなる中央の管理や制御も必要としない
・匿名情報の公開と検索
・ポピュラー情報の動的複製
・要請による情報在所の移転

15）この論文は，著者がインターネットに公開した。たとえば，http : //citeseer.ist.psu.edu/clarke99distributed.html などからコピーを入手できる。

金子氏の匿名性について述べた言葉を『Winny の技術』32 ページから引用する。

ここでは，匿名性を情報の第一発信者がわからないという意味で使うことにします。新聞やラジオの番組でも情報提供者が匿名で発言することがありますが，これは新聞社や放送局が匿名を保障することによって成り立っています。

この部分を読めば，Winny の目指した匿名性の意味がよくわかる。さらに，クラークがあげている 4 つの長所と合わせて考えると，ノードのキー情報を管理するサーバなどを必要としないことや情報が格納されたノードを移転できることなどから，技術的に匿名性がさらに高くなる理由がわかる。

Freenet による匿名性の実現は，公開する情報を細かいブロックに断片化し，それぞれの中身を暗号化することによっている。Freenet ネットワークでは，公開された情報は，このような手法で周辺のノードに拡散されてゆく。情報の入手は，ネットワーク内に検索をかけ断片化されたブロックを集めてゆくが，このとき断片を受け取ったノードは情報の第一発信者から情報断片を受け取ったのかどうかは判定できない。最終的にすべての断片を収集し複合化したノードも情報の第一発信者が誰だったのか（どのノードだったのか）を知ることはできない。しかし，検索をかけ情報を入手するのはネットワークが大規模になると非常に困難となる。また，ネットワークの隅々まで情報をいきわたらせることもノードの数のべき乗に比例する。ネットワーク内の通信量の急激な増加と個々のノードのディスク使用量の急激な増加をまねいてしまう。非効率性の問題が Freenet にはある。[16)]

おそらく金子氏は，この Freenet の匿名性の技術を研究している段階で，情

16）Freenet は，開発途上であって，いまだ，バージョン 1.0 はでていない。ソースプログラムが Java で記述されていることも実験的なプログラムであることを示す。これに対して，Winny は，Windows 上の C＋＋で書かれた。

報の匿名性をネットワーク上で実現させるのは，情報を直接やり取りするのではなく，間接的にやりとりすることが本質的であると見抜いたようだ。[17] そこで，すでに Web 情報の効率的な配信と匿名性の確保に広く用いられているプロクシーサーバの技術を取り入れることにしたようだ。このプロクシーサーバーの技術は，Web サイトが急増していく中でまだ組織の管理する LAN からインターネットへの接続帯域がそれほど広くなかった時代に，組織外の Web サーバーへ，LAN 内の複数台のクライアントからの接続要求をプロクシーサーバで代理することで外部への接続要求を節約するという概念から生み出された。プロクシーサーバは代理を行う際，どのクライアントからの Web サーバへの要求であることを隠すことも可能である。また，同じ Web サーバへのアクセスは，プロクシーサーバにキャッシュされた情報を再送出することで元の Web サーバの代理を行うこともできる。

プロクシーサーバの匿名性と効率性は，Web 誕生後それほど時間を経ずに考え出されたものであるが，これをうまく Freenet の非効率性の解決に利用したのは金子氏のアイデアである。その結果生み出されたものが，Winny1 であると言えるだろう。Winny1 は，2002 年 4 月 1 日の開発宣言のあとその年の 5 月 6 日に最初のベータ版が公開され 12 月 30 日に正式版として公開された。この開発前から正式版までの期間の長さを考えると，開発者の情熱とシステム開発能力の高さ，さらには利用者や支援者の広がりも見逃せない。この結果として，100 万人とも言われるユーザの利用に耐える P2P システムが日本で開発され広がった。

Winny の Freenet の情報拡散方式との本質的な違いをもう一つだけ述べておくと，それは，情報を格納したファイルそのものを断片化し拡散するのではなく，ファイルすなわち情報の内容と所在を要約記録したキーを Winny ネットワーク内に拡散すること，さらに情報を持つファイルのキャッシュを Winny

17)『Winny の技術』のページ 41 にある，「Freenet の匿名技術の本質を考える」の章参照。

ネットワーク内の中継ノードに作ることである。このあたりの詳細は，『Winny の技術』の中で作者自身により解説されている。

1993 年から 1994 年にかけて，まだ Web 技術が広く日本では知られていなかった頃に松山大学で Web 技術に関する実験を繰り返していた筆者としては，当時を振り返って，Anonymous（匿名性）と Proxy server（プロクシーサーバ）をネットワークに実装する技術には魅力を感じていた。共同研究者のカナダ出身で Web よりも前の分散型情報システム・ゴファーでメールを使って情報源からファイルを入手する仕組みを開発したフレッド・ブレンマーと初期のプロクシーサーバを構築していたが，大学のインターネット接続帯域幅が狭いことを解消する目的と，学内の学生達によるインターネット接続でのプライバシー保護の目的もあった。匿名性については，1994 年の 7 月から運用をはじめた英語俳句メーリングリストでの投稿者の匿名性を保護し，俳句の本質の議論から離れた無用なネットでの諍いを鎮めるのも目的であった。不特定多数が参加するネットワークでの匿名性と情報の効率的な公開と検索についての研究は続けられているが，現実のインターネットでの利用では，匿名性の悪用あるいは著作権保護された情報の公開が絶えない。P2P ネットワークの利用は，これらが原因で起きた事件のために，P2P システムをインストールしているだけで違法視され，その利用は制限される。

もうひとつ，違法性とは別であるが，フリーライド（ただ乗り）の問題がある。これは，ゲーム理論や経済学に登場する「囚人のジレンマ」と関係することとなる P2P ネットワークの効率問題である。この問題について，金子氏は講演当日も「なぜ Winny をオープンソースにしなかったのか」の質問に対して次のように答えている。質問者は，オープンソースにすれば，Winny をある意味で攻撃している「Winny に対するウィルスへの対策処理」をすることができたのではないかという主旨である。開発者の金子氏自身も「その対策は簡単ですぐできるが，自分は刑事被告人となっておりプログラムの修正は禁じられている」と述べた。『Winny の技術』の中で，Winny の効率に関係する転送先

リンク数のコントロールコード部が狙われることが多いと書いている。アップロードを抑えて，ダウンロード優先にしフリーライドをしようとするユーザが，その目的に合わせて Winny を改造することを避ける意図である。

Winny に関連した事件

新聞報道などで，大衆・民衆に広く Winny の名前が知られるようになったのは，2003 年 11 月 28 日に「京都府警察本部ハイテク犯罪対策室と五条警察署が 27 日に著作権侵害の疑いで愛媛県松山市の無職男性（19 歳）と群馬県高崎市の自営業男性（41 歳）を逮捕したこと」である。しかし，P2P 技術に関心のあるものからみると，その翌日に「コンピュータ著作権協会（ACCS）により経緯詳細の説明」であった。そこでは，Winny の暗号化を解読し，被疑者の IP アドレスや身元を特定し，送信可能にしている著作物の同一性を ACCS が第三者的な立場で，告訴していた任天堂株式会社とハドソン株式会社とともに確認したと説明された。

この ACCS による解説が正しいとすれば，完全な匿名性が技術的に Winny では実現できていなかったことの証明になる。しかし，どのようにして，Winny のその不完全な部分を京都府警察本部ハイテク犯罪対策室は解読したのか，あるいはソーシャル・エンジニアリングの手法が用いられたのか，その操作や技術的な詳細が公開されていないために不明である。

2003 年 11 月の事件では，愛媛県松山市の 19 歳の男性が逮捕されたが，2006 年 3 月の金子氏の講演の前には，愛媛県警で警察官が捜査情報をしまっておいた私物の PC から情報流出が起きたとされる事件がニュースに流れた。この講演の前後の時期にも愛媛県警ハイテク犯罪対策室は，徹夜で Winny ネットワークでの流出経路を追っていたはずである。また，セキュリティをビジネスとする会社もボランティアとして，この愛媛県警の情報流出源とその経路を独自に調査していた。あるボランティアの人によれば，この講演が終わった時点で「Winny ネットワークの中でキャッシュとしても流出した愛媛県警情報は発見

できなかった」ということであった。このボランティアは，Winny ネットワークの技術的な仕組みを理解している一人であり，継続しての調査をお願いした。それから，しばらくして愛媛県警から部分的な調査結果が発表されたが，その時点でボランティアに問い合わせた結果は「2 次的な情報源しかわからない」ということであった。

『Winny の技術』には，P2P ネットワークに関する作者のオリジナルなアイデアが公開されている。好みの似たノードをクラスタ化するクラスタリングのアイデアは，講演でも作者のオリジナルアイデアであると自負していた。あと，それに P2P ネットワークの中で検索の問い合わせにノードのネットワークへのアクセス速度を基準とした上流，下流の方向性を持たせるアイデアを加えたのが Winny 成功の鍵であった。世間では日本独創のソフトウェアが少ないと思われているが，そうとも言えない。小説家が小学生の頃から文学に目覚め，自分の表現手段として文芸の道を歩み始めた結果であるとするなら，プログラムを書くことで小さい頃から自分のアイデアや思想を表現する道があってもよいわけで，現代日本では PC が普及し始めた 1980 年代前半にそのような芽吹きをはぐくむ環境ができはじめたのである。

しかしながら，国語の教育はいろいろ批判があってもほぼ一貫して存続しているが，プログラムで自己表現をするというような教育は今の日本に存在する余地は無く，将来もわからない。また，日本の若者に不幸であったのは，そのような性向の少年・少女をオタクの一言で類別してしまい，彼らの作り出したものをオルタナティブな文化として差別してしまったことである。

この原稿を脱稿する直前に，愛媛県警の情報流出について，6 月 16 日に県警から調査結果が発表された。流出した個人情報については，これまで約 4,400 人分としていたが，それに約 1,800 人分を追加修正した。自動車ナンバー自動読取装置（N システム）で収集した情報で流出したものについては約 60 万台

分とその数字を明らかにした。しかし，Winny ネットワーク内部での経路などの詳細はもちろん発表されていないために，Winny のシステムのバグを利用したウィルスなのかどうかなど P2P システムの技術的な問題点を追求するための材料を得ることはできなかった。

この 6 月 16 日の調査結果がおそらく今回の愛媛県警の情報流出の最終報告となるだろうが，得られたものは，はじめにあげた，ケビン・ミトニックのいう「ヒューマン・ファクター」だけということになってしまう。私物の PC に捜査情報を入れていた捜査 1 課の警部のミス，さらには，N システムの情報が捜査終了後も消去されていなかったことなど，これらはすべて人間のミスであって，いくら高額のセキュリティ・システムに投資をしていたと仮定しても，情報漏洩は避けられなかった。県警はシステムの再構築のために各方面にアドバイスを求めているのだろう。筆者のところにも県警から 6，7 人の関係者が訪ねて来て次期システムについての意見を聞かれた。しかし，現段階でのセキュリティ対策は，KDDI の顧客情報流出事件[18] が起きた後の KDDI の株主総会で代表取締役社長兼会長の小野寺正氏の次のような発言に要約される。

「当時としては対策を講じていたつもりだったが，結果として不十分だった。流出の可能性として，ホストコンピュータにつながるマシンは，通常のパソコンであり，HDD が存在し，外部メモリも装着できるものだった。これが要因の 1 つだ，と考えている。今年に入ってからは，HDD を備えない端末，いわゆるシンクライアントに置き換えている。また，入退場システムも当時は IC カードだったが，現在は指紋認証を導入した。セキュリティ対策は強化してきたが，もう一度全面的な見直しを始めたところ。今後も十分対応していきたい。一方，技術的，物理的な対策だけで良いのか。悪意があれば情報が持ち出されてしまう可能性はある。社員に対する教育など人的な面でも対応していく」

18）KDDI のホームページで，「お名前，ご住所，ご連絡先お電話番号：3,996,789 名様分」と発表している。http : //www.kddi.com/news/kddi_home/news_topics/2006/0613/index.html

まとめれば，

・社内 LAN に接続する端末は，ハードディスクや外部メモリのないシンクライアントのコンピュータにする
・ID やパスワードだけの管理は不十分で，生体認証をもちいる
・人的な面での対策

となる。

マスコミ報道に見る愛媛県内ネット通販サイトでの情報流出事件を分析

平成 18 年 6 月 28 日の午後，インターネット通販サイト「極選！e－ひめ市場」において顧客のメールアドレスが漏れるという事件が発生した。このインターネット通販サイトは，南海放送，松山市内のホームページ制作会社，および愛媛県中小企業団体中央会によって共同運営されている。そのインターネット通販サイトのアドレスは，http : //himeichi.com/となっている。この himeichi.com のドメイン名登録を調べると，GMO インターネットの「ドメイン取るならお名前．COM」サービスを利用して，そのドメイン名 himeichi.com が登録されたものであることがわかる。その登録情報は，インターネットに次のように公開されている。

Domain Handle :
Domain Name : himeichi.com
Created On : 2005-05-18 19 : 13 : 56.0
Last Updated On : 2006-05-11 11 : 21 : 44.0
Expiration Date : 2007-05-18 10 : 11 : 33.0
Status : ACTIVE
Registrant Name : Fukuizumi Hideto
Registrant Organization : Hideto Fukuizumi

Registrant Street1 : 1-1-32 Yugun

Registrant Street2 :

Registrant City : Matsuyama

Registrant State : Ehime

Registrant Postal Code : 790-0031

Registrant Country : JP

Registrant Phone : 089-921-3132

Registrant Fax : 089-932-3221

Registrant Email : info@netcrew.co.jp

Admin Name : Fukuizumi Hideto

Admin Organization : Hideto Fukuizumi

Admin Street1 : 1-1-32 Yugun

Admin Street2 :

Admin City : Matsuyama

Admin State : Ehime

Admin Postal Code : 790-0031

Admin Country : JP

Admin Phone : 089-921-3132

Admin Fax : 089-932-3221

Admin Email : webmaster@himeichi.com

Billing Name : Fukuizumi Hideto

Billing Organization : Hideto Fukuizumi

Billing Street1 : 1-1-32 Yugun

Billing Street2 :

Billing City : Matsuyama

Billing State : Ehime

Billing Postal Code : 790-0031

Billing Country : JP

Billing Phone : 089-921-3132

Billing Fax : 089-932-3221

Billing Email : webmaster@himeichi.com

Tech Name : Fukuizumi Hideto

Tech Organization : Hideto Fukuizumi

Tech Street1 : 1-1-32 Yugun

Tech Street2 :

Tech City : Matsuyama

Tech State : Ehime

Tech Postal Code : 790-0031

Tech Country : JP

Tech Phone : 089-921-3132

Tech Fax : 089-932-3221

Tech Email : webmaster@himeichi.com

Name Server : ns1.netcrew.jp

Name Server : ns2.netcrew.jp

このドメイン登録情報から，himeichi.com サイトの管理者ならびに組織名が明らかとなる。インターネット通販サイト「極選！e－ひめ市場」の利用者であれば，誰でもインターネットに公開された情報からここまで知ることは可能である。この公開された情報の中から通販サイト管理者に直接電話をして情報を確かめることも可能となっている。しかし，ここまで自力で調べることができる一般のユーザは少ないのかもしれない。ネット通販の利用率が高くなればなるほど，ユーザへのネット基礎知識普及の必要性が高くなっている。

同月 29 日に通販サイト共同運営者のひとりである南海放送が記者会見を行った。それに対するマスコミの報道の様子を調べると次のようになる。29

日夕方の地元テレビ局のニュース報道とその時間帯は，RNB が 18 時 46 分から 1 分間，EAT が 18 時 20 分から 1 分間，ITV が 18 時 46 分から 1 分間。その内，EAT は，3 項目目，RNB と ITV は 1 項目目であった。ただし，NHK と EBC は放送しなかった。翌日 30 日の朝刊には，地元の愛媛新聞の他，中央紙の地方版で，朝日新聞，読売新聞，産経新聞，毎日新聞がそれぞれ 2 段から 8 段組記事で報道した。これらの報道記事によると，複数の顧客メールアドレス（X 人分）が誤って，別の顧客（Y 人分）に送信されたことが分かる。X と Y は，いくらなのだろうか。愛媛新聞によると，X＝15，Y＝19。ただし，X ＝ X1 ＋ X2 で，6 月 28 日に X1 ＝ 14，5 月 10 日に X2 ＝ 1 であることが，詳細に読めば分かる記事となっている。朝日新聞によると，X ＝ 15 で，X ＝ X1 ＋ X2 で，その X1 と X2 の日付と人数は，愛媛新聞と同じである。Y については，Y ＝ 19 と記事の末尾で触れている。読売新聞は，X ＝ 15，Y ＝ 19 で，X ＝ X1 ＋ X2 であるが，X1 と X2 の日付は愛媛新聞と同じであると公開したが，X1 と X2 の人数は公開していない。産経新聞は，Y ＝ 19，X ＝ 15 とし，X ＝ X1 ＋ X2 の X1 と X2 の日付と人数も公開している。ただし，X2 については，5 月とだけしか書いていない。毎日新聞は，他社の記事見出しが「メールアドレス 15 人分誤送信」とあるのに，「メールアドレス 14 人漏えい」となっている。毎日新聞は，X ＝ 14 と報道したのかと思い詳しく読めば，X ＝ X1 ＋ X2 で日付と人数は他社と同じだと分かった。なぜ見出しで 14 人となったのかと，もう一度記事を最初から詳しく読むと，「注文確認メールを誤って第三者に送り，注文主 14 人のメールアドレスが漏えいしたと発表した」とあるため，南海放送が記者会見で 14 人と発表したことを，そのまま記事にしたようである。この毎日新聞だけは署名記事となっている。

これらのマスコミ報道を分析すると，X と Y のどちらに主眼が置かれているかが分かる。もちろん見出しとなった X 人分である。Y が流出先人数で，X がミスで漏らされたメールアドレスの件数である。過去に起きた KDDI 株式会社のインターネット接続サービス DION の個人情報流出では，顧客約 400 万件

の情報が流出している。この事件と比較すると，X は 20 万分の 1 以下であり，流出数から見ればほとんど無視される規模なのかも知れない。これが NHK と EBC テレビ放送ではニュースとならなかった理由かもしれない。また，KDDI の流出事件では，X 人分の情報がどこまでどこへ流出したのか，報道発表の内容では明らかでないが，南海放送のネット通販では Y 人分のアドレスの範囲にしか流出していない。このネット通販の誤送信は，X と Y のアドレス集合内だけの限定された X アドレス情報が Y アドレス集合へ流れた事件となる。また，X と Y はどちらも himeichi.com の利用者である。5 月 20 日の Y への流出は，X1 ＝ 1 であったので Y が反応しなかったが，6 月 28 日は，X2 ＝ 14 であったために，Y がそのアドレス情報の多さ（といっても 14 であるが）に反応して，運営者に送信ミスの指摘があったのであろうか。ともかく全国的にマスコミで報道された情報流出事件とはまったく漏えいの性質が異なっている。

注文確認のメール送信は，コンピュータでなく人間の手によるものであったようで，原因はまったくのヒューマン・エラーであり，それはオペレータの単純なメール取り扱いの不注意であったことが分かった。メールの宛先として，‘To : ’に記述するか‘Bcc : ’に記述するかといったことで間違いがあったような記事が見られたが，それは間違いの本質ではない。注文確認メールの処理手順が，ホームページ管理会社で守られなかっただけのことである。

しかし，セキュリティ対策については，抽象的な対策議論で終わり，その結果としての具体的な対策方法で何かが抜け落ちていることが多いことに気が付く。その理由は，コンピュータセキュリティ責任者が，具体的な対策を考えるとき参考とすべきものがないことである。現代の IT 社会でめまぐるしく変化する情報環境の中で自分がどこに位置しているのか，それを知るためには現実との接点－システムあるいはプログラム－あるいは，その歴史的な過去を学ばなければならない。このために「コンピュータセキュリティ史」の研究が，いま必要となっている。

「セキュリティ史」への提案

セキュリティの研究を遂行するには，その歴史的過去に通ずることが重要である。近代日本を代表する数学者である高木貞治（1875－1960）は『近世数学史談』共立全書，昭和8年10月18日初版の附録1にある「回顧と展望」の中で1900年にゲッチンゲン大学に留学したときクラインの講義を聴講して感動したエピソードを述べている。高木貞治によれば，クラインは「三つの大きなA」ということを言ったそうだ。それは，19世紀に数学が，Arithmetic, Algebra, Analysis，という「三つの大きな花文字のA」に再編成されたことを指す。クラインは，「何でも具体的な表現をもとめた」。しかし，高木貞治は，今は「唯一つの小さなa，即ちabstract」になったと「回顧と展望」の中で述べた。クラインが「空虚な一般論，leere Allgemeinhelt」というとき，彼は「浅薄無用な一般論を指弾した」のである。

数学に比べれば，具体的な計算機が生まれてからの歴史がはるかに短いコンピュータセキュリティの研究は，IT社会の制度的な仕組みが大衆・民衆の中に根付くためには，空虚な一般論や抽象的な観念論でセキュリティ問題を扱ってはならない。より具体的なシステムあるいはプログラムでセキュリティを表現しなければならないと考える。コンピュータ・システムは人間の手によって作られた具体的なものであることを忘れてはいけない。コンピュータ・プログラムも具体的なハードウェアで動いている具体的なものであるから。

参 考 文 献

1）Kevin D. Mitnick & William L. Simon, The Art of Deception, Wiley publishing Inc., Indianapolis, 2002
2）Scambray, McClure, Kurtz, Hacking Exposed, Osborne/McGraw-Hill, 2006
3）金子勇，「Winnyの技術」，アスキー，2005
4）インターネット・ウォッチ，http : //internet.watch.impress.co.jp/
5）UNYUN,「ハッカー・プログラミング大全」，Shadow Penguin Security 東京，2001
6）高木貞治，「近世数学史談」，共立全書，昭和8年10月18日初版第1刷