ネット社会を安全に暮らす

―平成二六年度　懸賞論文論文集―

ネット社会を安全に暮らす

―平成二六年度　懸賞論文論文集―

論文集「ネット社会を安全に暮らす」の発刊にあたって

公益財団法人　公共政策調査会
理事長　片桐　裕

私ども公共政策調査会は、昭和六一年の設立以来、公共の安全の視点から広く内外の諸問題を研究し、関連情報の収集、整理及び分析を行うとともに、これらの成果の普及、政策提言等の事業を行ってまいりました。

国際情勢、国内の政治、経済、社会などの情勢が大きく変化する中にあって、会員各企業をはじめ関係の方々からの終始変わらぬ暖かいご理解、ご協力の下に、着実にその事業活動を展開してまいりましたが、平成九年度には設立一〇周年記念事業の一環として懸賞論文を募集しました。

この事業は、各方面から好評を得たこともあり、その後も毎年継続して実施してまいりましたが、平成二六年度も、警察庁、読売新聞社、（独法）情報処理推進機構のご後援、さらに（公財）日工組社会安全財団のご助成の下に、警察大学校警察政策研究センターとの共催で、『ネット社会を安全に暮らす』をテーマに、第一八回目の懸賞論文を募集することとしました。

情報化の推進は、社会全体に大きな利便をもたらし、インターネットは、多くの国民にとって、日常生活、教育そしてビジネス等、様々な分野においてもはや欠くことのできないものとなっています。しかし、他方で、違法・有害情報の氾濫、不法プログラムや不正アクセス等による情報の流出、また、最近では、インターネット・バンキングからの不正送金など、インターネットのもたらす様々な危険についても多く

の指摘がなされているところです。また、子供たちに対する家庭、教育機関におけるネット・情報教育も大きな課題となっています。

こうした認識の下に、当財団でも、ネット社会を安全に暮らすために、関係者はじめ社会が何をすべきか、何かできるのかという観点から、国民各層からさまざまな視点・切り口からの具体的提言を求めましたところ、これに対し、各世代・各方面の方々から四二編の応募がありました。

応募いただきました各論文について、論文選考委員会において真剣な議論、厳正な審査が行われた結果、今回は残念ながら最優秀作品の該当はありませんでしたが、五編が受賞作品に選ばれました。その中で、高校生及び女子大生に対する携帯電話等の利用に関する意識調査を自ら実施し、その結果を踏まえ、ネットトラブル、特にわいせつな画像のネット上への流出防止法を提言した上野貴弘氏、自身の担当する国語科の授業での標語創作活動を通じて生徒へのメール、ネットを利用する上での「情報モラル」教育の実践をまとめた久原弘氏、そして、子どもの安全を守る観点から現状の対策とその課題を考察され、五つの提言をまとめた竹中利衣氏の三論文が優秀賞として選ばれました。いずれの作品もネット社会を安全に暮らす上での参考になるものと思われます。

本論文集は、紙幅等の都合により受賞論文を含む二〇編に限定しておりますが、いずれの応募作品も、真摯にこの問題に取り組もうとする意欲にあふれた力作でした。

この論文集が広く各方面で活用されますようお願いいたしますとともに、論文集発刊を契機に、ネット社会を安全に暮らすための取組みが幅広い分野でなされていくことを期待いたします。

結びに、この事業の実施にご協力いただいた関係各位と応募者の方々に改めて深く感謝を申し上げ、発刊に当たってのご挨拶といたします。

平成二七年二月

懸賞論文受賞者記念撮影（平成27年1月19日）

主催者代表挨拶
（公財）公共政策調査会　理事長　片桐　裕

選考委員代表挨拶
小宮　信夫　立正大学文学部教授

来賓挨拶
岡部　正勝　警察庁長官官房参事官

優秀賞・読売新聞社賞受賞
久原　弘 氏

受賞者代表挨拶
久原　弘 氏

優秀賞・読売新聞社賞受賞
竹中　利衣 氏

優秀賞・読売新聞社賞受賞
上野　貴弘 氏

目 次

この論文集に掲載した原稿は、応募者各人の個人的なご意見を紹介したものであり、必ずしも公益財団法人公共政策調査会等の主催者及び後援各団体の見解を示すものではありません。

また、個々の論文における用字、用語、数字等については基本的に応募者の記述を尊重しています。

〔優秀賞〕

ネット社会を安全に暮らす
～わいせつ画像の流出を防ぐためにできること～

警察官（北海道警察）
上野　貴弘（36）

はじめに

本論文では、高校生等に対し携帯電話等の利用に関する意識調査を実施し、その結果から、ネットトラブル、特にわいせつな画像のネット上への流出を防止するための方法について論じる。

昨年発生した、三鷹市におけるストーカー殺人事件は世間に衝撃を与えた。犯人が女子高生のプライベー

トポルノ写真をネット上に流出させ、被害者に対し復讐をするという、いわゆる「リベンジポルノ」を実践したからだ。

ネット上に流出した画像を完全に消すことは不可能であり、ひとたび流出被害にあった人は、一生消えない傷を背負うことになる。

携帯電話等の技術の進歩はめざましく、今や簡単に写真や動画をネットに公開することが可能だ。よって、地方においてもネット環境さえあれば、都市と同じような事件は起こり得る。

筆者の住む農村地方でも、過去に高校生の男女が自らの画像を撮影して交換し、男子生徒が面白半分にネットへ流出させ、女子生徒を被害に遭わせるという問題が発生した。

このように、善悪の判断力が未熟な高校生にとっては、ごく身近なツールとなっている携帯電話等の危険性を指導教育しなければ、自らの個人情報や画像が流出し、一生を棒に振る可能性もある。

そこで本論文では、高校生などの若年層について、わいせつ画像流出による被害を防止するため、以下の方法で現状を把握し、結果の分析から防止策を検討することとしたい。

第一に、ネット上へのわいせつ画像流出に対する、現在の法規制を明らかにする。

第二に、高校生、大学生の携帯電話等利用時の意識をさぐるためアンケートを実施し、問題点を究明し、被害に遭う原因を考察する。

第三に、高校生にネットトラブル防止の講話を行い、実施後のアンケート結果から、どのような講話に実効性があるのかを検証する。

第四に、女子大学生との討論を通じ、若年層における人間関係について深く掘り下げ、ネットトラブルとその防止法について検討する。

最後に、被害に遭う人を一人でも減らし、ネット社会を安全に暮らすために、各関係機関による連携の必要性を提言したい。

第一章　わいせつ画像流出に対する法規制の現状と問題点

第一節　わいせつ画像流出に対する法規制の現状

自分のわいせつ画像、動画をネット上に公開された場合、公開した人間に対し、現状ではどのような法規制があるのか。

一　児童買春・児童ポルノに係る行為等の処罰及び児童の保護等に関する法律

被写体が一八歳未満の場合、その画像等が、性欲を興奮させ又は刺激するものであれば、児童ポルノ法の公然陳列罪（同法七条四号）に当たる。

この法は児童の権利を擁護する目的のため、必ずしも性器が写り込んでいなくても、性欲を興奮させ又は刺激するものであれば成立し得る。そのため、一八歳未満の者が被害者であれば、適用範囲は比較的広いといえる。

警察庁発表資料によると、平成二五年中の児童ポルノ事案の検挙件数は一、六四四件で過去最高を記録

し、大部分（八三・六％）にネットが関係していた（注1）。

二　わいせつ物公然陳列罪（刑法一七五条一項）

この法律では、被写体の年齢は問わないが、本法でいう、「わいせつ」とは、「いたずらに性欲を興奮又は刺激せしめ、かつ普通人の正常な性的羞恥心を害し、善良な性的道義に反する」ことが必要とされ、性器が写っている等の直接的なものがなければ、適用にならない可能性もある。

三　ストーカー行為等の規制等に関する法律

この法では「その名誉を害する事項を告げ、又はその知り得る状態に置くこと」（同法二条七号）や、「その性的羞恥心を害する事項を告げ若しくはその知り得る状態に置き、又はその性的羞恥心を害する文書、図画その他の物を送付し若しくはその知り得る状態に置くこと」（同法二条八号）が規制されている。

しかし、その行為が、特定の者に対する恋愛感情その他の好意の感情又はそれが満たされなかったことに対する怨恨の感情を充足する目的でなされる必要がある（注2）。

四　名誉毀損罪（刑法二三〇条一項）

自分にかかるわいせつ画像等がネット上に公開されることにより、社会的評価を低下させられたとして、名誉毀損罪が成立する可能性がある（注3）。

第二節　わいせつ画像削除の困難さ

ネット上に自分のわいせつ画像等が公開された場合、被害者は公開された画像等を早く削除したいと考

えるだろう。

削除は、その画像が公開されているサイトの管理者、サイト運営会社、サーバ管理会社等に依頼していくことになるが、削除するかはサイト管理者等の判断となり、また海外サイトの場合、日本の法律を適用することが困難な場合が多く、語学力の面などでハードルはさらに高くなる。

また、メールやＬＩＮＥ等で拡散された場合、直接データを持つ当人に削除を依頼していくしかない（注4）。

流出させた者の中には、リベンジポルノ（注5）のように犯罪と判っていても、自分の欲求を満たすため敢えて公開させる者もおり、流出した被害者は、見えない誹謗中傷に一生悩まされる。

警察が犯人を検挙しても画像が消去されるわけではなく、画像の回収削除は弁護士等と相談し自ら行う必要がある。

すなわち、一旦ネット上に画像が流出すると、全ての画像を削除することは事実上不可能であるから、根本的にはわいせつな画像を撮らない、撮らせないことが最大の被害防止対策なのである。

第二章　高校生等の携帯電話等利用の意識調査

第一節　調査概要

一　調査目的

現代の高校生、大学生における、携帯電話等でのネット利用意識について明らかにするためアンケート調査を実施した。

二　調査対象

高校生（一年～三年）　一、〇三五人
（内訳：地方八二四人　都市部　二一一人）
大学生（女子）（一年～四年）　二八六人
　合計　一、三二一人

三　調査方法・調査期間・回収率

アンケート調査。アンケート用紙を各校の教員から学生・生徒に配布、その場で回収（回収率一〇〇％）。
平成二六年七月四日から二一日までの期間。

第二節　調査結果と考察

一　ＳＮＳ利用はＬＩＮＥが八割、Twitterが六割、

㈠　携帯電話等所持の実態

携帯電話等の所持率は九六％に上る。

㈡　ＳＮＳ等の利用実態

利用しているＳＮＳ等は、ＬＩＮＥが最も多く（八二％）、次いでTwitter（六〇％）が続く。

ＬＩＮＥはメール機能を代替している無料アプリであるが、複数の人と同時にメールのやり取りが可能という利点がある。写真の送付もできるため、わいせつ画像の要求、送信はＬＩＮＥでも可能である。

㈢　ネット上のみでつながった人数

ネット上のみの知り合いがいると答えたのは三八一人で、全体の二九％になる。これは筆者の予想よりも少ない（表４）。

また、知り合いの人数は三八一人のうち、五人以下は二九％、六人から一〇人は一五％で、一〇人以下の層が四四％を占めた。継続してつながっている知り合いの人数は、一人から五人で三〇％、六人から一〇人

表１　アンケート調査実施人数内訳表

単位：人

区　分	高校							大学生
	地方						都市部	
	A高	B高	C高	D高	E高	F高	G高	
男	57	40	29	41	43	201	118	0
女	30	52	24	38	36	233	93	286
合計	87	92	53	79	79	434	211	286
合計	1035							
全合計	1321							

は八％で、いないという人も三四％いた（図2図3）。

知り合いが五〇〇人以上いるのは、現実的にはオンラインゲームを同時に行っている人や有名人などのTwitterフォロー数を友人と定義していると考えられる。

㈣　ネット上のみの知り合いとつながった方法

以上から、本アンケート対象の高校生等は、ネット上のみの知り合いの数もごく少数か、全くいないかが多数を占め、つながった方法も「友達からの紹介で出会う」が少数ながらも存在するなど、閉じられた範囲で行われているものと、現実世界で知っている人同士でつながっている状態があるとわかった。

ネット上のみの知り合いの多さがトラブルの元だと想定し、さらにＳＮＳの利用により交友関係がどんどん広がれば危険度も増すと考えていたが、わずか数名の知り合いだけならば、昔も文通などで会ったことのない友達がいたのと同じで、現代の高校生等も大多数はごく健全な交友関係を築いているものと考えられる。

二　トラブルを回避するための意識

㈠　家庭でのルール（高校生のみ）

㈡　フィルタリング設定状況（高校生のみ）

家庭で携帯電話使用に関するルールがあるのは二〇％、ないのは七三％である（表6）。ルールは、料金や使用時間に関するものが多い（表7）。

表２　携帯電話等を持っているか

単位:人

持っている	1263	96%
持っていない	58	4%
合計	1321	100%

表３　どんな SNS 等を利用しているか(複数回答)

単位:人

自分のブログ	48	4%
Facebook	334	25%
Twitter	796	60%
LINE	1087	82%
mixi	69	5%
google+	238	18%
(オンライン)ゲーム	349	26%
その他	34	3%
SNSはやっていない	111	8%
無回答	64	5%
回答数	1321	

※　% は、母数（1321）に対する割合。

図１　どんな SNS 等を利用しているか（複数回答）

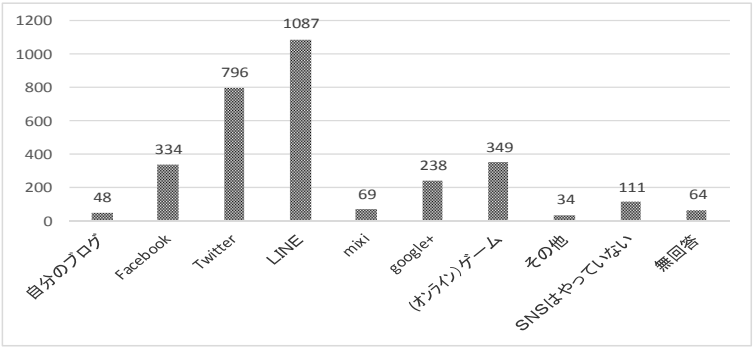


表４　ネット上のみでつながった知り合いがいる

単位:人

いる	381	29%
いない	848	64%
無回答	92	7%
合計	1321	100%

図２　ネット上で知り合った人数

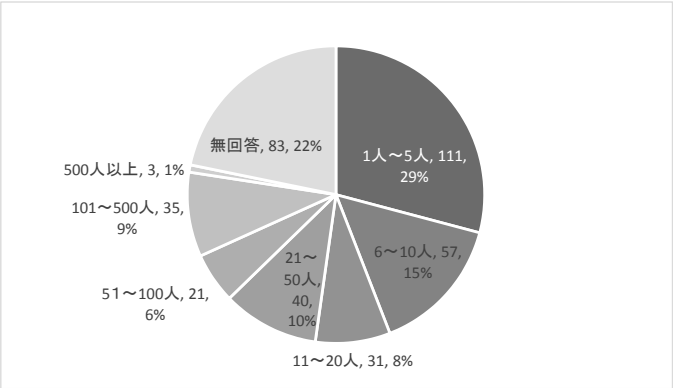
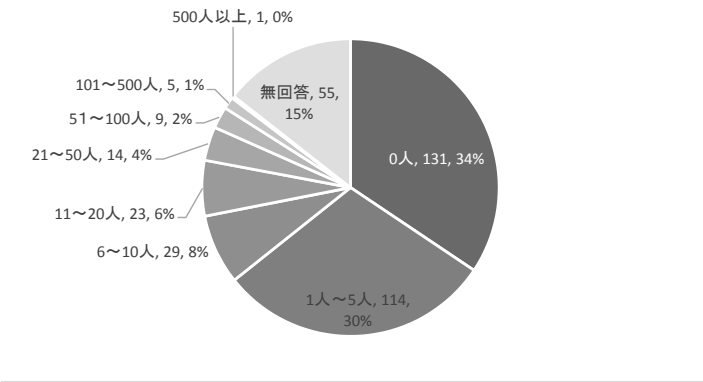


図３　ネット上の知り合いと継続してつながっている人数



フィルタリング（注6）は、「設定している」が三八％であるが、「していない・解除」は三五％だった。さらに、「わからない」が一七％おり、全く意識がない人もいることがわかった（表８）。

総務省が平成二五年に実施したアンケートでは、家庭でネット上のリスクについて話し合いをしている人が、よりネットリテラシーが高い（注7）というデータもあり、家庭でのルールやフィルタリング設定が子どもを守る上で重要である。

㈢　ネット上へ個人情報を公開する際の意識

ＳＮＳ等において個人情報を公開する際には何らかの注意を払っている人が大多数であり、主に「自分の個人情報を公開する」ことに気をつけていることが多いとわかった（表９）が、本来なら全ての項目を選択するくらい高い意識が必要である。

一方で、「特に気をつけていることはない」人が一九％いた。

今やネット上のあらゆる情報を組み合わせれば、個人を特定することは容易である。万が一、女性が顔写真を公開し、そこに目をつけた下心ある男性が、住所を特定しストーカー化すると新たな被害につながりかねず、個人情報の公開には十分注意しなくてはならない。

表５　ネット上の知り合いとつながった方法（複数回答）

単位:人

出会い系サイト	5	1%
Facebook	28	7%
Twitter	243	64%
LINE	123	32%
mixi	22	6%
google+	11	3%
(ｵﾝﾗｲﾝ) ゲーム	67	18%
友達などから直接紹介された	47	12%
その他	46	12%
無回答	10	3%
回答数	381	

※　％は、母数（381）に対する割合。

図４　ネット上の知り合いとつながった方法（複数回答）

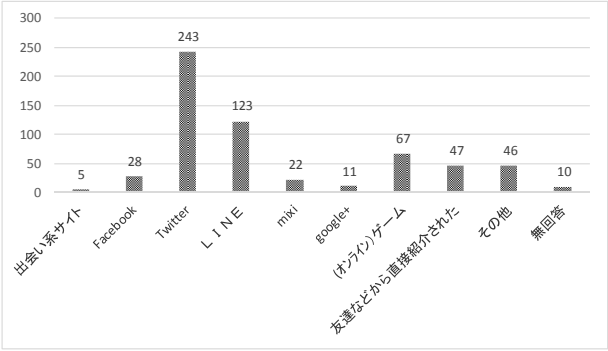


表６　家庭での携帯電話等の利用についてルールの有無

単位：人

ルールがある	205	20%
ルールはない	758	73%
無回答	72	7%
合計	1035	100%

表７　具体的な家庭でのルール（自由回答）

単位：人

利用料金の上限を決めている	58	28%
利用する時間を決めている	57	28%
利用する場所を決めている	9	4%
サイトの使用を禁止、利用内容を決めている	29	14%
守るべき利用マナーを決めている	43	21%
その他	3	1%
無回答	6	3%
合計	205	100%

表８　フィルタリング設定状況

単位：人

設定している	391	38%
はじめからしていない	292	28%
はじめはしていたが、途中で解除した	76	7%
インターネットが使えない設定になっている	17	2%
わからない	181	17%
無回答	78	8%
合計	1035	100%

㈣　巻き込まれたことのあるトラブルの種類

表一〇により、実際に「トラブルに巻き込まれたことがない」人が七二％であり、筆者の予想より多く安心できる数字である。

最近問題の、乗っ取られたアカウントからメールが来た人が二八％いた（表11）。万が一相手側の乗っ取りがわからなかった場合、連絡元の表示は友人となっており、もしわいせつ画像の要求をされた場合、友人だからと安心して送信してしまう場合もあるかも知れず、危険である。

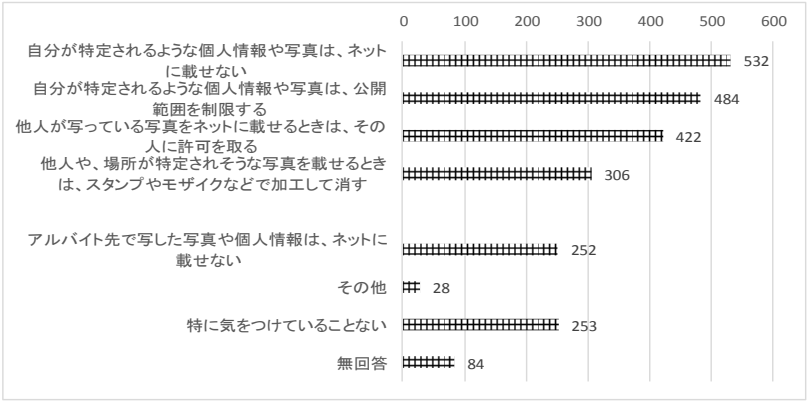
表９　ネットへの情報公開で気をつけていること（複数回答）

単位：人

自分が特定されるような個人情報や写真は、ネットに載せない	532	40%
自分が特定されるような個人情報や写真は、公開範囲を制限する	484	37%
他人が写っている写真をネットに載せるときは、その人に許可を取る	422	32%
他人や、場所が特定されそうな写真を載せるときは、スタンプやモザイクなどで加工して消す	306	23%
アルバイト先で写した写真や個人情報は、ネットに載せない	252	19%
その他	28	2%
特に気をつけていることない	253	19%
無回答	84	6%
回答数	1321	

※　％は、母数（1321）に対する割合。

図５　ネットへの情報公開で気をつけていること（複数回答）



㈤　ネットトラブルの相談先

トラブルを相談した、またはもしトラブルになった場合相談する人の候補は、友達五二％、家族四九％が多かった（表12）。

しかし、「だれにも相談しない」が一〇％いた。もしわいせつ画像を要求され困っていても、誰にも相談せず抱え込んで、結局送ってしまう人がいるかもしれない。

内容がデリケートな問題は友人や家族には言えないこともある。表一二では、警察に相談する人が八％と少なく、他の機関、特に政府系の機関に相談する人はほとんどない。各機関に窓口があって、相談がどこでも可能だということをより積極的に広報すべきだ。

第三節　わいせつ画像を要求されたことがある人の特徴

一　わいせつ画像要求、公開の違法性の認識

わいせつ画像を要求し撮影させたり、それをネットに公開したりすることが違法であることを知っている人は七九％であり、知らない人の二〇％を大きく上回っている（表13）。

二　わいせつ画像要求、公開の違法性の知識をどこで得たか

「わいせつ画像の要求、製造、ネットへの公開は犯罪になり得る」ことをどうやって知ったかを記述式で回答し、筆者がカテゴリー化して集計した（表14）。

ニュース、テレビが四五％を占めているが、これは三鷹の事件が放送されたことにより、世間に浸透し

15　ネット社会を安全に暮らす

表10　ネット上のトラブルに巻き込まれたことがあるか

単位：人

ネット上のトラブルに巻き込まれたことがある	266	20%
ネット上のトラブルに巻き込まれたことがない	950	72%
無回答	105	8%
合計	1321	100%

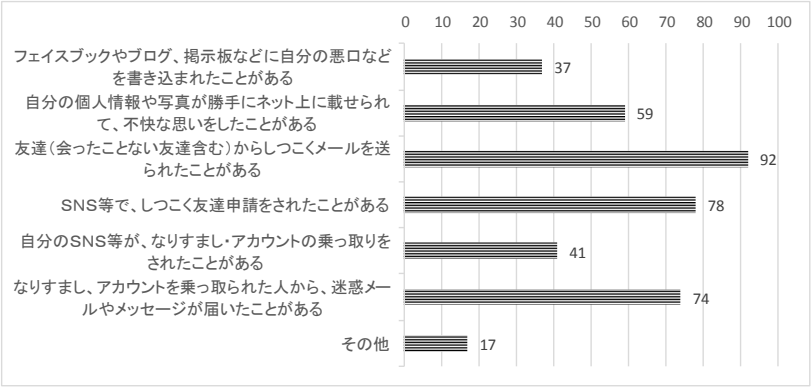
表11　巻き込まれたことのあるネットトラブル（複数回答）

単位：人

フェイスブックやブログ、掲示板などに自分の悪口などを書き込まれたことがある	37	14%
自分の個人情報や写真が勝手にネット上に載せられて、不快な思いをしたことがある	59	22%
友達（会ったことない友達含む）からしつこくメールを送られたことがある	92	35%
SNS等で、しつこく友達申請をされたことがある	78	29%
自分のSNS等が、なりすまし・アカウントの乗っ取りをされたことがある	41	15%
なりすまし、アカウントを乗っ取られた人から、迷惑メールやメッセージが届いたことがある	74	28%
その他	17	6%
回答数	266	

※　％は、母数（266）に対する割合。

図６　巻き込まれたことのあるネットトラブル（複数回答）



たためと考えられる。

テレビは有効な手段ではあるが、ニュースになっている時点で、すでに被害者が出ている。被害者をゼロにするには、事件が起きる前の段階での教育、啓発が重要である。

そのほか、学校関係（情報の授業、先生の話）も二五％いた。

また、「常識」だという人は、いまだ少数である。皆が常識だと言えるレベルまで、あらゆる手段で啓発が必要である。

警察や携帯会社など関係機関による講話を充実させるべきだと考える。携帯会社では専属チームが各学校を巡回し携帯電

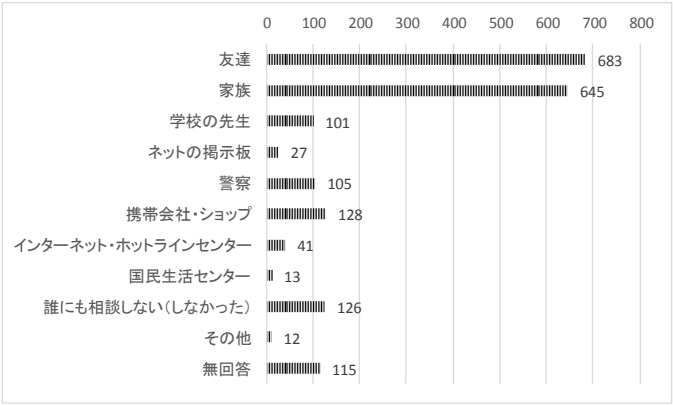
表12　ネット上のトラブルを誰に相談したか、したいか（複数回答）

単位：人

友達	683	52%
家族	645	49%
学校の先生	101	8%
ネットの掲示板	27	2%
警察	105	8%
携帯会社・ショップ	128	10%
インターネット・ホットラインセンター	41	3%
国民生活センター	13	1%
誰にも相談しない（しなかった）	126	10%
その他	12	1%
無回答	115	9%
回答数	1321	

※　％は、母数（1321）に対する割合。

図7　ネット上のトラブルの相談先（複数回答）



話利用の危険性を教える活動をしているし、全国各警察署でも、防犯の担当者が各学校に出向いてネットトラブル防止教室を開催できるから、学校と積極的に協働して啓発活動をすべきだ。

三　わいせつ画像要求四％の危険

回答数一、三二一人のうち、五〇人（四％）が「わいせつ画像を要求されたことがある」と回答した（表15）。

全体から見るとごく少ない数字であるが、ゼロではない。対象を全国の高校生にすると莫大な数になる。この層をいかに減らし被害を防ぐかが重要である。

第四節　わいせつ画像を要求されたことがある人の分析

一　地方、高校、女子の危険性が高い

表一六では、各校別に「わいせつ画像を要求されたことがある人」の内訳を示している。高校の各校とも、一〇名以下で該当者がいる。

A高からF高は地方の高校で、F高はその地域で中核になる普通高校である。F高では八名と多いが、全校生徒数も多いので割合は低く、二％である。

しかし、同じ地方でも、A高とC高でそれぞれ七％と九％で高い割合になっている。

表13　わいせつ画像流出の違法性

単位:人

知っている	1044	79%
知らない	260	20%
無回答	17	1%
合計	1321	100%

表14　わいせつ画像流出の違法性を知ったきっかけ（自由回答）

単位:人

学校関係	132	25%
家族	8	2%
常識	39	7%
ニュース、テレビ	236	45%
ネット	32	6%
友達、誰かから	34	7%
講話（携帯会社、警察など）	40	8%
合計	521	100%

一方G高校は都市部の普通高校で、地方の高校との対象のためにアンケートを実施したものである。都市部の高校のほうが割合は高いと予想していたが、二％と低くなっている。これは、むしろ都市部よりも、地方の小規模な高校においてリスクが高いことを示している。

また表一七で、男女別に見ると九四％と圧倒的に女子の割合が多い。そこで男子生徒が要求される場合を考察すると、いじめの対象として「下半身の写真を送れ」等と脅されている場合も想定される。これについては、本アンケートで考察することができなかったので、別の論を待ちたい。

高校、大学別では高校が七〇％であり、若年層のほうが要求されるリスクが高い。

二　わいせつ画像を要求された五〇人の傾向

わいせつ画像を要求されたことのある対象五〇人について、他のアンケート項目の回答との関連から、より深く掘り下げる。

㈠　ネット上の知り合いが多いとリスクが高い

対象五〇人の中で特徴的だったのが、「ネット上のみでつながっている人がいる」割合が六二％（表18）で、表四の対象全体二九％の二倍という点である。

また、その知り合いの人数を比較すると、全体では「一一人以上」は三四％（図2）であるが、対象五〇人は「一一人以上」が四二％で、「多数」の一六％を合わせると

表15　わいせつ画像を要求されたことがある

単位:人

されたことがある	50	4%
されたことがない	1169	88%
自分はないが、されたことがある人を知っている	82	6%
無回答	20	2%
合計	1321	100%

五八％になる。（図8）

これは、ネット上の知り合いと顔の見えないやり取りをしている人数が多いほうが、わいせつ画像の要求など過激な言動にさらされる可能性が高いことを示している。

㈡　個人情報公開についての意識

表九で、情報公開の際に意識している割合は全体の約七五％であった。表一九の対象五〇人では八八％であった。

つまり、わいせつ画像を要求された人のほうが個人情報の取扱いには注意を払っていたのにも関わらず、要求はされていた。これは、自分が個人情報の意識を高く持っていても関係なく、わいせつ画像の要求の危

表16　わいせつ画像を要求されたことがある人の内訳

単位：人数

		地方						都市部	
		A高	B高	C高	D高	E高	F高	G高	大学生
1年	男	1							
	女	2	2	1	1		4	1	3
2年	男							1	
	女	3		3	2	3	1	2	2
3年	男		1						
	女		2	1	1		3		4
4年	×								
	女								6
合計		6	5	5	4	3	8	4	15
母数（回答数）		87	92	53	79	79	434	211	286
全校に占める割合		7%	5%	9%	5%	4%	2%	2%	5%

表17　わいせつ画像を要求されたことのある人の内訳（性別・学年別）

単位：人数

		性別		学年計	高校大学別	母数(50)に占める割合
		男子	女子			
高校	1年	1	11	12	70%	24%
	2年	1	14	15		30%
	3年	1	7	8		16%
大学	1年		3	3	30%	6%
	2年		2	2		4%
	3年		4	4		8%
	4年		6	6		12%
性別計		3	47	50		
母数(50)に占める割合		6%	94%			

険は常に潜んでいることを意味している。

㈢　わいせつ画像の要求、公開の違法性の認識

表一三で、違法性を知っていたのは、全体では七九％であったが、表二〇においてわいせつ画像を要求された対象五〇人では八八％であった。

これも、わいせつ画像流出の違法性を知っていても、わいせつ画像の要求はされているということである。

しかし、実際に要求されたときに、法律違反であると知っていれば、それを盾に断ることもできるが、知らない場合は要求どおりわいせつ画像を作成してしまうかも知れず、危険性が高い。

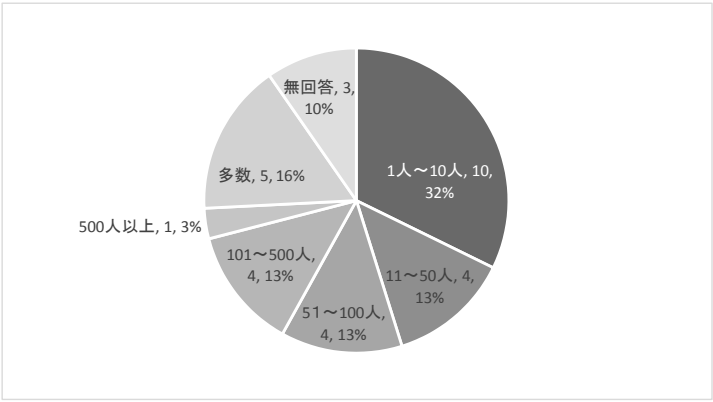
以上のことから、個人情報公開に対する意識も高く、わいせつ画像公開等の違法性を認識していても、ネット上の知り合いが多くなるとわいせつ画像要求のリスクが高くなることがわかった。

表18　ネット上のみの知り合いの有無

単位：人

ネット上のみの知り合いがいる	31	62%
ネット上のみの知り合いはいない	19	38%
対象計	50	100%

図８　ネット上のみでつながっている友人の人数（対象＝31人）



第五節　わいせつ画像を要求されても撮影しない防止策（自由記述から）

アンケートの中で、「わいせつな画像を撮影したりされたりしないためにはどうしたらよいか」との質問に、自由記述で答えてもらったところ、高校生と大学生の間で差があった。

高校生は、表現力の問題もあるが、大学生に比べ自己の意思や判断力に甘さがある回答が多く、「携帯電話を使わない」等の極論や、「がんばる」等のあいまいな意見が合わせて四二％あった。

「（たくさん要求されすぎて）もうどうでもいい」と投げやりになっている生徒には注意を要する。この女子生徒はネット上の友達が一〇〇人以上いた。

「会ったことのない人と連絡を取らない」など、自分の行動の基準を決めている人は二八％だった。意識や自覚を持って行動する人は一六％だった。（表21）

一方大学生は、「自分の行動は自分の責任で行う」という強い意志が感じられた。つまり、わいせつ画像を要求されても、自らの意見をはっきりと述べ、断ることができる人が三二％、行動基準がある人も三七％で、半数以上を占めた。啓発活動も一三％と多かった。（表22）

表19　SNS 等に個人情報を公開する際の意識

単位：人

個人情報公開時に気をつけている	44	88%
個人情報公開時に特に気をつけていることはない	6	12%
合計	50	100%

表20　わいせつ画像の要求、公開の違法性認識

単位:人

法律違反であることを知っている	44	88%
法律違反であることを知らない	6	12%
合計	50	100%

高校生は大学生に比べ他人との関わりにおける判断力が未熟である。教育のなかで、「自分の身は自分で守る。」「強い意志を持つ。」ことを指導し、「わいせつ画像の要求にはＮＯと言っても良い。」という明確な判断基準を示すことが必要である。

第三章　高校生に対する講話の実施

第一節　実施概要

一　実施の目的

ネットトラブル防止の講話を携帯電話会社および警察官が行い、講話後にアンケートを実施して受講者の意識を探る。

二　調査方法、調査期間、回収率、実施日

アンケート調査。アンケート用紙を各教員から生徒に配布。その場で回収したため回収率は一〇〇％。平成二六年七月二二日実施。

第二節　実施結果

一　講話の内容

本講話は、学校長より携帯電話会社および駐在所へ依頼があり、五〇分間で実施した。

表21　高校生の自由回答（抜粋）

極論	SNSをしない	60	10%
	女と関わらない		
	カメラ廃止		
	携帯持たない		
	恋人作らない		
	電子機器をなくす		
あいまい	危ないものをなくす	186	32%
	がんばる		
	気をつける		
	断る		
	しっかり考える		
	そんな人はだめ		
	ひたすら注意		
なげやり	もうドーでもイー感じになっている　うち気にしてないから	1	1%
相談	親や警察に相談	16	3%
	とりあえず相談		
	要求されたら友達や家族に相談		
規制	色で検出して肌色の多い写真は撮れないようにする	43	7%
	条例や法律を作る		
	罰を厳しくする		
	フィルタリングすることを法律にする		
啓発	教育する	18	3%
	ネットについてよく知る。そういう教育をする		
	犯罪であることを意識させるようなPR活動		
行動基準	会ったことのない人とネット上でからまない	163	28%
	会ったことのない人と連絡を取らない		
	個人情報載せない、画像とらない		
	無視		
	要求されたら関係を切る		
意識	意識の問題	90	16%
	個人が気をつける		
	自分の意見をしっかり伝える		
	自分の身は自分で守る		
	一人ひとりが気をつける		
	合計	577	100%

表22　大学生の自由回答（抜粋）

極論	携帯電話（スマホ含む）からカメラ機能をなくせばいいと思います。	2	1%
あいまい	断る	17	9%
	女子力をなくす		
相談	相談できる人に相談する。	2	1%
規制	拒否するのが一番だと思いますが、規制を行ってもらえると安心な気がする。	13	7%
	ネット制限のようなものをするべきだと思った。		
	もっと法律を厳しくする		
啓発	拡散されてどうなるのか実際の例を出して伝える	25	13%
	拡散のリスクを知り、自分の行動に対して責任を負うことを意識させる、喚起させる。		
	小さい頃から、いけないことだと徹底的に教育する。		
	犯罪になってしまうことや、画像が拡散されれば消すことは難しいという事実、自分の身を守ること、断る勇気について学校で伝える。		
	拡散のリスクを知り、自分の行動に対して責任を負うことを意識させる、喚起させる。		
	テレビ番組やチラシなどの注意を促すものを今よりも増やし、人の目にふれるようにする。		
	ネットの怖さを知らない人がSNSやネットをしているからこういうことになる。ネチケットも知らない人が最近多すぎる。そこから教えていくべき。		
	メディアで取り上げ、犯罪だと言う認識を持たせる		
行動基準	言われた瞬間に関係を切る。（ブロックなど）	68	37%
	危険と感じたら連絡をとるのを止める。アカウントがあれば消す。		
	絶対送らないと決める		
	そのような人とは関わりをもたないようにする		
	撮られたのがわかったらその場ですぐに消してもらう。画像を保存させない		
	ネット上でだけのつながりは避ける。連絡が来ても返事しない		
意識	意思を強く持つ。うまくかわす。嫌だとはっきり言う。逃げる。泣く。	59	32%
	嫌なものは嫌だとはっきり伝えること		
	断る。断っていいということを一般常識にする。		
	自業自得		
	自分の意志を持つ。そういった人とは関わらない。		
	自分の嫌なことははっきり相手に伝える		
	自分の身は自分で守るしかない		
	強い芯を持った人間になる。安売りしない（自分を）		
	人を簡単に信用しないこと		
	相手が誰であっても写真を撮らせる様なことはしない。好きな人が相手でもはっきり断る意志を持つ。		
	断る。断っていいということを一般常識にする。		
	合計	186	100%

携帯電話会社からは担当者が来校し、パワーポイントを用いて、以下の三点の事例を紹介しながら説明した。

① アルバイト先のレストランの冷蔵庫に入るなど度が過ぎたいたずらをＳＮＳに投稿し、損害賠償を請求された例

② 無料通話アプリ（ＬＩＮＥなど）でグループからある人を外すなど露骨な嫌がらせをしたところ逆に自分が外されたいじめ事例

③ ＳＮＳに制服姿の写真を載せた女子が、下心ある男に個人情報を探られしつこく電話等で誘われた例

担当者は各事例について、ニュースで報道されなかった当事者のその後の境遇なども説明し、筆者も大いに参考になった。

警察官は、最近のネットトラブルにかかる事件事例、特に被写体が一八歳未満であるわいせつ画像を他人に要求し製造させネットに公開すると、法律違反の可能性があることを説明した。

二　生徒の様子

同校は近年、ネットトラブルによって生徒指導に苦慮した経験から、トラブル防止について非常に熱心であり、生徒の携帯電話所持は認めているがＳＮＳ等の利用は禁止という厳しいルールがある。

生徒は他校より多くトラブル防止の指導を受けていて意識が高く、集中して真剣に講話を聞いていた。教員も全員が講話を聞き、同校の取組み意識の高さが伺えた。

三　アンケート結果

第三節　分析

一　講話の重要性

表二三で、「とてもためになった」「ためになった」が九九％に達した。生徒たちは真剣に話を聞いており、講話直後のアンケートということを差し引いても高い数字であり、講話の有用性が明らかになった。

二　講話内容には具体例を出す

表二四から、ネットトラブル防止のために生徒が欲している情報は、警察からの講話五一％、テレビ四六％、携帯会社からの講話四三％の順である。

これは、直前の講話で両者が具体例を出したことで、生徒が自分のこととして真剣に捉えることができたためと考える。ニュースも、実際に起きた事件のため、最も具体的な事例を示している。

高校生には具体的な事例を示すことにより「これはしてはならない」との判断の基準をより多く提示することが重要である。

三　講話後の意識の変化

表二五は、ネットトラブル防止のために今後どうするかを記述式で回答してもらったものである。「怪しいサイトには行かない」などの「行動基準」をあげた人が五五％であり、表二一の同カテゴリー

表23　ネットトラブル防止教室はためになったか

単位:人

とてもためになった	43	48%
ためになった	46	51%
役に立たなかった	1	1%
まったく役にたたなかった	0	0%
合計	90	100%

表24　ネットトラブルを防止するための知識を得る方法は（複数回答）

単位:人

友達との会話	40	44%
家族との会話	29	32%
学校の授業、先生の話	32	36%
ネット情報	25	28%
テレビ（ニュース）	41	46%
警察からの講話	46	51%
携帯会社の講話	39	43%
インターネットホットラインセンターの情報	16	18%
消費者センターの情報	5	6%
その他	0	0%
無回答	3	3%
回答数	90	

※　％は、母数（90）に対する割合

表25　ネットトラブルを防止するために今後気をつけたいこと

極論	SNSやらない	13	21%
	ネットを使わない		
	もう携帯を持たない		
	どうせ他のトラブルが出てくるので対策無意味		
あいまい	軽はずみなことしない	4	6%
相談	迷ったら親に相談	1	2%
規制	制限をつける	1	2%
行動基準	怪しいサイトに入らないようにする	35	55%
	リアルなコミュニケーションを大事に		
	ネットで個人情報を公開しない		
	知らない人の申請を受けない		
意識	自分で正しい判断をする	9	14%
	意識の向上		
合計		63	100%

の約二倍となった。

講話によって具体的に何をしてはいけないのかが理解できたので、行動基準をあげた人が多かったと考える。

第四章　大学生との討論

第一節　討論実施概要

一　討論の目的

アンケート調査により、広く高校生等の意識調査ができたが、ネットトラブルに巻き込まれないために実際のところどのような防止策があるのかについてより深く議論するため、討論の場を設けた。

大学三年生及び四年生の女子学生に協力いただき、学年ごとに一回ずつ、討論を実施した。

二　実施日

平成二六年七月一四日および平成二六年七月二二日

三　参加者

女子大学生（三年生一〇名、四年生一一名）

第二節　討論結果と考察

一　判断力の未熟さ

大学生がまず問題としたのは、高校生等の人間関係における判断力の未熟さである。

大学生となり交友関係も広がると、人間関係を構築する際に自己の意思や明確な基準が存在するが、自らの高校時代を振り返ると、判断の基準がはっきりせず、どうしていいかわからないときは「友達がやっているから」等と周りに流されて決定していたとのことだった。

物を盗むことは悪いことだと教えられ小さい頃から常識として知っているが、ネットの問題は常識となるまで教えられておらず、間違った判断をする余地はある。判断力が未熟であるからこそ、「これはだめ」といった明確な判断基準を教えていくことが必要である。

二　信頼関係の構築

次に問題としたのは、実際にわいせつ画像を要求された時の対応である。

大多数の人は要求されても常識的には断るだろうが、たとえば女子高生が彼氏から画像を求められ「断ったら嫌われる」と考えたり、現実世界よりネット上の人間関係に依存している女子が、おだてられて会ったこともない人から要求され、「断って関係が終わるのが怖い」と考えたりした場合はどうか。人間関係が壊れることを恐れ、送ってしまう人がいるかもしれない。

ここで、彼氏にポルノ画像を送ったことがある女性の事例を提示し、討論の議題とした。

事例は、彼氏が一〇歳ほど年上で、四年以上の交際暦があり、現在は遠距離恋愛で頻繁に会えない状況で、彼氏が「会えなくて寂しい」と暗にポルノ画像を要求したことに応え、流出の危険はないと判断して画像を送ったという内容である。

この事例をある学生は女性の心理を彼氏との信頼関係から分析した。

女性は、長い交際で相手の性格を理解し、流出などの悪用をしない、流出させて彼女を傷つけたりする人ではないと判断していた。その根底には当然愛情もあるが、相手との強固な信頼関係があるからできたとした。

「嫌われたくない」という心理でわいせつ画像を送ることと、信頼関係の元に送ることは意味合いがまるで違う。事例の女性が仮に画像を送らなかったとしても、きっと彼氏に嫌われることはないだろう。

画像を送らないから別れるカップルは、信頼関係があると言えない。まして会ったこともない人は信頼関係があるのかさえ疑問である。たった一回の判断ミスで画像がネットに公開され、一生苦しむ事態は絶対に防がなければならない。

信頼関係は、現実世界でのやり取りで成り立つこと、自分を安売りせず安易な判断をしないように教育することが大事である。

三　女性が常に被害者である風潮

たとえば高校生が、実際にわいせつ画像をネット上に公開され、親などに相談する際、体裁を気にして「私はいやだったのに、しつこいから送ってしまった。相手が悪い。」と弁解し、あたかも自分が被害者

のように振舞うこと、女性はいつも被害者で許される風潮があることが問題だとしている。

これは女子学生ならではの考え方である。流出された女性は確かに被害者ではあるが、撮影したのは自分の判断であり、自分の行動には責任が伴うことをしっかり教育しなければならない。

四　家族の常識

ネットトラブル関連のニュースなどを見て、親が子どもと話し合うことが、子どものネット利用に対する「常識」を形成する。

会話の中で、わいせつ画像の撮影が「いけないことだ」と言えば子どもはそう考えるだろう。子供たちを被害から守るためには、多様化するネットトラブルを親も勉強し、家庭の中でコミュニケーションを図っておくという、アナログな方法が大事であると考える。

五　新しい啓発の形

若年層の半数以上がTwitterを使っている現状で、各関係機関が必要な情報をTwitterで発信し、啓発活動をするものである。ネット利用に長けている若者たちにとって、ネットでの情報提供は便利で、その後の口コミも期待できる。

テレビ番組やＣＭに有名人や芸能人が出演し、ネットトラブルの体験談をして啓発することも影響力があって効果的である。

また、経験談として高校などのネットトラブル防止教室は、講義形式のため正直あまり真剣に聞いておらず、小グループ検討会や討論形式の授業がよいという提案もあった。

第五章　提言

アンケート調査、講話、討論をふまえ、高校生等をわいせつ画像流出の被害から守るため、筆者が提言したいのは以下の二点である。

第一節　既存の啓発活動の継続強化

一　学校

学校の授業で、ネットリテラシーを教えることは必要不可欠である。

これからは、教員側の研修も充実させる必要がある。現職の高校教員の話では、現在生徒が起こす問題の大半にネットが絡んでいるそうだ。積極的に研修を受け、生徒以上の知識で指導にあたるべきである。

また教育委員会が、学校に対し必ずネット関連講習の実施を通達するのもよい。そこに保護者等も参加し地域全体で勉強していくと意識も高まる。

二　家庭

家庭では、携帯電話等の利用にルールを作るべきである。親のネットリテラシーが高いと子どもにも伝わる。子どもと良好な関係を作り、ネットトラブル関連の事例について話し合って、行動の基準を示してやる必要がある。

三　関係機関による講話、情報発信

ネットトラブル防止の講話は、各機関で行っている。携帯電話会社の講話は専門のチームがいるので資料がよく研究され、非常にわかりやすい。

警察も薬物乱用防止教室などと並んで、ネットトラブル防止の講話を行っている。積極的に利用すべきである。

しかし、行政機関、とくに国の機関がネットトラブルの相談窓口を開設していても、認知度が低い現状にある。本論文の調査でも、トラブル時に相談したい相手に選択された割合は極少であった。もっと周知活動を行い、多様な機関がそれぞれの立場で、子どもたちをネットトラブルから守るために行動すべきである。

四　メディア利用

テレビの力は絶大である。報道で事件事例を放送することが周知活動、啓発活動に最も効果的である。

ネットを利用した新たな情報発信として、Twitter の利用を提案したい。各機関の視点でネットトラブル防止の情報提供をし、友人同士が口コミで拡散すれば、被害に遭いやすい若年層には効果的ではないかと考える。

第二節　顔の見える距離で各機関が連携し、地域の安全安心を守る

筆者は、北海道のとある農村地方で駐在所警察官として勤務している立場から、防犯や交通安全の講話

などを町民に行っている。

小さい町は、警察と住民との距離が近いので、たくさんの講話依頼があり、各関係機関との調整もスムーズであるし、何より講話対象者の大半が知り合いなので、皆真剣に話を聞いている。

つまり、「顔の見える距離」で各機関が緊密に連携し、かつ住民とも近い距離で関係を持つことにより、結果として治安維持を達成しているのである。

犯罪抑止には、検挙と予防の両面からのアプローチが必要である。

警察が犯人を逮捕しただけでは犯罪被害はなくならない。犯罪を予防し被害を未然に防ぐのも警察の重要な責務である。各機関団体が「安全安心なまちづくり」という同じ目標に向かい「顔の見える距離」で緊密に連携していくこと、住民一人ひとりが防犯意識を高く持ち、「自分の地域は自分たちの手で守る」と考え行動すること、そして、治安のプロたる警察官が先頭に立って、地域住民とともに汗を流し行動していくことが重要である。

おわりに

本論文では、特に高校生等の若い世代が被害に遭う、わいせつ画像のネット上への流出を防ぐ方法を、アンケート調査や講話、討論を元に検証した。

わいせつ画像の流出に対する法規制について、平成二六年七月一五日に児童ポルノ法が一部改正され、

性的好奇心を満たすために自分の意思で児童ポルノを所持した者にも罰則が設けられた。世界では、カリフォルニア州で「リベンジポルノ禁止法」が成立するなど、関連の法整備が進められている。

本文中にあった討論議題で、信頼関係に基づいて女性が自分の彼氏にポルノ画像を送ったとしても、別れた後、つまり信頼関係がなくなった時にリベンジポルノの危険性が現れてくる。日本でも法規制を行うことで、今後新たな被害を防止することができるだろう。

また、法による規制強化によってわいせつ画像の流出防止にどのような効果が現れるかは、別の論を待ちたい。

本論文は、筆者がネットトラブル防止の講話をする際、より現実的で臨場感あるものにするため、高校生の意識データを取るために行ったのが始まりである。アンケート前の筆者の予想では、高校生は何も考えず無法状態に携帯電話を使用していると思っていた。結果は一定の割合で危険な層はいたが、意外にしっかり意識をもって携帯電話等を使っていることがわかった。

筆者が大学生になって携帯電話を初めて持ってから一六年が経った。今の高校生はいわゆるデジタルネイティブ世代であり、携帯電話がある生活が当たり前である。便利だが悪用すると人が傷つくこともある諸刃の剣だ。

筆者の息子が三歳のときに、スマートフォンを自分で操作して、保存動画を延々と見ていたとき、空恐ろしさを覚えた。自分が親としてどのような主義で子どもに携帯電話を使わせるのか、ネットリテラシーを子どもに教えるにはまず自分の姿勢が問われると強く意識した。それを地域社会に拡大適用すると、地

域の子どもをネットトラブルから守るために、警察官として何ができるか、どんな姿勢で向き合い啓発していくか考えよとの課題を突きつけられた気がした。

携帯電話等の技術や機能は毎日進化し続け、昔は考えられなかったネットトラブルが起き、これからも新しい手口が現れ続けるだろう。

被害に遭う子どもたちを一人でも減らし、このネット社会を安全に暮らすために、これからも各関係機関が緊密に連携し、わいせつ画像を撮影しないことが無意識の常識となるまで、教育啓発活動を進めていく必要がある。

謝辞

本論文の趣旨を理解し快くアンケートに協力して頂いた、各高校の教頭先生には、アンケート集計結果と私の講話で恩返しします。

たくさんの貴重な意見をくれた大学生諸君、アンケート回答に協力してくれた一、三二一名の学生生徒の皆さん、ありがとうございました。

本論文の作成を許可してくださった署長、副署長、また各学校の教頭先生と私の橋渡しをしてくれた各町の駐在所勤務員の皆様にも、感謝申し上げます。

最後に、論文作成に際し陰ながら支えてくれた妻と子どもたちに、ありがとう。

（注1）警察庁：〝NO！！児童ポルノ「検挙状況・被害状況」〟：http://www.npa.go.jp/safetylife/syonen/no_cp/statistics.html（参照2014-8-16）
（注2）ストーカー行為等の規制等に関する法律（平成一二年法律第八一号）
（注3）清水陽平：〝リベンジポルノの削除と処罰――法規制の現状と新法の方向性〟：2014-5-13：http://synodos.jp/society/8056（参照　2014-8-16）
（注4）清水陽平：〝リベンジポルノの削除と処罰――法規制の現状と新法の方向性〟：2014-5-13：http://synodos.jp/society/8056/2（参照　2014-8-16）
（注5）清水陽平：〝リベンジポルノの削除と処罰――法規制の現状と新法の方向性〟：2014-5-13：http://synodos.jp/society/8056（参照　2014-8-24）
（注6）安心ネットづくり促進協議会：〝フィルタリングサービスを利用しましょう！〟：http://sp.good-net.jp/filtering/（参照　2014-8-22）
（注7）総務省：2013-9：〝平成二五年度青少年のインターネット・リテラシー指標等〟：http://www.soumu.go.jp/main_content/000247066.pdf（参照　2014-8-22）

資料　　携帯電話の利用に関する意識等のアンケート（高校生用）

このアンケートは、みなさんの携帯電話などの利用に関して、意識調査をするものです。
あてはまる答えの数字に○をつけてください。
調査以外の目的では使用しないので、安心して答えてください。
※ あなたの学年、性別を教えてください。　　[　　] 年　　（ 男 ・ 女 ）

問1　あなたは現在、自分専用の携帯電話等を持っていますか。
1 持っていない →問 11へ　　2 持っている （契約者は自分）→ 問2へ
2 持っていないがパソコンを利用している →問3へ　　4 持っている （契約者は親など） → 問2へ

問2　あなたの携帯電話等には、フィルタリング（アクセス制限）を設定していますか。
1 設定している　　2 はじめからしていない　　3 はじめはしていたが、途中で解除した
4 インターネットが使えない設定になっている　　5 わからない

問3　あなたの家庭では、携帯電話等の使用のルール（きまり）はありますか。
1 ある →どんなルールか一つあげてください（　　） 2 ない

問4　あなたは、携帯電話等でSNSやブログ、(ｵﾝﾗｲﾝ)ｹﾞｰﾑを利用していますか。（あてはまるもの全てに○）
1 自分のブログ 2 Facebook 3 Twitter 4 LINE 5 mixi 6 google+ 7 (ｵﾝﾗｲﾝ)ｹﾞｰﾑ
8 その他（　　） 9 SNS等はやっていない

問5　問4で、SNS等を利用している人について、アカウントを複数もっていますか
1 アカウントを複数持っている →どのSNSで？（　　） 2 複数アカウントはない

問6　あなたは、ネット上のみでつながった（実際に会ったことがない）人はいますか
1 いる →(人数:　　人くらい →[そのうち継続して連絡を取り合っている人数:　　人くらい])
2 いない →問8へ

問7　問6で「いる」と答えた人は、どのような方法でつながりましたか。（あてはまるもの全てに○）
1 出会い系サイト 2 Facebook 3 Twitter 4 LINE 5 mixi 6 google+ 7 (ｵﾝﾗｲﾝ)ｹﾞｰﾑ
8 友達などから直接紹介された 9 その他（　　）

問8　あなたは、次のようなトラブルに巻き込まれたことがありますか（あてはまるもの全てに○）
1 フェイスブックやブログ、掲示板などに自分の悪口などを書き込まれたことがある
2 自分の個人情報や写真が勝手にネット上に載せられて、不快な思いをしたことがある
3 友達（会ったことない友達含む）からしつこくメールを送られたことがある
4 SNS等で、しつこく友達申請をされたことがある
5 自分のSNS等が、なりすまし・アカウントの乗っ取りをされたことがある
6 なりすまし、アカウントを乗っ取られた人から、迷惑メールやメッセージが届いたことがある
7 その他（具体的に:　　）
8 トラブルになったことはない

→裏面につづく

問9　問8のトラブルに巻き込まれたとしたら、あなたは誰に相談しますか
実際に巻き込まれたことがある人は、誰に相談しましたか （あてはまるもの全てに〇）
1 友達　2 家族　3 学校の先生　4 ネットの掲示板　5 警察　6 携帯会社・ショップ
7 インターネット・ホットラインセンター　8 国民生活センター　9 誰にも相談しない（しなかった）
10 その他（　　）

問10　SNS等への書き込みなど情報を発信するときに、個人情報保護の観点からあなたが気をつけていることはありますか（あてはまるもの全てに〇）
1　自分が特定されるような個人情報や写真は、ネットに載せない
2　自分が特定されるような個人情報や写真は、公開範囲を制限する
3　他人が写っている写真をネットに載せるときは、その人に許可を取る
4　他人や、場所が特定されそうな写真を載せるときは、スタンプやモザイクなどで加工して消す
5　アルバイト先で写した写真や個人情報は、ネットに載せない
6　その他　（　　）
7　特に気をつけていることはない

問11　インターネット上に、他人の悪口や他人の個人情報を書き込んだりすると、その内容によっては犯罪になることを知っていますか。
1 知っている　→何で知りましたか（　　）　2　知らない

問12　他人（友達）の自画撮り画像（わいせつなものを含む）を要求したり送信させたり、それらをインターネット上にさらしたりすることが、状況によっては犯罪になることを知っていますか
1 知っている　→何で知りましたか（　　）　2　知らない

問13　問12に関連して、実際にわいせつな画像を送るように要求されたことはありますか
1 されたことがある　2　されたことはない
3　自分はないが、されたことがある人を知っている

問14　最近の事例として、ネット上で知り合った人から、個人情報やわいせつな画像を要求され、本当に撮影し返信してしまったところ、ネット上に拡散されたというものがあります。
一度ネット空間に拡散された画像は、完全に消すのは不可能といわれており、拡散された人は長い間苦しむことになります。
これを防ぐためには、わいせつな画像を撮影しないこと、たとえ恋人であってもわいせつな画像を撮影させないことが重要です。
では、わいせつな画像を撮影したりさせたりしないようになるにはどうしたらよいと思いますか
あなたの考える、防止策について自由に書いてください。

ご協力ありがとうございました。

携帯電話の利用に関する意識等のアンケート（大学生用）

このアンケートは、みなさんの携帯電話などの利用に関して、意識調査をするものです。
あてはまる答えに○をつけてください。
調査以外の目的では使用しないので、安心して答えてください。
※ あなたの学年、性別を教えてください。　　[　　] 年　　（ 男 ・ 女 ）

問1　あなたは現在、携帯電話等を持っていますか。
1 持っていない →問9へ　　2 持っている →問2へ

問2　あなたは、携帯電話等でSNSやブログ、(ｵﾝﾗｲﾝ)ｹﾞｰﾑを利用していますか。（あてはまるもの全てに○）
1 自分のブログ　2 Facebook　3 Twitter　4 LINE　5 mixi　6 google+　7 (ｵﾝﾗｲﾝ)ｹﾞｰﾑ
8 その他（　　）　9 SNS等はやっていない

問3　問2で、SNS等を利用している人について、アカウントを複数もっていますか。
1 アカウントを複数持っている →どのSNSで？（　　）　2 複数アカウントはない

問4　あなたは、ネット上のみでつながった（実際に会ったことがない）人はいますか
1 いる →(人数:　　人くらい →[そのうち継続して連絡を取り合っている人数:　　人くらい])
2 いない →問6へ

問5　問4で「いる」と答えた人は、どのような方法でつながりましたか。（あてはまるもの全てに○）
1 出会い系サイト　2 Facebook　3 Twitter　4 LINE　5 mixi　6 google+　7 (ｵﾝﾗｲﾝ)ｹﾞｰﾑ
8 友達などから直接紹介された　9 その他（　　）

問6　あなたは、次のようなトラブルに巻き込まれたことがありますか（あてはまるもの全てに○）
1 フェイスブックやブログ、掲示板などに自分の悪口などを書き込まれたことがある
2 自分の個人情報や写真が勝手にネット上に載せられて、不快な思いをしたことがある
3 友達（会ったことない友達含む）からしつこくメールを送られたことがある
4 SNS等で、しつこく友達申請をされたことがある
5 自分のSNS等が、なりすまし・アカウントの乗っ取りをされたことがある
6 なりすまし、アカウントを乗っ取られた人から、迷惑メールやメッセージが届いたことがある
7 その他（具体的に:　　）
8 トラブルになったことはない

問7　問6のトラブルに巻き込まれたとしたら、あなたは誰に相談しますか
実際に巻き込まれたことがある人は、誰に相談しましたか （あてはまるもの全てに○）
1 友達　2 家族　3 学校の先生　4 ネットの掲示板　5 警察　6 携帯会社・ショップ
7 インターネット・ホットラインセンター　8 国民生活センター　9 誰にも相談しない（しなかった）
10 その他（具体的に:　　）

→裏面につづく

41　ネット社会を安全に暮らす

問8　SNS等への書き込みなど情報を発信するときに、個人情報保護の観点からあなたが気をつけていることはありますか（あてはまるもの全てに○）

1　自分が特定されるような個人情報や写真は、ネットに載せない
2　自分が特定されるような個人情報や写真は、公開範囲を制限する
3　他人が写っている写真をネットに載せるときは、その人に許可を取る
4　他人や、場所が特定されそうな写真を載せるときは、スタンプやモザイクなどで加工して消す
5　アルバイト先で写した写真や個人情報は、ネットに載せない
6　その他　（　　）
7　特に気をつけていることはない

問9　インターネット上に、他人の悪口や他人の個人情報を書き込んだりすると、その内容によっては犯罪になることを知っていますか。

1　知っている　→何で知りましたか（　　）　2　知らない

問10　他人（友達）の自画撮り画像（わいせつなものを含む）を要求したり送信させたり、それらをインターネット上にさらしたりすることが、状況によっては犯罪になることを知っていますか

1　知っている　→何で知りましたか（　　）　2　知らない

問11　問10に関連して、実際にわいせつな画像を送るように要求されたことはありますか

1　されたことがある　2　されたことはない
3　自分はないが、されたことがある人を知っている

問12　最近の事例として、ネット上で知り合った人から、個人情報やわいせつな画像を要求され、本当に撮影し返信してしまったところ、ネット上に拡散されたというものがあります。

一度ネット空間に拡散された画像は、完全に消すのは不可能といわれており、拡散された人は長い間苦しむことになります。

これを防ぐためには、わいせつな画像を撮影しないこと、たとえ恋人であってもわいせつな画像を撮影させないことが重要です。

では、わいせつな画像を撮影したりさせたりしないようになるにはどうしたらよいと思いますか

あなたの考える、防止策について自由に書いてください。

防止策を講じても、要求によってわいせつ画像を撮影したり、中には（女性が）自ら進んでわいせつ画像を twitter などネット上に載せている場合もあります

このような人は、どんな心理で撮影していると思いますか

ご協力ありがとうございました。

〔優秀賞〕

情報モラルを考える
～標語創作をツールとした実践～

山口県立山口高等学校教諭
久原　弘（55）

一　はじめに

一五年前、高一の女子生徒から受けた相談は衝撃だった。パソコンの画面いっぱいに「死ね死ね死ね死ね死ね死ね死ね死ね…」の文字を羅列されたと泣きながらの訴えであった。理由はおそらく高校主催のミスコンテストの一位に選ばれたことではないかと本人の弁である。というのもミスコンテストの直後

より嫌がらせメールが徐々に増加してきたからだという。加害者は先輩の可能性が高い（本人弁）と思われるが、同級生の可能性もあり、まさに疑心暗鬼になっていた。それゆえ、とうとう彼女は家から一歩も出られなくなってしまったのである。しばらく不登校が続いたが、彼女が学校に戻ることは二度となく、そのまま進路変更となった。

当時、ネットはもちろん携帯も今ほど普及しておらずネット上の誹謗・中傷はそんなに多くはなかったように思われるが、それでもこんな問題が現実に起こっていたのである。それに比べると今は情報天国であり、かつては大人の持ち物であった携帯が小学生ですら普通に所有している時代である。そのためネット社会での諸問題が著しく増加しても何ら不思議ではないといえるかもしれない。

現在、私は通信制の高校で教育相談を担当しているが、本校では在籍生徒（約一、二〇〇人）のおよそ三分の二が不登校だった生徒であり、中でもネットによる誹謗・中傷等で不適応を起こした生徒が実に多い。通信制は、全日制や定時制などで不適応になった生徒が支援施設や病院を経由して入学してくることが多い。それが「通信制は最後の砦」といわれている所以でもあるが、全日制や定時制で、ネット社会における十分な支援を実施しておけば、少しでも通信に入学してくる生徒は減ると思われる。

私が以前、全日制（前籍校）にいた頃（平成一一年度～平成二三年度）、情報モラルを育成するための試み（標語創作をツールとした実践）を三年前（平成二三年度）に実施したことがある。前籍校でも教育相談を担当しており、当初は冒頭で述べたような進路変更にまでなった生徒も出るには出たが、年間にすればメールやネット上の諸問題はわずかであった。しかし、パソコンや携帯の普及とともに年々増え続け、

中にはうつ状態に陥り、リストカットにまで至る生徒も出てきていた。いわゆるメールやネット上での誹謗・中傷等によって心の健康度を著しく低下させている生徒が増加傾向にあるといえた。

そこで、私は前述したような試みを実施したわけであるが、その結果、少なからず一定の効果を得ることができたと思われた。本研究論文ではその実践を振り返り、どのようにしたらメール等での誹謗・中傷が減少し、情報モラル育成の向上につながったのか、その過程を報告したい。

二　ねらい～啓発活動としての標語創作～

㈠メール・ネット上における相談の現状

メールやネットにおける相談件数は一五年くらい前まで年間おおよそ二～三件であった。しかし、平成一九年度から二ケタ台になり、それ以後も徐々に増加し続け平成二三年度では、四一件であった。

最も件数の多くなった平成二三年度の実質人数は一年生が六人、二年生が一人、三年生が一人の計八人であった。全員が誹謗・中傷で悩み、最も多い生徒で一〇件、少ない生徒で四件であった。なお誹謗・中傷の内容は最も多かったのが、「うざい」でその他には、「死ね」、「学校を辞めてしまえ」、「早く消えろ」、「臭い」、「むかつく」、「顔を見ただけでも気分が悪い」等、人間性を踏みにじった言葉のオンパレードである。中には朝、昼、晩と執拗に誹謗・中傷メールを送信してくる加害者もおり、八人の内二人がうつ状態となり、二人ともリストカットをするようになった。その後二人とも神経科に通院しながら相談室登校

となったが、そのうち一人は、手首だけでなく太ももにもリストカットするようになり夏休みを前に進路変更となった。その他には対人恐怖症の生徒が一人で、後は相談室に誹謗・中傷の悩みを聞いてほしいと来室してくる生徒達である。ただこの生徒達にしてもこのまま誹謗・中傷が続くことがあれば、いつ鬱状態になるかわからず予断を許さない状態であるともいえた。またこうして相談に来ている生徒にしても氷山の一角であるとも考えられる。

㈡　メール・ネット上の誹謗・中傷の問題点

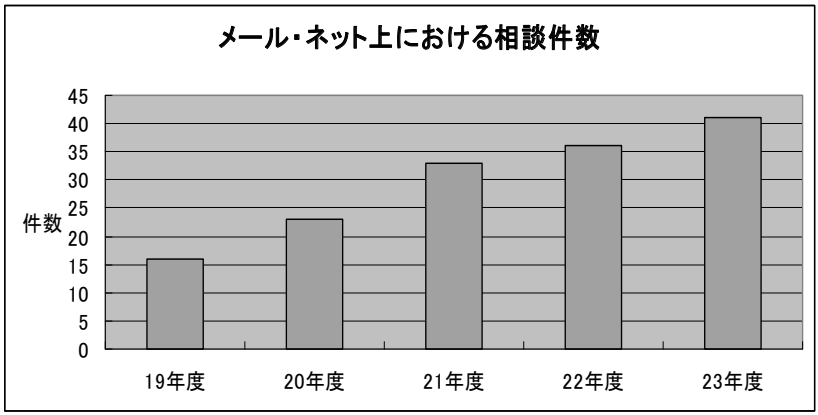
メール・ネット上における誹謗・中傷の場合、相手の姿は全く見えない。その見えないことをよいことに加害者はいくらでも心にたまっている悪口・雑言を吐き出すように書き込む。通常、生徒におけるいじめ等の人間関係における悩みは、比較的相手がはっきりしていることが多い。もちろん必ずしも成功するわけではないが、加害者の分析がしっかりできることもあり、チームとして連携をとりつつある程度対応の仕方もあるといえる。

しかし、メール・ネットでの誹謗・中傷の場合、前述したように発信者の姿は闇に隠れている。いわゆるわざわざ自分の名前を名乗って書き込むケースは非常に稀といわざるを得ない。そのため書き込まれた生徒は、例えばその言葉よりそれがおそらく同じ学校の生徒であろうと、うすうす感じながらも相手がクラスの人間なのか、先輩なのか、後輩なのか、もしかしたら他校かもしれないなどと不特定多数となり、不安もより一層増幅される。その結果、周囲がみんな敵に見え、他者の視線が気になる対人恐怖に陥る生

徒も中には出てくる。リストカットをした生徒以外で、前述したように一人ほどこの症状の生徒がいたが、つまりこれらが原因で不登校などの不適応を起こす生徒も少なからず出てくることもあるわけである。そこで、原因であるメールやネットでの誹謗・中傷を少しでもなくすため、より効果のある対応の必要性を強く感じていた。

㈢　学校の対応

当然、学校としてもこんな現状において指をくわえて見ているわけではない。平成一九年度より、朝礼等の全体会や学年を集めて情報通信におけるルールやマナー、セキュリティに関わる講話等（専門講師によるお話）をしばしば実施している。特に誹謗・中傷の書き込みにおいては、まず被害者がプロバイダに開示請求を提出し、権利侵害が明らかな場合、直ちに削除されることや、誰が嫌がらせメール等を発信しているのか、突き止めればいくらでも解明できることは生徒全員に伝えている。また人権教育においてもロングホームルーム等で『メール』という誹謗・中傷に悩む学生を主人公としたＶＴＲを視聴させ、その後グループ別に分けて討論会を実施し、



最後に感想文を提出させる啓発活動を行っている。これらの学校としての対応の結果、ある程度の効果はあったと思われるが、それが生徒の心にしっかりと浸透していたかというと、どうも私には疑問符が残ったのである。というのも前述のメール・ネット上の相談の現状のグラフからでもわかるようにメールやネットにおける相談件数が減少するどころか、むしろ増加していたからである。

㈣　標語創作を啓発のためのツールとした理由

もっと生徒の心の奥底に直接訴えるような啓発的試みはないかと、ネットを含め多くの情報に目を通し、模索していたとき、情報に関する啓発標語コンクールに複数リンクした。即座にそのＨＰを見たところ、ねらいや趣旨が、ネットにおける情報・通信のルールやマナーをしっかり守り、安心・安全に利用できるよう意識を高めることとある。

この瞬間、啓発標語創作が生徒支援のための一つのツールになり得ると考えたわけであるが、他にも十分すぎる利点が二つ考えられる。一つは標語は短歌や俳句、川柳とともに表現力はもちろんのこと、感性を育成するリソース（材料）にも十分なりうると思われる。また感性が育つことにより、より人間としての何が善で、何が悪なのか、倫理的判断力も養われると考えられる。

もう一つは標語創作はそのテーマについて自ら試行錯誤しながらも真剣に熟慮することで、それが心に浸透し、より啓発を高める活動になるとともに少しでも自己実現にも繋がると考えられる。そうすれば、加害者も自分の持っている可能性、もしくは秘められている力のすべてを実現でき、つまらない行動、こ

こでは誹謗・中傷などという非社会的な行為に走ることも極力少なくなるのではないかと思われる。

三　実践～五つの流れ～

実践を行う対象学年であるが、誹謗・中傷における相談に来ていた二年生（一人）と三年生（一人）の場合、その相談時期が主として一学期までであり、二学期以降は全く来ていなかった。ところが一年生（六人）の場合は、二学期以降も誹謗・中傷の件で継続して相談室に来ていた実情があった。また誹謗・中傷メールの文面（担任の先生や友人の名前等）より送信者が同学年である可能性が十分伺われた。そのため対象学年は一年生全クラス（四クラス一六〇人）とした。実践方法としては以下のように五つの流れで実施した。

(1)　情報通信に関するマナーを生徒に伝える
(2)　事例紹介（実際の被害事例）
←
(3)　啓発標語創作
(4)　話し合い／グループ別
(5)　情報通信の啓発活動に関する感想文を書く

(1)　情報通信に関するマナーを生徒に伝える

社会の情報化がどんどん進み、ネットやメールからのメリットも多く享受している一方、誹謗・中傷をはじめとする弊害も多発している現状がある。実際、誹謗・中傷を受けた生徒は、うつ等を発症するなどとてつもなく大きなダメージを受けることもある。そこで授業において情報・通信に関する以下のマナーについて生徒に伝える。

情報通信に関するマナー

○自分の発言には責任を持ち、嘘をついたり本当かどうかわからないことを正しいことのように書いてはいけない。
○掲示板やチャット、メーリングソフトに書き込むときには、注意深く言葉を選んで相手を傷つけないように心がけること。また顔が見えないからといって、年齢や性別、名前などについて嘘をついて、乱暴な言葉、人をののしるような言葉はもちろん、人の悪口を書いたり、いやがらせをしたりするのもやめること。

〈財団法人インターネット協会「インターネットにおけるルールとマナー」二〇〇五〉より

(2)　事例紹介（実際の被害事例）

メールやネットで苦しんでいる生徒が現実にいることを知ってもらうためにも実際に過去にあった事例を個人を特定できないようにすることはもちろん、また本人からの承諾の上紹介する。（Aさん、Bさんとも卒業生）

事例一

誹謗・中傷により不登校になってしまった生徒Aさん

存在自体がウザイと送信され、それも朝、昼、晩と定期的に送られてくる。しばらく無視し続けたが、それはエスカレートするばかりである。誰であるかは、おそらく文面から判断すると、学校の人間であることは間違いないであろうが、複数のようでもあり、なかなか特定できないでいる。

そのため人間不信から対人恐怖へと変化し、人の目を見るのが怖くなる視線恐怖症となってしまった。

そのためクラスにも入れなくなってしまい、いつの間にか学校にも遠ざかっていた。

事例二

誹謗中傷によりリストカットにまで追い込まれた生徒Bさん

話し方やふるまいが、調子に乗っているのではと非難され、「消えろ」とか「むかつく」と送信してくる。

初めは少し反論していたが、だんだん逆上してきて最後は「死ね」の連発である。

相手が自分のことを常に監視しているようなのに自分はそれが誰だかさっぱり分からない状況で不安で仕方がない。そのためイライラとストレスが高じて気が付いたらリストカットしている自分に気づく。このままではいつか死んでしまうかもしれないといった恐怖心の中で、やめようとする気持ちはあるにはあるが、なかなかやめられないでいる自分がいた。

(3)　啓発標語創作

情報通信の安心安全に関わる語句を思い当たるだけノートに書かせる。生徒に書かせた主な語句を抜粋すると以下のようになる。

生徒がノートに書き込んだ主な語句／抜粋

ネット	メール	モラル	誹謗	中傷	
大切	思いやり	被害者	届く	心	
送信	着信	ハート	気持ち	遊び心	
気づく	情報	道徳	倫理	通信	
意識	不快	迷惑	プライバシー	etc	

次にその言葉を五七五のリズムでパズルを組み立てるようにしっくりくるまで作り上げる。このときに必ずしもきっちりと五七五にする必要はなく、多少の字足らず字余りは全く問題ないことを伝える。字数よりも頭にすっと入ってくるようなリズム感のあるそれでいて「なるほど」と唸るような標語に少しでも近づけるようにじっくりと標語づくりに専念させる。数に制限は持たせず自由に創作させるが、一人あたり大体三句～五句くらいを目標にする。時間的には集中させる意味でもだいたい二〇～三〇分くらいを設定する。

生徒が実際に創作した標語の例

送信前　思いやりの心　忘れずに　　止めようよ　不快なメール　絶対に
情報に　振り回されない　確かな心　　常日頃　被害者の気持ち　念頭に
打つ前に　しっかり確認　何度でも　　思いやり　ネットでつなぐ　心と心
よいマナー　ネット社会を　幸福に　　ネットはね　人の性格　映し出す
少しだけ　遊び心が　相手を不快に　　ネット社会　ルール守って　大切に

(4)　話し合い／グループ別

グループ別にお互いの作品について話し合いをさせる。グループ内で生徒が創作した標語をそれぞれ発表し、どうしてそのような標語を創作したか、意図などを創作者自身が説明する。その後同じグループ内の他の生徒がそれについての疑問や感想を話し合う。以下に二事例（Xさん、Yさん）を紹介する。

事例一　標語：止めようよ　不快なメール　絶対に（Xさん）

この標語においてXさんの意図としては、本人にとって不快と思われるメールをしっかり考えて欲しいと話していた。つまり送信する前にまず自分がこのメールを受け取ったらどんな気持ちになるのかをいったんシュミレーションした後、相手が気分を害するかどうか、しっかり確認してから送信するべきであると考えたわけである。ここで他の生徒からの疑問として、具体的にはどんなメールが不快か、そうではないのかの線引きが意外に難しいのではといった声が上がっていた。それに対してXさんは、「死ね」とか「ウザイ」は言うまでもないが、真剣にその本人の気持ちになれば、ある程度判断できるのでは（勿論わかる範囲内になるが）と話していた。

事例二　標語：思いやり　ネットでつなぐ　心と心（Yさん）

この標語ではYさんの意図としては、相手を思いやるネットによって心と心を通い合わせ良好な人間

関係を作る大切さを話していた。ネットだからこそ話せることもそれによってより友人関係が親密になることもあるというわけである。これを聞いていた他の生徒からは人間関係を作るのであれば、ネットではなく直接会って交流を深めるほうがよいのではと指摘されていた。それに対してＹさんは以前自分自身が人前に出ると極度の緊張から全く話ができないときがあり、そんな時にメールでは話ができることに気づきその時の思いやりのある友達のメールから元気が出て立ち直ることができた経験を話していた。

(5) 情報通信の啓発活動に関する感想文を書く。

最後に感想文を書かせる。特に字数は指定せず自由に書かせることにした。その感想文の一部（四例）を以下に紹介する。

ネットでは誰かの心無い一言でひどく傷ついている人も多く、たくさんのトラブルがあります。しかし、一人ひとりが思いやりの心を持ち、マナーを守ることですばらしいコミュニケーションの場にもなります。今後、他者だけでなく自分のためにもしっかりルールやマナーを守っていこうと思いました。ネット社会は悪意を伝えることではなく幸せを広め、世界でつながるものだと一生懸命標語を創りながら実感しました。

情報社会で生きている私達は情報通信とかかわって生きているのでこの標語を頭をひねって作る

際には相手のことを思いやることが何よりも大切であると改めて感じました。いつも何気なく送っているメールも知らないうちに相手を傷つけているかもしれないので送る前には必ず読み直して本当にこれでいいのかきちんと確認したいと思いました。

今回、この情報通信の標語を考えてみて、改めてネット社会における自分の守り方、そしてネット上でのマナーを考えさせられました。インターネットは世界と自分を手軽につなぐことができますが、その手軽さゆえに誹謗・中傷などの様々な問題が起きています。これらを解決するには一人ひとりの相手を思いやる気持ちが大切ですが、標語を作ることでこの「思いやり」の気持ちを本当に深く考えるようになりました。

最近は情報化がどんどん進んでいます。本当に便利な生活になっていると思います。しかし、その便利の裏に実に多くの危険が潜んでいることを私たちは忘れてはいけません。標語を考えながら思ったことは、パソコンや携帯電話などを使うときは相手の立場に立って十分に注意する必要があると思いました。情報通信が安心かつ安全になるためには、世の中のすべての人がルールやマナーをしっかり守って利用しなければならないと思います。

四　成果と考察

㈠　実践の成果

標語創作の授業を終えた後、翌日よりいつもメールで悩み、相談を受けていた一年生がぽつぽつと相談室を訪れ、結局一週間以内に全員（六名）が来室した。その報告をまとめると以下の通りである。

生徒	報告内容
Ａさん	標語を書いて以降、嫌な事を書かれることがほとんどなくなりました。
Ｂさん	標語を書いてから何もいやなメールはありません
Ｃさん	今まで散々自分の悪口が書かれていたのですが、標語を書いた翌日に〝悪口を書いてごめんなさい。〟と謝罪の言葉まであったんですよ。
Ｄさん	あれ（標語創作）以降不快な書き込みはないです。
Ｅさん	一部無言はありますが、嫌がらせメールはなくなりました。
Ｆさん	標語を書いてからパタッと来なくなりました。

ある生徒は「標語を書いて以降、嫌な事を書かれることがほとんどなくなりました。」と。またある生徒は「今まで散々自分の悪口が書かれていたのですが、標語を書いた翌日に〝悪口を書いてごめんなさい。〟と謝罪の言葉まであったんですよ。」などと彼らは明るくすっきりとした面持ちで私に報告した。もちろ

んすべてが解決したわけではない。相談室に来室した生徒はほんの一握り、つまり氷山の一角かもしれないからである。しかし、そのわずかな生徒であろうと、少しでも生徒を支援できたことは教師として喜ばしいことでもあり、嬉しそうに私に話す生徒達の顔が非常に印象的でもあった。

またそれを裏付ける要因として、多くの生徒の心にある程度、この実践のねらいである情報モラルが浸透したのではないかと考えられたことである。というのも生徒の感想の多くが、たとえば例を挙げると「標語を真剣に考える中で、メールやネットが非常に便利なツールであると同時にその怖さも感じることができた。」、「話し合いの中で何気ない言葉が意外に相手を傷つけていることが改めてわかった。」「一生懸命に何度も標語を頭の中で練り直している中で、メールを送るに当たって相手の立場になって、相手を思いやる気持ちを考えるようになった。」等であったからである。

㈡　実践の考察

私が相談係として、情報における誹謗・中傷による多くの生徒を抱え込んだことから今回の実践を始めたわけであるが、この問題は生徒にとっても非常に身近な問題でもあったためか、多くの生徒が熱心に取り組んだと思われる。実際、最初の情報に関するマナーを生徒に伝える時点から非常に真剣なまなざしで聞いており、事例紹介では同じ学校の先輩ということもあり、ほとんどの生徒が大きくうなずくとともに中にはメモをとっている生徒までもいた。それだけ他人事として考えることのできないほどの生徒にとっては関心事だったのだろう。そのためか、標語創作活動に入るや否やほとんどの生徒が私語をすることも

なく黙々と創作にいそしみ、実に多くの生徒が、ほぼ一人平均三作品以上を創作し、中には一〇作品近く創作する生徒までもいた。標語を創作するということはそんなに簡単ではないはずであるが、ノートに思い付くまま先に語句を書き込んであったことも創作をスムーズに進ませた要因のひとつにはなったと思われる。

その後グループ別にお互いの作品について話し合いをさせ、感想を書かせたわけであるが、話し合いの中では、当初はしばらく沈黙が続き、どう切り出したらよいのか、かなり戸惑っている様子がどのグループにも見られた。しかし、自分の創作した標語を発表し始めると、自然と話に熱が入ってくる様子が手に取るようにわかった。中でも送信する場合、どんな言葉が相手を不快にさせるか否かが、多くのグループでの議論の中心になっていたが、ただ少なくとも明らかに気分を害するような言葉は避けるべきであり、真に相手の気持ちに寄り添って思いやる気持ちを考えるべきであるという結論に至っていた。またここまで送信する言葉についてみんなで真剣に議論する経験は、今までなかったであろうから生徒にとってもモラルにおける言葉というものについて真剣に考えるよい機会になったと思われる。

今回の実践はまずその意図をしっかりと考え、そこから言葉を抽出し、さらに紡ぐという非常に熟考を必要とする作業であり、さらに創作した標語をグループ別に話し合う活動であったが、ある程度効果があった理由を考えてみると、この熟考が最も効果のあった要因の一つになったのではないかと考えられる。というのも何度も試行錯誤を繰り返しながら真剣に言葉を紡ぐことで、心に染み込むがごとき情報モラルにおける啓発が感想文にもあったようにより高まったと思われたからである。またそれによって感性も養わ

れると同時に倫理観も育成されたのではないかと考えられる。

五 おわりに

この実戦を終えてみて結論としては、情報通信における啓発標語創作活動は少なからず効果があったと考えられる。しかし、青年期は疾風怒濤の時代であり、心も移ろいやすいため恒久的かといえば決してそういうわけではないと思う。ただ、少なくとも生徒自身の深層心理に「情報モラル」という観念の芽をある程度植えつけたことは確かであろう。

今後は、誹謗・中傷に苦しむ生徒を少しでも出さないためにもその芽をしっかりと育てていかなければならないと思う。そのためにも、この実践の継続はもちろんのこと、他にどのような支援方法が有効であるか、情報モラルの育成のためにもさらに研究を進める必要性があると思われる。

【優秀賞】

ネット社会における子どもの安全を守るための五つの提言

警察官（北海道警察）
竹中　利衣（33）

一　はじめに

現在は「ネット社会」と呼ばれる。パソコンや携帯電話だけでなく、家電製品やビルシステムまでもネットにつながっているこの社会は、社会全体が情報化されているといっても過言ではない。私たちの生活に欠かせない電気・ガス・水道といったライフラインの基幹システムも、独立したシステムとして運用され

てはいるが、ＵＳＢの媒介によって完全にその独立性を保つことは難しい。ネット社会において、私たちは簡単に世界中の情報を入手し、世界に向けて情報を発信できるようになった一方で、その便利さを悪用した犯罪に巻き込まれる可能性が高くなっている。

ネット社会が生み出す犯罪は、個人を対象としたいじめや詐欺、企業・組織を対象とした情報や金銭の窃取、さらに国家を対象としたサイバーテロ・サイバーインテリジェンスにまで及んでいる。私たちはこれらの犯罪の被害者となる可能性があるだけでなく、自分が興味本位で行った情報発信によって犯罪者・加害者となる可能性もある。

また、ネット社会の危険は、ネットを利用しない者にとってももはや無関係ではない。平成二七年度から導入される「社会保障・税番号制度（マイナンバー制度）」では、私たち一人一人に番号が割り当てられ、個人情報が行政ネットワーク上で管理される。私たちは、自分の番号と設定したパスワードにより、どこからでも行政サービスを受けることができるようになるが、ネットを利用しない者であっても、ネット上で自分の個人情報が取り扱われるようになることで、ネット上における危険とは無関係ではなく、個人情報を守るためには、ネット社会の危険性や情報セキュリティについて理解しなければならなくなっている。

このように、すべての人がネット社会の一員となる中で、ネット社会を安全に暮らすためには何が必要なのだろうか。

従来であれば、社会の危険に対しては法律による規制が有効であった。しかし、現代においてはネット社会の特徴であるグローバル性や情報技術の変化の速さから、法律による規制が追いつかない部分も多

い。また、安全を優先し、ネット社会に一律の規制をかけることで、ネット社会が持つ可能性や創造性が失われてしまうというジレンマもある。日本におけるネットの規制に関して、国は、犯罪に対する法律の整備を除き、できるだけ関係事業者の自主規制を先行させて、ネット上への一律の細かな規制については原則として事後的なものとする方針である。

つまり、ネット社会は、国による規制が及ばない部分が多いことから、安全に暮らすためには私たち自身がネット社会の危険を理解し、行動しなければならない社会である。本稿では、ネット社会を安全に暮らすために必要な対策について、子どもの安全を守るという観点から、五つの提言をする。

二　ネット社会と子どもの安全

二・一　子どもの安全を考える理由

本稿では、ネット社会における子どもの安全を考える上での、「子ども」を一八歳未満の情報端末を利用可能な者とした。その理由は以下の二点である。

第一に、下限年齢を設定しない理由は、情報端末の多様化と利用開始期の低年齢化が進行しているためである。情報端末の多様化により、パソコンやスマートフォンだけでなく、ゲーム機や音楽プレーヤーもネットに接続できるようになり、保護者が幼児（四歳以上）を対象とした子ども用タブレットや保護者が子どもに使わせるための知育用のアプリケーションもある。そのため、「子ども」には下限年齢を設けず、

情報端末を利用可能な者とした。

第二に、上限年齢を一八歳未満とした理由は、平成二一年に施行された「青少年が安全に安心してインターネットを利用できる環境の整備等に関する法律」(以下、青少年インターネット環境整備法)において、青少年を一八歳未満としているためである。従って、本稿においても有害情報等から守るべき「子ども」の上限年齢を一八歳未満とした。

さらに、ネット社会を安全に暮らすために必要な対策を、子どもの安全を守るという観点から考える理由は以下のとおりである。

まず、社会経験が浅く、物事の是非を区別する力が未成熟である子どもを守るために必要な対策は、ネット社会に暮らすすべての人にとって必要なことであると考えられるからである。

また、日本人の体感治安は実際の犯罪件数の増減に関わらず、メディアで取り上げられる子どもの被害・加害状況に左右されるという岡本［二〇一〇］の分析結果を踏まえると、ネット社会における体感治安を向上させるためにも、子どもの安全を守ることが重要な要素となると考えられることから、本稿では、ネット社会を安全に暮らすために必要な対策について、子どもの安全を守るという観点から考えることとした。

二・二　ネットの危険性と現状の対策

ネット上には、子どもにとってだけではなくすべての利用者にとっても、さまざまな危険があることは周知のとおりである。ネット上で従来から問題となっている不正請求や他人のＩＤを使ったなりすまし

などの詐欺や犯罪行為、またウェブサイトの改ざんやネットバンキングを悪用した不正送金などのサイバー犯罪、さらに、ネットモラルの欠如による誹謗中傷、いじめ、個人情報の漏洩、有害情報の氾濫などに加えて、現在は、サイバー攻撃により国を標的にしたサイバーテロ・サイバーインテリジェンスも行われており、サイバー攻撃の対象となる範囲及び被害は拡大している。さらに、子どもという観点からネット上の安全を考える場合には、これらの犯罪に巻き込まれる危険だけでなく、子どもがネット上で不用意に有害情報に接した結果、心身が害される危険も考えなければならない。

ネット上の危険から子どもを守るための現状の対策は、有害情報の規制、学校での情報教育、家庭での指導が挙げられる。

有害情報の規制については、青少年インターネット環境整備法により、携帯電話へのフィルタリングの普及が推進され、携帯電話事業者が有害情報へのアクセスを防ぐフィルタリング機能を提供している。情報教育については、情報の利活用能力（情報リテラシー）の向上に取り組むとともに、教育現場における情報通信技術（ＩＣＴ）の活用が進められている。家庭での指導については、保護者は、子どものネット上におけるトラブルに対する関心が高く、子どもに対してネット上の危険だけではなく、法令やマナーについても十分な指導をしていると考えられている。

子どもを取り巻く環境において、それぞれ必要な対策が取られているように思われるが、現状の対策には課題もある。子どもが情報端末を利用する際に、制限を設けず自由にネットに接続させることは危険であり、また無責任でもあるが、その反対に、子どもの安全を守ることに過敏になり、ある程度の判断力を

持った子どもに対してまで過剰な制限をすることは、子どもから学ぶ機会を奪い、危険に対処する力を失わせる可能性もある。以下に現状の対策の課題について検討し、必要な対策について提言する。

三　現状の対策における課題

三・一　フィルタリングの課題

子どもたちが、ネット上の有害情報や出会い系サイトなどの不適切なサイトにアクセスすることを防ぐために、青少年インターネット環境整備法では子どもが利用する携帯電話にはフィルタリングを設定することが推奨されている。同法では、携帯電話事業者が、子どもが利用する携帯電話に対して、フィルタリング機能を提供することを義務づけ、保護者は、契約の際に子どもが利用することを事業者に申し出ることを義務づけている。

有害情報へのアクセスを規制するフィルタリングの課題は二つある。一点目は、フィルタリングの方式が、基本的には二方式、つまり、事業者が適切であると認めたサイトへの接続のみを許可する「ホワイトリスト方式」と、有害と判断されたサイトへの接続を許可しない「ブラックリスト方式」しかなく、利用者である子どもの成長段階に応じたフィルタリングが難しいことである。もちろん、保護者が個別に設定可能なカスタマイズ機能や、保護者が利用を制限したいサービスやコンテンツを選択できる機能も提供されていて、子どもの成長に合わせて適切に設定を行えばフィルタリングも画一的な規制とはならないが、

保護者がこれらの機能を十分活用しているとは言い難い。内閣府の「平成二五年度青少年のインターネット利用環境実態調査」によれば、子どもが所有する携帯電話のうちスマートフォンが占める割合が平成二四年度の三六・〇％から平成二五年度は五六・八％へと大きく上昇したのに対し、フィルタリング等の利用率は平成二四年度の六三・五％から平成二五年度は五五・二％へと減少している。同調査では、調査対象の子どもと同居している保護者に対しても調査を実施しており、フィルタリングの認知度に関しては、フィルタリングを「知っていた」「何となく知っていた」という回答が九〇・四％であったことから、保護者はフィルタリングの必要性について認識しながらも、煩雑な設定を避け、子どもの求めに応じてフィルタリングを外してしまうことが多いという現状であることがわかる。

二点目は、スマートフォンが無線ＬＡＮなどでネットに接続した場合にはフィルタリングができなくなるということである。スマートフォンのフィルタリングは、携帯電話事業者が基地局を経由する通信に対して制限をかけている。そのため、それ以外のアクセスポイントからネットに接続する場合には、フィルタリングが無効となってしまう。この対策として、事業者側も無線ＬＡＮの使用制限をするアプリケーションソフトなどの保護機能を提供している。しかし、子どもたちは目当てのサイトに接続するために、フィルタリングや無線ＬＡＮの使用制限を回避する方法を探しあて、コンビニや駅などに設置されている無料の無線ＬＡＮスポット等を使って、保護者の目の届かないところから、より危険な方法でフィルタリングなしにネットに接続するようになっている。

保護者だけではなく、情報端末を使用する子ども対して、フィルタリングの必要性及び重要性を理解さ

せなければ、形だけのフィルタリングは無意味である。

三・二　教育の情報化における課題

文部科学省が推進する「教育の情報化」は、「情報教育」、「教科指導における情報通信技術（ＩＣＴ）の活用」及び「校務の情報化」という三つの側面から構成されている。「情報教育」については、子どもたちの情報活用能力を向上させることを目的に以前から行われていたが、平成一五年度から高校の授業科目に教科「情報」が新設された。「教科指導における情報通信技術（ＩＣＴ）の活用」については、デジタル黒板、デジタル教科書、教育用パソコンや校内ネットワーク等を整備し、ＩＣＴを活用した授業を行うことを目指している。「校務の情報化」については、教員の校務用パソコンの整備、校内ネットワークを利用した教員間の情報共有等により、校務を効率化して生徒に向き合う時間を確保することが目的である。これらを内容とする「教育の情報化」における課題は、「情報モラル教育」と「情報セキュリティ対策」である。

まず、課題の一点目である「情報モラル教育」についてである。教科「情報」の詳細な内容には触れないが、情報モラルに関しては机上でネット社会のルールを教えるだけという内容になってしまうことが課題である。情報モラルは、単に記憶させるだけではなく、子どもの行動を律する規範として身につけさせなければならない。そのためには、子どもが自ら、ネット上でのモラルを欠いた行為によって現実に犯罪の被害者又は加害者になるという危険を体験し、その危険を回避するためにモラルや情報技術を学ぼうと

思うようにしなければならない。その点において、机上のみで行われる情報モラル教育は「教育の情報化」の課題である。

次に、課題の二点目は「情報セキュリティ対策」である。文部科学省が実施した「平成二五年度学校における教育の情報化の実態等に関する調査」によると、教員の校務用コンピュータ整備率は平成二五年三月で一一一・一%となっている。しかし、これは全国平均であるため、整備率が未だ一〇〇%に満たない府県もある上に、校務用コンピュータのネットワーク化がされている割合は全国平均で八〇・三%でしかない。つまり、全国の学校では校務に教員の私用パソコンが使われている場合もあり、教員間でのデータ共有のための校内ネットワークの整備も完了していないという状態である。この調査においては、学校の情報セキュリティに関する具体的な取り組み状況までは示されていないが、未だに毎月のように生徒の個人情報が入ったUSBの紛失や私用パソコンの盗難があり、子どもの個人情報が漏洩する危険にさらされている状況から考えても、学校におけるハード面での情報セキュリティ対策は遅れていると言わざるを得ない。

三・三　家庭における指導の課題

生まれながらにしてネット環境が家庭にある現代の子どもたちは「デジタルネイティブ」ともいわれている。このデジタルネイティブも、従来型の携帯電話（いわゆるガラケー）やパソコンを使って育った二〇歳代以上の世代と、スマートフォンやタブレットが身の回りにある二〇歳未満の世代に分けることがで

きる。二〇歳代以上を第一世代、二〇歳未満を第二世代とするならば、第二世代である子どもの保護者はデジタルネイティブの第一世代である。そのため、保護者もスマートフォンやタブレットを使いこなせる世代であり、ネット上の危険だけでなく情報端末の取扱い方法などの技術的なことについても知識を持っている。子どもに対して十分な指導ができる条件はそろっているが、実際は、保護者と子どもとの間には家庭での情報教育に関して認識に差があるようである。

総務省の平成二六年版情報通信白書によると、保護者の五割が家庭において情報端末やネット利用時の危険性などについて指導を行っていると回答し、かつて指導を行っていたという回答を合わせると、家庭で情報教育を行った割合は七割にもなる。しかし、内閣府が実施した子どもを対象とした調査では、有害サイトやいじめの問題などのネットの危険性について説明を受けたり学んだりしたことがあるかという問いに対して、学校で学んだという回答が八割強で最も多く、保護者から学んだという回答が次いで多かったものの三割弱にとどまっている。この調査では、対象が同一世帯でないため単純に比較することは難しいが、保護者と子どもの認識の差が現れているといえる。内閣府が行った同一世帯における調査においても、インターネット接続機器の使い方についての家庭のルールに関して、七割弱の保護者がルールを決めていると回答したのに対して、子どもが家庭内にルールがあると回答したのは六割弱であり、保護者の教えたいことが子どもには十分に伝わっていないことがわかる。

ネットに接続できる情報端末の利用開始期が低年齢化し、家庭での指導の重要性が増す中で、家庭で情報端末を使用する際のルールを子どもに理解させ、守らせることが課題である。

四　提言

これらの課題に対して、子どもの安全を守るために必要な対策について、五つの提言をする。

四・一　提言一「子どもにアクセス許可を判断させるフィルタリング方式」

フィルタリングは、ネット上の有害情報や危険から子どもを守るために有効であるが、保護者が子どもの成長に合わせた設定をしなければ、子どもはフィルタリングを単なる障害とみなし、さまざまな手段を使って回避しようとする。この課題を解決するために、本稿は「子どもにアクセス許可を判断させるフィルタリング方式」を設けることを提言する。

この方式は、「ホワイトリスト方式」や「ブラックリスト方式」等によりフィルタリングをかけるが、その後のアクセスについては利用者である子どもの判断に委ねるようというものである。具体的には、アクセスしようとしたサイトがフィルタリングによりブロックされた場合、画面上に「どのような理由でアクセスが制限されている」か、また、「アクセスする場合は責任が生じる」ということなどが表示され、利用者が同意すればアクセスを可能とする方法が考えられる。

子どもに情報を取捨選択する力をつけさせるためには、保護者や事業者が情報を「見せる」か「見せない」かを決めるのではなく、子どもに判断する材料を与えて、自分たちで「見る」か「見ない」かの判断をさせることが必要である。この方法によれば、ある程度判断力のついた子どもに対して過剰な制限をす

ることなく、子どもの自主的な判断を求めることができるため、「子どもにアクセス許可を判断させるフィルタリング方式」を新たに設けることは有効であると考える。

四・二　提言二「実戦的なリスク教育の実施」

情報教育における課題に対して、「実戦的なリスク教育の実施」を提言する。

平成二五年に総務省が全国の高校一年生を対象として実施したインターネット上の危険・脅威に対応するための能力を数値化するためのテストの結果及び利用している機器やトラブル経験を尋ねたアンケート結果を総合すると、「トラブルに遭遇した経験のある青少年のリテラシーが高い」ことが判明した。また、同調査では、「インターネット上のリスクについて学習経験がある証少年のリテラシーが高い」ということもわかっている。つまり、子どもは自分が実際にトラブルに遭遇したり、学習によってリスクを間接的に体験したりすることによって、ネット上のリスクを自分で解決しなければならない問題として受け止め、解決策を見つけ出そうとしているといえる。

子どもに実際に起こりうるネットの危険を体験させることは、子どもが、情報モラルの大切さと危険を回避するための情報技術の知識の重要性に気付き、主体的に学ぼうとするきっかけとなる。

実戦的なリスク教育行うためには、岩手県立総合研究センターが開発した教材ソフト「情報サイト八」等の活用が有効であると考える。この教材ソフトは、実際の被害に遭わずにネットのリスクを体験することができる疑似体験ソフトであり、無料で配布されているプログラムをインストールすれば、校内ネット

ワークを使って、子ども達にインターネット検索、掲示板やフィッシングサイトなど実際のネット上と同じシステムでリスクを体験させることができる。さらに、ネットオークションや電子商取引などのコンテンツもあり、学年別にリスク体験ができるようになっている。このように、安全な環境において、子どもが情報技術を学びながら実際のリスクを体験し、その対処法を学ぶことは、モラルや情報技術の知識の重要性を知る上で効果的な方法であると考える。

四・三　提言三「身分を明確に規定した情報専門員の配置」

学校の情報化に伴い、情報機器や校内ＬＡＮなどのネットワークが整備されている一方で、情報セキュリティに対する対策が遅れているという課題に対処するためには、情報セキュリティに関する専門的な人員を配置しなければならない。情報端末や校内ネットの保守を担当する「保守専門要員」、パソコン操作や故障に対応する「対応担当者（窓口）」及び授業のサポートをする「ＩＣＴ支援員」をそれぞれ任務を分けて、身分を明確に規定して配置することを提言する。

文部科学省では、学校のセキュリティポリシーの作成や情報機器のセキュリティ管理を教員に担当させ、そのサポートを、民間企業やボランティア等の「ＩＣＴ支援員」で補うとしている。もちろん、部外の人材である「ＩＣＴ支援員」の具体的な任務は、情報教育に関する機器・ソフトウェアの設定や操作、教材等の紹介、活用や作成支援が主であるが、その任務の中には、授業や校務に使用する機器の簡単なメンテナンスも入っている。

しかし、現在の情報技術や情報セキュリティ情勢の変化の速さでは、授業及び校務と情報セキュリティを両立させるのは不可能であり、また、「ＩＣＴ支援員」の身分が明確に定められていない以上、部外の者に生徒達の個人情報が入った情報端末を扱えるようにすることは情報漏洩の危険がある。

学校は、情報インフラの整備によってサイバー攻撃の対象となり得る施設であること、また、巧妙化するサイバー攻撃に対しては単にパソコンを使える程度の知識を持った者では役に立たないことを認識しなければならない。企業においては、情報の重要性や情報漏洩のリスクが認識されており、ＮＲＩセキュアテクノロジーズ株式会社が行った調査によると、二〇一三年度の企業の情報セキュリティ関連投資意欲は過去五年で最高水準となっている。さらに、独立行政法人情報処理推進機構（ＩＰＡ）の試算によれば、情報セキュリティを専門とする人材が推計で八万人不足しているということからも、専門的な知識や技能を持った人材の早急な確保が必要である。教育の情報化を進めるにあたっては、情報漏洩を防ぎサイバー攻撃に的確に対処するためにも、身分を明確に規定した専門的な人材の確保が必要不可欠である。

四・四　提言四「保護者もルールを守ること」

子どもに情報端末使用時のルールを守らせるために、本稿では「保護者もルールを守ること」を提言する。このことは、改めて提言するまでもないように思われるかもしれないが、この当たり前のことが保護者の無自覚の内に守られていないのである。

平成二六年二月にデジタルアーツ株式会社が行った調査によると、未就学児の保護者層と高校生が、他

人の「ながらスマホ」に寛容で自分自身も同様の行為をする傾向があるという結果が出ている。情報端末を利用者する未就学児が増えているにもかかわらず、その保護者が常識やルールを守っていないという結果となった。保護者が守るルールは、特別なものにする必要はなく、家の中での使用時間を決めること、他のことをしながら操作をしないことなど、常識の範囲内のものでかまわない。重要なのは、保護者も子どもと同じルールを守ることである。子どもの学年が上がるにつれて、情報技術の知識に関しては子どもの方が詳しくなるが、保護者が子どもに教えるべきことは、情報技術の知識ではなく社会の常識やモラルである。現実の世界でしてはいけないことはネット社会でもしてはいけないということを保護者が実際に体現する必要がある。子どもたちはデジタルネイティブと言われていても、情報端末の操作ができるにすぎず、社会の常識やモラルについては保護者が教えなければわからないままである。まず保護者がルールを守ることこそが、子どもにルールを守らせる前提になると考える。

四・五　提言五「情報教育の場としての図書館の活用」

家庭での指導を効果的なものにするために、保護者が情報リテラシーを身につける機会が必要であり、本稿ではその機会を提供する場として「情報教育の場としての図書館の活用」を提言する。

保護者に対して、子どもをネットの危険から守る対策等の情報を提供する機会が多いほど、その家庭でのフィルタリングの導入やルール作りが積極的に行われることが明らかとなっているものの、保護者等に対して情報リテラシー教育を行う場が少ないのが現状である。また、情報リテラシーや子どもの安全なネッ

ト利用に関しての保護者向けの情報提供の機会として、不定期に開かれるイベントやセミナーはあるが、保護者がいつでも相談できる窓口を設置している自治体は少ない。そこで、図書館を保護者等の情報教育の場として活用することが効果的であると考える。

図書館の活用に際しては、生涯学習の分野でヨーロッパの中で成功事例とされているフィンランドが参考となる。大橋［二〇一〇］によれば、フィンランドでは、生涯学習（成人教育）を国際競争力を高める国家戦略の一つとして位置づけ、国家が財政的な支援を行って、生涯学習としての情報教育を行っており、そこでは図書館が重要な役割を果たしているという。フィンランドのある図書館では、定期的に情報教育の講座を設けており、その対象を小学生以下、小学生、親世代、高齢者及び全市民と分類して開講している。講座の内容も、単にネットを使うことを目的とするのではなく、ネットを手段として使い、情報を活用するための方法を教えることに主眼が置かれていることは日本における情報教育の参考となる。

フィンランドと日本では制度等に違いがあり、すぐに実現することは難しいが、情報教育の場として図書館を活用することは、人材や設備面から見ても有効であると考える。

五　おわりに

ネット社会において、便利さと危険性は表裏一体のものである。ネット社会を安全に暮らすためには、便利さの裏には必ず危険があることを忘れてはならない。本稿では、ネット社会を安全に暮らすために子

どもの安全を守るという観点から五つの提言をしたが、それぞれの提言に共通することは、子どもたちに、安全な環境を提供することではなく、情報を正しく取捨選択できる判断力を養う環境を提供することに主眼をおいたものとしたことである。

私たちは、ネット社会においても、安全とは誰かが作ってくれるものではなく、一人一人の意識によって作り上げるものだということを改めて認識し、子どもたちがネット社会の可能性や創造性を十分に生かすことができる環境を作っていかなければならない。

【参考文献】

1 生貝直人［二〇一一］『情報社会と共同規制 インターネット政策の国際比較制度研究』勁草書房
2 ウィリアム・パワーズ［二〇一二］『つながらない生活』プレジデント社
3 NRIセキュアテクノロジーズ株式会社［二〇一四］「『企業における情報セキュリティ実態調査二〇一三』の結果を発表」http://www.nri-secure.co.jp/whats_new/2014/0127.html（八／二〇確認）
4 大橋裕太郎［二〇一〇］「『生涯学習としての情報教育』を支えるフィンランドの図書館の特徴」メディア教育研究 第6巻 第2号 pp.1-13
5 岡本吉生［二〇一〇］「子どもの心の安全と社会問題」日本女子大学紀要 家政学部 第五七号 pp.17-22
6 閣議決定［二〇一四］「世界最先端IT国家創造宣言」
7 警察庁［二〇一四］「平成二六年警察白書」
8 齋藤長行・新垣円・田中絵麻［二〇一三］「青少年の携帯電話フィルタリングの利用実態及び普及に関する研究調査―青少年の利用実態を基にした啓発教育政策の評価と提言―」電気通信普及財団 研究調査報告書 No.28 pp.184-199
9 ジョナサン・ジットレイン［二〇〇九］『インターネットが死ぬ日』早川書房

10 鈴木謙介［二〇〇二］『暴走するインターネット』イースト・プレス
11 総務省総合通信基盤局消費者行政課［二〇一三］「平成二五年度青少年のインターネット・リテラシー指標等」
12 総務省［二〇一四］「平成二六年版情報通信白書」
13 デジタルアーツ株式会社［二〇一四］「未成年の携帯電話・スマートフォン利用実態調査」
http://www.daj.jp/company/release/2014/0310_02/（八／二〇確認）
14 独立行政法人情報処理推進機構［二〇一四］「『情報セキュリティ人材の育成に関する基礎調査』報告書について」
http://www.ipa.go.jp/security/fy23/reports/jinzai/（八／二〇確認）
15 内閣府［二〇一四］「平成二五年度青少年のインターネット利用環境実態調査」
16 文部科学省［二〇一〇］「教育の情報化に関する手引」
17 文部科学省［二〇一四］「平成二五年度学校における教育の情報化の実態等に関する調査結果」

【佳作】

情報発信力の高まりによる危険とその対処

会社員
（ジブラルタ生命保険株式会社）
野村　俊介（36）

はじめに

インターネットによって、子供でも簡単に全世界に公開する情報を発信することができるようになった。ただ、未熟さや軽率さのために情報発信でトラブルを引き起こしたとしても「自己責任」とされ、その後の人生に大きな傷を負ってしまうことも少なくない。現状は、情報発信の危険の大きさに社会的な環

境整備が追い付いていないと考えられ、その問題解決に向けて、情報発信力の高まりによる危険とその対処を考察する。

一章　インターネットによる情報発信力の高まり

一・一　インターネットが個人の生活に与えた影響

インターネットの普及により、我々の生活は大きく変化したが、中でも情報の収集と発信の面での変化は顕著である。

インターネット普及前に個人が得られた情報は、テレビや新聞などのマスメディアが流したものか、自分が本などから調査して得たもの、家族・友人などからの伝聞といったものに限られていた。マスメディアが流す情報は、量こそ多いものの、広く一般に向けたものであるために自分が求める情報との関連性は低く、かといって自分で調査をして関連性の高い情報を見つけるには多大な時間と労力を要した。家族・友人からの伝聞は正確性や客観性に欠けることが多く、得られる情報の量も非常に少なかった。

だが、インターネットの普及により、ＰＣなどを使用するだけでマスメディアが流す情報よりも遥かに膨大な情報を個人が収集できるようになった。さらにGoogleなどの検索エンジンが登場したことで、検索したい単語を入力するだけで、自分が求めるものに関連性の高い情報を瞬時に得ることができるようになった。検索エンジンの機能や精度は登場以来、大きく進化し続けており、検索方法が多少適切でなかっ

たとしても自動的に訂正したうえでの結果を表示することや、翻訳機能により海外サイトの情報を日本語の検索単語に対して表示するといったこともできるようになっている[1]。

情報発信という面では、インターネット普及前に個人ができることは情報収集以上に限られていた。特定少数のグループ内で情報を伝達するのでさえ、全員を集めて口頭周知するか、紙の資料を作成して配布するか、連絡網で伝言を繰り返していくかといった方法を取るしかなかった。不特定多数に向けて情報を発信することは一般個人には不可能であり、それができるのはマスメディア内部の人間か、マスメディアが取材対象とする人間だけであった。

その状況がインターネットで大きく変わった。インターネット経由のメールなどで複数人に同じ情報を瞬時に送ることが可能になったことに止まらず、ブログやTwitter、FacebookなどのSNSの登場により、不特定多数に向けても情報や意見を発信することができるようになった。またYoutubeなどの動画共有サイトや写真共有サイトによって、文字情報だけでなく音楽や映像などの芸術作品を全世界に公開することも可能となった。

一・二　個人の情報発信力が高まったことによる効果

個人の情報発信力が高まったことによって、一般個人にとってはマスメディアを経由しなくても注目を浴びることが可能になり、自分の夢を実現させたり生計を得たりする手段が多様になった。イギリスのジャスティン・ビーバーは、Youtubeで公開した自分の歌う動画が注目を集め、それが音楽プロデューサーの

目に留まって、世界的に有名なアーティストに上り詰めた[2]。またブログの世界においても、アフィリエイト（自分のサイト上に広告スペースを設け、そこから広告料を得る仕組み）の活用などにより、プロブロガーと言われる人が国内外で現れている[3]。さらに、マスメディアが取材対象とするような著名人にも、個人としての情報発信力の高まりは効果をもたらしている。著名人が公に向けて何かを発信する際、以前は記者会見などを開きマスメディアの記者に集まってもらうことが一般的だったが、現在は自身のブログに投稿することが多くなってきた。結婚や離婚、交際や出産といった著名人のプライベートに関する話題にはその傾向が顕著で、マスメディアに向けた記者会見などが開かれないことも珍しくない。この背景には、マスメディア側の編集や制作方針によって、本来発信したかった内容とずれてしまうのを嫌うことや、自分の都合に合わせたタイミングで発信したいといったことがあると推測できる。

二章　情報発信力が高まったことによる危険

二・一　どういった危険があるのか

ここまで記載した通り、インターネットによる個人の情報発信力の高まりは色々な効果をもたらした。しかし、効果と同時にインターネット普及以前にはなかった様々な危険も生み、その危険がネット社会を生きるうえでは無視できないものになっている。ここではまず、どういった危険が生まれたのかを考察する。

情報発信という行為は、より細かく分解すると「発信主体が、特定の情報を公開し、何らかの反応を得る」行為といえる。「発信主体」「特定の情報」「反応」という三つの要素からそれぞれどういう危険があるかを導き出すと、

① 発信主体が不正になる場合の危険
② 公開すべきでない情報が発信される場合の危険
③ 受信者からの反応が想定外のものになる危険

の三つの危険があると考えられる。

二・二 発信主体が不正になる場合の危険

二・二・一 概要

「発信主体が不正になる」とは大きく分けると、対象情報の所有・管理権限を持たない他人が無断で情報を発信してしまうケースと、他人が本人になりすまして情報を発信するケースに分けられる。前者は、氏名・住所・連絡先などの個人情報や異性交遊経験・行動履歴などの生活情報を他人が勝手に公開することなどで、後者は出会い系サイトなどに自分が交際や性行為を希望するような投稿を、他人から勝手にされることなどが該当する。前者は公開された情報自体は事実であるが、後者は情報自体もなりすまされた側の意図に反するという違いがある。

二・二・二　具体的事例

(A)　「2ちゃんねる」などの匿名掲示板に個人情報を晒された事例

インターネット上の巨大掲示板である「2ちゃんねる」に、自分の個人情報を晒されてしまったという事例は数多く、個々の事例が事件として報道されることもないが、質問サイト（「Yahoo! 知恵袋」や「教えて！goo」など）には晒されてしまってどう対応したらよいかを質問する投稿がいくつも出ている[4]。

(B)　痴漢募集サイトに自分を装った書き込みをされた事例

痴漢されたい人としたい人が出会うインターネット掲示板に、国税局職員が「ゆい」という名前で痴漢行為を求める書き込みをし、乗車後の電車内で標的となる女性を選び、スカートなどの服装の特徴や「鞄二つ持ってます」など、その女性の特徴を投稿し、別男性による痴漢行為を誘発させた[5]。

(C)　ＬＩＮＥアカウントを金銭の詐取に利用された事例

無料通信アプリＬＩＮＥで、第三者のアカウントを乗っ取り、そのアカウントの友人に電子マネーを購入させようとする詐欺事件が連続的に起きた。警視庁によれば、都内だけで一〇〇件、詐取された金額は六五〇万円程度にのぼる[6]。

二・二・三　危険が生まれた背景

他人の個人情報を公開したり、他人になりすましたりするのは、その人に対して何らかの攻撃意図や利用意図があることが大半である。こうした意図自体はインターネット普及以前から人間が抱いてきたものであるが、その意図を行動に移す際の心理的・物理的障壁が低いことと、行動で得られる効果が高いことがネット社会の特質であり、この特質が危険を高めていると考える。

インターネット普及以前に、特定の個人を攻撃しようとした場合、悪口を言いふらす、中傷のビラを撒く、無視などのいじめをするといったことが行われていた。また他人になりすまそうとする場合は、電話で声色をまねる、筆跡をまねた手紙を書く、変装するといったことが必要だった。これらは準備に長時間を要し、ビラ作成などには金銭もかかる。このため、他人を攻撃したい気持ちは芽生えても、実際の攻撃行為に至るまでに挫折してしまうことが多かった。また、これらの行為にはある程度の証跡が残ってしまうため、失敗した場合の懸念や、自分の行為が発覚し追及を受けることの懸念が、心理面で実行を抑制していた。

しかし、インターネット上においては、ＰＣなどで掲示板サイトを開き、攻撃する文章を書いて投稿するだけで行為が完結する。物理的な障壁はほとんどないと言っていい。また、匿名の掲示板であれば、警察などが介入しない限りは誰が投稿したかを特定されることはなく、類似行為も多数存在しているため、心理的な抑制要因が少ない。他人になりすますことにおいても、対象者のプロフィールを把握して写

真を入手する程度のことで準備は完了であり、誰でも短期間で容易に実行可能である。

こうした背景により、ネット社会では発信主体が不正になる場合の危険が生まれている。

二・三　公開すべきでない情報が発信される場合の危険

二・三・一　概要

「公開すべきでない情報が発信される」とは、法律や公序良俗に反する行為を発信してしまうケースと、業務上の立場で知り得た情報を発信してしまうケースに分けられる。前者には飲酒運転や万引きなどを告白することなどがあり、後者は有名人が宿泊しにきたことをホテル従業員が公表してしまうことなどがある。個人情報の無断公開などと異なり、情報の発信自体で本人は被害を受けないが、勤務先企業や学校などに非難や損害が発生し、二次的に本人が被害を受けることが多い。

二・三・二　具体的事例

(A)　外食アルバイト店員が店の冷凍庫に入った写真を投稿した事例

ステーキレストラン「ブロンコビリー」の足立梅島店で、専門学校生のアルバイト店員が店の冷凍庫に入り、その画像をツイッターに投稿した。投稿後、数分でツイッター上に非難が集中し、それに同店員が反論すると非難がさらに盛り上がり、運営会社にも抗議の電話が殺到した。その後、同店員は即日解雇に

なり、足立梅島店も閉店に至った[7]。

(B) 飲酒運転したことを投稿した事例

福岡大学の学生が、「帰宅。バイト飲みやった。飲酒運転は久しぶりでハラハラした」とツイッターに投稿した。後に、自動車ではなく自転車の運転であることが判明するが、自動車の飲酒運転行為と誤解されたことが災いし、大学に抗議のメールや電話が計一八件届いた。大学側は同学生の行為を「大学の名誉を傷つける不適切な行為」と認定し、三ヶ月の停学処分を下した[8]。

(C) 有名人の購入レシート画像を投稿した事例

俳優の玉木宏氏が成田空港内の売店で買い物をした際、同店の店員が無断でレシートを撮影し、その画像を同僚に送ったところ、その同僚が「今日お店に玉木宏さんが来ました」という文章とともにツイッターに投稿した。その後、玉木氏のファンなどから非難が殺到し、店側は事務所に謝罪するとともにホームページに謝罪文を掲載した。投稿した店員は懲戒解雇、レシートを撮影した店員は派遣契約の解除の処分をそれぞれ受けた[9]。

二・三・三　危険が生まれた背景

上記のようなことが起きる背景の根本は、「目立ちたい」「世間の注目を受けたい」「特別な経験を誰か

に伝えたい」といった欲求を人間が抱くためであるのは間違いない。だが、こうした欲求自体は、インターネット普及によって出てきたものでなく、人間が本能的に抱く欲求に近い。推測ではあるが、店の冷凍庫に入る、有名人が来たことを無断で記録する、といったことは昔から起きていたことであろうし、それを友人などとの会話で自慢したり、笑い話にしたりすることも珍しいことではなかったと思う。つまり、なぜこうした欲求が芽生えてしまうのかではなく、なぜインターネットという衆人環視の場で欲求を表現してしまうのか、自主的な歯止めがかからないのかを考える必要がある。

インターネットにより個人の情報発信力は大きく高まったが、それは全ての情報が強い伝播力を持つということではなく、伝播力を持つのはごく一部の情報にしか過ぎない。かつ、どの情報にその力が働くかを誰もコントロールできないという点が、インターネットの情報発信の特徴である。既存のマスメディアであれば、マスメディア側がどの情報を流すかを絞り込み、流された情報は全て、視聴率の差はあれども、個々人のコミュニケーションとは比較にならない強い伝播力を持った。このため、マスメディアに情報が流れる際には、取材される側もその伝播力を意識し、問題になるような行動を取ることは少なかった。これに対して、インターネットでは膨大な情報がマスメディア等の絞り込みを介さずに直接流れる。その膨大な情報の中で、多くの受信者の目に留まったものが「結果的に」伝播力を持つのであり、事前の把握・選別はできない。多少刺激的な内容を発信したとしても伝播力を持たないことがほとんどであり、それ故に情報を発信する際の抑制心理が働きにくい。

さらに、受信者側の「目立ちたい」という欲求が危険の深刻さを高める。違法行為や店員の背任的な行

動を見つけた場合、その発見者の投稿も少なからず注目を浴びることになり、特別な知名度や材料がなくても比較的容易に欲求を満たすことができる。このため、半ばゲーム感覚的に、獲物となる投稿を探す人が少なからず存在しており、そうした人達の目に少しでも留まってしまえば、情報が強い伝播力を持ってしまう。

以上のような発信側・受信側双方の背景により、公開すべきでない情報が発信された場合の危険が生まれ、それが増幅されている。

二・四　受信者からの反応が想定外のものになる危険

二・四・一　概要

受信者からの反応が想定外にものになるとは、情報発信者としては一般的なこと（もしくは自分が正しいと思っていること）を投稿しただけにもかかわらず、非難のコメントが殺到したり、インターネット掲示板や他人のブログに自分への批判が数多く投稿されたりすることを指す。インターネット用語では「炎上」と言われる。有名人や社会的地位のある人の実名での投稿が対象になることが多いが、一般人でも標的になった例はあり、その場合、単なる批判だけでなく発信者の個人特定をしようとするケースが多い。

二・四・二　具体的事例

(A)　有名人が飲食店の対応を批判したことに非難が多数発生した事例

『五体不満足』などの著書で有名な乙武洋匡氏が銀座のイタリアンレストランで食事しようとした際、車椅子であることを理由に入店拒否されたとツイッターに投稿した。レストランの実名を挙げての投稿だったため、その後、同レストランに対して抗議や批判の電話が殺到する一方、乙武氏に対しても「介助を受けることを当然と思っている」「レストラン名を挙げての批判はやりすぎだ」などの非難がインターネット上に多数書き込まれた[10]。

(B)　県議が病院での対応を批判したことに非難が多数発生した事例

岩手県議の小泉みつお氏が病院の会計時に番号で呼び出しされたことに怒り、その後、病院に抗議の電話を入れたことや、会計をせずに病院を抜け出したことを自身のブログに記載した。これに対して、インターネット上では「筋違いだ」「会計せずに出てくる方がおかしい」などの非難コメントが多数書き込まれ、同氏は謝罪の記者会見を実施したが、議員辞職を求める電話やメールも計七六二件来る事態となった。その後、小泉氏は自殺に至った[11]。

(C)　2ちゃんねるの批判をした女子中学生が執拗な攻撃を受けた事例

女子中学生が自身のＨＰに2ちゃんねるなどへの批判を書き込み、それが2ちゃんねる上で話題になると、同ＨＰに非難コメントが殺到した。さらに、女子中学生の学校名、実名、所属部活、担任教師などの個人情報が暴かれてインターネット上に掲載されたり、女子中学生の写真画像がポルノ画像と合成加工されて配布されたりするなどの嫌がらせが横行した。最終的に女子中学生は2ちゃんねる上で謝罪し、ＨＰは閉鎖された[12]。

二・四・三　危険が生まれた背景

自分としては正しいと思う言動をしても周囲から批判や非難を受ける、ということ自体は普通に生活をしていてもあることで、インターネットが普及したから発生するようになった訳ではない。ではインターネット上と非インターネットで何が異なるのかというと、インターネット上ではひとたび非難が集まってしまうと、その非難の数が非インターネットとは桁違いということである。非インターネットであれば数人の陰口程度で済んだものでも、インターネット上では万単位の非難になることもある。このため、非難を受けた側は、深刻な精神的ダメージとなったり、日常生活に重大な支障をきたしたりといったことになりやすい。

インターネット上でなぜ非難の規模が大きくなるのか。それには二つの要因があると考える。一つは、非難の積み重なりが見えるということ、もう一つは、まとめサイトやネットニュースの存在である。人間

はあるものに対して批判的感情を抱いても、自分一人ではそれを表現することは少ない。講義や会議などで「何かご意見ありますか」と問われても積極的に発言する人はあまりいない。だが、自分が抱いた批判的感情と同種の意見が既に多く掲載されている場合、それに追随して自分も表明することは心理的障壁が低い。インターネット上では、投稿が文字情報として残り、また紙媒体と違って容量の制限もないため、全量が閲覧可能な状態になる。このため、非難が集まれば集まるほど、追加の非難を受けやすい状態となり、非難の表現も過激なものが増えていく。

この非難の加速度的傾向をさらに強めるのが、まとめサイトやネットニュースである。これらは、インターネット上で話題になっている事柄を、半ば自動的に収集するような形で世に広める。従来のマスメディアであれば、まず報道すべき重要な事柄であるかどうかの判断があったため、瑣末な事象が報道されることは少なかった。例えば、県議くらいの知名度の人が議会でもない場所で多少の極論を言ったとしても、取り上げられることはほぼなかった。これに対してインターネット上では、元の事象自体の重要性とは関係なく、ある程度の注目を集めたことが報道され、その報道によってさらに多くの人目に晒されることになる。目にした人が増えれば非難を書き込む人も比例的に増え、先に述べた人間の追随心理も相まって、多次曲線的に非難が増加する。

以上のように、元の発言の重要性や過激さなどとは全く無関係に非難が広がる可能性があるため、誰のどんな発言でも想定外の反応を生む危険は内在している。

三章　情報発信の危険に対して取るべき対応

三・一　危険の内容や背景からの考察

ここまでインターネット上での情報発信においてどういう危険があるのか、またそれがどういう背景で生まれたのかを考えてきた。その背景に共通するものを抽出すると、二つのことがいえる。一つは、これらの危険を生む因子はインターネット上で新たに生まれたものでなく、人間が本来的に持つものだということ。もう一つは、インターネット上では多数側・攻撃側の形成および拡大が容易で、防御側・少数側は無力であるということである。発信主体が不正になる危険は、気に入らない人を攻撃したい、もしくは自分のストレスを他人への悪戯で発散したいという欲望によるものであるし、公開すべきでない情報が発信されてしまうのは、注目を浴びたいという普遍的な欲求が因子である。受信者からの反応が想定外になるのは、自分が許せないと思うことに対して非難を述べたいというありふれた欲求が引き金となる。

また、ひとたび多数の注目を浴びれば、そのことがさらなる注目を呼び、大多数の注目を集めるのもこれまで述べた通りである。インターネット上では「数」が力であり、大多数の理不尽な攻撃に対して一つの正論で対抗したとしても、数で埋め尽くされて正論が意味を持たない。

この二点から、危険自体をなくしたり危険から完全に逃れたりすることは不可能であり、危険が顕在化してしまったら無視・静観する以外の対応は取るべきでないということが言える。人間が本来的に持つ感情などに起因する以上、その危険がない状態で社会生活を送ることはできない。そして、膨大な情報があ

るインターネット上では、注目されなければその情報は存在しないこととほぼ同義である。防御のための積極的な対応がさらなる注目を呼ぶことも考えられる以上、どんなに理不尽な攻撃であっても対抗せずにやり過ごすことが最良の対応である。

それでは、情報発信の危険とどのように向き合っていくべきなのか。それには、自分がインターネットもしくはインターネットサービスで何をしたいのか、何を求めて利用するのかを明確化し、その志向に応じた危険対処をすることが必要と考える。この志向をいくつかのタイプに分類するため、「実名を出す必要があるかどうか」と「不特定多数に発信したいかどうか」という二つの観点で、四つの分類に切り分ける。（図3－1）

(A)　宣伝志向…実名を出す必要あり・不特定多数への発信願望あり
(B)　交流促進志向…実名を出す必要あり・不特定多数への発信願望なし
(C)　参加志向…実名を出す必要なし・不特定多数への発信願望あり
(D)　傍観志向…実名を出す必要なし・不特定多数への発信願望なし

以降はそれぞれの分類ごとに、どのような危険対処が適切かを述べる。

	実名を出す必要あり	実名を出す必要なし
不特定多数への発信願望あり	宣伝志向	参加志向
不特定多数への発信願望なし	交流促進志向	傍観志向

（資料）

図3-1　インターネット（もしくは特定サービス）に対する志向タイプ分類

三・一・一　宣伝志向における危険対処

このタイプはインターネットを通じて、自分の知名度を上げて実生活のビジネスに役立てたり、注目を浴びて世間の話題になったりという願望を持っている人が当てはまる。

この志向を持つ人は情報発信の危険を受容する、つまりできるだけ気を付けて情報を発信するという以外の対処はない。自分が発信する情報はテレビカメラの前で話すのと同じことという位の意識を持ち、自分のチェック意識に不安があれば投稿する前に必ず下書き保存し、時間を空けて再度チェックすることや、第三者に確認してもらうことなどの自主的な仕組みを作る。

三・一・二　交流促進志向における危険対処

このタイプは、インターネット上独自での交流やコミュニケーションを欲しているのでなく、あくまで実社会での友人などとの交流を促進するツールとしてインターネットを利用しているという人が当てはまる。

この志向を持つ人は情報発信の危険を抑止する、つまり発信で情報が伝播する範囲を狭くしておくという対処をすべきである。ＳＮＳなどでは投稿の公開範囲を設定できる[13]ので、それを「友人のみ」にするなど可能な限り狭い範囲に設定する。また、実名を公開したサービスに他のサービスから辿ることができないようにする。具体的にはメールアドレスなどの同じ情報を双方のサービスに載せるようなことをし

ない、実名を公開したサービス以外では顔写真を入れない、片方のサービスに投稿すると他のサービスでも自動反映されるような同期機能を使用しない、といった対応をする。

こうしておくことで何か不適切な投稿をしたとしても、実生活で同様の発言をした場合以上の影響を受けることがなくなり、危険の程度を事前に抑えることができる。

三・一・三　参加志向における危険対処

このタイプは、実生活と切り離して、インターネット上での交流やコミュニケーションを楽しみたいという人が当てはまる。

この志向を持つ人は情報発信の危険を軽減する、つまりインターネット上で危険が顕在化してしまったとしてもそれが実生活に影響を及ぼさないように対処をすべきである。具体的には、プロフィールの設定などで実生活の自分の特定に繋がる情報を入れないようにする。「東京都」などの居住地であっても絞り込みには繋がり、またそれを入れることでインターネット上の交流がより楽しくなるようなものではない以上、入力を避けることが賢明である。そして、投稿をする際には自分の特定に資する情報が入っていないかどうかだけを気を付ける。逆に言うと、内容の過激さや非難を受ける可能性などに気を払う必要はない（もちろん、法律や倫理に反する投稿を積極的にしてよいということではない）。

こうした対処をすることで、トラブルが起きたとしても完全に放置してしまえばよく、インターネット上での交流が一時的にやりづらくなるという以上の影響を受けることがなくなる。

三・一・四　傍観志向における危険対処

このタイプは、単にインターネットもしくはサービス上でのやり取りを見ていたいだけという人が当てはまる。

この志向を持つ人は情報発信の危険を回避する、つまり単純ではあるが、情報発信を一切せずに、閲覧だけに徹するという対処をすべきである。インターネット全体でなくても、このサービスでは書き込みを絶対にしないなどと決めてしまえば、そこから受ける危険は完全に回避できる。

おわりに

これまで情報発信のトラブルが起きるたび、「安易な投稿をするな」といった包括的な注意がされてきたが、あまり効果はあがっていない。また、インターネット自体はこれまでにない大きな可能性を持っているもので、それから無闇に遠ざけることは大きな機会損失を生みかねない。ここで述べた「自らの志向に応じた危険の認識と対処をする」ということをネット社会での一般的教養として啓蒙・教育することで、各自がインターネットを活用しつつ、情報発信の危険をコントロールできるようになると考える。

（注）

1　Google「検索のヒントの一覧」
http://www.google.co.jp/intl/ja/insidesearch/tipstricks/all.html　二〇一四年八月二一日。

2　ニューヨークの遊び方「Youtube から生まれる新しいスターたち（ジャスティン・ビーバーくんほか）」
http://nyliberty.exblog.jp/13311030/　二〇一四年八月二一日。

3　BLOGOS「現役で活動しているプロブロガーをまとめてみた」
http://blogos.com/article/65664/　二〇一四年八月二一日。

4　教えて！ goo「2ch に個人情報を晒された場合の対処法」
http://oshiete.goo.ne.jp/qa/2851448.html　二〇一四年八月七日。
教えて！ goo「cuちゃんねるで本名を晒されて困っています。」
http://oshiete.goo.ne.jp/qa/6367087.html?from=navi_recommend　二〇一四年八月七日。
Yahoo! 知恵袋「cuちゃんねるで 友達が名前等個人情報を出されて 困っています。 通報先って…」
http://detail.chiebukuro.yahoo.co.jp/qa/question_detail/q1484978469　二〇一四年八月七日。
Yahoo! 知恵袋「cuちゃんねるで誹謗中傷されました。削除依頼するには？」
http://detail.chiebukuro.yahoo.co.jp/qa/question_detail/q1120914106　二〇一四年八月七日。

5　msn 産経ニュース「ＨＮ『ゆい』＝「痴漢募集」女性になりすました国税職員が逮捕されても「痴漢サイト」は活況の異常…被害女性は電車に乗れなくなった」
http://sankei.jp.msn.com/west/west_affairs/news/130713/waf13071318000028-n1.htm　二〇一四年八月七日。

6　毎日 jp「ＬＩＮＥ詐欺：なりすまし被害六五〇万円 都内で一〇〇件」
http://mainichi.jp/select/news/20140722k0000e040180000c.html　二〇一四年八月七日。

7 msn 産経ニュース「ブロンコビリーがバイト撮影問題を起こした足立梅島店を閉店　バイト店員に損害賠償請求も」http://sankei.jp.msn.com/economy/news/130812/biz13081215490002-n1.htm　二〇一四年八月一一日。
8 READ二CH「福岡大学、Twitterに飲酒運転告白した大学生を三か月停学処分」http://read2ch.net/news/1311707555/　二〇一四年八月一一日。
9 朝日新聞デジタル「玉木宏さんのレシート無断投稿、成田空港の店員懲戒解雇」http://www.asahi.com/national/update/0926/TKY201309260257.html　二〇一四年八月一一日。
10 NAVERまとめ　「乙武 洋匡氏 イタリアンレストラン入店拒否騒動とその後の動向」http://matome.naver.jp/odai/2136937786229094901　二〇一四年八月二一日。
11 J-CASTニュース　「病院批判ブログ炎上の岩手県議が死亡、自殺か」http://www.j-cast.com/2013/06/25177961.html　二〇一四年八月二三日。
12 2ちゃんねる から子供たちを守ろう！　「2ちゃんねるに個人情報を晒された「女子中学生」の悲劇」http://anti2ch.blog61.fc2.com/blog-entry-5.html　二〇一四年八月二三日。
13 Facebook ヘルプセンター　https://ja-jp.facebook.com/help　二〇一四年八月二一日。

【佳作】

安全なソーシャルネットワーキング・サービスの利用のために
～若者の「炎上」問題と対策～

大学院生（京都大学法学研究科二年）
葛西　悠吾（23）

一　はじめに

現代社会においては、情報化が発展し、多くの人がスマートフォンやパーソナルコンピュータ、タブレット等を通じて、インターネットにアクセスし、便利な生活を送っている。インターネットを通じて我々は世界中と即座に繋がることができる。近年広く普及してきているのが、ソーシャル・ネットワーキング・

サービス（ＳＮＳ）と呼ばれるものである。ＳＮＳとは、インターネットを用いたコミュニケーションツールの一種であり、様々なものが運営されているが、例えば、ツイッター（一四〇字以内の短文を投稿するＳＮＳ）やフェイスブック（ツイッターよりは比較的長めの文章を投稿したり、写真アルバムを作ったりすることもできるＳＮＳ）等が代表的なものである。これを用いることで、個人の日々の体験や考えを、文章・画像・動画の形で広く発信・受信することができる。ブログと比べて、いつでも気軽に、短文や画像等を発信していくことが多いのが特徴である。

ＳＮＳを用いることで、我々は、遠く離れた友人とも気軽にコミュニケーションをとることができる。これは大変便利で、有用なツールである。筆者も、多数のＳＮＳをここ五年間ほど利用しており、毎日チェックを欠かさない。だがその便利さ・有用さの反面、ＳＮＳの利用からトラブルに巻き込まれるケースも少なくない。ＳＮＳの利用によって何らかの事件の被害者や加害者にならないためには、どうすればよいのか。ＳＮＳの持つ危険性と、その危険性への対策について、中でも問題になりやすい若者のＳＮＳ利用について本稿では検討していきたい。

二　若者のＳＮＳ利用と「炎上」問題

日本国内におけるＳＮＳの利用者数は、二〇一三年末には五、四八七万人で、二〇一四年末には六、〇二三万人に達する見込みであるという[i]。利用者数が年々増加するＳＮＳだが、その利用者は、若年

層が比較的多い[ii]。そして若者は、時にＳＮＳの危険性に思いが至らず、トラブルに巻き込まれがちである。そのなかでも、二〇代である筆者自身がＳＮＳを利用していて目にすることが多かったトラブルが、いわゆる「炎上」というものである。

ここでいう「炎上」とは、ＳＮＳに対する社会的に不適切な投稿等が、突然多くの人に拡散され、主に否定的な反応が殺到するものである。「炎上」は二〇〇四年頃からブログ等であったようだが[iii]、二〇一〇年頃からＳＮＳにおいても増え始め、二〇一三年には急激に増えたもので[iv]、近年のＳＮＳ利用の問題として非常に注目に値するものといえよう。

例えば、二〇一三年に若者の「炎上」の原因となった比較的有名なケースとしては、高校生がコンビニエンスストアの冷凍庫に頭部を入れた写真をＳＮＳにアップロードしたもの、駅の線路に立ち入った写真をＳＮＳにアップロードしたもの、大学生が神社で全裸になり、写真をＳＮＳにアップロードしたもの等多くのものがある（これらを含めて、各種報道からいくつか若者の「炎上」の例をまとめた図表一を参照。ただ、筆者自身が日頃ＳＮＳで広く情報を集めている限り、あまり大きくニュース等にならないものも含めれば、頻繁に「炎上」は起こっているように感じられる。例えば未成年者が飲酒をほのめかす投稿をした、等）。

これらのケースでは、「炎上」に伴い、個人情報がそれまでのＳＮＳへの投稿・プロフィール欄等から特定・拡散される等した（匿名利用であっても、住所・氏名等を過去の投稿等から特定され、インターネット上に流出されてしまうことは多い）。その後、損害賠償請求問題に至ったり、所属団体から処分を受け

たり、逮捕・書類送検されるに至ったりしたものもある。

このように「炎上」が起こると、当該人物のＳＮＳアカウントに大量の反応が届いて対応に困ることになるのみならず、実社会における問題も発生する。ＳＮＳの利用には、このようなリスクがあるため、安全なＳＮＳ利用のための対策を講じることが必要である。

三　なぜ若者の投稿は「炎上」しやすいのか

そもそも、なぜ若者のＳＮＳへの投稿は「炎上」問題に至りがちなのだろうか。多くのＳＮＳでは、誰でも登録すれば自由に文章の投稿・写真のアップロードをすることが可能であるから、「炎上」をさけるためには、そもそもその投稿の内容が社会的に不適切なものでないようにすることが重要である。そうすると、ＳＮＳに投稿する内容について、充分な注意が払われていないのではないだろうか。

総務省の調査によれば、我が国においては、ＳＮＳの匿名利用が好まれる傾向にあるという。ＳＮＳは、その多くが、自由にユーザのハンドルネーム等を決定することができる。そして日本では匿名利用者が七割を超えており、これは他国と比較しても顕著に多い[v]。

そうすると、匿名での利用による安心感から、社会的に不適切な内容の投稿をすることへの抵抗感が無くなってしまうのではないかとも思える。

しかし、総務省の調査によれば、過去に行った社会の一般常識やモラルに反する行為を匿名で投稿で

きるとしたら投稿したいかという問いに対し、投稿したいと回答した日本人は三パーセント未満にとどまる。そうすると、匿名利用と「炎上」リスクとの関係は明らかではないといえよう。ただ、我が国のＳＮＳ利用の特徴として、特に友人や仲間内等のプライベートを意識した利用がされているとの指摘がある[vi]。換言すれば、投稿した内容を、広く「見られている」という認識が低いということである。

ＳＮＳは、友人登録、フォロー（特定ユーザの投稿を、表示するように設定することをいう）等をされている人にのみ見られているのではなく、誰でも見ることができる、いわば全世界に向けて情報を発信するツールである。なかには非公開設定も存在するものの、確実に漏洩を遮断できるわけではない。非公開設定であってもスクリーンショット、引用、画像のダウンロードと再アップロード等により広まることはありうる。実際にこれまでに「炎上」した投稿は、多くが画像の形で保存され、再投稿されているのがインターネットで確認できる（いわゆる「魚拓」である。「炎上」した投稿が削除されても、ほぼそのままの形で出回り続けることとなる）。

「友人しか見ていないし、これくらい大丈夫だろう」という認識で投稿したものが、予期せぬ人々から反応され、「炎上」に至る、というケースは多い。このような、仲間内にしか見られていない、という誤った認識が、「炎上」問題の原因の一つとなっているのではないかと考えられる。

そこで、「炎上」を防ぐための手段として、まず、若者のＳＮＳ利用に関する認識を改めさせるということが考えられる。それに加え、ＳＮＳの利用自体に何らかの技術的な制約をかけることで、「炎上」の原因となる投稿を踏みとどまらせるということも考えられる。以下では、これら二つの手段について検討

していく。

四　「炎上」を防ぐための手段

㈠　倫理的手法（ソーシャルメディア利用に関するリテラシー教育）

総務省は、一〇代から二〇代の若年層は、ソーシャルメディア利用に関するリテラシー教育を受けている者が三六・八パーセントであり、全体よりも高く、若年層に対するソーシャルメディアに関するリテラシー教育は浸透しつつあるとする[vii]。

しかし、ソーシャルメディアを利用する若年層の割合が高いのに対して、未だソーシャルメディア利用に関するリテラシー教育を受けているのは半数未満であり、また他国よりも低い。

ソーシャルメディアがこれほど広く利用されている現代社会においては、小学校・中学校等の教育段階において、徹底したソーシャルメディア利用に関するリテラシー教育がなされるべきだと思われ、そのようなカリキュラムを必修化することも有効なのではないかと考えられる。

そこでは、ＳＮＳ等への投稿は、誰でも見ることが出来るものであって、仲間内だけで共有しているものではないということを強調するべきであり、また、「炎上」に至った場合にどのような損害、それに対する制裁等がありうるのかといったことも説明することが重要であろう。軽い気持ちで投稿した結果重大な問題が生じ得るということを、広く認識させることが、「炎上」リスクを回避するためには重要であ

る（なお、そもそも社会的に不適切な行動をしてはならないという規範意識についての問題と、ＳＮＳへの不適切な内容の投稿をしてはならないという規範意識についての問題は別問題である。前者についても教育は重要であろうが、この論文で述べているのは後者の問題のみである）。

また、ソーシャルメディア利用に関するリテラシー教育は、何も学校においてなされるものに限られない。パーソナルコンピュータやスマートフォン等の利用について、家庭での指導も、重要な役割を果たすものと考えられる。例えば、子供にスマートフォンを与える際、ＳＮＳの投稿は誰にでも見られ得るものであること、実際にＳＮＳを利用して重大な問題が発生するケースがあること等を保護者が説明するといったものである。保護者が子供に分かりやすく説明が出来るように、指導用の資料を配布する教育委員会等もあるため[viii]、これらも活用して広く家庭内での指導がなされることが期待される。また、総務省も、子どもでも分かりやすく情報セキュリティを学べるホームページを開設しており、これを用いて家庭での指導をすることもできよう[ix]。

さらに、企業やＮＰＯ等の民間団体の取り組みを積極的に活用していくことも重要であると考えられる。現在、地域での啓発活動や、無料での講座提供、更には、ＳＮＳやソーシャルゲーム等の正しい使い方・利用上の注意点を学ぶことの出来るスマートフォンアプリを提供している一般社団法人、スマートフォンを利用する上での危険性を疑似体験出来るスマートフォンアプリを提供している企業等がある[x]。講座への積極的な参加がなされるよう、広くこのような取り組みを周知していくことや、ソーシャルメディア利用に関するリテラシー教育に資するスマートフォンアプリの活用が期待される。特に、スマートフォンア

プリは、実際にスマートフォンに触れながら学んでいくことができ、今後のＳＮＳを含むソーシャルメディア利用に関するリテラシー教育に大変資するものであると考えられる。

ただ、スマートフォンアプリが存在していても、そのアプリが、それを必要とする人のスマートフォンにインストールされていなければ、それを実行することはできない。そこで例えば、このようなスマートフォンアプリを、スマートフォンにプリセットした状態で販売することができるように携帯電話会社やアプリ開発会社等に働きかけることや、店頭で、子供・若者が利用する場合には店員がこのようなスマートフォンアプリの存在を説明し、インストールを推奨すること、保護者がスマートフォンを買い与える際にまずこのようなスマートフォンアプリを用いた学習を促すこと等で、学習の機会がより与えられることとなると考えられる。

以上のように、現在において行われているソーシャルメディア利用に関するリテラシー教育がより普及していくように、各企業・団体等の取り組みを有効活用していくこと、また各企業・団体等が相互に協力していくこと等によって、学習の機会が広く与えられるようにすることで、インターネット上に自己の発言を投稿することの意味やそれに伴うリスクについての若者の認識が高まり、「炎上」のようなトラブルに巻き込まれることは減らすことができるではないかと考えられる。

㈡　技術的手法（フィルタリング）

現在知られている安全なソーシャルメディア利用の技術的手法としては、フィルタリングの活用があ

る。フィルタリングとは、特に青少年の健全な育成のため、不適切なサイト（例えば、出会い系サイトやアダルトサイト等）への接続を制限するサービスのことである。スマートフォンやパーソナルコンピュータにおいて、フィルタリングソフトを複数の企業が提供しており、これらを用いることで、青少年がより安全にインターネットを利用することができるようになる。

しかしながら、このフィルタリングにはいくつかの問題点があるといえる。まず、フィルタリングの利用率はさほど高くはないということである。二〇一四年六月に情報セキュリティーメーカーにより行われた最新の調査によれば、一〇歳から一八歳のフィルタリング利用率は四四・六パーセントと、当該メーカー比では過去最高にはなっているものの[xi]、それでも半数を下回っている[xii]。フィルタリングを利用しない理由として保護者から最も多く聞かれるのは「子どもを信用している」からであり、次いで「特に必要を感じない」からであるという[xiii]。子どもを信用することが悪いとは言えないが、気をつけていてもトラブルに巻き込まれ得るのがインターネットであり、危機意識が足りないと言えるのではないか。フィルタリングの有用性を、携帯電話販売店等でしっかり保護者に伝え、また保護者は家庭で子どもとインターネット利用につき話し合い、フィルタリングを積極的に活用していくことが望ましいと考えられる。

加えて指摘できるフィルタリングの問題点としては、フィルタリングでは「炎上」の問題を防ぎきることは難しいということである。フィルタリングは、青少年に不適切と判断されるサイトへのアクセスを遮断するものであるが、ＳＮＳの利用については、個別に設定しない限り、多くの人が利用するＳＮＳサイトは不適切とは判断されないと考えられる。そして、ＳＮＳが若者のコミュニケーションにとって重

要な役割を占めている現代において、むやみにＳＮＳの利用を禁止することも暴論であろう。そこで、ＳＮＳの利用と両立するような形でありつつ、従来のフィルタリングとは異なりＳＮＳの安全な利用に資するような、新たな技術的解決を図ることはできないだろうか。

私見としては、「炎上」が主に社会的に不適切な発言によって起こることに鑑みれば、ＳＮＳへの投稿内容に着目して、フィルタリングをかける仕組みを開発し、広く普及させることが、ＳＮＳの利用継続と両立する有効な「炎上」防止手段として考えられるのではないか。例えば、「殺す」「死ね」「爆弾」「飲酒運転」等、社会的に不適切な発言に繋がりやすい単語を指定し、指定された単語に該当する単語が含まれた文章をＳＮＳに投稿しようとした場合に、注意書きを表示して一旦その内容を本当に投稿してしまって良いのかを考えさせることで、「炎上」を防止することができるのではないだろうか。特に未成年者に対しては「飲酒」「タバコ」「飲み会」等の用語も加えるといった、必要に応じた制限をかけることもできる。また、画像の投稿によって「炎上」してしまうケースもあるため、画像を添付する場合には、その内容を判別することは難しいため、一律に注意書きを表示するようにすべきであろう。

投稿内容に着目した規制をかける場合に、指定した用語が含まれる投稿自体を不可能にしてしまうと、実際には不適切な発言ではない場合にも投稿が出来なくなってしまうし、仮にこのような規制を国家が主導した場合には、憲法二一条が保障する表現の自由に対する不当な制約にもなりかねない[xiv]。青少年を保護するためのパターナリスティックな規制であったとしても、表現の自由は誰にでも等しく認められ、またそれ自体非常に重要な権利である[xv]から、その規制の態様は最低限度のものであるべきであろう。この

ようなことから、投稿を不可能とすることは妥当ではないように考えるが、注意書きを表示して投稿内容を見直させるだけであれば、そのような弊害は起こらないし、一旦見直すだけでも、「炎上」の防止には有効であると考えられる（注意書き表示機能の例として、筆者作成の図表二を参照）。

このような機能を開発した上で、その普及策としては、ＳＮＳ運営会社が、登録されている個人情報（年齢）に応じて自動で設定することや、フィルタリング提供会社が、ＳＮＳへの不適切内容の投稿を自動で検知して注意書きを表示するようなフィルタリングを提供すること、国家が法整備をして設定を求めること等によって普及させることが考えられる。ただ、国家政策としてまでこのようなフィルタリングを要求するべきかについては疑問の余地があるし、フィルタリング提供会社による規制では普及に限界もあると考えられるから、ＳＮＳ運営会社がこのような機能を開発することや、フィルタリング提供会社がＳＮＳ運営会社と協力すること等によって、一律にＳＮＳにフィルタリングを組み込むのが望ましいのではないだろうか。このような取り組みに補助金を国が与えるようにすること等も検討に値しよう。

以上のように、技術的手法としては、現在あるフィルタリングの更なる普及のため各企業等が活動をしていくことに加えて、新たなフィルタリングの開発・普及によって、より安全な、ＳＮＳを含むソーシャルメディアの利用が期待できると考えられる。

五　おわりに

携帯電話、インターネットの進歩はめまぐるしいものがあり、いつでも誰でも簡単に世界とつながることができる世の中になった。これは一方で素晴らしいことであると言えるだろう。だが一方で、その便利さ・気軽さ故に、突然トラブルに巻き込まれることもある。ここまで述べてきた「炎上」は特にそれが顕著な例である。短い文章を、気軽に、指先ひとつで投稿できるのが当たり前になり、ひとつひとつの発言が、世界に広く発信されており、危険を伴い得るということの認識が薄れてしまい、身内感覚で発言した内容がある日突然「炎上」してしまう。振り返ってみると、筆者自身、多数の「炎上」事案をその目で目の当たりにするまでは、あまり何も考えずにＳＮＳに投稿していたように思われる。

何か起こってしまってから学ぶのでは遅い。本論文で対策として検討した倫理的手法、技術的手法が、発展・普及してうまく活用されていくことで、誰もが安全にＳＮＳを利用していけるようになることを期待する。

本論文では特にＳＮＳの利用と「炎上」の問題について扱ったが、「炎上」はインターネットをめぐるトラブルのほんの一種に過ぎないともいえる。ソーシャルメディア利用に関するリテラシー教育を充実させることや、技術的な安全策を講ずることは、「炎上」のみならず、不正アクセス、闇サイト、ネットいじめ等、広くインターネットをめぐるトラブルを回避するために、重要な役割を有する手段であると考えられる。様々な危険を分析し、それに応じた教育によってその危険の認識を広め、またそれに応じた技術

的な安全策を構築していくことで、多くのトラブルを回避することが出来るのではないだろうか。

i　CT 総研「二〇一四年度 SNS 利用動向に関する調査」available at http://www.ictr.co.jp/report/20140821000067.html。

ii　総務省「平成二六年度　情報通信白書」三四五頁。

iii　伊地知晋一『ネット炎上であなたの会社が潰れる!―ウェブ上の攻撃から身を守る危機管理バイブル』(WAVE 出版、二〇〇九年)四七頁。

iv　総務省「平成二六年度　情報通信白書」二九一頁。

v　総務省「平成二六年度　情報通信白書」二九二、二九三頁。

vi　総務省「平成二六年度　情報通信白書」二九三-二九五頁。

vii　総務省「平成二六年度　情報通信白書」二九五頁。

viii　京都府教育委員会・京都市教育委員会・京都府警察本部編「子どものケータイ・スマートフォン利用に関する保護者啓発用リーフレット」(二〇一四年二月)ほか。

ix　総務省　あんしんしてインターネットをつかうために　国民のための情報セキュリティサイト available at http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/kids/index.html。

x　総務省「平成二六年度　情報通信白書」二九九、三〇〇頁。

xi　デジタルアーツプレスリリース「未成年の携帯電話・スマートフォン利用実態調査」(二〇一四年七月一四日) available at　http://www.daj.jp/company/release/data/2014/071401.pdf。

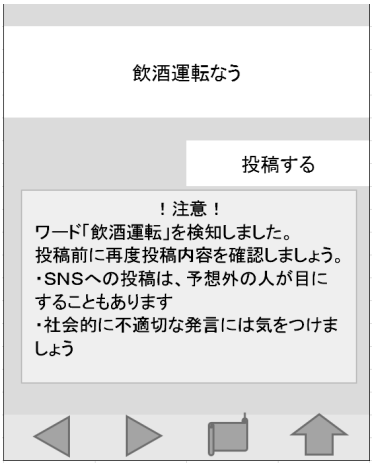
xii　内閣府「平成二五年度青少年のインターネット利用環境実態調査」(二〇一四年三月)一二六頁によっても、子どもが「機能限定携帯電話や子ども向け携帯電話」又は「その他の携帯電話」を持っていると回答した保護者(四八三人)に、その携帯電話にフィルタリングを使っているかを聞いたところ、「使っている」が四六・六%であった。

xiii　内閣府「平成二五年度青少年のインターネット利用環境実態調査」(二〇一四年三月)一三九頁。

図表 1

年月	炎上した人物	投稿内容	その後
2013年3月	大学生ら	ユニバーサル・スタジオ・ジャパンにおいて水上ボートアトラクションのボートから飛び降りるなどし、運転を停止させた行為の告白。	威力業務妨害容疑等で書類送検。
2013年6月	大学3年生	京都伏見稲荷神社で全裸になった写真。	大学は謝罪文をインターネットに掲載。学内処分。
2013年7月	高校2年生の少年	コンビニエンスストアのアイスケースに頭部を入れた写真。	当該コンビニエンスストアはアイスケース内のアイスを全て廃棄し、冷凍庫も交換し、警察に通報。威力業務妨害容疑で書類送検。
2013年8月	19歳の少年ら	ミニパトカーの上に乗った写真。	器物損壊容疑で逮捕。
2013年8月	高校生ら6人	神戸市営地下鉄の線路に侵入した写真。	神戸市交通局は警察に相談し、兵庫県警は鉄道営業法違反等の容疑で家裁送致。
2013年10、11月	16歳の少女	自身の性器の写真複数枚（複数回）。	児童買春・ポルノ禁止法違反とわいせつ電磁的記録媒体陳列の容疑で書類送検。
2014年5月	大学2年生	「僕だってのこぎりで人傷つけて回りたい」「明日授業中人を殺すことを考えている」などの発言。	警察に大学周辺を警備させたことについて威力業務妨害容疑で逮捕。

図表 2



xiv 憲法は、国家対私人の関係を規律するのが原則であるから、私企業が規制をかけること自体には直接的には憲法は適用されない。佐藤幸治『日本国憲法論』（成文堂、二〇一一年）一六四頁。しかし、私人間であっても表現行為をむやみやたらと制約することは望ましくはないだろう。

xv 民主主義国家において意見を自由に主張できることは不可欠の権利である。佐藤幸治『日本国憲法論』（成文堂、二〇一一年）二四九頁。

企業とネット社会について

パート社員
新井　光良（63）

はじめに

急速なソーシャル・ネットワーキング・サービス（以後略称：ＳＮＳ）の発展による弊害が社会問題化している。ＳＮＳを利用する従業員のささいな言動が引き金となり、取引先の企業情報や個人情報が漏洩し、企業のブランドイメージや信用失墜に繋がるトラブルが多発しているからである。

また一方で、企業はＳＮＳをソーシャルメディアの販促媒体として注力し、消費者の意見や、要望を瞬時に吸い上げることができるので、口コミ効果による商品売上増や、来店者の増加に結び付く有効な手段として活用している。その中で、企業においては、社員のプライベートな時間でのソーシャルメディアの利用を制限・管理をすることは、プライバシー侵害、表現の自由等の観点からも不可能といえる。個人がＳＮＳで日記を公表・共有するというコミュニケーション行為はごく当たり前の行為であり、それを誰も止めることはできないからである。同時に利用者は常にこのリスク特性を認識した上で、モラルある行動を取らなければならない。企業及び従業員、それと各自治体がＳＮＳのリスクにどう向きあっていくべきなのか、またその留意点について述べてみたい。

一　ＳＮＳ普及によるトラブルについて

ＳＮＳ、ブログ、動画共有サイトは総称して、ソーシャルメディアと呼ばれている。メディア利用者は、その特性を十分に理解した上で活用しなければならず、現在、その理解不足により大きなトラブルが多発し、社会問題化している。

利用者は、ＳＮＳが持つ以下の特性をまずは理解しておかなければならない。

■ＳＮＳの特性

(1)　ネットは世界中とつながっている公共の場。ネットに投稿するということは、世界中から見ることが

できるということ。

(2)　一回でもネット上に載った書き込みや写真は、世界中にいる不特定多数のユーザーが保存・拡散することが可能性であり、一旦、拡散したものは完全に収集、削除することは不可能になるということ。

(3)　顔写真や本名を公開している場合、個人の特定が容易にできてしまうということを予め認識しておくこと。

以上の特性をＳＮＳ利用者は念頭におき活用しなければならない。しかしながら、その無知さ、理解不足によって現在トラブルが多発している。ＳＮＳ絡みのトラブルは、大別すると二つに分けることができる。

一つは、出会い系サイトを利用した犯罪事件や、広告収入に関する詐欺行為。ＳＮＳがストーカー行為に悪用され、東京三鷹市の女子高校生が刃物で刺された痛ましい事件は記憶に新しい。この犯人は関西圏に住み、女子高生とはフェイスブック（以後略称：ＦＢ）で知り合っている。ＦＢは実名での登録が基本であり、もともと米国の大学生が同じ大学内での友達づくりのために開発したもので、会ったことのない人と簡単に友達になれるサービスが特徴となっている。

広告収入に関するトラブルでは、「簡単な作業で必ず儲かる」というような甘い言葉をかけ、商品詐欺に巻き込まれるケースが最近多く発生している。また、ＳＮＳの広告を見て、「サプリメント」を購入したが、いつの間にか定期購入会員になっており商品が送りつけられたという詐欺被害も多発している。

二つ目は、ＳＮＳを利用する企業の従業員が引き起こすトラブル。いわゆる不用意な書き込みや、遊

び半分での写真の投稿が炎上（他人への誹謗中傷・非常識な書き込みにより非難が殺到する状態）する事件が目立ってきている。

企業の従業員が巻き起こした事件で有名となったのは、製薬会社の社員が飲み会の席で、医薬品が不適切に使用されているとTwitter（ツイッター：ＳＮＳの一種）に投稿したところ、その発言はモラルに反する等の批判が殺到し所謂、炎上が発生してしまった。それまでの同社員のプログや過去の投稿内容から出身大学を含めた個人情報がネット上で暴かれてしまった。勤務先企業は実態を調査の上、謝罪文を公表しが、今度はその謝罪文に関して内容が「事務的」であるとして批判を招く結果となってしまった。その後、この企業は、ソーシャルメディアに関する内規を制定している。

引き続きＳＮＳというソーシャルメディア媒体との関係について、企業がなすべきこと、企業の一個人として若手社員が慎むべきことについて詳述する。

二　ネット社会と企業が取るべき行動

二―一　ＳＮＳ社会の恐ろしさ

上述の製薬会社社員は、会社の同僚との内輪話の内容を軽い気持ちでツイッターに載せてしまった。この時点で、もう少しＳＮＳに関する知識や怖さを事前に知っていればこのような騒ぎは起きなかったであろう。この社員は、ツイッターのプロフィール欄に実名を登録していた、そして、〇〇歳、女子、某

ＭＲ（医薬情報担当者）、居住地まで記していた。この情報をもとにネット利用者にＦＢで検索され、出生地、出身大学等の情報から、本人が特定されてしまった。軽率で無防備な言動といえが、情報発信者は友人や知人のレベルに読んでもらえればという安易な気持ちで書き込みをしたのだろう。ＳＮＳ社会の恐ろしさを世に知らしめた事件となった。

学生時代と違い、一企業人として注意を払わなければならない。ＳＮＳへの不用意な書き込みを慎むということである。そして、次のような言動は差し控えるとよい。いくつかの例を取り上げてみた。たとえば、

①会社帰りのスーパーで有名俳優Ａが買物をしている様子を見かけた場合。

友人に自慢したいがために、「今日、スーパーで俳優Ａが買物をしているのを見かけた。カッコ良かった」とTwitterにつぶやいた。書き込みは友人しか見ないだろうから問題ないと思って投稿をした。プライバシーを侵害する恐れが有るし、思わぬ攻撃を熱烈なファンから受ける恐れがあります。

②自社商品のＰＲをＳＮＳで情報発信をした。

自社商品の良さを宣伝になると思い軽い気持ちで、記者の公式サイトに書き込みをおこなった。内容が社員しか知りえない情報の場合、機密情報漏洩の恐れがあるため、危険な行為といえる。愛社精神が思わぬ事態に発展する恐れがあります。

③今日の出来事を仲間に知らせるためＦＢに投稿した。

ＦＢに会社名を公表しており、「今、出張先の福岡に来ています。おいしい〝うなぎのセイロ蒸し〟の

店が、取引先の隣にあったので昼食をそこで取った」と書き込んだとする。文章の前後の内容から、その場所が特定され、訪問先の位置情報や、取引先情報の漏洩に結び付く場合があります。

いずれのケースもＳＮＳの理解不足による不用意な書き込みがもたらした事例である。Twitter やＦＢなどの利用者は、スマホの急速な普及で今後も増大していくことが考えられるが、そこで問題となるのが〝ネット・リテラシー（インターネットに関する知識やマナー）である。早くからネットに親しんできた人にとっては当たり前のリテラシーも、新しく、ネット社会、ネットユーザーになった若者や、これまで親しみのなかったユーザーにとって、ネットの恐ろしさについては知識・警戒心が薄い。特に、スマホから一気にネット社会に飛び込んだ若者世代は、ネット社会の怖さがわからず、警戒心もあまりない。たとえば Twitter の場合、個人名や顔写真を公開した状態で、安易に非常識な書き込みをすると炎上するケースが最近やたらと多いし、被害を起しているのは残念ながら殆どが若者世代であるといえる。

ＳＮＳ利用者は、大震災時後に急激に伸びた。現在、ＳＮＳは、携帯電話以外の新たなコミュニティー形成手段、情報の共有媒体として拡大・成長し続けていることがわかる。

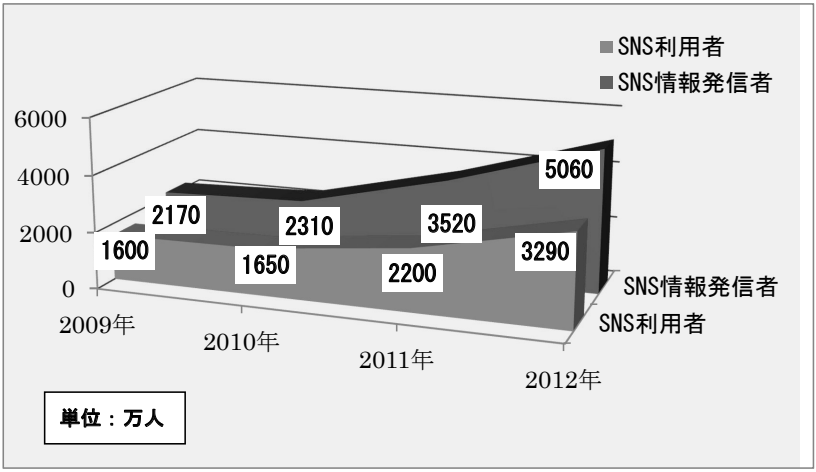
■個人（一企業人）として慎むべきこと

ネット社会において企業人としいて守るべきことは、

(1) 就業時間中は、「業務と無関係」のサイトの閲覧・書き込みをしない。

(2) ＳＮＳの利用に関しては、会社で定めた規範に従うこと。

【インターネット利用動向調査】情報元：インターネットメディア総合研究所



(3)　会社から書き込みの削除を求めた場合、速やかに対応すること。

Twitterやｆｂでの企業名の開示は、第三者にとっては「一個人（私人）」ではなく、「一企業人（公人）」となる。ネット上の発信には、細心の注意が必要である。私的な意見が「一企業人の意見」にすり替わる恐れも多いにありえるということを肝に銘じておくことである。

話は変わるが、私自身は現在二つのＳＮＳに登録している。ひとつは、趣味・旅行に関する交流が目的の情報交流サイトである。定年後、余暇が増えたので、同年代のリタイヤ世代間との共通の趣味仲間づくりの場として会員となっている。このサイトでは実名登録は必要なく、ハンドル・ネームでの登録がルールとなっている。全国各地の同年代の行動・生き方、考え方や共通の趣味についてのやり取り等楽しく活用している。

もうひとつはＦＢ。私はここにも詳細な個人情報や写真は登録していない。理由は、私的情報が故意に第三者によっ

【主な SNS の登録時に必要な個人情報】情報元：日本経済新聞社

	Twitter	FB	ミクシィ
名前	○	◎	○（友人公開）
ユーザー名（ニックネーム）	◎	×	◎
メールアドレス	○	○	○
性別	×	○	○（友人公開）
生年月日	×	○	○
住所（都道府県名）	×	×	○（友人公開）

《◎：必須項目　○：必要だが非公開可　×：不要　（友人公開）：友人には公開》

て悪用されるのではないかというリスクをはらんでいると感じているからである。なぜそう思うのか、それは、昨今、個人情報の流失・漏洩事件が後を絶たないのに他ならない。情報漏洩によって、迷惑メール等が増えるのではないかという危惧が有るからだ。

　ＦＢのようにインターネットのデータベースとその中の情報を引き出し、整理する機能を基に出会いや友達づくりができる機能は「マッチング機能」と呼ばれる。当初はキャンパス内という限定範囲であったＦＢが、世代、地域を超え一挙に全世界に広がっていた。一度広がると歯止めがきかない。ここにネット社会の恐ろしさ、危険性があるように思う。「みんなで広げよう友達の輪」も良いのだが、ＳＮＳという便利なツールには常に、「マッチング機能」が作動し、その繋がりを悪用する人間や組織が常に存在していることを認識しておかなければならない。

　私にもＦＢから「○○さんはお友達では有りませんか?」というメールがよく来る。現役時代勤めていた会社の同僚や後

輩であれば名前や写真で判断できるが、一度も逢ったことのない名前や顔立ちの人に対し、「マッチング機能」が働き、検索されてメールが送られてくるようである。考えてみれば恐ろしいことである。私の友人は東京在住で、私は現在宮城県に住んでいる。友人が宮城県や福岡県出身者の人と交互交流が成立すると同時に、その情報を元に、私の元に、交流案内メールが送られてくるのである。私個人としては、ＦＢに関してはある一定の距離を置いて今後も付き合っていくつもりである。

■ＳＮＳを使った消費者クレーム

ＦＢを含めてＳＮＳ媒体では、広告収入でサイトを維持しているといえる。画面のあちこちに広告が表示されている。利用者がアクセスすることにより、情報が分析され、ターゲットを絞りアプローチしてくる。有効な販売促進、マーケティング手段といえる。中には悪質な業者による広告も含まれているので注意する必要がある。被害が多いのはサプリメント関係の広告が多いようだ。サンプル購入ですといって初回だけ安い価格で案内し、細かい規約の中に目立たないように、一定期間後には、定期購入に移行すると記載されているものがある。初回は千円以下の商品が、二ヵ月後程立つと、商品請求額が数万円の書類が送られてくるケースもある。慌てて送金をしてしまうと会社との連絡が取れず、泣き寝入りせざるえない事件も発生している。

ＳＮＳに登録したプロフィールから嗜好、ユーザーの投稿内容等の情報からターゲットを絞り込まれてしまう。「マッチング機能」を利用したターゲットマーケティングである。似たような商法被害が今後

も増大するであろう。特に、高齢者は狙われ易いので注意が必要となる。

■ＳＮＳを使った企業クレーム

企業クレームで話題となったのは、外食チェーン店「丸亀製麺」と、ファッションの「しまむら」で起きた事件の二つだろう。二〇一三年四月、うどんチャーン店「丸亀製麺」の‘ざるうどん’を食べた客が竹製の笊にカビが生えているとＦＢに写真付きで投稿した。会社側は事実を認め、謝罪文を掲載した。その後、衛生面に考慮し、笊を竹製から、樹脂製に変更し、その商品の販売を再開した。

もう一つは大手衣料品メーカーの「しまむら」二〇一三年一〇月、ご存じのように店員にタオルケットに穴が開いていたと主婦がクレームを付け、店員の二人に土下座させ謝らせた写真をTwitter上に載せ、自宅まで謝り来いと言った。その後、主婦は強要罪で逮捕となった。

このようなトラブルを未然に防止するためには、企業は全従業員に対し、どのような書き込みや投稿をしてはいけないかを具体例を示し、基本ルールとしてハンドブック等の配布を実施するとよい。また、具体的な禁止事項（書き込んではいけないこと）を全従業員に周知・徹底しておく必要がある。

①機密情報の漏洩

・自社の未公開情報、自社製品やサービスに関するノウハウや機密情報

②プライバシーの侵害

・顧客・取引先企業、同僚・上司等の名前・年齢・性別・居住地の情報

③知的財産権の侵害

・他社商品・商標等を勝手に利用した書き込み

④名誉棄損

・個人や企業への誹謗・中傷、顧客への悪口

・根拠のない事実無根の他人への批判・不適切な行為・悪戯

⑤機微な個人情報

・思想・信条、宗教、人種、民族、身体・精神障害、犯罪・事故情報

⑥なりすまし、やらせ行為

・自社の製品・サービスを絶賛するような書き込み

従業員は企業人（公人）の一員であることを自覚し、多くの人、世界中の人が見ているのだということを自覚し行動を取らなければならない。ソーシャルメディアでの炎上を防止するために企業は、個人のネット・リテラシーを向上させるために教育を惜しんではならない。情報セキュリティ、個人情報保護、特許・商標、公序良俗、上記に掲げた①～⑥の禁止事項は総て、コンプライアンス（遵法）と密接に関連している。企業は派遣・業務委託社員やアルバイト社員の一人一人に到るまで、遵法精神を植え付けることが求

められており、従業員は、禁止事項を順守しなければならない。

ネット炎上を起さないためには、ネットを使う上での常識を忘れないこと、他人に不快感を与えるような書き込みは絶対に避けること、世間一般的にマナー違反とされるような行為や、後から批判を招く恐れが有るので自慢などをおこなわないことである。ＳＮＳ社会となった現在、個人の責任とモラルにおいて、自覚、自粛、自制を各自が持って遵法意識の高い行動をすることが求められている。

ニ－二　企業が取り組むべきこと

顧客との関係強化の有効な手段であるはずのＳＮＳも、一歩間違えると正しく活用しないと顧客のおかげで信頼も台無しとなる。

企業としては、従業員（派遣・業務委託を含む）全員にＳＮＳに関する利用ルール、規範（ガイドライン）を設けて周知・徹底を図ると同時に、この二つの事例を他山の石とし、常日頃から対応マニュアルを作成し、最悪の事態に備えておく必要がある。

どのような人が書き込みをするかというと、社内の場合は、正社員以外のアルバイト、派遣社員、入社内定者、新入社員が多いようだ。社外の場合は、クレーマー、投稿マニアからの書き込み、投稿が多い。そして、従業員の不適切な発言は、社員教育の不備、社員の質が疑われる結果を招き、特に社員でなければ知りえない業務上の情報漏洩や、プライバシーの侵害は、批判の度合が高いと言える。

そのためには、まず、自社のＳＮＳのリスク特性を知ることである。そしてしっかりとした仕組みと

してリスクアセスメントを定期的に実施することである。

それでは、どのようにしてＳＮＳのリスクに対応すればよいか。

①各企業は、その事業特性から、どのようなリスクが存在しうるのかを、まず洗い出してみる。

②次にそれを分析する。社内でも特に労働環境が悪い部署での発生が多い等、自社リスクの傾向を把握する。

③その傾向に沿って、平時と緊急時での対応の仕組みを作る。担当部署、相談窓口、責任者等を決め、体制を構築する。

④そしてマニュアルを作成し、社員に周知・徹底させていくことである。

単に、ＳＮＳのガイドラインを策定だけで終わるのではなく、総合的なコンプライアンス教育も同時に仕組みとして行う必要がある。特に、新入社員教育、アルバイト、派遣・業務委託社員への教育も徹底して実施しなければならない。何故なら、学生時代から既にＳＮＳを使いこなし身近なものになっているからである。また、そのネットワーク網を社会に入ってからの数年間はその結びつきが強いからである。企業人としての自覚が確立していないために、つい学生時代の感覚から抜け切れず、抵抗なくネットへの投稿・書き込みが多い傾向にある。裏を返せば私生活にＳＮＳが完全に浸透しているということである。炎上等のトラブルが発生する前、入社直後迄に教育することが望ましい。

また、ＳＮＳ使用にあたっては、誓約書を全社員と締結すると共に、ルールの周知・徹底を図ること。そして企業は、災害時の情報発信の対応マニュアルを作成し、日頃より訓練をしておくべきである。また、

企業にて公式ＳＮＳを開設・運営する場合には、サイト運営の目的、役割・位置づけを明確にし、サイト担当者が発言する内容に基準（公開範囲）を定め、そのコンテンツの基準も予めしっかりと決めておくことである。

ニ－三　政府・自治体に望むこと

私は宮城県民として感じていることは、今回の大震災で果たしたＳＮＳの役割は、大変大きかったと評価している。大規模災害時、固定電話や携帯電話は、通信回線がパンクする恐れがあるために、予め通話が規制されたために連絡が取れなかった。それに代わって、安否確認や救命救助連絡の役割を果たしたのがＳＮＳだった。また、災害時に生活の上で必要な物を支援して欲しいと思う被災者側と、被災者を支援したいと願う支援側との双方の橋渡しとしての役割を果たしたのもＳＮＳであった。

特にボランティア活動においては、受け入れ側の要望がホームページや、ソーシャルメディアを使用して伝えられた。ボランティア希望者は、現地の各ボランティアセンターに行く前にＳＮＳから情報（ボランティア・メニュー等）を得て、避難所の運営支援、炊き出し、壁新聞の作成・張り出し、行方不明者の張り出し、救援物資の輸送・配布、泥や瓦礫撤去、流出写真の洗浄等の各活動に参加することができた。

今回の大震災を教訓として、各自治体では平時より、地域のボランティア団体とのコミュニケーションを密にすると共に、大災害時に役立つＳＮＳを利用・運営できるネットワークの構築、そして活用できる人材を育成・訓練しておくことが求められる。是非とも前向きに検討をしてもらいたい。ハード面ばか

りではではなく、ソフト面も充実させておかなければならない。

おわりに

ＳＮＳは、インターネット上で形成されるコミュニケーション手段である。多くの人が参加し、相互にコミュニケーションを行い、同じ価値観を共有することによりコミュニティーが形成される。大切なのは、コミュニティーの形成の仕方と、ネット特性を十分に理解した上で活用することである。日本よりも早くネット社会になった米国では、ネットの特性を理解し、使いこなすための社会教育の講座が大学などに設けられ、多くの人が受講しているという。

昨今のスマホの普及は凄まじいものがある。大手三社三つ巴の販売合戦が展開されている。しかし、ラインによるいじめや自殺、不用意な投稿や書き込み、出会い系サイトを利用した誘拐・殺人事件やストーカー行為が後を絶たない。

各個人が節度とモラルを持ち、一定の距離を置いてＳＮＳに接していく必要があると同時に、我が国においても企業人はもとより、特に中高生や、高齢者へのネット・リテラシー教育を十分におこなっていくことが急務といえる。

私の提案は、スマホやタブレット端末、それらに搭載されているアプリを完全に理解している人は殆どいないと思われる。販売側は、使用者側（特に中・高校生）に対し、もっと正しいスマホやネット端末の

使い方、ＳＮＳ社会とは何か、スマホやネット端末の禁止ルール・マナー等、ＳＮＳの利用モラルについて、地方自治体、教育委員会とコンタクトを主導的に取りながら、学校に出向き生徒や、先生に対する研修・講演の場を設けて説明する必要があり、また、説明する責任があるのではないだろうか。

ネットを正しく理解し、学生時代を通して、また社会に出てからも、スマホやタブレット端末を安心・安全に利用してもらうための理解と知識を広めてもらいたい。販売大手三社は、各市町村において教育または講演を行うための実施計画を、各自治体や教育委員会に提出することを義務づけたらどうだろうか。ＳＮＳを利用した、いじめやストーカー被害が起こらぬようＳＮＳ利用に関する教育・講演を社会教育の必須項目と定め、実施を進めてもらいたい。

また、被害を受けやすい高齢者向けの対策としては、今般、法改正された悪質商法の被害から高齢者を守る「改正消費者安全法」の実効性に期待をしたい。今後の急速な高齢化によって、ＳＮＳを媒体とした犯罪も急増することが予測される。地域で配慮を要する消費者弱者を見守るネットワークの構築についても政府・自治体において進めてもらいたい。

最後に企業においては、ＳＮＳ取扱いの規定（ガイドライン）の制定と、ＳＮＳ利用の注意点・禁止事項をコンプライアンス（遵法）教育としてカリキュラムに組み込み、ｅラーニング等を活用した社員研修の場にて、実施・展開をお願いしたい。

ネット金融詐欺撲滅への取組について

無職
石田　勝啓（71）

はじめに

我国での近年急増して来たネット金融詐欺による深刻な被害は、これからのネット社会を安全に暮らす事を目指すには、非常な脅威となって来ています。

警察庁によりますと、「平成二五年だけでもネットバンキングの不正送金による被害は、過去最大の一、

三一五件、被害総額は約一四億円で、これは前年比の二九倍に上る。今回、被害が確認された約二五〇件は詐欺被害全体の約二割にあたる。警視庁幹部は、振り込め詐欺の被害を超える日も遠くないと焦燥感を募らせている。」としています(注1)。警察庁を始め関係諸機関の予防対策への懸命のご努力にも関わらず、状況が改善されない原因は、主にネットサービスの提供側、広告主、金融機関や利用者側にインターネットへの情報リテラシーは有っても、それらの総合的な連携理解の上に立った各分野の果すべき役割の詳細な明確化が不十分である事や、海外からの攻撃には捜査が及び難い等の事情がある為ではないかと推察されます。

ネット金融詐欺の発生原因は、インターネットとその仕組みを利用する検索エンジンの脆弱性等に起因し、それらに付け込んだ悪意を持った攻撃者からの様々の巧妙な悪用の結果に有ります。多発するネット金融詐欺の撲滅は、鋭意率先して取り組まれるべき緊急課題であり、私はこれらが人災で有る限り必ず撲滅し被害を大幅に激減できるものと信じております。これらの撲滅には、攻撃者の魔の手から利用者が餌食となる機会を可能な限り低減させる事で、攻撃者の攻撃意欲を削いでしまう事に有ります。ネット金融詐欺にはインターネットの脆弱性への根源的理解に基づけば、見えてくる総合的な解決策と個々の分野の果たすべき役割が詳細に明確になる筈です。

ここに私のドメイン名の重要性の根源に基づいた総合的な解決策と、各専門分野が果たすべき役割の明確化、及びそれらを安全に遂行できる日本語ドメイン名による広告と日常生活への有効活用につきまして、ご提案致します。

（注一）https://www.npa.go.jp/cyber/　https://www.antiphishing.jp/report/guideline/internetbanking_guideline.html

一　ネット利用者が先ず認識すべきこと

インターネットの仕組みとその発展的な利用の検索エンジンとは、もともと数多くの人々に広く利便性を提供するという趣旨の性善説に基づいているとされています。「～で検索」と言ったキーワードを検索窓に入力する形式の「検索エンジン」の利用は、広く目的とする情報を収集するために、中には悪意のある攻撃者によって仕掛けられた多くの偽情報や偽サイトをも容易に取り込んでしまうものであり、その中には想定外のものもあります。大手のポータルサイトによる検索エンジンの提供側は、検索量の多さも市場シェアを獲得する重要な要素となっています。また膨大な情報の一つ一つについても綿密にチェックできる訳では無く、もしそうすれば膨大なコストがかかり提供が難しくなって来ます。悪意のある偽サイトやコンピュータウイルス（以下ウイルスと記述する）をパソコンやサーバー等に取込まないようにする直接的な責任は、提供者側、広告主側、金融機関側、利用者側にありますが、利用者側以外が抜本的かつ具体的な予防対策に力を入れていなければ、利用者側に基礎的知識の欠如と油断が有れば容易に取り込まれてしまうものであります。

［ネット利用者が注目すべき基本的な注意点］

ネット利用者にとって、一般的にしてはならないとされている基本的な注意点が三点あります。

㈠　検索エンジンの検索結果や広告バナー等からの知らないウェブサイト（以下サイトと記述する）へのアクセス。

㈡　メールに表示されているＵＲＬ（注2）のクリック（特にＨＴＭＬ形式のメールなど）。

㈢　見知らぬ人からのメールや添付ファイルを開く。

しかしながら、利用者がこれらの事をそのまま忠実に実行すると、インターネットの利便性そのものが著しく阻害されてしまいかねないのも事実であります。この注意点は、危険であるかも知れないので実行するな と言う事であって、現在の使用環境である程度のセキュリティを確保する為には、利便性が阻害されるのはやむを得ないと言う事でしょう。

しかしもしも安全性が向上できる方法が有って、簡単に安全確認ができれば、この注意事項も実行できるようになる筈のものと考えます。

［ウイルス対策ソフトが無効な攻撃もある］

一般的には利用者が、インターネット、特に検索エンジンを積極的に利用すればする程、当然その脆弱性を利用して仕掛られたネット金融詐欺サイトに嵌められたり、サイバー攻撃によってウイルスに感染す

るリスクは増大するとされています。ウイルス対策ソフトなどを提供する多くのソフトベンダーも、ウイルスによる攻撃に対応した商品開発と販売をしています。しかし市販のウイルス対策ソフトは、新商品が販売され広く行き渡るようになるのと同時に悪意のある攻撃者にも出回り、彼らも常にセキュリティを通過するための開発研究をしていて、隙が有れば虎視眈眈と攻撃の機会を狙っています。

パソコン等にインターネットの脆弱性を補強する為へのウイルス対策ソフトのインストールとその更新は不可欠ですが万能では無く、対応が無力なものもあります。例えばネットバンキングでの金融決済の際に、専ら利用者のＩＤとパスワードや暗証番号、クレジットカード番号等の重要な本人認証情報を、正規や公式サイトの画面とそっくりの偽画面を提示して入力させる事によって窃取してしまう単純な攻撃で、ウイルスに依存しないものや簡単にセキュリティを通過してしまう程度の増加傾向にある不正プログラム（注3）、一部の単純形式のDDoS攻撃（注4）、そして全く新しい形式のサイバー攻撃等です。一般的な利用者の認識では、利用者側のパソコンに金融機関等から出されている最良のウイルス対策ソフトを入れて更新さえしっかりしていれば何もかも安全だとの誤解が多いのです。

［本人認証情報の入力前に必要な確認］

このような攻撃に利用者が対処すべき最低限必要な事は、後の［利用者の確認責任］の中でも述べていますが、本人認証入力画面の外見が正規や公式のＵＲＬのサイトと全く同一であっても、本人認証情報を入力する前に画面の左端上のＵＲＬアドレス窓でのＵＲＬやドメイン名（注5）が、正規や公式のもの

と一致しているかどうかの確認が不可欠です。利用者の安全の為には、このような予備知識が利用者側に事前に必要であって、利用者がウイルスの無いフイッシングサイトの入力画面とは知らずに、入力した個人情報を他人に知られて金銭を窃取されてしまう事も有り得るのです。

（注2）http://ja.wikipedia.org/wiki/Uniform_Resource_Locator
（注3）http://www.ipa.go.jp/security/txt/2014/q1outline.html
（注4）http://ja.wikipedia.org/wiki/DoS%E6%94%BB%E6%92%83
（注5）https://www.nic.ad.jp/ja/dom/system.html

二　ネット広告等の脆弱性を悪用したネット金融詐欺

インターネットの脆弱性に起因するネット広告、検索エンジンやその利便性も脆弱性もそのまま引き継いでいる検索連動型広告（注6）でのネット金融詐欺の被害が目立っています。

検索エンジンや検索連動型広告の脆弱性については、海外のウイルス対策ソフトを提供する多くのソフトベンダーや、国内でもＩＰＡ独立行政法人である　情報処理推進機構（https://www.ipa.go.jp/）等のセキュリティ専門機関でも、認識されて来ています。既に、ＩＴセキュリティの専業ベンダーとしては世界一の規模のマカフィー社は「検索エンジンの安全性に関する調査報告」で「検索結果の四％は危険サイト」と二〇〇七年六月から警告して来ました。さらに検索連動型広告については、「検索エンジンにキー

ワードを入力して上位に現れるサイトの危険度を調査したら、広告として表示されるサイトは、そうでないサイトの二・四倍も危険率が高い」とし、「悪人が検索連動型広告を使って被害者をおびき寄せて、コンピュータウイルスを感染させたり、ソフトウエアの不当な押し売りなどをしていることが数字で裏付けられた。検索エンジンの提供会社は広告により利益を得ているので、広告のチェックが甘くなりがちだ」と該社は指摘して来ています。

この数値は求めるサイトに到達する為に、画面左端上のＵＲＬアドレスバーにＵＲＬやドメイン名の入力の方が尊重されて利用頻度が高い米国での調査結果であって、日本のように殆どネット広告、検索エンジンや検索連動型広告の使用に頼っている状況では、実際はもっと数値が多い筈です(注7)。

最近の被害例では、yahoo の検索連動型広告に京都銀行（本店・京都市）のインターネットバンキングの取引画面を装った、偽検索連動型広告のフィッシングサイトが掲載され、これに利用者がアクセスして騙され、ＩＤとパスワードや暗証番号等が盗まれて不正送金により金銭が窃取される事件がありました。(注8)またこれに類似のネット金融詐欺例もあり、広告主の正規や公式のサイトを、悪意のある攻撃者がそのままコピーして外見上は全くそっくりのフィッシングサイトを簡単に作成し同時に検索エンジン最適化対策の情報もコピーしてネットに仕掛け、利用者が、事業主が広告しているキーワードで検索すると、正規や公式のサイトと同様にそのフィッシングサイトを検索結果の上位に紛れ込ませる手口です。検索結果に出てくる複数のサイトの中には、あらかじめ広告主の正規や公式のＵＲＬやドメイン名が利用者に提示されているもの以外の出所不明なものの中には、フィッシングサイトがあるかも知れないのです。さ

らにネット広告の顧客誘導によるネット金融詐欺で、ドライブバイダウンロード（注9）と言われ、例えば「パソコンの性能が低下しています」などと書かれた偽りのセキュリティソフトを買わせる広告にも注意が必要です。そして名古屋銀行（注10）や、webmoney（注11）等のネット詐欺事件も報告されています。もしも利用者が出所確認を怠ったサイトがフィッシングサイトや偽サイトであり、これに嵌って被害に遭うリスクは、広く存在しています。

（注6）http://ja.wikipedia.org/wiki/%E6%A4%9C%E7%B4%A2%E9%80%A3%E5%8B%95%E5%9E%8B%E5%BA%83%E5%91%8A

（注7）http://www.nikkeibp.co.jp/style/biz/skillup/spam/070618_50th/

（注8）http://www.mcafee.com/japan/about/prelease/pr_07a.asp?pr=07/06/05-1

（注9）http://www.asahi.com/articles/ASG2P6F5JG2PULFA035.html

http://ja.wikipedia.org/wiki/%E3%83%89%E3%83%A9%E3%82%A4%E3%83%96%E3%83%90%E3%82%A4%E3%83%80%E3%82%A6%E3%83%B3%E3%83%AD%E3%83%BC%E3%83%89

（注10）http://blog.livedoor.jp/antitheft/archives/1761311.html

（注11）http://www.nikkei.com/article/DGXNASFK1400U_U4A710C1000000/

三　ドメイン名の信頼性の根拠

任意のドメイン名が世界に一つしか無い事は、それ自体が信頼性の根拠となり得ます。特に日本発のド

メイン名のトップレベルドメイン（注12）で、例えば「.jp」、「.co.jp」、「.ne.jp」等の信頼性は、高いとされています。Whois 検索によって、登録者或いはこれを管理するレジストラが確認できる事で出所が明確となり、ドメイン名をＵＲＬアドレス窓に入力する事によって出てくるサイトは、登録者か登録者の代行者がサイトを立ち上げている限り、出所が明確となるので信頼性の根拠となり得ます。なぜなら万が一、サイトに不正行為が有って被害が発生すれば責任が糾弾されて、たとえドメイン名の削除やサイトの閉鎖後であっても、不正なサイトが存在していた履歴を基に被害者等から登録者に対して、責任の追及や損害賠償の請求等が発生してしまう可能性があります。また損害が大きければマスメディアで糾弾されて二度と信用の傷がついた同一のドメイン名を使用する事が出来なくなる恐れも生じます。特に日本発のドメイン名は、出所が明確な為不正行為が行われにくいと考えられます。

そしてトップページが正規や公式のもので、サイト内リンクページでのトップページのＵＲＬやドメイン名の最後に／で区切った後のディレクトリだけの追加や変わるものは信頼できます。

しかし外部リンクサイトでＵＲＬが全く変わり、トップレベルドメインが、「.com」「.net」等は、海外からの可能性もあり、その場合は注意が必要です。

（注12）http://ja.wikipedia.org/wiki/%E3%83%88%E3%83%83%E3%83%97%E3%83%AC%E3%83%99%E3%83%AB%E3%83%89%E3%83%A1%E3%82%A4%E3%83%B3

四　ネット広告の脆弱性補完によるネット金融詐欺低減

ネット広告や検索連動型広告等の脆弱性を悪用したネット金融詐欺の被害を撲滅し安全を確保してゆく為には、次の五つの各専門分野の個々の責任に於いて、以下の様な果たすべき役割が不可欠です。すなわち出口となるネット広告のポータルサイト提供者側、広告を依頼する広告主側、金融決済を司る金融機関側、入口での利用者側の各々と、それらの全体を横断的に包括する行政側の統合的な支援が必要となり、各分野での実践されるべき役割の周知徹底、横断的な行政指導や法整備化等が、完璧に図られる事が大切であると考えます。

[提供者側の確認責任]

ポータルサイトの提供者側は、広告主が掲載を希望する広告サイトの審査の際に、トップページ及び金融決済の本人認証入力画面との両方に於いて、次の内容の事前確認が不可欠です。

㈠　画面左端上のＵＲＬ確認窓でのＵＲＬやドメイン名が、正規や公式の金融機関のものと一致している事。

㈡　本人認証入力画面のＵＲＬが、https://で始まるＳＳＬ暗号化通信による認証画面で有る事。またサーバー証明書鍵マークは、ロック状態でクリックして出てくるポップアップ画面の認証内容が、信頼できる認証機関が公に発行しているものである事。

㈢　ポップアップ型の本人認証入力画面に正規や公式のＵＲＬ表示の無いもの。

以上の確認ができなければ、ネット上への掲載を拒否する責任がある。

（京都銀行のような事件に対する広告提供者側の責任は、益々増大する被害を防止すべき社会的責任の増大に伴い、相応に増大してゆくものと思われます。真偽確認のチェックが甘かったり確認漏れのミスは単に民事責任だけで無く重過失責任や、認識していたが敢えて実行されなかった未必の故意と言う社会的義務不履行の解釈から、刑事責任も今後は求められる可能性があり得ると考えます。）

［広告主側の周知責任］

㈠　テレビや新聞等でのマスメディアで顧客に周知させる「広告キーワード」の掲載の際に、併せてトップページ及び金融決済の本人認証入力画面での正規や公式のＵＲＬやドメイン名を必ず表記する。

㈡　さらに注意事項として、「広告キーワードによる検索結果のサイトから当該のＵＲＬやドメイン名のサイトだけを選択するよう」併記する

（現在は、単に「広告キーワード」だけの掲載のものが多く、極めて危険な状態です。）

［金融機関側の安全責任］

㈠　預金の利用者宛てに、ＵＲＬの真偽確認の為に必要な本人認証情報の入力画面のＵＲＬを親展で本人宛の郵送にて通知する。

勿論この場合、念の為届いた郵便物が郵送元の金融機関のものに間違いないか利用者が確認できる手だてが必要で、金融機関しか知り得ない利用者の口座番号等の一部や個人認証情報の一部を表記して、利用者の確認を得る事はやむを得ない。

（この通知により、利用者が本人認証入力画面のＵＲＬを知る事ができます。また金融機関のトップページが正規や公式のものでもＳＳＬ暗号化通信では無い為に、攻撃者から正規の本人認証入力画面にそっくりなフィッシングサイトの外部リンクが強制的に貼付けられた場合での安全確認にもなります。）

㈡　金融機関が提供するウイルス対策ソフト更新の際のポップアップ画面情報に、ソフトベンダーまたは当該金融機関の正規や公式のＵＲＬを併記する。

（これは万が一、偽サイト画面からの更新情報ならば危険な為、別にソフトベンダーや金融機関のサイトで、ウイルス対策情報についての真偽確認ができる為のものです。）

㈢　セキュリティ対策は最も不可欠で、特にファーミング攻撃（注13）やＳＱＬインジェクション攻撃（注14）等にも注意し、広告主ともサイト管理を含め密接に連携して安全対策を万全にする。

［利用者側の遂行責任］

利用者側は、トップページ及び金融決済の本人認証入力画面との両方で、安全手続きの補完ステップが不可欠です。

㈠　画面左端上のＵＲＬ確認窓でのＵＲＬやドメイン名が、正規や公式の金融機関のものと一致している事。

㈡　本人認証入力画面のＵＲＬが、https://で始まるＳＳＬ暗号化通信による認証画面で有る事。またサーバー証明書鍵マークは、ロック状態でクリックして出てくるポップアップ画面の認証内容が、信頼できる認証機関が公に発行しているものである事。

これらの本人認証入力画面の未確認が重大な結果となり得る事で、以上の確認が得られないものは、本人認証情報のＩＤとパスワードや暗証番号やクレジットカード情報等の入力を絶対にしない。

（京都銀行の被害例の場合、正規や公式のＵＲＬやドメイン名の基本形が、

www.kyotobank.co.jp/

であり、そしてさらに本人認証入力画面では、金融機関から利用者への提供や、別に正規や公式のトップページのＵＲＬで入力画面を立ちあげて確認した正規や公式のＵＲＬの本人認証情報の入力画面が、

https://www.parasol.anser.ne.jp/ib/index.do?PT=BS&CCT0080=0158

で有る事を確認し、入力画面のＵＲＬがこれと一致している事を確認します。）

㈣　バナー広告等のネット広告やリンクサイトでクリックする事によって立上って現れるポップアップ型の本人認証入力画面があり、左上のＵＲＬ確認窓に正規や公式のＵＲＬやドメイン名の表示が出ない

ものは、絶対に入力しない。

（これらは悪意のある攻撃者が仕掛けるフィッシングサイトの場合が殆どで、本人認証情報が知られる事から金銭が窃取されますし、個人情報は犯罪者間でも広く知れ渡る事にもなり非常に危険です。）

㈤　セキュリティ対策は不可欠で、特にＭＩＴＢ（マンインザブラウザ）攻撃[注15]は、本人認証情報が攻撃者に知られて預金や個人情報が窃取される恐れがあり、通常の対策ソフトに金融機関推奨ソフトは最低限必要である。

［行政側の支援］

（関係諸機関による安全対策情報、行政指導や教育指導、広報、法整備等）

ネット金融詐欺の発生原因は、これ迄、提供側、広告主側、金融機関側、利用者側の以上のような役割の不履行に起因するところが多かったので、行政では、あらゆる機会を通じてこれらの役割情報の周知徹底が図られるべきであると考えます。

そしてあらゆる業種での全ての本人認証情報の入力を求める金融決済画面のネット広告、中でも特にポップアップ広告について、画面左端上のＵＲＬアドレス窓での表示が無く真偽確認が出来ないものは極めて危険な為、広告主側に対して、国内での使用は禁止できるよう法整備化が望ましいと考えます。

（注12）http://ja.wikipedia.org/wiki/%E3%83%95%E3%82%A1%E3%83%BC%E3%83%9F%E3%83%B3%E3%82%BO

（注14）http://e-words.jp/w/E382A4E383B3E382B8E382A7E382AFE382B7E383A7E383B3E694BBE69283.html
（注15）http://securityblog.jp/words/790.html

五　広告は安全第一なら、断然日本語ドメイン名広告

［ＵＲＬの真偽確認がしやすく、直接的使用は真偽確認が不要］

遍く使用されている日本語は、一般の人は勿論、悪意のある人にも区別なく使用されているので、悪用される危険性も常に孕んでいます。しかし国内のネット社会では、任意の日本語の最後にトップレベルドメイン、例えば「.jp」が付く事で、最も保障された安全と信頼性、そして利便性の高い日本語ドメイン名[注16]となります。

英数字ドメイン名を日本人用の利便性に特化した日本語ドメイン名を広告に直接活用する事でＵＲＬの真偽確認が不必要となり、「広告は安全第一なら、断然日本語ドメイン名広告」なのです。勿論金融決済の本人認証入力ページは、トップレベルドメインが「.ＪＰ」による「日本語ドメイン名×ＳＳＬ暗号化通信」であるべき事は必須で、これにより海外からの攻撃者を撃退し、出所が明確である為リスクの低減に大きく貢献できます。

実用上は、現在の検索エンジン、ネット広告や検索連動型広告での脆弱性が伴う未完成システムを、ド

メイン名または日本語ドメイン名で安全確認を補完する形の間接的補完使用か、または完成度の高い日本語ドメイン名に置換して直接的使用をするかのいずれかの形での使用ができます。

㈠　間接的補完使用の有効例

利用者が検索エンジンや検索連動型広告を利用して、安全に目的のサイトに到達するには、検索結果に出てくる複数のサイトから、出所が明確なＵＲＬやドメイン名で安全確認を補完する二段階の手順が不可欠です。金融機関の例では、あらかじめ金融機関からＵＲＬ情報を入手してＵＲＬ確認し一致照合すれば間違い無いのですが、通常のＵＲＬの場合は、利用者にとって長い複雑な英数字文字の羅列が多くまた一見した瞬間的な理解性が悪くて、確認しづらい筈です。

京都銀行の例の場合、

トップページの正規や公式のＵＲＬの基本形が、

www.kyotobank.co.jp/

ですが、一見した認識性が優れて確認し易い日本語ドメイン名を利用すれば、

例えば、

京都銀行.jp

となり、本人認証入力画面では、ＵＲＬの基本形がＳＳＬ暗号化通信の、

https://www.parasol.anser.ne.jp/ib/index.do?PT=BS&CCT0080=0158

であり、利用者が確認を怠れば重大事になり得るので、この正規や公式のＵＲＬと、ネットでの画面左上のＵＲＬ確認窓のＵＲＬと真偽確認が必要ですが、複雑で長い英数字が羅列したこのＵＲＬは相当確認しづらい筈です。しかし日本語ドメイン名を活用する事で、同様に短く簡単に確認し易くできます。例えば、

https:// 京都銀行本人認証 .jp

等とすれば、利用者がわかりやすくて覚えやすくこれと一致照合するものだけに、ログインすれば良い事になります。

その理由として、確認の際、ラテン文字に代表されるアルファベットが一つの音価を表記する音素文字で、一文字ずつ漏れなく確認する必要がありますが、決まった語句でもスペルミスをする場合があり、時間と労力を要し確認ミスも発生しやすいのです。これに対して、日本文字の特に漢字は、一字が一義を表すことを重視した表意文字で、それぞれが個別の意味を持ち、熟語等も用い短くでき一見した瞬間的な理解性が高く、確認ミスも極めて少なくなります。また漢字に間違いが有れば原理上日本語ドメイン名にはならない為有利です。

特に、スマートフォン、携帯電話やタブレット端末等での狭い画面使用での一見した視認性や理解性は、抜群に優れています。

［検索エンジン利用での偽装ＵＲＬによる騙し対策にも有効］

検索エンジン利用の検索結果でのサイトのＵＲＬ真偽確認に、正規や公式のＵＲＬに似付かせた偽装ＵＲＬにも注意が必要です。サイト運営側が広く出所が明確な正規や公式の日本語ドメイン名やそれで構成されたＵＲＬを極力利用し、利用者は、出所が不明なものでも、ＵＲＬが成立するドメイン名との基本構成を良く理解し、正規や公式のＵＲＬを偽装していないかどうか、また内部リンクか外部リンクであるかどうかを判断して、疑わしいサイトは極力排除し、問題の無いサイトだけを活用する姿勢が有れば、リスクが低減できる筈です。

例えば、仮に「幸せ銀行」といった銀行とそのサイトが有るとします。この正規や公式のＵＲＬが、

http://www.siawaseginnkou.jp

だとします。さらに、

http://www.siawaseginnkou.jp/abc

で　/abc 以下はディレクトリ、正規や公式の内部リンクのサイトとわかり問題がありません。しかし、

例えば、上記の正規に似させた偽装ＵＲＬサイトとして

http://www.abc.com/siawaseginkou.jp

は、これが検索エンジン利用の検索結果ならば正規に似させた全く別のサイトなので、決して選んではいけませんし、もし正規サイトの画面クリックの結果ならば外部リンクに飛んでいる事が一目瞭然です。/siawaseginkou.jp 以下は、外部サイト abc.com のディレクトリです。また、

http://www.siawaseginkou.com

では、siawaseginkou.com は、例えばｎが一文字抜けている類似文字か誤字なので検索結果なら偽装ＵＲＬサイトで、正規サイトの画面クリックなら外部リンクのサイトです。これが日本語ドメイン名であれば、

幸せ銀行.jp

で、偽サイトに騙されにくくなります。内部リンクは例えば、

幸せ銀行.jp/abc

となり当該サイトと外部リンクとの区別が極めて視認性が良いため判別し易く、/abc 以下はディレクト

リ、内部リンクなので問題がありませんが、

http://www.abc.com/siawaseginkou.jp

これが検索結果ならば全く別の偽装ＵＲＬのサイトで、選んではいけませんし、正規サイトの画面クリックの結果ならば、外部リンクである事が一目瞭然です。

㈡　直接的使用の有効例

［正規や公式サイトの真偽確認が一切不要、完成度の高い安全性と利便性が有る。金融決済が必要な分野では必須］

利用者が検索エンジンや検索連動型広告を利用してサイトの真偽の確認作業数が多くなると面倒になって、この手順を無視したり省略すれば、当然ネット金融詐欺等に巻き込まれる可能性は増大します。

そこで、特に金融決済が求められるネットバンキングやネットショッピングの分野では、最初から当該金融機関名や事業者名をネット広告、検索連動型広告に使用されるものと同一名称か類似の日本語に置き換えた、日本語ドメイン名広告を優先的に採用する方が、遥かに顧客満足と安全視点から有効です。

これ迄通常使用されている英数字のドメイン名が、日本人には極めて難解で不便な為に日本では広告での使用には全然耐えられず、一方では脆弱性が高くフィッシングサイトに嵌る危険性が高いと分かってい

ながら、検索の利便性も有ってやむを得ず検索連動型広告等を使用せざるを得なかった訳です。しかし此処に来て日本人にはサイトの真偽確認の不要さと利便性から、直接的な日本語ドメイン名広告が有効となって来ました。

主管理推進機関の日本レジストリサービス（ＪＰＲＳ）（http://jprs.co.jp/）や日本語ドメイン名協会（http://日本語.jp/）でも、日本語ドメイン名の基本的特徴として、従来の英数字ドメイン名とは明確に異なり、日本人に馴染みのある日本語なので、「わかりやすい」・「覚えやすい」事が実証されています。欧米では、英数字のドメイン名が長年そのまま広告にも使用され続けられているので、同様に日本語ドメイン名もまたそのままで日本人向けに直接マスメディアによる広告でも、充分使用に耐え得る事になる筈なのです。

コスト的には、検索連動型広告が必ずマスメディアへのキーワード広告料が必要で、加えてクリック数によって広告料金が決まるネット掲載システムで高額の広告料がかかります。

日本語ドメイン名は初期登録料やその後の維持更新料だけの僅かな年間約数千円以内の費用で、広告料の安い小スペースのバナー広告等で済み、安全性効果をプラスした対費用効果が遥かに安くなる筈です。

日本語ドメイン名広告は、ＵＲＬ窓に直接に直打ちすれば、出所の真偽確認が不要で直接的に求めるサイトへの到達作業も一回で済み、提供者、広告主と利用者にとって一段と安全確実で低コストで済みます。

［電子メールでのＵＲＬ確認にも不可欠］

電子メールでのＵＲＬの紹介や案内は、通常長くて複雑な英数字の羅列なので、これが正規や公式のものであるかどうかの真偽確認は、利用者にとって困難な場合が多いのです。しかし短く理解し易くなる日本語ドメイン名構成のＵＲＬを使用すれば、正規や公式のサイトかどうかの真偽確認が容易または不必要となって、今迄のように、未知のＵＲＬや偽装ＵＲＬをクリックするリスクは、大きく低減されます。

多くの銀行では登録済だけでまだ運用実施はされていませんが、運用実施されれば、例えば、

京都銀行.jp　　や　　南都銀行.jp

の様に利用者がＵＲＬ窓に入力し、本人認証入力画面は、トップページからログインして引出せるのですが、直接直打で、

https://京都銀行本人認証.jp　　や　　https://南都銀行本人認証.jp

等と入力すると完璧に近くなります。

一般論として「.jp」の日本語ドメイン名の使用は、海外からのネット金融詐欺も含めた様々なサイバー攻撃を拒絶してウイルス感染のリスクを低減し、国内でも出所が明確な事等によるシナジー効果の為、直接的に広く使われれば使われる程、増々日本国内全般での安全性や信頼性が、必然的に向上してゆくもの

と考えられます。

以上私が述べて来ました方法は、勿論さらに個人、企業や官公庁等からの重要情報の窃取や改竄対策にも適用できます。例えば平成二十八年から全国一斉に実施予定のマイナンバー制度についても、完璧な安全性と信頼性が求められる為、例えばトップページを

マイナンバー制度.jp

本人認証入力画面は、必ず「日本語ドメイン×ＳＳＬ暗号化通信」形式の、

https://マイナンバー制度本人認証.jp

等とすれば良く、使用の利便性も向上します。

［ドット日本を採用し、広告使用の完成度を高める］

隣国の中国や韓国では、完成度の高い安全対策と広告利用への観点から、既に中国語ドメイン名のトップレベルドメイン「ドット中国」が二〇〇九年一一月から、また韓国語ドメイン名のトップレベルドメイン「.한국（ドット韓国）」が二〇一一年五月から運用実施されていて、全て全角入力ができます。日本では日本語ドメイン名のトップレベルドメインの「ドット日本」の利用への準備は、日本レジストリサービス（ＪＰＲＳ）、日本語ドメイン名協会に於いて、既に二〇一一年六月に事実上完成していますが、あと

一歩のところで総務省の承認が得られていないため、残念ながら未だに利用できない状況にあります。これが実現できると、例えば、

南都銀行.jp　　が　　南都銀行。日本

となり、全て全角入力もできる事でスマートな表現となって、完成度の高い安全性、利便性、高理解性の相乗効果で広告価値は飛躍的に向上するものと思われます。

（注16）http://ja.wikipedia.org/wiki/%E6%97%A5%E6%9C%AC%E8%AA%9E%E3%83%89%E3%83%A1%E3%82%A4%E3%83%B3%E5%90%8D

六　日本のネット社会を安全に暮らせる日本語ドメイン名の積極的活用

インターネットが原理的には通信網で無限大に繋がっていて、使用される基本ＯＳも一般利用者、企業や官公庁を問わず共通である為、ネット金融詐欺でも過少評価は危険です。増え続ける被害に有効な対策を打てないまま放置しておけば、海外からの攻撃手口がさらに他分野にまで多種多様に拡大し、多数の一般の利用者のパソコン等のネット関連機器を狙う大規模無差別のサイバー攻撃にまで進展してしまう事も有り得ます。

極秘裏に進行するサイバー攻撃によって感染が感染を呼び、占領された数多くのそれらの機器を踏み台

として、さらに金融、電力、通信、放送等の国家の重要インフラや原子力発電所、自衛隊基地等への、防御が難しいDDoS攻撃等の標的型飽和攻撃にも利用され得ます。そうなれば最悪、国家安全保障に関わる悪夢の様なシナリオも万が一にも現れかねない潜在的リスクが想定されます。

そこで日本語ドメイン名の積極的活用は、ネット利用者への広範囲な安全確保と利便性への貢献だけでなく、サイバー攻撃対策にも強い事に繋がり、次世代ネット社会の必然的要請となるでしょう。日本のネット社会を安全に暮らすには、安全安心の日本語ドメイン名の活用推進は、国策としても非常に重要になるものと考えます。

これらを含めました以上の私の解決策を、ぜひともご検討いただきましたら誠に幸甚と存じます。

インターネット基礎知識習得のための機会創出を提言する

主婦
猪野塚　久美子（59）

一　はじめに

インターネット上の「負の側面」や「危険性」は、「社会性や道義性が大きくかかわるもの」と「インターネットの基礎知識を習得することで自己防衛が可能となるもの」に大別できると考える。

この論文は、「インターネットの基礎知識を習得することで自己防衛が可能となるもの」に焦点をあて

論ずる。

「インターネットの基礎知識を習得することで自己防衛が可能となるもの」には、平成二六年度懸賞論文「ネット社会を安全に暮らす」の応募要項「別記」テーマ設定の趣旨のうち、次の三項目が該当する。

○ウイルスによる個人情報や企業情報の流出
○インターネット・バンキングへの不正アクセス等による預金流出
○スマートフォンアプリをインストールしたら、端末の中の個人情報が流出した

総務省　平成二三年版情報通信白書では、「情報セキュリティ、プライバシー、違法・有害コンテンツ」等の分野では「情報活用能力（図1）が高いほど、ＩＣＴ利活用の際の不安感が小さくなる傾向がみられた」（図2）と、報告している。

これは、情報活用能力が高いほど、インターネット基礎知識の習得率が高く、インターネット利用時において、自分自身でのセキュリティ対策が可能となり自己防衛力が高まるため、不安感が小さくなると推測される。

私自身の体験から、インターネット社会を安全に暮らす一手段として、インターネット基礎知識の習得が、最重要と考える。

インターネット基礎知識を習得することで情報活用能力も高まり、自己防衛力が高くなるだけでなく、インターネット利便性の享受向上にもつながる。

ちなみに、私の情報活用能力は、レベル中の上段（図1）に該当する。

ここで述べる「インターネット基礎知識」とは、主にインターネット用語・インターネットの仕組み・インターネットの利用方法・インターネット上のサービス・インターネットに関するマナーおよび法律・インターネット上の脅威と自己防衛手段、等に対する理解を指す。

また、「独立行政法人情報処理推進機構 二〇一二年度情報セキュリティの脅威に対する意識調査報告書」では、セキュリティに関する情報収集時の問題点（図3）として、五五・三%の人が、「知らない用語が多い」と答えている。

図1

情報活用能力のレベルとアンケート設問の選択肢の対応表

レベル	選択肢
レベル高	パソコン本体やインターネット接続等でのトラブルが起きても、自分で解決できることが多く、困っている人へのアドバイスもできる。
レベル中	パソコン本体やインターネット接続等でのトラブルが起きても、説明書やアドバイスがあれば、ある程度は自分で解決できる。
	トラブルへの対応は難しいが、ソフトウェアのインストールやネットワーク関係の設定等、説明書やアドバイスがあれば機器等の設定がある程度は自分でできる。
レベル低	機器等の設定は難しいが、メールの送受信、ホームページ閲覧、文章作成などパソコンやインターネットを利用することには支障がないレベルである。
	メール受信や特定のホームページの閲覧など、ごく簡単（定型的）な操作はできるが、状況に応じて利用方法を工夫することは難しい。

（出典）総務省「ICT 利活用社会における安心・安全等に関する調査」（平成23年）

図２　情報活用能力別にみた「情報セキュリティ」等四分野に対する不安感

（%）

	情報活用能力		
	低	中	高
情報セキュリティ	88.1	82.4	74.7
プライバシー	87.6	82.4	71.4
違法・有害コンテンツ	84.2	73.8	65.7
インターネット上の商取引	69.0	58.8	51.1

（四分野すべてにおいて、情報活用能力が高いグループほど、不安と回答した人の割合が小さい）

（出典）総務省　「ユビキタスネット社会における安心・安全な ICT 利用に関する調査」　（平成21年）

図３　セキュリティに関する情報収集時の問題点

（%）

	2010年	2011年	2012年
知らない用語が多い	50.6	54.0	55.3
内容が難しい	49.8	51.7	51.2
情報が多すぎる	35.4	36.4	36.6
自分から情報収集や勉強をするのが面倒	25.8	27.7	27.0
自分に関係がある情報なのかわからない	23.5	25.7	25.7
情報の更新が早すぎて追いつけない	23.6	23.5	25.0
情報がどこにあるかわからない	18.7	23.2	23.0
その他	0.4	0.5	0.4
特に問題点は感じていない	19.1	16.9	16.4

独立行政法人情報処理推進機構
「2012年度情報セキュリティの脅威に対する意識調査」

二〇一〇年の調査では、五〇・六％、二〇一一年の調査では、五四・〇％である。わずかずつではあるが、増える傾向にあることが気にかかる。

これは、インターネット社会が日々進化し、新しい技術、新しいサービスが創出されていく中で、年々、新しい用語が増えてきていることも関係していると推測される。

だが、日本においては、インターネット利用の開始時から現在に至る過程で、多くの人は、用語の内容を正しく知る機会に乏しく、インターネット基礎知識を学ぶ機会にも恵まれないまま今日に至っていると判断する。

「知らない用語が多い」ことは、インターネット利用時の安全確保に対して大きなマイナス要因となる。また、インターネット基礎知識を習得するには、インターネット用語の理解が前提となる。

私自身の体験をもとに、「インターネット基礎知識取得の重要性」を検証し、「インターネット基礎知識習得のための機会創出」を提言する。

二　体験

二―一　インターネット基礎知識の重要性

二―一―一　プログラミングの基礎的な考え方

慶応大准教授でありＮＰＯ法人「ＣＡＮＶＡＳ」理事長の石戸奈々子氏[*1]は、読売新聞八月一三日

の紙上で、次のように語っている。

パソコン、スマホなどのデジタル機器に囲まれて育った「デジタル・ネイティブ」世代が台頭している。教育もふさわしいものに変革すべきだ。特に重要なのは、パソコンを動かすプログラム（ソフト）を書く、プログラミング教育だ。　―中略―　私たちの社会は、ありとあらゆるものがプログラムで制御されている。銀行、病院、電車、自動車、家電など数えだせば切りがない。プログラミングの基礎的な考え方がわかっていると、何かトラブルがあった時にも対応できる力が身に付くのではないか。

私は、この「プログラミングの基礎的な考え方がわかっていると、何かトラブルがあった時にも対応できる力が身に付く」との考えに同感だ。

インターネットもプログラムで制御されている。

プログラミングの基礎的な考え方がわかってくると、インターネット利用時において、かなりの安全を自分自身で確保できると考える。

プログラミングの基礎を理解するのは、そうたやすいものではない、情報系の学校にでも行かない限りは、学ぶ機会に恵まれ無いのが現状であろうと思われる。

だが、私自身の体験から、少しずつでもインターネット基礎知識を積み上げて行くことで、プログラミ

ングの基礎的な考え方を理解できるようになると実感している。

前述の情報活用能力レベル高（図1）の人は、プログラミングの基礎的な考え方を理解していると判断する。

二―一―二　インターネット関連資格の取得

私は、二〇〇二年から二〇〇八年の間に通算五年ほど、派遣社員としてインターネットサービスプロバイダーのサービスセンターに勤務していた。

この期間は、インターネット回線が、アナログ回線やＩＳＤＮからＡＤＳＬへ移行し、ＡＤＳＬ全盛期を経て光ファイバーが台頭する時期に該当する。

回線の高速化に伴い、目覚ましい勢いで種々のサービスが提供され始めた。

新しく創出されるサービスを正しく理解するには、インターネット基礎知識習得が必要であると感じた。

そこで私は、仕事のスキルアップの為、ＮＴＴコミュニケーションズ・インターネット検定「.com Master ☆2003」「.com Master ☆☆2004」(*2)の取得を目指した。

受験勉強を始めた当初、職場のインターネット基礎知識豊富な技術者から、「どんなことでも質問してください。こんなことを聞いたら恥ずかしいかな、幼稚かな、などと気にする必要はありませんから。」と、親切に言っていただいた。

だが、日頃、メール送受信とホームページ閲覧しかインターネットを利用したことのない私は、テキス

トの一ページ目からちんぷんかんぷんで、何を質問してよいのかさえも分からなかった。

インターネット基礎知識の無い人にとっては、カタカナ語やアルファベット略文字ばかりのインターネット用語は、どれ一つとっても難解で戸惑いを感じるものだ。

くり返しテキストを読むうちに、カタカナ語やアルファベット略文字に馴染んでくる。するとおぼろげながらもテキストの内容を理解し始める。

一度、勇気を出して質問してみたことがある。

インターネット基礎知識豊富な技術者は、わかりやすく図を描いて説明してくださった。だが、ちょうど足し算と引き算を覚えたばかりの小学生が、方程式で問題の解き方を説明してもらっているようなすれ違いを感じ、納得がいく説明を得ることも違和感を解消することもできなかった。

インターネット基礎知識豊富な技術者にとって、私の質問は、あたり前すぎる事実であり、何を疑問に感じての質問なのかさえも理解することができなかったのだと、今となっては推測する。

仕事の場でも同様なすれ違いで、インターネット基礎知識豊富な技術者とインターネットを始めたばかりの利用者の間で、トラブルになることを何回か経験した。

これから先の時代は、インターネット基礎知識豊富な技術者とインターネット初心者の間に、通訳が必要になるのではないかと感じることもたびたびあった。

資格取得により、「ハードウエアとＯＳ」「アプリケーション設定と使いこなし」「インターネットの技術」「サービス提供」「利用に関する一般知識」と「インターネットの基礎技術」「インターネット接続に

必要な回線・機器」「常時接続環境構築に必要な設定に関する知識」「情報公開のための関連技術」「ネットワーク運用に必要な知識」「インターネットビジネス活用」の知識を得た。

今の私なら、あのときの私の疑問に対して、わかりやすく噛み砕いた説明をすることができる。

この後、情報処理技術者試験「初級システムアドミニストレータ」（＊3）の資格も取得したが、業務が終息期となりインターネットサービスプロバイダーの職を去った。

「初級システムアドミニストレータ」の資格取得で得た知識が、プログラミング理解に大いに役立っている。

二―一―三　インターネット基礎知識の活用

インターネット技術やサービスがますます高度になり複雑化し、インターネット基礎知識豊富な人と知識を持たない人とのかい離は、大きくなるばかりである。

昨今、サポートセンターに技術的な問い合わせをすると、すぐにリモートアクセスでのサポートを提案してくるのも致し方ないことだと感じる。

インターネット基礎知識豊富な技術者にとっては、利用者に説明しながら、問題点の把握やトラブル解消を行うより、リモートアクセスでサポートしたほうが容易であることは、想像するに至らない。

インターネット基礎知識を持ち合わせない利用者にとっても、リモートアクセスサポートは、自動でトラブル解消してくれるような感覚であり、とても便利なサービスではある。

だが、リモートアクセスサポートは、自分自身のインターネット接続端末を遠隔操作されることであり、悪意をもった担当者に遭遇してしまう心配を捨てきれない。

私は、自分自身の勉強のため、リモートアクセスによるサポートを断り、電話口でサポートをうけながら、自分でパソコンを操作してトラブル解消をすることにしている。

実際、時間はかかるが、トラブルを解消するごとに、資格取得で得た知識が有効であることを強く感ずる。

また、自分自身でトラブルを解消することは、新しい知識を得る機会にもなる。

今春、WindowsXP サービス終了に伴い、パソコンの買い替えが必要となった。

機種選びの参考のため、久しぶりにパソコン雑誌を購入してみた。

ほんの数年の間に、新しい通信規格や通信技術が台頭していることに驚かされた。

聞きなれないカタカナ語やアルファベット略文字も増えていたが、すでに習得しているインターネット基礎知識をもとに説明文を読むことで、そのほとんどを理解することができた。

過去に、インターネット基礎知識を習得したことは、現在もとても有意義なものとなっている。

インターネット利用において、インターネット基礎知識習得の重要性を実感している。

ニ―二　インターネット基礎知識習得の機会

ニ―二―一インターネット安全教室

インターネットは、車や道路に例えられることが多い。

現在のインターネット事情は、「無免許運転で高速道路を飛ばしているに等しい」と例えられている。

車を運転するには、知識や技術を学び、運転免許証を取得する必要がある。

だが、インターネットは、一九九〇年代後半から一気に広まり、この二〇年ほどの間に目覚ましい勢いで高速化し、多種のサービスが創出され、日常生活に不可欠なものとなった。

日本に住む多くの人たちは、インターネットの利用開始時から現在に至る過程において、インターネットに関する知識や技術を学ぶ機会に恵まれずに、今日に至っていると判断する。

それが、無免許運転に例えられる所以である。

インターネット利用に関しても、自動車教習所に相当する機会の必要性を通感する。

私は、二〇〇八年に、男女共同参画センター横浜北が主催する「女性のためのインターネット安全教室」に参加したことがある。

経済産業省、ＮＰＯ日本ネットワークセキュリティ協会（ＪＮＳＡ）、ＮＰＯ情報セキュリティフォーラム（ＮＰＯ-ＩＳＥＦ）協力。警察庁後援のセミナーである。

「迷惑メールやウイルス」「ファイル交換ソフト」「有害サイト」の怖さや、「無線ＬＡＮ」「個人情報」「ＳＮＳ」の安全な利用方法などを学ぶことができた。

動画を使ったストーリー仕立ての解説は、自分の身に置き換えて学ぶことができ、さほどインターネット知識を持たない人にとっても理解しやすく、とても有意義なものであった。

このセミナー開催は、たまたま市の広報で知った。

開催場所へは、バスと電車を乗り継ぎ二時間近くを要した。

インターネット上の脅威が、ますます拡大する中、自宅近くで開催される機会があれば、参加して新しい知識を得ていきたいと考えていたが、残念ながらその機会には恵まれていない。

平成二五年度の情報セキュリティ対策推進事業（全国情報セキュリティ普及啓発ネットワーク整備事業）インターネット安全教室実施報告書によると、

「インターネット安全教室」は、二〇〇三年から開催され二〇一三年までに、全国での開催数一、二一七回、参加人数七九、九〇〇人が受講したと報告されている。

とても有意義なセミナーであり、一〇年間もの期間の中で、この開催回数、受講人数は、あまりにも少なすぎてもったいないと感じる。

「インターネット安全教室」は、セキュリティ基礎知識に特化したセミナーであったが、他のインターネット基礎知識においても、同様のセミナー創出が必要と考える。

これらは、必要に応じて誰でもが身近に気軽にいつでも利用できる必要性があると考える。

ニ―ニ―ニ　インターネット初心者向けホームページ

私は、二〇〇八年からインターネット初心者向けのホームページ（＊4）を作り始めた。

これからインターネットを始める人や、始めたばかりの人たちにユビキタスネット社会（＊5）やインターネットのことを正しくわかりやすく伝えることを目的としたサイトである。

当時は、ユビキタスネット社会を目指して、日本国中、めざましい勢いでインターネット技術が進化し、それに伴うサービスもたくさん創出され始めた。

まだ、スマートフォンは出現していなかったが、携帯電話やゲーム機でもインターネットを利用できるようになり、子どもを巻き込む事件や犯罪も増えていた。

インターネットの世界は、「自己責任」とよく言われていた。

インターネット基礎知識を持ち合わせないが故に、必要以上に恐怖を感じたり、不利益を被ったりしている人たちを多く見てきた。

このような人たちが、少しでもインターネットの基礎知識を得て、安全安心に利用してもらいたいとの思いがあった。

インターネットサービスプロバイダーで派遣社員をしていた経験と、資格取得時に得た知識と、四〇冊を超える市販本を読み、内容を検証しながらサイトの記事を書いた。

それぞれの記事は、噛み砕いて、極力わかりやすい表現を心掛け作成した。

インターネット上では、評価をいただくこともあったが、一番、利用してほしいと思ったインターネット初心者の友人たちには、「難しくて理解できなかった。」と言われてしまった。

インターネット資格取得以前の私自身を振り返れば、難しく感じる内容であることは明らかであった。早急な必要性を感じて、どこから手を付ければよいのかさえもわからないまま作り始めてしまった後悔もあり、さらに噛み砕いたわかりやすい説明内容に作り替えることを決めた。

だが、その後、家族の看病と私自身も障害を抱える身となり、頓挫してしまった。

個人で取り組むのは、困難を極めると痛感した。

二―二―三　報道の場における「噛み砕いた解説」

八月二日の読売新聞の一面に「ルーター攻撃　通信障害」の見出しで、「ＤＮＳアンプ攻撃」の記事が掲載されていた。

インターネット基礎知識を持つ人であれば、この見出しだけで、障害の内容をある程度イメージすることが可能である。

また、自分自身のインターネット利用状況と照らし合わせて、何が必要で何をすべきかの判断が可能である。

記事には、通信障害の内容以外に、ルーターの説明も別記され、ルーターを狙った通信障害を図で表示している。

とても親切な扱いではあるが、インターネット基礎知識を持ち合わせない人が、どこまで理解できるかは、非常に疑問だ。

これは、私自身の体験から感じる疑問である。

もう少し噛み砕いた説明記事を添付してはどうだろうか、と考える。

一例をあげる。

○この記事内容の被害に遭わないためには、ルーターソフトの更新が必要です。

○ルーターソフトの更新は、メーカーやプロバイダー側で対処することができません。利用者個人が、自分自身で更新する必要があります。

○パソコンなどのインターネット接続端末でウイルス対策ソフト（セキュリティソフト）を利用していても、「ルーター攻撃」を防ぐことはできません。

○ルーターソフトの更新をしないと、知らぬ間に加害者になってしまう危険性があります。インターネットに関わる誤認逮捕事件は、このような事象から起きることが多くあります。

以上のような噛み砕いた説明を付記することで、インターネット基礎知識を持ち合わせない人も、事件の内容を捉えやすくなると考える。

最近、ＮＨＫのテレビ番組「首都圏ネットワーク」を視聴していて、振り込め詐欺等に対する注意喚

起コーナーがあることに気付いた。

このコーナーは、初めに、犯人がよく使う言葉などがキーワードとして示される。実際に起きた事件の概要の説明があり、警察から提供された実際の電話通話の音声が流れる場合もある。このような電話を受けた場合、どのように対応すればよいかの具体的な方法が説明される。毎回、異なるケースが放送され、似たようなケースの場合は、どこが異なるのか具体的な説明がなされる。女性アナウンサーが、ゆっくりはっきりとした口調で、簡潔な説明をするため理解しやすく、自分の身に置き換えてイメージすることも容易である。

ほんの二～三分のコーナーであるが、キーワードは、何回か繰り返されるため覚えやすい。親しみやすく、とても良いコーナーであると感じている。

インターネット関連事件に関しても、各報道の場において、同様の解説コーナーの創設が望まれる。報道の場での「噛み砕いた解説」は、多くの人にインターネット基礎知識を提供できると考える。

前述のセキュリティに関する情報収集時の問題点（図３）の「知らない用語が多い」の解消だけでなく、「内容が難しい」「情報が多すぎる」「自分から情報収集や勉強をするのが面倒」「自分に関係がある情報なのかわからない」「情報がどこにあるかわからない」を、併せて解消できると考える。

三　おわりに

私たちは、パソコンスクールや各自治体、企業、学校等が開催する講座などを利用して、身近にインターネットを学ぶ機会がある。

だが、それらの多くは、インターネット端末の操作方法やアプリケーションソフトの利用方法であり、インターネット基礎知識を学ぶ機会とは異なる。

インターネットが生活に必要不可欠となった現在、身の回りの身近なところに、インターネット基礎知識習得の場の創出が急務と考える。

そして、誰でもが必要に応じていつでも気軽に利用できる必要性があると考える。

また、新聞テレビ等、報道の場においての「噛み砕いたわかりやすい解説」の導入は、多くの人にインターネット基礎知識を提供する機会となり、日本のインターネット利用者全体の基礎知識底上げにつながると考える。

「ネット社会を安全に暮らす」為の一手段として、インターネット基礎知識習得のための機会創出を提言する。

私は、三年前に聴覚に障害を持つ身となった、ネットスーパーやネット通販が不可欠の生活である。

インターネットは、病気に関する情報収集にも大いに役立っている。

玉石混交と言われるインターネット上の情報であるが、とりわけ闘病ブログは、誠実に書かれているものが多く、会ったことも無い人たちからずいぶんと励まされた。

インターネット関連資格の取得を目指していたころには、自分自身が障害を持つ身になることなど考えたことも無かった。

同時に、インターネット基礎知識が自分自身の将来に、こんなにも役立つとも予想しなかった。

過去に、インターネット基礎知識の習得機会に恵まれたことを幸運に思う。

インターネットは、ますます日常の不便を解消し、多くの可能性を広げてくれると考える。

日常生活にハンディーを抱えている人こそ、インターネットを活用して豊かな人生を過ごしてほしいと願っている。

私は、生まれてはじめて論文というものを記述した。

「論文の書き方」の本を読みながらの執筆であり、至らないところは、ご容赦いただけると幸いです。

注

（＊1）専門は、ＩＴ教育。著書に「子どもの想像力スイッチ」。

（＊2）二〇一三年一〇月から認定資格レベルが一新される。

（＊3）平成二〇年度秋季からＩＴパスポート試験に移行。

（＊4）ぶきっちょ母さんのユビキタス知恵袋。
http://www14.ocn.ne.jp/~kaasan/

（＊5）総務省は、「e-Japan 戦略」に貢献するため、二〇一〇年に向けて「u-Japan 政策」を提言し、ユビキタスネットワー

ク社会の実現にむけて、いろいろな取り組みを始めた。

参考文献

NTTコミュニケーションズ インターネット検定　公式テキスト

総務省　情報通信政策　u-Japan 政策

総務省　平成二十三年版　情報通信白書

特定非営利活動法人　日本ネットワークセキュリテイ協会

平成二十五年度　情報セキュリティ対策推進事業（全国情報セキュリティ普及啓発ネットワーク整備事業）「インターネット安全教室」実施報告書

http://www.net-anzen.go.jp/（二〇一四年九月一日　最終確認および引用報告済み）

独立行政法人情報処理推進機構

二〇一二年度　情報セキュリティの脅威に対する意識調査　報告書

http://www.ipa.go.jp/（二〇一四年九月一日　最終確認および引用報告済み）

読売新聞

ネット社会における認識力と危機管理

警察官（警視庁刑事部捜査共助課長）
岸　昭利（55）

はじめに

今から三〇年ほど前の話になるが、アニメの「機動戦士ガンダム」の人気が高まり、私もテレビ、映画など夢中になって見た記憶がある。その中で妙に納得したのが「人は生存圏（人が生存できるエリアの意味で使っていたと思う。）が拡大するとともに認識力も拡大する。」というセリフである。

当時の私は「生物としての人間は狭い世界で生きる限り外界を認識する力が低くてもよいが、活動エリアが大きくなるほどより高度な認識能力が必要になる」と考えていた。

一　認識力とは

まず、「認識力」について考えてみたい。

㈠　自然人の持つ認識力

認識力とは五感（視覚、聴覚、嗅覚、味覚、触覚）によってもたらされる外部的情報の総合評価である。各感覚の能力には大きな差があり、感知する対象との距離が大きく影響を与える。

もっとも遠い対象物を認識できるのは視覚であって、*視力四（アフリカ人の祖先）の人は、一キロメートル先の直径七センチメートルほどの物体を認識できると言われている。

その次は聴覚、嗅覚と続き、触覚と味覚は直接接触を必要とするので、遠くから対象を認識することは不可能である。

*白鳥敬「人間の視力の限界は」

㈡　認識力の変化

このような生物としての「人」が持っている認識力は、時代とともに低下してきていると考える。前述

のアフリカ人の祖先の話ではないが、「より遠くを見る」能力は、視力を補強する機械が発達するまでは高い状態が維持・向上されてきたと考えるのが自然である。

それでは、どのような環境条件がこの認識力を向上させるのであろうか。

その答えは、認識力が外部的情報を集める目的を考えると見えてくる。すなわち、生物としての人は「生存するため」に外界の危険情報を早期に把握する必要がある。したがって、生物としての人が生きていく上で「危険」が大きい環境であるほど、認識力は高まるはずである。

㈢　認識力と情報収集能力

前述したとおり、認識力は五感によって成り立っているが、それぞれの感覚には情報収集力に大きな差がある。

短時間に、そして大量の情報を脳へ送り込めるのは視覚である。また、人の記憶に残される情報も視覚からのものが多く、これは映像の他に文字の情報も含まれるからであろう。

私個人は、聴力が「危険」に対する認識では最も優れていると考えているが、耳からの情報とは大半の人が発する言語のことであって、それに対しては素早い反応が求められるケースが多いであろう。すなわち、人同士のコミュニケーションは言葉によって行われ、認識→判断→回答という作業が常に行われているからである。

二　生存圏と認識力

㈠　生存圏の範囲

冒頭の「ガンダム」の世界ではないが、人は移動手段の進歩とともに生存圏を拡大してきた。すなわち、人の生存圏は移動手段・能力の向上と密接に関連し、この拡大傾向は人間の持つ本能によるものと考える。

狩猟によって生業を立てていた時代では、当然獲物の多いエリアに生存圏を設定したであろうし、農耕が主力産業となった時代では農作物を育てるための広大な土地（農地）を必要とした。また、貿易が巨額の富を生み出す時代になると移動手段も飛躍的に発展し、人の生存圏は急速に拡大したのである。

㈡　生活圏の拡大と認識力

このように考えてくると、生存圏の拡大が認識力を拡大させたのではなく、認識力の拡大が、言葉を換えれば認識力の向上が生存圏拡大を可能にしたのである。

ここでいう「認識力の拡大」は、視覚を強化する望遠鏡、聴覚を補強する聴診器や伝声管等のツールを指す。

このようなツールの発明は、人が持つ低い認識力を補うものであったが、人はなぜそのようなツールを欲したのであろうか。

㈢　認識力拡大ツールが発明された理由

人は文明の進歩とともに認識力拡大ツールをレベルアップさせてきたが、ついには遠隔地で会話できる無線機や高速で飛行する物体を発見するレーダーまで生み出してしまった。

私は、その根底にあるのは生物としての人が持つ「生き残るため」の本能であると考える。つまり、生き残るために邪魔となるもの、脅威となるものをいかに早く発見し、その対処方策を講じるために認識力拡大ツールの発展は続いてきたのである。

三　生存圏と生活圏

㈠　生存圏と生活圏の違い

両者の違いを明確に規定した論文は発見できなかったが、私的な考え方を述べれば、

「生存圏」は驚異のリスクを負いながら生きるため活動できる範囲

「生活圏」は大きな脅威のないエリアにおける日常生活を営める範囲

という違いがあるのではないか。

つまり、「生活圏」には生存を脅かすほどの脅威は存在しない社会と想定して以下本稿を進める。

㈡　ネット空間における生存圏と生活圏

現実世界における生活圏は、居住地周辺や仕事先など自分と既知の人々に囲まれているエリアであるから、当然脅威は少ないと考える。一方、生活圏を超えた世界である生存圏では、我々は脅威の存在をある程度意識しながら行動することとなる。ただ、厳冬期に冬山登山を行うような極端な例を除けば、日本国内で危険を感じる生活圏を認識することはない。

しかし、ネット空間ではどうであろうか。そもそも「生存圏」や「生活圏」の違いすら存在しない、言い換えればインターネットの世界は常に何らかの危険性の存在しているのである。

㈢　生存圏における危機回避

前述のとおり、生存圏において行動しようとする際は何らかの脅威が存在し、人はそれを避ける術を体得している。その術を支えているのが冒頭から挙げている「認識力」である。

例えば、猛スピードで走る車両にぶつからないのは何故か。走行している車両を視覚によって認識し、それが脳の記憶と照合され「衝突するな」と判断する。

爆発音がすれば、それは聴覚によって脳に伝わり「爆発場所から遠ざかれ」と判断する。

このように、外界の脅威に関する情報を脳へ提供し、その記憶と照合して正しい判断を促すうえで、この「認識力」は重要なツールなのである。

四　他人に対する関心と距離の関係

ここで、もう一つ視点から人の脅威について考察してみたい。

㈠　人間同士の距離による影響

「ひざ詰め談判」の言葉に代表されるとおり、他人に影響を与える説得は距離が近いほど効果的であると言われる。このように一定の距離内でコミュニケーションを繰り返す人間関係は、そうでない関係よりも濃密になる。家族関係がその典型例で、家族は血のつながりというよりも一つの共同体として暮らしていく過程で、その距離の近さゆえに濃密な人間関係を育てると考える。

㈡　通信手段の発展と家族関係

このような関係は、人々が家という「一個の容器」に閉じ込められることによってできあがったものであるから、この容器にほころびが生じると濃密な関係は次第に希薄になると考える。この「ほころび」こそ、家族と家族以外のものを結びつける「通信手段」である。

人類は文字を「記録」という機能で活用したほか、人から人へ情報を伝達する「情報」面でも利用してきた。この文字を活用した「手紙」は、一部の限られた人々が通信手段として利用したが、家という容器に大きな穴を開けるほどではなかった。

文明が進んで、電話が家の中まで普及しはじめると状況は一変する。すなわち、家の構成員である家族は、電話という通信手段によって家庭外の人と会話することが可能となり、それは家族同士よりも濃密な人間関係を築くことを可能にした。

そして、携帯電話と電子メールの登場はこの傾向に更に拍車をかけたのである。

㈢ 社会における人間関係

人口の増加によって街が作られ、そこに共同体としての社会が出来上がると、トラブルを防止するためのルールが作られた。権力者が統治上発出する命令から、地域社会の取り決めまで様々なものが存在したが、その根底にあるのは身近にいる人に迷惑をかけない精神である。

例えば、公共の道路の使い方である。自分の居住場所の前だからといって勝手に物を置けば他の人は通行できない。狭い道で前を見ていなければ衝突する。傘をさしていて人混みを抜けるには相互に傘が当たらないようにする。これらの行為は、知っている人であろうとなかろうと常に「自分の近くの人に関心を払い、気を遣う」ことが根底にあったのである。その理由は、遠く離れている者よりも物理的に「今いる空間」での人間関係を優先させたからである。

㈣ 通信手段の進歩が人間関係に及ぼした弊害

連絡手段を携行しない段階では、人は現時点で身近にいる人とトラブルを起こさないことが自分の安全

につながることを知っていたのであろう。そこには、マナーや規則の縛りもあったのであろうが、自分の知り合いと繋がっていないことが身近な人々への気配りを後押ししていたと考える。

ところが、携帯電話の普及は周囲の人々に気を配らなくても、常に家族・友人とつながっている安心感を与えた。公共の場所で自分の世界に閉じこもることに勇気と安心感を与え、携帯電話によってつながっている人への依存を高めたのである。

現在の都会における無関心社会はこのようにして生まれ、時の経過とともに社会のマジョリティとなっていった。

五　現実空間とネット空間における安全確保

人は脅威を避けるため、優れた「認識力」を持って生まれてきた。この力は現実空間における物理的脅威に対しては、安全を確保する上で非常に有用である。しかし、ネット空間でも同程度の安全を保つには、いかなる「認識力」が必要なのであろうか。また、人と人との距離がこの関係にいかなる影響を及ぼすかを考察し、ネット空間の安全確保方法を考えてみたい。

㈠　「認識力」の面からの考察

ア　ネット空間における認識ツール

ネット空間と人とをつないでいるものは、パソコンに代表される端末と呼ばれる機械であり、この機械を通して人の視覚、あるいは聴覚を通じて脳へと情報が伝達される。

視覚による情報が脳に伝達され、記憶の中にある脅威情報と照合されることによって人間は反応を起こすのであるが、ネット空間に関する脅威情報は、個人差はあるものの現実空間のそれに比べれば極めて少ない。

これは認識ツールや認識力の問題ではないかもしれないが、端末→視覚という経路だけでは十分な脅威情報は収集できないこととなる。

イ　視覚と聴覚の違い

それでは、聴覚を使った認識の方が脅威情報は効果的に収集できるのであろうか。先に述べたとおり、情報の収集力では視覚の方が聴覚よりも優れている。ただし、音声によるコミュニケーションという面を考えると、脅威情報を的確に捉えられるのは聴覚、つまり耳からの情報であろう。

携帯電話での通話とメール送受信を比べてみればわかりやすい。脅威が身近に迫っているのにメールを使用して知らせる人は稀であろう。これは、視覚と聴覚の問題というより、文字による伝達と言葉による伝達の違いであり、緊急性という面では言葉による伝達が優れているのである。

ウ　認識力を増加させるツール

自然界のウィルスも肉眼では見えないように、ネット空間でもウィルスに感染しないため特殊なツールを用いて認識力を増大させている。このようなインターネットセキュリティの仕組みはネット上の「病気」対策としては早期発見という意味で極めて有効である。

しかし、ネット空間における「犯罪行為」に対してはどうであろうか。

病気に対する防疫や予防接種と犯罪行為に対する防犯対策は根本的に異なる。どれだけ最新のウィルス対策ソフトがあろうとも、見えない相手が犯罪者かどうかは教えてくれない。このように考えてくると、現在の技術ではネット空間における人の認識力増加（強化）ツールは犯罪行為には無力かもしれない。

エ　脅威情報の蓄積による安全対策

このように考えてくると、ネット空間であろうと現実社会であろうと「自分で自分の身を守る」ためには、よりたくさんの「危険」を知っておく必要がある。ネット空間に対しては、「認識力」が不十分にしか働かないのであるから、「危険」を知ること、つまり脅威情報をできるだけ正確に、できるだけ大量に収集しておくことが肝要である。

そのためには経験に基づく情報の蓄積が最も有効であると考えられるところ、インターネットの経験がいくら長くても非日常的な事柄が少なければ（通常は多いとは考えられないが）、脅威への判断力がそれに比例して向上することはないであろう。これは現実社会の経験とはあまり連動しないから、経験豊富な大人でも、中学生あたりに騙される事案は起こりうるのである。

㈡　人の距離間からの考察

「四　他人に対する関心と距離の関係」で述べた通り、人は通信手段を使うことによって、遠くにいる知人を身近に感じ、結果として近くにいる他人よりも上位に置こうとするのである。

ア　見知らぬ人と関わらないことによる安全確保

この傾向は、「危険のものから遠ざかる」という根本的な生存本能に由来する。あるいは、社会の仕組みが進歩したことにより、見知らぬ人と関わらなくても非常時には公的な助けが得られるという安心感に基づくのであろうか。

いずれにしても、日本の近代文化が築き上げた見知らぬ人に対する思いやりの精神は、非常時は近くの人に助けてもらうという相互扶助的な考え方に基づいていたと考えられる。その相互扶助的な仕組みは、公的な救助システムの発達と通信手段の発達により失われてきたのである。

イ　脅威に対する判断力の低下

自宅に泥棒が入り、金銭や物が盗まれた。すぐ一一〇番通報して警察へ被害申告する人が多いであろうが、家族や友人に電話してから届け出る人もいる。今まで経験したことのない事態に対して、「まず相談」という選択肢を選んでいるのである。この違いは経験の多寡によるものと説明してもよいが、やはり公的援助システムを含めて「より精神的なつながりある人」に精神的な助けを求めたのであろう。つまり、「より精神的なつながりある人」が存在する人ほど脅威に対する判断力は鈍化し、たとえ一人暮らしであって

も携帯電話に依存する度合いが高いほど、物理的距離の近い人へは助けを求めない傾向が強くなる。

ウ　ネット空間が現実社会の距離感へ与える影響

以上のことを勘案すると、人が集まる社会における従来の安全システムは携帯電話をはじめとする通信ツールの進歩によって徐々にその機能を失いつつあり、人々をより危険性の高い環境へ追いやっているのではないだろうか。

すなわち、緊急事態において物理的距離の近い人に助けを求めるよりも「まず携帯電話で連絡」という判断は、危機管理上は大きなマイナス要素となる。

いずれにしても、ネット空間によってつながっている友人・知人がいざという時にすぐ駆けつけてくれるという感覚は高度に発達した通信機器による「まやかし」にほかならない。

六　ネット空間と現実社会をバランスよく生き抜くために

言うまでもなく、我々は現実社会において生きているのであり、ネット空間は情報集めや連絡のための道具に過ぎない。道具であるがゆえに、その危険性を正しく認識し、使い方を誤らない努力が必要である。あくまで、主たる生存圏は現実社会であってネット空間ではないのである。

それでは、安全にネット空間を利用し、現実社会の脅威を正しく認識するために何をすべきかを挙げさせていただく。

㈠　ネット空間における認識力低下を理解する。

現実生活における認識力は、視覚、聴覚、嗅覚によって入手した情報を総合的に評価して脅威の度合いを判断するのである。ネット空間では先に述べたとおり、ほぼ視覚によってもたらされた文字情報と真実性の裏付けがない画像によって判断の基礎となる情報が形作られる。そこには「正しく物事を見極める」ための自然的認識力は通用しないのである。

まるで、音のしない覗き穴から一部分しか見えない世界のように、極めて情報量が少ないのである。しかし、覗いている本人は比較対象がないため、そのあまりに狭小な世界に気付かないのである。

ネット空間における認識力がいかに低レベルのものであるかを認識する必要があるが、そのためには、常にネット空間を覗いている意識をもち、客観的に自分を見ることが大切であり、常にこれを意識するべきである。

㈡　携帯用通信機器に依存した人間関係の危うさを知る。

携帯電話に代表される通信機器を常時持っていることは、人間の信頼関係を高めるには非常に有効である。しかし、距離感を無視したこの依存関係は、緊急事態には大きな弊害になるのである。

携帯用通信機器が持ち主に与える安心感は、緊急事態には通用しないことを理解すべきである。暴漢に襲われた場合、ひったくりにあって物を盗まれた場合、急に具合が悪くなって動けなくなった場合など、

携帯用通信機器でつながった知人・友人はまったく無力である。

常に身近にいる人へ気を配り、「お互い様」の精神を涵養して社会生活を営むことこそ現代を生きる人間にとって大事な「危機管理」である。

㈢　自分の身は自分で守る精神を育てる。

人は平素集団の中で生活している。ところが、ネット空間へは通常自分ひとりで入っていくことになる。「自分を知っているのは自分だけ」というのは、大都会へ単独で出てきた状態と同じである。すなわち、自分の匿名性が強力に保証され、まさに「旅の恥はかきすて」状態になるのである。現実世界であれば、それでも緊急事態には援助してくれる人が表れる可能性があるものの、ネット社会では自分ひとりで全てを解決することが求められる。

ネット空間では、より高い自律心と高い倫理観が求められるのであって、これを持たないもの、未熟なものは立ち入るべきではないと考える。

七　教育と使用制限の必要性

以上のように考えてくると、ネット空間へ誰でも入ることができる現在のシステムは変えていく必要があると考える。そのキーワードは「記名性」と「倫理観」である。

㈠　記名性について

匿名性に対する言葉として「記名性」を挙げさせてもらった。ネット空間ではたとえＳＮＳのような制限されたグループであっても、常に匿名性は存在するのである。また、現実社会では困難な「他人へのなりすまし」も、ネット空間では性別、年齢などに全く関係なく行いうる。

ネット社会の安全を維持するためには、現実世界の「防犯カメラ」に匹敵する記録装置、あるいは記名性を担保できる仕組みが必要となる。あるいは、匿名性が担保されているエリアとそうでないエリアの住み分けなども必要かもしれない。

いずれにしても、現実社会において「危ないところには近寄らない」判断はある程度の情報があればできるし、行政機関からも提供される。ところが、ネット空間では「どのサイトが危ない」という情報は入手できないし、行政機関が情報提供することはない。

記名性をそのように確報するか、その反面、利便性や個人情報の面で反対意見も起こるであろうが、未成年者も同じ危険性のエリアへ入り込めることを考えれば、何らかの制限は必要であると考える。

㈡　教育の必要性

現在の学校教育は、知識を身につけるための活動は非常に力を入れて行われているが、社会生活を営むためのルールは家庭教育に頼っているのが現実である。

安全に生きるための知識は、各人が意欲的に求めようとすれば手に入るが、見えない空間を知識のないものが活動することは目隠しで道路を歩く如く、非常に危険である。

学校教育で新しいことを教えるときは、どうしても「いかに使うか」に重点が置かれるが、同じ比重で「他人に迷惑をかけない」教育も行うべきである。この部分は知識不足の親に依存するよりは、正しい知識を持った教育者によって統一的に行われることが望ましい。

㈢　使用制限の必要性

道路交通法上、自動二輪免許を取得できるのは一六歳以上である。現実社会ではこのような年齢制限は様々な分野で行われているが、これは同じ行為であっても子供には危険なものが存在し、それに対して社会が一定の規制をかけているのである。

このような規制は、もっぱら「少年の健全育成」を目的として行われるが、深夜における外出規制やゲームセンターへの立ち入り規制などは少年自身の被害予防の目的もあると考えられる。

ネット空間も有害サイトを児童へ見せないことを目的に「スクリーニング」を呼びかけているが、プロバイダ業者の協力に基づくもので、徹底されているとは言い難い。先に述べた「記名性」と同じ話になるが、少年であるがゆえに匿名性に潜む危険性はより高くなるのである。

したがって、端末と個人のつながりをより徹底させ、事前に登録された者以外はアクセスできない仕組みを作り、記名性を徹底させることが望まれる。

おわりに

インターネットの世界は、我々に「第三の眼」を与えてくれた。その眼を通して現実世界と違う世界を見ることができ、夢、あるいは知識に対する欲は大きく膨らんでいく。ただ、その夢が偽物でないという保証は誰もしてくれない。そんな危うい世界でなく、誰もが希望を持てる世界を築かなければいけない。たとえそれが「ネット空間」という世界であっても。

ネット社会を安全に暮らすための警察としての取り組み

警察官（警視庁）
齋藤　美帆（43）

一．はじめに

「出会い系サイトに登録したんですけど、出会いがないんです。出会ってもらえないんです。どうしたらいいですか。」

これは、私が約十二～三年前、ハイテク犯罪対策総合センター（現：サイバー犯罪対策課）在籍時、男

子高校生から受けた電話相談である。

当時、私は主に学校をはじめとする教育機関に出向いて、小学生から高校生までの学生や教師、保護者等に対し、ハイテク犯罪の防止についての講演をしていた。まだ「サイバー犯罪」ということばも「スマートフォン」も存在しなかった当時は日本におけるインターネットの人口普及率は四六・三％だった。それが、インターネットが社会基盤として定着し、多くの都民・国民にとって生活の一部となった今では七九・五％の人口普及率となるのに伴い、パソコンやスマートフォンなどの情報機器を利用したインターネットに関するトラブルの相談や犯罪は、日々新手な手口による被害が発生し、ネタが尽きることはない。新聞やテレビで報道されるような重大犯罪や被害の影響が大きい犯罪はごく一部であり、実際には犯罪には該当しなくとも、冒頭のようなインターネットに関する些細な心配ごとで悩んでいる人が非常に多いのが実態である。

そこで、サイバー空間を含めた現実社会において、治安を守ることが責務である警察の立場から、ネット社会を安全に暮らすための対策や提言を論じていくこととしたい。

二　実体験から考察する「安全なネット社会」とは

○　ネット社会を暮らす心構え

・ネット社会の弊害

「サイバー犯罪捜査に興味のある人は、挙手してー」

昨年まで警察学校の教官をしていた私は、警察官の卵である警察学校の学生に対し、「情報管理」という授業の始めに、必ず質問をしていた。

一八歳から二九歳までの警察学校の学生たちは、メールやＳＮＳが友人関係の構築ツールとして当たり前の環境で育ってきた若者たちである。義務教育の授業でパソコンを使用した文書やプレゼン資料作成や、子どもの頃からゲーム機器や携帯電話、スマートフォンを巧みに操作しインターネットを使いこなしている世代であり、情報機器を悪用したサイバー犯罪事件捜査を希望する若手警察官が増加していると推測していたが、実際は違うようだ。手を挙げる学生は、ほとんどいない。

簡易パソコンの機能を持ち合わせたスマートフォンなどの身近なツールによりインターネットの活用方法は熟知している一方、学習や仕事のツールとしてのパソコンとなると苦手意識が先行し、使いたがらない、あるいは使いこなせないという現実は、日々進化する情報化社会を支えていく若者たちの今後を考えると大きな課題である。

現代では、情報機器やインターネットを通じての「文字情報」によるコミュニケーションが主体になり、

対面して相手の反応を見ながら会話をしたり本音を聞き出したり、また、瞬間に発する「ことば」に集中する機会が減っているため、心の通った人間関係を構築することが苦手な若者が増えているのではないだろうか。

本来コミュニケーションを深めるためのツールに逆に依存してしまい、インターネットが使えない環境になると不安になり、孤独にさえ感じるという。また、ネット社会における被害者は、現実社会と比較して実態が見えない分ダメージが大きく、子ども同士のトラブルは登校拒否や殺人事件まで発生している。近年急増しているＳＮＳをはじめとするコミュニケーションツールを悪用した犯罪は、ネット依存社会の弊害であろう。

警察学校入校中は、デジタル社会から少し離れアナログ生活に身を置くことで、警察官として仕事をしていく上で重要な団結力や同僚愛を醸成する教育プログラムが組まれている。少なくとも義務教育の間は、家庭や学校では保護者や教員の意識をアナログ世界に向け、子どもたち自身がデジタル情報に左右されない、自分自身の意思や考え方による行動力を身につけるよう手助けしていくべきである。

情報化社会が生み出した脆弱性は、情報化の技術だけでは解決できない。情報化社会を生きている人間の思考力が必要である。

・ネット社会の相談所

数か月前、近くに住む七〇歳を超えた母親にタブレット端末を購入した。購入当初に基本的な使い方を

教えたところ、最近ではインターネットを利用した情報収集・検索だけでなく、ＳＮＳやゲームなど、ある程度使いこなせるようになっている。母親自身、パソコンをはじめ情報機器全般については無知であることを自覚しているので、変に触るとどうなるのかが不安で、教えられたこと以外絶対に操作しないという。子どもたちがゲーム機器やスマートフォンなどを興味本位で触りながら、なんとなく使い方をマスターしてしまうのと大きく異なる。ただ、母親の場合、タブレット端末の使用中に困ったり悩んだ時に、身近な駆け込み寺として、頼りにできる私の存在が一番安心であるという。経験したことのないグローバル化したネット社会に飛び込み共存していくには、身近に「自分にとっての相談所」が必要である。

ネット社会においても現実社会と同様、あらゆる危険や脅威がゴロゴロと転がっている。一番安全なのは、インターネットを使わないことであることは言うまでもない。しかし、メールやインターネットは正しく使えば、情報の収集・共有・伝達手段として非常に便利かつ有効である。安全なコミュニケーションツールとして活用し充実した生活を送るためには、危険や脅威とそれを回避するための対策を知り、身近にいつでも相談できる環境を構築することが重要である。

設定や利用方法について不安な場合は周囲の詳しい人に手助けしてもらうなど、利用者本人が少し気をつける意識を持つだけでもトラブルは大幅に減少するはずである。

ネット社会の危険性を知る―これが安全に暮らすための第一歩である。

○　ネットに関する相談

「元彼と私の家で撮った裸の写真がインターネット上でばらまかれてしまったのですが、すべて削除するにはどうしたらいいですか」

以前、女子高生が泣きながら相談をしてきたことがある。女子高生は被害者ではあるが、それ以前にデジタルカメラで裸の写真を撮らせること自体の警戒心不足を叱咤した記憶がある。

トラブルにあっている相談者や被害者は自分に都合いいことしか言わない傾向がある。ネット社会も現実社会と同様、トラブルに至るまでには様々な背景や経緯があり、相手からよく話を聞き冷静に判断しないと的確なアドバイスができない。

警視庁の電話によるサイバー犯罪相談窓口には、子どもから高齢者まで、男女関係なく、全国から様々な相談が寄せられる。自分にとっての相談所にさえ話せず、どこを頼りにすればいいか悩んでいる人も多い。被害者多数の犯罪や最新の犯罪手口の動向をいち早く把握できるところは、様々な行政機関で設置している相談窓口である。

現在では情報技術の進化により、スマートフォンなどで撮影した写真にはＧＰＳ情報も記録可能となった。なにも意識せず、ブログやＳＮＳに自宅で撮影したと思われる写真を掲載すれば、その写真を見た第三者が自宅の位置まである程度把握できてしまうのである。

冒頭のような嫌がらせも、今の時代ならさらに問題だ。その写真を入手した第三者が悪用すれば、被害

者の自宅近くを徘徊する、脅迫して金銭要求するなど簡単に想像できるし、実際このような事件も発生している。

そして、インターネットに限らず一度流出した情報をすべて回収することはほぼ不可能である。企業や組織で保有している個人情報が漏えいすれば悪用されるだけでなく組織の社会的信用を失い、取り返しがつかないことになる。昨今内部犯行により大量の個人情報漏えい事案が発生したところであるが、情報を守るためには技術的対策だけでなく、人的対策も重要である。

現在、警察におけるサイバー犯罪の相談を受ける体制は、専用電話か、警察署の生活相談あるいは犯罪被害相談の窓口が主体である。しかし、今後は、ネットに関する些細なトラブルや悩みでも、都民・国民のサイバー犯罪の被害防止のために、警察がより相談しやすい、頼りにしたいと思われる存在として認識してもらえるよう

・場所（交番や駐在所などの警察施設）
・人　（警察官の情報セキュリティに関する知識）
・モノ（インターネットに接続可能なパソコンやモバイル端末）

の「物理的セキュリティ」対策を早急に整備する必要がある。

○　ネットに関する犯罪

「オンラインゲームで、やっと手に入れたレアなアイテムが盗まれました。犯人を捜して、取り返した

いです。」

サイバー犯罪は、冒頭のような一個人の仮想空間上のものから、社会の機能を麻痺させてしまうサイバーテロや、政府機関や先端技術を有する事業者等から情報の窃取するサイバーインテリジェンスなど、国家の根幹を脅かすようなサイバー攻撃まで、多岐にわたる。仮想空間で発生した犯罪であっても、現実社会での日々の生活に大きな被害が及ぶものが多い。

警察は、サイバー犯罪も他の犯罪と同様、犯罪の発生や検挙については早期に公表し、世間一般に広く関心を持ってもらうよう努め、被害の拡大防止や予防を図らなければならない。コンピュータや情報機器を利用したサイバー犯罪といっても、犯人はコンピュータではなく、それを操っている「人間」である。コンピュータ対人間の攻防ではない。

「ＳＮＳにおいては、日本は外国と比較して匿名での利用が多い一方、匿名だからこそのリスクの認識をしている割合も高い」という統計がある。今後は、振り込め詐欺に代表されるような、日本特有のサイバー犯罪が発生する可能性もある。被害者、加害者ともに、低年齢化が進んだり、女性技術者による犯罪が発生したりする可能性もあるかもしれない。よって、警察は、サイバー犯罪や相談窓口に寄せられる被害者の生の声をタイムリーに調査・分析して実態を解明するとともに、先見の明で未来のサイバー犯罪の兆候を見抜き、発生抑止に効果を出さなければならない。

また、サイバー犯罪を取り締まる警察が、サイバー犯罪の踏み台にされたり、気がつかないうちに加害者になったり、あるいはネットワークに侵入されて警察情報が盗まれるような被害を受けることがあって

は話にならない。

よって警察は、警察を標的としたサイバー攻撃による防御のため、

・情報（警察で扱う情報すべて）

・インフラ（情報システムなどのネットワーク基盤）

の「情報セキュリティ」対策を万全に整備する必要がある。

○　ネット社会の光と影

・情報の真偽

平成二五年四月、アメリカ合衆国のボストンで、爆弾テロにより多数の死傷者が出たことは記憶に新しいところである。

アメリカ政府は、国の総力を挙げて捜査するよう指示し、数日後に容疑者の写真と監視ビデオを一般に公開した。情報メディアを活用し、容疑者特定に関する情報提供を広く呼びかけたところ、大量の画像データと家庭ビデオなどが捜査当局に寄せられたという。あるＳＮＳにも瞬時に膨大な情報が集まったが、善意で寄せられた情報とデマ情報が情報の錯綜を生み、逆に混乱を招いたとも言われている。

インターネットには、正しい情報や有益な情報だけでなく、虚偽や何の根拠もない風評、個人的な意見など、様々な情報が氾濫している。インターネットの利用者は、それら莫大な情報に惑わされることなく、冷静に情報の真偽を判断しなければならない。正しく利用することを前提とした利便性―「光」―の面に

目が向きがちであるネット社会に於いて、潜在している危険性―「影」―の面を常に意識していなければならない。

私自身、電話でサイバー犯罪の相談を受け、相手にアドバイスをしたところ、その直後、相談者により、私が一言も言っていないことがネットの掲示板に書かれていたこともある。

「インターネット上の情報はすべて真実ではない」のである。

・情報の価値

警察学校の学生に「個人情報とは何か」「警察情報が流出したらどうなるか」を尋ねても、反応が鈍い。しかし、今まで教わったことがなければイメージできないのは当然である。学生には、一警察官として仕事上で扱う情報の重要性だけ理解するのではなく、一社会人として自分のパソコンやスマートフォンに保有している情報にもセキュリティ意識を持つ必要性を指導してきた。

世間には、多くのポイントカードと呼ばれるものが存在する。コンビニエンスストアやスーパーマーケットで買い物したり、ガソリンスタンドで給油したり、インターネットショッピングしたり、普段の生活に密着した金銭の支払いによってポイントが付き、ポイントが貯まると現金やプレゼントに交換できるサービスである。

ポイント付与によって客の囲い込みするという店サイドの目的はあるが、私たちが日常的生活でポイントカードを使用することで、多くの個人情報を提供していることを意識している人がどれだけいるのだろ

うか。

例えば、「歩いて三分位の近所に住む三〇歳の男性が、平日三回程度、夜八時前後に、コンビニエンスストアに寄って、約二分間で、いつも決まった銘柄のビール二本と二〇〇円前後のおつまみを、電子マネー決済で買っていく」というように。

「個人に関する情報を提供する」とは、その情報が「世間一般に漏えいする」「悪用される」「気がつかないうちに加害者になっている」というリスクがあることを肝に銘じなければならない。

ポイント制度を非難しているわけではない。リスクを承知の上で、自分自身で情報の価値を判断し、受け入れたり提供したりすべきであることを、世間一般に広く周知させる必要がある。

○災害対策に学ぶ

・東日本大震災

「すいませんっ、つかまっていいですか?」

平成二三年三月一一日一四時四六分、東日本大震災発生時、私は若い男性警察官と交番勤務に就いていた。私が交番勤務に就いて、約一カ月過ぎたころであった。

大きな揺れを感じ、すぐにストーブを消して歩道に出た。すると、右から三〇代位のひとりの女性が駆け寄ってきて、私の右腕につかまってきた。すると、左からも、しゃがみこんだおばあさんが四つん這いになりながら、私をめがけて冒頭のセリフとともに、私の左足首につかまった。

私自身が大きな揺れに耐え得る支えを探す間もなく、ふたりの女性に右上腕と左足首をガッチリと完全にロックされてしまったのである。

今振り返ってみると、通行人のふたりの女性はなぜ近くにいた男性警察官につかまらなかったのだろうかと思う。普通ならたくましい男性警察官を頼りにしそうなものだが、いざという時に頼ってしまう存在というのは、同性であることなのだろうか。

警視庁でも、「女性の視点を一層反映した警察運営」に重点を置き、「女性の力」をより積極的に取り込み、女性の視点を始めとする様々な視点を警察業務に反映させることが、常に変化する治安情勢に敏感に反応するという観点から、極めて重要であることを身をもって感じたものである。

・「自助・共助・公助」

災害対応や防災対策の考え方として、「自助・共助・公助」が大切だと言われている。

自助とは、自分の身は自分で守る、自己防衛

共助とは、助け合い、相談

公助とは、行政機関の対応、防止活動

を言う。言い換えると、「個人」・「地域」・「行政」がそれぞれの役割を担い、うまく連携を取ってお互い協力すれば、被害を最小限にできるという考え方である。

この「自助・共助・公助」の考え方は、ネット社会から身を守るための心構えとしても当てはまる。ネッ

ト社会において、行政機関としての警察は犯罪被害防止活動を行い、それぞれ個人が自己防衛の対策を施し、相談窓口として地域コミュニティのリーダーを定め、地域と一体になって信頼の輪を築くのである。

東日本大災害後は、情報化社会の利便性と問題点について検討した組織・地域が多かったと聞くが、「人と人のつながりの大切さ」を再認識する機会だったとも言われている。ネット社会においても、「共助」の存在は非常に重要である。

三　警察と連携した取り組み

○民間事業者と警察　～「サイバー犯罪・サイバー攻撃への対策」

コンピュータ技術の急速な進歩によりサイバーセキュリティに関する脅威も大きく変貌している。サイバー犯罪の発生当初は自己顕示を目的とした愉快犯的な嫌がらせなどが多かったが、最近では組織ぐるみで標的を定め、相手に察知されずに侵入し、情報の窃取や社会インフラの破壊など、被害が甚大なうえ手口の巧妙化も顕著になっている。

多様化するサイバー犯罪に対処するためには、警察と民間事業者との連携が欠かせない。サイバー攻撃手法や高度な犯罪手口の情報共有や、サイバー空間での異常事態発生時の早期通報や必要な証拠保全の協定締結など、官民連携体制は整備されつつある。

また、警察機関から委託された民間事業者が積極的な事件化と事案の未然防止を目的として、ネット上

の掲示板等に掲載されたわいせつ画像や児童ポルノといった違法・有害情報や、出会い系サイトで児童を性交等の相手方となるよう誘引する書き込みを警察に通報したり、掲示板管理者に削除要請するなど、サイバーパトロールを実施している。年々サイバーパトロールの需要が増しており、任務の拡大など更なる体制の強化が望まれる。

他にも、今まで以上に民間事業者に対して積極的な事件化への捜査協力を要請し、サイバー犯罪の被害の再発防止や拡大防止を強化していく必要がある。

サイバー犯罪は時間的・距離的制約がない。世界規模のサイバー攻撃から国家社会を守るためには官民一体となり、お互いの立場を理解したうえで、情報交換や協力体制をさらに強化していかなければならない。

また、危険性の周知と自己防衛の教示は警察の努めであり、サイバー犯罪に限らず様々な犯罪被害防止の推進運動を展開している。個人を標的にしたサイバー犯罪については、従来のポスター掲示やパンフレットの配布だけでなく、コミュニケーションツールやデジタルメディアの分野に強い事業者とパートナーシップを組み、テレビCM、無料冊子、メールやインターネット、スマートフォンのアプリなどのメディアの力を最大限に活用していくべきである。情報発信や伝達手段も時代や対象となる世代に合わせて変えていかなければ、都民・住民の心には響かない。

○　教育機関と警察　～「子どもに対する情報リテラシー教育」

警察や教育機関が学校に出向いて実施する「交通安全教室」。簡単な交通ルールや標識を指導するだけでなく、疑似的に危険な体験をさせたり見せたりすることによって、交通安全の重要性を理解させるスケアードストレイトという教育手法がある。学校の校庭で、後部座席に人形を座らせたオートバイのドライバーと走行中の自動車が実際に衝突して、人形が吹っ飛ぶ事故現場の再現等を子どもたちに見せることによって、交通事故の危険性を理解させるのである。

インターネットの危険性についてもこの手法による体験授業を積極的に推進すべきである。警視庁では、身の回りに発生しやすい犯罪を題材にあげ、サイバー犯罪対策シンポジウムという公開授業を年に一回実施している。過去には、

・出会い系サイト
　～学生が出会い系サイトに自由に書き込み、男性の先生が女性になりすまして誘い出す
・ワンクリック詐欺
　～プレゼントの勧誘メールのリンク先をクリックし、料金請求される
・フィッシングサイト
　～母校のフィッシングサイトにアクセスし、個人情報が盗まれる

などを実施してした。

最近では、ネット事業者が学校に出向いてスマートフォンを使用した講義を実施したり、総務省も教員のためにインターネット教育用の教材を提供しており、インターネット教育に関するアプローチ方法は充実してきている。今後は、警察とネット事業者が協力して、メールやインターネットの疑似的な危険体験ソフトを作成して活用したり、警察官との合同授業を実施する体制づくりを積極的に推進すべきである。子どもたちには危険な体験だけでなく、犯罪につながることを理解させるために、警察官が説明することが有効である。

「トラブルに遭遇した経験のある青年のリテラシー力が高い」という統計がある。情報化社会では、情報活用能力よりもトラブル対処能力の有無が、将来的に大きな格差につながっていくのではないだろうか。

警察と教育機関が協力して、子どもたちにインターネット利用に潜む危険性を教え、正しい利用方法を身につけさせるとともに、保護者に対してもインターネットの利用に関する家庭内のルール作りや適切な管理の必要性について啓発するなど、保護者の理解や協力が不可欠であることを積極的に訴えていくべきであり、安全で安心なインターネット教育環境の整備に取り組む必要がある。

また、教育機関は子どもをはじめとする多くの個人情報を扱っているため、学校のインターネット環境におけるセキュリティ対策を万全にしつつ、インターネット教育にも積極的に取り組んでいかなければならない。今後は警察と教育機関が連携して、セキュリティ対策の相談対応やチェック体制の整備を推進し、情報リテラシー「情報の価値や真偽を見極め、活用する能力」を身につけるための教育制度の充実化を図る必要がある。

○　都民・国民と警察　～「地域コミュニティの構築」

警察は、地域コミュニティとの防犯体制を構築し、防犯講和やキャンペーン、災害訓練など定期的に実施している。問題は、このようなイベントは自分の意思で参加するものであり、不参加の人たちにどれだけ防犯意識を持ってもらうかということである。つまり、不参加が多い高齢者や一人暮らしの若者たちが、いかに興味を持ち、防犯意識を掘り起こし、真剣に取り組んでもらうかが大きな課題なのである。

若者の場合、情報を得る手段は、新聞や人との会話よりテレビやインターネットなどから得る情報が主である。スマートフォンやモバイル端末などの情報機器にかかわらず、インターネットを利用するからには利用するためのルールやマナー、あるいは利用する側の自己責任ということを十分認識させるための取り組みを強化しなければならない。

民間事業者との連携が重要であることは前述のとおりだが、警察と連携しているのは重要インフラ業者をはじめとする大手企業が中心である。今後は、警察－警察署であれば管轄警察署－が地域に密着した中小企業や団体を中心に、組織全体に対するサイバーセキュリティ対策や、組織に属している職員に対する個人所有の情報機器のセキュリティ対策についての防犯指導を実施する必要があるのではないだろうか。

地域が一丸となってお互いに助け合い、「必要な時に、必要な人に、必要な情報が行き届く」システム作りを推進し、子どもから高齢者まで、「ネット社会の自助・共助・公助」の普及を急ピッチで整備する必要がある。

○　警察を含む行政機関　～「対処能力の強化とスピード」

「検挙に勝る防犯なし」と言われるように、警察は年々悪質巧妙化するサイバー犯罪に対して傍観しているわけにはいかない。サイバー犯罪に対処するため、サイバー犯罪捜査要領等や情報通信技術に係る知識を備えたサイバー犯罪捜査員を育成することが急務である。そして、警察は急増しているサイバー犯罪やサイバー攻撃の取締まりを強化するだけでなく、未然防止活動も積極的に展開していかなければならない。

時代とともに犯罪の態様が変化し、それに呼応して捜査手法も変化し、都民・国民の警察に対する意識やニーズも変化する。警察も保秘主導の事件捜査から、近年では犯罪の発生の速報とともに注意を呼びかけるメールの運用や、情報提供の協力を要請する公開捜査のツィッターの運用を開始するなど、情報発信を積極的に展開するようになってきた。

しかし、日本の警察では、前述したボストンマラソンの例のような「情報提供を受ける」体制がまだ十分整備されているとは言えない。事件捜査だけでなく、幅広く犯罪に関する相談対応や情報収集をするためには、警察と都民・国民との間で、情報のキャッチボールができるインタラクティブな仕組みを構築し、信頼関係に基づいた協力体制や捜査環境を作るべきである。そして、私たち警察官は、タイムリーに社会の変化や都民・国民の要望を的確に捉え、期待と信頼に応えなければならない。

私たちが生活している「現実社会」の犯罪防止のパトロールや犯罪発生時の一一〇番通報と同じように、

「ネット社会」のサイバーパトロールや一一〇番通報の窓口が設置されているが、あまり広く周知されていないのが実態である。他にも、行政機関や各種事業者が提携し、様々な犯罪やトラブルの相談専門窓口が設置されているのだが、広く活用されないと意味がない。専門の相談窓口でもいい。交番でもいい。家族・親族でもいい。会社の先輩後輩や同僚、友人でもいい。都民・国民の平穏な生活を見守る交番のような存在の、ネット社会における自分自身の相談所を、身近に置く必要がある。そして警察は、ネット社会においても、都民・国民の平穏な生活をいつでもサポートできる心構えや知識を持ち合わせていなければならない。

情報化社会の今、インターネットを活用すれば、ある程度の確かな情報を収集することができる。調査するテーマやキーワードが同じであれば、検索結果もほぼ同じ情報を得ることができる。問題はスピードである。サイバー空間における時間の流れや技術の進歩に対応するためには、スピード感が重要である。

現在、サイバーセキュリティ基本法案が審議中である。産業界との情報交換、最新技術の調査、世界の犯罪動向の把握をいち早くキャッチし、早期に対応していく必要がある。

四．終わりに

私は、現在、警視庁全体にインターネット環境を網羅、整備する業務に携わっている。サイバー犯罪の捜査環境をさらに充実させ利便性を確保するとともに、都民・国民との窓口である各警察署の受付や、交

番などへのインターネット環境を整備充実させ、より親切な都民応接や住民サービスの向上を目標とした構想に基づいている。例えば、直接都民と接する警察機関にインターネットを活用できるモバイル端末があれば、地理案内や外国人対応にも大いに役立つであろう。

日本政府は、二〇二〇年の東京オリンピック・パラリンピック大会に向けて「世界一安全な国、日本」を創り上げる取り組みを開始させた。また、「世界最高水準の安全なサイバー空間の構築」も戦略に盛り込まれている。オリンピックの成功には、サイバー空間を含めた社会のセキュリティ対策が必須である。

現実社会もサイバー空間も変わらない。そのインテグレーションされた無限の世界は、産学官民一体となって「人」「知識」「情報」をフル活用した基盤整備によって、安全安心な街となっていく。

私たち警察は、都民・国民に対し、安全・安心を守っていくことが責務であり、犯罪のない社会の実現に貢献していきたい。

【参考文献】

・「青少年のインターネット・リテラシー指標等」平成二五年度版（総務省総合通信基盤局消費者行政課）
・「情報通信白書」平成二五年度版（総務省）
・「インターネット白書」二〇一三、二〇一四（株式会社インプレスR&D）

中高生のネット利用と「炎上」

東京大学大学院生
（総合文化研究科一年）
鈴木　あい（23）

第一章　中高生へのＳＮＳの拡がり

一―一　スマートフォンの普及

インターネットは今や社会インフラとして定着し、携帯電話やパソコンなどで手軽に情報交換ができるようになった。そして、スマートフォンの普及とともに、ＳＮＳ（Social Networking Service）が急速な

勢いで拡がりを見せている。デジタルアーツ㈱の調査[i]によると、何らかの携帯電話を持つ未成年者（一〇～一八歳）のスマートフォン所有率は五九・一％である。所有率を学校種別で見ていくと、小学校高学年（一〇～一二歳）三一・六％、中学生五四・九％、高校生九〇・八％で、女子高校生は九五・一％にもなるという。ＳＮＳ（Social Networking Service）とは、「ネットコミュニケーションサービスの一つで、ネット上で人と人とがつながるためのサービス」（田代、服部 二〇一三：七三）で、広範に「社会的な対人コミュニティを形成できる機能を提供するサービス」（櫻庭 二〇一〇：四九）を指すという。サービスには、Facebook や mixi などの個人のつながりが中心のサービス、ＬＩＮＥや Twitter など、チャット的な会話を楽しむサービス等がある。

一―二　ＳＮＳの利用状況

ここで、代表的なＳＮＳにおける高校生の利用状況を見ていきたい。総務省情報通信政策研究所と東京大学大学院情報学環・学際情報学府橋元良明研究室が共同で行った調査[ii]によると、代表的なＳＮＳにおける高校生の利用率は図一のようであったという。ＬＩＮＥの利用率が全体で八五・五％と最も高く、Twitter（六六・九％）や Facebook（二四・三％）がこれに続く。また、これらＳＮＳの利用目的としては、「友達や知り合いとコミュニケーションをとるため」（七一・八％）、「ひまつぶしのため」（五二・三％）、「学校・部活動などの事務的な連絡のため」（四八・九％）等が挙げられる。また、ＳＮＳを利用する際、悩んだり負担に感じたりすることとしては、全体では「あてはまるものはない」が四〇・九％で

最も多いが、「自分が書いてしまった内容について、後から『あれで良かったか』などと悩む」（二七・七％）、「メッセージを読んだことが分かる機能があること」（二二・四％）、「友だちとのやりとりをなかなか終わらせられないこと」（一七・六％）、「自分の書いたメッセージに反応がないこと」（一五・九％）等、多くの生徒が負担に感じることがあるという結果となっている。

一―三　「つながり」への強迫観念

橋元良明は、このような状況を鑑み、以下のように述べている。「ソーシャルメディア[iii]に没入する動機は人それぞれであるが、正の報酬として、孤独感が癒やされ、自分の心情や考えを多くの人に知ってもらえるという充足感がある。と同時に、ソーシャルメディアにアクセスしないと、親しいグループから仲間はずれにされたり、陰で悪口を言われたりするのではないか、という不安から頻繁にアクセスする人も多い。（中略）中高校生では、極端な場合、ソーシャルメディアでのつきあいをおろそかにするといじめにあうことすらある。グループの中心的なメンバーが、ささいな行動や心情をソーシャルメディアでつぶやくと、実際に賛同あるいは感心したか否かにかかわらず『いいね』ボタンを打たざるを得ず、質問形のメッセージには、すかさず回答を返さなければならない。（中略）スマートフォンは、従来型携帯電話よりネットへのアクセスがスムーズで簡便になった。（中略）その結果、以前よりさらに、居場所にかかわらず即答が要求される」。

橋元は、このような状況を「スマートフォンで加速する『つながり』への強迫観念」と表現している。

先述したように、中学生の過半数、高校生の九〇％以上がスマートフォンを所有している。また、現代の中高生にとって、ＳＮＳは、友人関係を構築、維持していくうえで、なくてはならない存在となっていると言えるだろう。そして、スマートフォンの普及、ＳＮＳの急速な拡がりの中起きている「つながり」への強迫観念とともに問題となっているのが、ネットの「炎上」である。

第二章　ネットの「炎上」

二―一　炎上の変遷と現状

ネットの「炎上」とは、「サイト管理者の想定を大幅に超え、批判や誹謗中傷が殺到すること」（田代、服部 二〇一三：一六〇）だという。二〇一三年頃から、Twitterをはじめとしたネットに投稿した写真が原因で「炎上」と呼ばれる騒動に発展する事態が多発している。

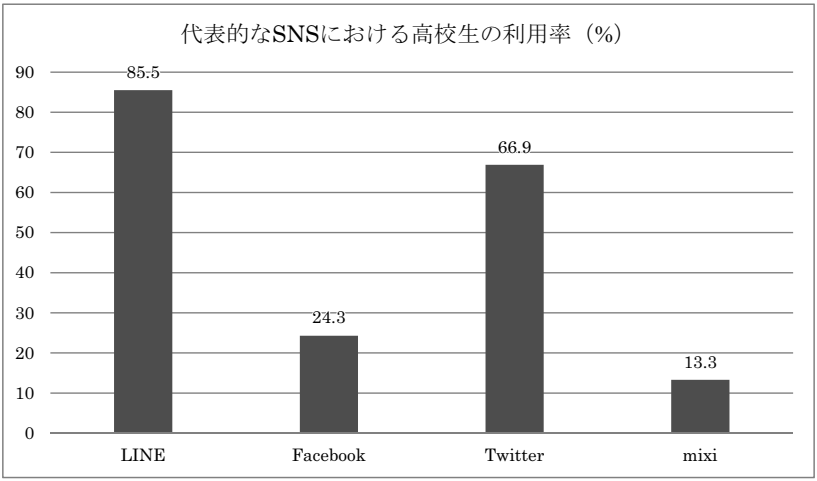
なぜ今炎上が多発しているのだろうか。ネットが普及する前の一九九〇年代前半は、利用者数も限定されていた。そのため、当時も誹謗中傷はあったが、誰が誰を攻撃しているか推察することがほぼ可能であったという（田代、服部 二〇一三：一六一）。しかしながら、二〇〇〇年代に入り、ブログやＳＮＳなどが普及した（田代、服部 二〇一三：一六二）。個人が手軽にＳＮＳなどを始め、気軽に情報を発信し、交流できるようになった反面、「不適切な情報発信」によりページに批判が殺到、どこの誰か分からない不特定多数の人々により炎上させられてしまうという事態が多発しているのである。ひとたび炎上が起

こってしまうと、不適切な情報が拡散するだけではなく、当事者は個人情報まで調べられ、勤務先や在籍する学校、内定先に「電凸（不適切な情報発信を行っていたことを電話で告げられること）」される。その結果、停学や退学の処分を受ける、内定先から内定を取り消されるといった事態が起きているのである。

二―二　不適切情報とは

炎上を引き起こす不適切情報とはどのようなものなのだろうか。「コンビニのアイスクリーム用冷凍庫に横たわる」「ピザ生地に顔を押しつける」「全裸でチェーン店のカウンターで食事をする」「食器洗い機に身体を押しこむ」…どれもTwitterに投稿された写真についてである。特に目立っているのは飲食店などの店員や客による悪ふざけツイートが次々に炎上したことだ。多摩市では、アルバイト店員による不適切なツイートにより老舗そば店が閉店に追い込まれる騒動まで起

【図表１　代表的なSNSにおける高校生の利用率 出典：総務省情報通信政策研究所「高校生のスマートフォン・アプリ利用とネット依存傾向に関する調査」より筆者作成】



こっている。これまで炎上したツイートは、未成年の喫煙・飲酒や、無免許、飲酒運転などの違法行為、勤務時間中にアルバイトが冷蔵庫に入ってみせるような不衛生な行為など様々であるが、その多くは未成年によるものである。

二―三　「正義すぎる人たち」がパトロールする社会

炎上「させる」側にはどういった意図があるのだろう。ダイヤモンドオンラインの調査[iv]によると、「炎上に参加して、対象者を『懲らしめよう』という人には賛同できる?できない?」という質問に対して、「賛同できる」と答えた人は二三%に上る。その理由としては、「インターネットは怖いという認識をもってもらえると思うから」「叩かれることで常識を知るきっかけになると思うから」「警察のような組織があるわけではないので、多少晒し者にする人がいないともっと酷くなるだろうから」「社会的制裁を受けて然るべき対象であるから当然の報いだと思うし、正直こちらに大したリスクはないから」「ネットの怖さをわかっていないから見せしめに」「懲らしめないと何もなく終わってしまうから」等といったものであった。「晒し者」「社会的制裁」「見せしめ」「懲らしめないと」という言葉からは、不適切な情報を拡散することによる「私刑」の意図があることが分かる。なかには「正直こちらに大したリスクはないから」というコメントのように「軽い気持ち」で拡散している様子の人もいるが、多くの人は、「悪いことは悪いと言わないといけない」という正義感に駆られて炎上に参加しているようだ。

作家の石田衣良はこれらの事態を受け、「正義すぎる人たち」と題し、ネット上のコラムにおいて以下

のように述べている。「この手のおバカ画像が炎上するパターンは決まっている。誰かが投稿した写真を、許せないといって別な誰かが探しだし、それにコメントをつけて、あちこちのＳＮＳで『晒す』のだ。拡散した画像を見た人たちが、なぜかひどく怒って、飲食店やコンビニに苦情電話やメールが殺到する。実際にはその地域に住む人でも、その店の常連でもない無関係の人間だ。（中略）不思議なのは、この手のおふざけ画像を探すためにネットを周回しているパトロール役がいること。見つけだすや、すぐに晒して火をつける者が存在するのだ。たいていは良識ある正義の味方の振りをして、過剰なまでにクレームをつけ、店側の対応を求める。（中略）おバカ写真一枚は果てしなく責任を追及されてしまうほどの罪なのか。ぼくが今の社会で息苦しく感じるのは、過剰なまでに正義を求める人たちの存在だ。（中略）怖いのはいつの時代も正義で、とくになんらかの刺激でプライドを傷つけられた正しさだ。自分が正義のサイドにあると信じる人たちの執拗さと復讐ほど恐ろしいものはない。考えてみると、（中略）『傷つけられた正義』によって裁かれた人たちが無数にいる。マスコミは集団リンチのように仕事を辞めるまでつつきまわす。しかも、正義と嫉妬を基にしたセレクトなので、つぎに誰が狙われるのかわからない。おバカ画像の若者も、（中略）〝犯罪者〟ではないのだ。まったく『正義すぎる人たち』は恐ろしい」。

石田の指摘する様に、これら一連のＳＮＳにおける炎上騒ぎにおいて、犯した違反と受ける罰の間に不均衡が認められる。本稿でみてきたように、これら一連の炎上事件の発端となったツイートをしたのは多くが未成年である。しかし、未成年であったとしても「この社会」は許さない。「正義すぎる人たち」がパトロールするこの社会においては、これらの不適切な情報発信をした人々は「犯罪者」なのである。

また、鈴木謙介は、炎上に繋がるような出来事というのは、対象となる人の振る舞いに対して、道徳的な立場から批判する人々、そして「正義」を建前に、おもしろがって批判している者によって引き起されているということ、そして、炎上におけるロジックとしては、「ネットで見つけた非道徳な振る舞いを糾弾する」という構図が存在することを指摘している（鈴木 二〇〇七：二〇八）。「道徳」と「正義」、この二つの言葉が現在のネット炎上を表すうえでキーワードとなるだろう。

二―四　デジタル・タトゥー（Digital Tattoo）

ここで、「デジタル・タトゥー（Digital Tattoo）」について説明したい。これは、二〇一三年二月にカリフォルニア州で行われた「TED Conference」において、生物科学関連のベンチャーキャピタルの役員やゲノム研究と投資を行う企業のCEOを勤めているファン・エリンケス氏が語った言葉である。これは、電子的な入れ墨、という意味合いだ。入れ墨を消すのは難しいと知られているが、我々が生活する中で、こうした入れ墨をデジタル空間で残し続けているという指摘である。エンリケス氏は、スピーチの中で、能動的な投稿（例：SNSへの投稿）や受動的な結果（例：Google等検索エンジンの検索履歴）に関わらず、人間の行動によってデジタルデータが記録され、ほぼ永久に蓄積されていくとし、「人間は不死になった」と表現する。つまり、ネット上に一度上がってしまった情報（＝「デジタル・タトゥー」）を完全に消すことは非常に難しく、自分の名前で検索をかけると、何年経っても過去の炎上事件がヒットしてしまうこ

とになりかねないのである。

このように、現代においては、たった一度の「軽微な呟き」（情報発信）による炎上は「厳格に処分」されるだけでなく、デジタルで記憶され、進学や就職を含め一生に影響を及ぼすことになるのである。

第三章　問題提起

これまで、中高生へのスマートフォンとＳＮＳの普及、そしてその状況の負の側面と言える「つながり」への強迫観念、ネットの炎上を見てきた。筆者は、これらの状況を受け、主に以下の二つの問題を提起したい。

三―一　中高生たちのネットの「閉鎖性」と「閉じられたメッセージ」

炎上のいくつかのケースは、本人は友人だけに公開しているつもりのサイトが、掲示板などを通じて「晒し」に遭うことをきっかけに生じたものである（鈴木 二〇〇七：一二五）。鈴木によると、若者たちが、世間からは「見えない」と（彼らには）思われている携帯電話向けのウェブサイトで、自分たちの手の届く範囲に閉じられたメッセージを送り合い、そしてその「閉じられた」ネットでの関係性が相互依存的で、強迫的なものになるケースも頻繁に生じるようになっているという（鈴木 二〇〇七：一二六）。この鈴木の指摘、そして先ほどの橋元の「『つながり』への強迫観念」という指摘を受け、筆者は以下のように考える。

中高生にとっては、ＳＮＳの世界はあくまでも友人同士のみがつながっている「閉じられた」世界であり、また、その「閉じられた」世界において「つながり」を求められる中、「友人に注目されたい」との気持ちから、（結果的に）不適切な情報を発信してしまうということが多いのではないか。ネットは世界中に開かれた空間である。しかしながら、中高生にとってネットは「内輪」であり、その中の仲間から注目、賞賛されたいがために取った行動が、炎上につながるのである。

三―二　ネットの利用者拡大と炎上、体感治安

次に、「体感治安」について考えてみたい。「体感治安」とは、国民が治安に対して抱いているイメージいし意識をいう。内閣府が実施した、二〇〇六年の「治安に関する世論調査[v]」によると、「ここ一〇年間で日本の治安はよくなったと思うか、それとも悪くなったと思うか」という問いに対し、「よくなったと思う」とする者の割合が一一・三％（「よくなったと思う」二・四％＋「どちらかといえばよくなったと思う」八・九％）、「悪くなったと思う」とする者の割合が八四・三％（「どちらかといえば悪くなったと思う」四六・六％＋「悪くなったと思う」三七・七％）であったという。また、警視庁が実施した、二〇一二年七月の調査[vi]によると、現在の東京の治安について「悪くなった」「とても悪くなった」と答えた人は全体の三三％で、「とても良くなった」「良くなった」との回答（二七％）を上回った。自分や家族が犯罪に巻き込まれる不安を感じている人は七七％に上り、「感じていない」との回答は二二％にとどまった。ちなみに、『犯罪白書』によると、日本の刑法犯の認知件数は、二〇〇二年には戦後最多件数を記録

した。しかし、その後二〇〇三年から減少、二〇一一年には二〇〇二年の約三分の一の件数となった。それにもかかわらず、多くの人々が体感治安の悪化を感じている。

筆者は、ネットの利用者拡大が「体感治安」悪化に大きな影響を与えていると考える。ネットを通して、私たちは日々多くの情報を手に入れている。その反面、犯罪の情報にも触れやすくなったため、それが人々の「体感治安」の悪化にもつながっていると言えるのではないか。

また、さらに指摘したいのが、このようにネットの拡がりが生み出した「体感治安」の悪化を背景に、不適切な情報発信をする者、その中でも特にまだ若い中高生を「リスク・ファクター（危険因子）」とみなし、炎上という「厳格な処分」を与える動きがあるのではないかということである。先述したように、炎上「させる」側の理由として、「多少晒し者にする人がいないともっと酷くなるだろうから」というものがある。「ただでさえ治安は悪くなっている。不適切な情報発信をする若者が将来大人になった時、これ以上の『犯罪』を犯さないよう（＝治安が悪化しないよう）いま『厳格に処分』しよう」－このような考えが、ネットの炎上の背景にあるのではないだろうか。

一方で、筆者は、不適切情報を発信する側でもなく、炎上「させる」側でもない、つまり炎上を見ている人々の体感治安へも、炎上が影響を与えると考える。炎上で用いられる批判、バッシングの言葉は、しばしば目を覆いたくなるほど冷酷なものであることが多い。また、不適切情報を発信した者に対して行われる「制裁」の中には、「その者の名前、住所、写真を掲示板に晒される」といった、「やりすぎではないか」と感じられるようなものもある。筆者は、このような炎上を目撃することで、あたかもウェブ全体が

炎上、そしてネット利用者の多くが「悪」であるかのように映ってしまい、不信感や不安感が広がり、それが「体感治安」悪化を加速させているのではないかと考える。

第四章　提言

以上、大きく分けて二点問題を提起した。ネットの最大の特徴である「世界中に開かれた空間」という点の十分な理解がほぼ欠けている状態で、中高生のネット利用が拡大しているのだ。また、ネットは人々の「体感治安」悪化の加速の大きな要因となっている。

これらを指摘したうえで、中高生がネット社会を安全に暮らすために筆者が提言したいのは、以下の二点である。

四ー一　教員と保護者を交えたメディア・リテラシー教育

まず、中高生へのメディア・リテラシー教育の充実を提言する。郵政省「放送分野における青少年とメディア・リテラシーに関する調査研究会」がまとめた報告書によると、青少年が獲得すべきメディア・リテラシーを「一．メディアを主体的に読み解く能力」「二．メディア機器を活用する能力」「三．メディアを通じてコミュニケーションを創造する能力」と類型化したうえで、「メディア社会を生きる力」と定義づけている。メディア・リテラシー教育に取り組んでいる学校はすでにあるとのことだが、先述したよう

に、中高生を含め未成年の不適切な情報発信による炎上は多発しており、さらなるメディア・リテラシー教育の充実が必要であると考える。

ここで主張したいのは、メディア・リテラシーを、子どものみならず、教員と保護者がともに学んでいくべきということである。内閣府が二〇〇九年から毎年実施する「青少年のインターネット利用環境実態調査」によると、二〇一三年のフィルタリングの利用率（携帯電話・スマートフォン）は小中高校の全年代で五五・二％と、前年の六三・五％から初めて減少した。背景には、その多機能さゆえに、親世代の知識が追いついていない事情があるという。ＫＤＤＩ中部総支社管理部の角真由美氏は「子供に言われるままに保護者がフィルタリングを外してしまうケースもある」と話す。

このような状況から、学校の授業で生徒のみに対してメディア・リテラシー教育を行うのではなく、教員と保護者もともにメディア・リテラシーを学んでいく必要があるのではないか。筆者は、中学校や高校の参観日に、教員・保護者・生徒が一緒になり、ワークショップ形式で、基本的なスマートフォンの使い方から、スマートフォンやＳＮＳを利用する上で悩んでいること（すぐに返事をしなくてはならない、自分の書き込みに対する友人の反応が気になる等）、実際の不適切情報発信による炎上の事例について「何が問題だったか」等を話し合うことが、メディア・リテラシーを身につけ、ネット社会を安全に暮らしていく上で有効ではないかと考える。これにより、教員や保護者が、子どもたちがスマートフォンやＳＮＳをどのように利用しているか、それらを利用する上でどのようなことを悩んでいるのか、情報発信する場合の注意点について理解しているか等を知ることができるだけでなく、自分たち（教員、保護者）

もスマートフォン、ＳＮＳについての理解を深め、子どもと一緒に「今後スマートフォン、ＳＮＳをどのように利用していくべきか」ということについて「対等に」話し合うことができるようになるのではないだろうか。また、ワークショップには、電気通信事業者といった専門家に参加してもらうのもよいと考えられる。

四―二　「忘れられる権利」の議論の必要性

二〇一二年一月、欧州連合（ＥＵ）は、「一般データ保護規則案（General Date Protection Regulation）」を提案し、第一七条に「忘れられる権利（right to be forgotten）」を謳った（田代、服部二〇一三：七二）。「忘れられる権利」とは、ネット上に掲載された不適切な個人情報の削除を求める権利である（『朝日新聞デジタル』二〇一四年七月一二日）。世界で初めて「忘れられる権利」が認められたのは、二〇一二年一一月、フランスの女性がGoogleに対し「過去の写真の消去」を請求して勝訴するという判例であるが、日本においても、検索エンジンのサジェスト機能で履歴を削除する判例がでている（田代、服部二〇一三：七二）。また、Googleは米国時間二〇一四年七月二五日、五月以降に同社が受理して対応した「忘れられる権利」の要請のうち、半数以上を承認したことを明らかにした。その結果、数万件のリンクがGoogleのサイトから削除されたという。五月から七月一八日までの間に同社に寄せられた要請の数は九万一、〇〇〇件で、関係するウェブページの数は三二万八、〇〇〇件以上だったという。

しかしながら、ネット社会におけるこのような新たな権利が求められている一方で、課題も存在する。

まず「表現の自由」と「知る権利」との両立である。ネットが個人の「履歴書」として機能することが、公共の安全に資する面も大きく、㈱情報通信総合研究所の中島美香氏は「公共性及び公益目的を有する言論となりうる公務員あるいは犯罪者等に関わる言説については、当事者の申し立てにより削除が命じられることには問題がないか、『表現の自由』との関係で、検索エンジンという『メディア』のあり方が問題となる可能性がある」と指摘する。どこまでがプライバシーとして守られる部分で、どこからが「表現の自由」という線引きは慎重にする必要がある。他にも、削除要請にこたえる企業側の負担等、現状ではまだまだ検討が不十分である。

筆者は、削除基準等について有識者で議論することはもちろん重要であるが、その中で、炎上が、炎上「してしまった」者の将来へ及ぼす影響について十分に検討すべきであると考える。先述したように、未成年は炎上のターゲットとなりやすく、たった一度の「呟き」による炎上は「厳格に処分」されるだけでなく、「デジタル・タトゥー」として一生に影響を及ぼすという現状がある。石田が指摘するように、彼らは「犯罪者」ではない。ネットが個人の「履歴書」として機能する面があるのは間違いないが、このような中高生の炎上に関しては、「忘れられる権利」を行使し、彼らがこれからの将来に向けて「やり直せる」環境を提供することが必要ではないだろうか。また、炎上というあまりにも大きすぎる「お祭り騒ぎ」による体感治安の悪化という負の側面を回避するうえでも、このような対応が必要ではないだろうか。

第五章　結語

ネット社会はさまざまな変化を伴いつつ、これからも拡がりつづけていくだろう。それとともに、中高生にとってのネット、ＳＮＳというものの存在も大きくなることが予測される。先ほど述べたように、中高生にとっては「現実社会」よりも「ネット社会」のほうが「大事」なものとなりつつある現実がある。本稿においては分量の関係で詳しく言及することはできなかったが、ネットで知り合った人と実際に会ってみたいという「リアル化」を望む声は、女子高生においては五六・六％にもなるという調査もある（『日経産業新聞』二〇一四年七月一五日）。このことからも、中高生にとっての「ネット社会」の「現実社会」に対する「優位性」をみることができるだろう。

筆者は、子どもたちが、ネットを「正しく」利用すること、そしてその便利さの裏にある負の側面を、教員・保護者も交え、ともに学んでいく必要があると考える。そして、最終的には、「メディア社会を生きる力」を身につけるうえで必要なことを、教員・保護者・生徒それぞれが自分で考えることができるようになることが大切であろう。一方で、万が一中高生の情報発信による炎上が発生した場合、彼らが将来に向けて「やり直せる」環境を提供することが必要ではないだろうか。

本稿が、ネット社会の安全に寄与することを願いつつ、本稿を結ぶことにする。

〈参考文献〉

・櫻庭太一　二〇一〇『インターネット文化論－その変容と現状』専修大学出版局
・鈴木謙介　二〇〇七『ウェブ社会の思想〈遍在する私〉をどう生きるか』ＮＨＫブックス
・田代光輝、服部哲　二〇一三『情報倫理－ネットの炎上予防と対策－』共立出版
・放送分野における青少年とメディア・リテラシーに関する調査研究会報告書

〈参考新聞記事〉

・「メディア読む力『育成を』　青少年向け、教材開発を支援－郵政省」『毎日新聞』二〇〇〇年六月二四日／二九ページ
・「見知らぬ人と『親友』『恋人』、ＳＮＳ子供に迫る危険－『実際に会いたい』四割、犯罪被害の温床に（日経ＢＰ専門誌から）」『日経産業新聞』二〇一四年七月一五日／二ページ

〈参考ＵＲＬ〉

・《未成年の携帯電話・スマートフォン使用実態調査》
http://www.daj.jp/company/release/2014/0714_01/
・高校生のスマートフォン・アプリ利用とネット依存傾向に関する調査
http://www.soumu.go.jp/iicp/chousakenkyu/data/research/survey/telecom/2014/internet-addiction.pdf

・「ネット依存」の日本的特徴は「きずな依存」
http://www.nippon.com/ja/currents/d00102/
・ダイヤモンドオンライン ザ・世論~日本人の気持ち~
「ツイッター炎上」をつくるのは誰か 炎上する側、させる側の論理
http://diamond.jp/articles/-/43633
・石田衣良 正義すぎる人たち
http://news.infoseek.co.jp/article/r25_appli_11221100000068997
・あなたの情報は、死んでもネット上を漂い続ける…
「デジタル・タトゥー」問題とは何か?
http://diamond.jp/articles/-/39794
・治安に関する世論調査 内閣府大臣官房政府広報室
http://www8.cao.go.jp/survey/h18/h18-chian/
・「犯罪に遭う不安ある」七七% 警視庁が体感治安調査『日本経済新聞』
http://www.nikkei.com/article/DGXNASDG2005H_R20C12A9CC0000/
・犯罪白書
http://hakusyo1.moj.go.jp/jp/nendo_nfm.html
・グーグル、「忘れられる権利」で諮問委 削除基準を議論『朝日新聞デジタル』
http://www.asahi.com/articles/ASG7D44MMG7DUHBI00V.html
・〝忘れられる権利〟はネット社会を変えるか?
http://www.nhk.or.jp/gendai/kiroku/detail02_3219_1.html

・グーグル、「忘れられる権利」要請の五〇％以上に対応
http://japan.cnet.com/news/service/35051443/
・「忘れられる権利」表現の自由とプライバシーの境はどこか?
http://app-review.jp/news/192152
・スマホ閲覧制限、普及急げ 利用率、小中高で減少 静岡
http://sankei.jp.msn.com/region/news/140226/szk14022602180000-n1.htm

i　調査対象：何らかの携帯電話・スマートフォンを持つ全国の一〇歳から一八歳の男女及び全国の〇歳から九歳の子どもを持つ保護者
調査期間：二〇一四年六月二〇日～二四日
調査方法：インターネット調査
有効回答数：一、二一八サンプル（未成年者六一八サンプル、保護者六〇〇サンプル）
実施機関：㈱マクロミル

ii　調査協力校：都立の全日制及び定時制の高等学校一五四校
調査対象：各高等学校において、各学年一クラスずつ抽出。
調査期間：二〇一四年一月七日～三一日
調査方法：無記名自記式質問紙調査。㈱山手情報処理センターにおいて、都立高等学校へ一括して調査票を郵送し、回収は学校が一括して返送。
有効回答数：合計一五、一九一票

iii　「SNS」と「ソーシャルメディア」の明確な定義、違いを説明することは難しい。しかしながら、橋元は「mixi、Facebook、Twitter などのソーシャルメディア」とウェブ記事上で述べていることから、本稿において筆者が使用す

る「SNS」の定義とほぼ同義で「ソーシャルメディア」という言葉を使用していると考えられる。

iv 調査対象：社会人男女五〇〇人。

調査期間：二〇一三年一〇月二三日。

v 全国二〇歳以上の者三、〇〇〇人を対象に実施、有効回収数一、七九五人。

vi 都内に在住または通勤・通学する九五四人を対象に実施、九二九人から回答（『日本経済新聞』二〇一二年九月）。

安全なネット社会を育てるために必要な教育

警察官（埼玉県警部補）
高井　俊孝（38）

一　はじめに

インターネットといえば、今や老若男女を問わず多くの国民が何らかの形で携わっており、日常生活に欠かすことができないものになりました。

今から一五年前、私が警察官を拝命した当時は、書類作成といえばワープロが主流であり、携帯電話も

カメラ機能やメール機能が画期的と考えられていた頃でしたが、現在は、書類作成のみならず、通信・伝達・決済に至るまでネットワークシステムを使用していますし、パソコンだけではなく、携帯電話、スマートフォン、ゲーム機等からもインターネットに接続できるようになったことで、その利用方法も多様かつ手軽になり、国民生活にもかなり密接してきているといえます。しかし、便利で生活に密着してきたぶん、インターネット関連の犯罪もより身近になってきており、その件数も増加しています。

ネット社会を安全に暮らしていくための方策について、本論文におきましては、若年層、特に一八歳未満の児童のインターネット使用にスポットをあてることにしました。インターネットは、どの年代も高い割合で使用していますが、一〇～二〇代は、利用割合が最も高く、流行に敏感で新しい物を積極的に取り入れようとする反面、社会的知識や経験に乏しい年代なので、ネット社会の危険性に直面しているのではないかと考えられるからです。また、児童のインターネット使用に関する問題は、児童の年代だけではなく、児童を指導する保護者等の年代の問題でもあり、幅広い年代を含んだ社会全体の問題として考えていかなければなりません。

初めに、インターネットに関係する事件で、児童が被害を受けた事件の比率や増加、実際に児童がどのような危険にさらされているのかなどを分析し、児童のインターネット使用が、いかに高い水準で危機に面しているか、危険性が年々高まってきているかを明らかにします。

次に、児童のインターネットに対する関わり方のうち、最も深刻なものは携帯電話からのインターネット利用であることを説明し、児童に対する学校の指導と保護者の指導を改善すべき点として焦点にあてま

す。

そして、学校と保護者の指導について、それぞれ児童を取り巻く環境、現在の指導とその問題点を挙げ、効果を上げるためにはどのような対策を行えば良いのか、その具体案を提言いたします。

二　サイバー犯罪における児童の割合

サイバー犯罪（不正アクセス禁止法違反、コンピュータ電磁的記録対象犯罪、ネットワーク利用犯罪）の検挙件数は、平成一三年は一、三三九件であったところ、平成二五年は八、一一三件と約六倍に増加しており、違法・有害情報を収集して警察庁に通報するインターネット・ホットラインセンターに寄せられる情報件数は、平成一九年（同センターは平成一八年開設）は一六、四一八件であったところ、平成二五年は一三〇、七二〇件と約八倍に増加しています。（警察庁サイバー犯罪対策統計）このように、インターネット関連の事件等は年々増加しており、十数年でその危険は私たちの生活により身近に迫ってきているといえます。

表1は、平成二五年までの三年間における、出会い系サイトやコミュニティサイトを起因として児童が被害を受けた事件の、罪種別被害児童数を表したものです。この表を見ると、児童買春、児童ポルノ法違反、青少年保護育成条例、及び児童福祉法違反（以下「児童買春等」と言う。）の罪名が全体の約九七～九八％を占めています。表2は平成一三年から平成二五年までのサイバー犯罪の検挙件数で、表3は、検挙件数

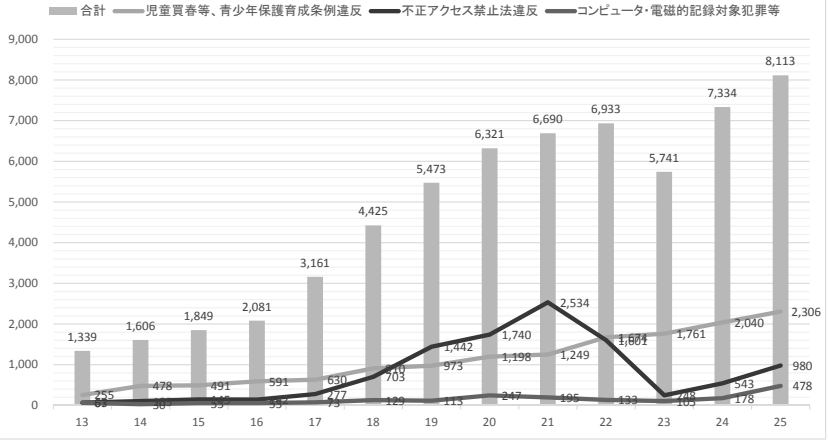
表1 【出会い系サイト・コミュニティサイトを起因として児童が被害を受けた事件の罪種別被害児童数】

		平成23年				平成24年				平成25年			
		出会い系		コミュニティ		出会い系		コミュニティ		出会い系		コミュニティ	
		件数（件）	割合（%）	件数（件）	割合（%）	件数（件）	割合（%）	件数（件）	割合（%）	件数（件）	割合（%）	件数（件）	割合（%）
重要犯罪	殺人	0	0	0	1.6	0	0	0	2.2	0	0	0	2
	強盗	0		0		0		2		0		1	
	放火	0		0		0		0		0		0	
	強姦	0		9		0		14		0		18	
	略取誘拐	0		1		0		2		0		3	
	強制わいせつ	0		7		0		6		0		4	
児童買春、児童ポルノ法違反	児童買春	160	97.2	176	98.4	117	97.2	182	97.8	71	96.9	226	98
	児童ポルノ	22		217		19		242		14		341	
青少年保護育成条例違反		46		637		30		596		31		678	
児童福祉法違反		46		38		46		32		38		22	
その他		8	2.8	0	0	6	2.8	0	0	5	3.1	0	0
合計		282		1085		218		1076		159		1293	

表2 サイバー犯罪検挙件数

区分＼年次	平成13年	平成14年	平成15年	平成16年	平成17年	平成18年	平成19年	平成20年	平成21年	平成22年	平成23年	平成24年	平成25年
合計（件） ④	1,339	1,606	1,849	2,081	3,161	4,425	5,473	6,321	6,690	6,933	5,741	7,334	8,113
不正アクセス禁止法違反	67	105	145	142	277	703	1,442	1,740	2,534	1,601	248	543	980
コンピュータ・電磁的記録対象犯罪等	63	30	55	55	73	129	113	247	195	133	105	178	478
ネットワーク利用犯罪	1,209	1,471	1,649	1,884	2,811	3,593	3,918	4,334	3,961	5,199	5,388	6,613	6,655
詐欺	485	514	521	542	1,408	1,597	1,512	1,508	1,280	1,566	899	1,357	956
児童買春・児童ポルノ法違反（児童ポルノ） ①	128	140	102	85	136	251	192	254	507	783	883	1,085	1,124
わいせつ物頒布等	103	109	113	121	125	192	203	177	140	218	699	929	781
青少年保護育成条例違反 ②	10	70	120	136	174	196	230	437	326	481	434	520	690
著作権法違反	86	66	87	174	128	138	165	144	188	368	409	472	731
児童買春・児童ポルノ法違反（児童買春） ③	117	268	269	370	320	463	551	507	416	410	444	435	492
出会い系サイト規制法違反	0	0	0	31	18	47	122	367	349	412	464	363	339
商標法違反	31	37	95	82	109	218	191	192	126	119	212	184	197
その他	249	267	342	343	393	491	752	748	629	842	944	1,268	1,345
児童買春等違反、青少年保護育成条例違反の合計（①＋②＋③）（件）	255	478	491	591	630	910	973	1,198	1,249	1,674	1,761	2,040	2,306
上記合計の全体における割合（①＋②＋③）×100÷④（%）	19.0	29.8	26.6	28.4	19.9	20.6	17.8	19.0	18.6	24.1	30.7	27.8	28.4

表3 サイバー犯罪検挙件数（表2をグラフで表したもの）



全体のなかの、児童買春等の割合を明らかにするため表2の値をグラフで表したものです。

いずれの件数も全体として増加していますが、平成一三年と平成二五年を比較すると検挙件数は一、三三九件から八、一一三件と約六倍であるのに対し、児童買春等の件数は二五五件から二、三〇六件と約九倍も増加しており、検挙件数のなかの児童買春等の割合も、約二〇％パーセントから約三〇％に増加しています。

このように、統計上におきましても、児童はインターネットの危険に高い水準でさらされていることが明らかであり、その危険性が年々高まってきているといえます。

三　児童のネットワークに対するかかわり方

㈠　児童の携帯電話使用

児童がどのようにインターネットにかかわっているのか、年齢一三～一九歳の平成二五年末におけるインターネットの使用率について、自宅パソコン七三・八パーセント、携帯電話一二・八パーセント、スマートフォン六四・一パーセント、タブレット端末一五・一パーセント、自宅以外のパソコン一八・八パーセントという調査結果があります。（平成二五年通信利用動向調査の結果）

しかし、平成二五年にインターネットに関する犯罪被害を受けた児童のうち、被害を受けた一五九人のアクセス手段は、スマートフォンを含む携帯電話が一三七人（約八六・二％）、同じくコミュニティサイ

トで被害を受けた一、二九三人のアクセス手段は、携帯電話（スマートフォンを含む）に関わるものが一、一七一人（約九〇・六％）、携帯電話が関わっていないもの（パソコン、インターネットカフェ等その他）が一二二人（約九・四％）となっており、パソコンその他が二二人（約一三・八％）であり、（警察庁サイバー犯罪対策統計）、児童が普段利用しているインターネットのアクセス手段はパソコン、携帯電話等と分散しているにもかかわらず、犯罪の被害を受けた児童のアクセス手段は、約九割がスマートフォンを含む携帯電話であるという現象が起きています。

このようなことをふまえると、児童の被害が増加してきたことについて、単にインターネットが身近になったという理由だけで片づけることはできません。児童被害におけるパソコンを使用した場合が一割であるのに対し、スマートフォンや携帯電話を使用した場合が九割であることを考えると、児童のスマートフォンや携帯電話の使用方法等に大きな問題があるのではないかと考えられます。

㈡　年代ごとの携帯電話所有状況

表4は児童の携帯電話・スマートフォンの所有率を調査した結果です。（平成二五年度青少年のインターネット利用環境実態調査）小学生の所有率は二～三割ですが、中学生になると約半数は所有しており、高校生になると約九七％にも達し、ほとんどの児童が所有している結果になっています。

このように児童の年代ごとの所有率を考えると、

①　中学生の年代は携帯電話を持っている児童数と持っていない児童数はほぼ同数である

②　高校生になると、殆どの児童が携帯電話を所有する
③　高校生で初めて携帯電話を持つ児童が全体の約半数である

ということが言えます。

㈢　児童の携帯電話に対する考え方

携帯電話について、児童はどのように考えているのでしょうか。身近なところですが、私には、今年中学一年生になる長女がおり、個人の携帯電話を持ちたがっていたので、所有させるかを判断するため、携帯電話に対してどのような考えを持っているのか聞いてみました。

携帯電話のメリットとしては「家族や友人と直ぐに連絡をとることができる」「情報が早く伝わるので、早い行動ができる」などをあげており、デメリットとしては「犯罪に巻き込まれやすい」「書き込んだことは簡単に消せないので、言葉をよく選ばなければならない」「ルールやマナーを守らないと周りの人に失礼になる」などと答えていました。

私としては、それらの意見により「最低限度の知識は持っている様子だ」と思い購入を認めたところですが、危険性や注意点などを知った経緯について質問したところ、「友達に聞いた」という回答であり、携帯電話が欲しい理由も「クラスメー

表4　青少年の携帯電話・スマートフォンの所有率

	小学生	中学生	高校生
平成25年度	36.6	51.9	97.2
平成24年度	27.5	51.6	98.1
平成23年度	20.3	47.8	95.6
平成22年度	20.9	49.3	97.1

単位：%

トの多くが持っているから」というものでした。

携帯電話の利点、便利な使用方法、ゲームなど児童にとって興味がある情報だけではなく、危険性などについても友人間で情報交換されている様子でしたが、長女が携帯電話を欲しがる理由は友人との通信手段、友人との関係を深めることにあることが分かりました。

児童が、携帯電話に対してどのように考えているのかを調査した結果（子どもの携帯電話等の利用に関する調査、平成二一年二月株式会社富士通総研）によれば、小学校六年生の児童が携帯電話を持った理由について、「保護者から持つように勧められた四六・七％」「塾や習い事を始めたから四一・四％」などが高い割合でしたが、中学生、高校生になると、その回答の多くは「友達が持っているから」が中学校二年生で三八・四％、高校二年生で四四・六％となり友人との関わり合いに変化していました。

そのように考えると、長女の回答も同年代の児童と同様の一般的なものであり、この年代の児童における携帯電話に対しての考えは、「友人とのつながり」を重点にしていると考えられるものでした。

四　現在の指導とその効果

児童がネット犯罪の被害を受けたり、トラブルに巻き込まれたりしないように教育、事業者、警察は協力して児童を犯罪の被害から守るための対策を講じています。

表5は、コミュニティサイトに起因する児童被害の事犯にかかる調査結果（警察庁サイバー犯罪対策統

計）のうち、平成二二～二五年の学校による指導状況についてであり、表六は保護者による指導状況についてです。

被害を受けた七割の児童が学校から何らかの形でコミュニティサイトの危険性を教えてもらっていたにもかかわらず被害を受けており、不登校のため教えてもらっていないと回答した二割の児童を除くと、学校に通っていたが教えてもらっていないと回答している児童は一割程度しかいないということになります。

また、被害を受けた児童のうち、四割は保護者から何らかの形で保護者から注意されていたにもかかわらず被害を受けており、六割の児童は保護者から指導を受けていないと回答しています。

この調査結果から分かることは、被害を受けた児童のうち

① 七割は学校から何らかの形で指導を受けていた

② 六割は保護者から指導を受けていない

ということとなり、学校における指導内容の充実と、保護者に対する指導の普及について更に改善をして行く必要性があると認められます。

五　学校の指導に関する提言

現在は、学習指導要領にインターネットの使用法やモラルの育成が組み込まれていますし、警察官が学

校に指導に赴いたりする取組なども行われています。

しかし、それらを「学校で教えてもらった」と答える児童の中にも被害者になってしまった者がおり、インターネットの危険性がしっかりと浸透しているとは言えません。どのようにすれば児童にインターネットの危険性を理解させ、安全な使用を行わせることができるようになるのかを、児童に対する学校からの指導に目を向けて提言します。

(1) 携帯電話の指導

現在多くの小中学校にはパソコン機器が導入され、実際に児童がパソコンを使用してインターネットに触れ合うような授業が行われています。しかし、携帯電話におけるインターネットの使用方法についての指導はありません。

児童にとってパソコンは、技術・専門的な使用、調査が主な目的であるのに対し、携帯電話はゲーム、ＳＮＳなどのコミュニケーションツールとしての使用が主な目的であると考えられます。学校の取扱いもパソコンと携帯電話では異なっていると考えられ、パソコンは「必要なもの」「学ぶべきもの」という位置にありますが、携帯電話は、「学校における教育活動に直接必要のないもの」と位置づけており、文部科学省の通知においても小中学校ではその持ち込みを原則禁止、高等学校においては制限すべきとしています。

しかし、携帯電話を使用した際に被害を受ける児童数がパソコンを使用した際と比較して圧倒的に多い

ことを考えれば、パソコンだけではなく、携帯電話を使用したインターネットの使用方法、危険性や、禁止行為を教える必要性があると考えます。

パソコンだけではなく、携帯電話も設置して実際に手に取らせ、その使用方法や危険性などを授業、実技を通して身に着けさせる必要性があるのではないでしょうか。

(2)　携帯電話の所有率をふまえた指導

児童が、個人的にパソコンを所有するというケースは少ないと考えられますが、スマートフォンを含む携帯電話は小学生で約二～三割、中学生が約半数、高校生になるとほとんどの児童が所有しています。小中学生に対し、「携帯電話の使用方法、危険性など」を学習指導として一律かつ具体的に教えると「まだ早い」「学校が携帯電話の所持を推奨しているようだ」「所持していないのに教えてもらってはこまる」などという問題点を挙げられる方もいらっしゃるかもしれません。しかし、中学生では半数であった所有率も、高校生になればほぼ全員になるのです。

現在の学校教育は、携帯電話を遠ざけるべき物として捉えているように感じますが、小中学生であれば近い将来は必ず使用することになる機器であり、高校生であればほとんどの児童が既に使用している機器なのです。

保護者や教師の指導を素直に受け入れやすく、かつ、義務教育期間中である小中学校においてこそ、携帯電話の使用に対する学習を取り入れるべきだと考えます。

(3) 情報入手先としての学校

児童が携帯電話等の情報を入手する相手方は、多くが友人であると考えられます。また、携帯電話のサイトには、出会い系やコミュニティサイトなど利用者の交友関係を広げる目的のものもあり、情報入手する相手方がそれらサイトで知り合った者であった場合は、そもそも友人であるかについても問われるところです。

携帯電話等のサイトが安全であるか否かを判断する場合、トラブルに遭遇した場合、サイトの使い方などで質問をしたい場合に児童が選ぶ選択肢は、自分で調べる、保護者等に聞く、友人に聞くなどが挙げられますが、学校、教師という選択肢はありません。

危険なサイトがある、犯罪の被害に遭うということを教師側から一方的に教えるだけではなく、児童にとって携帯電話等に関する質問相手となる、教師、学校という選択肢が必要です。児童が質問しやすい開かれた環境を学校や教師はつくるべきだと考えます。

(4) 性別によって異なる指導

インターネットの使用は男性と女性で違いがあります。例えば、出会い系サイト及びコミュニティサイトに起因する被害についてですが、平成二五年の統計によれば出会い系サイトでは児童一五九人の児童が被害を受けていますが、男性はゼロ、女性が一五九人であり、コミュニティサイトでは児童一、二九三人

のうち、男性は三二人、女性が一、二六一人です。（警察庁サイバー犯罪対策統計）このように被害を受けている児童のほとんどは女性であり、この種の問題は女性児童特有と考えられます。逆に、アダルトサイトの登録に関するトラブル、料金問題等については、男性児童が多いと推定できます。

このように、男性と女性ではインターネットの使用方法もさらされている危険性も異なっており、男女一律に同じ指導をしてもその効果は期待できません。性別に合わせた具体的な指導を行う必要性があると考えられます。

(5)　学校教育のなかの携帯電話

教育現場の声を聴こうと思い、私立女子高等学校で教師をしている友人に対し、生徒の携帯電話の使用状況などについて聴いたところ、予想に反する答えが帰ってきました。その高校では携帯電話の使用を校則で全面的に禁止しており、学生が契約することさえ許していないとのことでした。このように、進学、成績、児童の健全な生活に携帯電話は必要が無い物と位置付けているのが現在の学校教育だと考えます。

私も児童の携帯電話使用を積極的に応援していくつもりはありません。使用頻度が上がると犯罪に巻き込まれるなど様々な問題がついてくるからです。しかし、現在の制限を主とした指導では、真に児童をネットの危険から守っているとは言えません。

児童は学校生活の中で社会性を学び、マナーやルールを学んでいくのであり、学校教育で禁止し、遠ざけてしまったものは、学校生活や学校教育のなかで学ぶことはできません。児童は、自ら中途半端な調査

を行い、友人から聞いたことを鵜呑みにし、「みんな使っているから大丈夫」「使用者が多いから安全」という安易な判断を行うようになります。

そのまま安易な使用を続け、危険性や結果の重大性を判断することなくネット利用を続けていた者が、悪ふざけで写真をネット投稿して社会問題に発展させたり、不用意な書き込みで個人情報を流出させたりするのだと思います。

携帯電話のネット利用を正しく教えないまま児童に使用させるということは、運転技術を持たない者に自動車を運転させるのと同じであり、自己や他人を傷つけることになります。児童から携帯電話を完全排除することはできないのですから、携帯電話の使用を制限し禁止するだけではなく、制限の中にもその使用を認め、学校教育として教師が正しい携帯電話、スマートフォンの使用方法、危険性を教えるべきです。

六　保護者に対する提言

児童が犯罪に巻き込まれないため、被害を受けないようにするための最終的な注意や指導責任は保護者にあると考えますし、児童も困った時の相談相手として一番に親を挙げています。

しかし、先の調査で被害を受けた児童の六割が保護者から注意を受けていないということですから、保護者の児童に対するインターネットの指導は行き届いていないと言わざるをえません。

(1)　有害情報からの遮断

保護者は、児童のインターネット使用、特に携帯電話・スマートフォンの使用状況を確認し監視しなければなりません。

そもそも、インターネットにより犯罪被害を受けた児童の九割が、携帯電話・スマートフォンの使用からである原因は、児童が単独で使用する機会が多く保護者の監視が届いていないからです。

児童が使用する携帯電話等を監視し、違法・有害情報を遮断しなければなりませんが、そのようなサービスにフィルタリングがあります。平成二五年度青少年のインターネット利用環境実態調査によれば、児童の約半数（総数五五・二％、小学生六二・二％、中学生六一・一％、高校生四九・三％）がフィルタリングを利用しているにもかかわらず、同年のコミュニティサイトに起因する児童被害の調査結果では、被害を受けた児童のうちフィルタリングに加入していたのはわずか五・五％のみでした。これら調査からもフィルタリングサービスに加入していない児童の携帯電話等使用における危険性は明らかであり、フィルタリングサービスの有用性は十分といえます。

保護者は、フィルタリングサービスに頼るだけではなく、児童が使用する携帯電話の使用履歴を定期的に確認するとともに、児童に対しても「保護者から使用を監視されている」ということを知らせることが大切です。

フィルタリングサービスと保護者の監視により児童から違法・有害情報を徹底的に排除し遮断しなけれ

ばなりません。

(2) 保護者の知識向上

保護者が児童に注意しない理由に、保護者のインターネットに対する知識不足があげられます。ゲーム、ＳＮＳ、コミュニティサイト等は大人よりも児童の方が使い慣れており知識が豊富です。だから、児童がそれらサイトを利用していても、内容についての指導や注意ができず、「ただのゲームである」とごまかされてもそれを看破することが出来ないのです。

保護者は、「ＳＮＳやコミュニティサイトを自分は使わないから知らなくても良い」とか「子供にはそれらを使わないように注意してあるから大丈夫」と考えるのではなく、児童をインターネットの危険から守るため、児童が使用しているサイトや、社会的に問題になっているサイトなどの知識を取り入れるために努力し、保護者自身が有していなければなりません。

児童が使用しているサイトが安全であるか否かを児童に聞いているようでは、監視機能は全く役に立っていないといえますし、児童が保護者に対してインターネットの質問をしてくることも、判断を仰いでくることも無いと考えます。

(3) 保護者と学校等の連携

児童のインターネット使用における注意点を、学校は保護者会、学級通信等により保護者に配信してい

ますし、警察は職員が学校に赴いて指導し、注意を喚起させています。

しかし、保護者に対する指導は、最近発生した問題事例を紹介し、「危険です」「注意してください」などと言って一方的に児童の使用を制限させる方向に働きかけているだけに感じます。

保護者に対し、児童の間で流行しているサイトの説明や、そのサイトのどのような部分が危険であるのかについては今までも配信されていますが、それらをどのように使用すれば安全なのか、問題にあげられているサイトを継続して使用するための方法、危険を回避する方法など、その先の使用を継続させるための情報配信はありません。

学校や保護者が「危険だから使用を控えるように」と働きかけたところで、児童が素直に従うかといえば疑問です。現に、アカウントが乗っ取られるなどの不正アクセスが問題になっている無料通信通話サービスにつき、児童に対して注意喚起されているはずですが、どれくらいの児童がその指示に従って利用を中止したり控えたりしているのかを考えれば分かることです。

一方的な使用制限を行うと、児童はそれを隠れて使用する様になり、学校や保護者の監視が届かなくなる危険性があります。

安全なインターネットの利用を続けるため、児童に対して使用を継続させるべきか、それともやめさせるべきかを保護者が判断できるように、保護者に対して指導を行う環境整備が必要です。既に行われている取組みがあるかもしれませんが、学校ホームページなどで質問コーナーを作る、学校や保護者間で情報交換し、質問や回答をする機会や場所を作る、保護者に対し児童の携帯電話を確認させ、その点検結果を

提出させて指導するなど、学校と保護者が今よりも積極的に情報交換を行い連携して指導するべきです。

(4) 保護者の役割

フィルタリングを強化し、使用履歴の監視を強化し、学校等と保護者が連携すれば、より安全なインターネットの利用ができると考えられます。

しかし、保護者にとって最も重要なことは、児童のインターネット使用にとらわれるだけではなく、その日常に目を向け、児童の外見や内心の変化を見落とすことがないように注意し見守ることだと思います。

インターネットのトラブル等に巻き込まれている児童をいち早く察知し、救出するためには、服装が派手になった、高価な物品を持つようになった、食欲がない、元気がない、部屋に引きこもるようになった、家に帰らなくなったなど、児童からのサインを見逃さないようにしなければなりません。

それらを最初に発見できるのが保護者であり、一番重要な役割です。

七　おわりに

児童が関連するインターネットのトラブルは、無理に交友関係を広げようとし、金品や異性を求めた結果に生じたものといえます。

児童が受験勉強や部活動などに打ち込んでいるときは、児童にとって携帯電話もインターネットもそれ

ほど必要なものではありませんし、トラブルに遭遇することはないと考えますが、大学生になり社会人になると、仕事や、生活の向上、交際相手を見つけるためとインターネットに接する機会が増え、それに伴いトラブルに遭遇する危険性が高くなります。

将来的に児童がトラブルに巻き込まれ犯罪被害を受けることがないように、小学生のころから年代に合わせた指導が必要です。その指導を児童に浸透させるためには、保護者から児童、又は教師から児童という一方的なものではなく、親と子、教師と生徒、保護者と教師の連携が円滑に行われる社会と教育現場を整備しなければなりません。

インターネットや携帯電話の普及率が急増し、それらに関連する事件が増加している現在であるからこそ、しっかりとした指導方法や教育環境を確立させ、誰もがインターネットを安全に使用することができるような社会を育てていかなければならないと考えます。

【引用資料】

●警察庁ホームページ　サイバー犯罪対策　統計
○　サイバー犯罪の検挙状況等について（平成一三～二五年）
○　「インターネット・ホットラインセンター」の運用状況について
（平成一九～二五年）
○　出会い系サイト及びコミュニティサイトに起因する事犯の現状と対策について（平成一三～二五年）

○　コミュニティサイトに起因する児童被害の事犯に係る調査結果について（平成二二～二五年）

●平成二五年通信利用動向調査の結果（平成二六年六月二七日、総務省報道資料）別添二、図表一・九端末別年齢階層別インターネット利用率（個人）

●平成二五年度青少年のインターネット利用環境実態調査　平成二六年二月内閣府（青少年の携帯電話・スマートフォンの所有率及び所有機種）

●子どもの携帯電話等の利用に関する調査　平成二一年二月株式会社富士通総研（平成二〇年度文部科学省委託事業「先端的な情報通信技術を活用した教育・学習に関する調査」

個人と国家のサイバーモラル

警察官
大阪府警察本部
（生活安全部
サイバー犯罪対策課）
高本　崇（36）

一　はじめに

ネット社会という言葉は、あたかもインターネット上の情報通信網の中に、もう一つの社会があるかのような意味で私たちは使っている。ネット社会は、「サイバー犯罪」というものを生み出したが、それが社会問題の重要な一角をなすかのように言われ始めたのは、つい最近のことであるように思う。このよう

なネット社会の急速な拡大は、同時にサイバー犯罪の被害者や加害者を容易に生み出すこととなり、今やサイバー犯罪は、すぐそこにある危機と言えるほどのものとなった。

今般、私たちは、当たり前のようにインターネットの利便性を享受し、そこから得られた情報を活用しているが、サイバー犯罪の脅威に対して、どれだけの備えをしているだろうか。自分だけは大丈夫、こういう対策をしているから大丈夫、などと高を括ってはいないだろうか。日本の多くの人たちは、空き巣や自転車盗、痴漢犯罪などの現実社会における犯罪に対して、一定の自主防犯の意識を備えているが、一方で、インターネットの裏に潜むサイバー犯罪に対しては、その意識が低いのではないかと思うことがある。

この論文では、インターネットを安全に利用するにあたり、どのようなことが問題になっているか、またそれに対してどのように対応すべきかについて、私が日々の職務を遂行する中で感じたことなどを基に、その考えを述べていきたい。

二　サイバー犯罪の現状

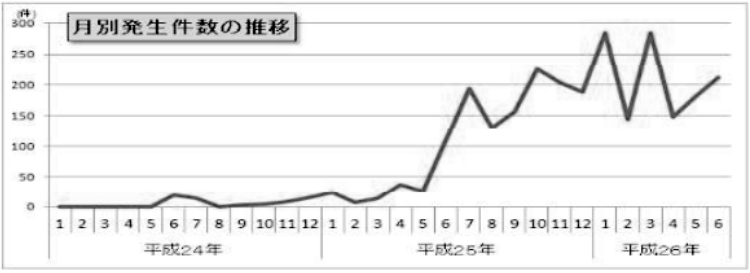
インターネットは、私たちの社会に急速に浸透し、今や「ネット社会」という新たな社会が私たちの生活の中に強く関わるようになり、現代人の大半が、この「ネット社会」による情報の恵みを享受している。こういった「ネット社会」も一つの社会性を帯びているという証拠に、「サイバー犯罪」と呼ばれる「新たな形態の犯罪」が誕生した。

警察庁では、「サイバー犯罪」についての統計を公表しているが、この統計によれば、サイバー犯罪の検挙件数及び相談件数は、近年上昇傾向にある。また現在「サイバー犯罪捜査」に携わる者としては、犯罪の量的な変化はもちろんのこと、質的にも年々劇的な変化を遂げていることを実感している。

例えば、「インターネットバンキングに係る不正送金事犯」について述べると、平成二五年六月頃から同事犯が激増し、さらに平成二六年上半期の時点で過去最悪であった平成二五年中の被害額を超えるなど、まさに危機的状況にある。また同じく平成二六年には、「無料通話アプリケーションに係るなりすまし詐欺」という全く新しい手口の犯罪が現れ、この発生件数も一時的に激増した。サイバー犯罪と対峙する全国の捜査員は、これら新たな犯罪の動向に対して柔軟かつ迅速な対

平成26年上半期のインターネットバンキングに係る不正送金事犯の発生状況

期間	件数	被害額
H26上	1,254	約18億5,200万円 （約148万円／件）
H25下	1,098	約11億9,300万円 （約109万円／件）
H25上	217	約2億1,300万 （98万円／件）



警察庁広報資料「平成26年上半期のインターネットバンキングに係る不正送金事犯の発生状況等について」より

応が求められているのである。

このような状況から、これら日々変化し拡大するサイバー空間を利用した犯罪に対する治安維持の実現は、もはや警察の力だけでは、次第に困難になりつつある。

三　サイバー犯罪の現場で感じること

三ー一　「まさか自分が」の被害者

私が身を置く大阪府警察においてサイバー犯罪対策部門は、それまで本部生活安全総務課の附置機関としての位置付けであったが、昨今のサイバー犯罪情勢に対応する必要性から、平成二五年にサイバー犯罪対策課に昇格した。

私は、現在同課で、各警察署への捜査支援、インターネットバンキングに係る不正送金事犯や詐欺サイト事案などの初動捜査、府民からのサイバー犯罪相談、学校や企業等に対する広報・啓発などの業務に従事している。

それらの業務に従事する中で、私が危機感を抱くのは、サイバー犯罪の被害者となった人たちの多くが「まさか自分が被害者になるとは思わなかった。」という感想を述べているということである。

三―二　サイバー犯罪とその要因

サイバー犯罪にはさまざまな被害があるが、その中でも特に多い被害の一つに詐欺被害が挙げられる。これは、たびたびマスコミでも取り上げられている「インターネットバンキングに係る不正送金事犯」「無料通話アプリケーションに係るなりすまし詐欺」などが該当する。これらの詐欺被害を受ける個人は、インターネットセキュリティ上の対策が不十分であることが多い。

例えば、「インターネットバンキングに係る不正送金事犯」は、正規利用者の情報を盗み取り、銀行サイトにアクセスして、利用者口座から不正に送金するという犯罪であるが、インターネットバンキングで送金する際に必要な利用者のパスワードや乱数等を盗み取る手口の主流は、コンピュータウイルスによるものである。

コンピュータウイルスは、インターネットサイトを閲覧しただけで感染するとも言われており、米国の調査によると、これらＩＤやパスワードを読み取るというコンピュータウイルスのうち、「Game Over Zeus」というウイルスは、世界中で五〇万台から一〇〇万台の端末が感染しており、そのうちの約二〇％が日本に所在すると推定されている。

私もインターネットバンキングに係る不正送金事犯が発生すれば、捜査員として、正規利用者に対し事情聴取等を行うことがある。実際に話を聞いてみると、正規利用者がパソコンにセキュリティ対策ソフトをインストールしていない、あるいは、インストールしていてもオペレーティングシステムなどが最新の

状態に更新されておらず、ウイルスの感染経路となる「セキュリティホール」を残したままの状態にしているケースが多い。

また「無料通話アプリケーションに係るなりすまし詐欺」は、犯人が無料通話アプリケーションに不正ログインした後、正規利用者を装い、その友人・知人等に「コンビニで電子マネーを買って、使用コードを送ってほしい。」などと依頼し、電子マネー価値を騙し取るという犯罪である。そして、その不正ログインの手口は、「リスト型攻撃（パスワードリスト攻撃／アカウントリスト攻撃）」であると言われている。

「リスト型攻撃」とは、何らかの手段により他者のＩＤ・パスワードを入手した第三者が、これらのＩＤ・パスワードをリストのように用いて様々なインターネットサービスに不正ログインを試みるという手口のことである。正規利用者が同一のＩＤやパスワードを使い回していると、いずれかのサービスからそれらが漏洩した場合、容易に他のサービスに対しても不正ログインされてしまう。「サービス毎にパスワードを変更するのが面倒だ、覚えきれない。」などと、同一のパスワードを複数サイト・サービスで利用していることで、このような被害に遭ってしまうことがある。

三－三　加害者のケース

一方、加害者となるケースで多いのは、ファイル共有ソフトによる著作権侵害、インターネット掲示板やＳＮＳ（ソーシャルネットワーキングサービス）等での書き込みによる名誉毀損等の犯罪があるが、一部の加害者には「軽い気持ちでやってしまった。」「まさか捕まるなんて思わなかった。」などと供述し

ている者もいた。

例えば、インターネット掲示板やＳＮＳの書き込みに関して言えば、「バイトテロ」という言葉が近年メディアで報道された。これは、アルバイト従業員などが就業中に悪ふざけで行った様子をネット上にアップロードしてしまう行為を言うが、結果として、その行為者は、当該企業や店舗などに対するイメージダウンを引き起こし、そして、閉店等に伴う多額の損害賠償訴訟にまで発展することもある。さらに、場合によっては業務妨害罪等として刑事訴追されてしまうこともある。

また、就業中でなくても極めて公共性に欠ける行為をネット上でアップロードした、あるいは、されたことにより、ネット上で不特定多数からの激烈な非難を受け、素性まで晒され、刑法犯として検挙されるというケースも発生している。

情報化社会が発達した今般においては、軽い気持ちで悪ふざけのつもりでやったことが、人生において大きなペナルティを負う原因にもなり得るのである。

四　サイバーモラル

四－一　「ＩＴの弱者」と「サイバー防衛力」

冒頭でも述べたが、サイバー犯罪捜査の現場で仕事をしていると、私たち現場捜査員が脅威と感じていることが、一部の国民には、深刻な問題として捉えられていないのではないかと感じることが多い。

本論文では、私はインターネットに関する知識が不十分な人たちのことを「ＩＴの弱者」と定義するが、ＩＴの弱者はそういった知識が不十分であるがゆえに、サイバー犯罪の脅威に対しても現実味がなく、セキュリティが薄くなっているのではないかという印象を受ける。

前述のサイバー犯罪の被害者に関して言えば、セキュリティ対策ソフトをインストールしていなかった、セキュリティホールをそのままにしていた、複数のサイトで同じパスワードを使い回していた、といったように、加害者に対して付け入る隙を与えてしまっているようなケースが見受けられる。

サイバー空間の脅威は、無防備なＩＴの弱者に対して容赦がなく、それどころかその他のＩＴの弱者を巻き込んで常習的にさまざまな攻撃が行われている。またＩＴの弱者が保有する脆弱性のある端末は、サイバーテロやサイバーインテリジェンス（諜報活動）の踏み台として利用される危険性があると言われており、また場合によっては、それが我が国の安全保障にも重大な危険を及ぼすことにも繋がりかねないのである。

他にも、企業等のウェブサイトにおいてコンピュータウイルス等が埋め込まれ、サイトを閲覧した者の端末が感染してしまうケースが確認されており、企業等のセキュリティ対策が顧客等に悪影響を及ぼしてしまうこともある。

私が問題としたいのは、セキュリティ対策が不十分なＩＴの弱者にどのように手を差し伸べて、個人ひいては国家全体の「サイバー防衛力（サイバー犯罪から自身を守る力）」を高めていくか、ということである。

この手の問題を論じる際に、しばしば「情報リテラシー」という言葉が用いられるが、私は、ここでは、「リテラシーを備え、自らのセキュリティに活かす能力」を「サイバー防衛力」と定義し、その言葉を用いて持論を展開していきたい。

この「サイバー防衛力」の必要性は、インターネットの不適切な使用により加害者になってしまう者にも言えることで、自らのリテラシーの不足により「サイバー犯罪に何らかの形で関与してしまう」という点においてＩＴの弱者と同様であると考える。

私は、国民の「サイバー防衛力」の底上げにより、ＩＴの弱者を減少させることこそ、サイバー犯罪そのものを減少させる有効な手段であり、安心で安全なサイバー空間を確保するために必要不可欠な要素であると考えている。

他国に比べると日本は、まだまだ「治安大国」であると言われている。しかし、ボーダレスなインターネットの社会において、我が国は果たして「ネット治安大国」と言えるだろうか。国内における「体感治安の良さ」がサイバー犯罪に対しては、かえってマイナスの影響を与えてしまっているのではないだろうか。

個人レベルにおいて、ＩＴの弱者がサイバー犯罪に対する防犯意識を高め、高い知識を習得し、それを自らのインターネットライフに「サイバー防衛力」として反映していくことは、今や緊急の社会的問題と言えるのである。

四ー二　「サイバーモラル」という考え方

近年、違法行為や他人に対する迷惑行為をしないということに加え、社会人として自発的に社会のために尽くそうと行動する公共心、あるいはモラルが重要視されている。私は、特にサイバー防衛力を備えるという公共心について、「サイバーモラル」という言葉を提唱したい。

私は、ここでいう「サイバーモラル」とは、「サイバー防衛力を備え、ネット社会において他者に迷惑をかけない、サイバー空間を安全で利用しやすいものにするという公共心」のことであると定義する。今や、個人のセキュリティ対策の不備は、個人の問題に留まらない。サイバー防衛力が十分でない人は、前述の無料通話アプリケーションに係るなりすまし詐欺でも言えるように、結果として周囲の者に迷惑をかけてしまいかねないのである。故にサイバー防衛力を高めるという自発的活動が、公共心やモラルとして求められてくるのではないだろうか。

国内において、サイバーモラルは、個人レベルにまで反映・醸成されることが必要であると考える。さらに個人スキルやモラルに影響力を及ぼすのが、その個人が属する集合体であるならば、職場、学校、家族などの集合体において、サイバーモラルの機運が高れば、その反映・醸成の効果もより大きいものになると考える。

警察も犯罪抑止の観点から、今以上に、関係団体と協力しつつ広報啓発活動を取り組んでいくことが求められている。

また、国家レベルにおいても、ＩＴの弱者の端末等が踏み台となって、他国のサイバー犯罪やサイバーテロに利用されてしまえば、国家的信用問題にも関わってくるおそれがあることから、サイバーモラルの醸成は、国家戦略としても枢要をなす課題であると言っても過言ではない。もはや、サイバー犯罪は、警察だけの問題に留まらず、他の行政機関や国内の各種企業・団体と連携して、国を挙げての対策が必要とされているところである。

現に平成二五年、政府によって打ち出された「サイバーセキュリティ戦略」において、サイバー空間の脅威に対する国家レベルでの指針が多角的に示されており、その中でも「リテラシーの向上」について述べられている。

今後、社会全体で周囲に悪影響を与えないようにサイバー防衛力を高めようというサイバーモラルの社会的機運が高まれば、ＩＴの弱者が徐々に減少し、サイバー犯罪の被害者の減少にも少なからず効果が出てくるのではないかと考える。

しかしながら、社会や人に自発的にリテラシーやモラルを醸成させることは、そう容易い問題ではない。私は、ここで、鍵となるのが「社会的評価」であると考えている。

四－三　情報化社会の拡大と、日本人の社会的評価

今後、情報化社会がさらに進展すれば、人の行動は瞬時にＳＮＳなどにより広範囲に拡散され、その人を取り巻く社会によって、良きにつけ悪しきにつけ、その評価がなされることが予想される。その結果、

サイバーモラルが十分でない人は、人に迷惑をかけかねない人として、その個人の社会的評価に悪影響を与える可能性がある。これは、前述のバイトテロや無料通話アプリケーションに係るなりすまし詐欺等がその顕著な例と言える。要するに、自己のサイバー防衛力の不十分さが、周囲の人の知るところとなり、ネット社会のみならず現実社会でも、不利益を被ってしまうこととなる、ということだ。そういった社会が「良い社会なのかどうか」は別にして、今後、情報化社会が進展するにつれ、「自らのサイバー防衛力やサイバーモラル等に関する行動が多数に評価されていく社会となる可能性がある」ということを一つの見解として提示しておきたい。

その一方で、日本人には「他人に迷惑をかけない。」「世間に恥ずかしい真似は出来ない。」といった他者との調和や恥を重んじる国民性がある。

そうであるならば、発想を逆転し、日本人のこのような国民性に訴えかけることで、社会や個人のサイバーモラルについても個々人に考えてもらうことが出来はしないだろうか。

本論文のキーセンテンス

到来しつつある「インターネットセキュリティが個人の社会的評価に影響する社会」において、日本人の国民性に広く訴えてサイバーモラルの醸成を図り、結果として、個人のサイバー防衛力を向上させ得る可能性がある。

これにより、個々人のサイバー防衛力もプラスへ転換することが出来れば、他国とはひと味違った、日本独自のインターネットセキュリティ対策・戦略の推進が可能になるかもしれない。

次項では、個人におけるサイバーモラルを高めるためのいくつかの方策について、既に行われていることも含め論じていきたい。

五　サイバーモラルとサイバー防衛力向上のための方策

五ー一　教育機関におけるサイバー授業の実施

国民レベルにおいて、サイバーモラルの向上に必要不可欠なのが、まずは教育である。インターネットが大人だけのものとしてだけでなく、未成年者においても幅広く利用されて久しいが、情報通信に関する教育、中でもが特に情報リテラシーやモラルに関する教育が十分に行われているとは言い難い状況でないだろうか。

今後、社会を担う子供達に対しても、サイバー犯罪の被害者や加害者にならないよう教育機関が情報リテラシーの教育をカリキュラムとして組み込む必要がある。また大学や専門学校においても、社会人として備えるべきサイバー防衛力について、情報セキュリティ関連カリキュラムを実施していくことも必要になってくるであろうし、その上でサイバーモラルについても教育していくべきであろう。

また、情報関連の専門教職員だけではなく、それ以外の教職員についても、今後は、情報リテラシーな

どについて生徒同様に一定の理解を得ておく必要がある。教職員に自己のサイバー防衛力の強化を目標として情報リテラシーの教養を積極的に実施していくことにより、各教職員のサイバーモラルを向上させ、模範的な姿を学生に見せることで、生徒にもサイバーモラルの向上を図ることが出来るのではないだろうか。なお現在、学校の教職員やＰＴＡ等から当課に対して、サイバー犯罪やインターネットの危険性についての講演依頼や相談も寄せられており、既に教育現場等におけるサイバー空間の脅威に関しては、その関心の高さを伺い知ることが出来る。

一方、サイバー空間の安全に関しても、人材不足が深刻な問題となっている。独立行政法人「情報処理推進機構（ＩＰＡ）」が企業アンケートなどから推計した調査結果によれば、情報セキュリティに従事する技術者約二六・五万人のうち、約一六万人が必要なスキルを満たしておらず質的に不足しており、加えて、潜在的に約八万人が量的に不足しているとのことであった。今後、各教育機関は、これらの新規に必要な人材を補うための人材育成についても、一般的な情報通信技術のみならず、情報セキュリティの技術についても積極的に推進していく必要もあるだろう。

五－二　一般企業等におけるサイバーモラル

一般企業において、近年「企業における社会的責任（ＣＳＲ：Corporate Social Responsibility」が重要視されている。大手企業の個人情報漏洩事件などにより、度々企業等の情報管理のあり方がクローズアップされるということがあった。また、インターネットバンキングに係る不正送金事犯において法人口座が

被害に遭う事案や、標的型メール攻撃によって社内ネットワークに不正プログラムが送り込まれ、情報が漏洩するなどといった事案も多数発生しており、企業もまたサイバー犯罪のターゲットとなっている。これらの事件の被害現場での事情聴取等でわかったことだが、企業内の情報セキュリティ対策に問題があるケースも残念ながら一部に見受けられた。企業がその社会的責任を果たし、社会的信用を保持するためには、社内の情報セキュリティ対策強化と、個人情報の厳重な管理という面でのサイバー防衛力が今や、企業運営上必須であると言える。

社員個人や企業組織におけるサイバー防衛力は、その企業のリスク・マネジメントに少なからず影響を及ぼすことから、社員への情報セキュリティ教育や社内規則の構築等が重要となってくると考える。

また一方で、例えば、一部の情報セキュリティ関連事業者は、サイバー犯罪やセキュリティ対策問題について、アーカイブ情報を無償で公開して注意喚起を行うなど、対外的なリテラシー向上に関する社会奉仕の取り組みを行っている。これ以外にも、サイバー犯罪について定期的な社内勉強会を実施している等、情報セキュリティ対策に熱心な企業・団体もある。私も企業などに依頼され講演に赴くことがあるが、多くの人からさまざまな質問を受けることからも、リテラシーを高めるための機運が一部で徐々に高まってきていることを実感している。

今後も、これら一般企業等の自発的な取り組みに対し、警察を含めた行政の積極的なバックアップを引き続き展開していかなければならないと考える。

五－三　行政等に求められること

政府や自治体に求められることは、企業や教育機関等の各団体との連携において、一定のイニシアティブをとって、有用な関係性の構築を図ることである。まさにその基本指針といえるのが、前述の政府による平成二五年の「サイバーセキュリティ戦略」である。行政のみならず、実にさまざまな分野に関して具体的にその方向性が提示されている。

行政においては、サイバー空間の脅威に関して、「情報セキュリティ関連事業者」や情報処理推進機構（ＩＰＡ）、一般社団法人ＪＰＣＥＲＴコーディネーションセンターなどとの連携強化により、情報共有とその対処法の検討を密にしていく必要がある。加えてサービスプロバイダ等の「インターネット事業者」や「金融機関」、「重要インフラ事業者」等の企業等とも不正アクセス等の被害情報や犯罪インフラ情報、またサイバー攻撃への対策等について情報共有を行うことが重要である。

つまり、断片的であっても、各種団体からの情報を取りまとめ、

サイバー防衛力を高めるための情報発信モデル

各種業界全体を巻き込んで、それらの情報を有機的に結合させていくことにより、日々変化するサイバー空間の脅威に対し、柔軟に対応することが重要なのである。

そして、これらの収集した情報や対処法を「教育機関」や「ボランティア団体」、「一般企業及び商工会議所等の経済団体」などの各種団体、そして、最終的には個人レベルにまでフィードバックしていかなければならないと考える。

ただし、教育機関や企業等へ情報提供を行う際、情報提供元からの迅速かつ正確でわかりやすい情報提供が求められるが、そのための枠組みをどのように構築するかが問題である。得た情報をどのようにフィードバックしていくかのシステムについては、極めて難しい課題であるが、行政が「情報セキュリティ関連事業者」や「ＩＰＡ、ＪＰＣＥＲＴコーディネーションセンター」との連携を密にして、情報アーカイブの共有や情報メールの配信など、既存の情報発信の手段に加え、これまでの行政になかった新しい情報発信の形を検討していくことが求められているのかもしれない。

五―四　警察に求められること

現在、警察においては、検挙と抑止の両面でサイバー犯罪対策の推進がなされている。

抑止対策としては、積極的な広報啓発活動を行い、タイムリーでわかりやすい情報発信を継続的に行っていくことが、国民と身近な存在である警察として求められるものであると考える。警察は、国民に密着した活動を行っており、既に様々な活動を行うための体制を確立している。サイバー犯罪対策に関しても、

地域防犯リーダーである自治会長や防犯委員などとの協力・連携がますます重要であると考える。

また、各種警察活動の中で得られた情報についても整理した上で、出来る限り速やかに「情報セキュリティ関連事業者」など関係団体へ情報提供を行っていくことも重要である。

平成二五年三月から大阪府警察が独自に開始した取り組みで、現在全国の警察で実施されている「海外偽サイトなどに係る被害拡大防止対策」の一環として、警察に寄せられる、閉鎖が難しい海外の偽サイト・詐欺サイトの情報をセキュリティ関連事業者に提供し、セキュリティ対策ソフトなどにより偽サイトをブロッキングしてもらうといった協力関係を築いている。

今後発生し得る新たな手口のサイバー犯罪に対しても、警察とセキュリティ関連事業者との間で「Win-Win」の関係を強化しつつ各種対策を行っていくことが重要である。

また、対外的なことだけでなく警察部内においても、現場警察職員自身がベテラン・若手に関係なく、サイバー犯罪の対処能力の向上と自身のサイバー防衛力を高めていかなければならない。

サイバー犯罪は、我が国の治安問題を大きく左右する問題であり、全ての警察職員が積極的な自己啓発によるサイバー防衛力の強化を図らなければならない。そのためには、警察組織における教養もますます重要になってくるであろうし、必要に応じて、専門的知見を有する一般企業や教育機関へ、警察職員の教養を委託することも重要であろう。

以上のように、今現在もその取り組みがなされているところであるが、サイバー犯罪対策は、警察のみならず、産学官の協力・連携を図っていく必要がある。

また、事件が発生すれば、事件捜査を確実に行い、そして、個々の被害者に対しても、再び被害に遭わないよう防犯指導を行っていくことで、地道にサイバーモラルの向上を推進していくことも重要である。

六　結びに

本論文では、個人のレベルにおいて、「サイバー防衛力」を高めるためには、他人に迷惑をかけないという「サイバーモラル」の向上が重要であると述べた。そして、サイバーモラルの向上は、その個人の社会的評価や、国家の信頼にも影響を及ぼすことであると論じた。「サイバー防衛力」という「技術・知識」を高めることで、「サイバーモラル」という「道徳意識」が付加され、人格形成がなされるということである。

それはまさに「道（どう）」の世界と似ている。

古来より我が国においては、その技術を鍛錬し、極めることを人生観などにまで昇華させるものとして「道」という言葉がある。剣術を鍛錬する道は「剣道」、茶でもてなす道は「茶道」、挙げればきりがないが、ネット社会においても、その「知識・技術」と「人としてのあり方」を追求し続ければ、それは立派な「道」たり得るのではないだろうか。

国民全体のサイバー防衛力を向上させようとするモラルが高まれば、我が国のサイバー防衛力も向上し、国内外からのサイバー攻撃やサイバー犯罪に対して、防御が強固な国となる。個々人がサイバーモラルを持ち、一定のサイバー防衛力を備えることで、個々人の社会的評価のみならず、ひいては、我が国の

世界的な信用にも通じるのである。

日本国民がネット社会においても、現実社会においても、モラルのある生き方により、世界中の人から信用され尊敬されるような国となって欲しいと心から願うものである。

【参考資料】

・警察庁「平成二六年上半期のサイバー空間をめぐる脅威の情勢について」
(http://www.npa.go.jp/kanbou/cybersecurity/H二六_kami_jousei.pdf)
・警察庁「平成二六年上半期のインターネットバンキングに係る不正送金事犯の発生状況等について」
(http://www.npa.go.jp/cyber/pdf/H二六〇九〇四_banking.pdf)
・警察庁「平成二三年 警察白書～特集Ⅱ：安全・安心で責任あるサイバー市民社会の実現を目指して～」
(http://www.npa.go.jp/hakusyo/h二三/honbun/pdf/〇六 tokushu二.pdf)
・内閣官房情報セキュリティセンター（情報セキュリティ政策会議）「サイバーセキュリティ戦略」
(http://www.nisc.go.jp/active/kihon/pdf/cyber-security-senryaku-set.pdf)
・独立行政法人情報処理推進機構（ＩＰＡ）「ＩＴ 人材白書二〇一四」
(http://www.ipa.go.jp/files/〇〇〇三八二八七.pdf)
他

【参考文献】

・サイバー犯罪対策概論―法と政策―　四方 光 著　立花書房

家庭教育のプロが教える「我が子とネットの正しい付き合い方」

自営業
館野　史隆（43）

はじめに

家庭教育のプロが「我が子とネットの正しい付き合い方を教える」。それが本論文の趣旨です。論文に先立ちましてまず最初に私自身の経歴と経験に触れておきたいと思います。私はかつて家庭教師の職に従事していました。指導した生徒さんは数にして短期指導の方を含めれば五百人以上。いわば家庭教育の〝プ

ロ〟を自認しております。家庭教師の仕事というのは子どもたちに学校補習や受験指導を行うのが主たるものですが副次的にそれ以外のことを教えることもあります。即ち、学習効果の向上、家庭教育の充実、生活サイクルの確立という観点から子どもと各種娯楽との関わり方についての指導をすることもあります。特に携帯電話とパソコンが普及した後はネットやネットゲーム（以下、ゲーム）と子どもの関係が密接なものとなり、これらとの関わり方が子どもの成績や学力に及ぼす影響も大きくなったことから、こうした娯楽との付き合い方についての指導を子どもたちや借越ながら保護者の方々にも行って参りました。本論はその時の経験をもとに子どもとネットの正しい付き合い方について提言を行っていきます。

ネットやゲームに過度に依存するようになった場合、さまざまな面で子どもの安全に影響をきたします。学力面でいえば学習意欲の減退、思考力の低下、成績不振などです。また視力の低下、姿勢の乱れといった身体面での不調の他に無気力化、（現実世界や将来に関心が持てなくなる）無関心化、引きこもり化などメンタル面でも悪影響を及ぼすことがあります。いかにネットやゲームと正しく付き合うかは現代の子どもの成長、発達にとっては重要な要素といえます。

そこでネットとゲームとの付き合い方に関する教育（以下、ネット教育）を施すことが求められるわけですがその基本的指針を述べておきます。まず「予防」と「治療」です。予防教育、予防活動をしっかりと行って子どもがネット依存、ゲーム依存に罹ることを前もって防ぐ。いわゆる「予防にまさる治療なし」です。もっとも子どもがネットやゲームに依存し始めても必ずしも手遅れというわけではありません。私の経験からいえば治療によってネット依存、ゲーム依存から子どもを立ち直らせることはできます。その

ためには適切なリハビリを施すことが要請されます。その具体的手法は後に実践報告を兼ねて紹介します。

次が「教え」と「導き」です。予防と治療が必要だとしても子どもたちはそれを自力ではなしえません。し方法論も知りません。それどころか、その必要性さえ多くの子どもは感じていないのが実情です。彼らをネットやゲームと正しく付き合わせるためには大人の手による教えと導きが必要なのです。

その教えと導きをなす際、「原理原則」に則って行うことが重要です。ただ闇雲に「ネットは禁止」、「ゲームは没収」などとやったら子どもは反発したり陰でコソコソやるようになり逆効果です。しっかりとした原理原則のもとに効果的な指導と訓練を子どもに課す。その手法は各論の部分で詳しく述べます。

一　「原因」と「特徴」を知る

同じネット依存、ゲーム中毒という症状であってもそれぞれ「原因」と「特徴」は異なります。以下は私の指導経験をもとにネット依存、ゲーム依存の原因と特徴を類型化したものです。

まず『現実逃避型』。これは現実逃避という目的に起因するものです。具体的には試験勉強、受験勉強、部活動、対人関係、進路選択など辛い現実から目を反らすためにネットやゲームに夢中になる症状です。一般的にはストレス耐性が低い子どもや目的（目標達成）意識の低い子どもがなりがちです。

次が『環境感化型』です。これは周囲の環境に影響、触発されてネットやゲームにのめり込む類型です。ここにいう「環境」には友人、先輩、家族、メディアなどがあげられます。自分に自信がない子どもやア

イデンティティの確立されていない子どもによく見られる症状です。

『惰性型』は目的もなくタラタラとネットやゲームに興じるタイプです。ネットサーフィン（興味の赴くままにウェブや動画を視聴する）、ネットジャングル（目的もなく見始めたウェブや動画に入り込んだまま、さ迷う）に代表されるようにただ時間潰しや暇つぶしのためにネットやゲームに興じるというのが特徴です。時間管理、自己管理能力の低い子どもがなりがちな症状といえます。

『疑似体験型』はネットやゲームの世界での疑似体験に喜びを求めるタイプです。具体的には動画の中の人物に自己投影をする、ゲームの中での高揚感、達成感に酔いしれる、チャットで見ず知らずの人と会話して満足感を覚えるなど〝非〟現実的な行為や体験に喜びを見出す（そこにしか見出せない）タイプです。この症状には社交性の欠如、共感性の低さ、現実世界での喜びや楽しみでは満たされない『自己不満足』感などに深い原因があるように思われます。右諸々の原因による不満足感、不充足感をネットやゲームの世界での喜びや楽しみに昇華させてしまう「癖」と「技術」と「快楽」をいつかどこかで身につけてしまったというのも原因の一つにあげられます。

『健全型』は上記各類型とは異なりネットやゲームと健全に付き合うことができているタイプです。勉強や部活動の息抜き、リラックスの一環として程よい時間、熱中度でこれら娯楽を楽しめている類型です。差し当たっては心配ありませんが絶対安心というわけではありません。あるタイミングでふとしたきっかけでネット、ゲーム依存に陥る可能性と危険性はあります。

以上がネット依存、ゲーム依存の原因と特徴です。ネット依存、ゲーム依存の予防策を講じる上では我

が子がどの類型にあてはまりうるか性格、環境、過去の経験などを手掛かりに探ることが必要です。治療策を講じる場合においても上記類型化をふまえて『５Ｗ１Ｈ』（いつ、なぜ、どこで、どの原因で、誰の影響で、どのように）でネット、ゲームに依存するようになったいきさつを知り依存、中毒要因を除去、改善することが求められます。また複数の類型にまたがるネット依存症、ゲーム中毒症もありますので万遍なく予防策を講じたり、さまざまな視点と角度から治療を行うことが必要な場合もあります。

二　ルールを制定する

我が子をネットやゲームと正しく付き合わせるための第一歩とは?その問いにははるか昔、かの聖徳太子が答えてくれました。聖徳太子は『十七条の憲法』を定めましたがこれは国としての決まりを定めるとともに見えざるが増大しつつある隋の勢力から国と人を守るために役人と国民の心構えを記したといわれています。子どもに節度ある生活を送らせるとともにネット依存、ゲーム依存という見えざるが、ひたひたと忍び寄るネット、ゲーム依存から我が子を守るべく資料一に示した、Ｋ君が作ったようなルールを制定しましょう。

詳しくは資料を参考にするとしてポイント説明をします。そもそも論としてルール制定の意義は「けじめをつけさせる」ことにありました。Ｋ君は少々、雑でルーズな面があったため（これが勉強にも少なからず影響していた）「やることはやる」、「守るべきことは守る」という意識を持たせようとしたのです。

男の子のお母さんの中には子どもがだらしない、遊んでばかりでけじめがないと悩まれている方も多いかと思われます。しかし、私が見てきた限り決まりごとを作り、守らせる習慣をつけさせれば子どもは少しずつ変わってきます。子どもとネットの関わりについての調査を指揮したヴィクトリー・ライド氏も「親はあきらめる必要はない、ルールを作れば必ず変わる」と述べていますがルールを作らせるということ自体に意義があると思うのです。

次に子どもが自ら作ったという点が重要です。この憲法は私とご両親の立ち会いのもとK君自ら作りました。大人たちの助言（これもまた重要）にしっかりと耳を傾けつつ各『条文』ごとに自問自答しながらK君自身の手で作った『自主憲法』です。マズローによれば人間は自己実現に向けて一歩ずつ成長するとのことですが中学受験という目標に向けてまず規則正しい生活を送るべく心を決めることがK君にとっての出発点だったのです。

実現という言葉が出ましたが『実現可能な』ルールを制定させた点もポイントです。受験生だからといってむやみにネットやゲームを禁じてしまったらストレスが溜まり、かえって勉強の効率も落ちてしまうものです。ですから、守れないルールや無理な決まりを作るのではなく確実にこなせる内容にしました。制限時間や遊ぶ時間帯を決めてあえて毎日ネットやゲームに触れることを許した（ご両親には許していただいた）のもこの『実現可能性』を最大限、考慮したゆえです。

またルールを簡明化した点にも着目してください。ある調査によれば規則が多過ぎたり複雑過ぎる企業は従業員が規則を守れずかえって遵法意識が薄れて生産性が低くなるとされます。大人だってそうなので

すから子どもは尚更です。分かりやすい、守りうる内容でかつ適度な量。これを重視しました。

因になぜ『憲法』だったかといえばK君が大の歴史好きだったから。好きな分野のものを題材にすれば取っ付きやすいですしややもすれば構えてしまいがちなルール作りも肩肘張らずにできると思ったからです。K君は受験までの期間、自ら制定した憲法を概ね守り第一志望に合格しました。合格通知を手にした時のK君の誇らしげな笑顔は今も忘れません。ついでながら社会の試験では聖徳太子の『十七条の憲法』が出題されたことを付け加えておきます。

三　〝マスト型〟の子どもを育てる『ADトレーニング』

家に帰っては宿題そっちのけでパソコンに向かい動画鑑賞に耽ったり、一目散に部屋に走りオンラインゲームに夢中になっている子どもは多いと思います。現代社会においてはネットやゲームとの関わりを一切断ち切ることは難しいでしょうが早くそうした習性（真っ先に遊ぶ）を変えないと前記した『惰性型』に見られるようにネット、ゲーム依存症になってしまいます。ここでは子どもを〝マスト型〟に変えるための『ADトレーニング』について説明します。

まず〝マスト〟とは英語で「しなければならない」の意味ですがここでは『ま』（まずやる）、『す』（すぐやる）、『と』（とにかくやる）の三つの言葉を集約したものでもあります。具体的には「しなければならないこと」、「やる必要性と優先度の高いこと」をまず、すぐ、とにかくやってからネットやゲームに向かわせる義務先行型ともいう習性のことです。その習性を身につけさせるために用いるのが

『ＡＤ（After Duty）トレーニング』（義務をこなした後にネットやゲームをやる訓練）です。その具体的訓練法について説明する前提としてトレーニング全般に通用する基本原則を資料二に示しておきます。

この原則は筋力トレーニングの場面のみならずさまざまな訓練の場において応用しうるものだと思われます。もちろん、〝マスト型〟の子どもを育てるための『ＡＤトレーニング』においてもです。ここでは右原則を応用した『ＡＤトレーニング』の実践例を紹介します。実践者はＹさん（中二女子）。Ｙさんはそれほどネット依存が進行していたわけではありませんがマイペースな性格ゆえ勉強や家の手伝いを忘れてネット動画に夢中になることがしばしばあったのです。そこで生活リズムの是正とネット依存の予防的措置としてトレーニングを実施しました。資料三はその初期メニューの一部です。

要点を説明します。まずＹさんのメニューを見て「義務」（宿題や手伝い）の時間と量が少ないと思われるかもしれませんがこれでいいのです。初期段階は「義務をこなした後に遊ぶ」という癖をつけるための段階ですから〝ＡＤ〟つまり義務の後にネット、逆にいえばネットの前に義務という習慣をつけることだけに意識を集中させればいいのです（『意識性』の原則）。

もっとも、よく見ると徐々にトレーニングの「量」も「質」も上がっているのが分かります。勉強時間も五分単位で小刻みに増えていますし内容も機械的に（つまり渋々、イヤイヤでも）できるものから読解、応用など複雑で思考力を要するものに、義務も自分の好きなもの（Ｙさんは大の大好き）から身の回りのもの、家全体のものというように「難易度」（Ｙさんにとって面倒であり抵抗が強い度合い）が上がっています。トレーニング原則中、『過負荷』、『ざん進性』の原則をそれぞれ応用したものですがこうしてメ

ニューの内容に変化を加えながら繰り返す（『反復性』）ことで少しずつ義務の比率を増やし、最終的にはネット視聴は最低限でいい、という境地を目指しました。

同じ「義務」をこなすならネットとゲーム利用に関する安全に留意した内容がよりいいでしょう。Yさんのメニューにおいて「犬の世話」、「祖父母宅への荷物届け」、「地域活動」などを取り入れたのはネット依存、ゲーム依存の危険に陥る、あるいは進行することを防止する目的があります。アメリカ精神医学会はネット依存の症状としてネット、ゲーム以外の活動に興味を失う、人間関係をおろそかにする、家族にウソをつくなどの行為をあげていますが子どもがこうした状況に陥る（進行する）ことを防ぐためには積極的に地域活動に参加させて人とのつながりを持たせたり、生き物と日常的に接することで生活の〝バーチャル化〟を防いだり、しつけに厳しいおじいちゃん、おばあちゃんに叱ってもらい言動を正す機会を意図的につくることが必要になると考えたのです。これはトレーニング原則中、『全面性』の原則に関わるものですが多角的な視野から子どもを鍛えるという視点が〝AD〟の習性を身につけさせるのみならず人間性を滋養するという意味においては必要だと思われます。

はじめはブツブツ文句を言っていたYさんもやがてはきちんと義務をこなせる子になりました。そのマイペースでちょっぴりおっちょこちょいな性格ゆえに時に手伝いを忘れて動画に走ることもあったようですが私が与えておいた宿題は徐々にちゃんとこなせるようになりました（指導開始時は「先生～、宿題、何だっけえ?」とあっけらかんと言うこともしばしばあった）。こうした例を参考にしつつに与えられた課題はしっかりこなす、義務をこなしてから楽しみ（ネットやゲーム）をやるという「筋力」をつけるべく

子どもにいや子どもとともに親御さんもトレーニングに励まれることを是非、お勧めいたします。

四　リハビリとしてのトレーニング

右にあげた『ＡＤトレーニング』は予防としてのみならずリハビリつまりネット、ゲーム依存がある程度、進行してしまった場合の治療法としても応用できます。ここでは『ＡＤトレーニング』をリハビリとして行う場合の留意点を私の指導経験をふまえてお伝えします。我が子のネット、ゲーム依存が重症化していると危惧されている保護者の方々、ぜひ参考にしてください。

基本的にＹさんに行ったようなメニューで訓練しますがリハビリとしてトレーニングを課す場合、ファーストステップつまり「慣れ」の期間を長めに設定してください。おそらくネットやゲーム漬けの怠惰な生活が身に染みていでマスト型の生活を送るのに必要な筋肉が衰えていますから「義務」の時間を短め、内容も簡単なものにしてなまった心と体をほぐすことから始めてください。結果や出来ばえは問わないでください。重い腰を上げて気の進まないことをやろうという気になったのに「もう少し身を入れて」とか「どうせやるならきっちり」などというのは子どもの心に水を差すようなもの。まずは「ネットやゲームをやる前にしっかりと義務をこなした」という行為自体に最大限の意義と価値を認めてあげることが親には求められます。この段階では結果『無』価値、（結果は重要でない）、行為『有（優）』価値（行為に意義がある）を前提に。やる気だって最初はなくていいのです。なにしろ今までネット漬け、ゲーム三昧

の生活を送っていたのですから目が覚めたように急に物事に積極的に取り組むようになるというのはありえないのです（親心としてそう望む気持ちはわかりますが）。ある日、いきなり「勉強好きに、俺はなる！」などと改心するのは漫画の世界ならともかく現実には考えにくいということを心に留めておくべきです。

マズローによれば人間の欲求は低次のものから高次のものにかけて段階的に上昇していくとされますが私か観察してきた限りネット依存、ゲーム依存から立ち直る子どもの心理は『イヤイヤ』（治療開始）、『仕方なく』（癖づけ）、『抵抗しつつ』（習慣化）、『決められたことゆえ』（定形化）、『生活の一部として』（日常化）というように〝低次〟から徐々に変化するものといえます。逆にいえば最初はやる気は低く（なく）ても、正しい方法論で治療を続けていけば必ず〝マスト型の子どもに変わることは可能です。

『歯磨き理論』というのは人間の行動心理に関する理論ですが端的にいえば「歯磨のように日常的、定型的に行っている行為は本人の意欲に関わらず習慣化する」というもの。幼い頃、あれほど歯磨きを嫌がっていた我が子もいつの間にか言われなくても毎日、勝手に歯磨きをするようになったのとネットやゲームとの関わりも同じことです。重度のオンラインゲーム中毒症であったＳ君が一日わずか三分の計算ドリルからリハビリを始め三ヵ月もするころには『ＡＤ』の習慣がついたように「ネットやゲームで遊ぶ前にやるべきことをやる」という既製事実を一つずつ積み上げて行けば子どもは変わるはずです。トレーニング原則にもあるように反復、継続が大切。指導のプロとして言わせていただければ大人が結果を急ぐとたいてい失敗します。焦らずじっくりリハビリに取り組ませてください。

五　ネット依存、ゲーム依存の危険シグナルを見抜け

どんな子どもでもネットやゲーム依存に陥る危険性はあります。そのことを前提にいかに早く危険シグナルを察知し、いかに適切な処置を施すかが子どもをネット依存、ゲーム依存から守るカギとなります。ここではその危険シグナルの見抜き方について子どもの生の姿を知る立場から説明します。

まず時期的なことをいえば『夏みかん』がキーワードです。よく育った夏みかんも外からの諸々の圧力によって内側が傷み、腐るものですが子どものネット依存、ゲーム依存もこれと同じです。おおまかに言いますと『な』（夏休み等の長期休暇）、『つ』（辛い、苦しい時）、『み』（みんなから取り残された、疎外されたと感じる時）、『か』（他者や自分の理想に適わないと感じた時）、『ん』（ん?これでいいのかと不安や心配を抱えた時）などがネットやゲーム遊びに依存し始めたり、依存度をさらに高める危ない時期だと思われます。

ところで子どもがネットやゲームに依存し始めたり、依存度を高めるようになる場合、どのようなプロセスを辿るのでしょうか。ボストン大学公衆衛生部門によるプロジェクト『ジョイン・トゥゲーダー』は薬物依存に至るまでには五つの段階が存在し徐々に依存度が高まりやがて中毒化すると説明していますが私が見る限りこれはネット、ゲーム依存にも概ねあてはまります。資料四においてはそれまでネットやゲームと縁がなかった、あるいは比較的、健全にこれらの娯楽に付き合えていた子どもがネット、ゲーム依存に陥ったり、依存度を高める心理プロセスを長年の観察から『ネット・ゲーム依存五段階説』としてまと

めました。

子どものネット、ゲームへの依存度はこのように高まっていくものと思われます。依存化を防いだり、進行を食い止めるためには我が子の言動をよく観察しておくことが必要です。

その観察の手掛かりとして今度はネット、ゲーム依存の行為の側面における危険シグナルについて説明します。もっともこの辺りのことは一般の書籍などでもしばし説明がなされておりますので長年、家庭という現場である意味一番、近い距離で子どもと接してきた者しかわかりえない兆候を中心にネット依存、ゲーム依存の危険シグナルの見抜き方を説明します。これらを参考にご家庭で予防策、治療策を講じたり場合によっては第三者、専門機関に相談されるなどの対処をされることが大切だと思われます。

いきなりですが、それまで勉強に無関心だった子どもが急に勉強の話をするようになったら実は危険な場合があります。勉強の話が危険?まあ、説明を聞いてください。まずは歴史から。最近のネットゲームには歴史上の人物や事件を扱ったものが実に多くあります。それまで社会や歴史にさして興味のなかった子どもが急に「あの人って?」、「あの事件は」などと口にし始めた場合、ネットゲームで興味を持ちさらにそれらをネットで検索したりしてはまっていることがままあります。特定の人物や時代、事件についてのみ関心を持ち始めたら要注意です。

英語について。私が教えていた生徒さんは中一でアルファベットもままならないのにやたら難しい単語の意味を質問するようになりました。英語に興味を持ったのかと喜んだのもつかの間、実ははまっていたオンラインゲームに出てくる単語なんですよね。普段、聞きなれない単語をいきなり口にしたり、その意

味を聞いてきたらネットゲームに取り憑かれている危険もあります。もしご兄弟がいらっしゃるなら「あんな単語、あの子の学年で習うの？」と聞いてみるのも危険察知の一つの手段でしょう。

字の乱れにも危険の兆候は現れます。薄い字、ミミズが這うような字、書く字の一つ一つがアンバランスである場合は危険シグナル。前二者はネットやゲームのやり過ぎで指や手首の筋力が衰えている危険が。また後者についてはネットやゲームのやり過ぎの結果、姿勢が乱れたり視力が落ちていたり遠近感にズレが生じている可能性があります。

勉強している時に利き腕（つまり鉛筆を持つ手）ではない側の腕を意味もなく動かすのは『ネットながら勉強』の症状です。つまり片手でマウスを動かしつつ『ながら勉強』をする癖が染み付いてしまっているのです。問題に集中してくると鉛筆を持っていない手で（マウス代わりに）消しゴムを持ち、無意識に手を動かす子どもはたいていがこの症状です。集中力と思考力が低下しますし視力の低下という危険とも関わりますのでやめさせましょう。

意外に知られていないのが聴力の衰えです。ある中学生の男子生徒はネットゲームのやり過ぎが原因で聴力に支障をきたし耳鼻科通いをするよいになりました。もっともこの生徒さんの場合、ゲームそのものに原因があったのではなく部屋で友達とオンライングームに興じているのを親にばれないようにカムフラージュで大音量のＢＧＭをかけ続けていた結果、一時的に難聴になってしまったのです。『個部屋とＢＧＭ』。ゲーム依存症に陥ったり進行させないために心あたりがある場合、一度チェックされることをお勧めします。

ある日いきなり、塾に行きたいと言い始めたら危険な場合も。友達の家がたまり場となっていてそこで仲間とゲームがしたいために外出の口実として「塾に・・」という場合があります。子どもがやる気になったといって手放しで喜んではいけません。一緒に通う友達をよく観察すること。また塾通いをさせる前に一ヵ月程、自宅学習をさせて本気度を確かめることも一案です。

友達が急に変わったら注意が必要な場合も。例えばネットゲームについていえば一つのクラスの中でも『熱狂派』、『常習派』、『ほどほど派』、『無関心派』くらいに熱中度に温度差がありそれに応じて〝派閥〟が出来上がっている場合が男の子についてはよくあります。子どもはえてして趣味の合う子と共に過ごす習性があります。観察材料の一つにしてみてください。

突然、夢を持ち始めたらネット依存の観点からまずい場合も。特にそれまで関心がなかった分野や領域の人、世界に憧れを抱いたり夢を持つようになったとしたらネット動画をあてもなく見る過程で表面的な憧れを抱いたり即席の理想像を描いているというパターンが実はあるのです。夢や憧れを「急に持つ」、その夢や憧れが「クルクル変わる」、抱く夢と憧れの「振り幅が大きい」という『症状』が見られたら先に述べたネットサーフィンで波に心を揺られていたりネットジャングルで彷徨いながら「浅き夢みし」を繰り返している場合があります。前記類型中、『現実逃避型』、『疑似体験型』の典型的な危険兆候です。

以上においては子どもとネット、ゲーム依存の危険シグナルを主に時期と段階と行為の側面から説明しました。先にも述べましたが大切なのはこれらの兆候が見られた場合、我が子の状況をよく観察、分析して然るべき措置をとるということです。その方法論についての解説、提言を次章で行います。

六　我が子を『ネット依存』、『ゲーム依存』から守るために親がなすべきこと

これまでの記述をふまえて本章ではまとめとして我が子を『ネット依存』、『ゲーム依存』から守るための解説、提言を行います。家庭教育のプロの立場から心構え、子どもとの接し方、ネット、ゲーム依存の予防、治療策について借越ながら子育て、家庭教育全般という観点からレクチャーをさせていただきます。

まず家庭科の授業です。総論としてネット、ゲーム依存とも深く関わる子育てに必要な『五大栄養素』の説明です。これらを念頭に記述を進めていきます。

最初の栄養素は『〝軽〟シウム』（カルシウム）。ここに〝軽〟とは「身軽さ」と「気軽さ」の二つを指します。子どもたちを取り巻く環境が、急速に変化する現代社会においては、身を軽くして、臨機応変に対応するフットワークが必要。それが前者です。後者は子どもと接する時の態度です。ネット教育も含めたしつけを行う場合、必要以上に肩肘張らずリラックスする姿勢も時に大切。「いい加減は、いい（良い）加減」。そんないい意味での気軽さを忘れずに。

次が『見られる』（ミネラル）。子どもは親のことをよく観察しています。ネットやゲーム遊びの仕方も含め我が子には常に見られているという意識が必要。その親の姿勢を子どもが真似るという意味で『見られる』は『まねらる』でもあります。

『わんぱく質』（タンパク質）は子どもの骨格をつくる上で欠かせない栄養素。精神科医の服部祥子氏は「幼い頃にした冒険の経験が子どもの自発性、創造性、自信を養う」と述べています。好きなことを見

つけ、自発的に物事に取り組む心と技と楽しさを身につけている子どもは安易な快楽に走ったりしないものですし、転んでも起き上がる図太さと逞しさを持ち合わせているもの。男の子も女の子もわんぱくでやんちゃなくらいに育てる心の余裕が親には求められます。

『シー・ボー』（脂肪）は静観の態度です。（シーっと）慌てず（ボーっと）気づかない振りも時に必要。もっとも取り（やり）過ぎると贅肉になって成長に悪影響を及ぼす危険があるのは体も心も同じ。

『〝ビター〟ミン』（ビタミン）は辛口の姿勢です。叱る時には厳しく、毅然として叱る。これはネット教育に限らず子育て全般にいえるしつけの重要な姿勢です。「然るべき（よくない事を正す）時は、叱るべき時」。このことを大人は心に刻んでおきましょう。以上が『五大栄養素』です。これらを前提に我が子をネット依存、ゲーム依存から守るための具体的提言を行います。

我が子にネット教育を行うにはまず親が現状をしっかりと把握することが求められます。親の世代の人には想像もつかないようなネットやゲームをめぐる環境が子どもたちの回りには広がっていることをよく認識してください。「メディアが至る所にある以上、その善し悪しを論じるのではなく子どもの環境の一部として受け入れなければならない」というマイケル・リッチ博士（『子どもの健康とメディアセンター』）の言葉はそのままネットとネットゲームにもあてはまります。我が子をネットやゲームと切り離せない時代にあることを理解してしっかり準備をしてください。

そうした観点からはネットやゲームについて親が学ぶことが強く要請されます。「私は機械が苦手で」、「今のゲームはわからない」などといってネットやゲーム遊びについて放任してしまう家庭では子どもが

好き放題にネットやゲームに興じて依存症に陥ったり、ますます依存度を高める場合が多いようです。図書館や書店に行けば、ネットやゲームとの関わり方に関する書籍は多数ありますし、定期的にネット教育についてのセミナーを開催している自治体も最近では増えています。こうした手段と機会を利用したり後に述べるように周囲の方に相談するなどして学習の機会をつくるようにしましょう。

親が見本になりましょう。親自身が目的もなく動画鑑賞に耽っていたりダラダラとオンライングームに興じていたら子どもに示しがつきませんし、そうしたけじめのない姿勢を子どもは見て、真似ます。時間を決めて、目的を定めてという具合に節度あるネットやゲームの利用をすることが求められます。前述したK君が制定した憲法のようなものをネットとゲーム利用に関する家訓として作って家族全員で守るようにするのもいいでしょう。大人が背中で示す。これを忘れずに。

指導のプロとしてアドバイスさせていただきますが、ネット教育を含めて子どもを育てる場面においては『スモールステップ理論』を取り入れることが効果的です。『スモールステップ理論』とは心理学者で行動分析学者の創始者でもあるフレデリック・スキナー氏が提唱したものですが要は最終的な目標を達成するためには「興味を失わせず、大きな失敗を防ぐべく目標達成を小刻みにする」というものです。Yさんのトレーニングにおいて義務の時間を小刻みに増やしていったのも内容にバラエティをもたせたのもこの理論の応用でもあります。私の指導経験からいっても「ここまでできた」と成果を『見える化』し小刻みかつ実現可能な次なる目標を内容に変化を加えつつ設定した方が子どもはやる気になります。ネット教育や、各種トレーニングを課す場面においては例えば、ネットを見る月間の合計時間が減ったとか、義務

とゲームの時間の比率が変わり義務の時間が増えたなど数値化したりグラフ化して次の目標を改めて掲げるという手法などが有益かと思われます。これはもちろん子育ての他の場面においてもいえることです。

目標設定と達成に関して「報酬」については注意が必要です。『飴と鞭』といいますが『飴』は厳禁だと個人的には思います。例えばネット利用について「時間厳守に関するこのルールを今月は守れたから、こんなご褒美」などというように一度、ニンジンをぶら下げてしまったらご褒美がないとルールを守れない、努力もできない子どもになってしまいます（そういう子どもを多数、見てきました）し、「次はこんなご褒美がほしい」、「誰々君の家ではこんなご褒美をもらっている」などとわがままを自己実現するべくより〝高次〟の報酬を子どもは要求してきます。少なくとも物質的な意味における報酬は子どものためを思うならやめるべきでしょう。

では『鞭』は?即ち、子どもがネットとゲーム利用に関するルールを守らなかった場合にいかなるペナルティを科すかという問題です。この点については労働事故災害防止における『体感訓練』が参考になります。『体感訓練』とは事故により心身に及ぶ危険を労働者自身に体感させることで自身の取り組みの甘さ、作業の杜撰さを反省させ後の事故防止の教訓にさせるというものです。私はかつて、どうしてもネット、ゲームについてのルールが守れなかった生徒さん向けに『ネット・ゲーム依存体感ワーク』として問題形式で数枚のプリントにまとめました。問題の主な内容は、〇ネットやゲームに依存し過ぎた場合の心身に及ぶ影響、〇進路や将来に及ぶ不利益、〇依存症が深刻化した場合に受ける治療の内容、〇仮に引きこもりになった場合の友達との関わり方の変化、〇要入院になった場合の家族の心労、経済的負担などで

す。こんな内容の問題を解かせることで起こり得る事の重大さ、深刻さに気づけば反省しかつネットやゲームとの正しい付き合い方を改めて知ることができるはずです。ペナルティとしてのみならず予防的処置からもこんな『定期テスト』を子どもに課すことを是非、お勧めします。

子育て全般にもいえることですがネット教育を行う場面において『兄弟同一視』は厳禁です。兄弟でも性格が違う以上、ネット、ゲーム依存の危険性は異なりますし各類型のどれにあてはまるかも、友人など周囲の環境から受ける影響の大きさも違います。一般的にいえば男の子の方が揮発性が高く(ネットやゲームにはまりやすい)、沸点も低い(ちょっとした事でネットやゲームに走る)もの。こうした男女の違いの例に見られるように子どもは個性が違う以上、同じ態度で同じ教育を施すというのは得策ではありません。「同じ家庭で育てた、ゆえに同じように育つという」合同条件はこと子育ての場面においては成り立ちません。ネット教育も個別性を前提にメニューや内容を考えてください。

自分をしっかりもっている子はネットやゲーム遊びに安易に走らないようです。そこでアイデンティティの確立が重要になるわけです。もっとも「こう育てれば、こう育つ」という科学的根拠に基づいたアドバイスはできませんが家庭という場で親子の関わり方をつぶさに見てきた『現場的根拠』からいわせてもらえば親が子どもの個性を認め、伸ばすという環境で育った子どもは自我意識をしっかりと持ち、自分の生き方、身の処し方がわかっているため周囲に容易に感化されることはないようですが逆に親にガミガミ言われたり価値観を押し付けられて育った子は無気力化して現実逃避に走ることが多いようです。これらはネット教育と直接関係ないように思われますが前記した類型化を見ればわかる通り子育ての仕方と

ネット、ゲーム依存は深い所でつながりと関わりがあります。これから我が子にネット、ゲーム依存についての予防策を講じる方も治療を施す場合も前記類型化を参考に自らのしつけや子育てのあり方と我が子のネット、ゲーム依存の関係を考え直してみたらいかがでしょうか。

最後にまとめとして我が子をネット依存、ゲーム依存から守るために親が持つべき『力』について説明します。まず『観察力』。ネット、ゲーム依存のシグナルを見抜いたり、我が子の症状、状況、周囲の環境を見つめる力です。この力を親が持つことがネット、ゲーム依存の早期発見、早期治療には特に重要です。

『放任力』も必要です。挫折した時や躓いた時に安易にネットやゲームに走らないよう困難に対処し自力で立ち上がる訓練をさせるべくあえて放任する心と勇気がこの『放任力』の主な内容です。

万が一、我が子がネット、ゲーム依存に罹った（罹りそうな）時に、冷静に判断して適切な処置を施すべく回りの人の意見に耳を傾ける『相談力』。若干、注意点をあげます。子どもと同年代の親はネットやゲームについての相談相手としてはふさわしくないようです。「家の子もネットばかりして」などと愚痴の言い合い、傷のなめ合いで終わるのがオチです。あらまほしきは先達なり。やや年の離れた子どもの、子育てが一段落した親がいいでしょう。子育てが一通り済んでいる親は子どものことを冷静、客観的にみられますのでネットやゲームの与え方、遊び方、しつけ方などについての有益な助言を反省をふまえてくれるはず。ただし十歳以上年の離れた子どもの親は相談相手としてはふさわしくでないようです。十年一昔といいますが十年も経てば子どもを取り巻くネットやゲームの環境も変わってしまうため的確なアドバイスは期待できないと思われます。我が子と五歳位年の離れた子どもの親でできれば同性の子どもの親が相談

相手としてはベストでしょう。

『叱責力』は子どもを正しい方向に導くために不可欠な力。子ども指導のプロの立場から言わせてもらえば子どもを正しい行き先に導くには〝BMW〟を運転することが不可欠。つまり〝B〟（ぶれず）、〝M〟（迷わず）、〝W〟（ワクワク）。因にワクワクとは欠点を修正することで得られる未来像のことです。もし子どもがネットやゲーム利用についてのルールを破ったら、毅然とした態度で、ためらうことなく、なぜルールを守る必要があって、そのことでと心と体に及ぶどんな危険が除去され、いかなる未来（たとえば勉強やスポーツ、進路などで得られる好ましい結果）が待っているかを教えること。この車は少ない労力で子どもを動かせるという意味で燃費がいいですよ。是非、我が子を正しい、明るい方向へ導いてください。

忘れてならないのが『家族力』。アルコール依存治療においてはしばし、『家族療法』といって家族の協力のもと患者を依存症から立ち直らせる手法がしばし、採られますがこれをネット依存、ゲーム依存の治療に応用します。F君は好きなサッカーを強い高校で続けると決め入試まで三ヵ月を切った段階で一念発起。勉強に専念するためそれまで寝る間も惜しんで！夢中になっていたネットゲームからの卒業を宣言。F君の熱意にほだされて家族一体となって協力。お父さんは晩酌をやめ趣味のゴルフを付き合いのみに。お母さんもはまっていた韓流ドラマを『冬ソナ』のみに（ヨン様だけは断ち切れなかったようです）。お姉さんはブランドの服とバッグを買うのを月に一回のみに（それでも多いか？）。

「先生も何か我慢してよ」とF君。教師として、大人として背中で示さなければならない私はF君の受験が終わるまで合コンの誘いを全て断りました。そんな家族の励ましと私の涙ぐましい努力のおかげで

（？）F君は見事に合格！こんな、ほのぼのとした家族力によるゲーム依存庄の乗り越え方も、あります。

ネット依存、ゲーム依存から子どもを守る最大の手段は好きなことを見つけること。心から好きで熱中できる『宝物』があれば無闇にネットやゲームに溺れることはないでしょうし仮にそうなったとしてもF君のようにそれを心の支えに依存症から立ち直れるはずです。大好きで夢中になれるものが見つかれば目標達成に向けて自覚ができ自ずと自己管理もできるようになるでしょう。そんな自分だけの宝物の見つけ方を資料五に『トレジャー・シート』としてまとめておきました。

人間の脳にはA10神経というものがあり「やって心地よいこと」、「成し遂げて嬉しかったこと」はやみつきになりさらに主体的に取り組む願望ができるといいます。心から夢中になれるもので達成感を味わえたならバーチャルな世界に逃げて虚しい快楽にうつつをぬかすこともなくなるでしょうし、現実世界と、またその中の等身大の自分と向き合いながら生きて行けるようになるはずです。ご家族で我が子の、我が子だけの『宝物』を見つけてみてください。

ここまで「我が子とネットの正しい付き合い方」というテーマで提言を行ってきました。私の指導経験をもとに解説を加えたものですがどの家庭でも応用しうるものばかりです。「人の子もすなるというネット教育を我が子にもしてみむとす」。是非、役立てください。もちろん、いつか私に子どもができたならこんな子育てとネット教育をします。そう、ぶれず、決して迷うことなく。

《資料一》　K君制定のネットとゲームと正しく付き合うための『七ヶ条の憲法』

第一条　ネットとゲームは時間を決めてやる
（平日は三十分土日、休日は一時間）
　☆けじめをつけるために制限時間を設ける
第二条　ネットとゲームは一日の終わりにやる
（宿題、予習、習い事の習字の課題、風呂掃除、皿洗いの後にやる）
　☆生活のペースを守るため、やるべきことをやってから遊ぶ
第三条　目的を書いてからやる
（何の目的でインターネットをやるか、どんなゲームをやるか示す）
　☆惰性で遊んだり、有害サイト等に手を出さないよう目的を明示
第四条　自室ではやらない
（ネットとゲームは自分の部屋ではやらずリビングでやる）
　☆ルール厳守を徹底するため両親の目の届く所で遊ぶ
第五条　食事中はネットやゲームの話はしない
（食事中は家族との会話を大切にするため、ネットやゲームのことは忘れる）
　☆家族とコミュニュケーションをとり、ネット依存、ゲーム依存を防ぐ
第六条　寝る前に読書を欠かさずする
（毎晩十分の読書を日課とする）
　☆ネットやゲームで興奮した心を落ち着け、かつ想像力を養うため読書
第七条　友達への三〝S〟は禁止
（友達をネットやゲーム遊びに『誘う』、『させる』、『そそのかす』ことはしない）

☆他の人のペースを乱さないため友達を巻き込まない

＊K君制定の『七ヵ条の憲法』に修正、解説を加えたもの

《資料二》トレーニング七原則

一　『過負荷』の原則
（日を重ねる毎に筋肉への負荷を増す）

二　『ざん進性』の原則
（レベルと負荷を少しずつ上げる）

三　『全面性』の原則
（筋力だけでなくさまざまな能力のアップを図る）

四　『反復性』（継続一生）の原則
（訓練の効果を得るため反復、継続する）

五　『個別性』の原則
（個々の実践者の状況や体力を考慮したプログラムを実施する）

六　『意識性』の原則
（いかなる筋肉をいかなる目的で鍛えるかをしっかりと意識する）

七　『特異性』の原則
（生じうる特異な事情をも考慮してトレーニングを実施する）

《資料三》Yさんの『ADトレーニング』の実践例

第一週目　漢字練習一〇の後にネット動画視聴五〇分
第二週目　計算ドリル一五分の後にネット動画視聴四五分
第三週目　英単語二〇分と犬の散歩の後にネット動画視聴四〇分
第四週目　国語読解プリント二五分と部屋片付けの後にネット動画視聴三五分
第五週目　数学文章問題三〇分と庭掃除の後にネット動画視聴三〇分
☆これ以外に土曜日は祖父母宅への荷物届け日曜日は親とパトロール・清掃等地域活動を『義務』の内容に加える
＊Yさん実施の『ADトレーニング』のメニューの内の一部を抜粋（上記各週の『義務』のメニューに他の内容の学習も加わる）

《資料四》『ネット（ゲーム）依存五段階』

第一段階『誘因』
何らかの要因によって、それまでネットやゲームに興味がなかった子どもが興味を抱いたり、健全に利用していた子どもが別目的で利用するようになる段階。挫折からの逃避やストレス解消、時間的、環境的事情からネットやゲームにはまるようになる。具体的要因としては成績不振、部活動での不調、レギュラーからの降格、友人、親、教師、先輩等との人間関係の悩み、友人、先輩、後輩、兄弟等に対する劣等感、友人、親等からのネット、ゲーム遊びの影響、時間の持て余しなど。

第二段階　『着手』

それまで、ネットやゲームに縁のなかった子どもが使用をし始めたり、ライトユーザー（頻度や熱中度が低い）だった子どもの利用頻度や、熱中度が高まる段階。

第三段階『享楽』

ネットやゲームで遊ぶ行為に『楽しさ』、『面白さ』、『快楽』を見出す段階。具体的にはネットやゲームで遊ぶことに、高揚感（気分がよくなる、テンションが上がる）、達成感（ゲームで上達することに達成感を覚える）、優越感（ゲームで勝つことで他者に、優越感を覚える）、隔離感（現実世界から隔離した世界の心地よさを知る）、逃避感（ネットやゲーム遊びに逃げ込むことで安心、満足する）を発見しかつその喜びを知る段階。

第四段階『日常化』

ネットやゲーム遊びが習慣イビ、日常化する段階。家に帰るとすぐにネットやゲームを始めたり、常にネットやゲームを気にし、ネットやゲームで遊ぶ時間が勉強、部活動、家の手伝い等の時間より長くなる段階。

第五段階『依存・中毒化』

ネットやゲームに依存して中毒化する段階。症状としては部屋に閉じこもりネットやゲームに興じる、家族との会話もそこそこにネットやゲームをする、ネットやゲームを禁じるとふてくされる、反抗的な態度をとるなどネットやゲームがないと生活に支障をきたすようになる重症化段階。

《資料五》好きなこと、やりたいことを見つけるための『トレジャー・シート』

一　『洗い出し』

何か好きで、何かやりたくて、何か向いているか考えます。そのための第一段階として『洗い出し』をします。以下の

ことを考えて紙に三〇個ほど書きましょう。

○楽しいこと
○できて、うれしいこと
○できないと、悔しいこと
○やっていると時間を忘れられること
○人に（親や親戚以外の人）に褒められた経験があること
○他の人に負けない（主観的判断でいい）と思えること
○努力を苦労と感じないこと
○その分野に憧れの人がいること
○人に反対されてもやりたいこと
○自分がその分野で活躍している場面を想像できること、想像するとワクワクすること

二　『絞り込み』

『絞り込み』を行います。上で書いたことから次のことをふまえて一〇個、選んでください

○やめられないこと
○やめたいと思ったことはないこと
○それなしではいられないこと
○それをやっていない状態や自分自身が嫌いなこと
○それをやっている自分が一番、好きなこと

三　『決め込み』

具体的に『決め込み』ます
○該当するものが一番多いこと

○それをやって失敗しても後悔しないこと
○改めて上で書いたリストを見て、それが一番、好きで楽しいと思えること

これらはあくまでも好きなこと、やりたいことを見つけるための第一歩です。やってみて向いてないと思ったり、楽しくないと感じたら振り出しに戻って他のことを見つけましょう。大切なのは好きなこと、やりたいことを見つけようとするプロセスです。こんな風に試行錯誤して見つけたものがあなたの『宝物』になるはずです。好きなこと、やりたいことが見つかればネットやゲームとも正しく付き合えるはずです。

サイバー犯罪情勢に即応するための インターネットホットラインセンターの 改善提言

大学生
（慶應義塾大学環境情報学部二年）
二宮　秀太（20）

第一章　はじめに

第一節　研究の意義と目的

本研究では、インターネットホットラインセンター（以下ＩＨＣとする）の運営の軸となっている「ホットライン運用ガイドライン」に焦点を当て、多くの人々が利用するサイバー空間におけるサイバー犯罪を、

利用者による発見・通報を手段として、防止活動に機能している、ＩＨＣの普及・機能向上に向けた施策を検討していく。

今日では、コンピュータ、スマートフォン、タブレットＰＣなどといった様々な電子計算機の普及により、多くの人々がインターネットを利用して生活を過ごしている。総務省による「通信利用動向調査」によると、二〇一三年にはインターネットの人口普及率は八〇％を超えた。利用者層も、小さな子どもからお年寄りまで、幅広い。また、インターネットの利用は、日常の検索を行う際にウェブ検索を利用するにとどまらず、Twitter や Facebook、mixi といったソーシャルネットワーキングサービス（以下ＳＮＳとする）サイトの活用、Yahoo! 知恵袋や2ちゃんねる等といった大型掲示板の利用のように、利用者間の情報交換ツールとして利用される機会も多い。

その一方で、近年では、インターネット上における規制薬物の広告、児童ポルノといった違法情報、犯罪その他の違法行為を引き起こす危険性があるような、公序良俗に反する有害な情報の流通が大きな社会問題としてあげられている。

本研究は、日々変遷を重ねているインターネット上における犯罪に対し、ＩＨＣが迅速かつ適切な情報収集と対処を行い、現行問題に見合った、適切な活動を行っていくための施策を提案することを目的とする。

第二章　ネット社会におけるインターネットホットラインセンター（ＩＨＣ）の現状

第一節　インターネットホットラインセンター（ＩＨＣ）とは

ＩＨＣは、警察庁の委託のもと、財団法人インターネット協会が管理・運営を行っている、日本におけるインターネット上の違法情報・有害情報の発信に関する情報収集と対処を目的とする通報窓口である。インターネットの利用者数は、二〇一三年には日本国内だけでも一億人を超え、日々無数の情報が交錯する。そのような多量の情報に対応するために、警察のみならず、インターネット利用者の通報によって違法情報・有害情報を発見する、いわゆる官民協働型の手法を用いた活動を行うＩＨＣが設置された。

ＩＨＣは、ホットライン運用ガイドライン検討協議会によって作成された、ホットライン運用ガイドラインに則って運営が行われている。また、ホットライン運営ガイドラインは一般のインターネット利用者の意見投稿を踏まえたうえで、見直し・改訂が重ねられており、現行問題に合わせた変化を重ねている。

ＩＨＣへの通報方法は、ウェブブラウザ内の通報ページからの通報とスマートフォン公式アプリケーションを利用した通報の二種類から成る。

第二節　対象とする違法情報・有害情報

ＩＨＣでは、インターネット上に流通している全ての違法情報・有害情報に対して対応するわけではない。インターネット上の情報には、その情報が違法性を有する情報、あるいは、公序良俗に反する情報

であるのかどうか、一見するだけでは判断が困難な情報も多く存在する。ＩＨＣでは、違法情報、あるいは有害情報であるということが明白であるもののみを対応しているのが現状である。また、違法情報・有害情報の定義、その具体的内容については運用ガイドライン上において規定されている。

第一に、違法情報については、運用ガイドライン上に以下のとおり規定されている。

「ホットラインセンターからプロバイダや電子掲示板の管理者等に対して送信防止措置等を依頼する「違法情報」の範囲については、インターネット上における流通が社会問題化している違法情報であって、ホットラインセンターにおいて適切かつ円滑に違法情報該当性を判断することができる情報を対象とすることが適当である」[1]

具体的には、①わいせつ関連情報②薬物関連情報③振り込め詐欺等関連情報④不正アクセス関連情報の四つの系統に分類され、違法情報自体を一〇種類に分類している。（六ページ表1参照）

ＩＨＣでは、これら一〇種類の違法情報に該当するもののみに対して削除対応や通報対応を行う。また、ＩＨＣから警察への通報を行ったことによって、二〇一二年には三、三〇三件の違法情報検挙をする成果をあげた。

第二に、有害情報については、運用ガイドライン上に以下の通り規定されている。

「ホットラインセンターからプロバイダや電子掲示板の管理者等に対して契約や利用に関する取決めに基づく対応を依頼する「公序良俗に反する情報」の範囲については、インターネット上における流通が社会問題化している情報であって、ホットラインセンターにおいて適切かつ円滑に、公序良俗に反する情報であるか否かを判断することができるものを対象とすることが適当である。」[3]

つまり、違法性は確認することはできないが、公序良俗に反すると判断される情報に対しては、有害情報と判断したうえで削除対応の対象と考えるということである。

では、公序良俗に反する情報とは、どのような情報のことを指すか。ホットライン運用ガイドラインでは、二種類の情報を指す。

第一に、情報自体から、違法行為を直接的かつ明示的に請負・仲介・誘引等すると考えられる情報である。例として、以下の一三種類をあげる。

① 拳銃の譲渡等
② 爆発物の製造
③ わいせつ物などの頒布
④ 児童ポルノの提供

⑤　公文書偽造
⑥　殺人・強盗・強姦・放火・障害・脅迫・誘拐
⑦　偽造通貨の交付・取得
⑧　臓器売買
⑨　人身売買
⑩　硫化水素ガスの製造
⑪　痴漢行為
⑫　不正アクセス

これらの情報は、ネット上に流通したとしても、一見するだけで違法性をもつような危険な情報であるか否かを判断することは難しい。しかし、これらの情報をきっかけに、犯罪を発生させることが十分に考えられるため、違法情報としてではなく、有害情報として対応すべきであると解釈することが適当である。

第二に、違法情報該当性が明らかに該当すると判断することは困難であるが、その疑いが相当程度認められる情報があげられる。

インターネット上にあげられる情報は、違法情報に該当する情報である可能性は否定できないが、確証がもてない情報が存在する。例えば、一八歳未満の被写体のポルノ画像の掲載は、児童ポルノ公然陳列として、児童ポルノ法に違反する違法情報である。しかし、流通するポルノ画像の被写体が一八歳未満なのであるか、一概に判断できない場合がある。被写体の年齢が一八歳以上であった場合、その画像に違法性

表１　IHC が定める違法情報[2]

違法情報の種類	違法対象となる法律
A. わいせつ関連情報	
①　わいせつ電磁的記録記録媒体陳列	刑法第一七五条第一項
②　児童ポルノ公然陳列	児童ポルノ法第七条第四項
③　売春目的の誘引	売春防止法第五条第三号及び第六条第二項第三号
④　出会い系サイト規制法違反の禁止誘因行為	同法第六条
B. 薬物関連情報	
⑤　薬物犯罪等の実行又は規制薬物（覚せい剤、麻薬、向精神薬、大麻、あへん及びけしがら）の濫用を、公然、あおり、又は唆す行為	麻薬特例法第九条
⑥　規制薬物の広告	覚せい剤取締法第二〇条の二 麻薬及び向精神薬取締法第二九条の二及び第五〇条の一八 大麻取締法第四条第一項第四号
C.　振り込め詐欺関連情報	
⑦　預貯金通帳等の譲渡等の勧誘・誘引	犯罪収益移転防止法第二七条第四項
⑧　携帯電話などの無断有償譲渡等の勧誘・誘引	携帯電話不正防止法第二三条
D.　不正アクセス関連情報	
⑨　識別符号の入力を不正に要求する行為	不正アクセス禁止法第七条第一号
⑩　不正アクセス行為を助長する行為	不正アクセス禁止法第五条

は認められない。しかし、もしも被写体の年齢が実際は一八歳未満であった場合、その情報は違法情報であるだけでなく、被写体の尊厳が大きく侵害される危険性をもつ。

また、たとえインターネット上に流出した情報の削除対応が完了したとしても、インターネット利用者が情報を保存している場合があり、その利用者が再度インターネット上にその情報を投稿すれば、再度、削除対応を行う必要性が出てくる。このように、インターネット上の情報は被害が広範囲に、急ピッチで広まる危険性があり、被害が広まる危険性を持ち合わせている。これについては、二〇一三年一〇月に発生した、三鷹女子高生ストーカー殺人事件におけるリベンジポルノ画像の流出からも見ることが出来る。

このような対処に喫緊性が存在する情報については、直ちに削除等といった対応を行う必要性がある。よって、これらの情報については、違法情報であるか否かの有無について問う以前に、有害情報であると判断し、対処するべきであると考えることが適当である。このケースに該当する情報は、児童ポルノ公然陳列の事例の他に、規制薬物の広告、不正アクセス行為を助長する情報が該当する。

第四節　ＩＨＣでは対応できない情報

ＩＨＣでは、違法情報・有害情報としてホットライン運用ガイドラインに規定されていない情報に対しては、削除対応を行うことができないとされている。例として、以下の情報があげられる。

① 犯行・自殺予告関連の情報

② ワンクリック、架空請求、フィッシング詐欺に関する情報

③ 迷惑メールに関する情報
④ 人権侵害（名誉毀損、プライバシー権侵害等）に関する情報
⑤ ヤミ金融による広告に関する情報
⑥ 知的財産権侵害に関する情報
⑦ 通信販売、ネットオークション等に関する情報
⑧ 不正アクセス、オンラインゲーム等に関する情報
⑨ そのほかの情報（死体の画像、未成年飲酒写真の掲載など）

これらの情報については、違法性・有害性を持ち合わせているのかどうか、慎重に検証を重ねなければその真偽を立証することができない。中高生のネットいじめ投稿を例示する。中高生がＳＮＳサイトに「○○ちゃん本当にキモい。死ね。」と投稿したとする。一見すると、この投稿は誹謗中傷を行っている、人権を侵害するような削除に値する情報かのように見える。しかし、この投稿は、中高生同士の軽いジョークであり、お互いに冗談だと理解しているのかもしれない。このように、一見するだけでは、悪意のある投稿であるのか否か、判断することができない場合がある。このような対応できない情報については、ＩＨＣ公式ホームページ上で相談機関の紹介を行うまでに留まっている。

第五節　外部協力機関

ＩＨＣでは、警察庁だけでなく、様々な機関との協力・連携によって運営を成立させている。機関の種類は、「パートナー」と「アソシエイツ」の二つに分類される。

パートナーは、ＩＨＣの活動に対する理解と賛同の下で、違法情報・有害情報に対する相談対応や、インターネット上での犯罪に巻き込まれないためのアドバイスなどといった、マルチなサポートを行っている関連機関・団体企業などのことを指す。現在は、以下の六機関がパートナーとして活動を協賛している。

・一般社団法人　テレコムサービス協会
・財団法人・日本ユニセフ協会
・ヤフー株式会社
・株式会社ヤマダ電機
・グーグル株式会社
・株式会社ソニー・コンピュータエンタテイメント

アソシエイツは、ホットライン運用ガイドライン上の違法情報・有害情報に対して、専門的な対応を行っている機関、団体、企業等のことを指す。これらの機関では、直接的に削除依頼を行われない情報に対し

て、必要に応じた専門的な見地を提供する。また、違法情報・有害情報の対象とはならない情報であっても、著作権等の侵害が認められる情報については、アソシエイツとの情報共有を行う。これによって、今後の侵害防止・対応に向けてアソシエイツが対応を行っていくこととなる。現時点では、下記の四つに分類されている。

① 誹謗中傷・プライバシー侵害情報
② ヤミ金融による広告
③ 知的財産権侵害情報
④ フィルタリング事業者

第三章　ＩＨＣ現行ガイドラインに関する考察と提言

第一節　ＩＨＣにおける現行の活動に関する考察と課題

ＩＨＣは、官民協働によるサイバー犯罪対策として、成果をあげてきた。しかし、今後の活動を行っていくにあたって、課題も残されている。

第一に、通報件数の向上のための検討の必要性があげられる。二〇〇七年に内閣府によって行われた、「インターネット上の安全確保に関する世論調査」における調査結果（図1参照）からも読み取れるように、インターネット利用者は、ＩＨＣへの通報にあまり積極的ではないということが見受けられる。

では、通報に積極的ではない理由は何なのか。同調査において、ホットセンターに通報しない理由について調査したところ、通報のための手順に不満を感じている声が多くあげられた。（図2参照）

現在は、公式ホームページ上の通報フォームとスマートフォン専用通報用アプリケーションの二種類の方法が通報方法として採用されているが、これらの通報手順の簡略化、新たな通報方法の開発が求められる。

第二に、対応できる違法情報・有害情報とインターネット上で発生する犯罪の間でズレが発生しうる点である。第二章第三節のように、現在のＩＨＣで対応できる違法情報の種類は①わいせつ関連情報②薬物関連情報③振り込め詐欺関連情報④不正アクセス関連情報の四類型一〇種類のみに限られている。その一方で、インターネット上における犯罪の種類は日々、変化を重ねている。しかし、現在のＩＨＣでは、これらの新たに生まれるインターネット上の犯罪手口に対する対策・対応が何一つ行われていないというのが現状である。このように、インターネット上に蔓延しているタイムリーな犯罪に対して、対応できるシステムがとれていないという問題点が指摘される。

第二節　ＩＨＣに対する提言

それでは、第一節で述べた、現時点での課題を解決していくためには、具体的にどのようなアプローチが必要であろうか。本稿では、二項に分けて二つの提言を行う。

第一項　ウェブ拡張機能の応用

本項では、通報件数の向上のための提言について述べる。第三章第一節で述べた通り、現在のＩＨＣへの通報方法では、「通報のやり方がよくわからない」「通報のやり方が面倒」のように、通報手順の難解さを理由に通報に参加したくないインターネット利用者が多く確認された。そこで、ＩＨＣ通報のためのウェブ拡張機能の応用を提案する。

ウェブ拡張機能とは、ウェブブラウザ用ソフトウェア（Mozilla Firefox、Google chrome など）に組み込ませることで、設定や操作の機能強化を行うもののことを指す。

現在広く利用されている拡張機能の例として、YahooJapan が提供している拡張機能「Yahoo! ツールバー」を取り上げる。Yahoo! ツールバーを拡張機能として組み込んだ場合、ウェブを閲覧している間、常に画面上に検索窓が表示される。これによって、どこのサイトを閲覧しているときでも、検索エンジンを手軽に利用することができる。つまり、「Yahoo! ツールバー」という拡張機能を用いたことで、「検索エンジンの利用手順の簡略化」という機能強化が行われたといえる。

ＩＨＣにおいても、拡張機能を使用した通報作業を可能にすれば、通報する手間の省略、作業簡略化が期待できる。現在の通報ページの場合、違法情報の掲載されているサイトのアドレスをコピーし、ＩＨＣのページを検索・移動し、通報フォームを選択、違法情報の掲載されているサイトのアドレスをペーストし、必要事項を記入することで、やっとのことで一件の通報作業が完了する。それに対して、拡張機能による通報作業を開発すれば、拡張機能によって画面上に表示されているアイコンをクリックし、

通報ボタンをクリックするだけで通報が完了される。（図3参照）これだけ通報作業を簡略化すれば、内閣府における「インターネット上の安全確保に関する世論調査」でもあげられていた、「通報のやり方がよくわからない」「通報の手順が面倒」といった意見に対する解決が期待できる。拡張機能の開発においても、パートナー・アソシエイツ機関からの専門的な見地を踏まえ、共同開発を進めていくことによって、連携の強化が期待できる。

第二項　「注意情報」、注意情報の情報共有制度の導入、注意表示機能の導入

本項では、対応できる違法情報・有害情報とインターネット上で発生する犯罪の間でズレが発生しうる点について述べる。第三章第一節で述べた通り、違法情報・有害情報の対象物はインターネット上で蔓延している問題のごく一部であり、タイムリーな問題についてはガイドライン改訂を行わない限り対応を行うことが出来ない現状にある。

そこで、ＩＨＣからの新たな対応情報の分類「注意情報」の導入、注意情報の情報共有制度の導入、注意表示機能の導入を提案する。

第一に、新たな対応情報の分類「注意情報」の導入を提案する。インターネット上の情報は、法的根拠がない限り、第三者が削除対応を行うことができない。その一方で、一般のインターネット利用者は、削除対応こそされないものの利用者に危害を加える危険性を持つサイトと隣り合わせにある状態にある。その上、そんな危険を持ち合わせている可能性のあるサイトだと警告が表示されるわけでもないため、危険

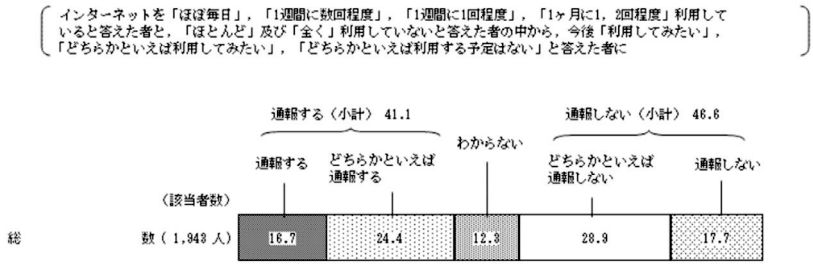


図1　ホットラインセンターに通報する意識[4]

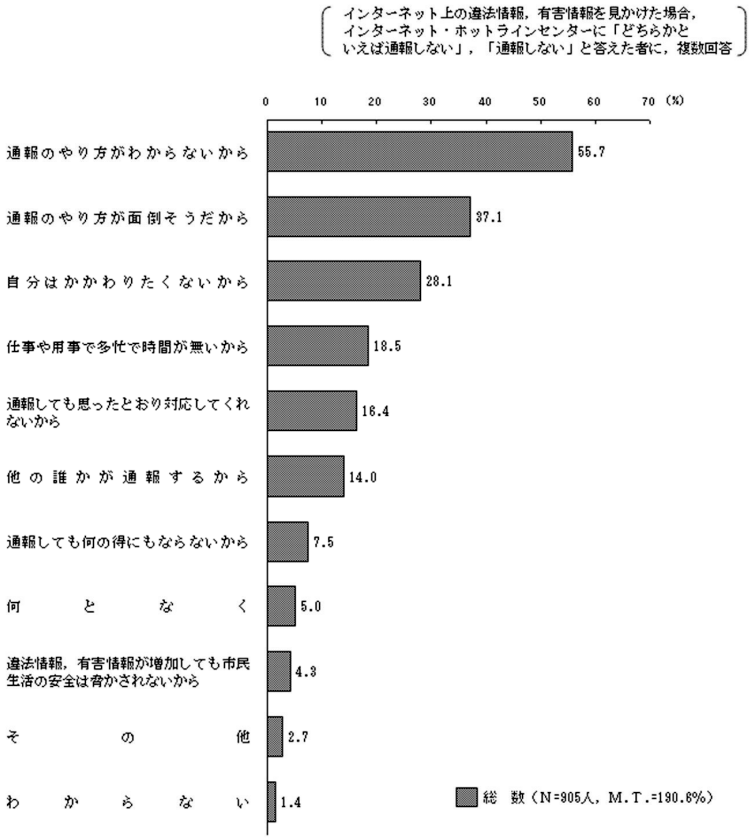


図2　ホットラインセンターに通報しない理由[5]

性について気づかないまま利用してしまう。そこで、通報された情報の中で、違法情報・有害情報に該当しないものの、利用者に危険を与える危険性がある情報、あるいは、誹謗中傷の表現が用いられるなど、利用者の気分を害する可能性のもつ情報を「注意情報」として対応を行うようにする。具体的には、ネットいじめ、不正ウイルスを自動インストールさせるサイト、著作権を侵害している可能性があるサイトなど、インターネット上における現行問題に応じて対象を追加する。注意情報に該当するサイトかどうかの判断は、ＩＨＣに通報された情報から、従来の違法情報・有害情報の分類する作業の時点で行う。

第二に、注意情報の情報共有制度の導入を提案する。現行施策では、違法情報・有害情報に該当しないが、危険性が予測される情報が紛れ込んでいた際には、アソシエイツ・他機関に情報共有が行われている。しかし、情報共有についての規定が明文化されていないため、どのような情報について情報共有を行うべきか否かについては、ＩＨＣの裁量にゆだねられているのが現状である。そこで、現在は通報対象とされていない情報についても、「注意情報」として通報の対象とし、注意情報については、ＩＨＣがアソシエイツ・他機関に情報共有を行う旨の規定を行う。規定通りに情報共有を行えば、情報共有はより円滑に進むことが期待される。また、通報対象の情報を増加とともに、アソシエイツ・連携する他機関の強化を行うことによって、専門機関における判断が必要な情報、たとえば、危険ドラッグのネット販売、ヤミ金融の広告、著作物の違法アップロード等、現代社会において問題となっておきながら、ＩＨＣでは取扱いを行っていなかった情報のほぼ全てを、対応の対象とすることが可能となる。

第三に、注意表示機能の導入を提案する。注意情報については、確固たる法的根拠が存在しないため違

法情報・有害情報のように削除対応を行うことができない。そこで、第一項にて提案したウェブ拡張機能を用いて、注意情報を含むサイトを表示した際には、「ＩＨＣに通報が寄せられた、注意情報該当サイトです」と表示させるように機能を組み込む。開発技術としても、事前に設定しているサイト（注意情報該当サイト）にアクセスされた時にエラーメッセージを表示させるという簡単なものになるため、開発における大きな課題点は見つからない。この機能の活用によって、知らず知らずのうちに危険なサイトに近づき、トラブルに巻き込まれる事例を防ぐことができる。削除こそはできないものの、一度通報を受けたサイトであると認識できるため、そのサイトに対する危機意識が高まり、問題に巻き込まれる

図３　通報ボタンモデル図[6]
拡張機能によって画面上に通報ボタンを表示する。拡張機能によって表示されている、右上の赤枠で囲ったボタンをクリックすることで、通報を可能にする。これによって、通報を簡略化できる。

リスクが軽減することが期待される。

第四章　結語

冒頭でも述べたように、インターネット上で発生する犯罪は日々変化を重ねており、それらに対する対応を行う必要性が求められている。本稿では、官民協働の形をとっているＩＨＣに注目し、現在の運営体制について調査を行い、その上での提言をすることを目的として、検討を進めてきた。

現在の運営体制では、指定された情報のみへの対応となり、対象外の情報については適切な対応を行うことが難しい現状が確認された。

現状として、インターネットホットラインセンターは情報の送り手である、情報先に対する対応のみを行っている。しかしながら本来は、ＩＨＣは、情報の受け手であるインターネット利用者の危機意識を高めることが求められるべきである。そこで、ウェブブラウザ拡張機能による注意情報表示機能をはじめとした施策を用い、インターネット上の犯罪をより身近に感じさせることで、情報の受け手である利用者の危機意識を高めることが可能である。現施策で行われている情報の送り手に対する対応だけでなく、新たに情報の受け手に対する対応策を講じ、双方向から対応策を行っていけば、インターネットを安全に利用できる可能性が広がっていくのではないだろうか。

そのような観点から、本提言策が、インターネット利用者のネットに対する危機意識を高め、より安全

な利用を可能にするための効果的なアプローチと考え、ＩＨＣに対し、本提言策の導入を強く求める。

最後に、本提言策が、すべてのインターネット利用者の「安全・安心」に寄与することを願い、本稿を結ぶこととする。

第五章　参考資料

第一節　参考文献

㈠　警察庁「平成二四年行政事業レビューシート　事業番号二九」（二〇一二年発表）

㈡　岡村久道「情報セキュリティの法律」日本法規（二〇一一）

㈢　岡村久道「インターネットの法律問題」商事法務（二〇一三）商事法務

㈣　四方光「サイバー犯罪対策概論」立花書房（二〇一四）

第二節　参考 web ページ

㈤　インターネットホットラインセンター公式ホームページ
http://www.internethotline.jp/
（二〇一四年七月七日閲覧）

㈥　ホットライン運用ガイドライン九訂全文（二〇一四年八月一日改訂）

http://www.iajapan.org/hotline/center/20140801public.html
（二〇一四年八月三〇日閲覧）
(七)　平成二五年警察白書　統計資料
http://www.npa.go.jp/hakusyo/h25/data.html
（二〇一四年七月七日閲覧）
(八)　平成二六年警察白書　概要
http://www.npa.go.jp/hakusyo/h26/index.html
（二〇一四年九月二日閲覧）
(九)　平成二五年中の「インターネットホットラインセンター」の運用状況等について　警察庁広報資料（二〇一四年四月二四日発表）
http://www.npa.go.jp/cyber/statics/h25/pdf03-2.pdf
（二〇一四年七月七日閲覧）
(十)　平成二五年中のサイバー犯罪検挙情報等について　警察庁広報資料（二〇一四年三月二七日発表）
http://www.npa.go.jp/cyber/statics/h25/pdf01-2.pdf
（二〇一四年七月七日閲覧）
(十一)　インターネット上の安全確保に関する世論調査　内閣府大臣官房政府広報室（二〇〇七年発表）
http://www8.cao.go.jp/survey/h19/h19-inter/index.html

（二〇一四年七月三一日閲覧）

㈢　インターネットバンキングの不正送金事案の発生について　滋賀県警察（二〇一四年三月二七日更新）
http://www.pref.shiga.lg.jp/police/seikatu/cyber/security/phishing.html
（二〇一四年八月三〇日閲覧）

注

1　ホットライン運営ガイドライン九訂五ページより引用
2　ホットライン運用ガイドライン九訂を基に筆者作成
3　ホットライン運用ガイドライン九訂一三〜一四ページより引用
4　内閣府大臣官房政府広報室、インターネット上の安全確保に関する世論調査より引用
5　内閣府大臣官房政府広報室、インターネット上の安全確保に関する世論調査より引用
6　筆者作成。ブラウザ画面はインターネットホットラインセンター公式ホームページより引用

ネット社会を安全に暮らす
～スマートフォンの落とし穴～

大学生（大東文化大学法学部四年）
初野　皓紀（21）

はじめに

「ネット社会を安全に暮らす」というテーマのもと、副題に「スマートフォンの落とし穴」というテーマで論じていく。近年爆発的にスマートフォンが普及して我々の暮らしが便利になる一方、様々な犯罪の被害がマスコミ等で報道されることが多くなったことである。

私が書く理由は二つある。従来、コンピューターウイルスやサイバー犯罪はコンピューターを中心に横行していたが、前述の通りスマートフォンの普及により、高機能高性能な端末が多数普及したことにより、サイバー犯罪がより身近になっている。また、近年未成年者がＬＩＮＥなどのコミュニケーションツールやTwitterやFacebook等のＳＮＳで犯罪に巻き込まれることが、頻繁に報道されている。このような現状からスマートフォンの利用について考えなければならないと思ったのが、この論文執筆の理由の一つである。

二つ目の理由として、漠然とスマートフォンでの犯罪が増えていることやアカウントの乗っ取り、金銭被害が起こっていることは知っているが、対策などについてしっかりと考えたことが無かったという思いになった。犯罪被害の対策を知らなければ、未然に防ぐことの出来る被害も防ぐことが出来ないと考え、本稿を執筆する過程で改めてスマートフォンでのセキュリティを考え直してみようという考えに至った。

最後に、これから私たちはどのようにすれば安全、快適にスマートフォンのような端末を利用していけるかを提言する。

一章　スマートフォンの現状とその正体

一　スマートフォンとは何か

まず、スマートフォンの問題点を論じる前にスマートフォンとは何か、私たちの生活にどのような影響

を及ぼしているかを論じてからスマートフォンの問題点・危険性などを論じていこうと思う。従来使われてきた携帯電話、最近ではガラパゴス携帯と呼ばれる端末とどのように違うかという視点から考えていこうと思う。本稿では、Apple のスマートフォン向けの OS（オペレーティングシステム、スマートフォンの基礎を構成するもの）である iOS や Google のスマートフォン向けの OS である Android 等は、特に明記が無い場合は区別なく扱う。

まず、スマートフォンの特徴の一つ目は、パソコン用の Web サイトを閲覧することが簡単に出来ることである。従来の携帯電話では NTT ドコモでは i モード、au では EZweb 等それぞれの携帯電話通信事業者が管理するネットワークで提供されていたインターネット接続サービスを使用していた[1]。

それに対して、スマートフォンでは前述のようなサービスを介さず、インターネットに接続することが出来る特性を持っている。

二つ目の特徴としては、スマートフォンは多種多様なアプリケーションを利用者自らダウンロードストア（iOS では App Store、Android では Google Play 等が代表格）でダウンロードをして使用することが出来る。このアプリケーションを利用して利用者はニーズに合った使い方が可能となっている。一方、ガラパゴス携帯では元々赤外線通信機能が搭載され、ワンセグ搭載でテレビを見ることが可能であった。しかし、スマートフォンのようなアプリケーションによるカスタマイズの幅は狭く、スマートフォンほど利用者がカスタマイズすることは出来なかった。

三つ目の特徴としてスマートフォンの処理能力は非常に高い処理能力を持っていることである。現在の

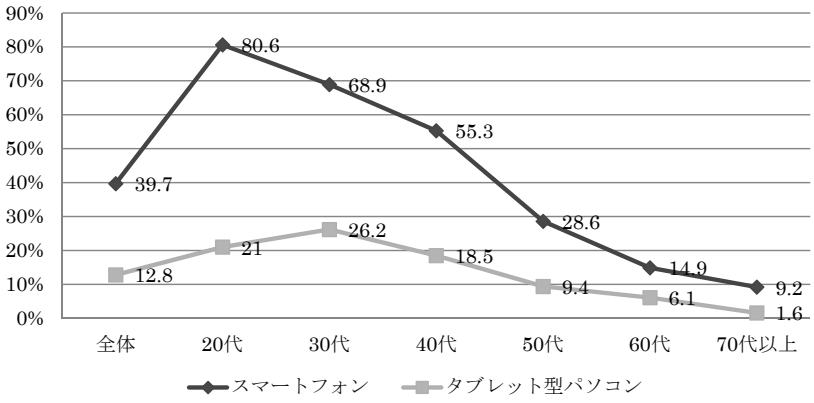
スマートフォンは、学校や企業でもよく利用されているWindows OS搭載のパソコンに引けを取らないほどの処理能力を持っている。このことからスマートフォンは手のひらサイズのパソコンと考えるべきである。

以上のような点からスマートフォンを従来の携帯電話であるガラパゴス携帯と同じものと考えるのは間違いである。前述の通り小さなパソコンということをしっかりと認識しないと場合によっては犯罪に巻き込まれることも考えられる。実際にスマートフォンを利用した犯罪は発生しており、この点については後述する。

二　スマートフォンの普及率

次にスマートフォンの普及率から現在の携帯電話の傾向を見ていこうと思う。二〇一四年第一四半期でスマートフォンの普及率は四〇％程となっている。世代別に見ると二〇代では普及率が約八〇％、三〇代では約七〇％となっている。対して、七〇代以上では普及率は一〇％

図表１　スマホ・タブレット普及率



出典：大和総研グループ　『スマホの正確な普及率は？』
http://www.dir.co.jp/library/column/20140522_008534.html

以下である[2]。このような現状から、世代によってスマートフォンの普及率に差があることが分かる。

ここでスマートフォンではないが、スマートフォンと近い性質を持っているタブレット型パソコンについても触れておこうと思う。近年スマートフォンと同じように普及が進んでいるタブレット型パソコンはWindows搭載の物もあるが、スマートフォンと同じようにiOSやAndroidを搭載するものが多い。そのため、使用方法や留意すべき点などがスマートフォンと共通する点が多い。

また、タブレット端末の国内出荷台数も伸びており、スマートフォン同様まだまだ、普及していくものと考えられる[3]。

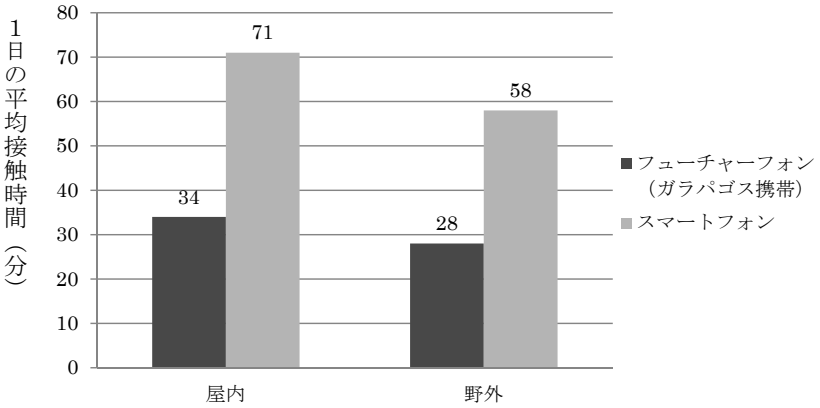
また、未成年者の普及率に限定すると、未成年者全体（一〇歳～一八歳）の所有率は六〇・四％となり、小学生（一〇歳～一二歳）で三七・九％、中学生は五五・三％、高校生は八七・九％となった[4]。このように未成年者、特に高校生はスマートフォンの所有率が非常に高いことが分かる。このことから、スマートフォンは若い世代には必要不可欠なものになっていることが分かる。

三　スマートフォンのサービス・利用度

次にスマートフォンの利用状況から現状を考えていこうと思う。図表2からスマートフォンの利用時間が屋内外を合わせると従来のガラパゴス携帯より二倍近い一二九分の接触時間があり、このような数字から、スマートフォンの存在は私たちに情報端末に接触させる時間を増加させる傾向があることが分かる。

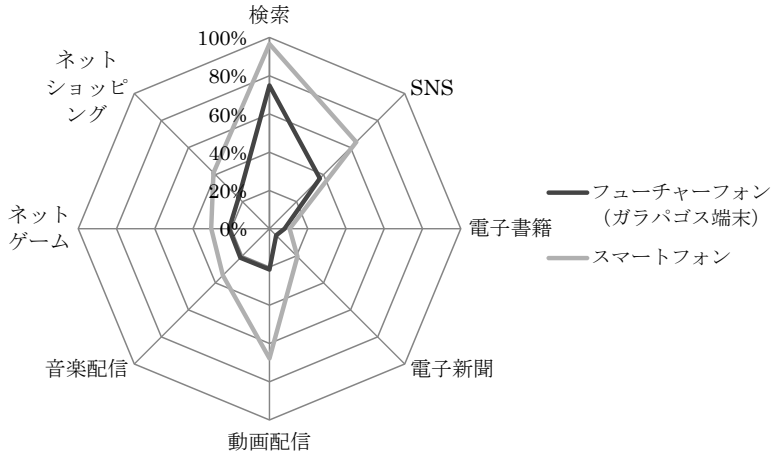
図表3からはユーザーがガラパゴス携帯、スマートフォンを利用してどのようなコンテンツやサービス

図表２　各端末のユーザーの接触時間



出典：総務省　『スマートフォンユーザーの特徴（従来型携帯電話ユーザーとの比較）』
http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h24/html/nc122310.html

図表３　サービス別利用動向の端末別比較



出典：総務省　『スマートフォンユーザーの特徴（従来型携帯電話ユーザーとの比較）』
http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h24/html/nc122310.html

を利用しているかが分かる。この図表からはスマートフォンはサービスの利用を促す効果があることが明確に分かる。特に検索、ＳＮＳや動画配信等インターネットを利用したサービスの増加が顕著であることが読み取れる。

以下のようなコンテンツが増加した背景として考えられるのは前述の通りのスマートフォンが高機能である点、画面が大型で動画視聴等に向いている点、４ＧやＬＴＥと呼ばれる高速で通信ができるモバイルデータ通信が行える点などが考えられる。

本章ではスマートフォンの現状や利便性について論じてきたが、次章では、スマートフォンの危険性や現在問題となっている社会問題について論じて行こうと思う。

二章　スマートフォンの危険性

一　個人情報漏えいの危険性

前章ではスマートフォンの基本事項やその機能について論じてきたが、本章ではスマートフォンの危険性や落とし穴について論じていこうと思う。またその対策については次章に回すことにする。

まず、近年話題になることの多い情報漏えいがスマートフォン上でも起こり得ることについて論じていこうと思う。

まず、スマートフォン上に保存されている個人情報はどのような物であるか確認していこうと思う。多

種多様な個人情報が保存されているスマートフォンだが、特に電話番号やメールアドレス、各種サービスのＩＤやパスワード、カメラで撮影した画像などが保存されていることが多い。また、クレジットカード番号を保存する機能を備えている場合もある（Apple 社の iCloud キーチェーン等）。

このように多種多様な個人情報が保存されているスマートフォンから情報漏えいが起こったら非常に大きな問題となる。また、クレジットカード番号等が漏えいした場合、不正利用されてしまう場合も考えられる。

さて、このような個人情報の流失の原因は何かという点について論じていこうと思う。まず、一番の脅威として考えられるのは紛失・盗難である[5]。やはり、スマートフォンも従来の携帯電話と同じように携帯端末であることから紛失や盗難が一番の脅威となることは簡単に予想することが出来る。

次に情報漏えいの原因として考えられるのは、スマートフォンを狙ったコンピューターウイルスや悪意を持ったアプリケーションが考えられる。コンピューターウイルスと言うと Windows を想像する方も多いかもしれないが、現在スマートフォンでもウイルスの被害が報告されている。

特に Android 端末での被害が多く報告されている、例えば有用なアプリに偽装してＳＭＳ（ショートメッセージサービス）を悪用するトロイの木馬やスマートフォンに搭載されているＧＰＳの位置情報を第三者に送信してしまうスパイウェアなどが過去に問題となった[6]。このようなトロイの木馬やスパイウェアと言われるものは、昔はパソコンでの被害が主流であった。しかし、現在ではスマートフォンでも被害が出ていることをしっかりと認識しなければならない。

二　金銭被害の可能性

前節ではスマートフォンにおける情報漏えいの危険性について論じてきたが、本節ではスマートフォンにおける金銭被害について論じていこうと思う。

まず、二〇一四年になり被害出て報道されるようになったメッセージアプリのＬＩＮＥ上の不正ログインにより、第三者にアカウントが乗っ取られた。さらに、その乗っ取られたアカウントから友人を装って電子マネー等の購入を促し、金銭をだまし取る被害が発生した[7]。またこのケースの場合、他のサービスで利用していたパスワードが流出し、それを利用して不正アクセスが行われた可能性も指摘されている。

このように日常生活を便利にするアプリケーションも使い方や管理方法を間違えると金銭被害に会う可能性を生むことがあるという良い例であると考えられる。また、このようなケースの場合自分だけではなく、知人や家族にも被害が及ぶことが予想される。

次にスマートフォン自体を乗っ取られる可能性について触れてみようと思う。

これは、ランサムウェア（Ransomware）と呼ばれており、マルウェア（コンピューターウイルスなどの総称）の一種である。スマートフォンやパソコンに勝手にアクセス制限を掛けて持ち主に金銭を要求するものである。

既に日本語版も確認されており[8]、すでに私達に無関係ではないことが分かる。マルウェア等を使って行われる金銭を要求する行為は近年様々な種類が報道されており、スマートフォンを使用する上での脅威

と考えられる。このようなマルウェアに対する対策等も次章で触れることとする。

また、ネットバンキングを狙った偽アプリケーションの存在も確認されている。例として、二〇一三年末に欧州で大きな被害を出した「Operation Emmental」（オペレーション・エメンタル）と呼ばれる事件が大きな問題となった。

この事件では、欧州でネットバンキングの安全性を高めるために広く使用されているスマートフォンを使った認証であるワンタイムパスワードを悪用して行われた。手法としては、パソコンに感染したウイルスによって偽サイトに誘導して、偽アプリケーションをダウンロードさせ、ワンタイムパスワードを盗み取って不正送金が行われた[9]。

また、欧州を狙った犯罪ではあったが、日本の銀行も攻撃の視野に入れていた可能性も指摘されており、私たちの銀行口座が狙われる可能性が高いことが分かる。

三　不正アプリケーションの脅威

本章では個人情報の流出や金銭被害の可能性について論じてきたが、本節では、その原因となりうる不正アプリケーションやプログラムについて触れる。

セキュリティベンダーのマカフィーの発表によると、スマートフォン向けの不正アプリケーションは増加傾向にあり、二〇一四年第一四半期で七五万件以上が発見され、累計では四〇〇万件近く発見されていると警告している。また、これらの不正アプリケーションが集める情報は多岐にわたり、「通信利用状況」

「実行中のタスク」「電話番号」等様々な情報を収集しているとされる。

不正アプリケーションではない、正規のアプリケーションでも位置情報等を収集していることがマカフィーによって警告されており、このような事例からアプリケーションの使用には最新の注意が必要であることが分かる。

また、スマートフォン監視システムが堂々と販売されていることも指摘されている。このスマートフォン監視システムは「ガリレオ（ＧＡＬＩＬＥＯ）」と呼ばれるリモートコントロールシステムである。このシステムを利用することによって、通話記録・メール・電話帳・位置情報・録音や写真撮影が可能とされており、スマートフォンが高性能な盗聴器になることが容易に想像できる。

しかし、この監視システムは高度なものであるため、金銭目的には使われないとされ、政治家やジャーナリスト等の監視に使われているのではないかとされている[10]。

四　ＧＰＳ機能の落とし穴

最後にスマートフォンによく搭載されているＧＰＳ機能の落とし穴について触れてみようと思う。現在ナビアプリなどで利用されるＧＰＳ機能だが、ここにもスマートフォンを使う上での危険性が潜んでいる。

もっとも簡単な例は自分で撮影した写真にＧＰＳで取得した情報が含まれている場合があることだと考えられる（スマートフォンの設定で変更が可能）。このようなケースの場合、簡単な処理で撮影した場

所などが他人に知られてしまうことも考えられる[11]。またこのような情報を持った写真をＳＮＳなどに投稿した場合自宅の住所などが流出する危険性も考えられる。

以上、スマートフォンの危険性について何点か論じてきたが、次章では本章で触れたような危険性を防ぐための方法やこれからスマートフォン等の情報端末とどのように向き合うべきかを提言していこうと思う。

三章　スマートフォンを安全に使うための対策と提言

一　スマートフォンを安全に使うための対策

本章では前章で触れたような被害に会わないためには、どうしたら良いかや私たちがどのようにこの問題に向き合っていくかを提言していこうと思う。まず、スマートフォンを使っている私達に忍び寄ってくる脅威に対してどのような対策があるかを論じていこうと思う。

スマートフォンを使用する上で最も基本的であり重要なセキュリティ対策はＯＳ（オペレーティングシステム）のアップデートである。一章でも触れたが、スマートフォンのＯＳはiOSやAndroidなどの違いはあるが、どちらも定期的にメーカーからＯＳのアップデートが配信されている。また、Androidの場合は機種によってＯＳのアップデートの有無やバージョンが違う場合があるので注意が必要である。

二つ目に重要なことはコンピューターウイルス対策をしっかりと行うことである。この対策をしないと

二章で論じたような個人情報の流出などの原因となり得る、これを防ぐためには前述のＯＳのアップデートも有効であるが、怪しいアプリケーションをインストールして使わないことが効果的であると考えられる。

このためにも正規のアプリケーションストアからアプリケーションをダウンロードすることが重要である。また、ＳＮＳ（ソーシャル・ネットワーク・サービス）等からの勧誘等が行われる場合があるが[12]、基本的にはダウンロードすることは危険であると考えられる。

しかし、正規のアプリケーションストアにおいても偽物が発見されたという報告[13]もあるので、完全に信頼することは危険であると考えられ、自分で情報を集めて自衛することが重要である。このような問題はAndroidにおいて発生することが多く、Androidを使用する場合はセキュリティソフトを使用することが望ましい。

だが、このセキュリティソフトにも偽物が存在していることも事実である[14]。そのため、セキュリティソフトを選ぶ際は量販店で販売しているものや、各通信業者が公式に配信しているアプリケーションを使用することがリスクの低減に繋がると考えられる。しかし、無料でも有用なものは公式マーケットで配信されているのも事実であり、しっかりと情報を集めて有効活用することも一つの手段である。

三つ目に携帯端末の宿命ではある盗難や紛失にどのように対処するかを論じていこうと思う。前述したとおり、スマートフォンは個人情報の塊であり、それを盗難・紛失されることは非常にリスクが高い。ではどのように対策をすればよいかと言う点では、現在では遠隔操作によってスマートフォンをロックした

りデータを消去したりすること出来る[15]。

二　スマートフォンを安全に使うための提言

本節では、スマートフォンを安全に使うための提言を行っていく。

一つ目にスマートフォンの情報を報道機関が今以上に利用者に対して告知することが重要であると考えられる。例えば、テレビのニュース番組や新聞の朝刊などでＯＳのアップデート情報などを目に付くところに掲載することによってアップデートを促すことなどが有効ではないだろうか。

このような手法を取ることによって、普段スマートフォンなどのデジタル製品の情報を集めない人々に対して情報を提供することが出来るのではないだろうか。また、この手法によって世代間のデジタルデバイド（情報格差）を減らすことが出来るのではないかと考えられる。

二つ目に未成年者に対するスマートフォン等のデジタル製品や情報リテラシーに対しての教育をさらに行うべきではないか。現在でも注意喚起等は行われているようではあるが、今後スマートフォンのような端末がより身近に生活に密接になると考えられるが、現状ではこのような時代に向けての教育が足りないと感じる。そのため、教育機関では情報を扱う授業を現在より増やすべきではないだろうか。

現在、小学生からスマートフォンを持つことも増えているので、早いうちから教育を行い、情報リテラシーを養うことが必要だと考える。また、そうすることによって、インターネットで犯罪被害に会う可能性を少しでも減らせるのではないだろうか。

三つ目に「ＳＴＯＰ（立ち止まって理解する）」「ＴＨＩＮＫ（何が起こるか考える）」「ＣＯＮＮＥＣＴ（安心してインターネットを楽しむ）」という考え方を日本でも普及させることである。これは米国のＡＰＷＧ（Anti-Phishing Working Group）とＮＣＳＡ（National Cyber Security Alliance）が共同で行っているインターネットを安全に使うための消費者向けセキュリティ普及啓発キャンペーンである[16]。

このキャンペーンではウェブサイト等にアクセスする前に「ちょっと立ち止まって、（例えば、そのウェブサイトにアクセスすることで）何が起こるか考える」意識を持つように呼びかけている。この考え方を普及させることによってインターネット上で犯罪に会う可能性を減らせるのではないだろうか。

最後に、不正アクセス等に対する厳罰化を進めることによってスマートフォン等での被害をなるべく減らすべきである。現在の不正アクセス禁止法では罰則は三年以下の懲役又は百万円以下の罰金となっており、厳罰とは言えないだろう。そのため厳罰化によって被害を抑止し、被害者を減らすべきである。

海外からの攻撃に対しては、対処が難しい場合が多いと考えられるので、前述したとおりマスコミの報道等で情報の共有等を徹底して行っていくべきである。

参考文献・参考資料

・岡崎裕史　『個人情報ダダ漏れです!』（光文社新書、二〇一三年）
・総務省　『電気通信サービスＱ＆Ａ』
http://www.soumu.go.jp/main_sosiki/joho_tsusin/d_faq/index.html

・警視庁　『スマートフォンを利用してる方へ』
http://www.keishicho.metro.tokyo.jp/haiteku/haiteku/haiteku414.htm
・独立行政法人情報処理推進機構セキュリティセンター　『対策のしおり』
http://www.ipa.go.jp/security/antivirus/shiori.html

注

1　総務省　『スマートフォンとはなんですか?』
http://www.soumu.go.jp/main_sosiki/joho_tsusin/d_faq/faq01.html
2　大和総研グループ　『スマホの正確な普及率は?』
http://www.dir.co.jp/library/column/20140522_008534.html
3　ICT 総研　二〇一四年度　タブレット端末市場に関する需要動向調査
http://www.ictr.co.jp/report/20140528000061.html
4　マイナビニュース　『未成年者のスマホ所有率、小学生は三八%、中学生は五五%、高校生は八八%に』
http://news.mynavi.jp/news/2014/03/11/132/
5　独立行政法人情報処理推進機構セキュリティセンター　『スマートフォンのセキュリティ<危険回避>対策のしおり』
http://www.ipa.go.jp/security/antivirus/documents/08_smartphone.pdf
6　独立行政法人情報処理推進機構セキュリティセンター　『Android　OS を標的としたウイルスに関する注意喚起』
https://www.ipa.go.jp/security/topics/alert20110121.html
7　Business　Media　誠　『金銭被害も：横行する L-2E サギ、あなたは大丈夫?』
http://bizmakoto.jp/makoto/articles/1407/03/news035.html
8　INTERNET　Watch　『ファイルの身代金を要求するランサムウェア、日本語で脅迫する亜種を確認』

http://internet.watch.impress.co.jp/docs/news/20140328_641886.html
9　読売新聞（ＹＯＭＩＵＲＩ　ＯＮＬＩＮＥ）『あなたのスマホが危ない！不正アプリ最新事情』
http://www.yomiuri.co.jp/it/security/goshinjyutsu/20140808-OYT8T50233.html
10　読売新聞（ＹＯＭＩＵＲＩ　ＯＮＬＩＮＥ）『あなたのスマホが危ない！不正アプリ最新事情』
http://www.yomiuri.co.jp/it/security/goshinjyutsu/20140808-OYT8T50233.html
11　岡崎裕史　『個人情報ダダ漏れです！』（光文社新書、二〇一三年）七四～八一Ｐ
12　独立行政法人情報処理推進機構セキュリティセンター　『スマートフォンセキュリティく危険回避＞対策のしおり
http://www.ipa.go.jp/security/antivirus/documents/08_smartphone.pdf
13　TrendLabd　SECURITY　BLOG　『正規マーケット「Google　Play」上で公開されていた「偽 Flash Player」の正体は？』
http://blog.trendmicro.co.jp/archives/7825
14　ＭＳＮ 産経ニュース　『Android（ＴＭ）搭載端末を標的にした偽セキュリティーアプリ詐欺が登場』
http://sankei.jp.msn.com/economy/news/140410/prl1404101638010３-n1.htm
15　マイナビニュース　『もしも、スマホを失くしたら？：iPhone、Android それぞれのアプローチ』
http://news.mynavi.jp/articles/2013/04/05/icloud/
16　フィッシング対策協議会　『STOP.THINK.CONNECT.とは』
https://www.antiphishing.jp/pdf/about_StopThinkConnect.pdf

ＬＩＮＥの恐怖と対策予防方法

警察官（兵庫県）
淵﨑　和樹（29）

一　はじめに

近年、パソコンが一家に一台というくらい普及しており、パソコンがない生活は考えられないものになりました。パソコンには、様々な使用用途がありますが、老若男女を問わず使用していると言えば、やはり、インターネットではないでしょうか。とても便利で、インターネットを使用すれば、素早く様々な情

報が得られ、その情報を世界中の皆で共有できるようになっています。

更に、近年では、携帯電話、スマートフォンが社会全体に大変普及しており、これらは、一人に一台というのが当たり前の時代になってきています。特にスマートフォンの普及は目覚ましく、最近では、昔の携帯電話、所謂、ガラケーを見る機会もすっかり減ってしまいました。スマートフォンの爆発的ヒットの一つの理由に、インターネットが手軽に使用出来ることが挙げられると思います。これにより、更に、インターネットを使用する人口が増えたのではないかと考えます。

私達が、子供の時には考えられないものが今では常識になっています。その一つがインターネットなのです。

しかし、一方で、この便利さにつけ込んで様々な問題や犯罪が増加しています。

・　ウィルスによる個人情報等の流出
・　インターネットバンキングへの不正アクセス等による不正送金
・　掲示板などによる、個人への誹謗中傷、薬物等の販売
・　ネット上へのわいせつ画像、児童ポルノ画像等の流出

等の様々な問題が発生しており、その内容は、年々巧妙化、加害、被害者の若年化等があります。

私は、ネット社会における様々な問題や犯罪の中で、携帯電話、スマートフォンはもちろんのこと、パソコンでも使用出来るアプリケーションである「ＬＩＮＥ」についてお話したいと思います。

二　ＬＩＮＥ

まず、「ＬＩＮＥ」の説明からします。ＬＩＮＥとは、韓国最大のＩＴ企業「ＮＨＮ」の日本法人「ＬＩＮＥ株式会社」が提供しているスマートフォン（ｉＰｈｏｎｅやＡｎｄｒｏｉｄ）、ガラパゴス携帯電話、パソコンに対応したコミュニケーションアプリケーションです。特に、スマートフォンでのＬＩＮＥは、若者を中心に大人気です。人気の秘密は、無料で電話（スマートフォン等パケット通信料定額制契約時に限る）やＴＡＬＫ等が出来ることであります。ＬＩＮＥをインストールさえすれば無料通話が出来るのです。今まで電話には必ず、通話料金というものが付きものでした。

しかし、これにより現代の中高生は、ＬＩＮＥ電話以外は使わない子達もいるそうです。更に、複数の友人と一つのグループとしてＴＡＬＫが出来ることや、文字を送らなくても喜怒哀楽などの感情表現をスタンプという機能で返事が出来ることも人気の一つだと思います。

また、自分のスマートフォン内のアドレス帳に登録している人がＬＩＮＥを使い出した場合、すぐに検索出来たり、相手に自分がＬＩＮＥを使用していることが表示されたりするのです。登録方法も簡単で、アプリケーションをインストールした後、メールアドレスとパスワードを設定するだけですぐに簡単に登録が出来て、自分のアカウントが作成出来ます、こう聞くと、便利で身近で良いことだらけの気がします。

しかし、その便利さや身近さゆえに、現在ＬＩＮＥを使用した問題や犯罪が増加しています。特に、

中高生系や若い女性が被害者となる犯罪が多発しています。

三　ＬＩＮＥを使ったいじめやＬＩＮＥを使ったストーカー問題

まず、ＬＩＮＥは、従来私達が使用していたメールと違ってＴＡＬＫと呼ばれるチャット形式のメッセージのやり取りが出来ます。メールと違い、チヤット形式なので、実際に話をしているような感覚になります。更に、メッセージは自分が消去しない限りは消えないので、前からのやり取りがすぐに確認出来るのです。中々忙しく返事が出来ない時でもメッセージを確認すると相手側には既読と表示され、メッセージを確認出来ていることが伝わるのです。

私達社会人にとっては、とても便利な機能であると感じます。しかし、この機能により、いじめやストーカー事案が発生してしまっているのです。一体、どのようなことでいじめ等に発展していくのかを説明すると

・　メッセージを送って既読になっているのに、返事が返ってこない
・　メッセージを送っても中々既読にならない

等です。この行為は、既読無視と呼ばれています。他にも理由はあると思いますが、主にこの二つのことが原因で、いじめやストーカー事案に発展するといつたケースが多いようです。

例えば、中高生の間では、ＬＩＮＥのグループＴＡＬＫ中に、既読無視をきっかけに仲間外れにされて、いじめを受けるようになったというケースです。いじめを受ける様になってからは、グループ内に登

録されていた人は皆グループを抜け、自分だけが残ってしまい、自分を抜いた新しいグループが出来て、そこで新たにＴＡＬＫがされているといったいじめに発展するのです。ストーカー事案の場合では、元交際相手から復縁を迫って来る等、連絡がしつこくくることから、段々と無視をするようになっていくケースです。すると、相手が逆上して内容がエスカレートしたり、事件にまで発展してしまったという事案もあり、実際に逮捕者も出ています。最悪の場合、相手を死に追い込んでしまう場合もあります。現実世界で発生しているいじめとは違い、ネットの中でのいじめであることから、している本人の罪悪感は薄く、また、発覚するのが難しいのが現状です。

四　ＩＤ交換掲示板

次に、最近、新たな出会い系サイトの形態として、ＬＩＮＥＩＤを貼り付ける掲示板が急増しています。ＬＩＮＥＩＤというのは、メールアドレスみたいなもので、個人を識別する重要なものとなります。友達にＩＤを教えれば、ＬＩＮＥ内でＩＤ検索を掛けることが出来るのですぐに友達を見つけることが出来るのです。例えば、友達と電話して長電話になりそうなのでＬＩＮＥの無料電話を使用することとします。その時にＩＤを教えてもらえれば、簡単に検索が出来てとても便利なのです。

しかし、そのＩＤは先程も言いましたが、メールアドレスと同じ意味を持つものなのです。

最近、ＬＩＮＥＩＤを掲示板に貼り付けるとそのサイトを見て気に入った人がいればＩＤ検索をして見知らぬ人と知り合えるといったサイトが急増しているのです。

掲示板は、ＬＩＮＥＩＤ以外にも、簡単なプロフィールや写真、相手を誘うようなコメントが書き込まれており、掲載されているＩＤを検索し連絡すると、見知らぬ人と簡単に連絡が取れるといった仕組みになっています。

このようなサイトは、ＩＤ交換掲示板と呼ばれており、新たな出会い系サイトとして危惧されています。特に、未成年や学生が、そういったサイトに知り合いを増やしたい、異性と出会いたい等安易な気持ちでＬＩＮＥＩＤを掲載し、異性と知り合い、被害にあうといったケースが多発しているのです。

初めは、相手もメッセージや電話などで連絡を取り合っていますが、お互いの距離が縮まってきたところで、会ってみようと次第に話がエスカレートしだします。そして、いざ会ってみると、プロフィールの人とは全然違う人だったり、最悪の場合、児童ポルノや、児童買春、強姦等の被害児童となってしまうのです。このような話をすると、一見被害者は女子ばかりの話に聞こえますが、被害者は、女子ばかりでなく男子児童でも発生しています。また、福祉犯罪以外にも多数の犯罪に巻き込まれていくケースが発生しているのです。

更に、ＬＩＮＥＩＤは、自分で決められることから、簡単なＩＤに設定していると、適当に検索してもヒットしてしまう可能性もあり、見知らぬ人から突然連絡が来ることもあるのでそのことを踏まえＩＤを設定しなければなりません。

五　ラインによるなりすまし行為

ＬＩＮＥは、メールアドレスと自分が決めたパスワードさえあれば簡単にアカウントが作成出来ると説明しました。そのパスワードと、先程出てきたＬＩＮＥＩＤとを同じものに設定している人が意外と多いのです。すると一体どのような被害や犯罪に巻き込まれる可能性があるのでしょうか。

ＬＩＮＥは普段、一度ログインすると自分でログアウトにしない限り自動ログインする仕組みになっています。一度ログアウトをしてしまうと、再度ＬＩＮＥを使用するにはメールアドレスと自分で決めたパスワードを入力しログインする必要があります。そして、この時に、他人のメールアドレスを入力し、その人が、パスワードとＬＩＮＥＩＤとを一緒にしている場合、ＬＩＮＥＩＤをパスワードとして入力すれば、他人のＬＩＮＥ内に不正アクセスをして、なりすましが出来てしまうのです。この行為は、不正アクセス行為の禁止等に関する法律として犯罪となるのです。最近、ｍｉｘｉ等から情報が漏れてしまい、その時のＬＩＮＥパスワードやＬＩＮＥＩＤとＬＩＮＥを同じに設定していたことから不正アクセスされたケースもあるのです。一度入り込み、そこから、新しいパスワードを設定してしまえば、元の利用者は、ＬＩＮＥが使用出来なくなってしまいます。この行為は、電磁的記録不正作出、供用となり、もちろん犯罪です。

そして、元の利用者が知らない間に、友人等に勝手に連絡されてしまい、トラブルに発展することや、そこから個人情報を入手されるといったケースもあるのです。

このように自分が知らない間に犯罪に巻き込まれてしまっているという被害が多発しているのです。

六　ＬＩＮＥの乗っ取り

次は、テレビや新聞等でも出ていた、所謂ＬＩＮＥの乗っ取りについてです。芸能人等も同様の被害を複数人が訴え、大変話題になりました。これは、他人のＬＩＮＥに不正アクセスし、利用者になりすまし、友人や家族等にスマートフォン等で使用するウェブマネーを買うように指示し、そのお金を騙し取るといった詐欺の手口です。

ウェブフネーとは、コンビニやネットで購入可能な電子マネーのことを言います。購入後、購入者のみが確認出来るパスワードをスマートフォンに読み込ませると、購入分の音楽がダウンロード出来たり、スマートフォン等で利用できるＳＮＳ等のゲームで課金出来るといった仕組みになっています。

一体、どのような手口になっているのかを説明します。まず、「今大丈夫ですか?」などの連絡が入ります。これに対して返事をすると、助けて欲しいという名目により、コンビニ等で販売しているウェブマネーを購入して欲しいと頼まれます。ウェブマネーの値段は様々ですが、一番高価なもので約三万円します。

欺されて購入してしまい、その旨を連絡すると、購人後に確認出来るパスワードを写真に撮り送って欲しいと頼まれます。そして、そのパスワードを写した画像を送ると、相手側が勝手にパスワードをスマートフォンに読み込ませ、ウェブマネーを騙し取られてしまいます。そして、最後には連絡が取れなくなる

といった手口です。

送られて来た側は、まさか、ＬＩＮＥが不正アクセスされて何者かに乗っ取られてるとは思いもよらないことから、友人や親族の一大事と思い、ウェブマネーを購入し、指示通りの動きをして、最終的にお金を騙し取られるのです。

振り込め詐欺の様に一度に、多額の金額は騙し取られませんが、ＬＩＮＥを使用しているので一度に多数の人に同じような内容で連絡が出来ます。その内の誰かが引っかかってくれれば良いという方法なのです。

このように、簡単に挙げただけでも、様々な問題や、犯罪に巻き込まれる可能性があることが分かっていただけたと思います。とても便利なだけに、リスクも多数あり、その事実を知っているか知らないでは大きな違いがあるのです。

七　ネットでの注意方策三つのポイント

では、どのようなことに注意していけば良いのでしょう。

私は、もっと皆がネット等に対する正しい知識を身に付けることが一番大切だと思います。現在の私達は、ネット等の便利さばかりに目が行ってしまい、デメリットやリスクといった部分はあまり気にしていないのが現状です。子供がいる保護者は、子供にその知識を正しく理解させる必要があると思います。保護者でもまだ、インターネット等に対しては苦手意識を持たれている方が大勢いると思います。しかし、

現在この情報社会において、インクーネット等を切り離した生活などはもはや考えられないはずです。まずは、学ぼうとする意識改革が必要です。よって、苦手意識を払拭して、子供のため、自分のために正しい知識を身に付けるべきです。そして、子供に正しい知識を身に付けさせれば良いのです。保護者が、注意して、子供たちが知らないうちに被害にあっていたということを防がなければならないと思います。

私は、ネット等に対して保護者が子供のために出来ることとして三つのポイントを挙げたいと思います。

まず、一つ目は「正しくインターネットを利用させる」です。現代社会でインターネット等を利用せずに生活することはもはやありえません。子供達は次第に興味を持ち始め、利用し始めます。そのために、それまでに保護者がしっかりと勉強をし、興味を持ち始める前から少しずつ子供に教えることが大切です。初めがとても肝心です。子供が成長しインターネットに対する知識、技術、モラル等が理解出来始めたら利用できる範囲を少しずつ広げていくようにすれば良いのです。

二つめは「家庭内にルールを作る」です。

子供だけでは利用させない。万が一トラブルに巻き込まれそうになった時はすぐに両親に相談する、ルールを破ったら一定期間使用禁止等、家庭内で独自のルールを作り、それを当たり前にすることが大切です。この時、保護者だけが勝手にルールを作るのではなく、子供と一緒に話し合いながら考えていくことが大切です。一緒に考えたことなら子供とのトラブルも少なくて済むし、何より、子供たちがそれを守るという意識を植え付けることが大事なのです。

三つめは「子供に持たせる機器にフィルタリング等を設定する」です。

現在、パソコン、スマートフォンを始め、携帯音楽機器や、無線ＬＡＮなどを使用するゲーム機などもインターネットを利用することが可能です。しかし、こういったゲーム機は子供たちが家から持ち出す可能性もあることから親の監視出来ない場所でインターネットを利用する可能性があります。そのため、子供たちに持たせるモバイル機器には、フィルタリング等を設定する必要があります。フィルタリングとは、インターネット上にある性的あるいは反社会的な情報を含んだサービスやサイトを一定の基準に基づいて選別し、子供達が利用する携帯電話やＷＥＢブラウザから閲覧できないようにするシステムを指します。最近では、パソコン以外でもスマートフォンやゲーム機、音楽プレーヤーなどもフィルタリング出来るようです。特に、スマートフォンはネット用のフィルタリングとアプリ専用のフィルタリングをすることによってより安全に使用することが出来るのです。

子供たちが見えないところで問題や被害にあわないためにも保護者が進んで取り組んであげることが大切です。

それは、ＬＩＮＥでも同じことが言えると思います。ＬＩＮＥももちろんインターネットを使用しており、ＬＩＮＥを使って様々な情報を得ることが出来ます。

ＬＩＮＥは、大人から子供まで利用しています。大人は、利用方法、メリット・デメリットに対して、自分で学ぶべきであると思います。しかし、子供は中々すぐに理解は出来ないでしょう。ここでも保護者は、子供のために自分が勉強して正しい使用方法を子供に教えることが大切です。

八　ＬＩＮＥでの注意方策三つのポイント

では、ＬＩＮＥを使用する際に何に気を付けるべきなのか。やはり、私は子供たちに、メリットとデメリットをしっかり説明する必要があると思います。私は、先程のネットと同様ＬＩＮＥでも三つの注意事項を挙げて説明します。

まず、一つめは、インストール時の注意事項です。ＬＩＮＥをインストールし登録を始めるとスマートフォン内のアドレス帳データを送信しますかと出てきます。これは、登録した時に、自動でアドレス帳に登録されておりＬＩＮＥを利用している人を友達という一枠で括ってくれる便利な機能です。しかし、全く知らない人や、不必要な人とも繋がってしまう可能性もあります。例えば、昔の友人の電話番号を現在は見ず知らずの人が使っている場合や、私用のスマートフォンから電話をかけたことがある取引先の人等が挙げられると思います。ＬＩＮＥの登録時、アドレス帳のデータは送信しなくても通常通り登録が出来ます。ですので、わざわざ情報を送る必要はありません。保護者は、子供がＬＩＮＥを使用する際は、その旨をしっかりと伝えましょう。手動で友達を検索していくように勧めていけば、初めは大変かと思いますが、不必要なトラブルに巻き込まれることはありません。更に、ＬＩＮＥの特徴、問題点などをしっかりと説明し、理解させる必要があります。

二つめは、利用時の注意事項です。

ＬＩＮＥの利用を始めてみると、初期設定のままだとアドレス帳に登録されている人でＬＩＮＥを利

用している人は友達枠に自動で登録されてしまいます。更に、自分がアドレス帳から削除していても、相手のアドレス帳に番号の登録が残っていると友達かもという枠に入ってしまい簡単に検索されてしまいます。このような場合、不要なトラブルに巻き込まれる可能性がありえます。ですので、自動で友達枠を追加せずに自分で見て選べる手動にするべきなのです。方法としては設定で「友だち自動追加」機能をオフにすると簡単にできます。

更に、勝手に他人から検索が出来ないようにするには、設定の「友だちへの追加を許可」機能をオフにすれば他人から勝手に友達枠に登録されることはありません。

そして、いつの間にか登録されてしまっている人、連絡したくない人、不必要な連絡ばかり送ってくる人がいると思います。そのような人に対しては、ブロック機能を使用して連絡を遮断してしまえば良いのです。相手に通知が行くわけではないので、自分が不必要と思う人物は気にせずにブロックしていけばよいのです。それがトラブル等から身を守る方法なのです。

最後の三つめは、パスワード関係の注意事項です。

まず、ＬＩＮＥについてですが、ＩＤ交換掲示板等を利用しないためにも、必要な時以外は設定する必要はありません。万が一ＬＩＮＥＩＤを設定する場合は、パスワードとＩＤを同じのに設定せず別のものにすることです。他人からの不正アクセスを防止するためにはパスワードとＩＤを区別して、更に誰でも想定出来てしまうパスワードにはしないことです。しかし、それだけでは、万全ではありません。現在、ＬＩＮＥ一連の乗っ取り事案が多発したため、パスコードと呼ばれる四ケタの番号を設定出来る

様になりました。これにより、何者かが、不正にアクセスしようとメールアドレスとパスワードを入力しても、更にパスコードを入力しなければ入れなくなりました。この機能を使って不正アクセス、なりすまし防止に努めて下さい。

また、親子で時々状況を確認し、少しでも疑問に思うことは相談出来る環境作りに努めていれば、いざという時に出遅れることなくすぐに対応出来ると思います。

九　終わりに

現在社会においてインターネットは切り離せない存在です。今回私が題材にしたＬＩＮＥというアプリケーションももちろんインターネットを使用するもので切り離せない存在になりつつあります。しかし、身近さと便利さがあるからこそ、それを利用した問題や犯罪が多発します。その状況等に大人や保護者が敏感に反応し、恐ろしさを子供たちに伝えることで、ずいぶん犯罪は予防されると思います。姿が見えないネット社会だからこそ、一歩間違えれば大きな問題に発展し、最悪の場合は、犯罪者になってしまったり、犯罪の被害者となってしまうのです。正しく安全に利用することで子供たちは守られていくのです。

ネットの怖さについて子供たちは、すぐに理解出来ないと思います。大人でも難しいと思います。しかし、それを見過ごせば防げたはずの犯罪やトラブルに巻き込まれていくのです。時間をかけてゆっくり理解を深め、徐々に出来る範囲を広げていってあげることが大切です。

ネット社会を安全に暮らすために、私は、大人や保護者が逃げずにしっかりとネットに対しての勉強を

して、子供たちに正しい知識を伝えていくことが大切だと思います。無知な子供たちが不必要なトラブルや犯罪に巻き込まれないためにも、ネットに対する苦手意識を払拭して学ぼうとする姿勢が、安全に暮らしていける第一歩であると考えます。

人間に優しいネット社会を作るために

会社員
（京都新聞社文化部専門記者）
森田　信明（64）

〈はじめに　―まだ未成熟な技術―〉

誰もがどこからでも瞬時に、自分の言葉や画像を世界へ発信できるようになり、かつて夢だったテレビ電話も簡単に可能になった。インターネット（ネット）は私たちの生活に革命的な変化をもたらした。何よりも重要なのは、誰もが情報の発信者になり得たことだ。国民が自由な発信や交流手段を得たことで、

「アラブの春」のように政治の民主化を進める大きな力にもなっている。

だが、一方でネットは多くの犯罪の媒介役になっている。Facebookや Twitter、ＬＩＮＥなど、種類も利用も増えたＳＮＳ（ソーシャル・ネットワーキング・サービス、会員制交流サイト）が悪用され、子どもたちが被害に遇う性的事件やいじめ、詐欺などの事件が後を絶たない。それがきっけになった悲惨な殺人事件も相次いでいる。不正アクセスによる預金の不正引き出しや、公共機関や企業のデータを盗み出す事件も頻発している。警察庁によると、サイバー犯罪の平成二五年の検挙件数は八、一一三件にのぼる（①）。水面下にはさらに多くの被害が潜んでいるだろう。

ネットはそういう明と暗の両面の顔を持ったツール（道具）なのだ。メリットが大きい半面、大きなマイナス面も抱えている。

軍事用に開発されたインターネット技術がビジネスに開放されたのは一九九〇年代だ。基本ＯＳのWindows95が発売され、「インターネット元年」と言われる一九九五年から二〇年程度しかたっていない。大きな「暗」の側面を残しているのは、まだ未成熟な技術である証明だろう。

サイバー犯罪の防止策を考えることは、未成熟なネット世界をより人間に優しいものに、どう発展させていくのか、を考えることでもある。

ネットの事件、事故を防ぐためには利用者が学ぶべきだ、とよく言われるが、問題は利用者だけでなく、ツール（パソコン、スマートフォンなどの機器やソフト）や社会のルール・制度の側にもたくさんある。三つ側面のすべてから取り組まないと効果のある対策にはならない。交通事故の防止には、利用者（運転

者、歩行者）、ツール＝自動車、ルール＝交通規則や道路整備―の三つ側面からの総合的な対策が必要なのと同じだ。

（Ⅰ）サイバー空間が持つ四つの問題点

対策を考える前に、ネット世界の持つ四つの問題点を点検しておきたい。高速で走る自動車が人間に大きな負荷を与える（事故が起きれば悲惨な結果を招き、運転にも緊張を強いる）ように、ネットも利便性の一方で人間の感覚や生活に大きな違和感や負担をもたらしており、その「壁」がさまざまな事故や事件の背景になっている。高速走行の危険性を知っているから安全対策ができるのと同じように、まずネットの問題点を掘り下げておこう。

（一）現実世界との落差

ネットが瞬時に距離を超えられるのはデータを極限まで単純化しているからだ。メールやＳＮＳは文字や画像だけ、つまり五感のほんの一部だけを伝えている。現実＝リアルの世界で人間同士が話す時は、相手の目や体の動き、喜びなどの表情も伝わる。私たちは多くの要素を伝え、感じ取りながらコミュニケーションしている。だから文字や画像だけが行き交うＳＮＳはあくまでも疑似的な交流や出会いでしかない。

ネットで得られる情報も同じだ。検索サイトを通じてホームページやブログなどから得られるのは、誰かが目的を持って公開した情報で、誤っていたり、古かったり、偏った、利益だけを狙った内容も多い。

京都大学の新総長に就任した霊長類学者の山極寿一氏は近著「『サル化』する人間社会」で、人間と最も近い同じ霊長類のゴリラの生態を例にとりながら、ネットのコミュニケーションが人間本来のものとは異質で、危険だ、と警鐘を鳴らしている。

人間と同じように家族を大切にするゴリラは、フェイス・トゥ・フェイスで顔を見合わせて相手の気持ちを理解し合い、競争による敗者をつくらず互いに共存して暮らしている。まるで牧歌的な時代の人間のような生活を送っている。群れで権力構造をつくって暮らすサルとはまったく違う。

人間も本来、ゴリラと同じようなフェイス・トゥ・フェイスで理解し合う生態を持っているが、ネットの世界はそれと相容れない原理で作られている、と山極氏は指摘する。

著書では「人間は、生身の体をなかなか乗り越えられないものです。生物学的な心が常に基盤にあり、昔からその部分はあまり変化していません」「私たちは言葉を使い、あるいはインターネット技術を使い、情報交換しているような気になっていますが、もっとも重要な情報は対面した相手の目を通して得られるはずです。人間は相手の言っていることだけでなく、その態度、顔、表情や目の動きから相手の性格をつかみ、評価をします」と書く（②）。コミュニケーションとはそれくらい全人的なものなのだという。だから山極氏は今も、携帯電話を持たないアナログ派で通している。

「『サル化』する―」には、コミュニケーションとは何かを考えさせる、楽しいエピソードが登場する。

若い時、ゴリラの調査でアフリカの森林地帯に滞在した際、洞穴で雨宿りをしていると、「タイアス」と名付けた子どものゴリラも雨宿りに来て氏をじっと見つめた。敵意がないのを感じ取ると一緒に洞穴に入り、氏の膝に乗りかかって寝込んでしまった。

研究を終えて帰国して二六年後、氏は再びその森に行った。年老いたタイアスと再会したとき、最初は誰なのか理解してもらえなかったが、氏がゴリラの挨拶の声を真似ると、タイアスの目は輝き、子どものような表情に戻った。氏を覚えていた。そして、かつてやっていたのと同じように、子どものゴリラと一緒に取っ組み合いを始めた。昔は楽しかったなー。タイアスがそういう気持ちを伝えているのが分かった。

四半世紀たっても忘れない、魂の通い合うコミュニケーションができるのがゴリラや人間なのだという。そう思うと、メールの薄っぺらなやり取りで何が伝わるのか―という気持ちになる。顔を見合わせる人間本来のコミュニケーションをもっと大切にしたい。

氏の話はネットの「虚」の世界に浸ることへの警告だが、なぜＳＮＳを通じた「出会い」で子どもや若者たちが騙されて被害に遭うのか、という背景の分析にもつながっている。加害者たちは相手に正しく理解されないからこそ、自分の意図を隠して巧みに騙せるのだ。

（二）孤立化の危険性

インターネットの欠陥とも言える特徴は、一人で孤立して操作することだ。何をしているか周囲からは分からない。孤立していることは助ける人間もなく、加害者には格好の空間になる。ＳＮＳで子どもた

ちが相手の誘いや恫喝に驚くほど無防備に応じてしまう理由がここにある。

見られていないことは攻撃する側を大胆にする。和田伸一郎・中部大准教授（メディア論）は著書で、二〇〇四年に起きたイラクで日本人のフリージャーナリストらが人質になった事件の際、ネットで「自業自得」とバッシングが浴びせられたことについて、無責任に誹謗中傷できるのは「ネットのバーチャルな空間と〈繋がった〉〈個室〉に退きこもることによってであり」「世界へと姿を現すことなく、臆病なやり方で悪を犯すことができるという側面である」（③）と、ネット社会の特性を分析している。

孤立し、隠された「個室」が犯罪や攻撃を生む空間にもなっているわけだ。

関連して知っておきたいことがある。口汚い罵りや悪意に満ちたデマ、悪質な個人情報の暴露、民族差別…と、ネットの掲示板やＳＮＳの世界をのぞくと、汚く、悪意に満ちた言葉が飛び交っている。表現の自由は最も尊重されなければならない権利の一つだが、飛び交う言葉はそれとは無縁のものだ。人から見られる恐れがないことが強い攻撃性を生んでいる、と心理学者は分析する。ネット空間は危険な心理的世界を生んでいる。

（三）ネット依存の罠

「インターネットを長時間使用し、やめられなくなった状態」が「ネット依存症」と呼ばれている（④）。文科省による平成二六年度の小中学生の学力テストの際に行われた携帯電話やスマートフォンの利用状況調査で、子どもたちの過剰なネット使用を示すデータが明らかになった。多くの子どもたちが「ネット依

存」、あるいはそれが疑われるような状態に陥っていた。

携帯電話やスマホで一日二時間以上、通話やメール、インターネットを行っている子どもの割合が中学生で三四・九％、小学生でも三〇・一％を占めており、四時間以上使っている子どもも中学生で一〇・八％、小学生で八・八％いた。ぞっとする数字だ。数字は年を追って増え続けている。

学力に影響しないわけがない。携帯・スマホを使っている時間の長さに応じて学力テストの成績は悪くなり、四時間以上使っている子どもと三〇分未満の子どもでは中学生の数学Ａの平均点（一〇〇点満点）で実に一七・〇点、小学生の算数Ａでも一三・二点の差があった。他の教科も使用時間が増えるのに比例して平均点が落ちていた。

また総務省が行った平成二六年度の高校一年生への調査では、スマホの使用が一日三時間を超える生徒が平日で三四・一％、休日では五〇・三％、五時間を超す生徒も平日で一二・五％、休日で二二・〇％にのぼった（⑤）。

国立病院機構久里浜医療センターの樋口進院長によると、ネット依存は感情が制御できない、思考力の低下など心身に深刻な影響を与える（⑥）。ネット依存の傾向は危機的な水準に達しており、子どもたち自身はもちろん、社会の未来も危うくしている。

ネット依存がもたらすひずみは大人の世界でも目立つ。最近同じテーブルに座りながら話もせず、別々にスマホの画面を見つめている不思議な若者たちをよく見かける。広い意味でのネット依存がもたらしたコミュニケーション不全の一つの現象だろう。

理化学研究所のＳＴＡＰ細胞をめぐる論文不正問題でクローズアップされた「コピペ（コピー・アンド・ペースト）」と呼ばれる他人の文章の盗用の横行も、ネット検索で手軽に他人の文章が調べられるようになったことが生んだ、ネット依存の現象の一つだろう。

大学では学生のコピペが横行しコピペ判定ソフトまで登場しているが、嘆かわしいことに新聞記者らのコピペ盗作も近年、相次いで発覚している。

下手でもいいから、自分の力で調べて考え表現するところから知的作業が始まる。だがネットは過去の資料を簡単に見やすくし、こういうプロセスを省略し「手抜き」しようと誘う副作用を持っている。ネット依存は知的能力を低下させるとともに、社会の基本的なモラルさえ揺るがしている。

（四）利益主義の構造

インターネット文化を特徴づけているのは、Google などの検索サイトや Facebook などのＳＮＳが、多くが米国発で、いずれも巧みな収益構造を持ち若い開発者たちが巨万の富を築いていることだ。いずれも随所に広告を掲示して閲覧や広告のクリック数に応じて収益が増える仕組みになっている。

検索サイトでは検索に合わせて関連広告が掲示され、クリックが増えやすい構造を作っている。利用者が見てくれれば収益が増えるため、検索サイトやＳＮＳは利用者を引き寄せる工夫を凝らしている。ネット依存には、強められたソフトの吸引力も大きく影響していることを知っておきたい。

精神科医の香山リカ氏は近著で、「依存性の高い製品を生みだすことができる企業だけが〝帝国〟とし

て急成長できる」というアップル社元幹部の言葉を引用し、ＳＮＳを「『餌付け』の仕組みを作ってユーザーを依存症にするビジネスモデル」（⑦）と指摘している。

誰もが改良可能なオープンソースのＯＳであるLinuxのような例もある。コンピューターソフトの公益性やコンピューター文化の発展を考えると、収益性に偏った形以外のソフトがあってもおかしくはない。将来はそういう方向に進む、と指摘する評論家もいる（⑧）。そういう目で、現在のネット文化を過渡的なもの、と批判的に見る視点も持っておきたい。

（Ⅱ）三つの側面からの対策

（一）利用者の対策

（ア）依存からの脱却

求められているのは、子どもに限らず大人も含めてネット世界と距離を置き冷静に活用する力を持つことだ。「情報リテラシー」（情報活用能力）という言葉もある。それを身に付けるために、まずスマホを手放す時間を増やすこと。そして現実＝リアルの世界で行動し家族や友人と対話しよう。リアルの世界の方がはるかに楽しい発見や出会いがあることに気付くはずだ。

子どもたちへの対策は、石川県が二〇〇九年に「携帯電話を持たせないようにする」という条例を制定するなど、条例で小中学生の携帯電話やスマホの利用を規制する自治体が増えている。

いずれも処罰のない努力規定で、石川県がそれで携帯電話の所持率を極端に下げられているわけではないが、親や子どもたちに携帯やスマホ利用のマイナス面や危険性を考えさせ、自分から所持をやめたり、使用を控えたりすることにつながる効果は大きい。

実際、私権の極端な制限は慎重であるべきだし、外部から強制して持たせないことが望ましいかは疑問だろう。「決められているから持たない」という他人任せの判断では限界がある。大学生や社会人になってから依存が始まるだけでは仕方がない。子どもたちが自ら危険性を理解し、距離を置いて使える力を身に付けるようになることこそ望ましい。

条例はその動機付けに活用する、と考えた方がいい。条例化しなくても、学校や地域で自主的に携帯、スマホの「追放」や「制限」に取り組む方法もあるだろう。

子どもたちが携帯やスマホを所持する場合、有害情報へアクセスできないフィルタリング機能は必須だ。二〇〇九年に青少年インターネット環境整備法が制定され、一八歳未満の子どもたちが使用する携帯には事業者がフィルタリングを提供することが義務化されたが、保護者の申請があれば解除できる。WiFi機能を用いるスマホは、事業者がフィルタリング機能の設置を推奨する形になっている。いずれにせよ、最後は本人と家族の判断だ。

平成二五年度の内閣府の調査では、携帯電話、スマホにフィルタリングを取り付けているのは小学生で六二・二%、中学生で六一・一%、高校生で四九・三%にとどまっていた（⑨）。本人や親の危険性の認識がまだ薄いことの表れだろう。

警察庁の調査で、出会い系サイトやコミュニティサイトを通じて犯罪に遭った一八歳未満の子どもたちの九四・五％、つまりほとんどがフィルタリングを用いていなかった（⑩）。フィルタリングの必要性と有効性を何よりも明白に示すデータだ。

神奈川、静岡県などのように子どもの携帯のフィルタリングを外す際、条例で保護者の書面による申請を義務化した自治体や、福岡県のように条例でスマホの推奨されるフィルタリングを示す自治体もある。冷静に考えると分かるが、フィルタリングがあって子どもたちの一般的な携帯やスマホ利用にどれほど支障があるのだろうか。用いなかった際の危険を考えると、フィルタリングは解除できない完全な義務化に変えるべきだろう。犯罪被害に遇いやすいという危険性を軽く見てはならない。

スマホのテレビＣＭが多いが、その際「一八歳未満はフィルタリング利用が義務づけられている」とテロップなどで呼び掛けるのも効果的だろう。

長く子どものネット利用問題と取り組んでいる下田博次・群馬大名誉教授は著書で、子どもたちが携帯電話でネット利用して起きた犯罪被害や非行の例を挙げ、国や業界の無策の責任を追及している（⑪）。だが電車の中や歩きながらスマホに熱中するなど、多くの大人たちがネット依存に近い状態に陥っていて、子どもだけに「持つな」「見るな」と言っても効果が薄いし、不毛だ。大人にこそスマホのリテラシー教育が必要な面がある。

子どもも大人も含めて生活の中で自然や人と向き合い、リアルの世界の方が面白いと感じてネットから距離を置くようになるのが最も望ましい。これまでのＩＴ教育はＩＴ技術を「習う」「覚える」という

受け身の技術教育が中心だったが、ＩＴに潜む危険性と、距離を置いて使うことを教える逆説的な「ＩＴ教育」が必要になっている。

思想家の東浩紀氏は近著で、ネットの網の目から逃れ自分の頭で考えるために旅に出て場所を変えることを勧め、自ら実行している。「ネットを触っているかぎり、他者の規定した世界でしかものを考えられない。そういう世界になりつつあります」「ネットにはノイズがない。だからリアルでノイズを入れる」(⑫)という言葉は、示唆に富んでいる。

（イ）基本の徹底

今年七月に発覚したベネッセコーポレーションの顧客名簿流出事件は、業務委託したデータベースの保守・管理会社のＳＥ（システムエンジニア）が金銭に困り、セキュリティーの設定対象外だったスマホにデータ複写が可能なことを発見して繰り返し犯行に及んだ。顧客データの管理体制に甘さがあったとしか言いようがない。

だが、さまざまなサイバー犯罪や事故の多くも、実は人間のミスや不注意が絡んで起きている。

サイバーセキュリティーと経営戦略研究会編「サイバーセキュリティー」で、門林雄基・奈良先端科学技術大学院准教授は「サイバースペースで起きている事故のほとんどは紛争などではなく、事業者の不注意やリスク認識の欠如、プログラムのミス、利用者の不注意などに由来するものである」(⑬)と指摘している。

コンピューターセキュリティーの情報収集に当たる社団法人ＪＰＣＲＴ／ＣＣが対応した事故の内訳

を調べると、七割がウェブサイトの管理不行き届きによるもので、技術的に高度なものは五％にも満たなかった。また、独立行政法人・情報推進機構（ＩＰＡ）が公開している不正アクセスの届出状況でも、不正アクセスのほとんどがウイルス対策ソフトの使用で防止されていたという（⑭）。

セキュリティーソフトの導入と更新、不審なメールは開けない―など、まずやるべき基本的な安全マニュアルをやり切ることが対策の前提になる。

安全管理で怖いのはベネッセの例で見られるように、実は社員など人の管理だ。社員の個人パソコンがウイルス感染しＵＳＢメモリーや社内メールを介して企業などのシステムにウイルス侵入を許すケースも目立つ。パスワードを知っている元社員によるデータ流出などの犯行も多い。これらは、アクセス権限を持つ人を段階に分け最低限に絞る、退職者が出た場合などはＩＤを変更するなど、セキュリティー管理を的確にすれば防げる。

サイバーテロでよく例に挙げられるイランの核関連施設のコンピューターがサイバー攻撃を受け遠心分離機が停止したのも、汚染されたＵＳＢメモリーを介してウイルスが侵入したといわれている。

だが基本的な安全対策をしっかり行った上に立っても、なお攻撃は完璧には防ぎきれない。人間が考えた技術だから、クリアされる危険性は必ず残る。つまり一〇〇％はない。リスクへの対応能力を上げるために、公的セクター、事業者、ネットやセキュリティー関連事業者らがそれぞれに不断の努力を重ね、連携を図ることが、社会全体のリスク対応能力を上げ最高の防御になるのだと思う。

ベネッセの事件後の会見を見て驚いたのは、「事故」「センシティブな情報ではない」と述べ、顧客に被

害を与えた加害者の立場なのだということやデータ流失の重要性を十分理解していない面があったことだ。認識の誤りこそが業者任せの甘い管理を招いたのではないだろうか。

流失した名簿は売買され拡散する。パスワードのような金銭につながるデータでなければ被害が少ないというのは正しくない。社会にはＤＶの夫やストーカーから逃れて生活する人もいる。流失した名簿により、身元を隠して生活せざるを得ない人たちが被害を受ける恐れもある。適切な対策を怠って情報流失を招いた企業や公的セクターに対する個人情報保護法上の責任を、より厳しく問うことを検討する必要もあるだろう。それが再発防止策になる。

（二）　ツールの対策

（ア）　人間に優しいソフト開発

ソフトも日進月歩だ。一〇年前と現在のパソコンやソフトを比べれば、別世界のように進化している。今後も大きく変わるだろう。それをより人間に優しい形で変えていきたい。

二〇一三年一〇月の女子高校生が殺害された三鷹のストーカー殺人事件など、子どもや若者たちがＳＮＳで出会った相手を誤って信用したために、被害に遇った事件を見ると、なぜそういう事件を防げるようにＳＮＳの仕組みが改良されないのかと疑問を感じる。

周囲が気付かないうちに加害者との接触が生まれ、犯行が急速に進んだ。これが（Ⅱ）で挙げた「孤立

化」がもたらす危険性なのだ。「孤立化」を防ぎ、犯罪を抑止できるようなソフトが求められている。

例えば、ネット上で出会った相手が違法な行為を要求した際、ＳＮＳやメールなら文字で脅迫、要求するわけだから、危険な文言を検知できる。検知したら本人や加害者に警告音を鳴らしたり、家族などに警告メールを送るソフトがあればいいわけだ。意外に簡単にできるのではないだろうか。

京都府立大の吉冨康成教授は、掲示板やＳＮＳに危険な言葉が使われていないかを自動的にチョックするソフトを企業と連携して開発し、それを使って京都の多くの学校の「ネットパトロール」に取り組んでいる。危険な言葉を発見したら教育委員会に報告し、いじめや差別事件、自殺の防止に効果を上げてきた。

ソフトの仕組みはシンプルで、チェックしたい危険な言葉を組み込み、当該学校の関連掲示板やＳＮＳをネットパトロールし、使われている書き込みがあれば自動的に検知する。吉冨教授は編著書で、二〇〇八年の秋葉原事件の際に家族が被害に遭った恐れがあるためネット検索をしていて、加害者の事件前の書き込みを見つけ、ネットパトロールを行えば犯罪予防に生かせることに気付いたと書いている⑮。ソフトの作り方など、他でも参考にできる事例だろう。さまざまな形で行われているサイバーパトロールの効果も物語っている。

ＬＩＮＥなど無料通話アプリの常時接続の問題も早急に対策が必要だ。子どもの利用が多く、ネットの利用時間を極端に長くするだけでなく、常時接続を切ることがいじめの大きな原因にもなっている。土井孝義・筑波大教授は著書で、いじめに結びつく常時接続の「つながり」が子どもたちの心理的なプレシャーになっている、と警告している⑯。子どもたちが使用する場合は、一定時間がたつと切断され

るようなフィルタリングの導入を検討すべきだろう。

一方、高齢社会なのに、現在のネットの世界が高齢者に使いやすいとは誰も思っていないだろう。今後、公共サービスや医療などでネットの活用が進む。高齢者にも使いやすいネットのツールづくりが急務だろう。

ネットの世界はなじみの薄いカタカナや英語が氾濫している。まずは理解しやすく、使いやすいツールがもっと必要だ。その上に立って、間違っても修正が効き、誤って契約したりしないようなソフトも開発が可能だろう。人間工学や行動心理学を活用すれば、人間をサポートするソフトはいろいろできるだろう。SNSの相手の安全性を判断する支援ソフトも可能かもしれない。人間に優しいネット社会になるよう、工夫できることはたくさんある。

日本の自動車や家電製品の長所は使いやすさだった。使いやすさや安全性の工夫こそ日本の得意分野だと思う。

また、プロバイダーなどにログ（通信履歴）の一定期間の保存と、犯罪捜査時の開示を義務付けることも重要だろう。犯行の足跡が残ることは被害者の「孤立化」を防ぐ対策になるとともに、外国のパソコンなども中継して行われる国境を超えたサイバー犯罪への対応能力を高める。

（イ）地域SNSの発展

現実の生活を助けるソフトの開発がもっと必要だろう。政府は地域社会の再生に力を入れているが、ここにSNSが大きな役割を果たせると思う。

Google などの検索ソフトは広い、抽象的な世界を対象としているが、私たちが生活する場所は身近な地域社会だ。地域社会の再生とは、地域の文化や人のつながり、経済などを成熟させることだと思う。ネットはこれを助ける効果的なツールになる。

遠い世界の曖昧な情報で溢れているサイトよりも、身近なことを支援するＳＮＳ。今、そういう地方の個性的な情報ネットワークが、住民や行政が連携して各地で作られている。

情報学者の西垣通・東京大名誉教授は著書で、ネットは地域社会でこそ力を発揮すると強調する。「人間にとって本当に価値（意味）あるものはローカルな場で生まれるのである。なぜなら、人間という生命体にとって価値（意味）とは、本来主観的で多元的なものであり、身近な人々との直接的なコミュニケーションを通じてつくられるからだ。決して、客観的で一元的なものとして天下りに与えられるわけではない」⑰という指摘は、将来の社会の姿やネットの役割を考える際に大いに参考になる考え方だ。

（三）ルールの対策

（ア）サイバー平和利用条約の締結

二〇〇二年四月、みずほ銀行でコンピューター事故が発生し、ＡＴＭや振替のトラブルが約一カ月間続き大混乱に陥った。三銀行の統合に伴うコンピューター連結のトラブルだったが、社会の重要なインフラ（社会基盤）の一つである金融機関のシステムに事故があった際の影響の大きさを認識させた。

軍事的なサイバー攻撃やサイバーテロは軍事施設だけでなく、さまざまなインフラへの攻撃と一体になって行われると想定される。相手国が明確な軍事行動という形を取らずに攻撃してくる際にも、インフラにサイバー攻撃を行う可能性が高い。みずほ銀行の事故のようにインフラが攻撃を受けた際、すみずみまでコンピューターで支えられた国民生活に与える影響は計り知れない。

その防御を強化しなければならないが、一方で日本は世界の民主主義国の中心的な国家として、こうした甚大な被害を与える、国家によるサイバー攻撃や、その準備をやめるサイバー平和利用条約の締結を世界に働きかけたらどうだろうか。

生物兵器や化学兵器は非人道的兵器として放棄する条約が結ばれているが、それと同じように考えたらいい。原発など核施設がサイバー攻撃で事故を起こした際は、核兵器使用と同様な大惨事になる恐れがある。

米国と中国が互いにサイバー攻撃を行った、と非難し合っている状況で、条約締結は容易でないだろうが、理想として目指すべきだと思う。科学技術立国を掲げる平和国家・日本の目標としても正しいだろう。宇宙空間の平和利用を定めた宇宙条約と同様なものだ。

生物、化学兵器は「貧者の核兵器」と言われ、シリアなどが開発していた。どこかの国が開発したサイバー兵器（技術）がテロリストに流失すれば、極めて危険な「貧者の核兵器」になる恐れがある。

それでなくても、サイバー犯罪の技術はブラックマーケットで売買されている時代だ。サイバー兵器が簡単に流失する危険性は十分ある。理性や対話によってそういう危険を取り除くためにも、平和利用条約

が必要だと思う。

（イ）インフラ企業の対策強化

サイバー攻撃によって鉄道、通信、電気、水道、金融など、インフラが被害を受けた時の影響は、（ア）で挙げたように極めて大きい。日本ではサイバー攻撃に備えるために、インフラ関連企業と警察庁などとの連携組織ができているが、これらの企業がサイバー攻撃への万全な防護対策をとることが法律で義務付けられてはいない。

だが、ＪＲ北海道のレール異常の放置や、死亡事故を招いた三菱自動車のリコール隠し、東京電力による原発点検記録の虚偽記載（二〇〇〇年、〇二年）などの例がある。利益を追求する企業と、国民の安全を担う公共判断とは別個な原理で動いている。インフラがサイバー攻撃を受けた際の被害の大きさを考えると、公共セクターが広い視野からチェックし判断する仕組みが必要だろう。防備がないと攻撃を受けやすい。深刻な事態が起きる前に、明確に対策を義務づける法律の制定を検討すべきだろう。

またサイバー攻撃は全く新しいウイルスが登場するよりも、従来より少し変更したウイルスやパターンで攻撃してくるケースが多い。ある企業や公的機関が受けた攻撃内容を知ることは、新たな攻撃への対策に欠かせない。欧州のようにサイバー攻撃を受けた企業などの報告を義務付け、その情報を集約して早急に対策を講じるシステムを設けるべきだろう。

社会全体でサイバー犯罪、攻撃を駆逐する仕組みを作り上げる必要がある。

〈終わりに〉

ネット犯罪への対策は、急速に進歩する科学技術とどう調和を図るか―という、現代社会が直面する最大のテーマの一つでもある。原子力、医療、ロボット、防災…と、他の科学分野でも同じような問題を抱えている。

その際最も重要なのは、技術のマイナス面にも目を向けることだ。二〇一一年の東京電力福島第一原発の事故の際、東電幹部が「想定外」と言って批判を浴びたが、関係者が「安全神話」を振りまき、原発のマイナス面にあまり目を向けない過信があったことが、地震学者による大地震の危険性の指摘を軽視するなど安全対策の緩みにつながった、とも批判されている（⑱⑲）。

ネット社会で起きていることも似たところがある。子どもたちが被害に遭う事件が続発し、情報流失や不正アクセス事件が相次いでいる深刻なマイナス面を改善しないまま、安易に利便性や利益ばかりを追求すると、多くの被害者を生む悲惨な事件や経験したことのない大きな被害を招く恐れがある。

より安全で人間に優しいものに―。私たちは今、スタートから二〇年経ったネットの世界を変える重要な中継点に立っている。

【参照文献】

① 警察庁広報資料「平成二六年上半期のサイバー空間をめぐる脅威の情勢について」
② 山極寿一著『『サル化』する人間社会」（集英社インターナショナル・二〇一四年刊）一七三ページ
③ 和田伸一郎著「メディアと倫理」（NTT 出版・二〇〇六年刊）一六〇ページ
④ 情報教育学研究会、情報倫理研究グループ編「インターネットの光と影」（北大路出版・二〇一四年刊）一〇二ページ
⑤ 総務省広報資料「平成二六年度　青少年のインターネット・リテラシー指標等」
⑥ 樋口進著「ネット依存症」（PHP 新書・二〇一三年刊）八二〜八九ページ
⑦ 香山リカ著「ソーシャルメディアの何が気持ち悪いのか」（朝日新書・二〇一四年刊）一五一〜一五二ページ
⑧ 加藤典洋著「人類が永遠に続くのではないとしたら」（新潮社・二〇一四年刊）三〇三〜三〇五ページ
⑨ 内閣府「平成二五年度　青少年のインターネット利用環境実態調査」
⑩ 警察庁広報資料「コミュニティサイトに起因する児童被害の事犯に係る調査結果について（平成二五年下半期）」
⑪ 下田博次著「子どものケータイ―危険な解放区」（集英社新書・二〇一〇年刊）
⑫ 東浩紀著「弱いつながり」（幻冬舎・二〇一四年刊）五、一五ページ
⑬ サイバーセキュリティーと経営戦略研究会編「サイバーセキュリティー」（NTT 出版・二〇一四年）一五三ページ
⑭ 同一五五ページ
⑮ 吉冨康成編著「インターネットはなぜ人権侵害の温床になるのか」（ミネルヴァ書房・二〇一四年刊）iiページ
⑯ 土井孝義著「つながりを煽られる子どもたち」（岩波ブックレット・二〇一四年刊）
⑰ 西垣通著「スローネット」（春秋社・二〇一〇年刊）一五〇〜一五一ページ
⑱ 東京電力福島原子力発電所事故調査委員会著「国会事故調報告書」（徳間書店・二〇一二年刊）八一〜九二ページ
⑲ 日本科学技術ジャーナリスト会議編「徹底検証！福島原発事故　何が問題だったのか」（化学同人・二〇一三年刊）二五〜三二ページ

【その他の参考文献】

国家公安委員会・警察庁編「警察白書」平成二五年版、二三年版
情報教育学研究会、情報倫理研究グループ編「インターネット社会を生きるための情報倫理」（実教出版・二〇一三年刊）
西垣通著「ウェブ社会をどう生きるか」（岩波新書・二〇〇七年刊）
紀藤正樹著「インターネット犯罪大全」（インフォバーン・二〇〇四年刊）
岡村久雄著「迷宮のインターネット事件」（日経BP出版センター二〇〇三年刊）
矢野直明著「IT社会事件簿」（ディスカヴァー・二〇一三年刊）
矢野直明著「インターネット術語集Ⅱ」（岩波新書・二〇〇二年刊）
読売新聞社会部著「親は知らないーネットの闇に吸い込まれる子どもたち」（中央公論新社・二〇一〇年刊）
唯野司著「ネット犯罪から子どもを守る」（MYCOM新書・二〇〇六年刊）
高橋和之、松井茂記、鈴木秀美編「インターネットと法・第四版」（有斐閣・二〇一〇年刊）
三浦麻子、森尾博昭、川島康至編著「インターネット心理学のフロンティア」（誠信書房・二〇〇九年刊）
松田美佐・土橋臣吾・辻泉編「ケータイの二〇〇〇年代」（東京大学出版会・二〇一四年刊）
岡嶋裕史著「セキュリティはなぜ破られるのか」（講談社ブルーブックス・二〇〇六年刊）
岡嶋裕史著「ハッカーの手口」（PHP新書・二〇一二年刊）
谷口長世著「サイバー戦争の時代」（岩波新書・二〇一二年刊）
「別冊宝島・サイバーテロの全貌」（宝島社・二〇一三年刊）
リチャード・クラーク、ロバート・ネイク著、北川知子、峯村利哉訳「世界サイバー戦争」（徳間書店・二〇一一年刊）
洋泉社編集部編「サイバー犯罪とデジタル鑑識の最前線」（洋泉社・二〇一一年刊）

豊かで安全なネット社会を築くために

アルバイター
山﨑　浩子（56）

一　はじめに

13／31、7／22、17／33、（15／17）、5／14、8／19、17／35、15／18（注1）

これらの文集を見た時、皆さんは何を意味する数字だと思われるだろうか？

――実は私が、アルバイト通勤時に阪急電車に乗車した時にその車両に乗車している人を数えて、それ

を分母にし、その中でスマートフォンやタブレット端末・インターネットに接続可能な音楽プレイヤーを車内で取り出して何らかの画面操作をしている人の数を分子にした分数である。例えば、一番最初の分数については平成二六年六月二六日木曜日に雲雀丘花屋敷、午前八時三〇分発宝塚行急行の四両目に筆者が乗車した時点で乗っていた人が三一人で、その中でインターネットに接続できる端末の操作者が一三人いたということである。この後、七月と八月について観察してみたが、電車内で約三割から四割の人が、スマートフォンなどの器機を指で触ったり、見ているのが実感できた。特に注目すべきはカッコ書きの数字で、この日は、たまたま近隣の高校の短縮授業の帰宅時間と重なり、制服の高校生が一七人も乗っていて、そのうち一五人がスマートフォンもしくはネットに接続できる音楽プレイヤーを操作していたのだ。もちろん、スマートフォン以外は、現在のところ電車内では、ポケット Wi-Fi 利用者でないとネットには繋がらないが、このような電車内での現状を見る限り、パソコンでネットというより簡単に持ち運びのできるコンパクトな端末でネットを利用できる人がいかに多くいるか、容易に想像できる。このことを念頭に置きながら、ネット社会がどのようになっていけば良いのか提言していきたいと思う。

二　ネットの現状

日本におけるネット人口は、平成二五年末で既に一億人を超えており、人口普及率は八二・八％ということが、総務省から発表されている。(注2)また、ネットユーザーの接続がパソコンかモバイル(携帯電話・

スマートフォン）かテレビやゲーム機などからかという調査では、複数の端末による接続が多いことが読みとれる。（パソコン七八・一％、モバイル八一・三％、テレビやゲーム機など一六・二％）また、機器の保有率では、携帯電話九四・五％、スマートフォン四九・五％、その他ネットに接続できる家電一二・七％と、ネットの可能性は、持ち運びのできるコンパクトな端末のさらなる普及にあると思える。さて、今度は未来を担う青少年にスポットを当ててみよう。小学生にまで携帯電話、スマートフォンを持たせる親が増えていると聞くが、内閣府の調査（注３）を見ると、携帯電話とスマートフォンの所有率は、小学生三六・六％、中学生五一・九％、高校生九七・二％で、高校生については、そのうちの八二・八％がスマートフォンで、前年に調査された所有率五五・九％から大きく数字をのばしていた。また、青少年がパソコンを利用する割合は、小中高ともに八割ぐらいで、そのうち九割がネットを利用していることも分かっているが、パソコン利用率が前年に比べて小中高ともに減っている。このことから、青少年のネット利用がパソコンから徐々にスマートフォンをはじめとする携帯できる端末に移っていくと予想される。また、日本では二〇二〇年の東京オリンピックに向けて外国人観光客からの要望の強いインターネット環境の整備（ＩＤやパスワードなしに使えるWi-Fiの Free Spot の拡大）が進められていけば、ますますインターネットの垣根が低くなるだろう。

さて、ここで視点をかえてみよう。ここ一〇年で急速に広まったインターネットは、その利用方法（モラル）や法整備などが十分に成熟せずに拡大しつづけているため、私たちにとってメリットだけではなく様々な問題を生じることになった。それは、小さな個人的な事から企業、国家の問題にまで及ぶ大きな事

まで含むが、最近のニュースを取り混ぜながら現状での問題点を羅列してみることとする。

①歩きスマホや、ながらスマホなどによる事故の多発や他人への迷惑。

②安易な書き込みによるツイッター炎上。

③視聴回数を増やす（違法行為を含む）の誇示的動画の投稿。

④引用表示をせずコピペをしたものをそのまま論文などに使用する。

⑤アダルトサイトや出会い系サイトなど犯罪につながりやすい有害サイトの存在。

⑥違法性の強い商品や違法な物を扱う闇サイトの存在。（危険ドラックなども簡単に手に入る）

⑦違法行為のやり方教授サイトの存在。

⑧ＳＮＳでのなりすまし詐欺。（今年の七月一一日の報道によるとＬＩＮＥのパスワードリスト攻撃により、友人になりすまし電子ポイントカードを搾取する事件が明らかになっている）

⑨ネット依存症（ネットゲーム依存を含む）になる人もいるが、日本では専門の治療機関がほとんどない。

⑪検索時に検索エンジンと企業などの関係性により検索順位が変わり、本当に必要な情報を探すのに時間がかかる場合がある。（情報量が多すぎて選択困難）

⑫社員・関連会社のモラルが低い場合の情報漏洩。（自分は気をつけていても、自分の情報を持っている人のセキュリティ意識が低かったり、情報の取り扱いが安易だと知らぬ間に個人情報が漏れることがある）⇑最近ではベネッセ事件。

⑬物や人物を直接見ないためネット通販やオークションでトラブルが起きる場合がある。

⑭気軽に（承諾なしに）他人の写真や情報を公開し、肖像権や著作権の侵害をしてしまう場合がある。

⑮ＧＰＳや検索エンジンなど利用の際、確かに企業に対して自分の情報を蓄積されることを承諾は一応しているが、それが逐一把握されていることを思うと不気味。

⑯ウィルスが存在すること。また、ウィルスを作成し販売する会社が世界にはたくさん存在し、各国政府もサイバー攻撃に備えてウィルスを購入している事実。（八月七日のウィキリークスのニュースで英国のGamma社のFinfisher（finspy）という国民監視用スパイウェアウィルスは、世界三六ヶ国が購入し導入して様々な場所に使われているらしく、これはセキュリティソフトに感知されない高いステルス機能を有するため対策が困難という情報があり、さらにこのfinspyがハッカーにより流出し、だれでもダウンロードが可能になっているとのこと。）

⑰ウィルスに対してセキュリティソフトが必ずしも追いついていないこと。

⑱サーバーに侵入して情報を抜き取ったり、ウィルスをばらまくハッカー（クラッカー）の存在。（九月二日のニュースで、iCloudからアメリカセレブの個人的写真がハッカーにより流出させられた報道がされた。）

⑲サイバー攻撃。（対立する相手に大量のデータを送り、相手のコンピューターをパンクさせるなど初歩的な事から、ウィルスをいざというときに作動させるように相手のコンピュターネットワークに侵入しておくという手の込んだ方法まで数々ある）

このように、個人のモラルに係わる事から、国家に係わる大きな危険性を孕むネット社会だが、危険性

の反面、大いなる魅力と可能性のある世界でもある。では、今度はネットの利点について書き記していこう。

①世界中に友達が作れる。（不特定多数の人とコミュニケーションできる）
②遠方への通信が安価にできる。
③買い物が簡単にできる。
④いろいろな情報が簡単に、しかも大概は無料で手に入る。
⑤辞書がわりに漢字や英語のスペルなどが調べられる。
⑥リアルタイムの情報が手に入る。
⑦世界に自分の考えや行動を発表できる。
⑧動画や音楽を楽しめる。
⑨動画やブログを配信して有名になることができる。
⑩世界を相手に商売が可能（アプリやスタンプを作って儲けられる可能性がある。）
⑪ブログや動画に広告をつけ、広告収入を得ることができる。
⑫口コミ情報（評価）があり、物を選んだり購入する時の参考にできる。
⑬ゲーム（将棋や囲碁も含む）をネットで知らない人とでも対戦できる。
⑭同時にたくさんの人と連絡を取り合える。

このような利点を生かして学校でも調べ学習や家庭での予習に活用する学校も出てきたし、買い物難民

の解消や、医療機関のカルテ共用や在宅勤務の拡大にもつながっている。近年、小学生などにも人気のＳＮＳ（ソーシャル・ネットワーキング・サービス）のＬＩＮＥは、仲の良い人だけでグループを作ってチャットができ、メッセージを相手が読んだことがわかる「既読」機能もあることから、電話やメールの代わりになってきている。また、海外では人気のFacebookは実名主義をうたっているため、ビジネスに利用しやすく、友達の友達を探すことで、いもづる式に友とつながることができるため、年配者が元同級生を探して同窓会を開いたなどという話題も聞こえる。

――利点は常に危険とつながっている。今迄書いてきた特徴に加えて未来にはどのような技術と結びつき、発展してゆくのだろうか。

三　ネットの未来

自宅で、じっくりネットを楽しむ時はパソコンが利用されるかもしれないが、普段は手軽な、タブレット・スマートフォンなど携帯に便利な端末での利用割合が増えていくだろう。また、Wi-Fi の free Spot 拡大で、どこでもネットの状態が日常化するかもしれない。既にめがね型端末や腕時計型端末も実用化されはじめている。さらに、マウスのクリックやスマートフォンやタブレットの画面タッチの難しいお年寄りや身体の不自由な人でも使える接続機器やアプリも登場している。それがますます発展し、どんな人でもネットを利用できる環境が整うと思われる。また、立体映像が楽しめる電子ホログラフィや、多言語翻

訳技術の進化で、より世界中の人達とのコミュニケーションが広がるだろう。また、今まで間違いや片寄った記述の目につくインターネットの情報の中から、正確で意味のある情報を探し出す技術や、情報と情報を組み合わせて新たな有益なアイデアを生み出す技術が確立されれば、新聞などのメディアにも多大な影響が及び、個々の読者に合った記事のパッケージ化や特定事件に関連した記事をパッケージして読者に提供する仕組みができるだろう。また、ロボット技術と結びつき、遠隔地からの作業指令やアクションで、新たな物を生み出せるかもしれない。一方で、便利なネットサービスのＳＮＳは、ますます利用者が増え、運営会社はその個人情報をデータ化し、顧客企業の宣伝活動に結び付けて巨額の利益を上げていくだろう。（眞淳平氏の記述による）

このようにネット上に、世界の技術や個人情報・国家機密などありとあらゆる情報が集積されていくと、より危険度も高まるのも事実だが、それを徐々にでも減らしていくことができるのは、私は唯一、幼少期からの教育だと思っている。そこで次章で提言したい。

四　子供たちの教育に何が必要か

日本において、子供たちがコンピュターやインターネットについて学校で取り扱う場面は、小学校では総合の時間の「調べ学習」、中学校では「英語教育」や「調べ学習」に、高校でも同様に「英語」、「調べ学習」、「情報」の時間にWord・Excelの使い方を練習する程度だと思われる。もちろん先生が熱心で、動画を

利用した予習学習（反転授業）に取り組む学校も読売新聞の教育ルネッサンスに掲載されていたし、インターネットを利用する時のマナーやルールについて、ＩＴ企業の専門家や警察の担当者を講師に迎えている学校もある。実際のところ私には高二と中二の子供たちがいるが、必ず年に一回講演会があり、子供だけでなく保護者もいっしょに学べるようになっている。それはそれで、マナーやルール作りに貢献していると思われるが、今や幼稚園児ですら母親のスマートフォンでうまく遊ぶ時代なのに、あくまでパソコン・ネットの利用法の学習に留まっているのでは未来が開けるとは思えない。そこで、子供の出生から高校時代までのＩＴ教育について考えてみることにした。

①妊婦さんの母親学級で、子供とネットについての教育を行なう。出生後しばらくは母親にネット接続を減らしてもらい、赤ちゃんと一緒なのにスマートフォンばかりみている状態を作らせない。

②子供の一歳児検診などの機会に、スマートフォンを子供に与えて子守をさせるという行動について考えてもらい、しばらくはネット接続を減らしてもらう。

③子供が三歳になって幼稚園や保育園に入園したら、子供には「挨拶」、「感謝」、「謝罪」（おはようございます。こんにちは。さようなら。いただきます。ごちそうさまでした。ありがとうございます。ごめんなさい。）の言葉を教え、アナログコミュニケーション力を高めるための第一歩を応援する。

一方で、母親など保護者に「情報モラル教室」を受講してもらう。

④子供が、年中・年長さんになりパソコンに興味を持ったら、石戸奈々子氏が論点（読売新聞）で提案したように、米マサチューセッツ工科大学メディアラボ開発の「スクラッチ」やそれに準ずる子供向

けの方式でプログラム教育を始める。彼女は小学校からの導入を進めていたが、直感を表現するプログラミングは、年中・年長さんでも取り組めると思う。もちろん③も続ける。

⑤小学生になったら、③、④に加えて、今まで学校で開催されてきた子供対象の「情報モラル教室」と日常でたっぷりアナログコミュニケーション力を養い、できれば総合の時間でプログラミングの授業とグループ学習などの対人発表の機会を多く含む授業を交互に行なう。パソコンを動かすソフトを少しでも考えることで新しい発想が生まれ、パソコンやスマートフォンに「使われる」のではなく、「使うためにいろんなことを考える」ようになるのだ。また、今後、家でも、習い事や学校の往き帰りにも常時デジタルツールと接するような状態の子供が増えることを考え、対人関係の強化のために、③で示した「挨拶」、「感謝」、「謝罪」の他に、自分のまわりの出来事に自分なりの見方や意見を持ち、姿勢正しく大きな声で発表できる力をつける教育をするのだ。

⑥中学校では、情報セキュリティーについても学べる仕組みを作り、現在はＩＰＡ（情報処理推進機構）などが主催して夏休みに合宿しながら行なう「セキュリティ・キャンプ」のミニ版を都道府県単位でできるようになれば、毎年少人数しか参加できない体験の拡大化が図れると思う。

⑦高校でもセキュリティーを徹底して学習できる環境を作り、アメリカのデフコンに出ることができる人材を育てるべきだと思う。

このように、今後の子供たちには、パソコンやインターネットを単に利用することや、モラルの学習といった、後付け的な勉強だけではなく、対人関係を意識した「しっかりした自分を形成するための手助け

をする学習と、想像し創造する力をつける学習をする」ことで、ネット社会の闇を打ち破り、犯罪を起こさない、周りに配慮できる人間に育てることができるのだと思う。

五　高齢者たちにも夢を

前章では理想論ばかりを書いたようで、二章で示した現実の問題には、直接対応できないではないかと、おしかりを受けるかもしれない。だが、教育とは大事なものだ。年配の人なら記憶されていると思うが、少なくとも五六歳の私は、各戸に一台電話機の普及した高度成長期育ちの人間だが、電話の受け方、話し方・長電話など、インターネットとは、レベルが全く違いはするが、学校や職場で教育を受けた。インターネットの取り扱い方の基礎的なことも同じだと思う。子供の頃から教育を受けることで、「歩きスマホ」や「ながらスマホ」は解消されるだろうし、ツイッターの書き込みも書き殴りで、すぐにクリックするのではなく、必ず読み返すこと。昔から日記に書くような内容や、妄想はネットには書き込まない。（日記帳なら笑い話でも、ハッキングされたり、見て欲しくない人や他人に見られたら奇人変人犯罪者のレッテルを貼られる場合もある）いかがわしいサイトや違法性の強い商品を探したり、のぞき見をしない。（ネット犯罪やウィルスをまき散らされるかもしれない）皆に見てもらう動画は自らのオリジナルで、他人に迷惑のかからないものに限る。（それで視聴回数を増やすことができる人こそ誠のクリエーターだ）調べ物をする時は、出所がはっきりしていないものは、真実ではない場合もあるので参考にとどめる。インター

ネットで情報を集めているつもりが、自分の行動を検索エンジン企業に提供して商売のネタにされていると思え。ネット上のアンケートなどには、できるだけ記入をしない。パスワードやＩＤは、使い廻ししたりせず、それぞれ違うものにする。もちろん、それでもハッキングする者もいるから、インターネットで利用する銀行口座には、あまりお金を入れておかない。ネットショップやオークションの商品は、ほどほどの物が届けば正解とする。町で見かけた人が、おもしろいといって勝手に写真や動画に撮って友人に送らない。ウィルス対策ソフトは常に更新すること。パソコン購入時に入っていたウィルス対策ソフトが最良の物とは限らないと心せよ。検索中にサイト内に「危険・あなたのパソコンは危険にさらされています。今すぐここをクリック」と表示されていて、そこをクリックしたとたん、パソコンが切れてしまい立ち上がらなくなった友人がいる。誘導型ウィルス散布には要注意。こんなふうに経験を蓄積すれば、私のようなネット音痴もなんとか危険を回避することができるので、世の高齢者の皆さんも、大丈夫ではないだろうか?ただし、若い時と違い指での画面タッチには誤操作がつきものだし、手の震えで、なかなかスマートフォンも使えなくなるかもしれない。だが、来たるべき高齢化社会を前に企業は使いやすい商品を開発してくれるはずだから、長生きして少し待って‼

六　未来へつなぐ、楽しいネット社会

インターネットの世界は、元来人間が創り出したものであるから、ウィルスや戦争とは無縁のはずだっ

たのに、自分の能力を誇示したり国家の利益を守るためにサイバー攻撃をしかけてくる国がある。日本は、ウィルス生産会社もなければ、セキュリティーを誇れる人材も少ない状態である。日本において安心・安全のネット社会を築き上げるには一にも二にも教育による人材育成である。しかも闇雲にデジタルツールに頼り、デジタルコミュニケーションにのみ重きを置く教育を施すと人間力が育たない。千葉大学の西田弘次氏によると、デジタルコミュニケーションは、アナログコミュニケーション力に勝つことはできないとのことだ。だから、プログラミングを学び、ネット端末を使いこなし、生活上で他人と直接触れ合わない生活を続ける人に、コミュニケーション力があるかと問うと、常に人と接している人の方が、他人や周りの人に良い影響を与えることができるといえる。かのスティーブ・ジョブズも新商品を発表する時は、大きな会場で、まるで大学の先生が講義するかのように、顧客やマスコミに、プレゼンテーションをしていた。

――日本の子供たちも、単なるパソコンやネット世界のオタクに育てるのではなく、周りに配慮をし、洗練した言葉を綴れるクリエーターに育ててほしい。未来の日本を担う人は、偏りのない考えを持ち、私たち老いゆく者をばかにすることなく、自分の考えや意見を堂々と世界に発信できる豊かな心を持ってくれることを心から願ってペンを置くことにする。

（注1）・阪急電車午前八時三〇分雲雀丘花屋敷発宝塚行急行四両目乗車における調査　Ⓐ
・同じく午後〇時三〇分宝塚発大阪梅田行急行七両目乗車時における調査　Ⓑ

一三人／三一人　平成二六年六月二六日　Ⓐ

七人／二二人　平成二六年六月二七日　Ⓐ
一七人／三三人　平成二六年七月一日　Ⓑ
（一五人／一七人）同右の高校生のみのデータ
五人／一四人　平成二六年七月一六日　Ⓐ
八人／一九人　平成二六年八月二二日　Ⓐ
一七人／三五人　平成二六年八月二二日　Ⓑ
一五人／一八人　平成二六年九月一日　Ⓑ

（注2）総務省情報通信白書（平成二五年度版）
インターネット利用者数　一億四四万人

（注3）内閣府調査（平成二四年度・二五年度）

（参考文献）

☆「気をつけようSNS」一～三巻　小寺信良著　汐文社
☆「二一世紀はどんな世界になるのか」眞淳平著　岩波ジュニア新書

（資料）

☆二〇一四年五月から九月までの読売新聞記事
五月三日「学ぶ育む」
五月二二日～三一日「教育ルネサンス」

五月二一日「スマホでサポート」
七月一一日「友人装い『ＬＩＮＥ』詐欺」
八月二三日「論点　サイバー対処人材不足」

ネット社会を安全に暮らす三つのコツ

警察官（警視庁高井戸警察署）
和田　大樹（21）

一　はじめに

はじめに、インターネット（以下ネット）が普及するに連れ、ネットに関連したトラブルや犯罪が発生し、増加傾向にある。こうした状況をとらえ、今回この論文を作成するにあたり、より多くの人に注意力を向上してもらいたいと考えている。つまり、できるだけ分かりやすく書き、年齢を問わず理解し、自分

で考えてネットを利用してもらいたいのである。

そのためにネット社会を安全に暮らす三つのコツとして

　見ない　載せない　登録しない

というスローガンを最初に揚げてから、以下に論じていこうと思う。

またネットの危険ということを考えると、大きく二つに分類されるだろう。一つ目は、ネットを利用した犯罪に巻き込まれること。二つ目は、ネット上のトラブルに巻き込まれることである。この二点について説明を踏まえながら話を進めていくことにする。

二　ネットを中心とした情報社会について

現代社会で、日本だけではなく全世界において、ネットという存在は、普段の生活にもそして仕事をする上でも欠かせないものとなっている。

小説、新聞、辞書などからの活字離れが進み、人が文字を手で書くことも大きく減った。大学の講義では大学ノートとボールペンではなく、ノートパソコンを利用し、課題（論文）にあってもノートパソコンで打ち込んだものを、ネットを介して提出するといったシステムが、既に存在している。

こういったネットの浸潤には、ネットの安易性という背景がある。

調べたいものが、その場で、数個の文字の羅列を並べることによって、簡単に出てくる。料理の作り方

から、トレーニングの仕方、あるいはさまざまな動画、画像。その情報量は膨れ上がり、はかり知れないものとなっている。

その結果、以前は何かを調べようと思ったときに、本屋に行って本を買ったり、図書館に行って本を借りたりしていたものが、今はパソコンを開くかスマートフォンやタブレット端末を出して検索するようになった。そしてまた、情報がより生活に近いものになったことから、非難や評価に関してもネットを通じてするようにもなった。

また、これは直接ネットに結びつく話ではないが、各種機械製品の機能が向上してきたことも、これらの要因を担っているのではないだろうか。例えば、電話がその一つだ。以前は誰かＡさんに電話を掛けようと思ったとき、電話の近くに置いてある電話帳を取り出し、Ａさんを探し出し、電話番号を回し、電話をしていた。そのため、よく掛ける相手の電話番号くらいはすぐに覚えてしまったものである。しかし現在は、携帯電話の電話帳の中から名前を探し出し、その名前を選択すれば電話が掛かってしまう。なので、どんなに頻繁に連絡を取り合う仲であっても電話番号を覚えることはあまりない。文明が、より楽なものを選びそれが普及することで覚える必要もなくなったからである。さらに最近では、その楽さに拍車がかかり、ネットを利用したツイッターなどのＳＮＳやＬＩＮＥのようなアプリ等といったツールを使用して連絡を取り合うように変化している真っ只中である。

さて、このようにネットが一般的になり、情報が昔よりも身近になったことで、数値として目に見える形で増えたものがある。

それは、ネットを利用した犯罪である。

警察庁の公表している「サイバー犯罪の現状」によれば、平成一三年と比べて一〇年経った平成二二年には、サイバー犯罪の検挙件数は約五倍になり、ネットワーク利用犯罪の検挙件数は約四・三倍になっている。つまり、ネット犯罪が大きなパーセンテージで増加したことがわかる。

その理由には、パソコンを扱うことに慣れている現代人が増えたことがあるだろう。専門的にネット分野の勉強をしている者も増大したはずだ。しかし、それが悪いことだという訳ではない。ただ、その技術を悪用する者がいることを忘れてはならないのだ。

ネットを中心とした情報合戦は、大きなリスクを孕んでいる。それは、発信者の秘匿性である。パソコンを専門として扱う者にしてみれば「秘匿性は限りなくない」と言えるのかもしれないが、一般人にとって、顔が見えない・名前が出ないというのは、ある種の可能性を見出してしまうものではないだろうか。

それは、「バレない。」という感情である。

あるものに対して、過大評価をしても誹謗中傷を重ねても、誰も自分が言っているとは分からない。たとえ顔を出しても信用性に欠ける。本当にその写真が本人のものか、知っているのは自分だけだ。

しかし、その考え方は間違っていることを断言しておかなければならない。先に述べたとおり、ネットを扱う専門家には、ネット上に文字を打ち込むだけで、ある程度の情報が分かってしまうのだ。いつごろ、どのあたりで、どんなパソコンがそれを入力したのか。

ただし、この秘匿性という考えがネット上の犯罪やトラブルを増やしている要因であることは、否定が

できない事実であることには変わりはない。

三　児童が関係するネット犯罪について

警察庁のデータによると、インターネットを利用した児童ポルノ事犯の検挙件数は、平成一三年には約一〇〇件であったものが、平成二二年になると七八三件にまで増加した。また「コミュニティサイトの利用に起因して児童が被害にあった一定の事件」として警察庁に報告のあった検挙件数は、平成二〇年は九九四件で、平成二二年になると一、五四一件に上ったという。

このように、ネット犯罪自体が増加するなか、児童が関係するネット犯罪についても増加していることが分かる。

この結果は、児童を狙う大人が増えたからなのだろうか、いや必ずしもそうとは言えない。寧ろその逆である。児童が関係するネット犯罪が増えたことは、ネットを利用する児童が増えたことに起因していると考えられる。

内閣府の調査によると、平成二五年度の調査で自分専用の携帯電話を持っていると答えた者が、小学生では三〇・三%、中学生では四八・八%、高校生で九六・四%であった。この数値は、毎年上昇している傾向にあり、以前よりも携帯電話を持ち歩いている児童が増加していることがわかる。

またその中でもスマートフォンを持っているとした者が、小学生では一三・六%、中学生は四七・四%、

高校生は八一・七％であった。

この結果から、特に中高生において、携帯電話を購入する際に、携帯電話そのものの電話機能やメール機能ではなく、ネット機能に重点を置いて携帯電話を購入していることがわかる。

しかしながら、ネットの使用率は上がっているにもかかわらず、現在そのネットに対する安性の確保等の教養が行われていない、もしくは教養が足りていない。

内閣府では、スマートフォンのフィルタリングの認知度に対する調査が行われた。フィルタリングとは、有害と思われるサイトにフィルターをかけて、アクセスを制限するものであり、スマートフォンでは、安全面から掛けるフィルタリングが、「携帯電話事業者が提供するフィルタリング」と「無線ＬＡＮに対応したフィルタリング」と「アプリに対応したフィルタリング」の三種類がある。このことを「知らなかった」と答えた者が、小学生で七七・八％、中学校が三二・八％、高校生が一九・四％、とフィルタリングに対する認知度が低い。

児童のネット使用が増加している中で、ネットへの教養が追いついていないことから、児童はネット上で大人から護られず、そしてネット犯罪という魔の手に捕まってしまうのだ。

四　ネットの必要性について

さて、私たちがネットを必要としている理由とはなんだろうか。理由は二つある。一つは、調べものを

する際に気軽に検索が出来る利便性である。そしてもう一つは、ネットにもうひとつの世界を創っている居住性である。

利便性という点については、パソコンで調べものをすることもその一端を有しているが、現代社会においての利便性はそれをさらに進んだ形となっている。

パソコンの「マウス、キーボード、ソフトウェア」という重い枠組みの検索ツールを取り払い、「アプリ」というワンタッチの手軽で簡単なものになった。スマートフォンやタブレット端末における「アプリ」は、多種多様にわたり、すぐに挙げられるものだけで、天気予報、音楽、電車やバスの時刻表、ゲーム、クーポンなどがある。遊戯的・娯楽的なものから、生活に密着しているものまで、用途にあった「アプリ」は実に多種多様である。

次に居住性という点については、ネットの娯楽的な面に起因するものである。ネット内のブログやツイッター、フェイスブック、ゲームにおいて、ＩＤを作成し、ニックネームをつけて、現実社会とは別人ないし離れた存在の自分をネット上にソウゾウ（想像・創造）する。アバターやキャラクターを作って、それを用いることで、あたかもそこに暮らしているような錯覚に陥る。また、顔が見えないからこそできる相談をしたり、グループ（サークルやギルドなど）を作って仲間意識を持ったりと、本来、現実社会で行われていたものが、ネットの世界でも営まれるようになった。さらに、ネットの世界を現実世界よりも重要視しているという者も少なくない。つまり、ネットの世界に自分の居場所というものを求めるようになったのである。

そして、これらネットの利便性と居住性とが重なり、より強く、ネットがなければ生活ができないという社会に変化してきたのである。

だからといって、安全のために、今更、ネットのない生活を送るべきだと言うには、あまりに時代に似合わない話である。ならば、私達はどうすれば良いのだろうか、どうするべきなのだろうか。

私達は、もっと真剣に、ネット社会を上手に安全に暮らしていくために、どうしなければならないのかということを考えなければならないのである。

五　ネットを利用した犯罪について

今までネットがいかに広まり、また犯罪が増加しているのかということについて言及してきたが、これらの犯罪は、どのようにして私達の前に降りかかってくるのだろうか。ここで、その例を挙げてみることにする。

一つ目に考えられることは、『不用意な閲覧』である。例えば、「アイドルの連絡先が分かる」や「幸運を手に入れる方法」などの文を見て、または性的好奇心を煽るような文章や画像から、悪質サイトのＵＲＬやバナーを選択してしまうケースがある。こうした悪質サイトは選択したことを通じて、両面をフリーズさせて、あるいは詳細な住所・連絡先を手に入れたふりをして、多額の金品を要求してくる事件につながっていく。

二つ目に考えられることは、『不用意な掲載』である。例えば、ブログ等において、住所や氏名を掲載してしまったり、それらが分かる写真・動画等を掲載してしまうケースだ。この場合、その家屋に嫌がらせが来たり、ストーカー事案に発展してしまうことがある。

三つ目として考えられるのは、『不用意な登録』である。昨今、ネットでブログ・ＳＮＳ等をする為には基本情報を登録しなければ始められないというものがほとんどである中で、そのサイトが本当に信用できるものかということを深く考えずに登録してしまうケースだ。その結果、無料だと思っていたサイトがいきなり有料に切り替わっていたり、迷惑メールが増えたり、または基本情報が漏洩したりという事態が起こってしまうのだ。

六　ネット上のトラブルについて

ネットの居住性は、ネットの依存性という言葉に置き換えることができる。ネットに新しい居場所を作り、その中にも生活感を見出すことで、そこから抜け出せなくなるのである。一般に対人関係で引き起こる「割り切れない」という気持ちが、ネットにも起こる訳だ。それはある種の中毒性を帯びていて、酷くなると一日中、そこに入り浸っていなければ気持ちが悪くなってしまうケースもある。

実体験と友人から聞いたことから話をすると、ネットという媒体で特殊な部分は、「返ってくる」という感覚である。

ブログ、ＳＮＳで言えば、自分の悲しいことや面白いと思ったこと、趣味や趣向など、自己的な感覚についてネットに上げる（up する）ことで、知らない誰か別の第三者から、それについて共感や賛同を得られる。若しくは、他の角度から同じ物を見たときの感覚を教わって新しい発見をしたりする。友達に話すには、少し戸惑うようなことでも、ネットの上なら、恥ずかしげもなく述べることができる。そして、それに対する別の意思が返ってくることに喜びを覚える。そうして、もう少し続けてみよう、もう少し話してみようという気持ちになるのである。または、同じ感覚を持った人に出会い、そしてネットを越えて、現実でも会おうとさえしてしまうのだ。

またネットゲーム（以下ネトゲ）で言えば、そのシステムが居住性を高めている。ネトゲは、個人で無料で進められることができるように始まって、そのほとんどが途中で行き詰ると仲間が必要になってくる。チームやギルドといったものだ。しかし、さらに行き詰ると、より強いチームに入らなければならなくなり、そのためには、自分も強くならなければならない。そしてより強い道具やカードを集めるために、課金制度に手を出す。さらに強いチームに入ろうとし、さらに課金を繰り返す。ある一定のところまでくると、今いるチームへの愛着が沸くようになる。お互いにログインを重ねることにより、助け、また助けられる。そしてチャット型のシステムにより、さらにその関係は密になる。サーバー側の課金をさせようとするシステムが、人のネットへの居住性を高めている。

そのネットへの依存は、やがて自分の感覚を外に出す捌け口にとどまらず、他人の感覚を否定するようにもなる。これが、ネット上のトラブルの火種となるのである。

否定はさらなる否定を呼ぶ。学校で、例えば三〇人のクラスがあったとする。すると、十人十色と言うように、三〇人三〇色のそれぞれ違った考えがあり意見がある。誰かの顔をうかがう者もいるだろう。しかし、ネットは、三〇人どころでは済まないのである。数万人数万色の考えが、誰も顔色をうかがわず、好き放題に「我が我が」と話をするのであるから、当然大きくなるのだ。いわゆる、ブログの炎上というものは、こうしたものの類だ。

それから、「叩く」という言葉がある。昔はマスメディアが、政治家や法人に対して批評していたものが、そう言われていた。汚職や嫌疑といったものを追及することだと理解していたが、ネット上にも「叩く」という言葉が使われるようになった。そこから変わったものは「叩く」の質だ。新聞や報道というものは、ある程度あるいは絶対の根拠を持って、その人物ないし法人を叩いていたのに対し、ネット上のそれは、人の噂のように尾ヒレ羽ヒレがついて叩かれていく。そして全く見当違いというものが信じられるようになる可能性が生まれる。逆に、どこからも圧力のかからない真実が語られるという可能性もあるが、前者の場合の方が圧倒的に多いだろう。

さて、連絡の取り合い方もＳＮＳやＬＩＮＥといったツールになり始めたという話をしたが、これもトラブルにつながっている。先述したとおり顔が見えないからこそ、話がしやすいというのは、知り合いに対しても同じことが言える。つまり、友達（クラスメイト）に対しても人前では言いにくいようなことを言いやすくなるということだ。そして、誹謗中傷や残酷な言葉の一方的なキャッチボールが発生してしまう訳だ。日本で昔から、重要な問題として騒がれているいじめの問題は、なにも暴力的な見える形にと

どまらない。ネットを使った書き込みなどの陰湿なものもある。現にＬＩＮＥによるいじめによって女子生徒が亡くなってしまった事件はまだ記憶に新しい。

「ネットは悪用されるのだ」ということを再認識し、ネットを利用していかなければならないだろう。

七　クラッキングについて

ここで、ネット上の危険として、ハッキングとクラッキングについて話をしたい。ハッキングという言葉は一般にコンピュータを駆使してネット上においてＩＤを乗っ取ったり、サイバー攻撃やスパイ活動を行うものとして広まっているが、実はそれは少し間違っている。ハッキングというのは、ネットの専門家が、ネット上のあらゆる問題を合法的に処理解決することであり、非合法的なサイバー攻撃等はクラッキングと呼ぶ。また、合法的に活動するものをハッカーと呼ぶのに対し、非合法に活動する者はクラッカーと呼ばれている。

クラッキングの方法としては、なりすまし、乗っ取り、スパイなどが挙げられる。なりすましとは、コンピュータのuserになりすましてコンピュータを立ち上げた部分から侵入し、情報ファイルの改ざん、盗難、破壊等を行うことである。乗っ取りとは、ネット上の情報は暗号化され複雑な文字列となって送信され、相手側がそのファイル解読するという流れになっているが、一般的なものであれば、ある程度の法則に従って暗号化されている。その文字列をいじることで、あたかも別人が送信したかのように見せかけ

たり、または故意に第三者が送信したように見せることである。スパイは、直接そのコンピュータのデータに入り、データ情報を抜き取ったり、改ざん、破壊することである。

いずれの場合も、クラッキングする側もされる側もネットにつながっていることが第一条件となる。つまりネットに入っていなければ攻撃をされることもないといっても良い訳である。

しかし「ネットの必要性」で述べたとおり、今更、ネットを切り離して生活をするというのは、いささか無理な話である。そのためには、やはりパソコンやタブレット端末におけるセキュリティプログラムが欠かせないだろう。その上にフィルタリングがあるのが現状だ。

八　ネット社会を安全に暮らす三つのコツ

かつてソクラテスはあらゆる論議を繰り返す中で言ったという。「知らないということを知っているということは、それだけで相手よりも優位である。」と。これは「無知の知」という考え方である。

例えば、「右手を使ってボールを前に飛ばす。」という動作について考えたとする。まずボールを右手に持ち、後ろに振りかぶる。手を前に出したときに、リリースポイントを見つけて手を離すとボールは前に飛ぶ。では、どうしたら、飛距離を伸ばすことができるのか。そのためには、より遠くに飛ばすために自分がどうしなければならないのか、その分からない部分を知っていなければ、修正していくこともまたできない。何も分からないままでは改善の余地もない訳である。ボールを遠く飛ばす投げ方としての、肩の

使い方を知らない、足の踏み込み方を知らない、ボールの持ち方を知らない等々、色々な要素がある中でそれを多く見つけることができれば、より多くの対処法を見出し、そしてより遠くに投げることができるようになるのである。

このようなことは、ネットを扱う上でも言えるのではないだろうか。私達は、ネットの危険性について知らないことばかりである、ということを知らなければならないのである。そうすると、危険性があることについて勉強し、その危険に対しての予防、抑止策として何を考えなければならないのかが見えてくる。

そして、私達がネットに関して無知であることを知らなければならない。私達は専門家ではないのだ。だからこそ、専門家に助け（アドバイス）を求めなければならない。セキュリティプログラムはどうしなければならないのか、フィルタリングは何を掛ければ良いのか等である。

しかし、専門家に頼ることだけが全てである訳ではない。それはネットを使う人自身がネットを扱うときに注意をすることで、ネットに無知な人であっても予防線を張ることができるということである。

簡単に言うと「ネット」と「自分」の間に一本客観的な線を引くことである。これが予防線になり得る。

ネットの絡む犯罪やトラブルには、その発端となる糸口が必ずある。予防線を引かないために、自分でどこかしらに情報を提供してしまっている（気付づかない内に提供してしまっている）からこそ、犯罪やトラブルに巻き込まれてしまうのである。

さて、ここで予防線の具体策として、ネット社会を安全に暮らすためのコツを三つ提案したいと思う。

まず一つ目は『見ない』ことだ。様々なサイトから送られてくるメールマガジンやそれに付いてくる

ＵＲＬ、それからサイトに載っているＵＲＬ、アダルト系のサイト等には、危険なウイルスが潜んでいる。それを見てしまったために、パソコンが固まってしまったり、サイトに入ったパソコンの情報が取られてしまったりする。なので、必要なサイト以外は極力見ないようにし、もし見るとしても慎重になって考えた上で、見る選択をしなければならない。

次に、二つ目のコツは『載せない』ことだ。特にブログやツイッター、フェイスブックといったＳＮＳでは自分の顔写真だけでなく、住所が分かるような写真等を掲載しているものが多く見られる。さらには、住所地や最寄り駅、出身校、在学校を載せていたりもする。ネットは数え切れない程多くの人が閲覧でき、また、見る側の人を載せた側は選ぶことができないのがほとんどだ。そのような中で、自分の個人情報を載せてしまうことはとても安直で危険な行為である。たとえ、ブログやＳＮＳに写真や個人情報を載せるとしても、自分とは特定できないようなものを載せるようにしなければならない。

そして三つ目のコツは『登録しない』ことだ。個人情報を登録するということは、相手側からすれば、特殊な技術を用いなくても、情報を入手することができる、至極簡単な仕事になる。一般の善良と思われた会社からの情報漏洩などが取りざたされる現代において、相手がネットというベールに包まれている会社であるのに、安易な考えで個人情報を登録してしまうということは、この上なく危険である。まず登録をしないことが一番望ましい形ではあるが、どうしても登録をする必要に迫られたときには、その会社が安全であるかもう一度調べ直し、また、その会社のサイト内にあるプライバシーポリシーや規約等をよく読んでから、登録をするようにしなければならない。かつ、その登録をした情報が、その会社の不手際に

よって漏洩してしまうかもしれないというリスクを持っていることを忘れてはならないだろう。

また、児童の関係するネット犯罪が増加傾向にある今日では、保護者が子供に『見せさせない　載せさせない　登録させない』といったブロックする取り組みをしていくことも重要になってくるだろう。

九　最後に

Boys, be ambitious（少年よ、大志を抱け）

札幌農学校（現北海道大学）の初代教頭である、ウィリアム・スミス・クラーク博士の言葉である。少年には大きな可能性が秘められている。目指す道、勉強の方向や量、そういったものでなりたい自分になれる可能性があり、そして未来を変えていく力を持っている。

ネットにも大きな可能性がある。それは良い意味でも悪い意味でも言えることである。ネットを使う手段、方法、ネットを何のために使うのか、そういったもので明るい未来を切り開く力にも、暗い未来を導くものにもなる。

これまでネットの危険性ばかりを取り上げてきたが、ネットは寧ろ、良い面で使われていることの方が多いだろう。

二〇一一年、東日本大震災の起きた年、日本は復興への強力な支え合いから、『絆』という言葉が広く使われるようになった。ネットにはこのような人と人とを繋ぐパイプとして機能することがある。例えば、

使わなくなった物をこれから使おうと思っている人にあげようとするリユース（Reuse）の取り組みであったり、政治家等と言葉のキャッチボールができるようになったことで意見や要望が伝わりやすくなったり、と次々と新しい使われ方がされるようになっている。ネットはその使用方法をさらに増やしていき、より良いものへと変わっていく、大きな可能性を持った媒体である。

また、人間は古来より情報の虫なのである。知りたいという欲求は本能的な部分で発生する感情であって、抑えがきかない。そして、簡単に『知る』ことができる媒体が、すぐそばに存在しているのである。

しかし、その中には未だに闇めいた犯罪やトラブルが眠っているという間違いない事実も存在している。だからこそ私達は、この便利な媒体をただ漫然と使うのではなく、石橋を叩いて渡るかのごとく、慎重になって使っていくことが求められているのである。

参考資料

・警察庁―特集Ⅱ：安全・安心で責任あるサイバー市民社会の実現を目指して
第一節　サイバー犯罪の現状
http://www.npa.go.jp/hakusyo/h23/honbun/html/1-toku2_1_1.html
・内閣府―平成二五年度青少年のインターネット利用環境実態調査報告書
第Ⅱ部　調査の結果　第一章　青少年調査の結果
第一節　携帯電話の利用状況
http://www8.cao.go.jp/youth/youth-harm/chousa/h25/net-jittai/htm/2-1-1.html

平成二六年度懸賞論文

「ネット社会を安全に暮らす」の応募要項

1　テーマ

「ネット社会を安全に暮らす」とする。テーマ設定の趣旨は別記のとおりであるが、応募に当たっては、論点を個別的な問題に絞り込み、テーマをそれに応じたものに適宜変更することとして差支えない。

2　応募資格

特に限定しない。

3　応募規定

(1)　応募論文は、

○　パソコン（ワープロ）で作成する場合の書式はＡ４判縦（横書き）、三五字×三〇行、文字サイズは一二ポイントとし、そのまま打ち出すこと。

○　市販の原稿用紙を利用する場合は、Ａ４判、四〇〇字詰めとする。作成に当たっては、黒インクの筆記用具（万年筆、ボールペン等）を使用すること。また、書式は、横書きでも縦書きでもよい。

○　用語の統一、パソコン（ワープロ）利用による語句の変換ミスには留意願います。

(2)　原稿の総字数は八〇〇〇～一二〇〇〇字（統計、図、表は別）とし、必ず目次及び八〇〇～

一二〇〇字の要約を付ける。文字数は厳守のこと。

(3) 応募論文の表紙には、必ず次の事項を明記する。

○ 住所（フリガナ、郵便番号）
○ 電話番号（自宅・携帯電話、ＦＡＸ、e-mail がある場合は、番号やアドレスを明記する。）
○ 氏名（フリガナ）
○ 生年月日（年齢）
○ 性別
○ 職業等（勤務先、役職名又は学校名、学部、学年等）
○ 論文のテーマ（個別的な論点に応じたテーマで可。）

※応募論文が未発表のものであることを示すために、「この論文は、未発表のものである。」と明記する。

(4) 他の著書、論文等を引用した場合は、その出典を明記する。

(5) 応募は一人一編とする。

(6) 応募論文の著作権は公益財団法人公共政策調査会に帰属し、応募論文は返却しない。

4 締切り

平成二六年九月五日（金）（当日消印有効）

5　応募及び問合せ先

〒一〇二―〇〇九三　東京都千代田区平河町二―八―一〇　平河町宮川ビル内
（公財）公共政策調査会
電話　〇三（三二六五）六二〇一　ＦＡＸ　〇三（三二六五）六二〇六

6　発表及び表彰

(1)　平成二六年一二月中の読売新聞に入選者名を発表し、併せて入選者には直接通知する。また、最優秀論文については、平成二七年一月中の読売新聞にその要旨を掲載する。

(2)　原則として、最優秀賞一編、優秀賞二編、佳作数編を決定し、入選者には、次により賞状及び副賞を贈呈する。

・最優秀賞　一編　賞状及び副賞（二〇万円）
・優秀賞　二編　賞状及び副賞（一〇万円）
・佳　作　数編　賞状及び副賞（　五万円）

なお、優秀賞以上の受賞者には、読売新聞社から「読売新聞社賞」が贈呈される。

(3)　平成二七年一月中に授賞式を行う。

7　選考委員

・片桐　裕　（（公財）公共政策調査会理事長）
・小宮　信夫　（立正大学文学部教授）

・佐々木真郎　（警察大学校警察政策研究センター所長）
・鈴木　基久　（警察庁長官官房審議官）
・坂東眞理子　（昭和女子大学学長）
・前田　雅英　（首都大学東京法科大学院教授）
・宮崎　緑　（千葉商科大学政策情報学部教授）
・山腰　高士　（読売新聞東京本社社会部長）

（五十音順、敬称略）

8　共催

警察大学校警察政策研究センター

9　後援

警察庁、読売新聞社、（独法）情報処理推進機構

10　助成

（公財）日工組社会安全財団

「別記」「ネット社会を安全に暮らす」～テーマ設定の趣旨

情報化の進展は、社会全体に大きな利便をもたらし、インターネットは、多くの国民にとって、なくてはならないものとなっている。しかし、反面

○ウィルスによる個人情報や企業情報の流出
○インターネット・バンキングへの不正アクセス等による預金流出
○学校裏サイト等での特定の学校、個人への誹謗中傷、ネットの炎上
○殺人等ネット上での犯罪予告
○闇サイトでの覚醒剤等の販売、報復目的等からの犯罪仲間の勧誘
○ネット上へのわいせつ画像、児童ポルノ等の流出

など、その負の側面が顕著になっている。

最近、パソコン、携帯電話、スマートフォン等の安易な利用により、

○出会い系サイトで知り合った相手とドライブしたところ、強盗等の被害に遭った
○食品等の上に寝そべった写真をＳＮＳに投稿し、アルバイト先の飲食店が営業廃止に追い込まれ、損害賠償を請求された

○交際を断った相手が、交際中のプライベート写真を、報復としてネットに掲示した
○スマートフォンアプリをインストールしたら、端末の中の個人情報が流出した
など、危険に結びつく事案が、多数発生している。

このように、様々な危険が存在するネット社会において、女性、子供、若者をはじめとするネットの利用者が、被害者になったり、また、不適切な使用で加害者になったりすることがないようにしなければならない。そのため、利用者、保護者、教員や政府、自治体、ネット関連事業者、教育機関等は、どのような対策を講じるべきか、ネット社会を安全に暮らしていくための方策について、提言を求める。

平成二六年度懸賞論文「ネット社会を安全に暮らす」応募者一覧

（氏名・年齢・性別・職業・テーマ）

新井　光良（63）男・パート社員　企業とネット社会について
石田　勝啓（71）男・無職　ネット金融詐欺撲滅への取組について
伊藤　鈴香（46）女・警察官　インターネットを使う技術～大人が授けるべき知恵～
猪野塚久美子（59）女・主婦　インターネット基礎知識習得のための機会創出を提言する
上野　貴弘（36）男・警察官　ネット社会を安全に暮らす
～わいせつ画像の流出を防ぐためにできること～
大川　暁（37）女・主婦　ネット社会を安全に暮らすには何が必要？
岡部　達美（21）女・大学生　ネット社会を安全に暮らす
～ネットでつなぐ安心して暮らせる社会をめざして～
奥村　一美（54）女・美術商・芸術活動　ネット社会と日本人の癖
葛西　悠吾（23）男・大学院生　安全なソーシャルネットワーキング・サービスの利用のために
～若者の「炎上」問題と対策～

カラカヤあゆみ（44）女・無職

岸　昭利（55）男・警察官
久原　弘（55）男・高等学校教諭
栗原　佑介（28）男・大学院生
黒﨑　昇次（45）男・大学職員
児玉　真一（26）男・警察職員
後藤麻理子（30）女・警察官

齋藤　美帆（43）女・警察官
佐生　綾子（48）女・保育士補助（パート）
杉浦　邦彦（56）男・自営
鈴木　あい（23）女・大学院生
須藤　裕美（30）女・フリーライター

守る必要のない、闘う必要のない社会を目指して
～ネット上の犯罪やいじめから子供たちを救う～
ネット社会における認識力と危機管理
情報モラルを考える～標語創作をツールとした実践～
安全なネット社会のための「消去権」の実質的保障
子どもを守るためのネット安全教育とは
インターネット教育の必要性
複雑多様化するＩＴ社会で国民が安全に過ごすために
～インターネットのドレッシング的活用を模索する～
ネット社会を安全に暮らすための警察としての取り組み
便利は人を不幸にする
八分後に訪れる恐怖
中高生のネット利用と「炎上」
ＷＷＷ（ワールドワイドウェブ・世界に広がる蜘蛛の巣）の蜘蛛に捕らわれた現代～ネットのない社会でこそ安全に暮らせるということ～

田内　寛倫	（29）	男・警察官	ネット社会を安全に暮らす ～日本全体でのネット問題対応策～
高井　俊孝	（38）	男・地方公務員（警察官）	安全なネット社会を育てるために必要な教育
高尾　健一	（44）	男・警察職員	遠隔操作可能性分析～解析物件が遠隔操作されていなかったことを分析するために～
髙本　崇	（36）	男・警察官	個人と国家のサイバーモラル
竹中　利衣	（33）	女・警察官	ネット社会における子どもの安全を守るための五つの提言
館野　史隆	（43）	男・自営業	家庭教育のプロが教える「我が子とネットの正しい付き合い方」
寺田　高久	（59）	男・会社員	ネット社会を安全に暮らす「こころのフィルタリングへ…」
中津　正充	（48）	男・無職	ネット社会に安全は存在しない
二宮　秀太	（20）	男・大学生	サイバー犯罪情勢に即応するためのインターネット
野村　俊介	（36）	男・会社員	ホットラインセンターの改善提言
初野　皓紀	（21）	男・大学生	情報発信力の高まりによる危険とその対処
藤田梨恵子	（26）	女・大学院生	ネット社会を安全に暮らす～スマートフォンの落とし穴～
淵﨑　和樹	（29）	男・地方公務員（警察関係）	若者に対するネット教育の方法論 ＬＩＮＥの恐怖と対策予防方法

松尾　剛行　（30）男・大学院生
都田　潔　（34）男・会社員
森田　信明　（64）男・会社員
八木佳津子　（56）女・ウェブ制作
山﨑　浩子　（56）女・アルバイト
大和　操　（59）男・警察官
吉松　幸彦　（45）男・求職中
和田　大樹　（21）男・警察官

ネット名誉毀損の加害者にならないために
～批判的なレビュー記事を例として～
ネット社会を安全に暮らす
人間に優しいネット社会を作るために
ネット社会を生きる
豊かで安全なネット社会を築くために
ネット社会の暮らし方
現代日本の学校教育の陥穽と、教育の本来あるべきかたち、そして、それらに基づいた安心安全な社会構築のための提言
ネット社会を安全に暮らす三つのコツ

以上四二名

この懸賞論文募集事業及び論文集は、財団法人日工組社会安全財団の助成により実施し、作成されたものです。また、左記の企業のご支援を得ています。

あいおいニッセイ同和損害保険株式会社
アクサ生命保険株式会社
旭化成株式会社
安全サポート株式会社
イオン株式会社
ウシオ電機株式会社
鹿島建設株式会社
関西電力株式会社
九州電力株式会社
京セラ株式会社
近畿日本鉄道株式会社
株式会社クラレ
株式会社クレディセゾン
株式会社ゲームカード・ジョイコホールディングス
株式会社神戸製鋼所
株式会社小松製作所
株式会社ＳＡＮＫＹＯ
清水建設株式会社
昭和電工株式会社
新日鐵住金株式会社
住友化学株式会社
セイコーエプソン株式会社
セコム株式会社
株式会社セブン＆アイ・ホールディングス
セントラル警備保障株式会社
綜合警備保障株式会社
損害保険ジャパン日本興亜株式会社
大成建設株式会社
株式会社たいよう共済
株式会社大一商会
大日本印刷株式会社
中国電力株式会社
中部電力株式会社
株式会社電通

東海旅客鉄道株式会社
東京海上日動火災保険株式会社
東京ガス株式会社
東京地下鉄株式会社
東京電力株式会社
株式会社東芝
東武鉄道株式会社
東北電力株式会社
トヨタ自動車株式会社
名古屋鉄道株式会社
南海電気鉄道株式会社
西日本旅客鉄道株式会社
日産自動車株式会社
日新火災海上保険株式会社
株式会社日清製粉グループ本社
日本ガイシ株式会社
日本製紙株式会社
日本生命保険相互会社
日本電気株式会社
日本電信電話株式会社
野村ホールディングス株式会社
パナソニック株式会社
株式会社博報堂
阪急電鉄株式会社
阪神電気鉄道株式会社
東日本旅客鉄道株式会社
株式会社日立製作所
富士通株式会社
本田技研工業株式会社
三井住友海上火災保険株式会社
株式会社三井住友銀行
三井住友信託銀行株式会社
株式会社三菱東京ＵＦＪ銀行
三菱ＵＦＪ信託銀行株式会社
三菱電機株式会社
明治安田生命保険相互会社
森ビル株式会社
株式会社リコー
株式会社りそな銀行

平成二六年度懸賞論文
ネット社会を安全に暮らす
平成二七年二月発行　九〇〇部（非売品）
発行　公益財団法人公共政策調査会
〒一〇二―〇〇九三
東京都千代田区平河町
二丁目八番一〇号
電　話　〇三―三二六五―六二〇一
ＦＡＸ　〇三―三二六五―六二〇六
印刷　株式会社キタジマ
〒一三〇―〇〇二三
東京都墨田区立川二―一一―七
両国キタジマビル
電　話　〇三―三六三五―四五一〇

後援　警察庁
後援　読売新聞社
後援　（独法）情報処理推進機構
助成　（公財）日工組社会安全財団