

子どものネット利用に関する 新たな問題と対策

「加害者化」と「攻撃価値の増大」に対する備えを

鈴木良介



CONTENTS

- I 進む加害者化と攻撃価値の増大
- II フィルタリングを中心とした対策の進展
- III 携帯電話への期待とアウトバウンド情報制御の必要性
- IV 「後期子ども」「半分大人」である高校生への対策が急務

要約

- 1 子どものネット利用の進展に伴う新たな問題が生じている。すなわち、子ども自身の「加害者化」と急速な「攻撃対象としての価値の増大（攻撃価値の増大）」である。
- 2 「加害者化」としては、「オンラインゲーム会社を装い、ID（認証番号）・パスワードをだまし取った中学生が検挙される事例」などが見られる。また、不正アクセス禁止法違反事件において、被疑者に占める10代の子どもの割合は、2001年以降の5年間で3.9%から30.8%まで増加した。
- 3 「攻撃価値の増大」としては、子どもがパソコン、携帯電話を利用する割合の上昇や、情報発信型Webサービスの隆盛などの影響を受け、子どものプライバシーが悪意ある攻撃者の目にさらされやすくなっている。
- 4 現状、行政・業界団体が注力している対策は、子どもによる「安全な情報の受信」を目的としたフィルタリングサービスである。導入がなかなか進まなかった本対策についても、2006年末には総務大臣により導入促進の強化要請がなされるなど、本腰が入りつつある。
- 5 今後進めるべき対策としては、「後期子ども」「半分大人」である高校生への対策が急務である。これには、携帯電話を中心に年齢妥当性がより高いフィルタリングの導入を進めること、子どもによる「安全な情報の発信」を目的としたアウトバウンド・フィルタリング（情報の発信に対する制御）を進めていくことが必要と考えられる。

I 進む加害者化と攻撃価値の増大

1 ネット利用に伴う古典的問題、新しい問題

「中学二年生の男子がちょっとした性的な単語について検索をしたところ、とんでもなくグロテスクな画像をうっかり閲覧してしまい大変なショックを受けた」「一つ年上のメル友に会おうとした女子児童を迎えたのは太った中年男性で、さらわれそうになった」

インターネットにはこのような危険や不快な事象に満ち満ちており、無垢なる子どもたちは守られなければならない——このような主張は、インターネット普及の当初より広く叫ばれてきた。

インターネット利用上の古典的問題としては、年齢不相応な有害コンテンツの閲覧や、いわゆる出会い系サイトなどを通じて「悪い大人」と接触することが挙げられてきた。加えて、「被害者であると同時に加害者になる」ウィルス問題や、メールの書き方やプライバシー情報の不用意な開示といったリテラシー上のトラブルが指摘されてきた。これらの有害性はいずれも減ぜられるものではないものの、これに加えて新しい問題が生じつつある。

その第一として、子どもがれっきとした加害者になる事例の増加、第二として、子どもが保有・発信する情報を攻撃対象とした問題の増加が挙げられる。

2 子どもが加害者になる事例の増加

「子どもが加害者になる」事件は、インターネット普及初期の段階においても発生していた。コンピュータウィルスの再配布のような

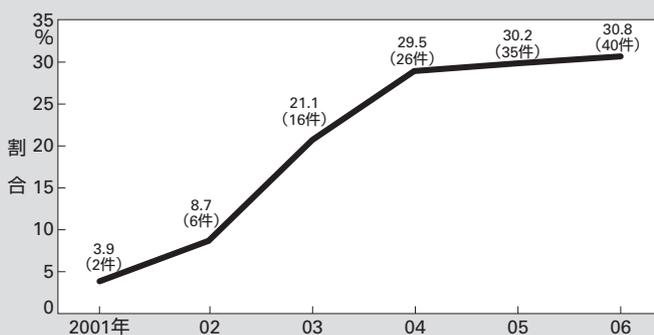
悪意なき加害行為は早い段階から多数指摘されていたし、インターネット上で得た有害情報に基づく違法行為（爆弾作成や毒物混入など）が行われる事件は、決して多くないものの、間欠的に見られた事案である。

そのような加害事案が依然として生ずる一方で、「れっきとした不正アクセス犯」として加害者になる子どもの割合が増加を続けている。不正アクセス禁止法違反事件において、被疑者が子ども（10代）である割合は、2001年には全被疑者中の3.9%（51人中、2人）であったが、2006年には30.8%（130人中、40人）まで増加している（図1）。

具体的な事例としては、「オンラインゲーム会社を装いID（認証番号）・パスワードを詐取した事例」（14歳：中学生）や、「アフィリエイト用ポイントを詐取しようとした事例」（15歳：高校生）、同じく「未成年のID・パスワードを詐取しオンラインゲーム上のアイテムを詐取した事例」（16歳：高校生）などがある。

背景には、幼少時からの情報機器利用率の上昇と、それに伴う技能の向上があり、そのうえで、不正行為のインセンティブとなる金銭的価値を有した情報を提供するサービスが、インターネット上で増加していることな

図1 不正アクセス禁止法違反にかかわる被疑者のうち10代の者が占める割合および件数



出所) 警察庁編「平成18年版 警察白書」ぎょうせい、2006年8月より作成

どが考えられる。また、不正アクセスの事例として、オンラインゲームにまつわるものが増加していることは顕著な特徴といえる。文献1

3 子どもの保有あるいは発信する 情報を攻撃対象とした事例の増加

オンラインゲームの存在は、「子どもが保有する情報の価値増大」の背景としても挙げることができる。前項で示したような単発での詐取行為の範疇を大きく超え、手当たりしだいにオンラインゲームのアカウント情報（ID・パスワード）の取得を行うことを目的としたスパイウェアが多く出現している。2007年度上半期に新たに発見された悪意あるコード上位50種類のなかにも、オンラインゲームのアカウント情報を攻撃対象としたものが含まれているとされている。文献2

侵害者は詐取したアカウント情報を用いて、ゲーム上の仮想通貨や重要アイテムを詐取し、最終的にはゲーム上の仮想通貨を現実の通貨に変換（リアルマネー・トレード：

RMT）して利益を手にするを目的としている。オンラインゲームに参加する子どもたちが保有するアイテムやゲーム内の通貨は、現実にも価値を持った攻撃上のインセンティブに足る情報なのである。

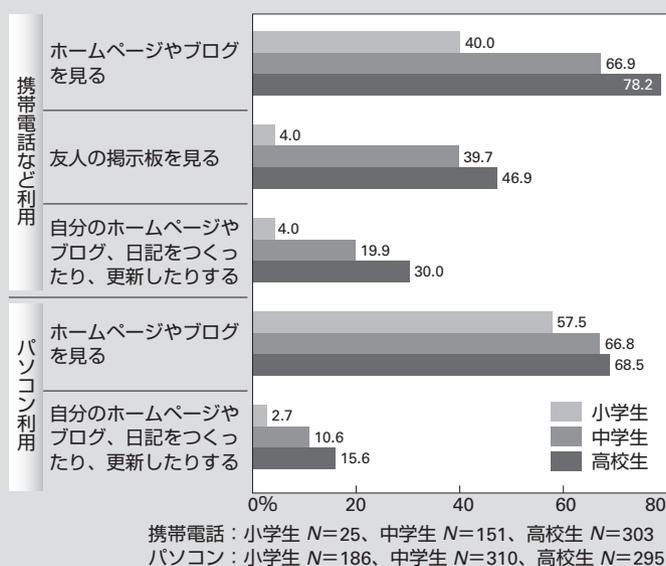
また、より直接的な危害につながりうる問題として、子ども自身のプライバシー情報が標的とされる事案も考えられる。「インターネットなどに不用意にプライバシー情報を公開するべきではない」ということは、インターネット普及と初期より繰り返し説かれてきたが、この点についても、子どもを取り巻く環境の変化を無視するわけにはいかない。CGM（消費者生成メディア）系サービスと呼ばれる、ユーザーが提供する情報を核とするサービスの増加である。

最も特徴的なサービスとしては、若年層を中心に利用率が高い「プロフ」サービスが挙げられる。プロフはプロフィールサービスを意味し、自己紹介を主たるコンテンツとして公開するものである。初対面の友達にプロフにおけるハンドルネームなどを伝えるといった、名刺代わりの用途で使われている。サービスによって詳細は異なるが、通常は無料で利用することが可能である。また、誰かのプロフを見るために特定の認証などは必要とされないことが多い。

具体的な記載内容としては、趣味、髪型、学校名、クラス、出席番号、居住地域、アルバイト先と出勤曜日、自分の顔写真、恋人と撮影したプリクラなど、かなり細かい情報が公開されているものも頻繁に見られる。

プロフほど極端なサービスではなくとも、近年のブログ、SNS（ソーシャル・ネットワーキング・サービス）の登場と流行は、子ども

図2 インターネットに接続された携帯電話、パソコンの利用目的



出所) 内閣府「第5回情報化社会と青少年に関する意識調査について (速報)」
2007年7月

もによる情報発信の促進に大きな役割を果たしている。インターネットにおける情報発信は中学生で約2割、高校生で約3割が実施しているという調査結果もある(図2)。^{文獻3}

情報発信環境が充実することに伴う多くの良い影響を否定はしないが、侵害者にとっては、攻撃対象となる子どもに関する大量の情報を入手する環境が整備されたともいえる。

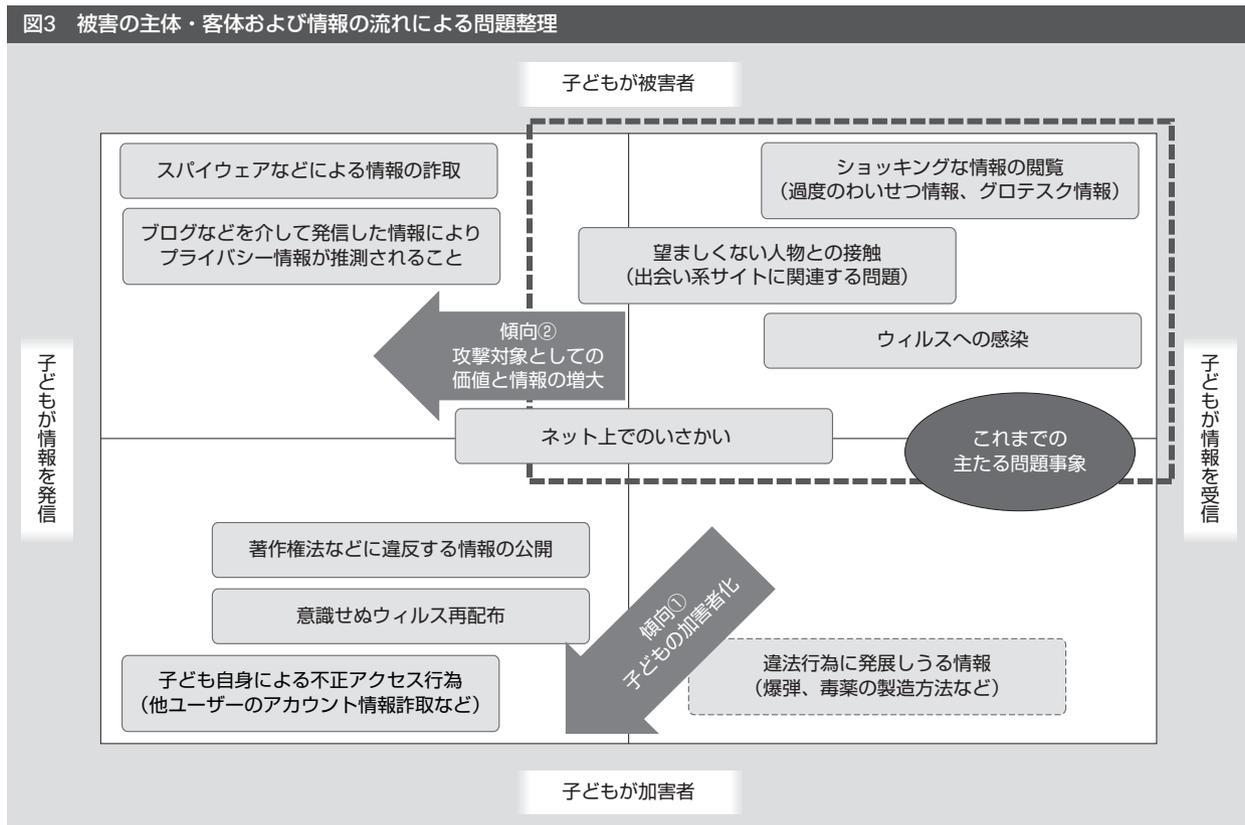
名前・住所・顔写真といった明確なプライバシー情報を自らが掲載していなくとも、蓄積された日記に含まれる断片的な情報や、掲載した一枚の風景写真からすらプライバシー情報が露呈する恐れはある。本人が注意していても、ブログへのコメント、トラックバックや、SNSサイトにおける友人の属性などから、執拗に情報が探り出される恐れもある。

結果として居住地や行動パターンが知られてしまい、つけ回されたり、身体的な危害を

加えられたりする恐れもあるだろう。そこまですらなくとも、知り得た情報をもとに心理的苦痛を与えるようなメールが繰り返し送りつけられることも考えられる。侵害者にはお手軽な嫌がらせにすぎなくとも、子どもの精神に甚大な悪影響を及ぼす可能性がある。

4 問題構造の整理

ここまで、子どもの「加害者化」および「攻撃対象としての価値と情報の増大」という二種類の問題が深刻化しつつある傾向を示した。ここで、有害コンテンツ問題など古典的な問題を含めた種々の問題事象の整理をする。「子どもが加害者となるか、被害者となるか」、および「子どもが情報を受信するのか、発信するのか」という2軸により整理すると、種々の問題は図3のように整理でき、上記の各傾向は図中に示した2つの矢印にし



て表される。

II フィルタリングを中心とした対策の進展

これらの問題への対策としては、制度的対応、教育的対応、技術的対応が考えられる。本章では、各事業者、行政機関などによってそれぞれどのような対応がとられているか、現状を概観する。

1 制度的対応

制度的対応としては、サービス利用上の規約の制定がまず挙げられる。

規約による対応として、事業者によるサービス利用上の年齢制限を実施している事例がある。代表的なSNSサイトでは、会員となるのに年齢制限を設けており、18歳未満のサービスの利用を禁止している場合がある。

制度的対応に関する先進的な事例として、リンデンラボが提供するサービス「セカンドライフ」において、厳密な個人・年齢認証サ

ービスがベータ版（試用版）として提供されていることが挙げられる。すべてのサービス利用に対して認証が必要とされるものではないが、同サイトにおける18歳以上限定のコンテンツをユーザーが利用しようとする場合には認証が必要となる。

米国のユーザーについては運転免許証、パスポート、国の発行する身分証明書、社会保障番号の下4桁などを用いて認証がなされるものとされている。^{文献4}

しかし、リンデンラボのように本人確認や年齢確認を厳格に実施しているサービスはきわめて少ない。多くは電子メールのアドレスさえ有効なものであれば利用できるサービスであり、年齢を詐称して利用した場合の処置としては、目立った問題事案に対して散発的に処分がなされているのが現状である。

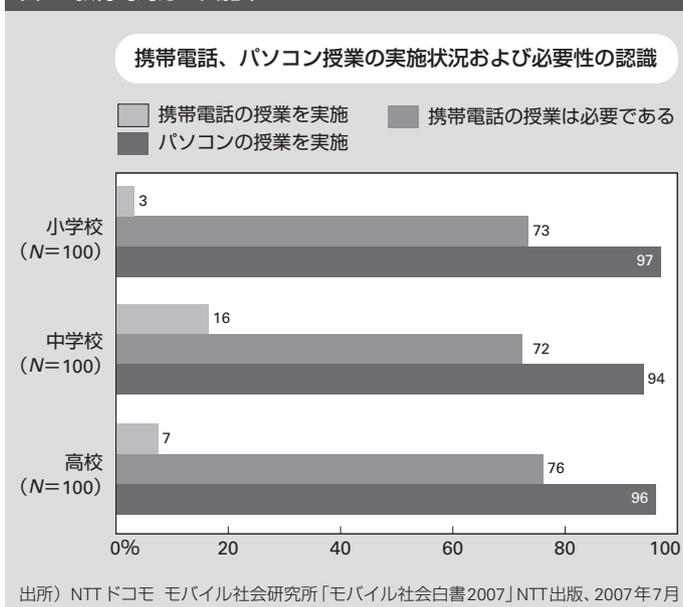
その他の規約による対応としては、ユーザーが記載する内容について、違法・有害情報の禁止はもとより、「登録個人情報の詐称」「他のユーザーが不快と感じる情報の発信」「個人のプライバシーに関する情報の発信」といった各項目を禁じ、違反した場合にはサービスの利用を停止する規約も、多くの事業者が定めている。

こちらも年齢詐称と同様、ある程度、トラブルが拡大・顕在化した際に各種の処分などがなされるのが現状であり、予防的な効果はそれほど大きくないと考えられる。

2 教育的対応

パソコンに関する教育は、小中高いずれも9割以上の学校で実施されている。内容についても、電子メール、インターネットの利用方法といった利活用方法に加え、情報モラル

図4 教育的対応の実施率



の必要性や、情報の収集・発信に伴って発生する問題・個人の責任についても、指導項目となっている。文献5

一方で、携帯電話については、学校教育の場ではパソコンほど取り組まれていない。生活指導の一環として行われることはあっても、機器の活用やモラル教育が体系的に実施されてはいないというのが現状である。

しかしながら、現場の教諭の認識としては「携帯電話に関する授業は必要である」とする意見が、小中高のいずれでも7割を超えている。また、その内容も、モラルや利用に伴う危険性を説く必要性が高く認識されている。しかし、実際の実施率は低くとどまっており、必要性を認識しつつも実施が進んでいない現状がうかがわれる（図4）。文献6

3 技術的対応

本節では、近年積極的に導入が進められているフィルタリング技術に注目する。

フィルタリングとは一般に、「定められた基準に従い、情報を選別すること」を意味する。また、狭義にはWebサイトの閲覧に伴う情報の選別に限定して使われることも多い。たとえば総務省などの定義では、「フィルタリングとは、インターネット上のウェブページ等を一定の基準で評価判別し、選択的に排除する機能のこと」とされている。

フィルタリングは、携帯電話、パソコン向けのいずれにも提供されている。先の問題整理に照らし合わせれば、本稿でいうフィルタリングによる対応は、有害情報などへの接触防止、すなわち子どもが情報を受信する際に生じる被害に対して、特に有効な対策であるといえる。

(1) 携帯電話利用におけるフィルタリング

まず、携帯電話利用におけるフィルタリングの現況について概観する。各携帯電話事業者は2003年以来、「携帯電話向けフィルタリングサービス」（表1）としてサービスを提供してきているが、認知率・利用率はそれほど高くなかった。2006年末時点での携帯電話保有者のうち、フィルタリングを「使っている」と回答したのは中学生で0.8%、高校生では1.1%である（次ページの図5）。

しかし、2006年末以来、携帯電話におけるフィルタリングについて、行政および業界による対応が強く進められている。2006年11月に、総務大臣によるフィルタリングサービス促進強化要請がなされたことを受け、各事業者は新規契約時にフィルタリングサービス契約を推進する体制を強化した。具体的には、親権者へのフィルタリングソフト導入に関する意思確認や、代理店等への指導強化を求めることなどが挙げられる。文献7

表1 各携帯電話事業者によるフィルタリングサービスの概要

事業者	サービス名	概要
NTTドコモ	• キッズ iモードフィルタ • iモードフィルタ • 時間制限	フィルタリングをレベル別に2種類用意。加えて、深夜・早朝時間帯のアクセスを禁止する時間制限サービスの提供も行っている
KDDI (au)	• EZ安心アクセスサービス • EZweb利用制限	アクセス可能なコンテンツだけをリストアップした専用メニューが、トップページとして表示される
ソフトバンクモバイル	• ウェブ利用制限	アダルトサイトや出会い系サイトなど、「特定のURL」へのアクセスを制限する

注) URL: ユニバーサル・リソース・ロケータ
出所) 各携帯電話事業者Webサイトの情報、および問い合わせ窓口への問い合わせにより作成

加えて、2007年2月には総務省、警察庁、文部科学省が合同で都道府県教育委員会ならびに都道府県警察に対して、フィルタリングの普及促進に関する依頼を実施している。^{文献8}

(2) パソコン利用におけるフィルタリング

次にパソコン利用におけるフィルタリングである。これは2種類に大別される。1つはインターネット・サービスプロバイダー(ISP)などが提供するフィルタリングサービスを利用する方法であり、もう1つは購入したソフトウェアをパソコンにインストールする方法である。ISPなどによるサービスの場合、携帯電話事業者の場合と異なり、月額数百円程度の価格が設定されている例が多い。ソフトウェアを購入し、それぞれのパソコンにインストールして利用する場合には、

数千円程度要するのが一般的である。

サービスにせよソフトウェアにせよ、いくばくかの費用は発生するものの、細かいフィルタリング設定などができる機能は魅力的といえる。小学生向け、高校生向けなど、妥当と考えられるフィルタリング設定群を基本設定とするソフトウェアも提供されている。

Ⅲ 携帯電話への期待とアウトバウンド情報制御の必要性

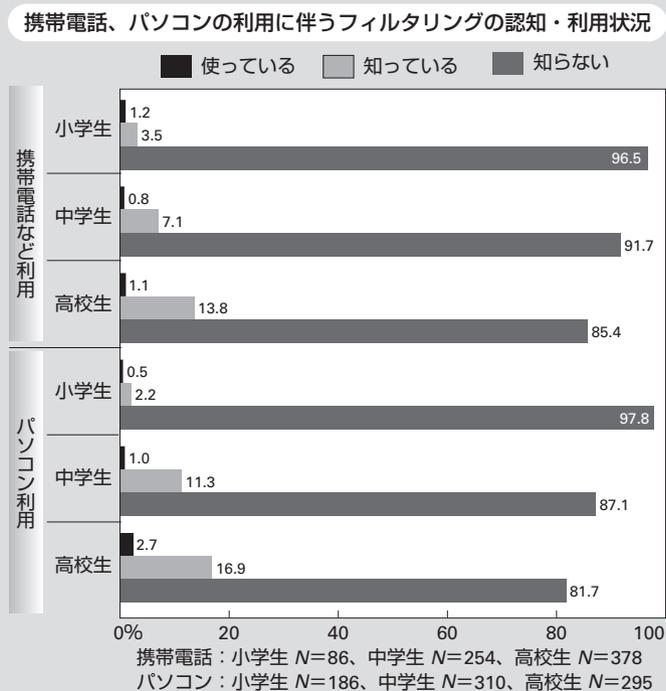
1 安心デバイスとしての携帯電話への期待

子どもが携帯電話およびパソコンを利用してインターネットに接続する割合は、いずれも年齢を重ねるごとに利用率が高まるが、それらの増加率は大きく異なる。小学生ではパソコン利用率が携帯電話利用率を大きく上回っているが、高校生になるとその数字は逆転する(図6)。

子どもの携帯電話利用率が高まるにつれて、「子供が安心して使える」ことに機能特化した携帯電話端末が各事業者により販売されている。具体的に製品化されているものとしては、防犯用ベルや端末の位置確認機能などが付与されているものが挙げられる。このような端末は、特に低年齢層の子どもにとっては物理的な安心・安全のために重要な役割を担いつつある。

携帯電話を介した情報の取り扱い上の問題についても、前述のとおり、設定したWebサイトにだけ接続できるフィルタリング(ホワイトリスト型フィルタリング)や、夜間接続の禁止など、かなり強力なフィルタリングサービスが標準で組み込まれており、低年齢

図5 フィルタリングの利用率



注) 回答は複数回答であり、「使っている」と回答したものは「知っている」と回答したものと重複している。それぞれの機器を利用している人が回答
出所) 内閣府「第5回情報化社会と青少年に関する意識調査について(速報)」2007年7月

層の利用にとっては、有用かつ妥当なサービスになりつつあると考えられる。

一方で、中高生（特に高校生）に対して小学生と同様のフィルタリングサービスを提供することは、親子間に利用ポリシーに関する壮絶かつ不毛な議論を巻き起こすことが予想される。結果として、親側が折れ、「フィルタリングはなし、定めるルールは利用額の上限のみ」という状況になっているのが現状における多勢であろう。

多くの中高生にとって、現状で最も重要なデバイスは携帯電話端末であると考えられる。また、普及率も高い。このような需要度の高い普及デバイスが必要最低限の安全性（たとえば、国内で出版できないような有害情報の除外）を保障したうえで、彼らにとって「ほとんど不満がないデバイス」であり続けることは、きわめて有意なことである。

現状、携帯電話におけるフィルタリングの設定は、一部の事例を除き小学生を中心とした「お子さま向け」に限定されているといっても過言ではない。今少し年齢妥当性の高いフィルタリングを選べるようにすることは、子どもにとっても事業者にとっても、社会全体にとっても有意義であると考えられる。

付記すれば、現状は確かに携帯電話が最も重要なデバイスではあるが、「携帯可能でインターネットへ接続できる」デバイスであれば、同様の問題は生じうる。近年、携帯用のゲーム機器に加え、携帯音楽プレーヤーについても無線LANなどを介したネットワーク接続への対応が進んでおり、そのような状況に鑑みると、これらのデバイスについても今後、現状の携帯電話に対するものと同様の注意が必要になると考えられる。

2 アウトバウンド情報に対する制御強化への期待

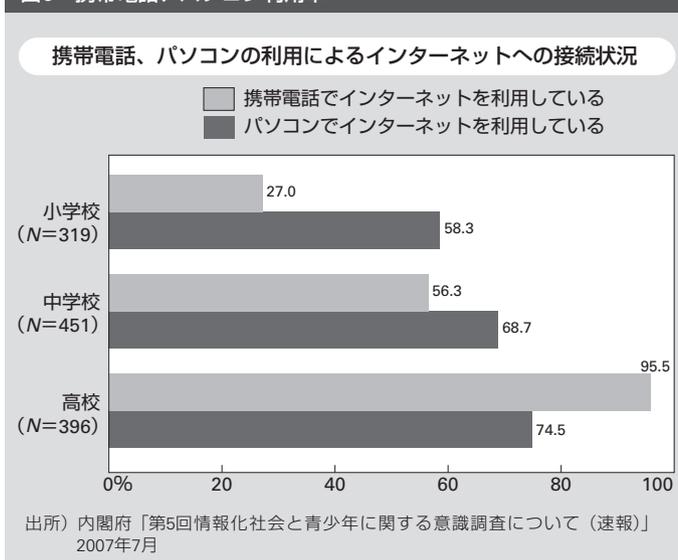
(1) インバウンド・アウトバウンド、両フィルタリングの併用が求められる

冒頭で「子どもの加害者化」および「攻撃対象としての子どもの価値増大」といった問題が隆盛しつつあることを述べた。

これらの問題はいずれも、「子どもによる情報発信」と密接な関係にある。前者は他者を欺くような情報を発信することにより子どもが加害者となるものであり、後者は自らのプライバシーに関する情報などを不用意に発信することによって、子どもが攻撃の対象として価値を増大するものであるからだ。

現状の対策として前述したフィルタリングは、厳密にはインバウンド・フィルタリングということができる。これは「子どもにとって不適当な情報や人が集まっているWebサイトに子どもを寄せ付けない」という考え方に基づく機能である。この機能はきわめて重要なものではあるが、今後はこれだけでは不十分、あるいは過度に利便性を減少させることになりかねない。

図6 携帯電話、パソコン利用率



5年前に「ユーザーからの情報投稿を可能とするようなサイトへのアクセスを禁止」とされたとしても大きな問題ではなかったろうが、CGM全盛の今日にそのような対応を取られれば、ほとんどのサイトは閲覧不能になってしまうだろう。

この流れが加速し、今後ますますCGM系のサイトサービスが増大することを考えると、「CGMサイトを閲覧することは差し支えないが、不用意に情報を発信することは制御する」といった対策を施すことが求められるようになるだろう。すなわち、これまでのインバウンド・フィルタリングに、情報発信を制御・選別するためのアウトバウンド・フィルタリングを併用することが必要になると考えられる。

(2) 安全性と利便性のバランスが取れたアウトバウンド・フィルタリングが必要

インバウンド・フィルタリングの導入が現在急速に推し進められていることは前節で述べたとおりである。この対策が進めば、子どもが受信する不適切な情報（インバウンド情報）に対する制御については、大幅な改善が期待できよう。

一方、アウトバウンド・フィルタリングについては、現状の各製品・サービスとも、あくまでインバウンド情報制御の補完という位置づけにとどまっている。

代表的なフィルタリングソフトの多くは、アウトバウンド向けの制御機能を何らかの形で備えてはいる。具体的には、「氏名、クレジットカード番号などのプライバシー情報をあらかじめ登録しておけば、該当文字列を含む書き込みを制御する」といった機能であ

る。このような機能は「親しか使わないはずのクレジットカード番号」など、絶対に入力されては困る情報に対しては有効だ。また、家庭でのルール上、プライバシー情報の入力を一切禁止する場合にも、有効なツールであるといえる。

しかし、安全性と利便性のバランスを考えた場合、「一切禁止」というのは安全性に偏りすぎた対策である。現実的には利便性を保持するべく、「このサイトならば、この種の情報の入力は控えるべき」といった、入力内容と入力先サイトのバランスを勘案した制御が行われることこそ望ましい。さらにいえば、メッセージの送り先（一般に広く公開されるのか特定の人へのメッセージなのか、その特定の人物は友人なのか初見の人なのか）までも踏まえて制御を行ってくれるような機能が備えられていれば理想的だ。

今後は、情報の入力先サイトの信頼性とともに、情報入力の許可・制限を実施する機能や、書き込み内容の文意を機械的に判断して警告を出すような、高度なアウトバウンド・フィルタリングの提供が期待される。そのような機能が提供されるようになれば、子どもが他者になりすましているかのような不適切な文面の場合には警告を出す、といった用例も考えられる。技術的には企業における情報漏えい対策などとも関連するところであり、今後の研究開発の進展を注視したい。

IV 「後期子ども」「半分大人」である高校生への対策が急務

安全性と利便性は一般にトレードオフの関係にある。「いかがわしいインターネットの

利用などは一切禁止」という家庭のルールを定めることは、その時点における安全性を最大にし、利便性を最小にする対策といえる。

子どもが小学生程度のうちは妥当な対策かもしれないが、高校生に同様の対応をすることは、2つの点で望ましくないだろう。第一にインターネットというきわめて有用な情報源を活用する機会を失わせてしまうこと。第二には、完全に禁止されると禁止されたデバイスを放棄し、管理が行き届いていない端末を探して逃げ込むことが予想されるからだ。

「後期子ども」「半分大人」である高校生への対策を考える際には、「子どもが利用することを望み、かつ親による制御が比較的効きやすい」携帯電話端末において、子どもの成長段階に応じた安全性と利便性を与えることが求められる。携帯電話に対して過度ではない、年齢相応な対応を行うことにより、無管理状態のデバイスに逃げ込むことへの抑止効果が期待される。

加えて、これは携帯電話、パソコンの双方に共通していえることであるが、アウトバウンド情報の監視・制御を行うことにより、子どもが加害者・被害者のいずれになることも防ぐことが求められる。繰り返しになるが、インターネット上には情報発信を促す魅力的な仕組みが数多く存在し、今も増え続けている。子どもがたぶらかされたり、まして子ども自身が他人をたぶらかしたりすることがないよう、情報の確認が行われるべきである。

進展めまぐるしい情報技術の世界では、問題の発生と対策がイタチゴッコとなってしまうのは、ある程度やむをえない。しかし「子どもがネットを利用するとどうということにな

るのか」と尋ねられたときに、かどわかしたりかどわかされたりといった話しか想起できないというのはあまりに悲しい。

できる対策を着々と進め、考えられる予防策はできるかぎり打ち、そのうえで「子どもがネットを利用するとこんなにハッピーな世界になる」という明るい道筋を示していくことが、大人の責務であろう。「お父さんはよくわからないから、よく考えて使いなさい」などといっている場合ではないのである。

参考文献

- 1 警察庁編『平成18年版 警察白書』ぎょうせい、2006年8月
- 2 シマンテック「インターネットセキュリティ脅威レポート12号」2007年9月
- 3 内閣府「第5回情報化社会と青少年に関する意識調査について（速報）」2007年7月
- 4 Linden Lab "Press Release: Linden Lab Introduces Identity Verification to Second Life," August 29, 2007
- 5 文部科学省「新学習指導要領（改正版）」2003年12月
- 6 NTTドコモ モバイル社会研究所『モバイル社会白書2007』NTT出版、2007年7月
- 7 総務省「報道資料：有害サイトアクセス制限サービス（フィルタリングサービス）の普及促進に関する携帯電話事業者等への要請」2006年11月20日
- 8 総務省、警察庁、文部科学省「報道資料：携帯電話におけるフィルタリング（有害サイトアクセス制限）の普及促進について」2007年2月16日

著者

鈴木良介（すずきりょうすけ）
情報・通信コンサルティング部副主任コンサルタント
専門は情報セキュリティ