

オーストラリアにおけるオンラインコンテンツ 共同規制体制と子どもの保護

香 取 淳 子

The Online Co-Regulatory Scheme and Protection of Children in Australia

Atsuko KATORI

Abstract: The Internet is a powerful tool for developing students' communication and information skills. Several statistical researches revealed almost parents of students thought the Internet effective to their children's study. But in relation to their children's Internet use, parents were worried about online pornography and their children's sexual relationship with strangers. In this paper, Austration co-regulatory scheme for the Internet content was investigated in detail and found it a second best for prohibiting students' inappropriate online behaviors. In conclusion, protection of children from the Internet content is thought to be achieved through public education and parental guide, not censorship.

はじめに

インターネットは生徒のコミュニケーション能力や情報技能を高めるための強力な教育装置である。だが、オーストラリアでの統計調査の結果を見ると、ほとんどの親はインターネットが子どもの学習におおいに寄与していると考えている反面、オンラインポルノへの接触、インターネットで知り合った大人との交際などを危惧していることが明らかになった。そこで本稿では世界でも厳しいといわれるオーストラリアのインターネットコンテンツ規制に焦点を当て、その特性を明らかにするとともに生徒の不適切なオンライン行動を阻止し、インターネットコンテンツから保護することの意味を考察することにした。

1) 統計でみる10代のネット利用の実態

(1) 教育装置としてのネット利用

06年1月、OECDは03年に実施した学習到達度調査（PISA：Programme for International Student Assessment）の結果に基づき、新たな分析結果を公表した。それを見るとオーストラリアの場合、生徒の100%が学校でコンピュータを使い、90%がインターネット利用者を信用していると答えており、世界でもトップクラスのネット利用者であることが明らかにされた。そこで、PISAの調査結果に基づいた分析の中の「生徒は技術主導で展開される豊かな世界で生きていく準備ができているか？」と題された項目から、オーストラリアの若者のネット利用に関する知見を抜き出してみると、以下のようなことになる。

- ・ 94%の生徒は家庭のコンピュータを使って学校の宿題をしている（OECDの平均は79%）。

- ・ 70%の生徒はワープロソフトを頻繁に使っている (OECD の平均は48%)。
- ・ 10%の生徒は教育ソフトをよく使っている (OECD の平均は13%)。
- ・ 74%の生徒は人物やモノ、考えに関する情報を検索するためインターネットをよく使っている (OECD の平均は55%)。

オーストラリアの若者は OECD 加盟国の若者の平均よりもはるかに多くコンピュータやネットを利用し学習に活用させている反面、教育ソフトを活用することが少ないことが判明した。OECDはこの調査結果に基づき、家庭での利用頻度の差異は家庭環境に由来するものであり、そこには社会経済的要因が関与していると指摘する。生徒が定期的にコンピュータを利用すれば学習効果もあがることが明らかにされており、とくにオーストラリア、ベルギー、ドイツ、韓国、スイス、米国でこの傾向が顕著であるとされている。

実際、ABA (放送を管轄する政府機関であり、2005年に ACMA に統合) と NetAlert (インターネットを安全に利用することを推進する政府機関) によって実施された調査研究 (2005) でもそれが間接的に確認されている。

ABA と NetAlert による調査結果 (2005) からインターネットに対する親の見解を見ると、上位から順に、「学校の勉強に役立つ」(76%)、「娯楽を提供」(35%)、「友だちや親といつでも接触できる」(16%)「研究技能を発達させる」(8%)「コンピュータ技能を発達させる」(4%)「ものごとの解明や発見を奨励する」(3%)であった。子どもたちがインターネットを利用することで知的能力が発達し、学校の勉強におおいに役立つと考えている親が多いことが明らかになった。子どもの年齢別で見ると、10-11歳、12-13歳の生徒の親がそのように考える傾向が高い。

質問紙調査と併行して実施されたケーススタディでも、インターネットは偉大な道具だと認識を示す親が多かった。たとえば、ベンディゴに住む13歳の娘の親は世界のことを知ろうと思ったらインターネットでわかるといい、メルボルンに住む12歳の娘の親もインターネットはすべての人に開かれた情報源だといっている。つまり、インターネットは誰にも開かれた情報装置であり、子どもが自発的に学習するための学習装置としてきわめて優れていると多くの親は認識しているのである。

(2) ネット利用に伴う課題

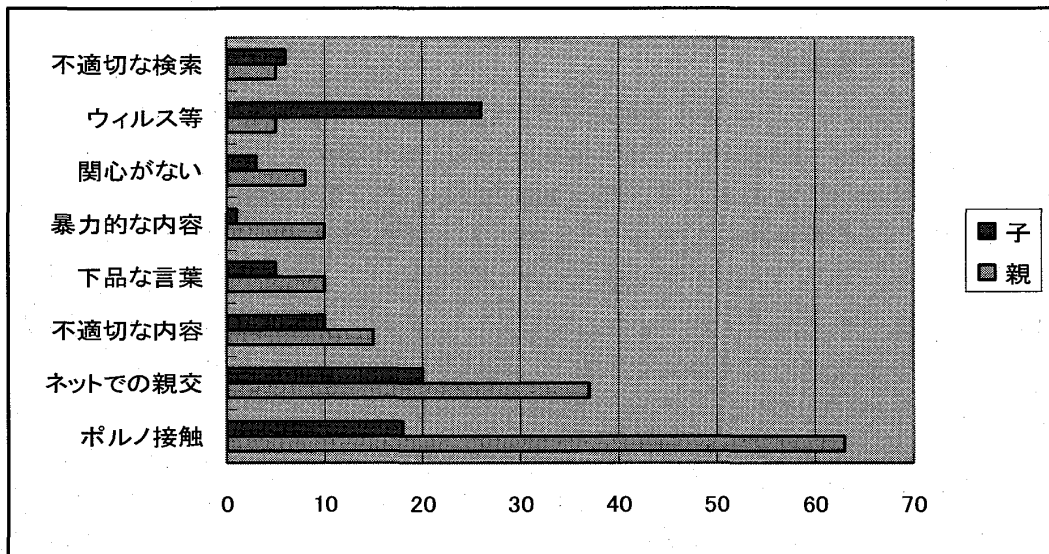
もちろん、インターネットにアクセスすれば子どもはさまざまな危険にも遭遇する。ABA と NetAlert による調査結果を見ると、親がとくに心配するのはポルノ情報への接触、ネットで知り合った人との交際、その他の不適切な情報への接触、等々である。だが、これらについては親と子どもの間に大きな認識の違いが見られる。

図1に見られるように、親はポルノ情報への接触やネットで知り合った人との交際を心配するが、子どもはそれほどでもない。子どもが心配するのはコンピュータに侵入してくるウィルスやハッカーであるが、親はそれにはほとんど関心を示さない。

このような認識の違いがさまざまな問題を引き起こしている。とりわけ深刻なのは子どもたちがネット上で知り合った大人と実際に親交を深め、性的な被害を被ってしまうことである。インターネットの普及とともにこの種の事件が増大し、いまなお減少してはいない。

たとえば、小児性愛者たちは友だちもいず、孤立している子どもを狙うといわれる。既述したように多くの子どもたちはネット利用者を疑っていない。だからこそ、子どもたちは無邪気にもネット上で心のうちをさらけ出してしまうのだが、その結果、彼らに親交の糸口を与え、いつしかその術中に陥ってしまう。そして何の危機感もなく実際に会ってしまったが最後、多大な被害を被ることになるのである。あまりにも無防備な子どもたちがいかに多いことか。その対策の一

図1 ネット利用に際しての関心事



資料：kidsline@home, ABA & NetAlert, p.38(April 2005) より作成

つとしてNetAlertはホームページ上で小児性愛者たちの多くがネットを利用して何をしているのか、一連の行動を列記し注意を促している (<http://www.netalert.net.au/>)。

- ・ 親交を形成する段階－小児性愛者がネットでターゲットとなる子どもと出会う。
- ・ 関係を形成する段階－この時点で小児性愛者は子どもの信頼感を得るようになる。
- ・ リスクを査定する段階－さらに親密な関係を形成するにはどの程度のリスクがあるのか、小児性愛者はその子どもに関する種々の情報を収集する。
- ・ 排他的段階－この時点で小児性愛者はその子どもとすでに「最高の友だち」としての堅い絆を形成している。
- ・ 性的段階－小児性愛者は子どもとの会話を性的なものに移し、オンライン上で性的行動に誘う。

こうしてみると、小児性愛者たちは段階を踏んで子どもを取り込んでいることがわかる。まず、名前も年齢も性別も偽ったまま情報のやり取りができるチャットルームを利用し、孤立している子どもを捜す。そして、周到的な準備を積み重ね、狙い定めた子どもに会う手筈を整える。子どもを準拠集団から心理的に切り離し、警戒心を解き、性的情報に馴染ませた上で実際に会い、やがては性的に搾取していくのである。子どもが実際に事件に巻き込まれるのは上記に記したようないくつかの段階を経た結果であるが、それぞれの段階でインターネットが関与している。

学校や家庭に不満を持つ子どももいれば、孤立している子どももいる。そのような子どもたちは救いを求め、友を求めてもう一つの社会空間であるインターネットに向かう。そこにもコミュニティがあり、顔を合わせることなく気軽に心情を吐露することができるからだ。現実社会に馴染めず、孤立している子どもほどインターネットを唯一の居場所にしがちである。そして、現実世界では得られない心の友をネット上で得たと思ったら、実は名前も年齢も性別すら偽った小児性愛者であったという悲劇が繰り返されている。だからこそ、オーストラリアでは連邦警察が特別チームOCSET(Online Child Sex Exploitation Team)を結成し、とくにチャットルーム、ウェブサイト、ショートメッセージなど子どもが事件に巻き込まれるきっかけとなるような場を取り

締まっている。

(3) オンラインの安全調査

05年12月、『十代のためのオンライン安全調査』(Online Safety for Teens survey)がインターネットポータルサイトの ninemsn (<http://ninemsn.com.au/>) と NetAlert (<http://www.netalert.net.au>) によって実施された。16-18歳の生徒とその親を対象に実施され、有効回答者は生徒が8918人、その親が3490人であった。ほとんどの親はインターネットを教育装置として高く評価していたが、その一方で小児性愛者やポルノグラフィーに子どもたちが接触してしまう危険性に強い不安感をかきたてられていた。とくにインターネット利用の多い子どもの親にその傾向が見られた。子どもが10代後半にもなると、親は子どものネット利用を管理しきれず、そのこともまた不安感をかきたてられる要因になっていると思われる。

実際、この調査では40%の子どもが「ネットで出会った人と会うかもしれない」と回答したが、そのうちわずか12%しか会う前に親に許可を求めると回答していない。また、男子生徒の43%は親に知られたくないネットコンテンツをダウンロードしたと回答し、63%が親の許可なくネットからファイルをダウンロードしたと回答した。親が知らないまま子どもがネット空間ではさまざまなオンライン行動を取っていることがわかる。

実は2001年に ABA が家庭でのインターネット利用について調査(回答者は11歳から17歳までの192人)を実施している。ネット上で不快なコンテンツを見たことがあるかどうかについての質問に対し、47%が暴力、ポルノグラフィー、裸体などの不快なコンテンツを見たことがあると報告した。不快なコンテンツのうち圧倒的多数がポルノグラフィーであった。この結果からはネット利用によって子どもは望ましくない性情報に晒されることが多く、それに付随して現実世界での性規範や性道徳の乱れが生じているのではないかと思われる。

はたして親は子どものオンラインでの行動をどの程度、管理しているのだろうか。『十代のためのオンライン安全調査』によれば、80%の親が子供のネット利用に際し基本原則を設けていると回答しているが、69%の子どもしかそのようなルールが設定されていると答えていない。また、71%の親は情報検索を目的に子どもはインターネットを使っていると思っているが、実際にはこの目的のためにインターネットを利用しているのは23%でしかなかった。さらに、84%の親は子どもと一緒にインターネットをしていると答えたが、24%の子どもはインターネットをしているとき、親はそばにはいなかったと答えている。このようにほとんどの項目で親と子どもの回答の数値に隔たりが見られた。この結果からは子どものネット利用を親は把握しきれず、管理するのはきわめて難しいことが明らかになった。

(4) 子どものネット利用と親の管理

05年11月、フリンダース大学が南オーストラリアで13歳から17歳までの114人の子どもとその親を対象に調査を実施したが、やはり同様の結果を得ている。たとえば、62%の親が子どものチャットルーム利用については専門的なガイドと支援が必要だと回答していたにもかかわらず、56%の子どもはチャットルーム利用について親は何もいわないと答えた。親の指導と支援を得ていると答えたのはわずか18%であった。

チャットルーム利用については興味深いことに、子どもの性別により親の回答に違いが見られる。親はほとんど関心を抱いていないと答えたのは女子生徒が43%であったが、男子生徒は76%であった。チャットルームを通して性的被害に遭いやすい女子生徒の親の方が危機感を抱くからだと思われる。この結果からは子どもの性的被害には性差がきわだっていることが示唆されてい

る。だが、この調査結果からも全般に親が子どものネット利用に関心を寄せることは少ないことが明らかにされており、親が子どものネット利用を管理するのはきわめて難しいのが実態だと考えられる。

一方、回答者の7%が暇さえあればインターネットにアクセスすると回答しており、嗜癖症ともいえるほど接触率の高い者がいることが判明した。回答者の平均的なインターネット利用は週当たり13時間に及んでおり、テレビに迫るほどの接触時間である。いまやインターネットは若者にとっての基幹メディアになりつつあるといえるが、これまで見てきたように、親が子どものネット利用を把握しきれず管理もできないのが現状である。

先述の『十代のためのオンライン安全調査』によれば、世帯主の98%がネット利用に関する費用を家庭の必要経費と考えていることが明らかになった。だが、925人の回答者のうち、21%がコンピュータウイルス、14%がクレジットカード詐欺、6%がプライバシーの侵害を心配していた。必要経費として扱われているのにインターネットはまだ安心して利用できる状況になっているとはいいがたいのが現状である。

さて、成長過程にある子どもに対してとりわけ配慮しなければならないのがネットコンテンツである。

ACTF(Australian Children's Television Foundation)は1982年に設立された非営利の機関であるが、子ども向けの映像音響コンテンツやオンラインコンテンツの質を高め、適切性を向上させていくことを目的に業務展開をしている。そのACTFは望ましくないコンテンツから子どもを保護するにはなによりもまず親や養育者の監視が欠かせないとする。子どものネット利用を技術的手段で監視するのではなく、養育者の目で見守るのが大切だというのだが、実際には親がいつも子どものネット利用を見張っているわけにはいかない。だから、現実的な対策として子どもが利用するパソコンにフィルタリングソフトをインストールすることをACTFは奨励する。現時点では必ずしも完璧なものではないが、やがては改良されていくだろうと期待し、オンラインコンテンツを技術的に選別するソフトを取り入れることを推奨するのである。

『十代のためのオンライン安全調査』では38%の家庭でパソコンに児童保護ソフトをインストールしていることが明らかになった。だが、このような保護ソフトを導入しているのは年間所得が10万ドル以上の家庭に限られており、ネット利用に関する安全保障には親の社会経済的階層性が深く関与していることが明らかにされた。この点からはコンテンツ規制になんらかの公的な措置を取る必要があるのではないかと思われる。

2) オンラインコンテンツ規制

(1) コンテンツ規制の体制

オーストラリアの場合、オンラインコンテンツ規制は政府と業界、コミュニティとの共同規制を展開している。これは政府機関であるABA(現ACMA)、ISP(Internet Service Provider)やICP(Internet Content Provider)などの業界、そしてコミュニティの3者が共同で不適切なインターネットコンテンツを規制して子どもを保護していこうというもので、オーストラリア独自の体制である。

グレインガー(Grainger, G., 1999)はこのような体制に至った背景には3つの出来事があったと説明する。すなわち、ABAによって実施された二つの調査(1995年, 1997年)と政府による規制原則の公表(1997年)である。

ABAが実施した1回目の調査結果から、1. ISPに対する施行規約の作成、2. オンライン環境下で子どもを保護するためのコンテンツ分類の役割を考える対策委員会の設立、3. コミュ

ニティの教育戦略の開発, 等々が新たに必要だということが判明した。

一方, 政府は1997年7月, 「オンラインサービスに対する規制枠組みの原則」を公表した。オンラインコンテンツに対する規制モデルはテレビや映画に対する既存の規制モデルよりも制約が少なかったが, これはネット利用を推進するための政府の意図が大きく反映されたものといえる。この原則の下でオーストラリア連邦政府がISPを規制し, 州と準州がICPを規制することになった。

ABAは2回目の調査を行いながら, ネット産業, 政府の関係省庁, 内外の教育やコミュニティ組織, 等々との連携を深めた。そして, ネット環境下での子どもの保護に関する問題を考え支援する対策委員会 (Children Content Online Task Force) を設立する一方, 国内で違法コンテンツが見つかった場合, 苦情処理をどうするかを考えるワーキンググループの設立にも関与した。そのためABAは国際インターネットコンテンツ評価連盟に参加し, 国際レベルでの関連作業にも関与し続けたのである。

1998年9月, ABAはソウルで開催されたユネスコのアジア太平洋地域会合に参加し, ユネスコがサイバー空間の法的枠組みを作成することを求め, そこにユニバーサルな原則を盛り込むことを推奨した。そして, モンテカルロで開催された会合ではこの提案が上程されたのである。

1998年11月27日, NOIE (National Office for the Information Economy) はオンラインオーストラリア・デイを大臣の名の下で開始した。情報経済の重要性を全国に幅広く告知するためである。また, ABAはネット利用の家族向けガイドをウェブ上に作成し, もっとも効果的で生産的な方法でネット利用ができるようにした。安全にネット利用を推進することで国家的教育戦略の実現にも寄与したことになる。ABAは1998年12月に最終報告書を提出した。こうして万端の準備が整ったところで1999年, オンラインサービス法が制定された。成立に至る経緯をまとめると以下のようなになる (表1)。

表1 オーストラリアのコンテンツ共同規制体制の設立をめぐる経緯

年月日	事 項
1995年7月	通信・芸術大臣がABAにインターネットを含むオンライン情報および娯楽のコンテンツの調査を指令。
1996年6月	ABAは大臣に調査報告書を提出。
1997年7月	通信・芸術大臣と法務大臣が共同で「オンラインサービスの規制枠組みの原則」を公表。通信・芸術省に提出された原則に関する提案が求められた。
1997年8月	通信・芸術大臣はABAに一連のオンラインコンテンツ問題について第2回目の調査を指令した。
1997年9月	通信・芸術大臣は国立情報経済局 (NOIE) の管理者に通告した。
1998年2月	ABAは子どもとオンラインコンテンツ対策委員会 (CCOTF) を設立した。
1998年4月	オーストラリアで苦情ホットラインを調査するためワーキンググループが生まれた。
1998年6月	子どもとオンラインコンテンツ対策委員会がABAに報告書を提出した。
1998年7月	ABAは通信・情報・経済・芸術大臣に第2回の調査の進捗に基づき, 中間報告書を提出した。

1998年 9月	犯罪停止全国会議がオンラインで発見された違法なコンテンツに対する苦情ホットラインの提案を是認した。
1998年 9月 ・10月	ABAはモンテカルロで開催されたユネスコのサイバー法に関する専門家会議に参加した。ここでソウルの会合で出された提案が上程された。
1998年10月	インターネットコンテンツ評価連盟（ICRA）が結成された。ICRAはABAがメンバーである国際コンテンツ評価のワーキンググループに置き換ったもの。ABAはICRAの関連グループの一員として引き続きこの国際会議に参加した。
1998年11月	NOIEは情報経済の恩恵を理解できる人々を増やすためにオンラインオーストラリア・デイを開催した。ABAはオンラインオーストラリア・デイの活動の一部としてインターネットウェブサイトにもオーストラリアファミリーガイドを立ち上げた。
1998年12月	インターネット産業組合（IIA）はこの実践コードの「採用版」を公表した。ABAは通信・情報技術・芸術大臣に第2回調査の最終報告書を提出した。
1999年 2月	通信・情報技術・芸術大臣は公式に1999年にオンラインオーストラリアを開始し、情報経済に国民の関心を集中させた。
1999年 3月	UNESCOの支援を得てABAはインドネシアのバリで開催されたアジア太平洋会議を主催した。
1999年 4月	政府は上院で「修正放送法（オンラインサービス）1999年」を導入した。

資料：Internet Content Summit 1999: Policy Panel より作成

（2）表現の自由と子どもの保護

さて、コンテンツ規制でとくに重要なのは表現の自由の尊重と子どもの保護とのバランスである。グレインガー（ibid. 1999）は表現の自由の尊重は必ずしも絶対的なものではないと主張する。表現の自由の尊重とコンテンツ規制とのバランスが適切なものかどうかを決定するのは国民と民主的に選出された政府だとし、子どもの保護のためにはコンテンツ規制を厳しくすることは正当だと主張する。そして、オーストラリアは両者の適切なバランスにきわめて敏感だといっているが、既存のメディアコンテンツには厳密な規制が貫かれているのに、インターネットコンテンツにはまだそのような規制が適用されていないことに言及する。

ちなみに現在の体制では「1992年放送法」第5条のコンテンツ要件でR、RC、Xと指定されたコンテンツのみに限定されている。それに反し放送事業者はそれより多くの規制に従わなければならない。たとえば、PG、M、MAと指定された番組は放送時間帯が制限されているし、広告やスポンサーにも要件が課せられている。また、ニュースや情報番組は公平で正確であることが要求される。だから、FACTS（Federation of Australian Commercial Television Stations）は現在の体制下ではインターネットのストリーム映像はテレビと同じ要件に従う必要はないことに言及し、そのことの矛盾を指摘するのである。それは放送法第5条で「インターネットコンテンツ」は既存メディアとは別個のものとして扱われているからだが、それでは対応しきれないのが既存メディアのコンテンツがインターネット上で流通するようになる近未来の状況である。

ところで、オーストラリアもその加盟国である「市民および政治権力に関する国際規約」（ICCPR: International Covenant on Civil and Political Rights）の19条には以下のように記され

ている。

1. すべての人は干渉されることなく意見を持つ権利がある。
2. すべての人は表現の自由を持つ権利がある、それは探索する（取材の）自由、（あらゆる種類の情報や考えをさまざまな表現形態で）告知する（報道の）自由を含む権利である。
3. この条項の第2項で規定されている権利の行使は特別の義務と責任を伴う。したがって、一定の規定に従う必要があるが、それらは法によって規定され、不可欠のものだけである。すなわち、
 - a. 他人の権利や信望の尊重
 - b. 国家の安全、公衆の秩序、公衆の健康あるいはモラルの保護、等々。

以上の規約は次のような原則を含むオーストラリアの国家分類コード（National Classification Code）と同様のものといえる。オーストラリアでは出版、新聞、コンピュータゲームなどのコンテンツに対し、以下のような規定が設定されている。

- a. 大人は読みたいものを読み、聞きたいものを聞き、見たいものを見るべきである。
- b. 少数民族は傷つけられたり、妨害されたりするようなコンテンツから保護されるべきである。
- c. すべての人は不適切で望みもしないコンテンツに晒されることから保護されるべきである。
- d. 以下の点を公益に照らして考慮する必要がある。
 - i 暴力、とくに性的暴力を大目に見たり、けしかけたりするような表現
 - ii 下品な表現で人を描くこと

こうしてみると、規約に示された勧告が国民に一定の指針を提供したことは確かだ。だが、最終的に施行細則を決定するのは政府である。民主的に選出された政府が適切だと思うバランスを貫くには、この勧告によって政府の選択の自由が束縛されるべきではないとグレインガーは考える。というのも、ネット社会のフロンティアでは政府がきわめて重要な役割を果たすからである。

ちなみにグレインガー（ibid. 1999）はパトリシア・アウフデルハイド著の『コミュニケーション政策と公益』を引用して、以下のように記している。

「サイバー空間は形式上、地上とは別世界ではないし、地上の司法権が及ばないわけではない。政府はサイバー空間で生まれたルールや慣習を尊重し、この新しい世界を非効率な規制や検閲で押さえつけるべきではないとしているが、ネットサーフィンする人々や詐欺集団がネットで行っていることを国家が統治できないというのはばかげたことだ。国民の代表であり民主的な価値の保護者として国家はサイバー空間と伝統的な社会を統合するための権利と責任を持つべきである」

実際、オーストラリア政府機関であるABAはインターネットコンテンツには自己規制と共同規制で対応するという方法で政府、産業、コミュニティに有益な指針を提供した。産業やコミュニティを動かしながら、インターネットコンテンツの共同規制体制を推進していくにつれ、ABAはたしかに最先端の事情に通じた規約を持つようになるだろうし、新たな地平を切り開いていくことにもなるだろう。

（3）DCITAの抱えるコンテンツ規制に関わる課題

当時、DCITA（Department of Communications IT and the Arts）には解決しなければならな

い多くの課題があった。国際問題、トラフィックの増加、アクセスを制限されたメカニズムの検出、利用者の差異化、ストリーム映像と非ストリームの映画、海外のISPへのアクセス、等々である。そこでOvum社に関連事項について調査を依頼した。調査を依頼されたOvum社は報告をまとめるのに際し、課題を以下のように整理した。

① 国際問題

まず他国のコンテンツをコントロールしきれないという問題があった。ある国が違法なコンテンツを恒常的に発信していたとしても、その国からのコンテンツをすべて遮断することができないという問題があった。もちろん、その国の拡張子に基づきすべてのコンテンツを遮断することはできるが、だからといってその国からのコンテンツをすべて遮断したと保障することはできない。どのような拡張子を持つURLからのコンテンツでも世界中どこからでも配信されうるからだ。また、URLの代わりにIPアドレスを使うことによってこの種のフィルタリングをすり抜けることもできる。

たとえば、「uk」サイトの場合、IPアドレスの所有者リストを作成し、指定したIPの要求を拒むことはできるが、同じIPアドレスから生み出された多様なURLを持つ多くのサイトが現れてしまうことが多い。これはたとえ遮断された拡張子を持っていなかったとしてもそのアドレスからのすべてのサイトが遮断されてしまうことを意味している。

② トラフィックの増加

次に、トラフィックの増大という問題がある。市販のフィルタリング製品はトラフィックの増大を監視できる。だが、事業者はトラフィックのモニターは一般にシステム管理者によってそのパフォーマンスを調べるために利用されていると指摘していた。このことからフィルタリング製品が分析のために利用されていないことが示されている。

③ アクセス制限システム

アクセス制限システムにも問題がある。たとえばユーザーネームやパスワードなどによって一定年齢以下の利用者が制限されたコンテンツにアクセスすることを拒むことはできる。だが、そのような安全装置を使っていないサイトには子どもは簡単にアクセスしてしまう。また、利用者がアクセス制限システムを通過したかどうかはわかる仕組みは素材がうまく保護されていることを示しており、利用者が素材にアクセスすることが承認されたことを示す。だが、商業的に利用されていないフィルタリングシステムではアクセス制限システムによって利用者を把握することができない。つまり、アクセス制限システムでは利用者がアクセスするコンテンツが信頼でき、承認されたものだと保障することにはならないのである。

④ 利用者の細分化

利用者の細分化も問題である。サーバーやファイアウォールをベースとした製品の事業者は利用者がそのシステムにログインできるようにしている。これは個々の利用者のフィルタリングのレベルに基づき個別にフィルターをかけるためである。たとえば、子どもがポルノグラフィのサイトにアクセスするのは拒否するが、大人がそのようなサイトにアクセスするのは許すといったようなものだ。もしフィルタリングシステムを利用することを選択しない利用者が現れたら、利用者のアカウントは凍結され、その後のすべてのアクセスにフィルターがかけられなくなる。

⑤ ストリーム映像と非ストリーム映像

ストリーム映像と非ストリームの映画も問題である。ファイルタイプのフィルタリングはメディアファイルやストリーム（例：MPEG, Quicktime）コンテンツを分析することができない。ただ、映像をデータから抜き出すことができれば、分析が可能になる。もしこれらのうちかなり

の部分に性的な映像が含まれるなら、そのデータは遮断される。しかし、現時点の映像分析の技術ではこれはまだ十分に実践的なものではないし、企業からそのような需要もなく、この優先順位は低い。

⑥ 海外の ISP

海外の ISP 事業者についても問題がある。もし政府がすべての ISP 事業者にインターネットフィルタリングを義務づけるのなら、法によって保護されている ISP を通してインターネットにアクセスする利用者はインターネットアクセスの際にフィルターがかけられている。これに不満を抱く利用者はいわゆる「サイバーストーカー」になってフィルタリングを回避することを選ぶしかない。サイバーストーカーとはインターネットにフィルターをかけることを強制する国内法を無視するために海外の ISP を使う人のことである。アクセス手段が PSTN (Public Switched Telephone Networks : 公衆交換電話網) か、衛星かモバイルかにかかわらず、これを避けるためにできることはほとんどない。もし利用者が国際電話料金を支払い海外の ISP の会員になるために料金を支払うつもりがあるのなら、彼らはどんなに義務付けられたフィルタリング制度でも無視することができる。海外の ISP にアクセスする電話回線を遮断することによってしかこれを妨げることはできない。

以上、Ovum 社は2002～03年の時点での課題を上記のように整理した。インターネットコンテンツを巡る課題の中でとくに DCITA に必要とされていたのが、フィルタリング技術についての分析であった。

(4) フィルタリング技術の検証

2000年1月1日、オンラインコンテンツの共同規制体制が始まった。この体制は主に以下の3つの要素で構成されている。

1. 業界の慣例法および1992年放送法第5条の下での ISP や ICP の規制
2. 脅迫、攻撃、良識のある人が見て不快と思うような方法でインターネット伝送サービスすることを罪とし、国家法や州法および1914年の連邦犯罪法の下でコンテンツ制作者、コンテンツ伝送者、コンテンツ利用者に罰を科す
3. コミュニティ教育や研究調査、国際連携などの法によらない規制

さて、1992年放送法第5条には業界の慣例法の展開も含まれていた。業界法の遵守は最初の段階では強制的なものではないが、ABA が ISP あるいは ICP に法を遵守するよう指令すれば、彼らはそれに従わなければならない。さらに、もし業界法が不十分なものと判明したら、ABA は強制力のある業界基準を創設しなければならないとされていた。

さらに、第5条の規定は ABA によって管理された不服申し立て機構にも適用される。だから、誰もが不快なコンテンツ、あるいは違法なインターネットコンテンツについて不服を申し立てることができる。禁止されていることが明らかな国内コンテンツの場合、ABA は強制執行できる逮捕状を当該 ICP に発行し、そのコンテンツを提供しないように指示することができる。また、禁止されていることが明らかな海外のコンテンツの場合、ISP がその責任の対象となる。そのため第5条では ISP にコスト回収を含め、この法の補遺にリストされているフィルタリング製品を1つ以上導入するよう要求する。ABA はこれらのフィルタリングメーカーに対し不服申し立て機構によって禁止されていることが明らかな海外のコンテンツを公表している。だから、フィルタリング製品は ABA が公表した規制内容を逐次、更新できるものでなければならない。

既述したように、DCITA (Department of Communications IT and the Arts) はフィルタリング技術の分析をメルボルンにある欧州の調査会社 Ovum 社に依頼した。Ovum 社が DCITA に提出した調査報告書によると、2003年1月に DCITA に指名され、インターネットコンテンツの規制技術、とくに ISP のフィルタリング技術に焦点を当てて技術評価をするよう依頼されたと書かれている。具体的な目標は以下のようなものであった。

- ① オンラインコンテンツの共同規制体制が開始された2000年以降、新しい遮断技術、フィルタリング技術が登場したのか、そのような技術は以前のものより有効になっているのか、等々についての技術的なアドバイスの提供。
- ② これらの技術の金銭コストあるいは管理要件 (利用者および ISP にとって)、インターネットの実効性に関する技術の潜在的影響などについてのアドバイスの提供。
- ③ 海外の政府管理下のフィルタリング技術やその他のアクセス管理技術の概観

第5条の履行に向けて見直しが行われるのは1992年放送法の下での要件である。そのためフィルタリング技術を全般的にチェックし、アクセス制限システムにそぐわないR指定の海外作品に対する利用者のアクセスを制限できるかどうか技術チェックする必要があるのである。

(5) Ovum が提供する4つのシナリオ

Ovum はインターネット上でコンテンツを規制し、コントロールするのに4つのシナリオを想定した。それぞれの特性については後述するが、各シナリオを俯瞰すれば以下のように位置づけることができる。

表2 各シナリオの特性

シナリオ1	シナリオ2
<p>(自己規制)</p> <p>ISPがサービスとしてフィルタリングを提供し、利用者は望むならそれを採用する。政府の関与は最低限。</p> <p>事例：イギリス</p>	<p>(政府が自己規制を推進する)</p> <p>政府は望ましくないコンテンツを定義づける際、先を見越して行動するスタンスを取り、支援者のように行動する。潜在的なサービス提供者であるICRAはこれを政府が関与する最高のシナリオと考える。</p>
シナリオ3	シナリオ4
<p>(政府が業界にフィルタリングを義務づける)</p> <p>政府はISPにすべての望ましくないコンテンツにフィルターをかけるよう強制する。政府は望ましくないものについて定義する。</p> <p>事例：シンガポール</p>	<p>(望ましくないコンテンツは政府によって遮断され、フィルターをかけられる)</p> <p>政府はインターネットバックボーンあるいはネットワークにフィルタリング体制を施行する。</p> <p>事例：中国</p>

資料：Internet content filtering, 4 April 2003, pp.9-11より作成

注：ICRA: Internet Content Rating Association

① シナリオ1： 自己規制

フィルタリングはISPによってサービスとして利用者に提供される。利用者は個々の要求にしたがってISPのサービスメニューの中から選択して組み込んでもらう。分類されたコンテンツを伴うURLリストは地方の事情や文化的な事情に基づきフィルタリングソフト事業者によって作成される。必ずしもすべてのISPが同じ事業者のものを使用するわけではなく、このリストはISPによって異なる。ISPはサービス料金を徴収できるから、フィルタリングは収入の一つとなる。ISPはPCベースのフィルタリング、サーバーベースのフィルタリングあるいはその両方の組み合わせで選択メニューを提供する。

一方、政府はサイトを遮断するよう指示することができるし、とくに両親にフィルタリング技術を導入するよう勧告することもできるが、政府の関与は最低限のものでしかない。コンテンツ提供者は制作を奨励され、コンテンツの評価には責任をもつ。事業者はコンテンツ提供者の評価に基づきコンテンツを分類し、そのような評価システムを提供することに責任を持つ。表2に示したように、事例としてはイギリスがこれに該当する。

② シナリオ2： 政府が自己規制を促進

シナリオ1と同様、フィルタリングはISPによってサービスとして提供される。利用者は個々の要求に従ってサービスを選択して組み込むことができる。政府は分類されたURLやIPアドレスリストを作成する供給事業者を選別し契約する。そして、コンテンツがどのように分類されるべきかを決定し、最終的にそのリストに責任を持つ。同じURLあるいはIPアドレスリストはISPによって使用されるすべてのフィルタリング技術の下で使用されるから、全国規模で一律にフィルターをかけることができる。

一方、ISPはPCベースで提供されるフィルタリングとサーバーベースで提供されるフィルタリングとを選択できるが、このシナリオ2では新しいURLリストと統合するためサーバーベースのフィルタリングが中心になっている。ISPはサービス料金を設定できるので収入を生み出すことができるが、全国規模のURLリストの提供は政府の管理下で運用される。フィルタリング製品はISPが選択する。公開された基準はフィルタリング技術事業者にとって重要だが、これらの基準は政府によって運用され、政府が評価システムの開発を支援する。表2に示したようにこれはオーストラリアが望ましいものとしている事例である。

③ シナリオ3： 政府がフィルタリング業界を管理する

政府が管理するすべてのISPは加入者にフィルタリングサービスを提供しなければならない。ISPと利用者ともフィルタリングサービスの利用を選択することはできない。シナリオ3では利用者が望む場合だけ、ISPに要望すればフィルタリングの選択をすることができる。ISPにはPCベースのフィルタリングかサーバーベースのフィルタリングかの選択肢がある。だが、サーバーベースのフィルタリングの方が政府の取り締まりが容易で、ISPが法令遵守を証明するのも容易である。

政府がフィルタリングの様式を管理しており、選択しようとするれば、サーバーベースのフィルタリングなら容易に承認される。政府はISPが使用するためのフィルタリング技術事業者の公認リストを作成し、保持する。フィルタリングには厳しい規制の枠組みがある。政府には成人向けとその他「望ましくない」コンテンツを規定する責任があるが、業界が政府とこの問題について議論する機会はきわめて少なく、政府がリストを作成し、ルールを規定する。表2に示したように事例としてはシンガポールがこれに該当する。

④ シナリオ4： 政府がすべての望ましくないコンテンツを遮断する

ISP も利用者もともにフィルタリング技術の施行を選ぶことはできない。あらゆるコンテンツの遮断あるいはフィルタリングは政府によってネットワークやバックボーンレベルで行われる。政府は遮断すべき URL や IP アドレスのリストを作成し、すべてのコンテンツの状態を説明する責任を持つ。政府の体制下ではフィルタリング技術事業者に商業市場に参入する機会はない。たとえば成人と子どもといった異なるグループごとにコンテンツの遮断リストを使い分けるための条項はない。表2に示したように具体的な事例としては中国がこれに該当する。

3) 対抗する見解と結論

(1) オーストラリアのコンテンツ規制体制への批判

既述したようにオーストラリアはインターネットコンテンツに対し共同規制体制を取っており、その中核にフィルタリングソフトによるコンテンツ規制を位置づけてきた。だが、これについては異論がある。たとえば、キャラドック・デイビス (Caradoc-Davies, B., 2002) は1992年放送法の第5条を見直した報告書の中で以下のような見解を述べている。

「絶え間ない技術変化の時代には厳しい制約を課したとしてもたちまち時代遅れになってしまう」と記し、フィルタリング技術を使ってコンテンツ規制をすることの無効性を示唆する。さらに、「唯一の現実的な対策としては、個々人がしっかりとした判断力を身につけるべきである」とし、何よりも大切なのは受け手の情報判断力であり、その力を養成していくことこそ重要だと指摘する。そして、オーストラリアが展開しているコンテンツ規制は、技術的社会的に失敗しているばかりか人権の側面から見ても失敗であったと評するのである。そして、以下のように整理する。

① 技術の側面からみた失敗

オーストラリアでアダルトコンテンツを禁止しても効果は低い。というのも、インターネットでもっとも多いのは海外で制作され、海外から発信されているコンテンツだからだ。たとえ禁止したとしても、その効果はごく少数のアダルトコンテンツ業者を米国に移住させてしまう程度のものでしかない。ところが、米国では表現の自由が憲法の最初の修正条項で保障されているから、事業者が移住してもインターネットでアダルトコンテンツの発信を制限することはできない。だから、コンテンツ規制によって事業者が海外に移住してしまったために、アダルトコンテンツを規制できないまま、オーストラリア人が支払うコストだけが嵩むようになったのである。

こうしてみると、第5条はオンラインサービスについての誤った見解の下で構築されているように見える。インターネットの強みはその分散構造にある。そして、分散構造のネットワークシステムは検閲の効果を弱めるばかりではなく、相互にむすびついたときに大きな力となる。だから、厳格な法規制にもかかわらず、コンテンツを制作しアクセスする個人の数はインターネット上で増え続けている。中央集権的なシステムの検閲は分散構造に適合できず、インターネットでは検閲が非効率だと確認されるだけである。

② 社会的側面からみた失敗

インターネットコミュニティは米国で設立された。これに象徴されるように米国には表現の自由の文化がある。ところがオーストラリアの第5条はこの文化を無視し、抑圧的な検閲規制を課すことを強いる。この条項の制定はオーストラリア国内では怒りを呼び、世界では嘲笑を生んでいる。というのも検閲は映画や出版のように限定された情報源や流通機構のメディアでしか有効ではないからである。

そもそも検閲しなければ子どものポルノや虐待を取り調べ、告発することができないというものでもない。インターネットを検閲しない米国ではFBIが子どものポルノや虐待などを告発している。逆にオーストラリアでは表現の自由を奪うほど厳格に検閲を行い、フィルタリングソフトの使用を奨励するが、それが子どものポルノを発見しにくくしている。

③ 人権的側面からみた失敗

インターネットは個人が表現したものを発信し、地理的境界を越えてコミュニティを形成する機会を提供する。これらのコミュニティでは人々は面と向かってはいえないようなことを話題にするが、とくに性に関する問題を取り扱うことが多い。インターネットの匿名性、遠隔コミュニケーションの機能ゆえである。たとえば、匿名だからこそ心を開いて日ごろいえないような心情を吐露する。遠隔コミュニケーションだからこそ暴力で虐げられている女性がインターネットを心のはけ口とするといった具合だ。

ところが、第5条は大人から人権としての表現の自由を奪う。告発の恐れやコンテンツの適法性を気遣ってISPが勝手にその種のコンテンツ提供を取りやめてしまうからである。ISPの過剰なまでの法令遵守が人々のネット上で悩みを表現しようとする気持ちを奪っているのである。

人権のユニバーサル宣言19条には以下のように書かれている。

「何人も意見を持ち、表現する権利を持つ。この権利は誰にも干渉されることなく意見を持つ自由、どのようなメディアでも、境界領域のものでも、情報や考えを求め、受け取り、それを伝える自由を含む」

ところが、第5条のどこにもこの権利が是認される規定がない。米国では表現の自由は憲法の最初の修正条項によって保護されているし、ドイツ憲法の第5条1項にも「検閲がない」という記述があるとされる。1990年のニュージーランド権利法案14項でも「何人も表現の自由の権利を持つ。どんな種類の情報や意見でも求め、受け取り、どんな形式でも知らせる自由を含む」と記されている。

こうしてみると、インターネットの検閲が支持されていない西側の自由民主主義国では、オーストラリアの第5条を有効に履行できないことになる。というのも、それらの国々がこの第5条を無効にするようなコンテンツや技術資源の保有者だからだ。つまり、オーストラリアが厳格なインターネットコンテンツ規制をかけたとしてもグローバルにコンテンツが流通する時代には効果をあげることができないのである。また、アクセス制限システムを使用すれば、利用者はコンテンツにアクセスするたびに自分をシステムに認識させなければならず、匿名性を放棄せざるを得ない。したがって、このシステムは大人が表現の自由を行使しようとする場合の障壁となる。

(2) 結 論

オンライン事業者のオウングル(Aungel, M. 2002)は基本的にオーストラリアのウェブサイトのコンテンツ規制の方針に賛意を示しているが、インターネットの性格上それはきわめて難しく、人々の権利を奪うだけの結果に終わりがねないことを指摘する。そして、インターネットコンテンツへのアクセスの自由を失いたくない多くの利用者は抵抗するだろうと記す。だからこそ、第5条の遵守に関連して自発的なスキームを施行してはどうかと彼は提案するのだ。つまり、子どもの保護を最高の優先順位にするが、それをインターネットに固有の表現の自由に影響を与えず達成する必要があるというのである。

たとえば、オーストラリアのインターネット事業者に自己検閲という自発的なスキームに参加

するよう奨励してみてもどうかと彼は提案する。もし適切なフィルタリング技術がISPに導入されれば、サイトの評価が表示され、利用者にそれが認識される。コンテンツ評価は現行の分類にしたがって、G, PG, M, MA, R&Xとする。オーストラリア人がアクセスしたいと思う国際的なサイトにもオーストラリアの検閲コードを適用する。コンテンツのガイドラインはインターネット上で公表し、いつでもダウンロードできるようにしておき、すべてのインターネット事業者が自分のサイトの評価を知ることができるようにする。オウングルはこのような自発的なスキームを提案するが、その理由はそれが表現の自由を侵害しないと思われるからであった。

2006年に公表されたサーバーベースのフィルタリングについてのRMIT分析研究所の報告書を見ると、ISPの規模が大きいほど、ネットワーク構造と設計の面からフィルタリングの展開が難しくなると指摘されている。そして、入出力のデフォルトを切り替え、他のフィルターを迂回することによって不適切なウェブサイトにもアクセスできてしまうこと、十分な警告もなく映像やサイトが遮断された場合、利用者は欲求不満になり、イライラすることなどが報告されている。フィルタリングの性能調査の結果からはフィルタリングはまだコンテンツ規制として万全でなく、ときに利用者の不快感を高めていることも明らかにされたのである。

オーストラリアのコンテンツ規制を厳しく批判していたキャラドック・デイビス (ibid., 2002) は第5条が子どもの保護に失敗しているだけでなく、大人を追い詰めていると指摘する。そして、子どもの保護は公的な教育や親の指導を通してなされるべきであって決して検閲によるべきではないと指摘する。たしかにフィルタリングの技術向上がはかばかしくないことを考えれば、当時、ABAが提唱した第3の領域を充実させていくのが効果的ではないか。すなわち、コミュニティの力、教育の力を充実させることによる「内なる」コンテンツ規制である。

すでにNetAlertはインターネットコンテンツから子どもを保護するため、総合的な対策を検討している。ネット利用の安全ガイドブックも教師用、両親用、図書館司書用と用意し、子どもを取り巻く環境そのものをネット利用の安全教育の場にしようとしている。NetAlertやABA(現在はACMA)を中心とした実践的な活動の積み重ねを見ていると、たとえ時間がかかろうと子ども自身のコンテンツに対する判断力を養成していくことが、表現の自由を損なうことなく子どもを保護する方策であり、着実な効果を収める唯一の対策ではないかと思われる。

文 献

ABA & NetAlert (2005) *kidsonline@home: Internet use in Australian homes*.

ACTF(2002) *REVIEW OF THE OPERATION OF SCHEDULE 5 TO THE BROADCASTING SERVICE ACT 1992*

Annual Report 2004/2005, NetAlert Limited.

Aufderheide, P. (1999) *Communications Policy and the Public Interest; The Telecommunications Act of 1996*, The Guilford Press, 323p.

Aungle, M. (2002) *Submission for the review of the operation of Schedule 5 to the Broadcasting Service Act 1992*, Dimension Data Australia. 1 November 2002.

Caradoc-Davies, B. et al. (2002) *Submission on the Review of Schedule 5 ("the Schedule") to the Broadcasting Service Act 1992*, 2 November 2002.

DCITA(2005), *REVIEW OF THE OPERATION OF SCHEDULE 5 TO THE BROADCASTING SERVICE ACT 1992*,

Flinders University media release 15, Nov. 2005

Grainger, G. (1999) *A Co-regulatory Scheme for Internet Content: The Australian Approach*. Inter-

net Content Summit 1999.

Ito, Y. (2001) *International Covenant on Civil and Political Rights*, University of Tokyo. pp11-12.

OVUM(2003)*Internet content filtering: A Report to DCITA.*

RMIT TestLab(2006) A Study on Server Based Internet Filters: Accuracy, Broadband Performance Degradation and Some Effects on the User Experience.

Submission Draft Model State/Territory Legislation On-line Content Regulation, EFA, 29 September 1999.

Watchtower Bible & Tract Society of New York v. Village of Stratton, 536 U.S. 150(2002),
(<http://www.oyez.org/oyez/resource/case/1498/>)

参照 URL

http://www.acs.org.au/icdl/content/upload/files/pdf/PISA_04.06.pdf#search='OECD%20PISA'

<http://www.netalert.net.au/01579-Why-do-Paedophiles-find-the-Internet-attractive.asp?qid=22883>