

携帯取引において顕在化している消費者保護及び
権利強化上の問題に対する政策指針
(内閣府仮訳)

DSTI/CP(2007)5/FINAL

2008年5月6日

OECD 消費者政策委員会

序文

本政策指針は、モバイル産業において発生している消費者保護と地位向上の問題に関して、2008年6月17日から18日にかけて韓国のソウルにおいて開催された『インターネット経済の未来に関する OECD 閣僚会議』の会合に、OECD 消費者政策委員会（CCP）によって検討・提言されたものである。この政策指針は2007年に CCP によって完成させられた携帯取引に関する報告書（OECD、2007a）の研究と結論に基づいている。

本指針は、2008年4月16日の委員会によって機密解除された。本書類は OECD の事務局長の責任の下で出版される。

©OECD / OCDE 2008。

目次

序文	1
携帯取引において顕在化している消費者保護及び権利強化上の問題に対する政策指針	3
I. はじめに	3
II. 情報開示の限定性	5
III. 未成年者の保護	12
IV. 携帯電話の不正使用と安全問題	18
附則1 未成年者保護：OECD 諸国における法律と自主規制	25
附則2 OECD のモバイル産業問題に関する機関	29
参考文献	31

携帯取引において顕在化している消費者保護および権利強化上の問題に対する政策指針

I. はじめに

携帯取引の発展

本稿の論点である携帯電話商取引は、「携帯電話電子商取引」あるいは「m コマース」としても知られており、典型的には通話のために使われてきた小さい、手持ちの携帯端末を使って、ショートメールサービス（SMS）や、マルチメディアメールサービス（MMS）、あるいはインターネットという手段を使って、ワイヤレス通信サービスとネットワークを通して行なわれる商取引とコミュニケーション活動を意味する。「携帯電話会社」は、携帯電話契約者にサービスを提供する会社を指す。「携帯取引事業者」は、製品やサービスをモバイル環境を通じて直接販売する会社、もしくはウェブサイト運営者（Yahoo! や eBay など）や、サイト運営者（携帯取引事業者を補助する存在、複数の第三者ベンダー費用を処理して携帯電話会社に転送して、携帯電話契約者に請求をするような）を通して販売する会社を指す。「携帯電話契約者」は、携帯電話契約に対して料金を支払う個人を指す。

運営上の基盤の集中とともに、モバイル産業は現在インターネットに基盤を置いた電子商取引の中で広がっている。このことはモバイル産業を電子商取引の他の形式から区別することをますます難しくしている。モバイル産業がそれ自体ではインターネット・アクセスを必要としない一方で、さらにより多くの携帯電話商商業の取引がウェブ（HTML、TCP/IP）、ワイヤレスアプリケーションプロトコル（「WAP」）と i モードのような通信システムプロトコルを使って行われ、そして電話がワイヤレスコミュニケーションネットワーク（例えば「3G」）に接続した。加えて、ますます多くのパーソナルデータ端末あるいはスマートフォンが、今では無線で通話をすることが可能である。

モバイル産業は現在多くの OECD 諸国で急速に発展している。これらの国において、ますます多くの個人が最先端の携帯電話やその他の高性能の端末を手にし、現在固定されたコンピュータで可能なこととは異なる広範囲の携帯電話サービスから利益を得ることを可能にしている。1997 年と 2005 年の間に、OECD 各国の携帯電話契約者数は合計して 1 年で平均 24% の割合で増加している。（OECD、2007b、98 頁）

現在、携帯電話契約者はそれらの端末を使って以下の事が可能である

- ・ 映画、音楽、着信音、あるいはゲームのような、コンテンツを買って、ダウンロードすること
- ・ オンラインゲームをして、そしてオンラインで賭け事をする事

- ・ 携帯電話の画面上で天気予報やニュース、携帯テレビやテレビチャンネルとともに放映されている番組の情報を接続すること
- ・ 位置測定技術を通じて自分用に合わせた情報を手に入れること
- ・ ネット銀行や金融サービスに接続して、そして取引をすること
- ・ 携帯電話に掛かる支払いを、クレジットカードあるいは携帯電話代に請求して支払いをすること
- ・ 商品やサービスを購入する支払い端末（「電子財布」）として、そして
- ・ 双方向のテレビ番組で投票すること。

第三代携帯電話サービス（3G）の発展によって、高速のインターネットアクセスが提供され、オーディオ、そしてより品質が高い画像を装備した携帯電話は、端末への消費者の興味を拡大し、そして新しい商業用アプリケーションとしての可能性を広げた。

もう1つの発展は増加する子供たちによる携帯電話の使用と接続に関する。子供たちが攻撃的で不適切で下品な携帯電話のマーケティング慣行から効果的な保護を受けた上で、携帯電話の使用からの便益を保障することは、すべての利害関係の中心的な挑戦になっている。

消費者に発生している携帯取引の課題

消費者政策委員会（CCP）は長年携帯取引の発展を追ってきました。2007年に、委員会は報告書（OECD、2007a）を発行し、携帯電話商取引の概観を提供するとともに、それが消費者に投げかけるであろういくつかの中心的な挑戦を明らかにした。報告書は携帯端末は消費者を魅了するようなユニークな特徴（携帯端末は使うのが簡単で、携帯電話のサービスが利用可能であれば使う場所を選ばない）をもっている反面、画面の小ささ、限定された記憶容量とメモリ容量、電池の耐久性や低い処理能力等の固有の技術的な制限も露呈している。

本政策指針は、市場が十分に成熟した国で発生した中心的な問題の多くに対して、関係者が実務的な処置を提供することを目指している。その他の問題も時がたつにつれ多く出現するであろう。従って本ガイドラインは包括的な政策の原則と行動を提供するというよりは、現在と将来の携帯電話商取引が投げかける課題の分析とこれからの調査を導くようないくつかの原則を提供することを主眼としている。これらの課題は仮説例のかたちで以下述べられている。

委員会は3つの問題に焦点を合わせることに決めた

- ・ 携帯端末の上に表示可能な情報が限定されるために引き起こされる問題（小さな画面とその他の技術的な要因による）
- ・ 未成年者の商業的搾取の危険性の増加
- ・ 不正使用やデータ保護違反とプライバシーの危険で明らかにされた携帯端末の脆弱性

当委員会は電子商取引における消費者保護に関する 1999 年 OECD ガイドライン（「電子商取引ガイドライン」）（OECD、1999）を考慮に入れて、これらの問題を調査することを決めました。大半の国が電子商取引ガイドラインに含まれる原則が携帯電話商取引に当てはまると考えた一方で、これらの原則がどのように効果的に携帯電話会社や、ウェブサイト運営者、金融とその他の商業サービスを統合するサイト運営者やモバイルベンダー、そして携帯電話契約者に適応されるかを明らかにすることは有益であるとした。そうする上で、当委員会は消費者保護、セキュリティ、プライバシーとスパムに関するその他の OECD の協定書で該当するものから最善の試みを取り入れることとした。（附則 II）

II. 情報開示の限定性

電子商取引ガイドラインは、消費者は電子商取引において、知らされた上での決定をすることができるように、契約の前に、消費者が提供されるべきであると指摘している。いつも正確で、そして容易に入手可能であるべき情報は以下の通りである（コラム 1）：

- ・ 事業に関する情報と利用可能な紛争解決メカニズムの情報
- ・ 提供されている商品あるいはサービスの特徴；及び
- ・ 要件、条件、支払い方法と費用を含めた契約自身についての詳細

コラム 1. 電子商取引ガイドラインでの主要開示規定

電子商取引ガイドラインの第 2 部は次の一般的な原則を設定した：

- ・ 第 2 条（「公正な事業、広告とマーケティング慣習」）は以下のような一般原則を定めた。事業者は欺瞞的、誤認、詐欺的又は不公正とみなされるいかなる慣行にも従事すべきではない；消費者へのマーケティングを行う事業者は消費者に不合理な被害のリスクをもたらすような慣行に従事すべきではない；並びに事業者は自らと商品やサービスに関する情報を、明確で、目立つように、正確で、そして容易に入手可能な方法で提供すべきである。
- ・ 第 3 条 C（「オンライン開示 - 取引についての情報」）は、事業者は消費者が取引をするかどうか知らされた上での判断ができるように、取引期間、条件と費用

についての十分な情報を提供するべきであると述べている。情報は明確で、正確で、そして容易に接続可能であって、そして「事業者により徴収されまたは課される総費用の細目」を含まなくてはならない。

・ 第4条（「確認プロセス」）は消費者が購入の詳細を再検討して、はっきりした、知らされた上での慎重な取引締結への同意をつくれる方法があるべきであることを示す。そして消費者が完全で、正確な記録を保持することが可能であるべきであることも述べている。消費者は最終的に取引を締結する前に取引を取り消すことが可能であるべきである。

・ 第6条（「紛争解決と救済」）は事業者が苦情を取り上げるための公正で、効果的で、透明な、そして内部メカニズムを消費者に提供するように奨励する。この点に関して、2007年消費者の紛争解決及び救済に関するOCDE理事会勧告は民間企業に、「消費者が苦情を関係のある事業者と直接公平で、効果的で迅速な方法で解決する機会を無料で提供する効果的な内部苦情処理の過程」を確立することを求めている。

消費者にこのような幅広い情報を提供することは、小さな画面サイズや多くの携帯端末の限定されたメモリーや記憶領域といった固有の技術的な制約のため、携帯電話商取引においては難しいことである。携帯電話サービスや商品のために提供するものは、基本的にはSMSあるいは携帯電話電子メールの形式で行われる。加えて、それらは携帯電話で接続したインターネットウェブサイト上を通して現われるかもしれない。携帯端末とインターネットの繋がりの増加によって、たとえ情報の要件が仮に満たされたとしても、それは携帯電話契約者にとって、技術的な理由により、十分に接続ができないかもしれない。

事業者、商品およびサービスと取引プロセスに関する情報への接続

テレビの売り込み

電子商取引の小売り業者が携帯電話に登録してある顧客の1人にテレビの売り込みを送信した。その売り込みは会社についての全ての情報、テレビと販売金額及びその他の条件が会社のウェブサイト上で利用可能であるとし、そしてURLを提示した。顧客はWebページを調べずに、商品を注文した。彼が領収書を受け取ったとき、彼は高い送料と手数料に驚いた。彼は会社に苦情を言ったが、しかし価格についての全ての詳細はウェブサイトで提供されたということを知らされた。

上記の事例で、携帯取引事業者は電子商取引ガイドラインの第3条第二節に含まれる、情報の必要条件に従っているように思われます。しかしながら、インターネット上でただ

利用可能なだけの情報が携帯電話契約者によって十分に入手可能であるであろうかどうかについては疑義があるかもしれない。何人かの消費者は携帯電話あるいはコンピュータによっても、インターネットへのアクセスを持っていないかもしれない。それに対して、政府は、電子商取引ガイドラインの第3部（「執行」）のような対策の下に行動をして、携帯取引事業者に以下のように奨励することができる：

- ・ あらかじめ基本的な契約上の情報を SMS で提供する。これはそのような文章の長さが現在の通信事業者が課した制限と、このような情報を印刷することができないことから、部分的な解決策でしかないことを認識する。
- ・ 商用の申し出に対しての関心を表明している携帯電話契約者に、完全な情報を文書の形で郵送する。
- ・ 消費者が購入についてのいっそう詳細な情報を手に入れるために、電話をすることができる電話番号を提供する。

加えて、政府はこれらの問題について以下のように対処できる：

- ・ 自主規制や優良事例の普及を通して、消費者が取引を決定するかどうかに必要な完全な情報を、簡単に接続できるような技術の発展によってできるよう、民間企業のリーダーシップを推奨する。

将来、ワイヤレスデータを長距離にわたって提供するための技術は、携帯端末とコンピュータの間のデータの転送を促進することに関して、有用かもしれない。

確認プロセス

望まれない定期購読契約

消費者が携帯電話を使ってビジネス誌への1カ月の無料のオンラインアクセスを提供しているウェブサイト到达了。彼は申し出を受け入れるために SMS を通して自分の詳細情報を提供した。しかしながら彼はページの一番下にあった契約条項に気付かなかった。そこには、1カ月の後に彼はサービスに対して支払わなければならないと書いてあった；その条項を見るには大きく画面をスクロールする必要があった。消費者は二カ月後にこのサービスに対する料金を含んだ携帯電話代請求書を SMS で受け取ったときに驚いた；彼は試用期間の終わりにその定期購読希望を示したことを覚えていなかった。

上記の例で、消費者はサイトにアクセスした、しかし試用期間の終わりにそのサービスを購読する彼の意志を確認していなかった。サービスプロバイダはそれにもかかわらず消費者がすでにサービスを注文したと主張した。

上記のシナリオは携帯電話契約者が、注文された商品あるいはサービスを確認して、どんなエラーでも修正することができるように、契約の締結の前に提案された取引についての明確な、そして完全な情報を受け取って、そして契約条項を含めて、携帯端末の上に作られた、提案された取引の適切な記録を維持するか、あるいはプリントアウトする機会を与えられるべきであることを示唆する。(電子商取引ガイドライン、第2部、第2条と4条)もし携帯電話加入者がこのような事前の情報を受け取らないなら、次のようなことは有益であるかもしれない：

- ・ 全ての契約内容の再検討と情報を知り購入に関する慎重な同意の表明の可能性を提供されるまでは、携帯電話取引において、携帯電話契約者はその取引から撤退することができる。

加えて、携帯電話契約者は、自分のサイトに訪れる人から個人情報を得てそれらを搾取し悩ますような不公正で勝手な携帯取引者から、保護されるべきである。そのような危険から、携帯電話契約者を守るには、携帯電話会社が情報（名前と電話番号のようなダイレクトリ情報以外のもの）をジョイント・ベンチャーのパートナーあるいはマーケティング目的の独立した請負人などの第三者に顧客の許諾なしに開示することへの制限に関して、既存の保護が適切ではない場合には、そうした制限を適切に設定しうるだろう。携帯電話会社の情報収集業務の明白な公表を義務化するといったその他の規則も他同じく考慮されうるだろう。

株購入

消費者が携帯電話上で株の売りを注文するために彼の銀行に登録した。彼はすでに取引を確認したと思って、オーダーの詳細を承認した。彼は詳細情報を確認するためには承認ページを下にスクロールしなければならなかったことに気づかなかった。取引を承認する過程は明らかに示されなかった。結果として、取引は実行されなかった。

上記の例で、金融サービス提供者は取引を実行する必要について消費者に知らせていたが、しかし、取引過程において、それを確認する機会を与えることに失敗していた。携帯電話の画面サイズと容量の限界を考慮に入れた取引の実行を保証するための注意が払われる必要がある。注文に関する基本的な情報が提供された後に、以下のように消費者がすることは有益であろう。

- ・ SMS あるいは電子メールによって取引の確認を受ける。
- ・ 携帯電話と同様にインターネット上でも注文の状況の確認を簡単にできる方法を提供する。

紛争解決と救済

電子商取引ガイドラインの第2部第6条（「紛争解決と救済」）では、事業者が苦情を取り上げるための公正で、効果的、透明な内部メカニズムを持つことを奨励している。この原則は、民間会社の参加者に「消費者に彼らの苦情を直接関係のある事業者と解決する機会を平等、効果的、そして迅速な方法で無料にて提供する効率的な過程の内部の苦情処理、」を設立することを推奨した、2007年OECD消費者の紛争解決と救済に関する理事会勧告でさらに発展されている。

契約の複雑な連鎖

双方向テレビ

テレビタレントショーが、視聴者らの携帯電話を通して短いコードを送ることによって、彼らのお気に入りの競争者に投票をするよう求めた。電話の価格は10秒間スクリーンが一番下に細かい文字で公表されただけだった。さらに、文字は視聴者がテレビスクリーンから視聴者が通常座るであろう距離から読むのは不可能だった。携帯電話には確認プロセスが送られてこず、投票した後で、視聴者はただ投票に感謝するメッセージを見た。携帯電話契約者は、料金が携帯電話サービスの請求書に現われるまで、プレミアムレート（標準的な送信のコストより高い値段）でメッセージサービスが課金されていたことに気がつかなかった。視聴者がその課金を携帯電話会社に異議を申し立てると、携帯電話会社から、料金は支払わなければならない、問題は自分でテレビ番組会社に持ち込まなければいけない、と言われた。

携帯電話交通切符

消費者は、彼の住んでいる地区の市内バスや列車、市街電車で携帯電話を切符として使用することができる、交通切符を彼の携帯電話を経由して国営鉄道会社に注文した。彼が市街電車に乗っていた時に、彼はその携帯電話切符の認証に失敗し、車掌によって止められた。結果として、車掌は彼にすぐに切符代を支払うように要求して、そして、消費者がすでに切符を購入していたことを証明することが不可能であったので、追加の罰金を徴収された。家に戻って、消費者は二つ目の切符代と罰金を弁償するように彼の携帯電話会社に支援を求めた。

携帯電話会社はこの件に関して携帯電話会社には責任がなく、消費者がその要求を鉄道会社にすべきであると言われた。

最初の仮説は二つのメディア、伝統的なテレビと商売の間の相互作用が携帯端末を通して実行されたことを示す。これは携帯電話商取引でプレミアムテキストメッセージをビジネスモデルとして使用するという傾向を明らかにする。仮説は携帯電話契約者にとっての以下のような多くの問題を提起する： i) いつ消費者がプレミアムメッセージングサービスに接続しているかがわからない、 ii) 確認プロセスの欠如、 iii) 携帯電話会社の効果的な苦情解決と請求書問題の保障体制の欠如

苦情解決に関して、両方のケースが、どちらの企業が直接消費者のクレームを処理することに責任があるかについて、明快さに欠ける。典型的には、モバイル基盤を通じた商品やサービスは携帯取引事業者に代わって、消費者の携帯電話会社によって携帯電話加入者に請求される。ある場合では、携帯電話商取引サービスの提供における関係は上記の二番目の例に示されるように、特にサービスへの代金が消費者の銀行口座やクレジットカードに記載される場合は、いっそう複雑である。

少数の OECD 諸国では、輸送会社と携帯電話会社の間で消費者が携帯端末を輸送チケットとして使えるように、輸送会社と携帯電話会社の協力関係が設立されたか、設立されつつある。これらの国で、消費者は携帯電話代請求書、クレジットカード、あるいは現金送付などのいくつかの方法によって課金される。これらの多角的な取引では、どの企業が消費者紛争を処理して、そして救済を提供することに対して責任を持っているかを消費者に明確であるべきである。

上記の2つの例は携帯電話会社と携帯取引事業者に以下のように奨励することが有益であるかもしれないと提案する：

- ・ 消費者の苦情に対して、公正で、効果的で、そして透明な内部メカニズムを確立すること。
- ・ 複雑な契約において、苦情を扱う責任を明らかに示す。優良事例は、この点に関して、事案の特定の状況と事案の特徴を考慮に入れて携帯電話会社か、輸送会社か、あるいは両方の、いずれかが消費者に対して責任があるかについて、ガイドラインを提供することである。

さらに、携帯電話商取引への参加者が、2007年 OECD 消費者紛争解決と救済に関する勧告によって推薦されているように、苦情処理や消費者満足規範、返金制度、裁判外紛争処理制度といった保証メカニズムの方法を考慮に入れるべきである。（「消費者紛争解決と救済勧告」附則第2条 A.7）

携帯電話会社、携帯取引事業者、ウェブサイト運営者、携帯金融事業者と政府が消費者苦

情を扱って、そして複雑な携帯電話商取引取引から生じている消費者問題を解決するために公正で、効果的で、そして透明な自己規制メカニズムや政策と手続きの確率に向けて協働することは有益だろう。

国境を越えた問題

高価な腕時計

ある消費者が安い価格において豪華な腕時計を宣伝したウェブサイトへのリンクが書かれた SMS を受けた。彼は同じモバイルサイトですでに類似の商品を買っていたのと、彼の母国語での情報を含んでいたのも、消費者は宣伝が本物であることを確信した。従って彼は腕時計を買うという注文をした。腕時計が配達されないのも、消費者は会社の顧客サービス課に苦情を言い、彼が商品を購入した事業者が実際は彼の国に本拠地を置かない別の会社によって経営されていたことが分かった。彼が政府の当局に苦情を言ったとき、事業者が国外に位置していたことから、何もすることができなかったと言われた。

電子商取引ガイドライン第2部3条 A i) 及び iii) は、事業者は、消費者に事業者の正確な、明確な、そして容易に接続可能な情報（地理的な情報も含めて）と、紛争を解決する方法を提供するように要求している。このような情報と救済メカニズムは国境を越えた取引に対する消費者の信用を強化するために必要で、加盟国に国境を越えた紛争で消費者救済策の有効性を強めることを求める *消費者の紛争解決及び救済に関する勧告* によっても求められている。（附則、第3条）

関係者は国境を越えた携帯電話商取引取引で消費者苦情を扱うために効果的な紛争解決メカニズムを確立することが求められている。

弱い消費者のための携帯電話商取引への接続

消費者の紛争解決と救済に関する勧告 で述べられているように（附則第2条、A.6）、携帯電話商取引が発展するにつれ、弱い消費者のための特別な必要性は考慮されるべきである。例えば、低い視力を持っている人々が小さな携帯画面上で開示情報や断り書きの記載を見ることは特に問題であるかもしれない。

Ⅲ. 未成年者の保護

たいていの OECD 加盟国で、未成年者（言い換えれば一般的に 18 歳以下の人々）は、商取引の契約、例えば音声での通話や彼らの携帯端末での商取引などのようなものを結ぶ法律上の能力を持っていない。これは、しかしながら、必ずしも彼らが彼らの親あるいはその他の成人によって契約されたものの一部である端末を使って商取引に携わるのを阻止してはいない。また若干の国で、未成年のうちの年齢の高い者が、未成年者にもかかわらず、事前の親の同意を得たことを条件に、そのような契約を結ぶことは可能かもしれない。このような未成年者の取引についての親の管理は現在自分自身の端末を所有する未成年者数の急激な増加のために危機にさらされている。(OECD2006、5-6 頁) 未成年者に間違っ

- ・ 携帯電話会社に年齢認証システムを適切に設定するよう奨励する。

しかしながら、今のところ、年齢認証技術は広範囲にわたって発達したとは言えない。これは厳しい問題である。携帯電話会社は例えば、子供たちに実年齢を入力する代わりに彼らの生年月日を入力するよう要求するなどして、年齢情報を詐称しにくくする方法で集めることができる。しかしながら、年齢認証技術がなければ、子供たちが偽の年齢情報を提出することでサイトの年齢判定メカニズムを避けることは難しくなく、それゆえ不適切なサイトに入り込んだり、あるいは親の認可なしで取引に携わることができる。これは、どんどん子供たちが携帯端末からオンライン活動に参加するにつれて、子供への追加的な安全措置を提供することができる補完的な技術の必要性を際立たせている。

親は通常、連絡方法やセキュリティを改善した携帯電話を彼子供用に提供するが、子供の携帯電話の使用はそれを超えて進んでいる。(OECD、2006、ページ 8) 彼らはますます料金のかかるサービス（着メロのダウンロード、ビデオ、チャットやゲームなど）に引き付けられている。結果として、彼らは商取引に携わっている。そして i) 有害であるか、あるいはアダルトサイトへのアクセスと ii) 積極的なマーケティングによる予想外に高額な取引のような危険にさらされている。

電子商取引ガイドライン第 2 部第 2 条は「事業者は自分たちが接している情報を完全には理解できない子供を対象にした広告やマーケティングに特別の注意を払わないといけない。」ことを規定する。この原則は子供たちと交流し、取引するモバイルサービスプロバイダ、携帯電話会社とその他の携帯電話商取引サービスを提供している事業者を規定する。

有害であるか、あるいは成人の内容への接続

成人専用

15歳の少年が、無料で新しいインターネットサイトを閲覧できるという勧誘のテキストメッセージを受け取った。彼はメッセージに返信して、そしてサイトのアドレスを獲得した。彼はサイトにアクセスし、それが性的にきわどいデータを含んでいることに気がついた。彼はこの勧誘を母親に報告し、母親は携帯電話会社とすぐに連絡を取り、自分の子供が誘惑を受けたことへの憤慨を伝えた。携帯電話会社はそのようなやり取りを止めるように最善を尽くしているが、いくつかの不適切な内容が滑り込んでしまうと説明した。子供がSMSに返信したとき、彼の連絡情報（例えば電話番号など）は潜在的顧客リストに登録されてしまった。彼はその後、勧誘のメッセージを次々受け取り、心配した母親は息子への新しい携帯電話を買うことを余儀なくされた。

無料の写真サイト

15歳の少年が友人たちからただで成人向き写真を提供しているウェブサイトについて知った。彼は、彼の親がしっかりとどのようなウェブをみているかを監視することが不可能であることを知って、彼の携帯電話を使ってウェブサイトアクセスした。ウェブサイトは、ユーザーは18歳以上でなければならない、という警告を含んでいた。彼は彼が18歳以上であると返答し、即座にアクセスを認められた。

事業者は未成年者が彼らの携帯電話端末からアダルトサイトにアクセスするのを阻止するいっそう効果的なツールを開発することを考えるべきである。電子商取引ガイドラインは、加盟国は「消費者を守るツールとしての技術の継続的な開発の民間部門のリーダーシップを奨励するべきだ」と述べている。(第3部、iii)、「執行」)。

インターネットにアクセスするコンピュータを使う消費者からある特定の内容をおくすのために、ソフトウェア開発に労力が割かれてきた。携帯電話商取引環境でこの問題に対処するために、ある国では携帯電話会社が自発的な行動規範あるいはガイドラインが、アダルトサイトへの子供のアクセスを制限することに対して設定された(附則1)。これらの枠組みにおいて、携帯電話会社、消費者を巻き込んだ事件へのいくつかの以下のような対応策が支持されている：

- ・ 親と子供のための認識向上キャンペーンを発展させる。
- ・ 興味を持つ対象は18歳以上か、あるいは参加への親の承諾を持っていないと警告をすべての音声と映像広告で行う。
- ・ 宣伝の内容分類化(アダルトサイトを一般の人がアクセスできるところから規制)

- ・ いっそう効果的な年齢認証手順の開発をする。

未成年者を守るために探究されうるその他の方法：

- ・ オンラインにおいて加盟国の子供たちを守っている既存法と規則をモバイル環境に適用する。
- ・ 携帯電話会社にアダルトサイトへの子供たちのアクセスを防ぐ事を助けるフィルタリングという選択肢が利用可能なことを親に知らせるよう奨励する。
- ・ アダルトサイトサービスを扱っている携帯取引事業者が i) 未成年を効果的に守る国内担当当局と協力する、ii) これらのサービスへの子供のアクセスを防ぐ適切なセーフガードを設定する
- ・ 例えばもし子供がアダルトサイトにアクセスしたら親にお知らせを送るような仕組みを設ける；
- ・ 端末が不適切な内容にインターネットでアクセスするのを阻止できるようなフィルタリングサービスを親が設定できるようにする。

マーケティング対象とされる子供達

着メロと関連アイテム

13歳の少女は、以前着メロを買った携帯取引事業者から彼女の携帯電話に送られてきた種々のメッセージに興味をそそられた。携帯取引事業者は彼女にあらゆる種類の商品およびサービスを買うよう勧めた。彼女は結局追加の着メロ、ゲーム、星占いを買うことになった。彼女の母親は携帯電話会社に広告メールを途中で遮断するように頼んだが、しかし携帯電話会社はそうする力がないと述べた。

望まれない広告

10歳の少年が彼の母親と一緒にショッピングモールで買い物をしていた。彼らがある店を歩いて通り過ぎたとき、彼は様々なお店から彼の携帯電話に広告が発信され、興味をそそられた。彼はこの新しい携帯電話のサービスに驚き、彼の母親に自慢した。母親は息子の端末にインストールされていたブルートゥースという技術の特性に気が付かなかった。彼らが家に帰ったとき、母親は今やブルートゥースによって可能になった、望まれない広告には良くない面があることを心配した。

電子商取引ガイドライン（第2部、第2条）で設定されているように、子供たちは彼らが接している情報を完全に理解する能力を持ってはいない。子供たちをターゲットにする汚い携帯電話商取引のマーケティングを防ぐことは難しいかもしれないが、携帯電話会社

に以下のようなツールを適所に配置するよう奨励することによって、それを制限する可能性はある：

- ・ 攻撃的なマーケティングのテクニックと携帯端末による支払いを確認する方法について親と子供を教育する。
- ・ 子供に誘惑を与えるような特定の広告、あるいは広告のタイプを防御する。
- ・ インターネットアクセスに制限を置く。
- ・ 未成年者である子供に与えられる端末としての携帯電話購入の禁止；あるいは
- ・ 親が識別する発信元以外からの全ての携帯電話メッセージを禁止（ホワイトリストとして知られる）

携帯取引事業者が購入者が未成年者だとわかる携帯電話商取引購入に対して、成人の認可を必要とするよう、奨励されうる。

「望まれない広告」の例は異なったタイプの問題を提起する。この場合、広告がブルートゥースを使って子供の電話に発信された。このような宣伝をすることは携帯電話会社を通して行なわれておらず、記録にも残っていない。この例は、親が子供によって使われる携帯電話端末の技術的な能力と特徴を認識している必要があることを示している。彼らは問題が発生したとき、これらの特徴をどのように修正することができるか知る必要がある。

携帯電話会社によるサービスの過剰消費

清涼飲料自動販売機

12歳のある少女が6学年クラスの代表に選ばれたとき、彼女は大喜びだった。昼食休みに、彼女は、彼女のクラスの同級生に清涼飲料を買うことによって、彼女の感謝を表現することに決めた。噂は急速に広まり、そしてまもなく彼女におごってもらうのを待つ300人の若い友人が現れた。彼女は携帯電話を飲み物の支払い使った。全体の料金は彼女の携帯電話の画面に現われた。毎月の請求書が彼女の家に着したとき、彼女の父親は400ユーロの料金を見てぼう然とした。

双方向ゲーム

16歳の若者が彼の誕生日のために携帯電話をもらった。彼の母親は彼に使いすぎないように注意した。若者は同意して、そして約束を守るように努めた。しかし、彼はテキストメッセージと双方向ゲームが非常に安かったのを見て、彼は多くの少ない料金が合計してかなりの額となっていたことを知らずに、たくさんサービスを使った。合計の月極の請求書は200米ドルに達した。

上記の例で見られるように、親はいつも彼らの子供の携帯電話の活動を監督する立場にないかもしれない。結果として、親はたくさんの料金を彼らがサービスや商品の購入に使ってしまうことを、阻止することができないかもしれない。テレビゲームと競いあうものは未成年者が特に狙われやすいようである。上述の双方向テレビの例で例証されるように、このようなゲームに対しての参加の費用についての情報は、常に明らかで参照可能であるというわけではない。

学校の構内あるいはショッピングセンターの自動販売機は未成年者のもう1つの誘惑の例である。彼らの携帯電話から、未成年者は自動販売機の上に表示された電話番号に電話をして、その購入への支払にすることができ、それは翌月の電話代請求書に現われる。

前出の特別価格サービスも同じく若い消費者の誘惑の一例である。これらのサービスは固定電話、ファクス、インターネット、テレビと携帯端末を含めて、いろいろなメディアを通して情報とエンターテイメントを提供する。子供たちはそれゆえ容易に競争、チャットなど幅広い分野のサービスに携帯電話などから電話をすることで接続することができる。典型的に、特別価格サービスの電話代は標準的な電話代より高つく。産業界は、未成年の携帯電話端末による消費を規制するような技術的なツールを開発し洗練し続けることによって支援することができる。このようなツールは、事業者に対して、消費者に情報と親や保護者の認証を求めたり、場所と時間の制限のような販売の条件や制限をする、電子商取引ガイドライン（第2部、第3条C.v）と一致する。

クレジットカード会社によって使われるアプローチはこの点に関して適切であるかもしれない。カードが個人に発行された後に、会社は本人の同意の下、彼らの家族メンバーへの追加のカードの発行を、元の契約者の限度額内で許す。信用限度額は限定され得、そして請求書が支払いのために最初の契約者に送らる。さらに、いくつかの国で、親が契約に特別な合意を提供しなければ、未成年者がクレジットカードを持つことができない。

いくつかの国では、さらに先に進んで、携帯電話会社により大きい責任を与えている。(附則1) ある国では、SMSを通じて参加するテレビゲームに関しては、携帯電話会社によって招かれた料金を親に弁償しなければならない。またある国では、一つのアクセス番号からのサービスの購入限度額を設けないコンテンツ提供者は違法とみなされるかもしれない。

未成年者による過剰消費を妨げるのを助けるために、関係者は以下のようにすることができる：

- 例えば親に子供のテキストメッセージの数に対する制限や、ダウンロード可能な

購入品に対する金額の制限を確立し、子供が携帯電話を使用して生じさせることができる金額に上限を設定する能力を提供する。

- ・ ユーザーが取引の種類を制限することができるように設計される携帯端末を奨励する。
- ・ 携帯電話会社に、出費が確立された上限を超えるとき、注意やお知らせを親に送るよう奨励する。

子供と位置情報¹

追跡継続

12歳の携帯電話ユーザーがインターネットで、彼女の電話番号を登録し、彼女が確認した人々の場所（ソーシャルマッピング）についての情報を受け取ることができる位置情報サービスに登録した。彼女はこれは彼女の学校の友人たちがその地域にくる時がわかって、テキストメッセージを送り、彼らに会うことができる、面白いチャンスだろうと信じた。彼らも彼女について同じく位置情報とプロフィールを受けとることができる。このような情報がどのように保護されるのか、あるいは誰がそれを見ることができるかについての開示がなく、確認プロセスさえない。彼女が携帯端末上のそのプログラムを止めるときでさえ、位置データは停止しない。彼女の親は彼女がこのようなサービスを契約したことを知らなかった。

上記の例は子供達に影響を与える、プライバシー、オンライン活動、携帯電話の消費の変わりによって取り上げられた問題を例証する。その他の、子供と成人両方に影響を与えるかもしれないプライバシーの問題は、下の「位置情報のプライバシーとセキュリティー問題」で議論されている。多くの OECD 国で、第三者への特定のタイプの位置情報の提供は非合法である；しかしながら、若干の国にこのような保護の程度に関してまだ未完の問題がある。追跡と第三者とのデータ共有についての情報開示の欠如は、これらの行為を成人に警告するプロセスが欠如しているので、多くの国で大きな影響を与える。全てを情報開示することが問題を扱うのに役立つかもしれないが、それは十分ではないでしょう。

電子商取引ガイドラインは、すでにマーケティングビジネスが消費者に不当な被害の危険をもたらす可能性が高い行為に従事すべきでないといったいくつかの一般原則を作っている（第2部、第2条の第2の paragraph）。そして事業者が自身と提供する商品あるいはサービスについての情報を明確で、目立ち、正確で、そして容易に入手可能な方法で提出すべきであるという原則を含めて一般的な信条を明らかにした（第2部2条の第3番目の paragraph）。ここで、追跡情報は、事業者が取引の要件、条件と価格に関する十分な

¹ 位置情報は地理的な位置の情報と、携帯端末の移動の情報の両方を含む。

情報を消費者が取引に入るべきかどうかについて、知らされた上での決断をすることができるようにするために提供しなければならない、という原則から検討されるべきである。このような情報は明確で、正確で、そして容易に入手可能でなくてはならない。上記のとおり、電子商取引ガイドラインは同じく消費者を守り、権限を与えるような道具としての技術の開発で民間部門のリーダーシップをとることを奨励する。それを目指して、事業者は以下のようなことができる：

- ・ 追跡について明確な情報開示をする。
- ・ 第三者とデータを共有することを明確に情報開示し、それをどう制限するかについて明確な公表をする。
- ・ これを成人の認可が必要とされるサービスとして扱う。
- ・ なるべく初期設定で、特別な追跡サービスを止めるというオプションを提供する。

IV. 携帯電話の不正使用と安全問題

携帯端末の小ささと機能性は泥棒にとって以下の点で魅力的である。 i) 端末を再利用したり、転売する、ii) 法的な所有者の名前で、不正や違法な方法で商売をする、iii) 個人の機密情報を入手する。盗難の危険性は、携帯端末と同じように公共の場で持ち運ばない、すえつけや大きめのノートパソコンのような標準的なコンピュータより、様々な面ではるかに高くなる。

携帯電話の不正使用

携帯電話の不正使用の危険性への認識を高めてもらうことは、事件数を下げるのに役立つであろう。電子商取引ガイドラインの第2部第8条に述べられているように、関係者は「協力して消費者のオンライン活動に適応される、消費者保護の枠組みへの認識を高めるように、電子商取引に対する消費者教育に励まなければならない」。消費者が携帯端末を盗まれたり失くしてしまった場合に何をしなければいけないかを教育することは、他の不正使用を防ぐ重要な点である。したがって関係者は以下のように一緒に協力するべきである：

- ・ i) 認識を高める；ii) 携帯端末を紛失や悪用から守る原則；そしてiii) 消費者が携帯端末の紛失や悪用に気がついたときに何をすべきかの指針などの情報を消費者に提供する

短期間の大買物

ある消費者が携帯電話をなくしたが、すぐに見つかるだろうと思って、電話会社にも警察にも連絡をしなかった。3日後に、警察は消費者に彼の電話が見つかったと連絡した。しかしながら、電話が失われた時から警察がそれを見つけた時までの間に、誰かが高価な携帯サービスをおよそ 2000 米ドル分も使っていた。消費者は彼が全額を支払う必要があると知ってショックを受けている。

上記の例は端末へのある種の暗号化や、サービスへの暗証番号などによって提供された安全対策を使うことの重要性を強調する。携帯端末が見つからないとき、すぐに気づくことの重要性も強調する。盗難の場合、以下によって責任を制限できる可能性がある：

- ・ 消費者に携帯電話会社が制限している責任限度額より低い限度額を設定することを可能にする。
- ・ 必要に応じて遠隔操作や技術的な端末で、消費者が端末を機能停止にして不正使用を防ぐ手段を提供する。
- ・ 全ての商行為や端末の機密情報に接続することに、暗証番号を使用することを要求する。
- ・ それらの端末への接続を制限するために、パスワードの使用や、その他の技術が大事であることを消費者に教育する。

SIM カードの暗証番号は、一般に「0000」が初期設定となっている²

- ・ 端末の不正使用をやめさせるために、携帯電話会社と携帯端末卸売業者は i) 初期暗証番号としてランダムな数字を設定する。そして、ii) 消費者に初期の暗証番号を最初の使用時に変更するように促す。

通話中のサイン

ある若い女性が仕事から家に帰る途中に、彼女の携帯電話を失った。彼女が盗難に気づいたとき、彼女はすぐに彼女の携帯電話会社に電話をした。数回、回線は通話中だった。他の時は、顧客サービスを 20 分待った後で、彼女は諦めた。数日後に彼女は携帯電話会社と連絡を取ろうとしていた間に彼女の携帯電話がおよそ 1000 ユーロのサービスを購入するのに使われたことを知って激高した。

² これはいくつかの OECD 国の携帯電話で使われている Code Division Multiple Access(CDMA)には適応されません。

携帯電話契約者が電話回線が込み合っている等の理由から、携帯電話会社の盗難担当者に連絡できなかった期間まで、加入者に端末の不正使用に責任を負わせたままでは、公平性の観点から疑問がある。連絡の困難さは消費者を不当な被害の可能性にさらし、電子商取引ガイドラインや、そして消費者の紛争解決と救済に関する勧告（第4部）とも一致しない。このような状況を避けるために、携帯電話会社が次のようにすることが奨励される：

- ・ 例えば端末の紛失や盗難を電子メールやオンライン上で、簡単に報告できるような十分な手段を提供する。
- ・ 消費者が「入力する」事によって、紛失若しくは盗難にあった端末を使用不可能にする特別な回線を設定する。

多くの国で失われた携帯電話のための報告メカニズムを改善する努力が行われた。ある国では、携帯電話会社が協力して紛失届けの出た携帯電話をすべてのネットワーク上から48時間以内に排除するという憲章に署名した。携帯電話は国際携帯電話身元確認番号（「IMEI」）³が装備されているので、それぞれの会社が遠隔操作を通じて携帯電話をロックして、使用不可能にすることがSIMカードとIMEIに制約を加えることで可能である。

携帯電話が支払い端末として使用される場合、クレジットカードの使用とは責任が異なることは指摘されるべきである。あるOECD国で、消費者は、多くの場合、盗まれたクレジットカードの支払額には責任を持たない。一方、携帯電話が支払い端末として使用される時、携帯電話加入者は同じレベルの保護を保証されない。たいていの加盟国の携帯電話会社は、SIMカードあるいはICチップの無許可の使用によって起こされたいかなる損失もカバーしない。しかしながら、少数の国では、通信サービスのあらゆる種類の不正使用から生じた責任を制限するように法律を改正した。この問題を扱うために、政府と産業界は以下の方法を望むかもしれない：

- ・ それらの携帯電話の使用に対しての責任を保護する方法として、；電子商取引ガイドラインと消費者紛争と救済に関する勧告が述べているように、消費者債務の制限と請求の払い戻しのメカニズムは消費者保護を助ける強力な道具になる。

³ CDMA ネットワークテクノロジーを使っている携帯電話は、端末を特定できるIMEIのような、電子連続番号（ESN）を装備している。

外国での休暇

ある女性が外国で夏休みを過ごしているとき、市場で買い物をしていた間に、携帯電話を盗まれた。彼女は損失を後悔したが、それが遠距離通信ネットワークと互換性がないので、携帯電話会社が彼女の電話は外国では使えないと言っていたので、悪用されることについて心配していなかった。したがって、彼女は家に帰るまで、紛失を報告しなかった。携帯電話会社は彼女に悪いニュースを知らせた。およそ 20000 米ドルが彼女のアカウントにチャージされていた。彼女の携帯電話が外国で使えないのは本当であるが、携帯電話会社は彼女に IC チップ（あるいは SIM カード）が彼女の電話から取り除かれて、そして異なった端末で使うことができることを言い損ねていた。会社はこのことは提供した情報では、明確ではなかったことを認めたが、彼女に支払うことを強く主張した。彼女はこれを法廷に持ち込み、勝訴した。

上記の例で、携帯電話会社は彼女の IC チップの外国での動作に関する完全な情報を顧客に提供すべきだった。電子商取引ガイドラインの第 5 章、第 2 部で規定されるように、消費者は安全な支払い制度とそのメカニズムによって与えられる安全のレベルについての情報を提供されるべきである。より多くの消費者が外国で携帯電話を使うにつれて、この原則は特に重要性を増す。従って以下のような努力がなされるべきである：

- ・ 携帯電話化入者が、端末を購入するときに、彼らの端末が外国で作動するのか、明確で完全な情報を受け取ることを保証する。
- ・ 携帯電話自身が外国で使えなくとも、端末の IC チップが不正使用されることがあることを、購入時に警告する。

悪質なローン

ある男が、ローンを契約するために、職場の同僚の許可なしで同僚の携帯電話端末と電話番号を使った。ローンを契約するために、彼は携帯電話契約者の名前を示したメッセージを送った。ローン会社は送り主のそれ以上の身元確認をしなかった。

他人の携帯電話を使って、誰かの名前で購入をするためにことを許すことは以下の二つの点から電子商取引ガイドラインの第 5 条に反する： i) 支払いの安全性 ii) 公正な事業、広告とマーケティング（なぜならそのような慣行は消費者の不当な被害の危険性を高めるため）。そのような慣行を防ぐためには、安全装置とそのためのツールは携帯端末上での契約の締結に関して本人確認することが有効かもしれない。これは以下の方法である程度対処されることができる：

- ・ 携帯端末に口座を持っている本人からの注文だけに注文を制限する
- ・ 加入者の身元を、SMS や携帯電話電子メール、あるいはパスワードなどの情報を使うことによって確認する。

携帯電話の安全性

モバイル銀行業の違反

ある携帯電話契約者がたった1つのクリックでいつでもどこでも、無料のモバイル銀行のアプリケーションに接続できると宣伝する、無料のモバイル銀行サービスの広告を受けとった。広告は消費者が明細表をみることや、アカウント間の送金、そして請求書を受け取って、そして支払うことが、家のパソコンを使ってするのと同じようにできると述べていた。プライバシーと安全管理を保証するのを助けるために、モバイル銀行のアプリケーションはパスワードで保護されて、暗号化され、そしてさらにどんな不正使用からも消費者を守ると述べていた。テキストメッセージで送られた広告には申込書へのリンクを含んでいた。携帯電話契約者は申し込みを完了し、サービスに登録して、そして使い始めた。

翌月、携帯電話加入者はアプリケーションと銀行のデータへの接続への高額な料金を含んでいる請求書を受け取った。銀行の広告はこれらの料金を明らかにしていなかった。その翌月、消費者は無許可の引き落としが銀行口座で起こったことを知った。彼女は携帯電話会社が料金を削除するようにしようとしたが、彼女を銀行に差し向けただけだった。そして調査の後に、消費者の銀行のデータは安全ではなくて、危険にさらされていたようだと言明した。

この仮説のケースは消費者に以下のような問題を提起する i) 携帯電話の、特に支払い端末としての安全性； ii) データへの接続費用；そして iii) 妥当な紛争解決と救済システムの利用。ここでは、ワイヤレスセキュリティーや消費者保護問題に焦点を合わせ、他の二つは双方向テレビと携帯電話交通チケット、高価な時計に関してすでに述べているので参照下さい。

携帯端末はモバイル銀行業のような幅広い動作を実行することができるミニコンピュータにどんどんなっている。ノートパソコンやより小さい端末を支えているワイヤレスネットワークの安全性はますます共通のニュースの話題になっている。侵入者はインターネット・アクセスを持っているたいのコンピュータと同様に、例えば電子メールウイルスなどを通して、消費者のワイヤレスコンピュータあるいはネットワークに入ることができる。さらに、ハッカーなどは携帯端末から情報を得ること（例えば、ブルートゥース、

ラジオ周波数身元確認（「RFID」）チップ）、携帯端末を感染させること（例えば、アプリケーションダウンロードを通して）等の追加の方法があるかもしれない。スパムとマルウェアが現在コンピュータほどは携帯端末上で流行していないが、携帯電話取引の使用と価値が上昇すると、個人情報や金融のデータを得ることの重大性や、携帯端末を使ったスパム詐欺、個人情報窃盗等も増加するであろう。

さらに、上述のように、携帯端末を支払いに使うことはいつそう一般的になっている。若干の国で、携帯電話での支払は、SMS、あるいはテキストメッセージによって行なわれているが、一方で他の国々では、携帯端末に REID チップを装備しているので、読み取り装置の前にただかざすだけで支払いの情報を送信することが可能である。これは新しい安全上の危険を広げるかもしれない。

電子商取引ガイドライン（第二章、二条「プライバシー」）はこの状況を、事業者の消費者に対する電子商取引が、プライバシー保護と個人情報の国際流通に関する OECD 行動指針（「プライバシーガイドライン」）、2002 年情報システム及びネットワークのセキュリティのための OECD ガイドラインに従い、1998 年グローバルネットワークにおけるプライバシー保護への OECD 理事会宣言を考慮に入れ、行わなければいけないということの延長線上に定めている。しかしながら、追加的措置の必要性があるかもしれない モバイル産業への参加者が以下のようにすることは有益であるかもしれない：

- ・ 消費者が携帯電話商取引で遭遇するかもしれないプライバシーの課題と、その危険性を抑制する可能性がある手段を知らされることを保証する。
- ・ 安全への予防策と組み込まれた安全措置の開発を奨励する。
- ・ 携帯電話会社にデータ保全方針と情報漏えいと不正取引の防止を実行するように奨励する
- ・ 消費者の情報が危険にさらされたり、彼らが経済的損失を被ったときに迅速で効果的な対応策の提供をする。

位置情報のプライバシーと保全問題

無許可の追跡

ある携帯電話会社は全地球位置把握システム（「GPS」）あるいは三角測量（端末から発生する信号を利用する）ことによって、携帯電話の使用者の位置を把握する。その会社は、マーケティング会社が個人に合わせた広告あるいはお知らせを携帯電話契約者に送ることに使うために、位置情報と加入者の情報を販売した。ある携帯電話契約者は了解しておらず、彼女のこのような個人情報の転送を許可してもいなかった。彼女はそれらのお知らせに課金されるかもしれない（例えば近くの安売りのテキストメッセージや、

インターネット接続時のポップアップメッセージなど)。彼女は追跡によって気分を害されていて、情報が（盗まれるか、あるいは買われることで）犯罪者にわたる可能性があることを心配している。

上記の例は追跡による位置情報による課題を例証している。問題は情報安全確保プロセスの欠如と、上述の子供の保護（追跡の継続）の例で論じたように、非緊急時の目的で追跡を停止する仕組みの欠如にある。

位置情報の安全に対する保護の必要性は、事業者・消費者間の電子商取引を規定した 1980 年プライバシー規則（第二部、7-10）にあるプライバシー原則、1998 年グローバルネットワークの保護に関する OECD 理事会宣言を考慮に入れて行われなければならないとした、電子商取引ガイドライン（第七章、二部）の原則によって扱われている。

事業者が以下のようにすることは有益であろう：

- ・ 消費者に全ての収集されている位置情報と、それらの情報の使用の目的を明確に開示する。
- ・ 消費者に第三者とのデータの共有を制限するとともに（緊急時を除く）、そのような情報が誰と共有されるのかについての決定を見直せるような機会を提供する。

加えて、位置情報を集める会社は、特にデータの機密性が高かったり、特定の個人が識別できるような情報への安全確保には適切な措置を講じなければならない。

附則 1

未成年者の保護：いくつかの OECD 国における法と自主規制の体制

成人向けの内容へのアクセス

携帯電話が引き起こす課題に対して、多くの国で対策がとられた。オーストラリア、デンマーク、ドイツ、日本、韓国、ノルウェー、英連合王国とアメリカでは、例えば、携帯電話会社が成人向けの内容へのアクセスを制限するための自主規制を発達させた。アメリカでは、いくつかの携帯電話会社が成人の内容へのアクセスを制限し、親がそれをコントロールできるようにするために、自発的な内容の分類とインターネットの接続の規制を採用した。www.ctia.org/advocacy/policy_topics/topic.cfm/TID/36 参照) これらのガイドラインの下で、参加している携帯電話会社は現在すべての成人向けのウェブサイトを禁止し、そして 18 歳以上か親あるいは保護者の許可がない場合はそのようなサイトへのアクセスを制限している。さらに、子供のインターネット保護決議（「CIPA」）は E-レートプログラム（適格な学校と図書館のためにある特定の技術をより入手可能にするプログラム）に参加している学校と図書館に、わいせつであったり、児童ポルノを含んでいたり、あるいは未成年者に有害な内容へのインターネット・アクセスを制限するか、あるいはフィルタリングする技術的保護策を含めて、インターネット安全政策を持っていることを証明するように要求している。

加えて、ヨーロッパとアメリカの両方でガイドラインを設定する国際的な集団である携帯電話マーケティング協会（「MMA」）、は最近アメリカの 13 歳以下の若年期へのマーケティングの優良事例を改定した。<http://www.mmaglobal.com/bestpractices.pdf> 参照) 例えば、ガイドラインは音声と映像の公開のために、参加者が 18 歳以上であるか、あるいは親の許可を持っていないと規定する。同じように、2007 年 2 月、ヨーロッパの代表的な携帯電話会社は、未成年者や子供により安全な携帯電話の使用のヨーロッパの枠組に合意した。http://ec.europa.eu/information_society 参照) このような枠組みの下で、携帯電話会社は親と子供の認識向上キャンペーンを支援するとともに、商業的な内容の分類（成人向けの内容を一般的にアクセス可能な内容から制限する）と年齢認証手続きの発展の支援をしている。

子供の個人情報保護

国は子供を守るためのオンライン上の既存の法令・規則を携帯電話環境にも同様に適応することを研究している。例えば、アメリカでは、連邦法がオンライン・サービスでの 13 歳以下の子供たちの個人が特定できる情報の収集、使用、開示を禁止する。これはプライ

バシー政策についての通知、子供の情報を収集することへの両親の許可の確認（限定的な例外あり）、子供の情報についての親の確認と削除、そしてその情報の安全性を守る仕組みの必要性、を含む。

携帯電話によって提供されたサービスの過度消費

いくつかの国はさらに進んで、携帯電話会社に対してより大きな責任を課している。フィンランドでは、消費者苦情委員会はテキストメッセージと一緒に遊ぶテレビゲームを含んだサービスの提供者の責任を確立した。携帯電話会社は根拠がない利得を受けたことが判明した。親が子供に親の携帯電話を使うことを許していたという事実が、子供に合法的にテレビゲームのような商取引を行う事を許したかは疑問がある。決定によって、消費者は払い戻しの資格を得ました。

マーケティング対象の子供たち

電子商取引ガイドラインは事業者が子供を対象にした広告あるいはマーケティングをするときは、子供達は接している情報を完全に理解する能力を持たないかもしれないので、特別な注意が必要だと勧告している。同様に、MMA ガイドライン（パラグラフ 4.0）は提供される「全ての種類のデジタルコンテンツの販売促進や消費に子供を巻き込むプログラムは、全ての業界の参加者が持つことを期待されている倫理的懸念と、責任、敏感さを課されている。」と述べている。いくつかの国が法律や規則でこのようなマーケティングを制限しているが、ほとんどが携帯電話につきものの特異性への対策を持っていません。1つの例外がイギリスで、携帯電話による子供を対象にしたスナック菓子の広告が禁止された。

アメリカ版の MMA ガイドラインは 13 歳以下の子供を直接対象にした、短距離とマルチメディアワイヤレスメッセージに関して（パラグラフ 4.0 参照）、すべてのワイヤレス産業の参加者に対して、サービスがプレミアム料金であるならば、その旨と；実際の値段ともし通常のメッセージ料金もかかるならばその旨を、すべての音声と映像の広告で明らかにすることを求めまし。ガイドラインはそのサービスに関係した料金や課金が無い場合を除いて、「無料」の文字は使えないことも述べている。

フィンランドでは、保護者業務決議が未成年者は年齢相応の取引だけをおこない、ほとんど重要性を持ってはならないことを規定する。フィンランドの通信マーケット決議の下で、フィンランドの通信規制当局が通信業務のための禁止カテゴリーを定義する。加入者、例えば親が、彼ら自身が電話したりテキストメッセージを送ったりしたくない追加

料金サービスのタイプを決定することができる。特定のサービスのカテゴリーを禁じる、または問題のカテゴリーに属するすべてのサービスを禁止する。消費者オンブズマンも未成年者の携帯電話契約者の状態に関してその向上を交渉し、その点に関して事業者とも協力してきました。消費者オンブズマンは携帯電話会社にも請求、苦情、保証の適切な扱い手として携帯電話会社の注意を引いている。

携帯電話の不正使用

フィンランドで、契約者の身元確認の問題が調べられた。法務省は、例えば、SMS 簡易ローンに、政府の法律の改正法案を立案するためにワーキンググループを設立した。消費者の身元確認は現在携帯電話の契約についての情報と社会保障番号のみに基づいている。ワーキンググループはいつそう信頼性が高い方法でクレジット会社が顧客を識別する法的義務があるべきかどうか検討するだろう。

プライバシーへの懸念

フィンランドの電子通信のプライバシー保護に関する法令は、直接の電子広告が消費者に送られる前に、消費者からの許可を得ることを要求している。データ保護オンブズマンと消費者庁 / 消費者オンブズマンは例えば、「友達に伝えて」商法と呼ばれる商慣習に関して、受信者からの事前の許可を要求するガイドラインを発展させた。（「友達に伝えて」商法とは、消費者が商品の秘密情報、紹介目的の割引、コンテスト招待と他の広告メッセージを彼らが知っている人々に電子メールあるいはテキストメッセージによって転送することを指す）

フィンランドの電子通信のプライバシー保護に関する法令は個人情報と位置情報の機密性も扱っている。これは個人情報の商業用の目的での処理や、位置情報の処理及び公開への制限を含みます。また、位置を特定される者のサービスごとの同意の必要性もカバーする。15 歳以下の未成年者の場合は、保護者が位置情報を処理する事の決定に責任を持つ。

アメリカでは、携帯電話会社がユーザーの位置情報を第三者に転送することは、消費者所有のネットワーク情報（CPNI）に関する法的規制によって制限されている。特に、アメリカの連邦通信法令の 222 条は、ワイヤレス位置情報の公表あるいは使用は、指定された緊急事態でワイヤレスユーザーの緊急電話への返答や、自動現金データの転送などを除いて、消費者の事前の承諾がない限り禁止している。さらに、要求されていないポルノや広告の攻撃を管理する法案（CAN SPAM）は、契約者の事前の承諾無しに、インターネットを通じて、ワイヤレス端末に直接送られる携帯電話の商業用メッセージを禁止している。

加えて、アメリカの電話消費者保護法令（「TCPA」）は、電話とテキストメッセージのワイヤレス携帯端末への通話を含んで、自動ダイアルシステムや人工的なあるいは事前に録音されたメッセージを使用していかなるワイヤレスの電話番号にかけるの事を禁止している。

附則 2

携帯電話産業問題に関わる OECD の協定書

消費者保護協定書

- ・ 1999 年 電子商取引の文脈での消費者保護のための OECD ガイドライン
(1999 OECD Guidelines for Consumer Protection in the Context of Electronic Commerce.)
- ・ 2003 年 国境を越えた詐欺的及び欺瞞的行為から消費者を保護するための OECD ガイドライン
(2003 OECD Guidelines for the Consumer Protection against Fraudulent and Deceptive Commercial Practices Across Borders (OECD, 2003)) これは、全てのオフラインとオンラインの詐欺行為を国内及び国際レベルで撲滅するための枠組みである。
- ・ 2007 年 消費者の紛争解決及び救済に関する OCDE 理事会勧告
(2007 OECD Recommendation on Consumer Dispute Resolution and Redress (OECD, 2007c))
これは、消費者に彼らの苦情を解決し、救済を得る効果的なメカニズムを、国内及び国境を越えたレベルにおいて提供することを目指している。
- ・ 2008 年 オンライン個人情報窃盗への OECD 政策指針
(2008 OECD Policy Guidance on Online Identity Theft)

安全、プライバシーとスパム対策の協定書

- ・ 2002 年 情報システム及びネットワークのセキュリティのための OECD ガイドライン
(2002 OECD Guidelines for the Security of Information Systems and Networks (OECD, 2002))
これは、国際的に互いに結びついた社会で、セキュリティの危険に国内でのアプローチとの調和を保證する方針を設定したものである。
- ・ OECD (2007d)、電子認証に対する勧告及びガイドライン
(Recommendation and Guidance on Electronic Authentication)
www.OECD.org/dataOECD/32/45/38921342.pdf
- ・ 1980 年 プライバシー保護と個人情報の国際流通に関する OECD ガイドライン (OECD, 1980)

(1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data)

これは、個人情報の収集と処理に関する方針を含んでいる。

・2007年 プライバシー保護法の執行に係る越境協力に関する理事会勧告 (OECD、2007e)

(2007 OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy)

これは、加盟国の当局にプライバシー法の施行に関して、他国の当局と協力し、補助しあう事を要求している。

・2006年 OECD 政策手段提案のスパム対策ツールキット

(2006 OECD Anti-Spam Toolkit of Recommended Policies and Measures)

これは、スパム対策の戦いに国際的な協力を容易にし、OECD 加盟国間のスパム対策の主導権の施行する補足的な政策を設定する提案のまとめを提供することを目的としている。

文献

- EC (European Commission) (2006), *Special Eurobarometer Safer Internet*, May 2006, http://ec.europa.eu/information_society/activities/sip/docs/eurobarometer/eurobarometer_2005_25_ms.pdf.
- EC (2007), *12th EU Implementation report on European Electronic Communications Regulation and Markets*, COM(2007)155, 29 March 2007, http://ec.europa.eu/information_society/policy/ecom/doc/implementation_enforcement/annualreports/12threport/com_2007_155_en.pdf.
- ITU (International Telecommunications Union) (2004), *Mobile phones and youth, a look at the US student market*, February 2004, www.itu.int/osg/spu/ni/futuremobile/Youth.pdf.
- OECD (Organisation for Economic Co-operation and Development) (1980), *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, OECD, Paris, www.OECD.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html.
- OECD (1999), *Guidelines for Consumer Protection in the context of Electronic Commerce*, OECD, Paris, www.OECD.org/document/51/0,2340,en_2649_34267_1824435_1_1_1_1,00.html.
- OECD (2002), *Guidelines for the Security of Information Systems and Networks*, OECD, Paris.
- OECD (2003), *Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders*, OECD, Paris, www.OECD.org/sti/crossborderfraud.
- OECD (2006), *OECD Anti-Spam Toolkit of Recommended Policies and Measures*, OECD, Paris, www.OECD-antispam.org/.
- OECD (2007a), *Mobile Commerce*, DSTI/CP(2006)7/FINAL, www.OECD.org/sti/consumer-policy.
- OECD (2007b), *OECD Communications Outlook 2007*, OECD, Paris, <http://213.253.134.43/OECD/pdfs/browseit/9307021E.PDF>.
- OECD (2007c), *Recommendation on Consumer Dispute Resolution and Redress*, OECD, Paris, www.OECD.org/dataOECD/43/50/38960101.pdf.
- OECD (2007d), *Recommendation and Guidance on Electronic Authentication*, OECD, Paris, www.OECD.org/dataOECD/32/45/38921342.pdf.
- OECD (2007e), *Recommendation of the Council on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy*, OECD, Paris, www.OECD.org/dataOECD/43/28/38770483.pdf.