



Global Business Dialogue on Electronic Commerce

# **GBDe 2003**

## **提 言 書**

(仮 訳)

**2003 年 11 月 6 日**

## 目 次

I. 消費者信頼構築 WG.....	3
1. インターネット決済.....	4
2. 求めざる電子通信、通称“スパム”多角的取り組み....	19
3. ADR（裁判外紛争処理）ガイドライン.....	37
(GBDe と Consumers International との合意に基づく)	
II. インターネットの未来 WG.....	50
1. ブロードバンド.....	53
2. サイバーセキュリティ.....	78
3. RFID.....	85
III. アドボカシーWG.....	88



Global Business Dialogue on Electronic Commerce

## 消費者信頼構築WG

2003年11月6日

議長：	Hermann-Josef Lamberti
(欧州/アフリカ)	COO & Member of the Board Deutsche Bank
共同議長：	日本電気
(アジア/オセアニア)	取締役専務 川村 敏郎



Global Business Dialogue on Electronic Commerce

## 消費者信頼構築WG インターネット決済

2003年11月6日

議長：	Hermann-Josef Lamberti
(欧州/アフリカ)	COO & Member of the Board Deutsche Bank
共同議長：	日本電気
(アジア/オセアニア)	取締役専務 川村 敏郎

## 1. はじめに

適切な支払いシステムが存在することが、電子商取引の発展の上で極めて重要なことに疑いはない。インターネットが形ある購入物の発注のみに利用されていた時には、支払いはその物品の配達時に伝統的手段をもって執り行なうことも出来た。しかしながら、取り扱う物件がデジタル製品やサービスとなると（例えばニュース、音楽その他の娯楽関係、ソフトウェア、金融サービスなど）、適切な支払方法が必要となってくる。対応する支払い業務処理を伝統的な物理的書類ベースのシステムに頼ることなく（つまり、一貫したオンライン処理で）行うことが、電子商取引発展上の基石となる。それは、ビジネスと消費者の双方に利点を与えて、世界的なマーケットを拓くことになる。

## 2. 現状

現状は満足行くものではない。古典的な支払手段は何かしらの紙片（例えば現金や小切手）の物理的な交換に頼るか、手書きの署名を必要とする（例えばクレジットカードやデビットカード支払いシステムに於ける様に）。<sup>(注1)</sup> 古典的な支払いシステムをオンライン環境に適用する上での問題点は、それらのシステムがインターネット上では提供されていないインフラストラクチャに頼っているという事である。

過去10年間に及び、特別にオンライン向けに設計された数々の新しい支払いシステムが開発されてきた。現金をそれで置き換える新しいサイバー貨幣を作り出したシステムも、新しい認証システムに基づいたシステムもあった。しかしながら、その様な新支払いシステムにとっての典型的な問題点は、電子商店の方ではその様なシステムが納得行くだけのマーケットシェアを取らぬうちは中々受け入れたがらないと云う事であり、一方、顧客の方でも一部の電子商店でしか使えぬようなシステムは使う気がしないと云う事であった。その結果として、どの新支払システムもその存在を支えるに必要なだけの顧客を獲得できなかった。支払いシステムというものは、スケールのビジネスであるから、取扱高が少なくでは存在し得ないのである。そこで、多くのシステムは消え去ってしまった。投資家はそのシステムからの収入或いは収入予想に満足しなかったからである。

---

<sup>(注1)</sup> 物理的に存在する販売現場においては、個人暗証番号（PIN）で手書き署名が置き換えられることがある。しかしこの手法をオンラインに適用しようとした場合には、個別網の様な安全な通信環境を必要とし、従って、インターネットには適用できない。

この様にして、オンライン経済には未解決の問題が残されてしまった。未だに古典的な支払いシステムが、多くの場合には何らの不正使用防止策も取り入れられぬままに、オンラインに適用すれば何がしかの不正使用は有り得るということ勘定に入れた上で、利用されてきた。その典型的な例が、カード番号又は口座番号だけを送信するクレジットカード支払い又は直接デビットカード支払である。たとえ通信チャネル自身の安全が確保されていても（例えばSSL送信の様に）、商店側にしても支払いサービス提供者側にしても、実際に数字を送信してきた人物の特定は出来ないのである。カード又は口座番号の不正使用が起こった場合の金融リスクは、多くの場合には商店か支払いサービス提供者又は保険によってカバーされている。しかしながら、結局のところ、支払不成立による損失や保険のコストは商品の価格に転嫁されることになって、商店と顧客の双方にダメージを与える。

加えて、この安全性の問題は顧客に負のイメージを与える。そして顧客はインターネット上でカード番号や口座番号を伝えることを恐れるようになる。

その結果、このままで物事が推移していくと、支払システムが電子商取引発展上のボトルネックになってしまいかねない。

### 3. 我々の調査結果

現状を踏まえ、合わせて電子商取引における支払システムの重要性を考えて、G B D e は世界各国の様々な産業セクタを代表する関係者に対して、一体主として何がインターネット決済を妨げているのかと問いかけた。

この調査を通じて得た、問題解決に向けての鍵となる意見は、支払システムの市場は明らかに取り扱うビジネスの規模に支配されるので、どの様な新しい支払システムもそれが既存のインフラストラクチャを前提とするもので無ければ出現することが難しい、という事であった。そして、多くのビジネスリーダー達は、もしどこからも利用出来て安価でしかも使い易い認証システムが存在すれば、それは、インターネット決済システムを構築する上で大いに役立つだろうという点に賛成した。それは不正使用問題が認証問題に大きく関わっているからである。

ビジネス規模の問題を抱えるからこそ、認証システムの標準化の問題は総ての支払システムにとって重要である。さもないと、個々の支払システムを様々な異

なる認証システムに適合させる為に多大な努力を要することになってしまう。技術的な相互互換性の確保の問題は、国際的な法制度の整合問題と並んで、国際的な支払システムをコストをかけずに実現する上で重要である。<sup>(注2)</sup>

#### 4. 認証 - インターネット決済システム実現の鍵

調査結果に基づき、G B D e は認証こそがインターネット決済システム実現上の鍵であると申し述べる。加えて、認証は支払の為にだけ重要なものではない。商業的な活動の中には、情報の交換にも認証を要するものがある。<sup>(注3)</sup> 一般的に言って、法的に拘束力のある契約を結ぶ際には認証が必要となる。加えて、多くの電子政府応用では法律によって顧客認証が義務付けられている。<sup>(注4)</sup>

インターネット決済は認証と密接な関係がある。実取引の世界では現金なるものの存在が、認証なしでの物品購買を可能にしているが、それは取引が不可逆だからである。しかしながら、他の総ての場合において（小切手の場合でも、デビットカード又はクレジットカードの場合でも）、現金移動は直ぐには実行されない。正確には、買い手は売り手が買い手の口座から何がしかの金額を移動して良い、と約束するだけなのである。もし買い手が後日に支払を拒否するという最悪の場合には、売り手は要求の実行を訴訟に持ち込まねばならない。訴訟には事実が要求される。特に売り手は、顧客から受け取った意思表示書が認証されたものであって、しかも改竄されていないこと（信頼性）の証拠を示さなくてはならない。

我々の調査結果によれば、不正使用の問題は、主として認証の欠如によるものである。他の問題、例えば信用度合い評価の適用誤まりの様な問題は少数である。つまり、顧客が誰であるかを明確に確認できさえすれば、売り手というものは顧客が請求書に対して支払えるだけの金を持っていない顧客であるかどうかの扱い方を心得ていると、回答者は考えているということである。

騙しの手段の一つに、成りすましがあがる。最悪の場合には、総ての身元の証明を盗み出してしまふ。これは、身元証明が盗まれた者にとって、不愉快極まるものである。成りすまされた者は支払を拒否するが、売り手は被害者のことを支払拒否常習者と看做してその後の取引を拒否するかも知れないし、また、被害者の

---

<sup>(注2)</sup> 未だに国際的な支払システムの実行は多くの報告義務を伴い、それが故にコスト高であり、かつ煩わしいものになっている。

<sup>(注3)</sup> 例えば、金融サービスにおける口座の開設や保険会社との間の契約の解除

<sup>(注4)</sup> 例としては、ドイツにおける電子的手段による税申告が挙げられる。

名前がブラックリストに掲載されて広く流布されるかも知れない。

しかも加害者の方は、被害者の正しい身元データを把握した上でそれを使っているかも知れない。その結果、取引要求が成された時に被害者が支払を要求される様な覚えは無いと言い張れば、売り手の方はカード番号ないしは口座番号しか把握していないものだから、支払を約束した者は実は被害者でなくて加害者の方であることの証拠を示すことも出来ない。

何れの場合でも、商業活動への障害が生じる。多くの場合には、顧客を引き留める為に売り手が損をこうむることになる（保険支払を受けられない場合）。

信頼を確保する為のインフラストラクチャの存在がこの問題を解決する。しかしながら、インターネットは、学術社会で使い始められた当時から、自由で制約の無い情報アクセス手段であって、認証を必要とすることなど無かった。それ故に、認証のインフラストラクチャは、既存のインターネットの上に付け加える新しいレイヤーとして建設されねばならない。その様な信頼確保の為のレイヤーを付け加えることは、技術的には難しいことではない。しかしながら、信頼確保の為のレイヤーを付け加えるには、それなりのコストがかかる。問題は、そのレイヤーの初期の利用者への利点が、それをを用いて安全に通信できる相手の数が限られるが為に、限定的にならざるを得ないということである。この良く知られる成功限界利用量の問題が、最近に至るまでのシステム提案者の活動の障害となり、その経済的な成功を妨げてきた。

## 5. 如何にして信頼のインフラストラクチャを構築するか

インフラストラクチャの魅力は、既にどれ位の数の顧客と、合わせて応用サービスの提供者とがそれに加入を済ませているかに依るところが大きいので、如何にしてそのインフラストラクチャを成功限界利用量に達せさせるかが、成功を収める上での重要な要因である。GBDeは、ビジネス、政府、消費者団体など総ての関係者とオープンな話し合いを行って、どの様にして現状の行き詰まりを打破して、この成功利用限界量を作り出すかについて議論したいと考える。様々な産業セクタや公的機関を統合しての率先的な実行団体（ひとつ又は複数）の設立が最も構想実現の可能性に近いと考える。

私企業・公共的機関連携（PPP）は、他の形でも組織出来よう。政府自身が確たる認証を可能とするチップにIDを埋め込むことが考えられる。この場合には



産業界は公的機関へのサービス提供者にもなれるし、また、そのIDとチップとを用いた民間の応用サービスを構築することも出来る（例えば支払システムなど）。

別の方法としては、産業界の各社が協同組織を作って必要な投資を行い、インフラストラクチャを作り上げることも考えられる。この場合には政府機関は、法律の枠組みを変えてでも、産業界が作り上げた仕組みを電子政府応用に用いることを約束するべきだし、その様な仕組みの共同マーケティングに貢献すべきである。GBDeは、上記のうち、どちらのやり方が優れているとは云わない。しかしながら、もしインフラストラクチャの運営が民間の手に任される場合には、公的機関はその利用を誓約するべきだし、公的機関が自らの手で別のインフラストラクチャを作ることは避けるべきである。

多くの国において、既に電子署名法が成立している。その様な国々においては、原理的には法的拘束力のある契約に電子的に署名することが可能である。しかしながら、現実には電子署名は狭い分野でしか使われてこなかったか、或いは、全く利用されてこなかった。多くの国ではデジタルIDが発行されず、民間の投資家は信頼のインフラストラクチャを作り上げることに躊躇している。それは、投資が巨額にのぼる上に、回収が疑問視されるからである。

以上のことから、政府が自らはインフラストラクチャを運営しないと決意するならば、政府は以下の点で民間の実行組織を支援すべきである。

- ・ 参入障壁を下げる。特に確立済みの方法が使える様にして、民間の投資が最小限で済む様にする。
- ・ 国際的な政策協調を図って、個々のシステムが孤立せぬ様にする。
- ・ 電子政府応用を立ち上げて、最大の顧客となること。

## 6. オンライン詐欺に関する幾つかのコメント

二者が相対で商売する時には、何時でも、片方が他方を騙す危険があるものである。オンライン環境下では、詐欺行為を行うことは、より易しい様に思える。商売はお互いの顔を見ることなく行われ、連絡は本名でなくとも行うことが可能で、安全な認証を行う手段にも乏しい為である。

支払約束書に行った電子署名に法的拘束力が無い限りは、支払（予定）人が自分の支払を承認した覚えは無いと言い張ることも有り得る。その場合、受取人は、支払（予定）人の口座情報が悪用されたのか、それとも支払（予定）人がただそれは何かの間違いであろうと強弁しているだけなのかの切り分けが出来ない。そ

の結果、多くの場合に、売り手は損失を自分で負わねばならなくなる。

仮に顧客の情報が悪用された場合に、顧客は返金要求をすることは出来るが、その過程で、多くの顧客がもう懲り懲りだと思ふ様な目に会って、しばしば電子商取引から手を引いてしまう。我々の調査によれば、そのマイナス効果は甚大である。従って、インターネット決済システムの導入によって、オンライン取引を安全にすることは、売り手が詐欺によって被る損失の減少に役立つのみならず、オンラインで買い物をしたいと考えているもののまだ実行には移していない多くの潜在的顧客をオンライン取引に誘引することにもなる。

加えて、裁判外紛争処理手段（ADR）を提供したり、トラストマーク制度を充実することも、顧客の信頼を増すことに役立つ。この点については、既に先年来 G B D e が多くを述べて来た。

## 7. 法制度

電子商取引は、本質的に、国境を越える。国内法は、その旨を理解した上で、他国の法律との整合を取らねばならない。

国々にバラバラで調和の取れない法制度は、障壁を作って電子商取引の成功を制限する。G B D e は既に、東京提言やブリュッセル提言の中で幾つかの点について指摘してきた。しかしながら、我々の調査では、まだ多くの電子商取引事業者が特に決済の分野で、調和の取れない法制度によって妨げられていると感じている。

## 8. 新しいビジネスモデル

信頼の為のインフラストラクチャを作り、それに基づいた新しいインターネット支払システムを構築することには、多大な投資が必要である。この投資に対する見返りは、新しいインフラストラクチャが広く利用された場合のみ見込めるものである。とても、民間の一企業がその様なインフラストラクチャを作り上げられるものではない。そこで、セクタを越えての協力が必要である。

政府もこの努力の一員に加えられる。特に法令改正による規制緩和によって、初期投資が最小で済む様にして頂きたい。特に、高価につく様なやり方の実行を指示することを止めて頂きたい。

## 9. マイクロペイメント

我々の調査に依れば、マイクロペイメントの重要性評価は、業界毎に異なっている。電子的手段での配送に適した物品やサービスを取扱う業界にとっては、マイクロペイメント手段の存在は有効である。例えば、少量情報の配信サービス（新聞記事の一部など）や、個別要求情報の伝達サービス（地理上の所在情報や電話番号など）には、適切な課金システムが必要とされる。

マイクロペイメントシステムが無ければ、低価格の商品はネット上では販売されないか、予めサービスに加入した者だけに販売される様になるだろう。しかしその場合でも、一件毎の購入の承認を行うことは困難であろう。この事実は、サービス対象を予めそのサービスへの加入を承認した顧客に対してのみに限定するもので、そのサービスを初めて利用しようとする顧客に対しては、参入障壁を築いてしまうことになる。

実務上の理由で、多くの場合にマイクロペイメントシステムは既存のインフラストラクチャの上に構築される。<sup>(注5)</sup> この場合には、ああせい、こうせいと要求する様な規制が、最大のシステム構築障壁となる。マイクロペイメントにおける支払要求毎のコストは、極めて小額に留めなければならないからである。

## 10. 勧告

我々の調査に基づき、世界各国の諸企業からの情報に併せ、更に以上述べてきた考察から、GBDeは以下を勧告する。

1. 認証は、支払のみに留まらず総てのインターネット上での業務処理の実現上の鍵である。安全な認証を可能とする（PKIの様な）信頼の為のインフラストラクチャを構築することは、民間と公的機関の共同努力を必要とする。それ故に、もしその様な信頼の為のインフラストラクチャが公的機関自身の手によっては運営されない場合には、GBDeは以下を勧告する。
  - ・ 政府は、信頼の為のインフラストラクチャの構築努力が最小限で済む様に、法制度を改正すべきである。取り分け、既存のやり方が活用出来る様に（例えば、金融分野において用いられている方法）。
  - ・ 政府は民間の手による信頼の為のインフラストラクチャを電子政府応用

---

<sup>(注5)</sup> 例えば、電気通信事業者が運営しているインフラストラクチャの上に構築される。

に用いて、独自仕様の導入を避けるべきである。

- ・ 民間は業界セクタを越えての推進団体を作り、そこにサービスプロバイダーや応用サービスホルダーも、金融サービスプロバイダー、電気通信サービスプロバイダー、オンライン商店、コンテンツプロバイダーに合わせて加えて、基本概念の合意を目指すべきである。
  - ・ 消費者団体もこのプロセスに加わって、消費者に対してこの信頼の為のインフラストラクチャの利用を呼びかけるべきである。
  - ・ 民間（全業界）と政府と消費者団体は共同して、信頼の為のインフラストラクチャの利用によってメリットを得る総ての参加者に対する、公正なコストとプロフィットの分配モデルを作り上げるべきである。
2. 各国の法制度は未だにうまく折り合っていない。ある国でインターネット決済システムを運営するサービスプロバイダーは他国においては運営を拒絶されるかも知れない。時には、マイクロペイメントの利用者ですら手間隙かけて識別せねばならぬことが要求される。政府はその様な過剰監督障壁を引き下げるべきである。
3. G B D e は信頼の為のインフラストラクチャも、その上でのインターネット決済システムも、最初から世界一斉に実現に移されると考える程に楽観的ではない。それ故、各国において構築されていく個別のシステムを結び合わせる為の相互互換性が肝心である。政府と、そして各国における民間の関係者は、国毎のシステムがオープンスタンダードを受け入れるべく働きかけていくべきである。

## インターネット決済付録：質問と回答の評価

### 設問と評価

1. 非常に少数の e/m（電子／モバイル）決済事業者しか損益分岐点に達しておらず、多くの新しいサービス事業者がサービスを終了せねばなりません。この状況の理由は何だと思えますか。

		評価結果
a)	決済は規模のビジネスである。決済サービス事業者が利益を出せる様になる迄、その集約に向けての活動は続く。	++
b)	各(国際的な)決済システムはクレジットカード支払に基づいていなければならず、新たなサービスを提供する事業者のための余地はない。	○
c)	顧客および/ または販売事業者は、e/m 決済サービスでの支払を希望してはいない。	(-)
d)	顧客は情報プラットフォームとしてインターネットを使用するが、取引きのためには使用しない。従って、e/m 決済システムには実際の必要性はない。	--

2. オフラインの世界では、顧客は、デビットカード、クレジットカード、小切手、現金、及び、プリペイド、など異なったタイプの決済システムから選んで来ました。オンラインの世界ではどうあるべきでしょうか。

a)	(学童のように)クレジットカードや銀行口座を持たない顧客にのための決済システムを提供しなければならない。	○
b)	顧客が匿名で利用できる オンライン決済システムが必要である。	○
c)	顧客のリスクを先払いした金額に限定するプリペイドシステムが必要である。	(+)
d)	マイクロペイメントを処理するための新しい解決策が必要である。	(-)
e)	サイバー世界には現金の等価性がない。過去の全ての民間での試みは不成功であった。従って中央銀行はサイバーマネーの発行を行なうべ	(-)

	きである。	
f)	インターネットはオフラインの世界とは異なっている。クレジットカード又は銀行口座に基づく決済を提供すれば十分である。	○

3. 詐欺はインターネット取引にとって重要な問題であると言われています。この要因となっているのは何でしょうか。

a)	詐欺は主に認証の欠如による。	++
b)	主要な問題は、未だに信用を取引きの基本としていることである。	○
c)	法的な結論を得ることは、特に国際間の貿易においては、余りにも困難か余りにも費用が掛かる。	+
d)	詐欺は精神の問題である。甚大なリスクもたらずものではなくても、顧客は詐欺に脅えている。決済サービス事業者と販売業者は詐欺に対処することができる。	++

4. しばしば、セキュリティに関する懸念が、顧客が e/m 決済システムを使用しない理由であると言われています。セキュリティに関する問題の核心は何でしょうか。

a)	セキュリティ問題は、殆どが技術的な性格である。	○
b)	セキュリティは、(PKI のような) 共通的な信頼基盤がないことが問題である。	+
c)	顧客から見て、安全なシステムは余りに高いか余りに不便である。	+
d)	顧客は、余計な取引料金なしに安全な取引を期待している。	++
e)	販売業者だけが、セキュリティを無料で提供する決済システムを運用する。	-
f)	既存の e/m 決済システムは、その評判より良くなっている。顧客が安全でないと感じる理由は、理屈いよりむしろ心理的なものである。	+
g)	幾つかの(新しい) 決済システムは、十分な保証のレベルを上回っている。これによって、システムは余りに複雑になった。	+

5. 今日のオンライン世界には、共通的な認証基盤がありません。これは、インターネット決済にとってどういう意味を持っているのでしょうか。

a)	もし共通的な認証システムがあったら、インターネット決済システムを導入し、クリチカルマス問題を克服することは大いに容易である。	++
b)	そのような認証システムは、PKI に基づいているべきである。	(+)

6. 金融分野は最も規制されているものの1つです。幾つかの規則は e/m 商取引で機能するようには作られていないでしょう。インターネット決済システムはこの問題の影響を受けているでしょうか。

a)	消費者が(幾つかの) インターネット決済システムに加入することを困難又は不便にしている法的障壁がある。	(+)
b)	インターネット決済システムの運営を経費が掛かる様にしている(報告要求のような)法的義務がある。	+
c)	論争解決のための手続きが余りに困難である。	+
d)	矛盾した法的システムが、国際市場に参入しようとする決済システムに対する障壁となっている。	++

7. 今日、数多くの異なるインターネット決済システムがあり、一部はその国に根差した異なる国内的なオフラインの決済構造に基づいています。共通運用性はクリチカルマス問題を解決する為の鍵でしょうか。

a)	技術的な共通運用性の欠如は、販売業者にとって新しい決済システム採用の障壁となる。標準化の改善が必要である。	+
b)	主要な(特に国際間決済での)問題は、技術的なものではなく、釣り合いの取れていないオフライン決済システムである。	(+)
c)	これは標準の問題ではなく、ビジネスモデルの問題である	0

8. 最後に重要な質問です。今日、e/m 決済システムで最も重要な問題は何であるのかをお尋ねします。

a)	信頼のインフラが必要である。	++
b)	法的な状態は e/m 決済システムへの障壁になってしまった。	
c)	新しいビジネスモデルが必要である。	++
d)	効率的なマイクロペイメントシステムを求めている。	+

e)	効率的な国際間決済システムを求めている。	<b>+</b>
f)	それは単に時間の問題である。私達には更なる忍耐が必要である。	
g)	E/m 決済に対する需要はない。	
h)	その他:	

(評価結果のマーク)

- ++ : 強く肯定
- + : 肯定
- 0 : 中立
- : 反対
- : 強く反対
- (+) : 回答が分かれているが、多くが肯定
- (-) : 回答が分かれているが、多くが反対



## 回答結果の分析図

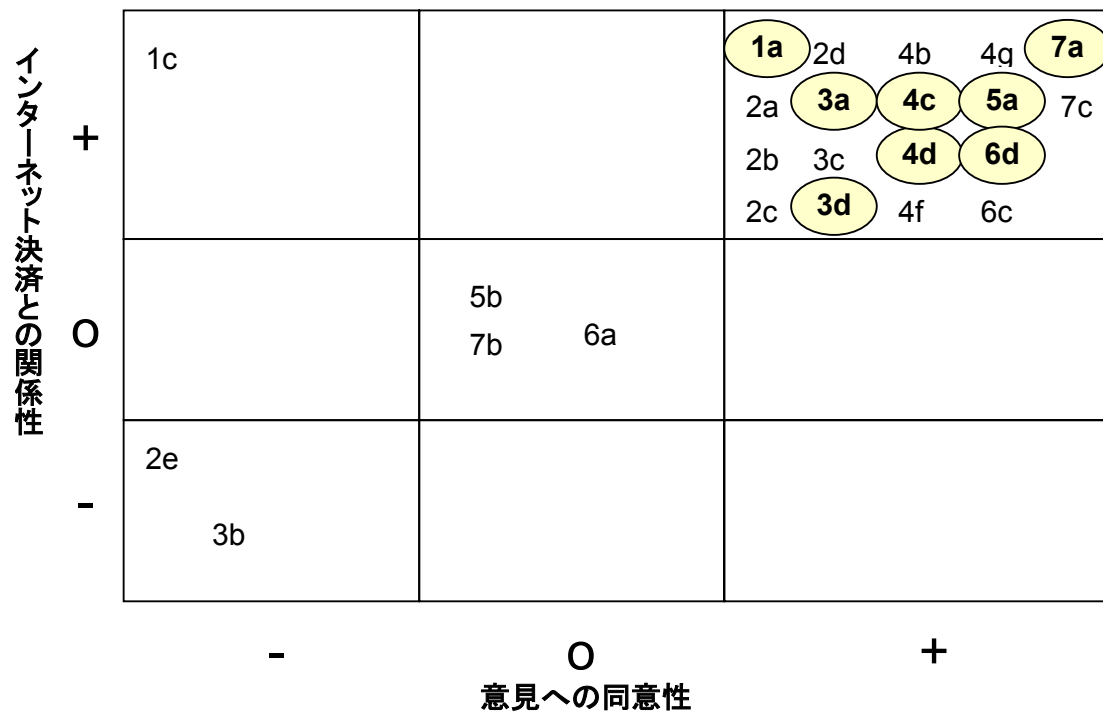


図1: ほぼ回答に合意の取れた設問

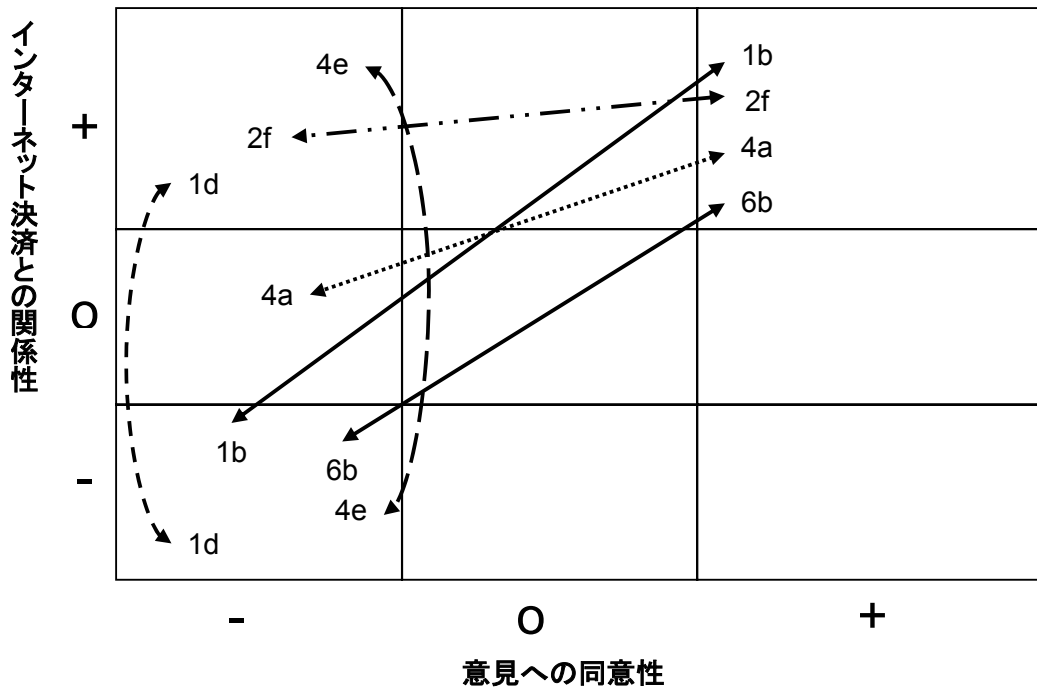


図2: 回答に意見の分かれた設問

図1と図2についての注釈

回答意見が分散して、その結果まとまった意見に集約されなかった設問は、最も多かった代表的な回答のみを図中に示しました。

導き出された考察

1. 図1に表した回答は、多くの同じ意見が示されたものです。特に集中しているものは丸印で示しました。この考察結果が今年のGBDe提言の基礎となっています。
2. 図2に表した回答は、設問に対して意見の分かれているものです。従って、インターネット決済の領域において異なる考え方があるとの理解の上で、これらも提言作成の元となっています。



Global Business Dialogue on Electronic Commerce

消費者信頼構築WG  
求めざる電子通信、通称“スパム”  
多角的取り組み

2003年11月6日

ラポーター： Michael Sabia  
(米州) President & CEO  
Bell Canada Enterprises Inc.

## I. 序章

インターネットの発展は教育、通信、商業、雇用などに於ける機会増加をもたらした。インターネットは人間と人間との間での相互関係確立手段に革命をもたらし、世界に向けての個々人の発言の自由の実現や情報授受・発信の自由実現の為の基本的かつ欠かせざる手段に迄発展した。<sup>(注1)</sup> しかしながら、社会的目的、商業的目的を遂げるに十分なほどに優れたインターネットの資質が、同時に濫用され易いものとなっている。

電子メールは最も昔から使われてきて、かつ、基本的なインターネットの応用であって、未だに最も広く使われており、何百万人もの人達が通信及び情報交換手段として利用している。電子メールは迅速かつ効果的な企業内部通信及び情報交換手段として、企業がその事業を運営する手法を変えてしまった。同時に企業の製品及びサービスと顧客との関係のあり方を劇的なまでに変えてしまった。多くの産業に於いて電子メールは、その顧客に対して支援を提供する上での最も効率の高い手段になっており、これを用いての新製品や新サービスに関する迅速な通知も行われている。

求めざる電子メール、通称“スパム”<sup>(注2)</sup> が世界的な問題になってきている。というのは、それがインターネットに対する顧客の信頼に直接の影響を持つからである。そして関係者に対して膨大な対応策コストを強いるが為に、地球規模のインターネット社会が本来もたらすべき利点や機会を阻害する存在になっているからである。

求めざる電子メールの顧客への影響には様々なものがある。まず受け取り手は時にその攻撃的さらには時として不法な内容に戸惑い、選び捨てる為に時間と金を失う。次に大量のスパム流入によってインターネットの動作が緩慢になる。更には受け取るべき電子メールがスパム防止の為にフィルターに掛けられて除去されてしまう。逆に送り手から見て、送ったメールが途中で阻止されてしまう。顧客のインターネット利用料支払がスパムの取り出しのために増してしまう。更には、インターネットを使うのが嫌になってしまっ、その結果、情報社会の恩恵に乗り遅れてしまう。などなど。

---

(注1) サイバー倫理についての GDe 東京勧告 (2001 年 9 月) 参照

(注2) 本提言に於いては、求めざる電子通信、求めざる電子メール、スパム、なる用語はさほどの差なく使われている

ISP（インターネットサービスプロバイダー）の方では、求めざる電子メールそのものを運ぶ為にも、それが引き起こす問題に対応する為にもインフラ整備の為の支出を強いられることになる。伝送容量を増やさなければならないし、サーバーを増やしさらに高級化してスパム阻止機能、それを動作させる為の管理機構、ブラックリストの整備などをしなければならない。ISPはスパムによって自らのブランドネームが傷つけられることにも憂慮せねばならない。ISPの顧客が、自分が加入しているISPだってスパム問題への対処に責任があり、またそれを解決する能力があるはずだと思っているからである。だからISPは一方ではスパムが多いのだ、スパムのせいで動作が遅いのだ、と云う顧客の苦情に対して人手を掛けねばならないと同時に、他のISPに対しては自らの顧客の一部がスパムを流したという理由で自らの顧客総てが他のISPから見てのブラックリスト対象になってしまうぬ様に抗議を続けなければならない。結局のところ、これらのコストは顧客に対してISPが課金する価格に跳ね返るのである。

インターネットを業務に利用している企業の経営者としては、社内網と一般インターネットとの接続点におけるスパム対策用のファイアーウォールやフィルターへの投資が必要になる。加えて、従業員の業務遂行効率が下がったり、従業員に不満が溜まることも業務運営コストの増加となる。そして従業員は家に帰れば、今度は顧客としてスパム問題に対処しなければならないのである。

既存の顧客との連絡手段や新規顧客への勧誘手段として電子メールを自らの商売遂行の為に使っている方々に対して、我々はスパムの存在によって本来正当である商業活動に対する顧客からの不信感が増大してしまうのではないかと心配する。この問題が広がっていくと、そもそも正当な商業活動においても、インターネットを用いること自体が問題視されるようになる可能性もあると云う事である。加えて、正当な電子メールもフィルターによって阻止されてしまう可能性があることによるマーケティングコストの増加も考えられる。

求めざる電子通信の悪しき衝撃は、単に古典的な電子メールの範囲に留まるものではない。有線・無線のインスタント・メッセージング、以前からあるボイスメールなどの分野でも問題視されてきている。

加えて、求めざる電子通信の共通の問題が種々の形で、世界中に現れてきている。例えば、北米や欧州において当初はスパムは不要な商業勧誘レターや、詐欺の手段であった。しかしながら最近では、これに加えて危険な内容をもたらすようになってきた。日本においては、迷惑メールと迷惑サイトの組み合わせが使われて、

少女達の自発的売春、集団自殺、老人からの金銭詐欺などの形で現れてきて社会問題になっている。

別の一寸変わった形での問題が中国から日本に向けてスパムが送られると云う国際問題の形で現れている。日本と中国とでは、大略似ている漢字を使っているのであるが、同じ漢字に割り当てられている文字コードが異なっているので、メッセージの総てが文字化けしてしまって、スパムを受け取った日本側では一体何が書かれているのかすら全く分からず、当然そこから何の意味も見出せない。イライラさせられる事と、リソースを無駄使いさせられるだけなのである。

インターネット社会の進展は、ここに発生したスパムの様な問題への協調的な解決手段の必要性を強く求めている。この一筋縄ではいかない求めざる電子通信、通称“スパム”、の問題の負の衝撃を本質的に軽減するためには、複数の対策の詰まった道具箱が必要である。その内容として必要なものは、自主規制、対応技術、教育、法制度整備、そして国際的な協調であって、政府、民間企業及び市民社会からの協力が必要である。

## II. 求めざる電子通信、通称“スパム”を定義する

極く初歩的なレベルでは、“スパム”とは受け取り手にとって送って欲しくない、又は期待していない電子的手段による通信と解釈できる。しかしながら、求めざる電子通信の問題に解答を与えようとするいかなる試みにおいても、その試みを意味のあるものとする為には、誰もが以下の事柄について共通の理解に達していることが必要である。即ち、我々は何について話し合っているのか、どの様な観点が優先的に、しかも如何様な手法によって検討されるべきであるかと云う様な事についてである。これ迄何年も掛けて多大な労力が、一体スパムとは何であるかを定義する為に費やされてきたが、現在に至るも誰をも納得させ得るに足る定義は出来上がっていないのである。

現在取られている幾つかの手法に付きまとう危険は、マーケティングの為の総ての商業通信を求めざる電子通信だと決め付けてしまうことである。であるから、先ずは正当な商業通信が詐欺だの求めざる連絡だのから分離され得る様な定義を採用することに優先度が与えられねばならない。この両者を分離することは、一貫し、協調の取れ、目的のはっきりした政策発動を可能にするであろう。

この意味において、求めざる電子通信が通常持ち合わせる性格について考えることが有用である。それらは以下の四つの異なるカテゴリーに分類される。

a) 受け取り手の期待に関して：

- 不安感をもたらす又は期待外（有形にしる無形にしる、承諾を得ていない）。
- 過去には送り手との間の関係が全く無い。

b) 通信文の内容に関して：

- イライラさせたり、攻撃的である（例えば、チェーンレター、悪ふざけ、ポルノグラフィ、個人的関係を結ぼうとの勧誘、信仰の押し付け）。
- マーケティング、コマーシャル。
- 非合法又は詐欺（例えば、小児ポルノ、ねずみ講、騙し広告）。

c) 送り手の所在に関して：

- 送り手の所在不明又は返送不能。
- 物理的な所在住所その他の送り手についての情報の欠如。

d) 通信形態に関して：

- 通信の打ち切り又は今後の受信拒否を連絡する為の手段の欠如。
- 大量無差別送信（例えば、自動的手段による大量の無差別送信）。
- 受け取り手の電子メールアドレスを入手せんとする手法（例えば、Webからの電子メールアドレスの取り出し、或いは送り先不明で戻される電子メールを監視してそれ以外のアドレスを抽出する手法）。
- 類推電子メールアドレスを用いての暴力的な送り付け、一斉攻撃的送り付け。
- オープンリレーの不正利用。

しかしながら、以上の四つのカテゴリーを見てみると、より実質的な手法は、求めざる電子通信をその形態や含まれる内容によってではなく、そのとんでもない振る舞いや受け取り手の期待感への反し方によって定義して、それ故に主観的な要素を可能な限り排除した上で、それらを求めざる電子通信と判定することではないかと思われる。

### Ⅲ. 既にコンセンサスが得られていることの上に

この事に関しては大多数が賛成している訳であるが、最も迷惑な求めざる電子メールというものはそのメッセージの中身又は送り手の存在について、何らかの欺瞞を持ち合わせているものである。この受け容れ難い欺瞞的振る舞いに脚光を浴びせることで、求めざる電子通信とは、どの様な通信手段であるかを問わず、以下の様な性格を一部或いは全部揃えて持ったものだと定義することが出来るであろう。

- オプトイン或いはオプトアウト原則のいずれによるかを問わず、受信の承諾を受けていないもの。
- 個人情報を盗み出そうとするもの。
- 主題、送信元、又はメッセージの内容に不正な情報や要求を含むもの。
- 詐欺を目的とするもの。
- 返送アドレス情報が間違っているもの。

求めざる電子通信の定義として大量通信や高頻度通信を挙げることは、今や実効的ではない。電子メールを顧客との間の正当な通信手段として商用に用いている会社はそれでは困惑するばかりだし、電子メールの送信者達は（善悪を問わず）その気になりさえすれば、大量の電子メールを小分けにして送り続けるだけでこの分類をすり抜けてしまう。

だから、送り方の違いで善悪を議論するよりも、上記の大方が賛同している求めざる電子メールの持つ性格に注目した方が生産的である。

およそ 60%の電子メールが偽りのヘッダーや詐欺的内容を持っていて、それらは上記の定義によって容易に求めざる電子メールだと断定できる。これだけの分量が取り除ければ、問題への対処はより易くなる。多くの国において、既存の個人情報保護法の適用と偽りに満ちた求めざる電子メールが氾濫する問題への対応との間には、まだまだ距離がある。それ故に、最も悪質で熱心なスパムメールの送信者達は、同時に最も捕まえにくい者達である。法の執行者は、このような詐欺行為に手を染めている者の摘発に全力を尽くすべきである。

プライバシーの観点から見れば、この 60%もの有害電子メールは、不法であり、その内容に偽りを持つものであるから、個人情報保護法違反以前の問題である。しかし、残りの 40%の方の電子メールにもより害の少ない求めざる電子メールは含まれるのであって、こちらにおいては個人情報保護が問題となる。この問題



の解決にあたっては、関連業界のベストプラクティスが重要な要素となろう。(注  
3)

#### IV. 対応策道具箱手法の必要性

情報化社会においては何事にあたるに際しても、益々全ての関係者の協力を得ての極めて精巧な取り扱いが必要となる。求めざる電子通信の全てをインターネット利用者の生活環境から取り除くことが不可能だとしても、それが固定インターネットの世界においてもワイヤレスインターネットの世界においても、少なくとも以下の手法の組み合わせによって制御され、管理され、減少させられるべきである。その手法としては、自主規制、技術的解決、教育、法制度整備、それに国際協力が挙げられる。既に一般的にこの対応道具箱の手法は、増加を続ける求めざる電子通信への対応策として必要だと認められており、その中には総ての関係者に課すべき役割があると考えられている。しかし、対応策としての道具の種類や、関係者毎の役割は、時と共に変化していくであろう。

##### 1. 自主規制と行動規範

この求めざる電子通信の問題を解決しようとしてISPが考えた、様々な自主的な実施策が既に存在している。或る種の実施策が広く実践されているのに対して、中にはむしろ求めざる電子メールの増加を招いてしまうとして中止されてしまったものもある。ISPには有効な手段の導入が勧告される。しかしながら、ISP毎にその事業規模も持っているリソースの量も異なる。それ故に自発的な対応策の導入は、自己裁量に任されるべきで、法律で義務付けるべきことではない。政府、法執行機関、消費者団体などのこの問題についての総ての関係者は、実際にこの問題と戦っているサービス業者への衝撃の深さ、実際に適用可能な手法、そしてサービス業者毎にそれら手法を導入する能力を持ち合わせるかどうかの度合いが異なることを、よく理解すべきである。

---

(注3) 消費者信頼、とりわけ個人情報保護についてのGBDe東京勧告(2001年9月)を参照のこと

## 2. 技術的対応

インターネット関連の産業界は、求めざる電子通信の問題に対応する為の技術的解決策の開発に、引き続き興味を示している。或る手法においては、求めざる電子メールをそれが受け取り手のメールボックスに届けられる前に排除する事が試みられ、また別の手法ではメール到着後のメールボックスからの摘出が試みられている。ISPはフィルタリングシステムの使用に関心を増しており、その適用が自らのビジネスモデルを通じてその顧客だけに対して出来るようにしている。例えば、それはサービスの一部として、或いは別のサービスとして定義されている。

しかしながら、どの様なフィルタリングシステムにおいても、正当な電子メールを間違えて求めざる電子メールと見なしてしまう危険が付きまとう。これは擬似陽性問題として知られている。技術的解決手段については、その他にも問題点が指摘されている。例えば、多くのフィルターは求めざる電子メールを送ってきたサーバーを丸のままブロックしてしまうが、本来ブロックされるべきは求めざる電子メールを送り出した送り手だけのはずである。

求めざる電子メールの問題を解決する技術的手法の一つとして、これは長年の教育プロセスを経ねば実現出来ない事だが、フィルタリング技術をエンドユーザー側に植えつけてしまうことが考えられている。相当の速さで新しいフィルタリング技術の開発が進められており、これらが教育プロセスを経て広く利用されるに至ることが期待されている。それが実現すれば、消費者に求めざる電子メールの問題に対処する為の力を与えたことになるだろう。今後は消費者にも、入手可能な技術的対応手段を導入して行くことが勧められる。

## 3. 周知徹底と教育

ISPは、その顧客が自分自身を求めざる電子メールから守ることについての教育と、どの様にしたら求めざる電子メールと戦えるかについての説明を、既に行っている。実際に内容を良く理解していて、自らを問題から守るべく手段を講じている顧客はあまり苛立ちをつのらせることも無く、ISPに対して文句を言うてくることも少ない。また、求めざる電子メールを送る様な行動をISPが許す訳が無いと知っている顧客は、自らその様なことをする前や、その様なことをする者にコンピューターを使わせる前に、二度考えて、結果として取り止める。

ISP は様々なやり方で顧客を教育する。例えば、詳細な方針や実践方法の制定、サービス利用上の行動規約の策定、想定質問解答集の準備、この問題に特化した情報の提供と関連リンク集の作成、警告書の送付、自らが顧客に対して電子メールを送信することを通じての正しいやり方の例示、などなど。

ISP 自身が先験的に、求めざる電子通信問題やその解決についての情報を探り出すべきである。加えて、より先進的な ISP は、ISP 相互間での情報交換を一般的には求めている。それは、もし或る ISP が自分のネットワークから求めざる電子メールが出ていく事を防げれば、それだけ他の ISP のネットワークに入っていく求めざる電子メールの量が減るからである。これは業界全体の問題であるから、業界団体にはその加入社及び加入社の顧客を教育し、世界中の他の地域の業界団体と協力して行く役割があろう。

消費者団体には、増加を続ける求めざる電子通信問題への消費者の関心を高め、消費者における求めざる電子通信問題の解決を助ける役割がある。消費者こそが、受け取った電子メールが自らが求めているものか否かを判断するに足る最も良い位置に居るのである。両親はその子供に対して、電子メールアドレスなどの個人情報オンラインで他人に漏らすことの無い様に教育して欲しい。自らを守ることで、消費者も又、求めざる電子メールの量の減少に貢献することが出来る。例えば、どんな求めざる電子メールを受け取ったかを報告することによる。だから、消費者には自らを教育するに足る十分な見返りがあるのである。

電子通信が政府にとっても社会の構成員全体にとっても重要性を増す中で、政府はそのあらゆる階層において、消費者に対してどの様にしたらその身を守れるか、更には、求めざる電子メールの減少に貢献できるか、についての知識を植え付けると云う重要な役割を担っている。学校においても、知識の植え付けと教育がなされるべきである。

#### 4. 法制度的解法

既存の法律に基づく政府の取り締まり強化や市民運動の展開、オンライン上の問題を含めて対応できる様にする既存法の改正、更には、新法の制定など、求めざる電子通信の問題に対処する為には、色々な形での法制度的な解決策が考えられる。

新法による解決策に総てを委ねてしまうことの危険は、新法には見落としによる電子商取引への思わぬ悪影響が含まれる可能性があり、また結局のところ欺瞞的行動を取る者に対して僅かな防止効果しか与えられないかも知れないということである。

加えて、求めざる電子通信の問題解決には世界協調して事に当たろうとの一般的な了解があるにも関わらず、今のところまだ新法を十分な検討を経ずに急いで取り決めてしまおうとの考えが一部の政府にあって、それが部分的な対応策に終わってしまう恐れがある。既に 1999 年に、GBDe は各国政府に対してこれから先の求めざる電子メールへの対策としての法律は国際的に矛盾無く制定されるべきであると、警告している。<sup>(注4)</sup>

必要なことは真に調和の取れた国際的な法制定手法であって、それが求めざる電子メールの問題と戦うのに有効であるならば、インターネットのみを対象とする法律であっても、一般法であっても構わないのである。

上記の如く、どの様な新法を考えるにしてもそれにつきまとう問題は、技術やビジネスモデルが常に変化して行く中で、この求めざる電子通信の問題を定義することにある。様々な法律的手法を用いての新法案が出てきているが、果たして世界的な問題としての求めざる電子メールの問題に歯止めを掛けるだけの実行力があるかどうかの証拠は少ない。それらの新法案の多くが、正当な商業通信のためのインターネット利用者に対して負担を多くしてしまうなど、負の効果を合わせ持っている。

どの様な新法の導入を考えるにあたって、その他に陥り易い幾つかの落とし穴がある。例えば、もし新法が求めざる電子メールの送信者を海外に追いやってしまっていて、その地での取り締まり執行が更に困難になれば、その法律は無効どころかかえって有害となる。それ故に世界規模での法制度協調の重要性は増大する。その結果故意ではなくとも、国際的な発言の自由を抑制してしまい、うっかりとして、消費者が自分のメールボックスの制御権を失う様な結果に終わってしまうかも知れない。更に、不適切な法の導入を行えば、国民を保護することについての政府の能力に関する国民の信頼は低下するであろう。

---

(注4) 消費者信頼に関する GBDe バリ勧告 (1999 年 9 月)

## 5. 国際協調

インターネットは国際的な接続手段であるから、その上を流れる求めざる電子メール、通称“スパム”の問題は世界的な問題であると、広く認識されている。この問題は、国内法というものが伝統的に国毎に異なっていて、その効果が及ぶ範囲の組織にのみ適用されるという事実とあいまって、複雑化される。だから国際協調は、あらゆる階層及びあらゆる関係者において必要である。

例えば、議論の内容を深めようとする努力の中で、消費者団体が一緒になってスパムの様な重要なインターネット関連の問題について発言して、その様な問題についての自らの考えを世界中の政府や民間企業に対して発信し得るようになってきている。自主規制も産業セクターによっては導入されてきている。例えば、通信販売業界は本来的に国際的な存在であって、国内法の相互間の協調など待ってられないのである。様々な法制度的解決策の実効を上げてスパムの“安息所”を排除する為に、政府は協調して、国内的な消費者保護法を持ち合わせないその様な“沖合い縄張り”についても圧力を掛けて、国際的な法制度実効協力を促すことが出来るはずである。

## V. 産業界への勧告

### インターネットサービスプロバイダーに対して

#### ● 自主的な対応策を採用すること

以下に示す実施対応策は広く導入されている。他の策はむしろ逆に、求めざる電子メールを増加させるのに役立ってしまうと見られている。<sup>(注5)</sup>

- 「求めざる電子メール送信の為にそのサービスを使ってはいけない」とする利用規定を持ったサービス契約を制定して、それを適用し、実行すること。
- 国内においても国際的にも ISP 間の連携を強化して、考え方や利用規定間の協調を図ること。

---

(注5) 同様の自主的手段が、有害コンテンツ対策に関する GBDe ブラッセル勧告で提言されている。(2002年10月)

- 同一のアドレスやアカウントから一日あたりに送信することの出来る電子メールの数の制限を加えること。
- 個人顧客と商用顧客の違いを考慮した上で、適切な内部規定を設けること：
  - 顧客についての正確な情報を収集すること、求めざる電子メールの送信者が悪用する機会を減少させる様な顧客の取扱い方を採用すること（例えば、同じ名前や同じクレジットカード番号で開設できるアカウントの数を制限するなど）、プライバシー原則を尊重しつつも先験的に求めざる電子メールの送信者を見つけ出してその者との契約を解除すること（例えば、疑わしいメッセージの隔離、制定した一定限界値を超えるものがないかどうかの検査、その結果浮かび上がった対象への調査と必要に応じた契約解除）、などなど。
- ネットワークサービスの内容を適切なものにして、自らのネットワーク内外のスパム送信者に狙われる機会を低減及び排除すること。
- ホットラインの開設、通報専用電子メールアドレスの設定、その他の苦情受け付け窓口の設置。
- 国内外の他の ISP との間での、相互連絡及び対策の広域拡大適用が出来るルートの設定。或る ISP が求めざる電子メールが送られてきたという理由で他の ISP からの通信をブロックしてしまう前に、何故そのブロッキングを行わねばならないか、更にはどうすればそのブロッキングを行わずに済むかについての情報をその相手方の ISP に通知することを約束する了解が結ばれることが望ましい。
- さらに、もし不適切なブロッキングが行われた場合には、速やかにその復旧に向けて行動するとの ISP 間の協定。
- 外部で作成された然るべきスパム送信者のブラックリストを使つてのブロッキング。
- 自らのネットワーク内でのブラックリストの作成と、そこに記載されたスパム送信者から送られたメールの受け取り手顧客のメールボックスへの送信のブロッキング。もし法律上可能であつて、社会慣行上にも問題が無いなら、その様なブラックリストの ISP 相互間での交換。

## ● 法執行への協力

ISP も被害にあった企業も、法執行への協力度を高めるべきである。企業は、告発の為に最適な情報を法執行者に対して提示できるはずである。

- 認定送信者リストの設定

業界慣行上問題の無い振舞いをする優良電子メール送信者の“ホワイトリスト”を作り、そこからのメールを優先させることは、自主規制手法を適用する上で有効である。このアプローチを取れば、自主規制の有効性が認められて行くし、オンラインマーケティングへの顧客信頼も増すであろう。既にこの様な“ホワイトリスト”を自らのサービスの範囲で使っているISPが存在する。この先の目標はその様なリストを公開し、業界内での周知のホワイトリストにして行く事である。この様なホワイトリストの国際化が広まって行けば、ISP毎の求めざる電子メールに対する現行の取扱方針も、より精緻なものに変わってゆくかも知れない。そして将来には受け取り先の端末で、受信可能先リストとして使われるかも知れない。

- ID、デジタル署名、デジタル認証利用の勧め

既に幾つもの会社が手を組んで協力グループを作り、識別、認証、要求の正当性確認などがインターネット上で利用できる様に、標準化を進め様としている。認証毎に与えられる保証のレベル又実際の認証のやり方の差、更には認証局（CA）毎に発行する認証の標準化や互換性の問題など、これが広く受け入れられる迄に解決が必要な主要な問題が幾つか残っていて、その解決が図られねばならない。<sup>(注6)</sup> 求めざる電子メール問題との関わり合いに関して云えば、上記の様な問題の解決策や信頼マークの手法などが、今その応用として考えられているトランザクション処理通信の範囲を越えて、広く電子通信一般に適用される可能性がある。結果的に電子メールですら、上記の様な要求を満たすことが必要だとの業界慣行になるかも知れない。

- ネットワークの濫用を防ぐ為の業界協力

かつてはインターネットが如何にオープンで相互に接続されたネットワークであるかの象徴だったオープンサーバーの存在は、今や世界的に深刻な問題を引き起こしている。それは、オープンサーバーが簡単にスパム送信者に乗っ取られてしまうからである。誰もが簡単に、オープンサーバーを使って、大量の求めざる電子メールを他社の電子メールサーバーに流し

---

(注6) サイバーセキュリティについてのGBDe東京勧告(2001年9月)を参照。

込んでしまえるからである。どうも、甚だ宜しくなく構成されたメールサーバーを根絶し得る見込みは無いが、ISP が共同して、悪い振舞いをするオープンリレーサーバーを見つけ出し、ブロックし、再構築を促し、或いは締め出してしまうことは、疑いもなく、貴重な産業界の資源の有効利用を図ることにつながる。

#### ● ISP 間で了解の取れたフィルタリング策

これ迄フィルタリングは、一体どれが正しい電子メールで、どれがその反対の求めざる電子メールであるかを一番良く知っている受け取り手の方でこそ行うべきだとされてきた。しかしながら、ISP が共同してのアプローチが求めざる電子メールの総数を実質的に減らす上で有効だとの認識が出来上がる迄の間は、各 ISP は外部から入手したブラックリストや自ら作成したブラックリストを使って、求めざる電子メールのフィルタリングやブロッキングを続けなければならないだろう。この様なやり方は、引き続き、契約書や利用規定上の文面によって正当化されることになるだろう。しかしながら有効なブロッキング手段を適用するということは、同時に大量の正当な電子メールも取り去ってしまうことにつながる。ISP は、多分世界的に最も大規模なサービスプロバイダーの仲介調整の下で、どの様なレベルの技術的フィルタリングを行うべきかについての協調を図る必要がある。

### 電子メールの商業的利用者に対して

#### ● 自主的な実施対策を採用すること

以下はその例である。状況次第ではあるが、これらのやり方が商業的利用者採用されている。

- 電子メールアドレスの収集、利用及び開示に関して、広く認められている公正な取扱い習慣及び適用される個人情報保護法の許す範囲で、適切かつ有効なその実効策を策定し、それを遵守すること。
- 顧客との間に未だ商業的關係が成立していない場合には、出来ればオプトインの手法を用いるなど、既に商業的關係が成立している顧客に対するとは別の手法を用いること。
- 電子メールの主題欄に、ハッキリした内容でかつ目に付き易い形で、こ



これは商業的勧誘メールであると記すこと。

- 以後の電子メールの受信に対する、明確で容易なオプトアウトを提供すること。
- 正確でかつ常に更新済みの送り先及び受信拒否者の電子メールアドレスリストを持つこと。
- 第三者から入手した電子メールアドレスのリストを用いる時には、ハッキリとした形でかつ理解し易い内容で、オプトアウト機能を用意した上で、先ずは顧客の承諾を得ること。
- 同じく第三者から入手した電子メールアドレスのリストを用いる時は、その最初に届ける電子メールにおいて、そのメールアドレスを入手した方法を個々に説明すること。

#### ● 国際的に受け入れられる様な行動基準を編み出すこと

正当な商業的電子メールはスパムとは違うと云うことを明らかにする流れの中で、通信販売協会その他の業界団体は、業界行動規範を作り、関係者が合意調印した上でそれを公表すべきである。そのガイドラインの原型となるべきものは既に存在しているのであるから、これをより精緻なものにし、形を変えるなどして、受け入れ可能な、求めざる電子メール対策の業界標準にすれば良い。その様な業界標準は国際的な視野の下で作られ、国毎に異なる様々な法律的要求を満たすものでなければならない。電子メールアドレスの入手をより困難にすることも、長期的には求めざる電子メールの数を減らし、顧客の信頼を増大させる。

## VI. 政府への勧告

世界各国の政府は、急速に増大しつつあるこの求めざる電子メール問題を解決する上で、重要な役割を担っている。

### 法の執行

政府は法の執行に当たる行政機関に対して、既存の関係諸法及び消費者保護法の施行に関する解釈や、応用の幅をより大胆に広げるべく指導すべきである。既存法の国内的及び国際的な適用は、時間は掛かるかも知れないが有効であり、合わせて世界各国の政府は求めざる電子メール退治の役目を真剣に果たそうとしているとのメッセージを違反者に対して送ることになる。

## 国際的協調と協力

各国政府は求めざる電子通信問題の解決に向けての協調された対策案を共同策定する為の、国際的な政策基盤を作り出す機会を求めるべきである。プライバシーの問題とも密接に関係しているものの、求めざる電子通信問題の国際的な解決に向けての最も効率の良い手段は、より広範な問題であるサイバーセキュリティの問題と一緒に考えていくことであろう。

その意味において、政府の取るべき対応には以下が含まれよう。

- 政府と民間との間で情報を共有するメカニズムを作り上げて、しかもそれを法的に正当化すること

インターネット上での不正行為に関する情報を時宜を得て共有することは、犯人を突き止めてその者に正義を知らしめる上での重要な要素となる。しかしながら、民間企業間にその様な特別な目的の情報交換メカニズムを作り上げることににおいては、トラスト禁止法との関係が出てくるので、それを実現する上ではこの点についての明確な当局の意思表示が必要となる。加えて、政府と民間との間にその様な情報チャンネルを作るに際しては、プライバシー、情報保護、情報保存などの局面においての適切なセーフガード措置が必要となる。これはサイバーセキュリティの局面における政府、民間情報共有の場合と同様であって、多分この二つの要求を同時に取扱った方が能率が良いであろう。

- 国境を越える詐欺行為に対しての国際的に同意された法執行

インターネットは本質的に国境を越えていくから、国境を越えた協力は必要不可欠である。或る国の法律が厳しくとも他の国の法律が寛容であれば、スパム送信者は必ずやより関係法の内容が緩やかな国に移動して、そこにスパム安息所を作り出してしまふ。各国政府は法の違反者に対しては、追及、告発、犯人引渡しの国際的取り決めが各国の法執行部門の間にあると云うことを確約すべきである。

- 各国政府機関から提出された情報に基づく悪名高き求めざる電子メール送信者についてのグローバルリストの作成、及び正当な理由がある場合におけるその自由閲覧可能性

求めざる電子メールの送信者を列記したブラックリストの利用については、様々な意見がある。一般にはブラックリストは個人又は個々の組織によって管理されていて、公表物ではなく、勝手に閲覧できるものでもなく、作成に当たってはプライバシーなど無視されていて、手順を踏んだからとして入手できるものではない。しかしながら、そのリストの存在があまりに認識され、その内容が信頼に足る様なブラックリストがあれば、それはISPにとって、求めざる電子メールの数を減らそうとする努力を払う上で、大変に役に立つものとなる。その様なリストを作り上げようとする試みにおいては、同時にまた間違っただけでそのリストに載せられてしまった者に対して事前に通知を与えて、そのリスト上への記載が実際に行われる前に、無実だから止めてくれと反論する機会を与える様な機構をも、備えねばならない。

## 新法

既存法の執行のみでは不十分な時には、新法の導入が必要となる。しかしながら、多分如何なるインターネットのみを対象とした新法も必要性が無い。それよりも既存法がオンライン環境に適用できて、その結果求めざる電子通信の問題にも対応できる様に修正されるべきである。例えば、既に存在する、詐欺、不正広告、侵入などを禁止する法律の修正によって。

政府は、以下の様な内容の国際的な法制度の協調を成し遂げるべきである。

- 重い刑事罰の適用や、もしそれが適切な場合には民事罰の追加適用によって、被害者の権利の現状復帰を図ること。
- 何が正義に反し、欺瞞的で、慣行に反するかを定義して、何が不正行為かを明確にさせること（例えば、送り手の名前・アドレスやヘッダーに偽りがあってはいけない、など）
- 詐欺行為とは何かについては明確にさせること（例えば、アカウントハッキング、オープンリレーの不正使用、他人を欺く為の同一人による複数アカウントの開設、電子メールアカウントやドメインネームの不正登録、など）

政府は同時にまた、スパム送信者を雇用して、その者に求めざる電子メールを送らせることによって利益を得ている黒幕の存在を突き止める事の可能性について、思い巡らすべきである。大多数の求めざる電子メールは、消費者に何かを買

うことを決意させるのがその目的であるからして、基本的にはそれを目論む悪徳商人又はマーケッターを捕まえ出すことになる。この場合、政府はまた以下についても考えるべきである。

- 黒幕にはどのような形での責任が問われるべきか。
- 黒幕とスパム送信者との間でのどのような証拠又は因果関係が、その様な責任を問う上で必要か。

## 教育と周知徹底

真に協調的な進め方の一環として、政府、民間企業、それに消費者団体は共同して、国際的な消費者教育のキャンペーンを張るべきである。消費者と云うものはこの場合、問題を複雑化する一部ではなくて、問題解決を容易にする為の一部として見なされねばならない。それには教育に関する新しい考え方が必要で、その様な教育を通じて消費者に対応力が与えられなければならない。以下が必要である。

- 求めざる電子メールに対するフィルタリング手段の様な、技術的解決策が消費者に与えられること。
- 自らの身を自分で守るのに役立つユーザーガイドが作られること。
- 消費者の権利、報告義務及び問題が生じた時に得られる救済策についての理解が得られる様にする事。



Global Business Dialogue on Electronic Commerce

消費者信頼構築WG  
ADR（裁判外紛争処理）ガイドライン  
GBDeとConsumers Internationalとの合意に基づく

2003年11月6日

## 初めに

e-コマース（特に、国際間のB2C）は、消費者が紛争が生じた際にも自分の利益が十分に保護されると感じさえすれば、縮小することなく成長するだろう。同時に、業者の方は（特に中小企業(SME)）インターネット取引に起因する消費者紛争の困難な問題に直面するかもしれない、という事に関心がある。

国際的なインターネット取引に起因する紛争の裁判所への訴えは、しばしば、適用すべき法律、及び、管轄権という難問によって複雑化される。更に、国際的な裁判手続きに掛かる費用は、紛争対象となった品物やサービスの価格よりも高価なものになるかも知れない。もし裁判が紛争を解決する唯一の手段ならば、それは国際的なe-コマースにおいて消費者の信頼を高めることもなく、業者に対してはその商圈を地理的に制限するように働く強い力となり、これにより、競争や消費者の選択が制限されることになるだろう。

例えば欧州連合内や米国内という地域レベルでさえ、消費者保護における消費者の権利やレベルについて、政府間に広く異なる見解がある。完璧な準拠法の国際協調や合法的な管轄権の国際協定は、理論上は理想的な解決かもしれないが、これが近々の内に満足な形で実現されるとは思い難い。

状況は、少なくとも合法的に管轄する裁判所の問題について、同じくらい困難である。消費者は業者が存在する外国の裁判所に訴えることを望まないのも、単なる「出荷国原則（country of origin）」の適用は、オンライン取引の信用を押し上げるのには十分ではないことを産業界は認めている。反対に、オンライン顧客がいる可能性のある全ての国の様々な異なる法律、手続きおよび法の及ぶ範囲等に対応しなければならなくなる様な国際的な取引には、業者は熱心にはならないので、「消費国原則（country of destination）」の適用もまた正しい答えにはならない。さらに、多くの場合、国境を越えての判決実行のコストおよび複雑さが実効的な救済の道を塞いでしまい、この原則は消費者に対しては幻の保護を与えるだけになるかもしれない。

恐らく、このジレンマから抜け出し、e-コマースにおける消費者信頼を得るための重要な鍵は、厄介で高価な裁判所への訴えの代わりに、司法に依らない魅力的な紛争解決手段を、インターネット業者が彼らの顧客に対して提供することである。

オフライン世界では、裁判外紛争処理(ADR)システムは、(顧客満足システムの枠組みの中での) 企業との単純な接触によっては解決されない消費者の苦情を伝える為の有効かつ迅速で効率的な方法としてまったくの成功裡に利用されており、更に、(少なくとも世界の一部では) まだ限られてはいるが、B2C インターネット取引に関係しての ADR の肯定的な経験が既に報告されている。

ADR により、消費者は適正に適時な方法で訴えることができる。ADR によって、両当事者は、政府行政機関や裁判所に訴えることによる遅延やコストを回避できる。さらに、ADR の使用は行政や司法システム(小額裁判所が存在する場合であれ)に対する過重な負担を低減する一方で、同時に、一般的には、消費者が ADR の結果に不満がある場合には、法的な救済を求めるとの消費者の権利を保護する。とどめとして、消費者保護機関や法廷が紛争解決の際に限られた救済策しか提示できない(法律などで規程されている場合は特に) のに対して、ADR は両方の当事者を満足させるに足る柔軟かつ創造的な解決を見つけ出すことが出来る。

この GBDe ペーパーは、オンライン ADR システムを提供中の民間組織を含め、地球上の全地域の莫大な数の企業および業界団体の実際的な経験に基づいて書かれたものである。その内容については、政府および消費者組織の代表者からの意見をも取りいれて議論し作成されたものである。

このペーパーは、インターネット業者、ADR サービスプロバイダーおよび政府への勧告から成る。ガイダンスは、ADR システムの使用と開発に役立てるものである。勧告は、効果的な ADR を求めるビジネス側の要望を満たし、かつ、e-コマースに関する消費者の高度な信頼を形成する様な政府の政策活動を提唱するものである。

### 定義

この勧告の中で使われる「裁判外紛争処理(ADR)」という用語は、物品の売り手又はサービスのプロバイダーと最終消費者の間(B2C)で「電子的(主にインターネット)」に行われた契約に起因する義務に関係した紛争を解決する、法廷以外の公平な組織によって行われる全ての方法をカバーする。

「仲裁」「調停」「和解斡旋/交渉」のような、ADR の概念の中のものより明確な区分は、しばしば混同され、不正確に適用される。しかしながら、そのような区分は、手続きにおける、紛争解決オフィサーの役割及び結果の強制力と関係があると考えられる。

「仲裁 (Arbitration)」は、通常、当事者とは関係ない1人あるいは複数の仲裁者が、両当事者に事実および彼らの論点(口頭または書面手続き)を提出させ、最終的に公平性によるか又は法律によるかして判断を下す、と言う手続きである。準拠法は、殆どの場合当事者間の合意によって決定される。仲裁はその定義により、通常、最終決定であり拘束力を持つ。それ故に多くの場合、国境を越える企業-消費者間(B2C)の、管轄権を超えた取り引きに簡単に適用されるのは困難であろう。

「調停 (Mediation)」は、通常、調停人が、両当事者が合意に達するまで、両者間で和解提案とその対抗提案のやり取りを単に相手方に伝える、と言う手続きである。調停人は交渉に干渉せず、最終合意を記録するだけである。両者が合意して、調停に成功した場合その結果は法律上の契約であり、その効力の範囲内で執行可能である。

「和解斡旋 (Conciliation) / 交渉 (Negotiation)」は、通常、当事者とは関係ない和解斡旋人が公平な歩み寄りに向けて当事者を積極的に導く、という手続きである。この手続きは法的なものではないが、そのかわりに、準拠法を詳細に調査する必要がない。両当事者の法的権利および義務についての理解(対立するかもしれない)は、勿論意味合いを持つが、それよりも、公平性が決定要因となるだろう。(最終)提案が両当事者間で合意された場合、それは契約として扱われ、その効力の範囲内で執行可能となる。当事者が妥協点を見出せない場合には、両者のいずれもが裁判所に持ち込むことは自由である。

正常な商売感覚に発する販売後のサービスとして、業者によって提示される消費者との間の両者間に純粹に閉じる内部紛争解決業務は、裁判手続きに対する代案ではなく、取引きに関する意見の不一致の場合に救済を得ようとする消費者に対して十分な公平性の保証を提供するものではないかもしれない。しかし、もちろん、ビジネス/消費者間での直接的な解決は、それが可能でさえあればB2Cインターネット取引きに関する顧客の苦情を解決する好ましい手段である。これらのサービスは「顧客満足システム」と呼ばれ、救済の段階の1ステップとなり得る。例えば、顧客が業者によって提示されたADRの使用を望む場合にも、ADRオフィサーに訴える前に、そのようなサービス(コールセンター、苦情サービスなど)に最初に苦情を申し立てることを勧められることがあっても良い。



## 範囲

これらの勧告は、e-コマースの中でもっぱら企業-消費者間(B2C)の紛争について取り扱う。ADRは、まだ比較的知られておらず行なわれてもいない。企業間(B2B)取引に起因する紛争の解決は、オフライン・オンラインの場合ともに、非常に高度な業界自主原則に従い、殆どが拘束力のある仲裁に従う形を取っている。消費者保護と消費者信頼の問題は、この意味合いにおいてB2Bには無関係である。従って、B2B ADRのための新しい勧告を生み出す必要もないし、B2C紛争解決と同じパラメーターの下でB2Bに関する問題に取り組むことも適切ではない。

既に運用に入っているか設立途上にある、B2Cインターネット取引のためのADRシステムに関する調査によると、それらの多くは、(監査法人、銀行、保険会社、法律事務所などの)企業のグループ、業界団体、(大学を含む)公共機関、あるいは消費者団体の計画の下で、しばしば独立したビジネスとして、設置されていると分かる。それらは、スポンサーからの支援と利用料金によってコストを賄っている(スポンサーは、通常、その顧客に特定のADRシステムのサービスを提示する業者である)。いくつかの実例では、パイロットプロジェクトとしての扱いで政府から資金が提供されている。理屈の上だけから云えば、人々は、十分な公平性が保証される場合には、個々の業者によってADRシステムが設立されていてもそれを排除しないだろう。

この文書に記載されているビジネスへの勧告は、紛争が生じた場合それをADRへ提起する様に顧客に推薦するインターネット業者、及びサービスとしてADRを提供する機関、の両者にむけられたものである。

## インターネット上の業者への勧告

### 企業内の顧客満足プログラム使用の促進

紛争の際の最初でかつ好ましい救済方法として、インターネット顧客に対して、企業が運営する顧客満足システムへ申し入れる機会が提供されるべきである。取引のタイプおよびシステムの性質によっては、そのようなアプローチはADRの有効な代案として役に立つであろう。例えば、安価な商品を販売する業者は、ADRシステムを確立するより、むしろ全ての顧客に無条件の返金保証を提示することを選択するだろう。何れの場合にも、ADRメカニズムの利用に先立ち、顧客の苦

情が最初に企業組織内の顧客満足システムに向く様にさせることが望ましく思われる。

### **ADR の可能性の提案**

十分な顧客満足が企業内のシステムによって保証される場合を除き、B2C 取引に使われるウェブサイトの顧客に対して、業者としてはオンライン取引から生じる紛争の解決を1つ以上の指定されたADRシステムに提起する準備のあることが通知されるべきである。ADRによる紛争解決に関する情報は、行動規範(トラストマーク)に関連する枠組みの中で一般的な販売条件の一項目として、あるいは提供が必要な総ての情報の一部として提供されるべきである。

ADRは紛争が生じた場合に顧客が自主的に取り得るひとつの手段として提示されるべきものであり、契約上の責務とされてはならない。

### **結果拘束力のある仲裁**

業者は一般に、消費者をその結果に拘束する仲裁の利用を避けるべきであり、その理由は消費者の電子商取引に対する信頼を傷つける可能性があるからである。逆に、トラストマークがその加入業者に対して仲裁結果への拘束を義務付けることは、電子商取引における消費者信頼の増進に役立つであろう。消費者に結果拘束を求める仲裁の利用は限定的な場合に限られるべきであり、その場合には公平性、透明性及び公的説明性の原則が明らかに適合されなければならない。顧客が自らを結果拘束するような仲裁に参加するかどうかの決定は、紛争発生以前ではなく、発生後に十分な説明を受けた上で、自発的に行われなければならない。

### **ADR 条件の通知**

潜在的な顧客には、ADRへの提起の条件(オンライン、その他)、コスト(無料、公称料金、業者によって賄われるコスト、等)、ADR(仲裁、調停、和解斡旋/交渉など)の法的な性質、そしてその結果(拘束/非拘束/業者のみ拘束、実行性)、およびその他の審判所、特に法廷への関わり方に関して通知されるべきである。

### **報復の禁止**

業者は、顧客が紛争に関してADRサービスプロバイダーとの接触を開始したから

の理由で、顧客に対するいかなる報復措置をも取るべきではない。

## ADR サービスプロバイダーへの勧告

### 公平性

その決定が自立的に行われていると認知されるためには、ADR 職員は公平でなくてはならず、これにより、ADR を提供する組織の評価や信用を高めることとなる。適切に構成された監視組織の設置や、明確な基準に従った紛争解決オフィサーの任命、などの適切な方法によって、公平性が保証されなければならない。ADR サービスの運営構造は、総ての点において中立性が保証されるように作られねばならない。

紛争解決職員は、紛争を解決する際に、業者および消費者の圧力から絶縁されなければならない。紛争額が重要な場合や、ADR の結果が両当事者を最終的に拘束する場合には、より一層高い透明性（例えば、(判定理由の説明を求める権利を持つ) 当事者に紛争解決オフィサーの名前が知らされるなど) が配慮されるべきである。業者が特定の仲裁サービスを繰り返し利用する場合には、可能な限り、紛争解決にあたる ADR オフィサーは継続的に中立性を保証するために、輪番交代を行うべきである。

### ADR オフィサーの資格

紛争解決オフィサーは、職務を全うするに足るスキルと訓練成果を身につけるべきである。公式の弁護士資格およびライセンスは要求されるべきではない。

### 利用のし易さと利便性

ADR システムは、何れの国からも容易にアクセス可能であるべきである。オンラインアクセスは好ましい選択と言えるだろう。訴えを行なうに際しての状況説明要求は必要最小限に抑えられるべきである。顧客は、書式整備及び提出に当たり可能な限りのガイダンスを受けるべきである。さらに、業者、ADR および顧客の夫々が異なる言語を使うことに起因するであろう問題について適切な対応が成されるべきである。

## 迅速性

実効性のために、消費者と業者の両方の要求に合う限り、ADR システムは紛争を迅速に解決しなければならない。如何なる場合にも、法廷よりも迅速に満足な結果を提供しなければ意味がない。

## 消費者にとっての廉価性

ADR サービスは、無償もしくは適度なコストで、消費者に提供されるべきである。尤もこの際、取るに足らない安易なクレームの回避は考慮されるべきである。ADR システムの公平なふるい分けプロセスが、これを可能にする。ADR に先立って顧客満足プログラムへ苦情が持ち込まれれば、クレームの本質の早期評価が可能となるだろう。

実際、ADR のコストは、消費者およびビジネスの両方にとって、公式の行政及び法的な手段を取るより著しく低いだろう。これは、証言、審問、法的な代理人の設定、および海外旅行を要する個人の出廷を含む公式の手段に掛かる時間と金銭の両方をコストに換算して考えると、全く正しい。

## 透明性

ADR システムは、公表された手続きの規則によって機能するべきであり、そこには救済を求める顧客が、提示された ADR を使用するか、法廷に訴えるかを決定する為に必要な適切な要素について、すべて明白に記述されるべきである。

ADR システムの信用と満足を確保するために、以下の情報が含まれるべきである。

- 取り扱う紛争の種類、地域の範囲、紛争の価額、に関する既存の制限、
- 問題を取り扱うに当たってのルール： 消費者が予備的に適合すべき条件（例えば、業者によって提示される顧客満足システムを救済を得るために最初に試みること）、他の手続き的な規則として、手続きは書面か口頭か、全面的に又は部分的にオンラインか、口頭の審問が可能か又は必須か（両当事者個別か同席か）、本人の出席又は代理人の可能性、使用する言語、
- 判断の形態とそれに到る判定手順
- 要員リストの公開、個々の事件のための紛争解決オフィサーの選定過程、当事者が判定根拠の説明を求めることの出来る可能性
- 両当事者が手続きのために、或いは判定額に応じて支払うことになるであろう

う費用、

- 判定の根拠となるルールの種類（法規程、公平性、行動規範など）
- 進行の方法、判定結果は公開か、訴えおよび手続きの取り扱いの機密性；
- 合意された結果の執行性、および他の請求の可能性。

ADR プロバイダーは、取り扱った総ての ADR ケース及びそこで行なった判定の評価が行える様な年次報告を公表すべきである。その際、特定の事件に関する情報およびデータの機密性を尊重すべきである。評価として含まれるべきは、少なくとも、依頼されたケースの総合リスト、そのうち ADR に至らずに解決したケース、ADR により解決したケース、それに ADR によっても解決しなかったケースである。可能な限り報告書には、ADR に至る前に、又は ADR によって解決した結果が、業者又は消費者のいずれに有利に運んだかの報告が含まれるべきである。片側又は両側にとって結果拘束力のある仲裁の場合には、業者の身元、紛争の種類、更には可能な限りにおいて、紛争結果が業者と消費者のいずれに有利に終わったかの情報が公開されるべきである。

## 代理原則

ADR 手続きは、そのすべての段階で、第三者による代理又は支援される権利を当事者から奪ってはならない。

## 適用規則

産業界、消費者および政府が e-コマースにおける消費者の信頼を高める為の戦略的な重要性を ADR システムの発展に求める主な理由の 1 つは、ADR では正式な法廷手続きにおいては適用される詳細な法規則についての煩わしく費用が掛かり難しい調査を行なうことなく、適切な方法で紛争を解決することができるからである。政府は特に、この方式によって消費者及び企業両者の権利が保護されることにつき確信する必要があり、合わせて国際間の e コマースの発展を阻害するような行動を取ることを避けねばならない。

ADR 紛争解決オフィサーは、公平性および(または)行動規範に基づいて判断を下してもよい。ADR 判断の根底となるこの柔軟性が、世界的な消費者保護の高い標準の発展の機会をもたらす。

## 消費者認識

消費者と業者の双方が仲裁措置に合意する特別な場合を除いては（下記参照）、消費者はADR手法を選ぶことによって法廷に立つ権利を行使することを疎んじることとなろう。

ADRは紛争が生じた場合に顧客が自主的に取り得るひとつの手段として提示されるべきものであり、契約上の責務とされてはならない。それ故に、当事者にその決定が拘束力を持つことが前もって通知され、当事者がこれを受け入れた場合のみ、紛争解決オフィサーの決定が、両当事者を拘束しても良いであろう。同様に、業者は、紛争が発生するに先立って拘束力のある仲裁の使用の約束を、消費者から求めるべきではない。これは、法廷に訴える権利を消費者から奪うことになるからである。

## 法執行機関への照会

インターネット業者側に、詐欺、虚偽、様々な悪用の疑いが見られた場合には、ADR サービスプロバイダーは顧客の承諾を得た上で、紛争の内容を法執行機関に紹介すべきである。

## 政府への勧告

ADRのための法的な枠組みに関する研究により明らかになったことは、法的な枠組みは国際的な協定と幾つかのレベル（連邦／州、地方／国など）での法律との間で分裂してしまっている、ということである。結果として、世界的な適用のために考えられたADRシステムは、多くの条件（必ずしも適合性をもつとは限らない）に配慮しなければならない。これらの要素のいくつかは、例えば、紛争をADRに訴えるための合意は紛争の発生後しか始めてはならないという要件のように、容易に調整が可能である。他に調整の難しい要素もある：例えば、幾つかの国の暗号化または認証に関する法律は、オンライン手続きに適切なレベルの機密性およびセキュリティ保持を不可能にしており、また、いくつかの国ではオンラインでの契約締結を認めていない。

他方、多くの政府は、ADRが、電子商取引が適切に機能するための、および消費者信頼を高めるための必須要素であるという、GBDeの立場を共有すると公表し

ている。従って、GBDe は、政府がこの勧告に沿った政策方針を採用することを期待する。

### **裁判管轄と準拠法についての国際ルール**

ADR は多くの紛争に適切な解決を与えることができるが、理想的な場合でさえ、少なからぬ紛争が法廷で終結せざるを得ぬことは認識されるべきである。したがって、合わせてまた、その様な問題が ADR システム側に提起されることもあるので、GBDe は、まだ e-コマースに関する裁判管轄権と準拠法の問題が、至急企業投資および消費者信頼の両方を促進する方法で、扱われる必要があることを明白に申し述べたい。この点についての GBDe の姿勢は、1999 年の準拠法 (Jurisdiction) WG が発表した「パリ勧告」に書かれている。

### **顧客満足システムおよび ADR の使用促進**

B2C 商用紛争の解決に関する ADR システムとその役割について、積極的に周知認識の促進を願いたい。合わせて、顧客満足システムを設ける企業の継続的な努力を認めてほしい。これは、ADR あるいは業者に対する法廷訴訟手続きのいずれかの開始に先立って使用されるべきである。さらに、法廷へ訴える代わりあるいはその前に、ADR システムを使用する様、政策的に消費者を啓蒙すべきである。

### **教育とトレーニング**

ADR システムプロバイダーが行う、ADR オフィサーに対する教育活動の支援と促進を願いたい。

### **効力ある ADR システムの勧奨**

政府には、ADR に先立つ救済の第一手段として、各企業内の顧客満足システムの利用を奨励してほしい。政府は、その存在が独立で、運用に透明性があり、その利用が高額でなく、柔軟性がある、社会説明性のある、高品質な ADR サービスの開発に関して、それを誰が経営しているかに関わらず偏見なしに、支援と促進を行うべきである。ADR サービスプロバイダー間に適切な競争状態を導入し、更に、ADR サービスプロバイダー間に業務協定を結ばせることに力点が置かれるべきである。

規制を導入する時にはいつでもそうであるが、政府認定制度を導入するか、又、導入する場合にはどの様に導入するかは決定については、その問題についての熟慮と利害得失バランスの評価についてのみ追及されるべきである。認定制度の開発にあたっては、消費者と企業それぞれの利益について、公平かつ透明かつ経済性の見地に加えて、電子商取引発展と云う究極目的が考慮されねばならない。

どのような政府管掌の評価方法も、消費者団体、産業界、その他の関係者に計られねばならない。可能な限りにおいて、他国や他地域での同様な試みとの間での協調も図られねばならず、これは評価方法に関して国際的な原則やルール、自主規制を開発せんとする動きと調和を取るためである。

### **公平性あるいは行為規範を基礎とする ADR**

ADRシステムが公平性あるいは行動規範に基づいて機能を果たすことを認められたい。紛争解決オフィサーに対して公式の弁護士資格および免許の所持を必須条件とすべきではない。調停/仲裁手続きを業務として行うことを、免許された弁護士だけが行えるべく法的に規制している国があるが、規制緩和および適切な法的枠組み設定の方向に向かうべきである。

### **グローバルな ADR へのアクセス及び ADR の適用**

他国の政府や国際機関との共同作業により、世界的に適用可能な ADR システムの開発を促進し、ADR に関し世界的な視野を持っていただきたい。

### **ADR への最新技術の適用**

消費者紛争を解決するために革新的な技術を使用することに対して障害を作ることの差し控え、オンライン ADR における適切なレベルの機密性およびセキュリティの適用に対する障害を除去願いたい。これは、主に認証とセキュリティに関する法律に起因する。

### **ADR のための手続き要件および形式要件の最小限化**

ADR が法廷制度とほぼ同等の手続き要件に従わなくてはならないと言う一部の国の法律の要件を除去して頂きたい。同様のことが、オンライン ADR の使用を阻害する特定の形式要件にも当てはまる。ADR に入る両当事者は 結果に関する充分



な透明性および情報がある限り、彼らが望むなら、手続き構造からは自由とされるべきである。

### **オンラインの状況へのオフライン ADR の要件の適合**

国内法又は国際条約において、オンラインで紛争解決条項を含む契約を完了することを禁止することを止め、既存のオフライン ADR のための法制度的な枠組みをオンラインの要件に適合させられたい。

### **官民の政策協力**

消費者とビジネス双方のニーズを反映し、顧客に理解し易い十分に多様性ある ADR システムを達成すべく、バランスを維持するために官民の緊密な協力を確保することを提案したい。

### **強制措置**

もし、ADR サービスが自ら宣言した運営方針と運営方法を守らぬ場合には、適切な強制措置をとられたい。



Global Business Dialogue on Electronic Commerce

## インターネットの未来 WG

2003 年 11 月 6 日

共同議長：                   NTT DATA  
(アジア/オセアニア)       代表取締役副社長  
                                  中村 直司

共同議長：                   Cobos Stofberg  
(欧州/アフリカ)           CEO  
                                  MIH

## インターネットの未来

インターネット利用が進化するに従い、重要な新しい課題が登場することがますます常態となりつつある。

G B D e はインターネット関連事業の先導者として、インターネットの将来の発展に直接影響を及ぼす課題について政策提言を行ってきた。G B D e では、インターネットの未来ワーキンググループを編成し、実業界と政策立案者の双方に一般的なガイドラインとして役立つような構想を組み立てた。

中でもG B D e は、ブロードバンドとサイバーセキュリティに関するこれまでの提言を、国際環境の変化を考慮して更新した。これに加えて、インターネットの未来ワーキンググループは、R F I D を政策立案者と実業界がともに注意深く考慮しなければならない可能性をもった課題として取り上げた。

G B D e メンバー企業は、ブロードバンドサービスの急速な発展と採用を促進する諸条件を支持する点で一致団結している。ブロードバンドネットワークとそれを利用するサービスは、それらの発展を成功裏に導くような条件を整備した国や地域にとって経済成長の重要な動因となった。インターネットが持つ経済的なポテンシャルを十分に実現させるためには、ブロードバンドネットワークが広く利用可能であり、その利用が広がることが極めて重要な要因となっている。これは高速接続を提供することにとどまらず、利用者に様々な革新的なサービスやコンテンツを、競合するが相互接続性のある複数のオープンなプラットフォーム上で提供することである。この文脈で、革新的なビジネスモデルがネットワークの特性とコンテンツの提供の相互補完的な関係を利用して発展する。

電子商取引は、情報化社会全体と、電子政府、Eラーニング、Eヘルスといった市場の継続的な発展というより広い文脈を照合しつつ考えなければならないという理解を、インターネットの未来ワーキンググループの成果は、反映している。

G B D e のサイバーセキュリティに関する提言は、このより広い経済的な視野を考慮に入れたものである。今日、サイバーセキュリティ上の失敗や事故、過失は電子商取引の範囲とはるかに超えた様々な事業活動に影響を及ぼし得ることは、次第に認識されつつある。

G B D e が 2 0 0 1 と 2 0 0 2 年 の 提 言 で 取 り 上 げ た デ ジ タ ル コ ン バ ー ジ ェ ン ス へ 向 け て の 幅 広 い 動 き に よ っ て 、 こ れ ら の 課 題 は 影 響 を う け て い る 。 よ っ て 、 今 日 の 事 業 環 境 に お い て も 、 こ れ ら の 提 言 は 重 要 性 を 失 っ て い な い 。 実 際 、 多 く の デ バ イ ス と 機 器 を 相 互 接 続 し よ う と い う ユ ビ キ タ ス ネ ッ ト ワ ー ク の コ ン セ プ ト は 急 速 に 現 実 の も の と な り つ つ あ る 。

G B D e は 、 イ ン タ ー ネ ッ ト の 未 来 の 発 展 に 向 け た 適 切 な 枠 組 み を 政 府 お よ び そ の 他 の 関 係 者 と の 緊 密 な 協 力 関 係 の も と に 創 り あ げ る た め に 、 提 言 を 行 う 。

# インターネットの未来 WG ブロードバンド

2003 年 11 月 6 日

ラポータ                   :       Josef Cornu  
  
(欧州/アフリカ)           Assistant to Chairman & CEO,  
Member of the Board  
  
Alcatel

## インターネットの未来ワーキンググループ

### ブロードバンドに関するGBDe提言

#### I. ブロードバンド：インターネットの未来に向けたビジョン

##### 1. 共通ビジョン

GBDeメンバーは、ブロードバンドは将来のインターネットの発展にとって重要であるという共通ビジョンを共有する。

GBDeメンバーは、今日の公共政策が将来のビジョンと関連して構築されるべきであると考えている。ビジョンの実行に関わる疑問は、仮定ではなくタイミングであり、その答えは以下の項目の解決法となる。

- 消費者の利益：高速のオンラインブロードバンド接続は、家庭ユーザー、業務ユーザー双方を、生活の質を高める情報化社会に参加し、利益を享受できるようにする。
- 新しいステークホルダーの参加機会：これまで参加する方法が無かったか、考慮されていなかった労働人員や生産的な活動は、ブロードバンドによってより多くの参加機会が得られる。例えば韓国では、ブロードバンドは女性のオフィスワーカーや主婦が、オンライン株取引に半分以上の時間を費やすようになった。この理由には、ブロードバンド接続の「常時利用可能」という性質と、PCやインターネットの利便性の向上が挙げられる。他の新しいステークホルダーの中には、特に地域市場に対する新しい配送経路を使う音声・映像コンテンツの製作者および提供者を含んでいる。
- 経済全般の潜在的成長：利用者の関心を維持し、オンラインアプリケーション（銀行取引、ショッピング、株取引など）の双方向性を促進する上で、応答時間を1秒以下にすることは不可欠である。経済成長は、個々のアプリケーションがファイルやウェブページをダウンロードする応答時間にますます依存している。このことは、ブロードバンドが高速バックボーンだけでなく、ユーザーの家や職場への不可欠な「入口(on-ramps)<sup>1</sup>」を提供しているということを含んでいる。
- 生活様式、教育、保健および市民社会の広範な参加の促進：eヘルス、電子政府、eラーニング、eコミュニティおよびe社会の領域におけるアプリケーションは、全ての市民にとって毎日の生活を改善する潜在性を持っている。ユビキタスブロードバンドは、こうしたアプリケーションを利用可能にする

---

<sup>1</sup> 入口(on-ramps)と出口(off-ramps)： 入口と出口は、自動車が主要な高速道路へアクセスする手段であると同様に、ブロードバンドはインターネットのファイバー基盤が可能にする超高速網へアクセスし、利用するために必要な手段である。

だけでなく、地域に関わらず、全ての社会領域におけるデジタルデバイドの橋渡しをする。社会グループ間（都市と地方、富裕層と貧困層、社会条件に恵まれている層と恵まれていない層、および性差間の成長と繁栄）の格差は、ユビキタスブロードバンド接続とサービスの提供を通じて橋渡しができる。

2002年のブロードバンド提言を作成するにあたり、GBDeメンバーは何点かの緊急な事象に取り組み、実施する必要があることを強く主張する。

## 2. インターネットの未来に向けた貢献

コンテンツと通信の双方の視点から、ブロードバンドがインターネットの環境をどれだけ変えるかを実感することは重要である。

- ブロードバンド接続は、新しいビジネスや社会的アプリケーションを設計する基盤を提供する一方で、より柔軟で双方向性のあるインターネットの構築に不可欠な高速の「出入口」を提供する。
- ブロードバンドは特定の技術基盤に特定されたものではなく、多様で競争的なオープン基盤<sup>2</sup>を通じて提供されることを認識しており、ブロードバンドは新しいマルチメディアブロードバンドサービスやコンテンツ産業の成長を促進する。
- ブロードバンドは、インターネットベースの通信効率について、双方向的な商用アプリケーションが不可欠とする一瞬の応答時間にまで速める。様々な種類のコンテンツの輸送路としての、単一のインターネットベースの基盤を通じて可能になる。
- 創造的なコミュニティや他のプレイヤーへの新しい収益の流れを保証する一方で、新しく効果的な技術的保護手段や電子的権利管理（DRM）は、有益なコンテンツを不正使用から保護する。こうした技術的保護手段は、ブロードバンド網におけるコンテンツの公開の促進や、より良い経済成長の循環につながる環境を創造する。

## 3. ビジネス、経済および社会全体へのインパクト

### a) 革新的ビジネスモデル

ブロードバンドは、新しいマルチメディアやコンテンツの収益をもたらすサービスの機会を創造する。そして、ブロードバンド接続の販売を制限する現在のビジネスモデルの価値を付加する。自由な市場を基盤とした、オープンで競争的な環境は、革新的なブロードバンド価格の提供を促す。従って、バリューチェーン

---

<sup>2</sup> ADSL、ケーブル、ファイバー網、無線LAN、衛星、固定ラジオ、第三世代携帯電話、電話線技術およびDTT（デジタル地上波テレビ）のように、多様な技術をベースにしたもの

上のビジネスパートナーは、新しく異なった収益分配のバランスに必然的に発見する。

ブロードバンド網は提供者と利用者の双方に対して、適度に集中された市場において、適度に調整された利用者のプロフィールを利用した、豊富でより多様化したコンテンツの利用を刺激する。その結果、収益性が向上する。同時に、世界市場へ直接接続することによって、コンテンツおよびサービスプロバイダーはより幅広い消費者にサービスを提供できる。全てのステークホルダーは、収益増大の恩恵を得る。

この後の「c)社会へのインパクト」で詳細に触れるが、ブロードバンドを基盤とした新しいシステムは、民間部門において非常に大きな新しいビジネスの機会を創造する。このシステムは、全市民の生活の質を改善することに使われ、世界的な多くの社会的課題の解決を支援する。

#### b)経済的利益

ブロードバンド網およびサービスは、発展の成功につながる解決法に結びついた国や地域にとって、非常に有益な成長の原動力となっている。韓国は、その好例である。ブロードバンドサービスは1999年中盤に開始された。サービスの豊富さは、韓国の家庭におけるインターネット接続の増加をもたらしている。1999年中盤では全てのインターネット接続のうち、家庭が占める割合は15%であったのが、2001年終盤では50%以上になっている。今日では、そのうち90%以上の接続がブロードバンドである。同時に、インターネット利用は一週間につき16時間以上にものぼる。このことは、13歳から40歳までの年齢層において、既存のテレビ視聴からインターネット利用へ移っていることを示している。その上、地域のコンテンツやサービス提供者の増加が進んだことで、ウェブサイトへの接続の80%が海外のものであったのが、韓国のものに変わった。この影響は、地域における動きだけでなく、中小企業の生産性にとっても重要である。

同じ状況は、欧州や北米でも起こっている。欧州では、双方向性のあるマルチメディアサービスの巨大市場の出現は、パーソナルコンピュータの利用者とそれ以上に多く存在する家庭のテレビ視聴者に影響するが、これは経済全体に対する大きな潜在性を示している。2006年には、400億ユーロ近くある接続収入のほかに、欧州の固定網における新しいブロードバンドサービスによって、およそ400億ユーロの収益を上げるものと思われる。投資額は大きく、新しいサー



ビス部門の発展は、来る数年間のうちに欧州の経済発展の解決法になるものと思われる。そのうえ、他部門の影響による成長は、年間で600億ユーロになると予測されており、これは欧州におけるGDPの50%の増大を示す。

同様に、潜在的な影響が米国において予測されている。電気通信産業（オペレータおよびサプライヤー）と、コンテンツ産業のような関連部門への影響は年間5000億ドルになると予測されている。高速技術および商用化による雇用創出は100万人以上になると予測されており、これは欧州における影響に匹敵する。今日、欧州では1700万人のブロードバンド利用者が存在し、その71%はADSLを利用している。欧州では、旧来の固定網からブロードバンドへ変更する割合は今年初めから上昇している。新しいブロードバンドサービスの巨大市場を創出する前提として、ヨーロッパ人の3分の2が、2010年の段階で固定網からブロードバンド網への変更する割合が年間およそ7%であることが必要である。

カナダでは、オンラインビジネスの増大に伴って、航空宇宙、医薬、通信、コンピュータ、部品、森林、貨物、ライフサイエンスおよび製紙産業において10%から30%のコスト削減を達成したことが評価されている。さらに、ブロードバンドはすべてのカナダ人市民にとって生活の質の向上に大きく寄与するものと思われる。毎秒56Kビット以上のインターネット接続速度を使う家庭の割合は、2000年から2003年にかけて20%から60%にまで伸びた。政府は、全てのカナダ市民に対してブロードバンドサービスが準備されることによって、接続速度の増大や、都市と地方との間のデジタルデバイドを克服する目標を設定した。

#### c)社会への影響

概して、中央政府と社会にとって、全市民の生活の質を改善することは、重要な優先事項である。インターネットを基盤にした技術はこのような業務を支援する。銀行、ショッピング、学習および業務用途に関連した生活の用務の多くは軽減される。ブロードバンド技術の利用は、公共サービスをオフラインからオンラインへと移行させる新しいアプリケーションで、以前は低速であるために実行できなかったものの利用を促進するものと思われる。このことはまた、全ての部門において新しく革新的なサービスを導入することにもなる。

ブロードバンドは他の社会的問題の解決を助ける。例えば、(1) ビデオ電話によって、離れた市民の間の距離を短くする。(2) 家庭から職場への遠隔勤務

によって、交通渋滞を緩和し、勤務時間を柔軟にする。(3) eヘルスは、全ての市民に提供することが可能な新しい手段である。(4) 遠隔監視は安全性の向上に寄与する。(5) 分散したコールセンターやブロードバンドを利用した中小企業、公共サービスは、社会の分散的な発展に寄与する資産である。(6) ブロードバンド網による遠隔教育や他のサービスは、先進国だけでなく、途上国の発展を促す。

## II. ブロードバンドサービスへのチャレンジ

GBDeメンバーは、ブロードバンドサービスの発展に関する以下の主要なチャレンジを認識している。

- すべてのバリューチェーンの参加者（コンテンツ所有者、アグリゲーター、ネットワーク管理者、アクセス提供者、インターネットサービスプロバイダー、および消費者）が恩恵を得る革新的なビジネスモデルの出現。
- ブロードバンドサービスを促進する上で必要なクリティカルマスと規模の経済性を作る、オープンで相互接続性のある標準と基盤の役割。(端末機器、セットトップボックス、およびその他の消費者向け端末の相互接続性、および末端間のサービスの相互接続性など)
- 連続的に提供される無線・有線ブロードバンド網における伝送サービスと、コンテンツとの独立性。(消費者に統合サービスを提供するサービスプロバイダーを考慮に入れて)
- 公的機関との協力において行われるインターネットベースの緊急時・セキュリティサービスの発展と同様に、ベストエフォート型データサービスとして、同一の接続網を通じた高精度のリアルタイムパケット通信サービスの提供
- 知的財産権、コンテンツ保護、電子的権利管理技術およびソリューションの方法(ブロードバンドサービスへの投資に対する信頼性を高めるため、著作権侵害を回避することと同じ)
- ブロードバンド網を通じた新しいコンテンツの提供を促進する、コンテンツおよびコンテンツ流通権に関する規制の方法。
- 衛星、無線ブロードバンドおよびデジタル地上波テレビを含む、接続料金の低減を実現する新技術。漸進的に、これらの技術は多くの国で巨大市場の規模の経済を達成する。また、サービスプロバイダーは、地方が意義ある発展を遂げられるように、ブロードバンドを過疎地域に広める大きな誘因をもたらす。
- グローバルな協力と対話は、制度、技術、市場の実践および標準に関する調和につながる。また、ブロードバンドサービスとコンテンツが容易に入手できるグローバルな環境づくりにつながる。

### Ⅲ. G B D e 提言

#### 1. 政策提言

##### 政府と民間部門がブロードバンドの成功に貢献する

この分野では、民間部門はブロードバンドサービスの発展に役割を負う。政府は、ブロードバンドサービスの利用を促す環境づくりを行う政策を推進すべきである。G B D e メンバーは、政府が以下の方法で、ブロードバンドの需要を刺激する財政条件の整備と投資の実施を進めることを奨励する。

(a) 公共サービスの改善と電子政府（電子入札を含む）、eヘルスおよびeエデュケーションへの投資の加速

(b) 財政的誘因の提供（例えば、遠隔勤務を促進する税制面の優遇；サービスを利用する際の基本コストを変えるのに必要な計画の早期化、非都市地域においてブロードバンドが普及する事例の展開、および、既存の手法のより広範な市場取引など）

(c) ブロードバンド端末の購入を促すための一部エンドユーザーへの支援（図書館、学校、病院および何らかのデジタルデバイスによる障壁によって隔絶された市民など）

(d) 公共、民間の活動分野の一部において、電子政府、電子商取引に対する市民および消費者の信頼を増大させる環境の促進、および、サービスプロバイダー、コンテンツ提供者、消費者に対して、安全な技術を提供する環境の促進。

国家レベルの公共機関はブロードバンド利用者を特定の国家的対象から外すべきである。

それぞれの国には、意欲と市民と事業者が、ブロードバンド接続を備えるよう公式に述べられた対象が求められる。また、長期的にブロードバンド技術に投資する良好な環境を整備する必要がある。欧州連合では、2005年には、インターネット接続の半数がブロードバンド接続になるとするeヨーロッパの目標に到達するためのあらゆる方法が探られなければならない。

政府は推進主体として、ソリューションやビジネスモデルとの幅広い対話を行う。

民間部門は、ブロードバンドサービスを通じたの新しいソリューションやビジネスモデルを開発する一方、業界を越えた提携や協力の実施や、試験サービスの実施によって開発を進めている。マルチメディアのバリューチェーンにおける、ビジネスパートナー間の革新的なビジネスモデルの各局面において、政策立案者は推進主体としてすべてのステークホルダーが継続して対話できるように橋渡しをする。

新しい双方向ブロードバンドサービスは、適切な規制環境の恩恵を得るべきである。

ブロードバンドは、新しく、創造的なサービスの発展と提供のための豊富な環境を提供する。しかし、サービスの革新は、不合理で障壁の高い規制障壁が無く、市場参入が負担にならない時に起こる。

GBDeは、こうしたサービスは過去の規制構造から解放されるべきであると考える。いくつかの例では、過渡期には困難から解放されず、すべての参加者は標準的な市場で競争できるようにしなければならない。いずれにせよ、すべての参加者（既存のサービスやインフラの提供者や、新規参入者に関わらず）は競争的な情報社会サービスに十分に参加できるようにしなければならない。

欧州では、ブロードバンド上の全てのコンテンツサービスに関する良い枠組みについて、電子商取引指令が明確に示している。実際、そうした新しいサービスは情報社会サービスとして扱われ、そうしたアプローチはより多くの規制の枠組みを適用することなく、将来にわたって維持されるべきである。

米国では、連邦政府がブロードバンド普及戦略の調整について、展開を求められている。この戦略には、合理的な目標、すべてのプロバイダーに対する規制の基準、州と連邦政府との間の適切なバランス、映像および放送サービスのよう、異なる基盤が競争的に提供される公平な機会が含まれている。

アジアでは、二つの先進的ブロードバンド市場があり、日本と韓国は近年、部門毎の規制を導入した。複数の接続基盤上で多くの適切な市場が形成されている点が注目されている。

全ての地域で、豊富なコンテンツのオンライン利用が促進され、コンテンツへのアクセスと、コンテンツ流通の市場に関するある程度の水準が保証されるべきである。

#### 定期的に各国のブロードバンド政策の進捗を確認する必要性

技術、市場双方が恒常的に劇的な変化を起こすため、e ジャパンやe ヨーロッパのような主導的取り組みの進捗を定期的に確認することは不可欠である。政府および民間部門は、恒常的なベンチマークだけでなく、国のアクションプランを再検討する際も協力すべきである。

## 予想される規制と、ブロードバンドへの投資を促進する競争環境の整備の必要性

ブロードバンド提供者が、革新的な製品およびサービスに対して実質的な投資を行うことについて安全だと思ふ際には、ブロードバンドインフラおよびサービスの促進において、より多くの進展が起こる。競争原則によって発生する予測可能な規制の枠組みと、全ての市場参加者にとって市場が存在することを保証することは、革新をもたらしながらブロードバンド基盤とサービスへの投資を促進する。

## 2. 産業の提言

### 相互接続性のある標準

供給者とサービスプロバイダーはオープンな標準を開発し、複数の関係者が様々なレベルのバリューチェーンに居る中で、競争的なサービスの枠組みと、競争的なブロードバンドサービス環境の整備を促進することについて、合意を得ることが必要である。しかし、そうした環境においては、消費者が家庭に複数のボックスを無理に設置させるようなことがあってはならず、単一の「インターフェイスボックス」ですべてのサービスが利用できることが望ましい。同時に、終端構造は異なる通信規格や標準によって必要以上に複雑になってはならないことは重要である。

従って、この二つの補完的目標は、相互接続性を支持する標準の定義を推進することによって定義される。(a) ホームネットワーク端末(セットトップボックス等)は新しいサービスとは独立すべきである。(b) コンテンツ提供者とアグリゲーターは同一のコンテンツを異なった接続基盤を通じて提供できるようにしなければならない。(しかし、提供を強要してはならない。)GBDeは、配送経路とは独立して、異なる消費者向け端末間の相互接続性を調整するいくつかの標準化団体における産業界の協力を促進する。

### デジタルデバイドは除去される必要がある

発展途上国におけるブロードバンド技術の提供は、民間部門が情報通信技術を通じた商用活動の適切な見返りに対する目標と同様に、それぞれの国の経済的発展と貧困の軽減を実現する目標と合致する。上述したチャレンジと提言は、同じくここでも適用される。この状況下で、政府は市民にサービスを広め、情報通信技術に良い規制的・財政的状況の変革を促す大きな役割を担う。実行された折には、ブロードバンド技術は、市民、消費者、中小企業、および政府が、経済的格差から起こる不公平や、教育、訓練、地理的分離などの格差から克服することを支援する。

### 3. 社会的提言

#### ブロードバンドの利用によるすべての市民生活の質の向上の拡大

すべての市民へのブロードバンドサービスの提供は、人々の生活や業務の様式を大きく改善させる潜在性を有している。生活の質という局面において特に、アプリケーションの提供には考慮が必要である。特に、以下の領域における発展に言及すべきである。

- a) eヘルス（オンライン医療サービス、遠隔医療、ブロードバンドの専門的医療、研究への応用）
- b) eラーニング（電子化および国の標準的教育資料への適用、遠隔教育、共同教育、マルチメディア情報センターへのアクセス、管理の視点（登録および記録の追跡））
- c) eワーキング（在宅勤務、仮想ネットワーク、ビデオ会議）
- d) 電子政府（電子投票、課税、免許交付、図書館、その他行政サービス）
- e) eコミュニティ（協力アプリケーションや資源共有の開発）

市民に良い影響のあるこれらのサービスによって提供される可能性は、より多くの発展途上国にとって大きいものである。これらの国々は多くの不利益を克服しなければならない。上述したアプリケーションは、デジタルデバイドの橋渡しを行い、ブロードバンド基盤の促進とブロードバンドサービスの提供によって、成果の中核となりうる。

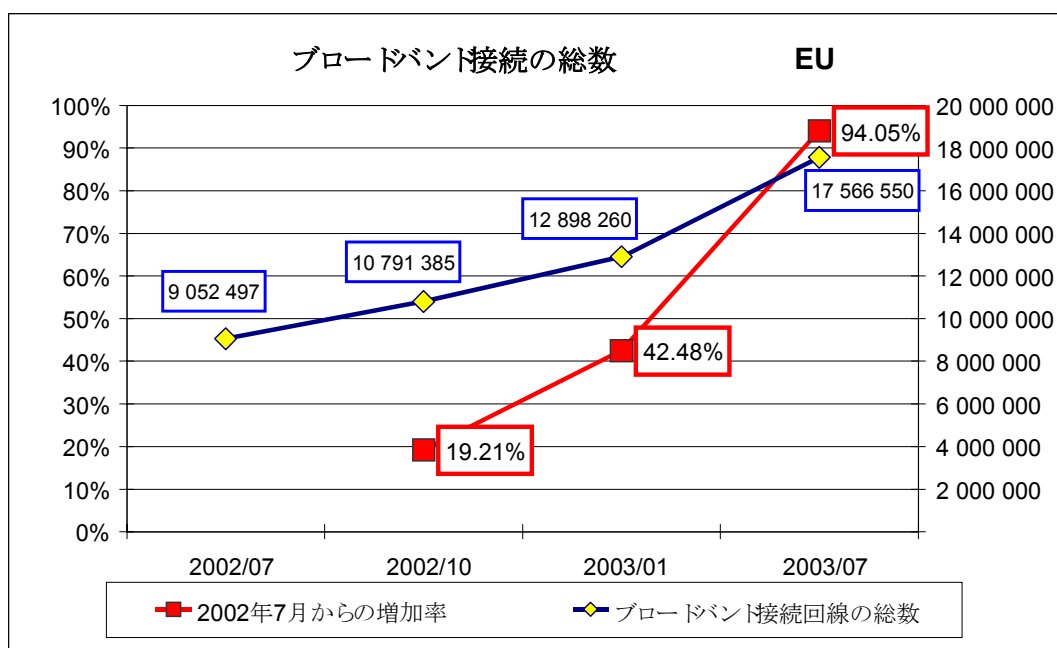
GBDeは、これらの手段が、インターネットの未来における一般的なブロードバンドのビジョンの実現を支援し、利益を収穫することを支援するものと確信する。

## ブロードバンド；欧州の事例

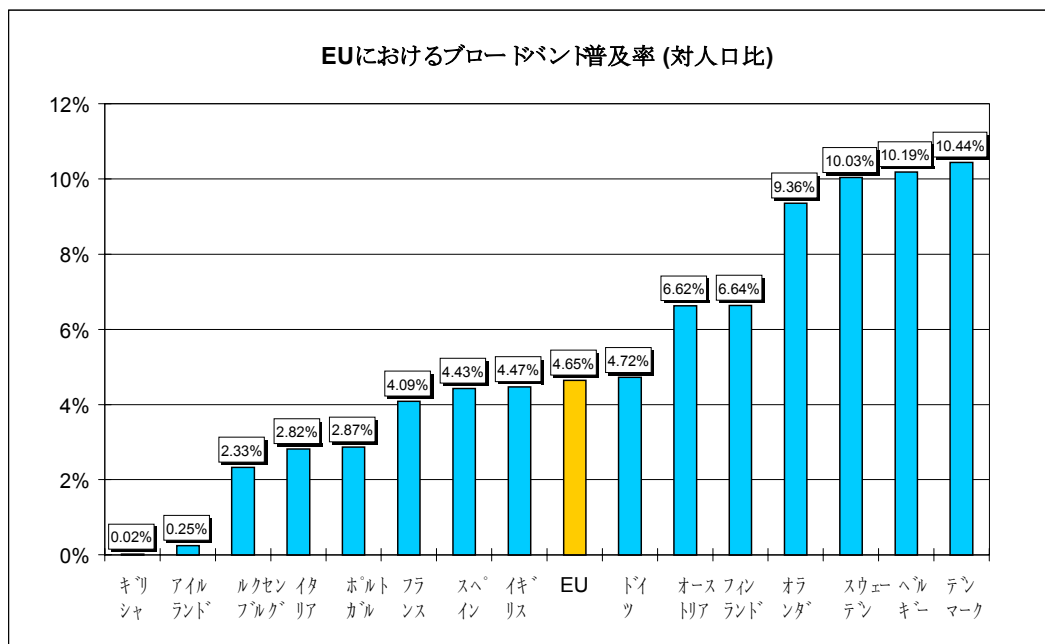
2003年7月1日時点で、EUには17 566 550のブロードバンド回線があり、これは同年1月1日と比べて、36.19%の増加に相当する。これらのブロードバンド回線のうち、12 579 164回線（全体の71.6%）は、DSL回線であり、4 987 386回線（28.4%）は他の伝送手段、大部分はケーブルモデムを使って提供されている。

2003年の最初の6ヶ月間に、合計4 668 290のブロードバンド回線が追加された。これは、2002年の下半期の3 845 763回線増と比べると、顕著な増加である。

以下の図に、成長の傾向を示す：

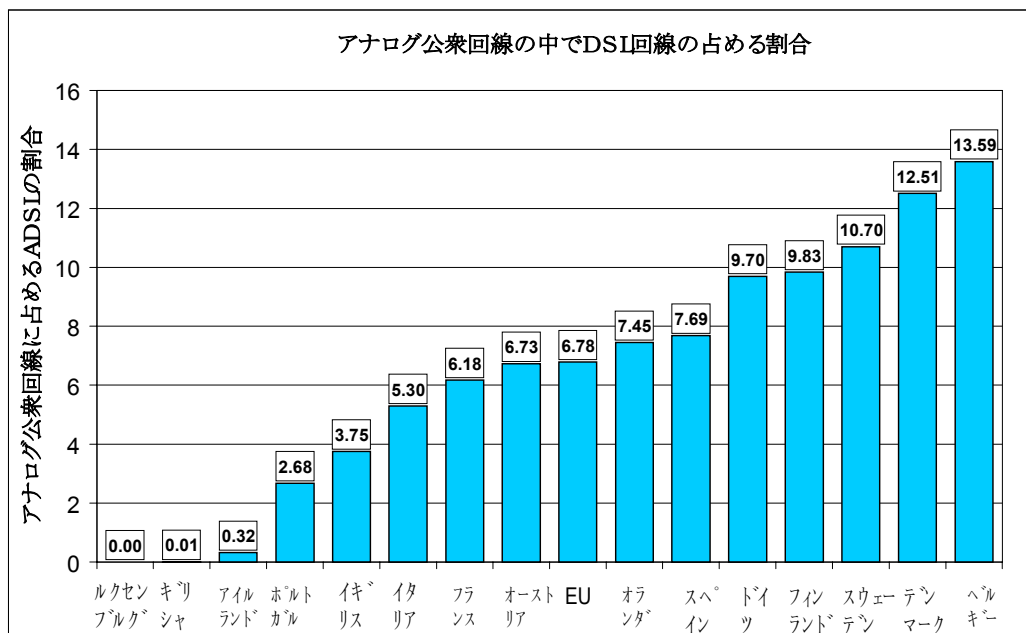


次の図は、国別に国民一人当りのブロードバンド普及率を示している。



最後に以下の図は、DSL回線を提供しているPSTN回線（アナログ公衆回線）の割合を示している。





欧州におけるブロードバンド普及の成功を分析するにあたっては、EU 全体での先駆的な試み（例えば、e ヨーロッパ）や国家レベルでの政策（例えば、スペインの Plan Info XXI）も含めた多くの要因を考慮すべきである。しかし、ここでは、ブロードバンドを成功裏に普及させるためのインフラストラクチャでの競争の有益さをもっとも良く示す範例として、ベルギーの事例に焦点を当てる。

## ベルギーにおけるブロードバンドの成功要因

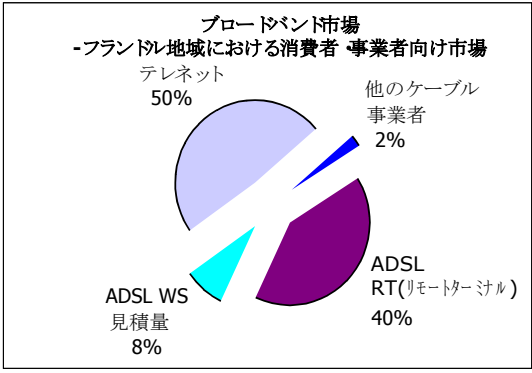
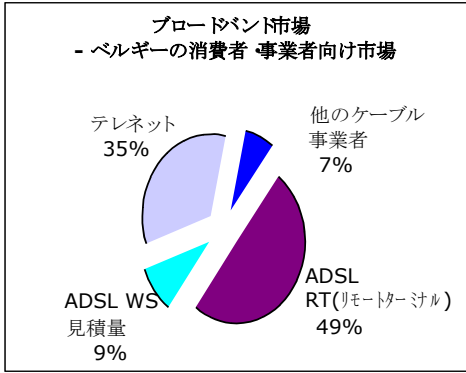
ベルギーはブロードバンドビジネスにおける成功を謳歌しており、以下の要因がこの事例を説明できる。

### インフラストラクチャにおける多様性と競争

- ベルギーでのケーブルの普及率は、欧州で最も高いレベルにあり、全世帯の98%に普及している。DSLに関しては、インフラストラクチャは、全世帯の約98%をカバーしている。この結果、消費者はブロードバンドケーブルサービスとベルガコム (Belgacom) あるいはベルガコムのインフラを利用している他のキャリアが提供するDSLの両方にアクセスできる<sup>3</sup>。この2つのインフラと技術が競争していることがベルギーにおけるこれまでの成功物語を説明することができるので、この要因がベルギーにおけるブロードバンド普及の鍵である。
- ベルギーにおけるブロードバンド市場は、100万契約を超えており、これは実際、世帯あたりの実際の利用者としては、非常に高い普及率となっている。
- 消費者向けおよび事業者向けの市場セグメント (CBS) に関する以下の統計が示すように、ケーブルとDSLはベルギーでは競合関係にある。フランドル地域では、ブロードバンド市場をケーブル技術がリードしており、テレネット (Telenet)、ベルギーにおけるケーブル大手は、このマーケットの50%を押さえている。

---

<sup>3</sup> ケーブル分野とは逆に、DSL技術はベルギーでは完全に規制されている。その規制下でベルガコムが規制されたビットアクセス(BROBA)の参照価格を地域レベル(BROBA I)とATMスイッチレベル(data connectivity-BROBA II)で開示している。これによって、他の事業者はベルガコムが敷設した既存のネットワークインフラを用いながら独自のDSLサービスを末端消費者向けに開発、販売できる。



## 商品のデザイン

- ベルギーにおける成功事例を説明するもう一つの重要な要因は、（下り回線）が非常に高速という特徴を持ったブロードバンド商品のデザインに関連している。ケーブルサービスは、最高で4メガ（Mbps）の速度を提供している。ベルガコムは、消費者向けに**3メガ**（下り）のDSLサービスを提供しており、これはADSLの個人向け基本サービスにすでに含まれている<sup>4</sup>。
- このような3メガのサービスは、“ベスト・エフォート型”契約で全人口の84%をカバーしており、“常時接続”型の契約でも60%をカバーしている。
- ベルガコムは、この比率を徐々に増やすべく新しいネットワークインフラに投資し続けている。

## 価格

- ベルギーにおける広範囲かつ急速なブロードバンドの展開の第三の鍵は、ブロードバンドサービスが非常に低価格である点に見出される。例えば、ベルガコムのADSLの基本的なサービスは、末端消費者レベル30ユーロ（付加価値税込み）であり、この非常に低価格がベルギーの特徴である。
- また、ベルギーのADSLサービスは、品質対価格比でみると欧州において最も高くなっていることも要因の一つとして掲げるべきである。

## 政府の政策

- 学校と図書館におけるインターネットアクセスを推進してきたこと（I-Line project）
- “e-inclusion”プログラムを定義したこと（新しい政府協定）
- PCの普及率を高めるために“PC privé context”を推進すること
- 電子政府サービス：
  - 個人ならびに事業者による税金の電子申告
  - 2007年までにすべてのベルギー国民のためのE-IDカードを実現すること
  - インターネットを使った個人の公的記録への安全なアクセス
- 遠隔ならびに在宅勤務を推進するために：
  - 行政によるPCならびにインターネット回線への投資
  - 遠隔勤務者にとってより魅力的で適切な法的枠組みを分析し定義すること。

---

<sup>4</sup> ADSL GOサービス：ダウンロード速度は3メガ（Mbps）。

## この成功事例をさらに発展させるための要因

- 規制の状況

上述のように、ベルギーでは、ケーブルとDSLの両方の普及率が欧州において第一位であり、これはこの2つのインフラの激しい競争の結果に起因する。

しかし、ベルギーにおける現在の規制の状況は、ケーブル分野をあらかじめ規制下におくべきではないことを示唆している。

このような状況は重要である。電気通信ネットワークとそのサービスの規制における技術的中立性の原則および現在のケーブルとDSLサービスの競争をさらに推進することを鑑みれば、2つの技術は同一の規制の下に置かれるべきであるという結論に辿り着く。

- 公共政策：

ベルギーでは、PCの普及率があまりにも低すぎる。政府は端末の普及率を上げるために必要とされるすべての手段を講じるべきであり、その結果として情報社会へのアクセスを可能とすべきである。PCは、情報社会へのアクセスのための解決策の一つであるが、他のタイプの端末も考慮されてもよい。

この戦略の成功を保証するには、実業界との更なる協働が必要であろう。公的な権威や機関とのさらなる協働も一貫性があり効率の良いコミュニケーションのために必要となるだろう。

## カナダにおけるブロードバンドアクセス

カナダのブロードバンド普及は、OECD諸国の中で比較すると、韓国について二番目に高い。カナダ人のおよそ60%がオフィスあるいは家庭で日常的にインターネットを利用しており、60%の家庭がインターネットアクセスを持っている。これにより、カナダ人は世界的に見てインターネットに接続された最も大きな利用者となっている。これらインターネットを利用する世帯のおよそ半数（3500万人強、総世帯数の30%に相当）が、ケーブルモデムあるいはDSLブロードバンドアクセスサービスに契約している。2003年末までには、この数字は総世帯数の35%にまで上がり、さらに2005年までには50%を超える<sup>5</sup>と期待されている。人口1000人当りで見ると、カナダのブロードバンドアクセスの普及率は、アメリカ合衆国のほぼ2倍の水準で推移してきているが、アメリカ合衆国は、最近このギャップを埋め始めている。

カナダにおけるブロードバンドアクセスサービスの急速な展開の主たる要因はケーブルとDSLブロードバンドネットワークの競争であり、その結果としてもたらされた積極的な販売促進活動と価格戦略である。

カナダのケーブルテレビのインフラストラクチャは、電話のネットワークとは独立に発展し、93%以上の家庭に繋がったものである。新しい市場機会を早い段階に認めたカナダのケーブル事業者は、1996年にブロードバンドのインターネット接続サービスを開始した。これは世界で最も早い。

カナダの電話事業者も、DSL技術を使った高速商用インターネット接続サービスを1996年に開始した。これもOECD諸国では最初である。DSLサービスを提供するためのネットワークの設備更新が都市部で進むにつれて、2000年には、電話事業者はケーブルテレビのブロードバンド利用者とダイアルアップを利用している自社の顧客の両方を狙った積極的な販売促進活動と価格戦略で、ケーブルテレビの初期のリードに挑戦し始めた。2000年の終わりには、DSL利用者はほぼ50万人増加し、この数字は2001年には2倍以上となった。

電話事業者とケーブルテレビ事業者の、個人利用を狙った激しい競争は、ブロードバンドサービスへの需要を喚起し続けた。2003年には始めて、ブロードバンド接続の世帯数がダイアルアップ接続の世帯数を上回った。更に、ブロードバ

---

<sup>5</sup> IDCカナダ、2003年から2007年までのカナダにおけるインターネット接続とブロードバンド市場に関する予測（2003年5月付）

ンド接続の世帯の中でも、DSL利用者がケーブルモデム利用を上回った。

この顧客獲得競争によって、価格は低水準にとどまっている。DSLもケーブルモデムも、個人向けサービスの価格はサービス開始以来月額ほぼ40カナダドル（30米ドル）でおおよそ安定している。近年になって、電話事業者もケーブル事業者も接続スピード別の新しい価格プランを導入したことにより、一部の利用者にとっては若干の価格の高騰が見られる。しかし、低価格のサービスが提供されつつあることと、インターネット接続サービスと他のサービスを抱き合わせたサービスの登場を考えると、目に見えた高騰の可能性は低い。

電話事業者もケーブル事業者も第三者に対してブロードバンドアクセスサービスを提供することが義務付けられている。しかし、末端価格の低さを反映して、事業者間取引はあまり発展してきておらず、既存のケーブル、電話事業者が国内のどの地域においても主要な供給者のままである。

固定無線、衛星を含めた第三の技術は国内全域で提供されているが、主に人口密度が非常に低い地域でのみ利用され、全体としては大きな影響をおよぼしていない。いくつかの無線（Wi-Fi）技術の試行的プロジェクトが進行中である。モントリオール・トロント間を結ぶ旅客列車の中で無線ブロードバンドアクセスを提供する準備もこの一つである。また、政府は最近インターネット接続といった用途向けにさらに電波周波数帯を割り当てる計画を発表した。

従業員100人未満の小規模事業者向けのブロードバンドサービスは、全般的に、家庭向け市場と同じパターンを辿ってきている。2002年には半数以上が高速インターネット接続技術を利用し、DSLアクセスの方がケーブルよりも人気がある。小規模事業者向けの価格競争もまた厳しく、最近の値下げにより、アクセススピードと付帯サービスによって価格は変動するが、月額60～90カナダドル（42～65米ドル）になっている。より大規模な事業向けには、ブロードバンドアクセスは、一般に専用線、フレームリレー、ATM、VPNといった技術を用いてインターネット接続と企業のその他のデータ通信ニーズを統合した形で提供され、比較可能な統計は入手できない。

カナダにおけるブロードバンドの成長の主な要因が競争であることは確かであるが、他に重要な要因もある。特に、政府は早い段階から社会経済的発展にとってインターネット接続とブロードバンドが重要であることを理解していた。1998年から一連の先導的な試みが、産業省（Minister of Industry）の“Connecting

Canadians”という行動計画のもとにスタートした。この行動計画は、電子商取引にとって親和的な政策環境を確保することを目指した。中でも、技術中立的な課税枠組み、電子的な記録に対する電子署名のための法的枠組みの創設、個人情報保護、オンライン取引において消費者保護をするための業界自主規制ガイドライン整備の促進などがある。また、野心的な電子政府計画を策定し、その結果、過去数年間カナダは、行政サービスのオンライン化の程度を比較する国際的な調査において高い位置を占めつつけている。

カナダ人は、新しいコミュニケーション技術の利用においても特に受容性が高いようにみえる。たとえば歴史的にみて、ATM、テレホン・バンキング、デビットカード等の新しいサービスに適応するカナダ人は、アメリカ合衆国と比べて早く、2001年には、38%の個人が税金の電子申告を行った。また、オンラインゲーム、音楽のダウンロード、教育・訓練、在宅勤務といった広帯域を必要とするインターネットサービスの利用についても、カナダには世界で最も多くの利用者がいる<sup>6</sup>。

カナダの広大な地域とそれと比較して少ない三千二百万人の人口のために、都市部の外に住む20%のカナダ人にもブロードバンドサービスを提供することが大きな挑戦である。すべての公立学校と図書館を2000年までにインターネットに接続するという初期の目標を世界で最初に達成した後、政府は民間と協働して2005年までにすべてのコミュニティがブロードバンドアクセスをもてるようにしようとしている。この“Smart Communities”と名づけられた先導的な試みは、コミュニティ“チャンピオン”のリードのもと一定の資格を満たすコミュニティに公衆ブロードバンドアクセスを展開するための資金援助であり、民間企業に競争させながら行う。これに加えて、ブロードバンド普及を加速するための先導的な試みがすべての行政のレベルで増加してきている。これらは例えば、行政機関のための請負契約、コミュニティレベルでのプロジェクトのための頭金の確保、インフラストラクチャのプロジェクトのための資本提供、機器製造業者の研究開発のための優遇税制、ブロードバンドアクセスへの需要喚起のためのオンラインコンテンツ開発支援などである。

---

<sup>6</sup> Veenhof, Neogi and van Tol, *高速な情報ハイウェイ：カナダのブロードバンド* カナダ統計調査, 2003年9月（2003年4月のITUワークショップ「ブロードバンドの普及促進：カナダ事例」を引用）

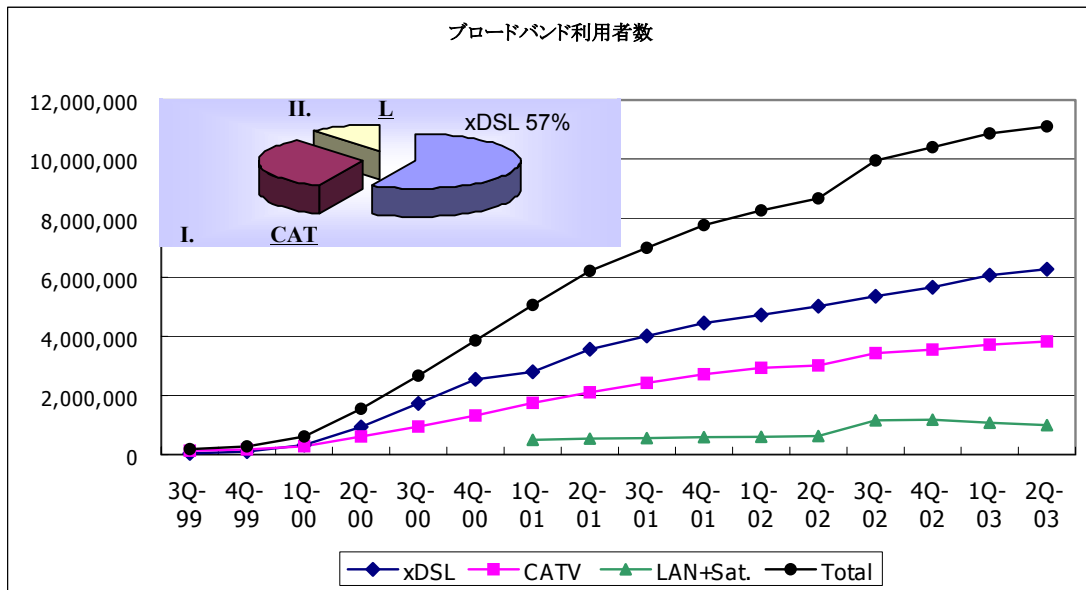


## 韓国におけるブロードバンドの現状

### 1. 韓国におけるブロードバンド：概要

世帯普及率で72%を超え、ブロードバンドアクセスで世界一となった韓国にとってブロードバンドは、新しいタイプのライフラインコミュニケーションサービスとなった。小学校から大学までの98%以上がブロードバンドインターネットに接続され、情報技術を用いたオンライン教育を行っている。インターネットを流れるパケットのほぼ50%は、特に主婦、ホワイトカラー、学生といった女性によるものである。また、株式売買の70%以上と銀行取引の14%は、今日、インターネットを経由しており、特に女性による積極的な参加が見られる。コンテンツについて見ると、インターネット利用者の74%がAV (Audio/visual) インターネット放送を視聴し、30%以上がインターネットゲームや音楽ダウンロードを利用している。さらに、25000以上のインターネットカフェが国内に広がっている。

また、無線LANや2.3ギガヘルツの周波数帯域を利用した携帯インターネットといった無線インターネットに対する需要についてもかなり良いトレンドがある。これらのことを総合すると、韓国はすでに「いつでも、どこでも、どのような端末からも」コミュニケーション可能というステージに入ったことは明白である。



## 2. 2003年6月時点での普及率

ブロードバンドサービスの初期段階ではケーブルモデルが採用されたの対して、ADSLは1999年の第三四半期から韓国のブロードバンド市場に広がっていった。1999年では、CATVとADSLの普及率は、それぞれ0.97%と0.3%に過ぎなかったが、ADSLが“テイク・オフ”して以降、韓国のブロードバンド市場は、一年以内にADSL契約者が百万人を突破し、2001年の第一四半期には200万人を超えた。2003年6月時点では、1100万人を越える契約者がブロードバンドインターネット接続を利用しており、これは韓国総世帯数の72%にも上る。

韓国は今ブロードバンドサービス展開の第一フェーズを終え、VDSLと固定・無線の統合サービスの第二フェーズへと移行しようとしている。VDSLは2002年11月に商用化されて以降、日に日に人気を集めている。

グラフに示されている通り、LAN（光ファイバーを使ったイーサネット）によるブロードバンドサービスが増加していることは、注目に値する。

## 3. 価格と競争の諸側面

韓国では、ブロードバンドサービスの価格は広範囲にわたっている。最も人気のあるサービスは、4万ウォンであり、これに1万ウォンを追加すると無線LANサービスを受けられる。

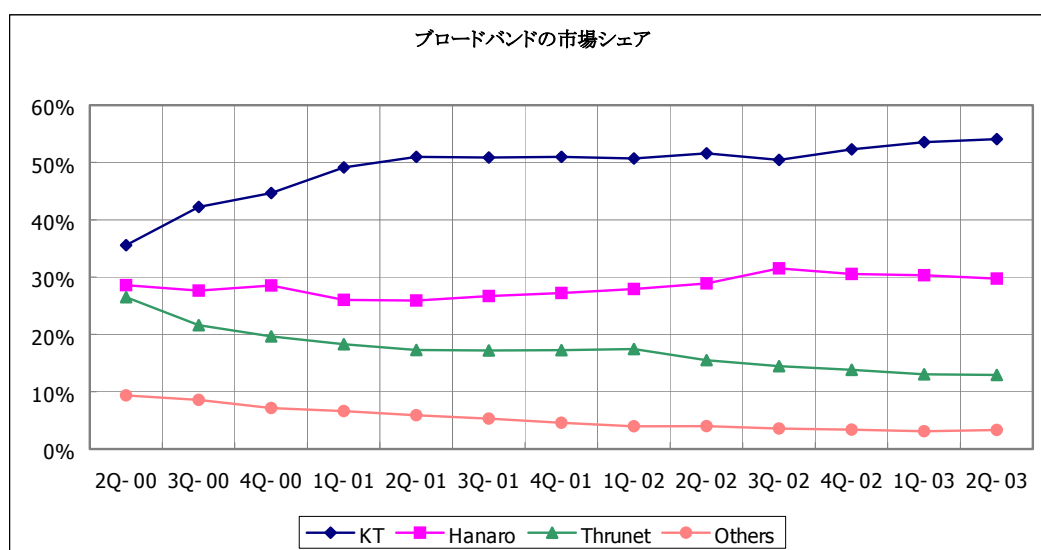
2002年時点では、中小企業向けの複数端末接続可能なADSL接続の契約者数は11万であり、この契約では1本のADSL回線に最高16台のコンピュータを接続することができ、価格は4万ウォンから25万6千ウォンである。

韓国におけるブロードバンド接続サービスの急速な発展の主な要因は、キャリア間の競争、高い人口密度、市場が生み出す需要、そして情報化社会へ向けた政府の支援プロジェクトである。これらの要因が、積極的な販促活動と競争を生み出した。

韓国では、コリアテレコム（KT）、Hanaro Telecom、そして、ThruNetの三社が主要なブロードバンドサービス提供者であり、互いに激しく競争している。KTは、1999年の第三四半期からADSLサービスを提供し始めたが、全国のブロードバンド利用者の49%に相当する500万を超える契約者を抱え、世界的に見ても主要な地位を占めるインターネット接続サービス提供者である。

Hanaro Telecom は、積極的な販促活動と価格戦略により、K Tに続く 27%のシェアを確保している。

今日では、ネットワーク接続サービス市場はすでに成熟段階にあり、サービス提供者の収入の伸びは鈍化している。



#### 4. 国家の政策的環境—戦略

韓国政府は、21世紀の新しいビジョンとしてK I I（韓国情報基盤）を打ち立てることに成功した。ブロードバンドインターネット基盤は、グローバルな先駆的取り組みとしての「e-Korea イニシアティブ」の実行によって整備された。

競争を促進する政策については、政府はI S P（インターネット接続事業者）の大幅な規制緩和によって競争を促進しオープンアクセスネットワークを確立した。

さらに、韓国政府は消費者の住宅までの回線を更新することを促進することによって、ブロードバンドサービスを提供可能とする利用者側の環境整備のための多大な努力を行った。典型的な政策の一つは、住宅内のコミュニケーション品質に正式の証明書を発行するというものであり、世帯に大きな影響を与えた。ブロードバンドサービスの第二フェーズを成功させるために、韓国政府は産業界と協力して様々な政策と規制手段を準備しつつある。これは、固定・携帯統合と放送通信融合を含む次世代のブロードバンドサービスをターゲットとしたものである。

## アメリカ合衆国におけるブロードバンドの状況

### 1. 概要：合衆国におけるブロードバンド

米国においては、ブロードバンドの普及は、CATVインフラを用いるケーブルモデムと優先電話のインフラを用いるDSLという2つの有線技術にほとんど依存している。合衆国におけるブロードバンドの普及は、経済的に競合関係にある多くの諸国と比べて、決して早くない（たとえば、韓国やカナダ）。原因のいくつかを列挙すると、人口学的、地勢的なハンディ（DSLが届く範囲に居住する人口の割合の低さ）や、利用回数や利用時間によらない固定料金制を採用している地域電話会社の料金制が、ダイアルアップ接続を相対的に安価にしている事、DSLと比較してケーブルモデムに有利に働く規制、ブロードバンド普及を促進する政府の計画やインセンティブの不在などが挙げられる。産業化の進んだ30ヶ国から成るOECDメンバー諸国と比較すると、合衆国のブロードバンド普及率は第六位（6.9%）であり、韓国（21.4%）、カナダ（11.4%）、ベルギー（8.5%）、デンマーク（8.3%）、そしてスウェーデン（8.1%）に比べて遅れている。

### 2. 2002年12月時点での普及率

合衆国連邦通信委員会（FCC）によれば、2002年12月時点で、ブロードバンド契約者数は19,823,684人であった。これは全人口の6.9%を占め、その内650万人がDSLを利用し、1130万人がケーブルモデムを、そして、190万がFTTHや無線などを利用している。ブロードバンドの普及率は過去2年間に劇的に増加し、より多くの電話回線がDSLサービスを提供できるように設備更新され、消費者にとってブロードバンドサービスが魅力的となるような価格で提供されるようになった。以下は、OECD諸国と米国の普及率の比較表である。

OECD加盟国（一部）におけるブロードバンド利用者数

2002年12月	DSL 利用者	ケーブル利用者	他の利用者	利用者合計	利用者割合
韓国	6,386,646	3,701,708	39,959	10,128,313	21.4
カナダ	1,642,554	2,008,566	-	3,651,120	11.7
ベルギー	517,000	326,181	25,813	868,994	8.5
デンマーク	307,055	133,003	5,784	455,842	8.3
スウェーデン	424,000	153,700	142,500	720,200	8.1
<b>アメリカ合衆国</b>	<b>6,595,532</b>	<b>11,300,000</b>	<b>1,928,152</b>	<b>19,823,684</b>	<b>6.9</b>
スイス	195,220	260,000	-	455,220	6.3
日本	5,645,728	1,954,000	206,189	7,805,917	6.1
ドイツ	3,195,000	56,845	70,000	3,321,845	4.0

イギリス	590,000	779,319	2,000	1,371,319	2.3
OECD	30,058,261	23,075,208	2,625,176	55,758,645	4.9

### 3. 価格と競争の局面

様々な基盤同士の競争によって、価格の低下圧力と様々なサービスの抱き合わせが生じている。1990年代の後半には、CATV業者はケーブルモデムサービスを提供できるようにネットワーク設備を更新し、CATV、インターネット、そして(場合によっては)地域電話サービスを一まとめにしたサービスを提供し始めた。既存の地域電話会社は、高コスト、低いリターン、そして競争相手にネットワークを開放する義務を課せられる脅威などを理由として、DSL市場への投資は活発ではなかった。最近になって、主要なILEC (incumbent local exchange carrier ; 地域レベルでの交換機を持っている既存電話会社) は、顧客のおよそ80%に対してDSLを提供できるようになったかもしくは、そうする計画を発表している。また幾つかのILECはこの普及率を挙げるために「リモートターミナル設備」や、FTTHプロジェクトへの投資を行う計画を発表している。ILECは、ケーブルモデルに対抗して、DSL、地域電話サービス、そして(場合によっては)携帯電話を抱き合わせたサービスを提供している。いくつかのILECは、衛星TV放送事業者との提携によりDSLを使ったビデオサービス、有線、無線を統合したサービスを提供する計画を持っている。多くの単品のDSLあるいはケーブルモデムサービスは、月額30ないし40ドルの価格帯にあり、より高速のあるいは同期を取るサービスについてはより高い価格が設定されている。

### 4. 国家的政策環境—戦略

ブロードバンド普及のための統合的な国家政策は米国にはない。今日まで、政府の活動のほとんどは、2つのブロードバンド基盤の間の規制上の平衡を保つために様々な(規制上の)義務をはずすことに注力してきた。FCCは、ILECがそのネットワークを第三者に開放しなければならないという義務を課しているが、光回線とブロードバンドネットワークに関してはこの義務を解除しようと試みており、いっぽうでは、ケーブルモデム提供者については、ネットワークの解放義務も提携関係のないインターネット接続事業者に対して強制的にアクセスを提供する義務もないという現状を維持しようとしている。しかし、過去の政府が電話と電気に関して持っていた計画と同様のマクロ経済的な観点からのブロードバンド普及を国民全体に及ぼす戦略はない。



Global Business Dialogue on Electronic Commerce

# インターネットの未来 WG サイバー・セキュリティ

2003年11月6日

ラポータ： 東京電力株式会社

代表取締役会長

田村 滋美

## サイバーセキュリティ

### 1. 「セキュリティ文化」の実践

情報システム及びネットワークの利用と情報技術を取り巻く環境の劇的な変化、ネットワークや情報システムの相互接続の増加によって、セキュリティに関する新しい課題が浮上してきた。OECDのセキュリティガイドラインは、「セキュリティ文化」の発展を促進することでこのような状況に対応し、情報システムやネットワーク全体のセキュリティの向上を目指すものである。

GBDeは、この「セキュリティ文化」の考え方を支持し、企業の視点でサイバーセキュリティに関する議論を昨年から続けてきた。2002年10月のブラッセル総会においては、5項目の提言を公表し、セキュリティ文化の実施について、OECDやAPEC、関係各国政府関係者と議論を続けてきた。

一般に、GBDeはセキュリティ文化の実現にあたって、企業が果たすべき役割は、「企業のセキュリティ」と「社会全体でのセキュリティ」の2つの側面において、十分な施策を施すことだと理解している。GBDeは電子商取引、特にネットワーク上の商品やサービス市場に焦点を当てている。B2C電子商取引が発展するにつれて、市場は重要インフラとしての機能を持つようになり、セキュリティ障害は大きな打撃になる可能性も出てくる。そのため、「企業のセキュリティ」の範囲は企業内だけではなく消費者や取引の関係者にまで及ぶのである。また、企業自らの責任を認識し、役割を果たすだけでなく、個人ユーザレベルでのセキュリティの実践についても、企業が果たすべき役割は非常に大きいと考えられる。

#### (1) 企業のセキュリティ

ブラッセル提言でも述べたとおり、企業にとって情報とネットワーク資産は金融資産と同様に重要なものである。企業は顧客にコンタクトし、サービスや商品を提供する手段として、情報システムに依存している。また、企業のシステムやネットワークに損害が起きれば、企業自身のコストが増大し損害をもたらすだけでなく、一般のネットワークユーザや市民社会の日常生活に多大な損害をもたらしてしまう。企業としては、情報システムやネットワークに関する脅威や脆弱性に適切に対応することによって自らの資産を守ると同時に、自らの設備を安全に保つことによって社会全体のサイバーセキュリティを確保すべきである。

GBDeは、企業内のセキュリティを十分なものとするためには、次の4つのレベルで、それぞれ必要な対策を講じることが重要だと考える。

**a. エグゼクティブ**

2002年提言にも述べたとおり、CEOをはじめとする企業の上級経営者は、情報とネットワーク資産を企業にとって重要なものと認識し、情報セキュリティに関する責任を持つことが重要である。そのために、セキュリティポリシーを制定し有効に運用することによる首尾一貫した対応が必要である。

**b. ネットワーク管理者**

企業は、サービスや情報システム機器の提供者としてだけでなく、情報システムやネットワークを所有・運用する者としてOECDガイドラインの「セキュリティの設計・実装」の原則を重視し、実施しなければならない。ネットワーク管理者は、エグゼクティブの正当な指揮の下、この役割を果たすことが求められる。

**c. 社内ユーザ**

一般ユーザは、企業が定めたセキュリティポリシーやガイドラインに従って正しく社内ネットワークを利用すべきであり、不正利用をしてはならない。

**d. 社外ユーザ**

GBDe は既に、トラストマークや電子署名、有害コンテンツ対策、インターネット支払い等の消費者信頼に関する提言を行ってきた。ここでは、B2C市場における消費者と企業の責任分担について取り上げる。(次章で述べるように、個人も情報社会の参加者としてサイバーセキュリティを確保する役割を持っている。)

インターネットプロバイダやB2C市場における商品・サービス提供者は、個人のインターネットユーザと様々な関係を持っている。例えば、ベンダーは、インターネット上の消費者に商品を販売するに多くのネットワークシステムを運営し、注文・支払などのプロセスを処理している。このような関係は、一般的に契約書やオンライン契約などにより定義されている。情報システムとネットワークを守るための個人と企業の責任のバランスは場合により違ってくる。企業は、電子商取引のセキュリティを確保するためには、顧客だけではなくインターネットサーフィンをしているユーザも企業のセキュリティの範囲として考慮する必要がある。その際に企業が注意すべきポイントは以下の通りである。

- 個人ユーザとの関係を再検討。(企業に近いユーザと一時的なユーザを区別)
- サイバーセキュリティに関する企業とユーザの関係の定義、公表された契約事項による相互責任の提示。



- サイバー攻撃に対する定期的な状況報告と情報更新。
- 個人ユーザに関わるセキュリティ脅威への対策。
- 企業のヘルプラインやコールセンターにおけるセキュリティの認識。(オンライン取引の失敗・中断はセキュリティ障害の前兆の可能性はある)
- セキュリティ対策の広い周知。

それぞれの企業がこの4つの段階において十分な対策を施すことにより、ネットワーク社会におけるセキュリティのレベルが全体として向上するのである。GBDe は、OECD、APEC などのフォーラムでの議論を通じて、官民協力や情報共有の実施などを検討し、関連するフォーラムやワークショップのパネラーとして GBDe 提言の普及につとめてきた。このようなアドボカシーを通じて、GBDe はセキュリティの重要性認識向上に貢献してきたのである。

## (2) 社会全体でのセキュリティ

サイバーセキュリティは、IT の世界だけでなく、経済社会システム全体の中で考慮されるべきである。情報化社会は、電子商取引による経済発展・雇用拡大と電子政府による医療・教育など公共的サービス提供の二つの推進力によって実現される。サイバーセキュリティの確保はそのいずれにとっても必要不可欠な要素である。

### a. 社会全体として適切なレベルのセキュリティの必要

今後情報化社会がグローバルに拡大し、プラスの社会的インパクトを一層もたらすためには、電子商取引や電子政府のメリットを安全に享受できるような適切なレベルでのサイバーセキュリティが世界的に確保されていることが必要である。このような「適切なレベルのセキュリティ」をグローバルに実現するためには、セキュリティの必要性をネットワーク社会の市民・企業・政府が等しく認識し、そのために必要な対価をそれぞれで分担すべきである。一部の企業は既に十分なセキュリティの確保された情報システムとネットワークを構築してきたが、依然として適切なレベルのセキュリティが確保されていない企業も数多く存在する。もし企業や個人がそれぞれの立場のみを考え利便性やコスト削減を追求すれば、セキュリティに対する投資は抑制され、ネットワークや情報システムのセキュリティレベルはそれに伴って低下するだろう。

低いセキュリティレベルのネットワークにおいては、外部からの攻撃や内部の不正利用による損害が容易に生じ、被害は他のネットワークユーザに容易に波及する。このような「安全ではない」ネットワークや情報システムの下では、ネッ

トワーク利用者は電子商取引や電子政府実現によるメリットを得ることができない。企業や政府がセキュリティの投資を抑制することは、自らのネットワークや情報システムを危機にさらすだけでなく、ネットワーク社会の市民に予想もしないダメージを与える結果となりかねないのである。

#### **b. 投資に見合ったセキュリティ**

OECD ガイドラインに述べられているように、企業は、社会全体でのサイバーセキュリティ実現にあたって、他の関係者と同様、その役割に応じた責任を負う。一般に競争的な市場においては、企業は、それぞれの判断でどのレベルのセキュリティを求めるかを決め、各自の投資に応じた分だけセキュリティのメリットを享受すべきである。企業は自らの希望によって、従来のオープンネットワーク環境下でこれまでと同じレベルのセキュリティの中に留まることもできるが、さらに多くの投資をすることによって従来よりも安全なネットワーク環境下で電子商取引や電子政府導入によるメリットをより安全に享受する権利を持つ。これは企業だけでなく、個人ユーザにもいえることである。

ユーザは相当するコストを支払うことによって自分の求めるセキュリティレベルのサービスや機器の提供を受けることができる一方、サービス提供者はクライアントの求めるセキュリティレベルに応じて、幅広くセキュリティ関連機器、ソフトウェア、アクセスなどのサービスを提供すべきである。サービス提供者としての企業は、自分の提供する機器やサービスのセキュリティレベルについて適切に情報を開示し、ユーザがどのようなセキュリティレベルにあるか十分に認識できるようにサポートすべきである。

ユーザは、自らの支払ったコストに見合っただけのセキュリティのメリットを得ていることを明確に認知し、さらに高度なセキュリティを求めるのであれば、追加してサービスの対価を支払うか、さらに高価で安全な機器を購入して利用することもできる。もし、ユーザが非常に高度なセキュリティを要求するのであれば、企業は、そのユーザを他のユーザから切り離し、より高度なセキュリティのサービスを提供することも考えられる。例えば、市民社会の生活に関わる重要インフラを提供する企業は、重要インフラであるネットワークや情報システムをオープンシステムとは切り離して管理・運営することにより、さらに高度なセキュリティを提供することができる。

#### **c. 個人ユーザの役割と企業**

政府や企業だけでなく、個人ユーザがサイバーセキュリティに果たす役割は非常に重要である。既に述べたように、電子商取引の市場で個人ユーザは顧客あるいは加入者として企業のセキュリティにも密接な関連がある。GBDe は、ベスト

プラクティスを含む、企業の活動が、個人レベルでのセキュリティの責任にも貢献していると考える。

個人ユーザは、サービス提供や機器購入に際して、提供者側と締結する契約を締結することが求められ、この契約上の義務によってネットワーク社会参加者としての個人ユーザの責任が定義される。企業は、その定義付けを確実にかつ明確にするための重要な役割を担っている。

GBDe は契約や約款がネットワーク社会における個人ユーザの責任を規定することにより適切なレベルのセキュリティが効率的に実現されると考える。サービス提供者と個人ユーザの責任がはっきり分割されることにより、個人ユーザにとっても望ましいネットワーク社会が実現するのである。

#### d. セキュリティの標準化

2002 年のブラッセル提言にも述べている通り、GBDe はこれまでもセキュリティの標準化に関する様々な議論を実施してきた。GBDe は、いかなる特定の管理・認証の方法を推薦・支持することはなく、管理・認証に関するセキュリティ標準がグローバルなベースで政府、民間の活動によって採用され、運用されることを提言してきた。

上記のような問題に照らして考えると、「適切なセキュリティレベル」は、国際的に互換性のある標準によって明確にされるべきであり、同時に、標準化の議論を通じて国際的に普及していくことが期待される。これからも GBDe は標準化団体等との議論を通じて、客観性のあるグローバル標準が情報化社会における「適切なレベルのセキュリティ」を実現するよう、支援していく。

#### 提言

GBDe は、ネットワーク社会におけるこのような企業の重要な役割を十分に認識した上で、新たに次の項目を提言する。

- GBDe は、政府が、重要インフラ保護し電子政府などの公共サービスを安全に提供することを提言する。各国政府が公表するサイバーセキュリティ政策は、このような政府の責任を明確に認識したものであるべきである。
- 企業の視点からは、セキュリティ確保の実現に当たっては経営層のリーダーシップが不可欠である。GBDe は、ICC/BIAC の「経営層のための情報セキュリティ確保」を支持し、今後も ICC/BIAC をはじめとした団体と対話を続けていく。
- GBDe は、企業によるセキュリティに関する情報共有は upstream と downstream の両方でなされるべきであることを提言する。「Upstream 情

報共有」は、攻撃やサービス妨害（DoS）等ネットワーク上の重要なインシデント情報を CERT 等の機関で共有し、今後の被害拡大にそなえるものである。その際には、サイバー攻撃の被害者の身元情報が漏れないよう政府機関や情報センター等の機関を通して「匿名性」が確保されるよう考慮すべきである。一方「downstream 情報共有」は、企業が自らのセキュリティ関連の機器、ソフトウェア、アクセスなどのサービスをユーザに提供するにあたって、それぞれがどのようなセキュリティレベルにあるのか、脅威や脆弱性にはどのように対応するのか等の必要な情報を提供することである。

- GBDe は、世界中すべての地域において、情報化社会の市民が電子商取引や電子政府によるメリットを享受できるように、「適切なレベルのセキュリティ」が保たれるべきであることを提言する。GBDe は国際機関や各国政府、民間団体や市民社会との対話を通じて、グローバルに実現すべき「適切なレベルのセキュリティ」の内容を明確にするように努力する。
- GBDe は、企業がセキュリティ文化に関する個人ユーザの責任を明確化することにより、ネットワーク社会のセキュリティレベルが向上すると考える。また企業がハードウェアやサービスを提供する際には、ユーザの投資に応じて適切なセキュリティレベルを提供すること、またユーザの義務と責任について明確な記述をすることが求められる。GBDe はこのような企業の取組みがセキュリティ文化の一部である個人ユーザの責任の履行を担保することを提言する。



Global Business Dialogue on Electronic Commerce

# インターネットの未来 WG RFID

2003 年 11 月 6 日

ラポーター :                   NTT DATA  
(アジア/オセアニア)       代表取締役副社長  
                                          中村 直司

## インターネットの未来

### R F I D

#### はじめに

R F I D (Radio Frequency Identification) 技術は、コンバージェンスとユビキタスネットワークという趨勢的变化において重要な要素であり、情報化社会に重要な意味合いをもっている。

R F I D技術は効率を高め、在庫管理を革新し、製品デザインとマーケティングを改善するポテンシャルを持っている。しかし、G B D eはこの技術がデータの収集、モニタリング、と保存に関してプライバシー問題を惹起しうることも認識している。

R F I Dが、事業者と消費者の両方にもたらす可能性のある影響を鑑み、G B D eは2004年にこの問題を取り上げるための作業計画の可能性を探っている。

#### R F I Dの概観

R F I Dとは、個別の物体を識別するために無線を使用するという技術の総称である。対象を識別するための最も普通の方法は、製品を識別するためのシリアル番号とその他の情報をアンテナに貼り付けられたマイクロチップに記憶させることである。このマイクロチップとアンテナを一体としてR F I DタグもしくはR F I D発信機と呼ぶ。R F I Dの読み取り機は、R F I Dタグが発信する電波をコンピューターが利用できる形へと変換する。

電子商取引の真の成功のためには、R F I Dの普及が前提として不可欠であると考えられる識者もいる。R F I Dの重要な要素の一つは、それが物理的な世界とヴァーチャルな世界を結びつけることができる点にある。物流ネットワークが電子商取引のネットワークと統合されて運用されるためには、サプライチェーンを動く製品と、製品管理システムとを直接結びつける必要がある。

産業界にとっては、R F I Dは製品の製造から小売、そして消費者による利用に至るまでの製品のライフサイクル全体をモニターできる潜在的な可能性を提供している。

消費者にとっては、R F I Dは製品の製造元や利用履歴を確認する機会を与え、品質保証の新しい次元となりうる。

## 将来の議論の範疇

GBDeは、RFID技術がもたらす可能性について、多くの利害関係者の議論を喚起することを支援すべきであるというのが現段階での見解である。すでに、個人情報保護、相互運用可能性の確保、標準化などの課題が重要であると認識されている。GBDeは、RFIDの採用をめぐる今後の対話において、以下の課題が取り上げられる必要があると考えている。

### a) 個人情報保護

RFIDの便益を認めつつ、産業界は個人情報保護とセキュリティにとってこの技術がどのような意味を持つかも考えるべきである。すでにRFIDを用いて個人を追跡したり、個人の購買パターンに関する情報を収集したり、個人の安全が脅かされる危険性を懸念する声がある。これらの懸念の幾つかは、消費者の側に情報のコントロールをもっと与えることと規制によるコントロールのバランスによって解消できるであろうという理解もすでにある。

GBDeはすでに個人情報保護について包括的なガイドラインを取りまとめている。RFIDの利用に関する提言の中に、このガイドラインを統合していく可能性もある。

### b) システムの信頼性

RFIDの将来の発展のための重要な要素として、システムの信頼性が挙げられる。もっとも差し迫った懸念は、RFIDタグからのデータが盗聴されることや、不正な改ざんを被る危険性である。

### c) 消費者への教育

消費者教育は、RFIDに関する今後の対話の中核を占める。RFID技術とその利用、および管理についての議論のために消費者が参加できるように、また、RFID利用がもたらす便益を理解できるように、正確な情報が提供されるべきである。

### d) 標準化

製品識別、タグとのデータ通信、製品とそのステータスを記述するための諸標準の調整と採用が必須である。これらの共通化された相互運用可能な標準がなければ、RFIDタグのコストが幅広い利用の妨げとなるであろう。



Global Business Dialogue on Electronic Commerce

## アドボカシーWG

2003年11月6日

議長： Carlton Fiorina  
(米州) Chairman & CEO  
Hewlett Packard

共同議長： 日本ユニシス  
(アジア/オセアニア) 代表取締役社長  
島田 精一

共同議長： Gina Nieri  
(ヨーロッパ/アフリカ) Executive Director  
Mediaset S.p.A.



## 1. 概要

- (1) 2003年度の活動は、ブリュッセル総会での合意に従い、ワーキング・グループとして策定した”Advocacy & Policy Cooperation Task Force” (February, 2003)を基にした Advocacy Work Plan によるものであり、公式または非公式に各国政府や業界団体への PR, 啓蒙活動を推進するものである。
- (2) アジア・オセアニア地区においては、特に ASEAN 各国を対象とした活動が中心であり、APEC TEL, APEC ECSG, AITS などの APEC 関連各会議への積極的な対応により推進されてきた。この結果、WG1 および WG2 の GBDe 日本シェルパ・メンバーと連携し、計26回(11カ国)のアドボカシ活動が実施された。

## 2. アドボカシ活動について

- (1) 対象組織、団体
  - OECD
  - APEC
  - Consumers International
  - GTA( Global Trustmark Alliance)
- (2) アドボカシ内容
  - Consumer Confidence (ADR, Trustmark, Privacy, iPayment)
  - Convergence ( Broadband )
  - Cyber Security
  - E-Government
  - IPR
  - Digital Bridges/WSIS
  - Taxation
  - Trade
- (3) 現在、各地域での GBDe アドボカシ活動をまとめ、GBDe Global Advocacy リストの作成を行っている(世界18カ国35回の活動を実施)。この内容は、2003年度 GBDe 総会にて報告をするとともに、今後の GBDe 活動広報に利用する。

### 3. 2003年度における今後の活動 (計画中)

第3回日台電子商取引委員会との GBDe 合同会議を企画、準備中。

日程：12月3日

場所：台北

対象：台湾政府関係者および台湾企業（經濟部国際貿易局に人選依頼中）

アジェンダ（案）：

- Trustmark/Privacy
- Cyber Security/Convergence
- RFID
- IPR

以 上

## GBDe Advocacy Activities 2003

	Event	Date	Venue	Group	Principal Issue/s	Representation
1	2002 Seoul International Seminar on e-Commerce	12-13/12/2002	Seoul, Korea	Korea Institute for Electronic Commerce	Consumer Protection, IPR, Cyber Security	Sherpa
2	METI (Ministry of Economy, Trade & Industry), Japan	19/12/2002	Tokyo, Japan	METI	Multiple Issues	Sherpa
3	<b>GBDe Sherpa Meeting</b>	<b>11/1/2003</b>	<b>Cairo, Egypt</b>	<b>Egyptian Govt, ABFICT</b>	<b>Multiple Issues</b>	<b>Sherpa</b>
4	Arab Business Forum for Information & Communication Technology	11/1/2003	Cairo, Egypt	ABFICT	Multiple Issues	BSC, Sherpa
5	OECD/APEC Global Forum, Policy Frameworks for the Digital Economy	14-17/1/2003	Honolulu, USA	OECD/APEC	Cyber Security	Sherpa
6	APEC ECSG 7th meeting	13-15/2/2003	Chiang Rai, Thailand	APEC ECSG	Privacy, Cyber Security	Sherpa
7	<b>GBDe Advocacy Meeting</b>	<b>19/3/2003</b>	<b>Washington DC, USA</b>	<b>US, Canadian, Japanese Govts, Consumers International, BBB</b>	<b>Multiple Issues</b>	<b>Sherpa</b>
8	OECD Meeting	7/3/2003	Tokyo, Japan	BIAC, OECD	Trade System Outlook	Sherpa
8	APEC TEL27 Meeting	22-29/3/2003	Kuala Lumpur, Malaysia	APEC TEL	Multiple Issues, Cyber Security	BSC, Sherpa
9	METI, Japan	24/4/2003	Tokyo, Japan	WG on Info Tech & e-Commerce	Multiple Issues, WTO	Sherpa
10	<b>GBDe Advocacy Meeting</b>	<b>19-20/5/2003</b>	<b>Brussels, Belgium</b>	<b>EC, WSIS Secretariat</b>	<b>Multiple Issues</b>	<b>Sherpa</b>
11	ETNO Dinner	19/5/2003	Brussels, Belgium	ETNO	Convergence	Sherpa

12	EU Meeting	20/5/2003	Brussels, Belgium	EU	Digital Signatures	Sherpa
13	European Internet Foundation	20/5/2003	Brussels, Belgium	EIF	WSIS	Sherpa
14	Council of Europe Meeting	21-22/5/2003	Strasbourg, France	Council of Europe	Privacy, Cyber Security	Sherpa
15	<b>GBDe Advocacy Meeting</b>	<b>2-3/6/2003</b>	<b>Kuala Lumpur, Malaysia</b>	<b>Malaysian Govt, ASEAN</b>	<b>IPR, Trade, Digital Divide</b>	<b>Sherpa</b>
16	METI, Japan	3/6/2003	Tokyo, Japan	WG on Info Tech & e-Commerce	Multiple Issues, WTO	Sherpa
17	<b>GBDe-GCD Meeting</b>	<b>5-6/6/2003</b>	<b>Madrid, Spain</b>	<b>Global Cities Dialogue</b>	<b>e-Government</b>	<b>BSC, Sherpa</b>
18	<b>GBDe Spam Workshop</b>	<b>17-18/6/2003</b>	<b>Ottawa, Canada</b>	<b>ILPF/GBDe/ Canadian Govt/US FTC</b>	<b>Unsolicited Electronic Communication - spam</b>	<b>Sherpa</b>
19	EC eGovernment Conference	7-8/7/2003	Cernobbio, Italy	European Commission	e-Government	Sherpa
20	WSIS Intersessional Meeting	15-18/7/2003	Paris, France	WSIS, ICC	WSIS	BSC, Sherpa
21	Nippon Keidanren Mission on Doha Development	16-18/7/2003	Geneva, Switzerland	WTO	Trade Issues relating to Cancún Ministerial	Sherpa
22	<b>Inter-Governmental Meeting</b>	<b>23-24/7/2003</b>	<b>Washington DC, USA</b>	<b>US Govt, Canadian Govt, Japanese Govt, European Commission</b>	<b>Multiple Issues</b>	<b>Sherpa</b>

	Event	Date	Venue	Group	Principal Issue/s	Representation
23	APEC ECSG 8th meeting	14-23/8/2003	Phuket, Thailand	APEC	Privacy, Cyber Security	Sherpa
24	APEC ETSG Meeting	14-23/8/2003	Phuket, Thailand	APEC	Multiple Issues	Sherpa
25	5 <sup>th</sup> WTO Ministerial Meeting	10-14/9/2003	Cancún, Mexico	WTO	Trade	BSC, Sherpa
26	MPHPT (Ministry of Public Management, Home Affairs, Posts & Telecomms)	15/9/2003	Tokyo, Japan	MPHPT	Multiple Issues	Sherpa
27	Auto ID Center EPC Symposium	15-17/9/2003	Chicago, USA	Auto ID Center	RFID	Sherpa
28	WSIS Prep Com III	15-26/9/2003	Geneva, Switzerland	WSIS	WSIS	BSC, Sherpa
29	ASEAN Telecom Ministers Meeting	18/9/2003	Singapore	ASEAN Telecom	Multiple Issues	BSC, Sherpa
<b>30</b>	<b>GBDe Sherpa Meeting</b>	<b>22-23/9/2003</b>	<b>New York, USA</b>	<b>GBDe</b>	<b>Multiple Issues</b>	<b>Sherpa</b>
31	Computer Science Conference	24/9/2003	Leipzig, Germany		Internet Payments	Sherpa
32	METI	29/9/2003	Tokyo, Japan	METI	Multiple Issues	Sherpa
33	OECD ICCP Meeting	2-3/10/2003	Paris, France	OECD	ADR	Sherpa
34	APEC TEL28 meeting	4-10/10/2003	Taipei, Taiwan	APEC TEL	Cyber Security	Sherpa
35	3rd ASEAN Internet Trust Symposium	9-10/10/2003	Kuala Lumpur, Malaysia	ASEAN	Multiple Issues	Sherpa
36	Consumers International World Congress	13-16/10/2003	Lisbon, Portugal	Consumers International	ADR	Sherpa
37	OECD Information Security Workshop	14-15/10/2003	Oslo, Norway	OECD	ADR	Sherpa
38	EC Workshop on Spam	16/10/2003	Brussels, Belgium	European Commission	Spam	Sherpa

39	ICPEN Conference	9-10/10/2003	Helsinki, Finland	ICPEN, ICC	ADR	Sherpa
40	ITU Telecom World	12-18/10/2003	Geneva, Switzerland	ITU	Multiple Issues	BSC
41	OECD CCP Meeting	16-17/10/2003	Paris, France		ADR	Sherpa
42	Keidanren (Japan Business Federation )	28/10/2003	Tokyo, Japan	Keidanren(Japan Business Federation )	Multiple Issues	Sherpa
43	<b>GBDe CEO Summit</b>	<b>5-6/11/2003</b>	<b>New York, USA</b>	<b>GBDe</b>	<b>Multiple Issues</b>	<b>BSC, Sherpa</b>