GBDe 2005

提言書

（仮訳）

２００５年１０月１７日

目　　次

ユビキタス　ネットワーク　ソサエティ　ビジョン

２００５年１０月１７日

議長：　村上　輝康

理事長

株式会社　野村総合研究所

１．はじめに

ユビキタスという言葉は、長く存在していたが、最近になり良く耳にする言葉となった。意味は、「多くの場所で」、「多くの場所に同時に」とか「何処にでも存在する」などがある。IT の世界では、１９８０年代の終わりに、アメリカの研究者が、利用者が存在を意識しないような形で、環境に溶け込んでしまうような、コンピューターの利用形態について使ったのが初めとされている。

このユキビタスという言葉は、２１世紀の始まり頃に、日本で良く使われだしユビキタスパラダイムとも呼ばれ、その中には、「ユビキタス　ネットワーク」、「ユビキタス　コンピューティング」、「ユビキタス　インフォメーション　ソサエティ」などの多くのコンセプトが含まれている。ユビキタス　パラダイムは、日本で生成され発展して社会インフラの重要な一部となりつつある。そして、韓国をはじめ多くのアジア諸国で共有されはじめている。２１世紀も２００５年に入り、インターネットの世界は、益々その広がりを世界中で見せている。しかし、このネットワークの成長とユビキタス環境の展開は、色々な意味で今後の課題を浮き彫りにしつつある。

GBDe では、過去数年にわたり、多くの課題定義と解決の活動を提言の形で行うグループ・イシューグループとして数多く持ち、主に電子商取引で起こりえる複雑な課題や問題を議論してきた。過去５年間の間に、ユビキタス　ネットワークのコンセプトが形成され、それに伴う社会環境へのインパクトも明確に見えて来た。また、このインパクトは、今後ユビキタスの普及への提言と言う形で議論される必要がある。

２００４年１１月にマレーシア　クアラルンプールで開催された前回の GBDe 世界総会では、「ユビキタス　ソサエティ　フレームワーク」と称し、ユビキタス社会への提言が行われ、その活動は、２００５年に「ユビキタス　ネットワーク　ソサエティ　ビジョン」と言う新たな提言となり、ここに至っている。

２．各国のユビキタス　ネットワーク関連のＩＴ政策

国境を越えた世界的な IT 戦略ともなりつつあるユビキタス　ネットワークは、その発展の為に各国の政府によるＩＴ政策としての共有が重要となる。ここに、各国のユビキタス　ネットワーク関連のＩＴ政策を列挙する。

2.1 u-Japan （日本国）

日本では、2001 年以降、国家ＩＴ戦略として、ブロードバンド化を強力に進める e-Japan 戦略が推進されている。これをいっそう進化させるＩＴ戦略として、総務省が打ち出したのが、2010 年をめざす “u-Japan (Ubiquitous Net-Japan)”政策である。日本は、今後、少

子高齢化や、若年者雇用、安全・安心社会の実現など、数多くの社会経済的課題に直面することになるが、u-Japan とは、それらの諸課題が、ユビキタス　ネットワークのＩＣＴを活用して、解決されているような社会のことである。u-Japan 政策とは、そのような社会を実現するための一連の政策パッケージである。総務省では、この u-Japan 政策を実現するための2015年までの長期研究開発戦略として、ＵＮＳ戦略プログラムを発表している。ＵＮＳは、Ubiquitous Network Society の頭文字をとったものであるが、それは、同時に、このＵＮＳ戦略プログラムを構成する３つの基本コンセプト、Universal Communication, New Generation Network, Security and Safety の頭文字でもある。また日本では、経済産業省もユビキタスＩＴ環境を活用する　“Vision for Information-based Economy and Industries　Vision”を打ち出している。

2.2 u-Korea & IT839 Strategy（韓国）

韓国では、日本の e-Japan や u-Japan の政策の流れと同じように”u-Korea 推進 IT8・3・9 戦略 “と呼ばれる政策が打ち出されている。また、そのルーツは、“e-Korea vision 2006” 政策としてスタートした。IT839 は、８つのサービス、３つのインフラ、９の成長エンジンを戦略のコアとしている。また、その戦略は、“U-Home”、“U-Government”、“U-Commerce” と“U-society” のコンセプトを持ち、最終ゴールには、“Convenient Life”、“Happy Life”、“Safe Life”と“Rich Life”をうたっている。そして IT アプリケーションを幅広く社会に普及させ、IT による利益を社会に与え、同時に社会その物を健康的で安全な環境にする方向性を持っている。

2.3 e-Taiwan and m-Taiwan（台湾）

台湾においても、”e-Taiwan”と”m-Taiwan”の動きがあり、２００２年に打ち出された”e-Taiwan”は、”Challenge 2008”とも呼ばれ、台湾の STAG ボード（Science and Technology Advisory Group）により作られた。コンセプトの中には、1) e-movement. 2) e-life. 3) e-business. 4) e-transport. 5) To establish Broadband Service to over 6 million households　などが、含まれている。また、”m-Taiwan”と呼ばれる関連政策も打ち出され、そして現在は、新たな”u-Taiwan”政策コンセプトをドラフト中である。

2.4 i2010 - A European Information Society for growth and employment（ヨーロッパ）

ヨーロッパでは、ユビキタス関連の政策活動として”eEurope2002 “と”eEuropa2005”などが、進められて居るが、”eEuropa2005”は、その最終ステージの部分まで到達した。その後の活動としては、今後５年を考えた“i2010”政策が打ち出されている。これは、まだ構想の部分も多いが、1) Single European Information Space. 2) Innovation and Investment yielding more and better jobs. 3) Inclusive European Information Society などのコンセプトを主軸に雇用の促進、より良い公共サービス、生活水準の向上などの政策が考えられ

ている。（注：ヨーロッパでは、ユビキタス　ネットワークというコンセプトよりも、アンビアント　インテリジェンスというコンセプトを用いる場合が多い。）

2.5 WSIS（ITU 及び UN 関連の世界会議団体）

WSIS とは“World Summit on the Information Society”世界会議団体で、ＩＴＵの呼びかけで多くの国際連合機関が参加して、グローバルな情報社会の諸問題を、グローバルな枠組みで議論する場を確立している。2003 年のジュネーブでのサミットで諸問題についての問題提起を行い、2005 年のチュニス　サミットでそれらについて結論を提示する予定である。ユビキタス　ネットワークについては、2003 年のジュネーブサミットでも議論されたが、2005 年 5 月には日本で、８５カ国、６００名以上が参加して、ＷＳＩＳテーマ別会合の、東京ユビキタス会議（Tokyo Ubiquitous Network Conference）が成功裏に開催されている。チュニス　サミットでは、デジタルデバイドやインターネット　ガバナンスの在り方が主要なテーマとなるが、ユビキタス　ネットワーク社会の展望についても議論が行われる予定である。

2.6 その他の関連活動

官民学の対話や民から官への政策提言などの活動では、APEC の情報通信会議である TEL (Telecommunication and Information Technology)や、世界会議の ECSG (e-Commerce Steering Group)などの場でも活発なユビキタス社会の到来に関する意見交換が行われており、GBDe では、アドボカシーの活動の一環として、積極的にこれらの関連会議に参加して意見を述べている。

３．ユビキタス　ネットワーク　ソサエティ　ビジョン２００５年提言課題

２００５年のユビキタス　ネットワークソサエティ　ビジョンの提言活動では、下記の課題とそれらに関連するテクノロジーについて検討された。

課題

1. **Privacy Concerns**
   プライバシーに関する課題
2. **Security and Social Safety Concerns**
   社会のセキュリティと安全に関する課題
3. **National ＩＴ　Strategies**
   各国のＩＴ政策におけるユビキタス　ネットワーク政策の共有
4. **Negative Aspects of the Ubiquitous network Society**
   ユビキタス　ネットワーク社会の負の側面に対して
5. **IPR and Copyrights**

知的財産の所有権、著作権、コピーライトなどの課題

6. Developing e-Commerce in Developing World
   これからネット社会に進んで行く国々の課題と電子商取引の普及について
7. Spectrum Allocations, Interoperability and Standardization
   周波数割り当て、相互運用、標準化について

テクノロジー

- RFID　IC タグ
- Mobile Applications　モバイル　アプリケーション
- Sensor Network　センサー ネットワーク
- Networked Appliance　情報家電
- Home Entertainment Network　家庭での娯楽向けネットワーク　コンテンツ
- PLC - Power Line Communications　パワーラインコミュニケーション

3.1 Privacy Concerns
プライバシーに関する課題

ユビキタス社会の到来により、ネット上でやりとりされる情報は増え、またそれは、特定個人のプライバシーの問題へとも発展する。また、ユビキタス社会で活用されるアプリケーションや技術の個々の方式や部品もプライバシーの課題をかかえている。これらのプライバシーの問題は、Preemptive に論じられ、解決策が見出される必要がある。しかしながら、それが、過度に強調されすぎて、技術の発展の芽を、早期に摘んでしまわないように、ＧＢＤe は、常に目を光らせておく必要がある。

RFID　RFID(IC タグ)は、物流や商品の小売などで普及を始めているが、RFID に含まれる情報などが個人情報保護の観点から色々な懸念事項を生み出している。プライバシーガイドラインナドガ提示されるなどの努力がなされているが、そのガイドラインの普及と啓発が広まる必要がある。GBDe では、RFID の利用に関して２００４年秋から２度のアドボカシー会議を開催し、主に米国の業界、消費者団体、政府機関などと活発な意見の交換を行った。また、GBDe は、今後もこの課題に関してアドボカシー活動と提言を続ける。

Mobile and Sensor Network モバイル環境とセンサーネットワークもプライバシーに関連する課題を持っている。主にそれらは、位置情報をもととした動きに関する情報である。また、この「動き」のプライバシーの課題は、今まで人の動きに限られて居たが、ユビキタス社会の発展によりそれが“人と人”、“人とオブジェクト”そして“オブジェクトとオブジェクト”とその範囲を広げている。

Home Entertainment Network　ホーム　エンターティンメント　ネットワーク・家庭での娯楽向けネットワーク　コンテンツは、そのコンテンツ配信がネットワーク化されたことにより利用者の利用に関する情報などがプライバシー問題となる課題が出て来た。

3.2 Security and Social Safety Concerns
社会のセキュリティと安全に関する課題

ユビキタス環境と社会では、利用するネットワークインフラの発達によりそのネットワークを行き来するデータのプロテクションが必要となる。安全なユビキタス環境無しでは、社会インフラとしてのユビキタス　ネットワークは実現しない。この分野は、同時に、新たな大きい事業機会を提供するものでもあることに留意する必要がある。

また、ユビキタス技術の利用により安全が確保されより良い社会環境が見出せる場合もある。昨今世界では、テロリズムに対する社会的懸念が起こっているが、RFID　IC タグを埋め込んだパスポートや身分証明書の利用により社会安全への貢献もできる。

3.3 National IT Strategies
各国のＩＴ政策におけるユビキタス　ネットワーク政策の共有

ユビキタス社会が発展するためには、それを支える各国の政策とそれらの政策を他の国々が理解し、個々の政策を取り込み統合させる理念が必要である。アジア圏では、ユビキタスと呼ばれる動きも、ヨーロッパに行けばアンビエントインテリジェンスと呼ばれ、また米国では何でも繋げると言うコンセプトをもととしたエキストラ　インターネットがそれを指すと言われている。各国では、違った国情をもとに、バラエティに富んだユビキタスネットワーク社会への IT 政策や戦略が展開されている。これらが、一同に集まりお互いに、差異を認識しあうとともに、共通点を見出し、それを伸ばしていく努力を積み重ねていくことによって、そこに世界規模の発展が産まれてくるであろう。

3.4 Negative Aspects of the Ubiquitous network Society
ユビキタス　ネットワーク社会の負の側面に対して

とかく新しい物を受け入れる前には、ネガティブ思考と呼ばれるものが発生する。インターネットの到来により人々と社会の利便性は、向上したが、それに伴い色々な問題が浮上した。GBDe の２００４年の「ユビキタス　ソサエティ　フレームワーク」の提言の中では、招かれざる電子メールの”Spam”に関して論じられたが、２００５年に入ってもこの”Spam”による被害は拡大するばかりか、他の脅威であるウィルス、フィッシング、スパイウェア、トロイの木馬、そしてインターネットのサービスの提供に障害を与える DOS アタックもネットワーク上に蔓延している。

２００５年の GBDe 提言の中にサイバー　セキュリティ　イシューグループが、これらの脅威について検証を行い、また同時にこれらの脅威を阻止する為の世界的活動について述べている。特に、ネット上での犯罪、事件や事故が発生するたびに、マスコミは、サービスの提供者の不備やユーザーの安全に対する自覚不足などを指摘するが、ネット先進国に置いてもこれらのネット犯罪に関しては犯人を罰する法整備が遅れているのは、事実である。

サイバー　セキュリティ　イシューグループの調査によれば、残念ながら、現行のインターネット環境では、世界規模で犯人を探し当てる方法や仕組みにも限度があるとの報告もされており、ネクスト　ジェネレーション　ネットワーク（NGN）や、インターネット　ガバナンスに関する議論の必要性も上げている。また、これらの課題は、幅広く世界規模で議論されるべきである。

3.5 IPR and Copyrights

知的財産の所有権、著作権、コピーライトなどの課題

ユビキタス　ネットワーク技術を用いた娯楽的なコンテンツ利用は、拡大している。これは、ユビキタスの色々な環境である「色々な場所で」、「動きながら」、「家庭にて」などで多く広まり、そしてもう一つの環境である「ビジネスの場にて」でも普及を始めている。そして利用されるネットワーク娯楽コンテンツも音楽、映像・映画、ゲームなどと幅広い。これらコンテンツの知的財産の所有権、著作権、コピーライトなどの問題は、インターネットが社会的に利用し始まった１９９０年代の初め頃より課題として指摘されて居た。

GBDe では、２０００年から２００１年にかけて、IPR – Intellectual Property Rights 知的財産権についてのイシュー　グループを開催した。この時の調査によれば、一部の国では、国のレベルで法的にネットワーク娯楽コンテンツに課税を施し、その著作所有者に金銭面での還元を行っているケースも見受けられた。このような国レベルでの課税の仕組みを作らなければならない背景には、コンテンツに対するコンシューマーによるフェアな利用が望まれない状況が存在していたからである。ここで重要な点は、コンテンツ製作者が、自分の創作に対してフェアなリターンを得られなければ、その製作者が良質なコンテンツを作らなくなってしまうという問題も潜んでいる。

しかし、必ずしも、コンテンツに対する課税の仕組みが、知的財産の所有権と著作権の問題を解決する正しい方法とは限らず、各国には、違った事情が存在する。GBDe としては、その国々に合った解決方法を民と官が一体となり見出すことを提言する。特に、モバイルポータブル音楽配信機器の普及と新たなコンテンツ課金方式の登場により業界では、この議論は、大変熱いものとなっている。

Mobile (Portable Music Player) モバイル　ポータブル音楽配信の普及以前に、インターネット利用者の間では、長らく「インターネット上のコンテンツは、何でもタダである」と言う、間違った解釈が広まっていた。これに伴い、モバイルに限らず、インターネット上のパソコン間などでは、音楽を違法に配信するサーバーなどが構築され一時は、音楽著作権無視の無法状態が続いていた。米国などでは、これらの配信サーバーに対しての法的措置なども取られた。

その後、米国のパソコンメーカーの一社が、ポータブル音楽プレイヤーを販売開始し、その関連サービスとして定額でコンシューマーに受け入れられやすい価格帯での音楽配信ダウンロードサービスを開始した。この流れは、合法的に著作権と利用料を守る仕組みを生み出し、音楽配信の仕組みのあり方に一石を投じ、世界的に普及し始めた。２００５年の８月の時点で、約 20 カ国にてこのサービスが展開されており、今後この方式がデファクトスタンダードとなることが期待されている。 産業界、利用者の双方は、この方式が、この問題にひとつの具体的な解を提示するという点に、着目すべきである。

Home Entertainment Network ホーム　エンターティンメント　ネットワーク・家庭での娯楽向けネットワーク　コンテンツでは、音楽配信業界の動きと違いあまり映像業界全体での知的財産の所有権、著作権、コピーライト対応の纏まった動きが無い。一部では、個別技術によるコンテンツの物理的なプロテクションが検討され試行された。その中には、電子透かしや XML によるメタ　データ　コンテンツ手法などもある。しかし、ネットワークのブロードバンド化による高速化と帯域の拡大により、高解像度の映像コンテンツの家庭での利用が拡大している。すでに懸念されている知的財産の所有権、著作権、コピーライト問題への対応として、映像業界でも、音楽業界で普及しつつあるコンテンツ管理と課金の仕組みなどの利用検討が世界規模で行われるべきだと考えられる。

3.6 Developing e-Commerce and Ubiquitous Society in Developing World
これからネット社会に進んで行く国々の課題と電子商取引の普及について

新たにネット社会へと進む国々に対するネットワークの普及による電子商取引の拡大は、インターネットの社会的普及の始まった１９９０年代初頭からの共通課題であった。世界の何処の国もネットワークは、小規模で低速な物から始まり、どんどん普及していった。GBDe 発足当時は、欧米でもダイアルアップ接続による低速回線利用が主流で、後にブロードバンドが広まって行った。

新しい通信技術とサービスが数多く生み出される前の１９９０年代中頃と比べると２００５年の今これからネット社会へと進んで行く国々は、色々な選択肢を持っている。カエル

飛び（リープフロッグ）と呼ばれる技術普及もその手法の一つで、固定系のネットワークを確立してから、無線系のネットワークの構築にむかうのでなく、はじめからモバイル環境のワイヤレス　テクノロジーを組み込んだハイブリッドなネットワーク構築の構築を行うことも発展途上国におけるネット社会普及の早道なのかもしれない。

特に、ラスト　ワン マイル問題と呼ばれる、利用者の家などへのネットワーク終端の１マイル弱の距離へのインフラ普及には、地上線のバックボーン　ネットワークと組み合わされたワイヤレス技術などの構築が考えられる。

また、社会インフラが全体的に遅れている国々の場合は、通信インフラの前に電力インフラの普及と言う課題が先な場合もある。これらの電力インフラが未整備で展開中の国々には、例えば、電力線上に情報通信信号を流す PLC　パワーラインコミュニケーションの手法も取り入れが可能と考えられる。

しかし、ワイヤレス技術を使ったハイブリッド　ネットワークやパワーラインコミュニケーションを利用する場合も、他のネットワーク環境への影響を良く考慮してその展開を進める必要がある。技術的には、ネット社会にまだ入って居ない国々でも、リープフロッグ的にネット社会を広めることは、可能かと思われる。

3.7 Spectrum Allocations, Interoperability, and Standardization
周波数割り当て、相互運用、標準化について

ユビキタス　ネットワークを実現する機器、アプリケーションやサービスは、何らかの形で、通信インフラを利用し、その帯域や周波数に関連した課題に直面する。特に、近年では、ワイヤレス　コミュニケーションの普及に伴い、スペクトラム　アロケーションと呼ばれる周波数割り当ての問題が発生する。この問題は、GBDe にて過去にも議論された。（２００２年の“Convergence”　提言、２００４年の「ユビキタス　ソサエティ　フレームワーク提言」）特に、周波数の効率的かつコスト面でも安い提供の仕組みが望まれている。また、別な観点からは、世界の何処でも利用が可能な周波数帯の統一的なルーリングも望まれている。周波数の利用形態により制約がかかる技術には、１）RFID（IC タグ）、２）モバイル、３）センサーネットワーク、４）情報家電、５）パワーラインコミュニケーション　などが上げられる。

相互運用に関しては、上記の周波数割り当ての問題と似た課題を持っている。ユビキタスネットワークを実現する環境下では、機器やアプリケーションが、国境を超えて移動し、またネットワーク接続を行う。特に、ユビキタス　ネットワークの特徴でもある、「場所を問わず」、「移動中でも」、「家庭においても」、「ビジネスの場でも」シームレスなサービス

を享受できるためには、必然的に相互運用性が望まれる。相互運用性が求められる技術には、１）RFID（IC タグ)、２）モバイル、３）センサーネットワーク、４）情報家電などが上げられる。

標準化と規格の統一については、さまざまな議論が有る。技術的には、毎日のように新しい技術革新が起こり、さまざまな違った規格が思案される。特に、情報家電の領域では、今後さまざまな規格に関する新技術が登場すると思われる。ユビキタス環境における情報家電も広い意味で考えると次の機器にあてはまる。1) パーソナルコンピューター 2) 電話通信機器 3) オーディオ　ビジュアル系 4) テレビ 5) RON　（実物系ネットワーク）

ここで、ユビキタス　ネットークを構成する注目すべき機器とアプリケーションの課題の中に、ワイヤレス技術を用いた物が有る。これらは、１）オーディオ　ビジュアル系 エンターティンメント機器、２）家庭電化製品、３）パーソナルコンピューターなどで今後普及が進むと思われる簡易ワイヤレス接続の WPAN 方式・Wireless Personal Area Network protocols などで議論がされるべきところである。

RFID（IC タグ）　RFID の普及においては、世界的な標準化の動きがある。国際的な流通標準化機関である GS1(Global Standard One)の傘下にある EPC Global は、流通分野における RFID システムの普及にむけて取り組んでいる。RFID に搭載されるコード（EPC : Electric Product Code）は、流通業界が採用するコード体系である GTIN – Global Trade Item Number をサポートすると表明している。また、類似の動きに日本のユビキタス ID センターが採用するコード体系である “ucode” もある。このように、コード体系を標準化し情報交換を効率化するための様々な取り組みがなされているが、今後は、その情報を利用するアプリケーションの利用環境の標準化、体系化が望まれよう。例えば、製造、流通、販売情報の他に、例えば国際流通においては避けて通れない国毎の文化の違いや、各国の法制度の違いなどを効率的に解決する手段として RFID を利用する事も、今後考慮されるべきかと思われる。

Mobile モバイルに関しての課題で良く知られている物に携帯電話の利用周波数がある。最近では、国を超えて利用できる携帯電話も普及を始めたが、国によっては利用が出来ない、または、規格が違うなどの利用者に取っては難点もまだ見受けられる。利用者の観点から見れば、規格統一の動きである“３G”やその IMT２０００関連規格、そして今後展開される新規格の“４G”などは、支持されると思われる。今後も、このような規格と周波数の統一が可能となることが望まれる。GBDe では、今後もこれらの課題についての提言を幅広く行う。

Networked Appliance　情報家電 家庭電化製品も進化をとげ、ユビキタスネットワークインフラに接続可能な製品が今後出て来る。特に、オーディオ　ビジュアル系の情報家電製品では、ユビキタス化が特に進むと思われる。これらの機器においては、ユニバーサル　デザインと総合運用性などの課題がある。

歴史的には、家庭電化製品に関しては、地域や国により別々なインフラが普及し色々な規格が世界的に混在している。利用電力を見ても　１００V、１２０V、２００V、２２０V から交流周波数の５０ヘルツや６０ヘルツなどの違った規格や、ビデオ規格でも NTSC や PAL と言った、違った物がある。今後は、ユビキタスの環境の到来により、コンシューマーの利便性を考えた規格の統一やインターオペラビリティが望まれる。

WPAN の課題 情報家電の接続に関するプロトコルに WPAN　－　Wireless　Personal Area　Network がある。WPAN は、IEEE の規格の８０２．１５に部類され、現在では、その中の Bluetooth プロトコルが家電の一部やパソコン機器で普及している。WPAN は、ごく小さなエリア（数ｍとか数フィート）の中を結ぶ小規模なワイヤレス　テクノロジーで、今後は、他の８０１．１５関連規格であるウルトラワイドバンド（UWB-Ultra　Wide Band）や、ZigBee などの技術が登場してくる。

ZigBee は、IEEE により８０２．１５．４と規格定義されたが、その利用周波数帯については、世界的に良く議論されず、またアドボカシー活動も活発に行われなかったため、各国に置いては、規制の中で認められている周波数帯を利用するという状況である。米国では、９１５Mhz 帯、ヨーロッパでは、８６８Mhz 帯が割り当てられ、そして日本では、２．４Ghz が使われると予測されている。情報家電の可能性を広げる新しいネットワーク技術ではあるが、規格が統一されても、使われる周波数が国ごとに違うと利用の利便性は薄れる。今後は、これに続く UWB などの新たな IEEE８０２．１５規格の利用も計画されているので、利用周波数などは、出来限り世界統一を望みたい。

４．まとめ

２章の「各国のユビキタス　ネットワーク関連のＩＴ政策」で述べられた通りに、世界では、ユビキタス　ネットワーク社会に向けたい色々な政策の動きがある。これらの動きは、特にアジア圏やヨーロッパが主体で動いている傾向が見受けられる。しかし、今後は、ユビキタス　ネットワークのコンセプトが世界的に広まり、発展的に普及して行く兆しが見える。

この ICT（インフォメーション　コミュニケーション　テクノロジー）パラダイムシフトが実現する為には、世界的にほぼ同じ方向に向かうユビキタス　ネットワーク社会のビジョンの共有が望まれ、この新たなパラダイムを GBDe の民間主体のイニシアチブをもとに、幅広い国に働きかけて支持を求めることは、今後の電子商取引にも、新たな可能性をもたらすものとなる。GBDe では、その発足当初より、参加者がお互いに協力しあい、絶えず新しい流れを作り続けているが、今後、電子商取引に新たなフロンティアを拓くために今必要なのは、このユビキタス　ネットワーク社会のビジョンの共有なのである。

GBDe の参加各国の動きを見ると、固有な問題や共通課題などが数多く見受けられる。しかし、GBDe のような世界規模の民間主体の提言団体が存在するので、世界規模の相互協力や民から官に対する提言などが行える。GBDe のアドボカシーの活動を通じて、解決の方向に向かえる課題は多い。

GBDe の発足当時は、インターネットが普及し始めたばかりで、ナローバンドがそのアクセス主体であった。また、電子商取引を主体とした、アドボカシー活動が主流であったが、いわゆるＩＴバブルの崩壊によってＧＢＤｅは、非常に厳しい試練の時を経験した。２１世紀を向かえ、ユビキタス　ネットワークの普及によりネット社会の形態も進化し、ユビキタス　ネットワーク　ソサエティ ビジョンが誕生し、電子商取引にも、新たな可能性が開けてきている。GBDe は、政策提言とアドボカシーを今後も活発に続け、常に、電子商取引の新たなフロンティアの開拓に注力し続けるべきである。

電子政府

２００５年１０月１７日

議長：　古川 一夫

代表執行役 執行役副社長　情報・通信グループ長＆ＣＥＯ

株式会社　日立製作所

１．始めに

我々GBDe は、’01 年 電子政府 Issue Group を設立し、以下の提言をしてきた。

Deleted: WG

‘01：企業と政府の関係から観た望ましい電子政府の条件を提言
‘02：市民と政府の関係から観た望ましい電子政府の条件を提言
‘04：政策・制度・法形成過程へのネットを通じた参加システムの条件と参加システム構築を提言

その理由は、政府・自治体はその国・地域において、最大の調達者，購買者であり、最大のデータ、コンテンツ保有者であって、その業務・サービスの電子化及びネット対応化は、その国・地域の IT インフラ整備，電子商取引を推進するからである。

確かにここ数年、途上国を含む多くの国で電子政府の実現，促進が国の政策として挙げられ、進められてきた。UN Global E-government Readiness Report 2004 によれば調査 190 ヶ国のうち 170 ヶ国でインターネットに対応している（cf. http://www.cnpan.org/egovernment4.asp)。特に、各種の登録，申請，申告に関する中央官庁の業務・サービスは、多くの国で、その一部でも実現されつつある。

しかし、地方では、必ずしも中央程進んでいるとは言えない。財政と人材の不足がその原因として挙げられる。
我々企業は、普段の活動では地方自治体の方が接点が多い。地方自治体の電子政府実現促進が望まれる。

我々は、更なる電子政府の実現，促進の手段・方策の 1 つとして、オープソースソフトウェア(以下 OSS と表記)の適用推進を提言したい。

２．オープンソースソフトウェア(OSS)の定義，特長

(1) OSS とは、ある共通の性格をもつソフトウェアの使用許諾(ライセンス)群の下に使用・流通が許諾されるソフトウェアの総称である。
それらの使用許諾は、
- 配布・再配布に制限が課せられない事、
- 無償で使用許諾がなされる事、
- 使用が許諾される対象，用途に制限がない事、
- ソースコードの公開・配布が義務付けられている事、
- ソースコードの改変が許諾されている事、

という性格をもつ。
商用のソフトウェアが様々なライセンスの下にその使用が許諾されている様に、OSS のラ

イセンスも複数存在し、それぞれに許諾条件が異なることに注意しなければならない。又、OSS＝無償のソフトウェアという認識も誤りである。無償であるのは使用許諾に関してのみであり、OSS に関するサービス(保守，技術サポート，配布等)は有償で提供されるのが通常である。

OSS の具体的ソフトウェアとしては Linux が最も知られている。

(2) OSS を採用する事により期待されている効果は以下の通りである。

① 仕様が公開され、希望する誰もが実装可能なオープンな標準に準拠したソフトウェアプロダクトを、政府，自治体が調達する事により、ベンダー各社が同じ基盤の上で競争する事が可能となる。その結果として、政府・自治体の選択肢が拡がり、より低コストで電子政府が実現できる。

② 仕様が公開されているソフトウェアプロダクトを採用する事により、情報システム間のインタオペラビリティ実現が可能になり、それにより、開発，メンテナンス，他システムへの移行に柔軟に対応可能となり、政府や自治体は、特定の製品やサービスへのロックインを避け、将来に渡る調達の自由度を確保し易くなる。

③ 仕様が公開されている事により、将来に渡る自由度と柔軟性を確保でき、将来的に別ソフトウェア製品へ移行をする際に必要となる人材のスキルトレーニングのリスク、データの変換リスク，運用上のリスク等をより少なくする事が期待できる。

④ インターオペラビリティの確保が容易となり、異なる政府機関を含む関係機関間の相互接続とデータの自由な交換が可能となり、企業，国民及び関係機関が必要とするサービスをタイムリーかつ効果的に提供できる事が期待できる。

⑤ ソースコードが公開されており、改変が許諾されているので、当該ソフトウェアの開発者以外の多くの人間が、ソースコードの検査に携さわる結果、悪意あるコードの混入により、機密情報や個人情報が漏洩する危険が比較的少ない。又、該当ソフトウェアにセキュリティホールが発見された場合でも、当該ソフトウェアの開発者に依存することなく、第三者がそのセキュリティホールを埋める事が出来る。

⑥ ソフトウェアの利用及び用途に制限が加えられていないので、ソフトウェアもしくは、その一部のコードを電子政府を構成する他のソフトウェアに再利用する事が出来る。

３．OSS を巡る動向

我々は、GBDe のメンバーおよび友好関係にある団体・組織などを通じて、以下のような OSS 適用・採用の推進状況についてのレポートを得た。紹介したい。

３．１．アジアでの状況（CICC からのレポートより）

日本の NPO である CICC は、日本の METI の支援を受け、’03 年 3 月タイでの「第 1 回アジア OSS シンガポール」を開催している。その後、’03 年 11 月第 2 回(シンガポール)，’04 年 3 月第 3 回(ベトナム)，’04 年 9 月第 4 回(台湾)，’05 年 3 月第 5 回(中国)，’05 年 9 月

第6回(スリランカ)を開催している。ここではアジア10数ヶ国の政府，学術，民間の情報関係者が集まり、アジアにおける OSS 適用推進について討論している。(cf. http://www.asia-oss.org)

その報告によれば、既にマレーシア，韓国，インド，インドネシア，ベトナム等いくつかの国が公式に OSS の採用促進を政策として掲げている。

３．２．日本の状況（日立からレポート）

政府の IT 政策「e-Japan 戦略 2004」の中で、OSS 開発の促進を支持し、これに伴って、経済産業省支援により、GBDe メンバーである IPA を中心に OSS 活用基盤整備事業や日・中・韓の連携による標準化作業等が進められている。

IPA による OSS 導入実験の結果、教師達の 70%から Linux が学校での利用に適しているとの評価を得ている。経済産業省は、本年度、さらに自治体での導入実験を計画中である。また、IT 戦略本部の“2005IT 政策パッケージに従い、政府は、新たなオープンソースソフトウェア調達のガイドラインを策定中である。又、自治体では、島根県の電子入札（＝電子調達）システム、北海道の共同アウトソーシングシステム、長野県の設計積算システムなど県レベルを始め、鹿児島県徳之島天城町の特産品サイトなど町レベルまで適用が進んでいる。更に、本年度中に高知県や岡山県等、８自治体が共同で基盤業務パッケージソフトウェアを開発し、オープンソース化する作業が進められている。

又、民間企業が中心となり、「日本 OSS 推進フォーラム」が設立され、官・民連携による OSS 普及に関する課題解決策が検討されている。

政府・自治体の OSS 適用を支援するため、民間の OSS 専門家を政府・自治体の CIO 補佐官として派遣する動きもある。

３．３．マレーシア状況（MDC からのレポートより）

公的機関へのオープンソース（OSS）普及に対するマレーシア政府のイニシアチブは、首相府直属機関、Malaysian Administrative Modernization and Management Planning Unit（MAMPU：マレーシア行政近代化管理計画庁）が指揮を取っている。

OSS イニシアチブは、効率的かつセキュアで質の高いサービスを提供するという公的機関の ICT フレームワークの中で、OSS を利用する価値を構築し、高めるためのビジョンを掲げ、下記の目的を達成するために設立された。

- 所有者のコストを軽減する。
- 利用するソフトウェアを自由に選択できるようにする。
- システム間の互換性を高める。
- ICT 産業を発展させる。

- OSS 産業を発展させる。
- OSS のユーザおよび開発者のコミュニティを発展させる。
- デジタルディバイドを緩和させる。

マレーシア政府の「公的機関オープンソース・マスタープラン」は以下を目標としている。

- 戦略的方針およびフレームワークの構築。
- 実装計画およびロードマップの作成。
- 公的機関における OSS 実装を支援する Open Software Competency Center（OSCC）の設立。
- 政策、標準、ガイドラインの形成。

以下が、OSS 実装の主な利点である。

- ベンダのロックインが防止できる。
- 世界的で、無償の、非独占的かつ永久的なライセンスが付与される。
- 無料のソースコードバージョン管理ソフトウェア。
- 優れたソフトウェアセキュリティ。
- コンフィギュレーションマネジメント（プラットフォームおよびコンパイラー)。
- ソフトウェアの変更/改良および試験が可能。
- ソフトウェアの修正、配布が無料あるいは制限なくデバッグ可能。
- ドキュメントのアップデート。
- ベンチマーキングおよびパフォーマンスの調整。

実装プログラムを推進し、公的機関における OSS 実装支援、指導を行う単一の窓口として機能している Open Source Competency Center（OSCC）は、以下の役割を担うために設立された。

- 知識および経験を共有するためのナレッジバンクとして。
- 意識の構築、OSS および OSCC の推進のため。
- 公的機関の職員に対する OSS 教育および保証プログラムの指揮、調整役として。
- OSS 実装に関して政府機関を促進、調整、支援するため。
- OSS の研究開発プログラムの指揮、促進、調整および監視のため。
- OSS 実装を推進するための政策、ガイドラインおよび標準の形成。

OSCC の 2005 年の目標：

活動	目標
認識	▪ CIO および IT 部の職員 100% が OSS について認識する。
スキル向上	▪ IT 関係の職員 60%に OSS の訓練を受けさせる。 ▪ IT 関係の職員 10%に OSS の資格を取らせる。 ▪ 学校の IT 研究室の教授 20% に OSS の訓練を受けさせる。
教育	▪ 大学教育機関 40%が OSS を利用した授業を行う。 ▪ 学校の IT 研究室 20%が OSS を利用した授業を行う。
調達	▪ 新たに調達したサーバ（ハードウェア）の 60%がオープンソースの OS に対応する。
実装	▪ 学校の IT 研究室 20% が Office 統合ソフトを組み込んだ OSS を設備する。 ▪ ウェブサーバ（ソフトウェア）の 60%に OSS を利用。 ▪ 職場のインフラ（email, DNS, Proxy）の 30%に OSS を利用。 ▪ デスクトップソリューション（e.g. web browser, email reader）30%に OSS を利用。

３．４．台湾状況（III からのレポートより）

Deleted: メンバー

（1）背景

フリーソフトウェア産業の成長は、国家の IT ハードウェアおよびソフトウェア業界の発達度を測る指標となってきた。また、フリーソフトウェア産業により、台湾全体の競争力を高める重要な基盤がもたらされるだろう。企業がフリーソフトウェアを安価で利用できるようにするため、また台湾のソフトウェア産業の総合的な競争力を高めるために、2002 年 6 月 3 日、立法院科技及資訊委員會（the Sci-Tech and Information Committee）は、「台湾産業界の競争力及び独立性を高めることを目的に、バリアフリーのソフトウェア開発環境におけるソフトウェアの自由な研究開発を奨励する」会議を開催した。会議には、様々な機関および団体の代表が招待され、台湾が採用すべき戦略が話し合われた。

2002 年 6 月 20 日、行政院は、フリーソフトウェア推進会議を招集した。会議開催中、次のことが決定された。経済部は、フリーソフトウェア推進チームの組織、推進のためのメカニズムの構築に関してだけでなく、役割分担および作業項目実施のタイムテーブル設計

についても責任を負うものである。これに続き、行政院国家情報通信イニシアティブ（NICI: National Information & Communication Initiative）の第6回会議において、フリーソフトウェア推進委員会の設立および経済部工業局によるフリーソフトウェア推進チームの結成が決定された。これらの決定に従い、フリーソフトウェア産業奨励計画が立案された。この計画の実施により、台湾のフリーソフトウェア産業の促進、フリーソフトウェア利用の推進、情報の共有および交換につながることが期待されている。

（2）開発戦略

1．法的枠組みの強化および適切な奨励策の整備
2．研究開発および人材育成の重視
3．製品開発および新案出願
4．業界標準および認証メカニズムの構築
5．フリーソフトウェアコミュニティ開発および国際的協力の推進
6．ビジネスチャンスおよび市場開発の促進
7．フリーソフトウェア商業化の推進
8．フリーソフトウェアユーザー基準の拡大

（3）主な施策

1．　フリーソフトウェア産業促進の計画、推進、評価を効果的、包括的に管理するため、フリーソフトウェア研究開発を促進するため、フリーソフトウェアアプリケーション開発に適した環境を構築するため、政府は、行政院国家情報通信イニシアティブ委員会（NICI: National Information & Communications Initiative Committee）のもと、フリーソフトウェア推進委員会（FSSC: Free Software Steering Committee）を設立した。通常、FSSCは3ヶ月に1度召集されるが、特別に緊急の問題を扱う際は、必要に応じて、別に召集が行われる場合もある。
2．　経済部工業局は、NICIのもとソフトウェア作業委員会を設立した。この作業委員会は、FSSCの諮問機関としての役割を果たす。FSSCより委託されたタスクの実施、フリーソフトウェア産業促進戦略の立案、フリーソフトウェア推進イニシアティブの発揮、作業実施状況および達成状況の検討などを行う。
3．　フリーソフトウェア産業促進に適した環境構築支援のため、政府は、製品の互換性認証、業界標準の形成、人材育成サービスの提供、国際的な協力の促進を行う。
4．　政府は、大学、専門学校、研究機関のフリーソフトウェア技術促進への参加を推奨し、フリーソフトウェア産業に必要な人材育成を支援する。
5．　政府は、フリーソフトウェア産業を促進する分野を特定し、特に重点を置く。また、計画実施戦略の立案、必要な施策および補助政策の策定を行う。主な促進分野は、継続的に毎年選定する。選定後、承認を得るためFSSCに提出する。2004年の主な促

進分野は、業界の発展および促進、製品テストおよび認証、コミュニティの開発および技術応用であった。

6． フリーソフトウェアの著作権およびライセンス契約の保護・管理メカニズムを強化するため、またフリーソフトウェアの作成・配布を推奨するため、フリーソフトウェア産業促進に関連する法および政府調達規制の形成あるいは改正を行う。

7． 国内のフリーソフトウェアコミュニティが国際的交流活動へ参加することを推奨し、台湾のフリーソフトウェアコミュニティの規模および質を向上させる。

8． 国際的に利用可能な中国語ソフトウェアの開発、フリーソフトウェア産業の情報提供サービス向上を目的として、台湾・中国間の連携を強化するためのメカニズムを構築する。また、フリーソフトウェア産業が開発した製品が、確実に市場のニーズを満たすためのメカニズムの構築も必要となる。

9． 政府の技術開発プログラムへのフリーソフトウェアソリューションの採用、および公共事業入札の際のフリーソフトウェアの利用を推奨する。

10. フリーソフトウェア企業の技術、製品、市場開発の分野への支援を目的に、研究開発を推奨するため、経済部の産業に特化した技術開発プログラム、製品開発プログラム、プロジェクトローンを活用する。

11. 政府の IT 構築およびそれに適した環境の達成において最大限の透明性を確保するため、政府機関がオープンソースコード方式の採用を主張することを奨励する。

12. フリーソフトウェアに対する市場の需要をシュミレーションするため、政府調達および eTaiwan 計画への参加を効率化する（公正な競争の原理に違反しない限りにおいて)。

３．５．ブラジル状況（NEC からのレポートより）

2003 年 10 月 29 日、ブラジルのルイス・イナシオ・ルーラ・ダ・シルバ大統領は、OSS、デジタルブリッジ、政府のシステム･インテグレーションを推進、計画、実施するために８つの技術委員会を設立する法律に調印した。OSS 推進および実装の調整役として、大統領府直属の機関である国立情報技術研究所（ITI：National Institute for Information Technology）が任命された（www.iti.gov.br)。

ITI は、ブラジル行政機関における OSS 実装の基本方針および活動を定めた最終報告書を承認した。18 のガイドライン、12 の基本方針、29 の主な活動が規定された。

承認されたガイドライン：

１）IT イニシアティブのコスト削減を推進するため、OSS に根差したソリューション、プログラム、サービスを優先する。

２）システムおよびユーザインターフェース開発のためのウェブプラットフォームを優先

する。
3）サービスおよびアプリケーションの ICT（情報通信技術）プラットフォーム開発のためにオープンスタンダードを採用する。
4）OSS の一般利用を促進する。
5）OSS 利用により国民へのサービス改善を図る。
6）国民が公的サービスへアクセスする際、プロプラエタリ（独自）・プラットフォームの使用を義務付けない。
7）デジタルデバイドプログラムの基礎として OSS を活用する。
8）プライバシーおよびセキュリティに関する法律を考慮しながら、システムの完全な監査、セキュリティを確保する。
9）レガシー（既存の）・システムとの相互運用性を促進する。
10）現行のプロプラエタリ・システムの改良を制限しない。
11）レガシー・システムのオープン・システムへの段階的移行を推進する。
12）OSS と互換性のあるハードウェア獲得を優先する。
13）自発的・協力的な OSS システムの自由配布を確保する。
14）政府および地方自治体の内外における OSS イニシアティブの向上と共有を推進する。
15）OSS に根差した新しいビジネスモデルの採用を推進する。
16）OSS 適用に向けた公的機関の風土改革を推進する。
17）OSS 利用に向けた公務員の教育を推進する。
18）OSS に関する国家政策を形成する。

また、2003 年 10 月、OSS は国家政策として掲げられた。政策名は、「ソフトウェア・リーブル・イニシアティブ（SOFTWARE LIVRE Initiative)」。ITI（国立情報技術研究所）が調整を行っている。

（OSS 適用を政策として掲げている政府機関や市、州）

2003 年 11 月 24 日、ブラジル連邦政府は OSS の利用を正式に推奨した。それ以後、ブラジル上院・下院議会、議員室、経済省、ブラジル政府連邦データ処理サービス（SERPRO)、ブラジル農牧業研究公社（Embrapa)、Eletronorte 社、Petrobras 社、サンパウロ地下鉄公社（Sao Paulo Metro Company）など様々な公的機関が段階的にシステムの移行を行っている。

（OSS を適用している州）

ブラジルの 27 の州のうち 11 州が、公共システムにおける OSS 利用を推奨している。このイニシアティブは「プロジェクト・ソフトウェア・リーブル」と呼ばれ、次の州に採用された。バイア、サンパウロ、マトグロッソドスル、リオグランデドスル、パラナ、エスピリトサント、ミナスジェライス、ペルナンブコ、リオデジャネイロ、サンタカタリナおよび連邦区である。

サンタカタリナやペルナンブコなどは、他の州が非政府組織として留まる一方で、正式にこのイニシアティブを採用した。

（OSS を適用している都市）
2001 年、リオデジャネイロ州のリオダスオストラス市は、OSS を標準として正式に適用し、TATUI と呼ばれる独自の OSS を開発した。TATUI は、すべてのコンピュータに幅広く配備された。

ペルナンブコ州の州都であるレシフェ市は、2001 年に OSS 利用を州法第 16.639/2001 に制定した。

（指摘されている利点と課題）
主な利点について、リオダスオストラス市やその他ブラジルの機関は、ソフトウェアライセンスのコスト削減ができること、ニーズによりソフトウェアをカスタマイズできる柔軟性があること、OSS アプリケーションを実行する限られたマイクロコンピュータの使用を継続することができる可能性があることなどを挙げている。課題としては、公務員の教育の必要があることを指摘している。

３．６．OSS に関する GBDe 事務局レポート

Deleted: 5

（１）世界における OSS

IT リサーチ＆コンサルタント会社であるガートナーは、OSS は、2005 年の IT 関連の話題の中心であり、最も熱いトレンドであると述べている。またガートナーは、2010 年までに Global-2000 の IT 企業は、インフラ中心のソフトウェア投資のうち 80%を、またビジネス用ソフトウェア投資のうち 25%を OSS 製品への投資として考慮するだろうとしている。OSS は、ライセンス料からサービスやサポートへと、収入源を移動させることにより、ソフトウェア市場に革命を起こすと期待されている。

アメリカ以外の世界の主要政府は、Linux や OSS を採用しているか、あるいは採用へ向けたプロセスを歩み始めている。OSS、特に Linux は、ソフトウェア開発の最善のモデルであり、経済成長の原動力であると考えられ、世界中の国や地域に拡大している。各国政府は、OSS の採用を、有望なトレンドを生み出す手段と考えている。

Linux は、約 4 年前にヨーロッパで採用され始めたのを足掛かりに、世界中で利用されるようになった。2001 年、ドイツ国会は、政府は「その採用によりコスト削減可能」な OSS を利用すべきであるとする決議案を採択した。2 年後、技術顧問団が欧州委員会に、ある報告書を発表した。この中で、OSS は、ヨーロッパの輸入への依存を改善し、「地方に多大な

機会をもたらすもの」とされている。地方は、「情報技術産業の法則を変え得る」可能性を持っている。

2004 年、195 億米ドル相当の Linux 関連技術がポーランドとロシアにおいて販売された。同時期、インドの主要 7 団体がアプリケーションソフトウェアおよび開発事業を Linux に移植し始めた。7 団体とは、Indian Railway Catering and Tourism Corporation、South Asian Petrochem, Ltd、Kotak Mahindra Bank、IDBI Bank、Central Bank of India、インド財務省、西ベンガル政府である。

ラテンアメリカの大規模市場トップ 6 は、最も急速に Linux の採用を進めている地域である。アルゼンチン、ブラジル、チリ、コロンビア、メキシコ、ベネズエラがトップ 6 である。IDC（International Data Corporation）の最新の報告書によると、「Linux の OS は、ラテンアメリカのベンダやユーザーコミュニティに広く受け入れられている。Linux の OS は、OS ソフトウェア市場で最も急成長している」ということである。

（2）インドにおける OSS

2005 年 8 月、ベンダ 2 社が、Linux 搭載で約 230 米ドル（9,9990 ルピー）の初心者向け PC に着手した。これらのイニシアティブは、Dayanidhi Maran 通信情報技術相（MCIT: Ministry of Communications and Information Technology）によって支援されてきた。現在、インドでは 1,500 万人が PC を所有しており、国内で 500 万のインターネット接続回線が引かれている。インド政府の目標は、2010 年までに、PC 所有人口を 7,500 万人に、インターネット回線を 4,500 万に増加させるということである。

またインド政府は、高価格のプロプラエタリ・ソフトウェア（専売権付きソフトウェア）を利用しなくて済むよう、チェンナイに OSS を開発するオープンソースセンタを設立した。

（3）中国における OSS

中国は、ソフトウェアプライバシーに対する国際的圧力（特にアメリカからの圧力）によって、OSS 採用へと追い立てられた。Red Flag 社は、Asianux は世界で配布されている Linux のうち最もポピュラーなものの 1 つだと主張している。また、Red Flag 社は、特にサーバーに強いことから、中国の Linux デスクトップの市場シェアのリーダーとなっている。中国のソフトウェア産業は毎年 30%ずつ成長してきたと報告されている。2004 年、中国政府機関は、Linux OS のコピーを約 2 万 7,000、RedOffice パッケージのコピーを約 12 万購入した。(Linux Journal 2005 年 6 月 18 日号より)

（4）ブラジルにおける OSS

大統領主席補佐官とのつながりを持つ、ブラジルの国立情報技術研究所（ITI: National IT Institute）は、これまで利用されていたプロプラエタリ・ソフトウェアを OSS に交換するというプログラムを発表した。ブラジル政府は、公的機関を OSS プラットフォームに移行させることを計画している。

現在（2005 年 6 月）、そのプロジェクトに割り当てる資金を巡り、いくつかの議論が行われている。ITI は、2 億レアル（8,540 万米ドル）を要求したが、財務省計画局は、ソフトウェア移行の費用を 5 千万レアル（2,130 万米ドル）と見積もった。また財務省は、ITI が提案したような総合プロジェクトとしてではなく、資産や必要に応じ、各省庁がそれぞれにこの移行に対処することを希望した。ITI は、OSS への移行は 5 千万レアルで可能だということを認めたが、プロジェクトはスローペースでしか進まず、全ての省庁の移行を完了することはできないだろうとしている。

３．７．GCD メンバー市の状況（GCD 事務局からのレポートより）

Deleted: 6

Global Cities Dialogue（www.globalcitiesdialogue.org）のメンバー都市を対象にしたインタビューによると、地方自治体は、電子政府実現に OSS の役割がいかに重要かということをますます強く意識し始めていることが分かる。インタビューを行った都市の中では、OSS に関して望ましい政策を掲げている都市は数えるほどであったが、近年、大半の都市（対象都市の 75%）が OSS アプリケーションを採用しているか、あるいは市政における情報技術の採用やデジタルディバイドを解消することを目的としたプロジェクトの開発に OSS が一役買ってくれると見込んでいる（ブラジルなど）。

地域コミュニティでの OSS 採用の現状は、未だ十分ではないと考えられているが、OSS ベースの運用システムやオフィスアプリケーションの開発を望む声は増加しているようである。

インタビューを行った都市は、主にサーバ、ウェブサイト、イントラネットなどに OSS アプリケーションを利用している。最も評価されている OSS の利点は、コストの低さ、使い易さ、高いフレキシビリティ、ベンダからの独立性などだけでなく、市民・市政間のコミュニケーションの改善に OSS がもたらす可能性が挙げられる。特に、OSS およびコンテンツは、「コミュニティの創造性および生産性を促進するだけでなく、市民および市政の目的であるポータルサイトを強化するための新たな手段」（ボローニャ市の”Iperbole”という市民メットワークなど）と考えられている。

ドイツでは、市民および企業へのオンライン行政サービスの促進（公的契約の登録から譲渡に至るまで）のためだけでなく、国家、地域、地方レベルでの行政サービスに対する電子決済システムなど、革新的な署名および暗号化技術に基づいた電子政府ソリューションを実施するため、OSS を広く利用してきた[ハンザ同盟都市ブレーメンの“Governikus”システムなど]。

フランスでは、行政がフリーソフトウェアの開発や e-Administration（行政）プロジェクトの実施支援が行えるよう、”AdmiSource”と呼ばれる共同プラットフォームが提案された。電子政府のエンジンとしての OSS およびフリーソフトウェアの重要性は、欧州議会においても認識されている。近年、欧州議会は、欧州委員会が提案した「ソフトウェア特許指令（コンピュータを使った発明の特許取得に関する指令)」を否決している。

実際、行政の OSS 実装の成功は、ユーザーがこの新しいソフトウェアを受け入れるかどうかに左右されるだろう。従って、OSS 実装のプロセスに市民を参加させること、彼らの要望およびニーズを考慮に入れることが重要となる。ユーザーの要求がそれほど厳しいものでなければ、OSS 開発への投資に都合のつかないソフトウェア製作者の障壁を除去することもできるだろう[ミュンヘン（ドイツ）など]。

４．電子政府への OSS 適用促進に関する課題と解決策

これまでの各種の場で指摘されている事は以下の通りである。その解決策として我々は以下を提案したい。

(1) OSS 適用事例が少なく、その効果が充分認識されていない。

→ ・政府や自治体等公的機関の情報システムへの適用を政策として決定・公表する。
・先ずモデル的に政府、自治体のシステムに適用する事を行ない結果・評価を公表する。

(2) OSS を提供できるベンダーが充分育っておらず、競争状態になっていないので、本来のメリットが発揮され難い。

→ 官・民・学一体となった技術者育成策を決定し実施する。

(3) IT ベンダの中では、政府システムへの OSS 適用が進むことにより事業規模が減るのではないかとの懸念からビジネスの影響が見通せず、要員確保や教育等の投資が進まない。

→政府は、OSS 適用によって下がったシステム構築におけるソフトウェアコスト差分を、より高度なシステム実現へ、ベンダの IT サービスに適切な支出を確保する。

(4) 国際的な又、多くのシステム間のインタオペラビリティを確保する為の OSS に関する基準，標準とその適用範囲が定まっておらず、どの範囲について、何に従えば、他の OSS

Deleted: 3

適用システムとのインタオペラビリティが確保されているのかの標準がない。
→ 国際的に官・民・学連携した組織，場を設け、各国，各機関の知恵を出して、適切な範囲の、適切な標準を、適切な順序で定め公表する。

OSS と言えども、電子政府構築の手段として万能ではない。我々民間企業は、サーバやデジタル機器などへの適用を通して、より良い適用の仕方，その効果と課題及びその解決策を示していく。

各地の OSS 適用状況，政府状況を報告して頂いた GBDe メンバーMDC(マレーシア)，III(台湾)，NEC(日本)及び GCD，GBDe 事務局のご協力に深謝します。

国際小額取引

２００５年１０月１７日

議長：　Dr.　Shyue-Ching Lu

President

Chunghwa Telecom（中華電信）

はじめに

過去の調査結果を見ると、ｅコマースの発展のためには適切な決済システムの存在が不可欠である。実社会の動向を見ると、過去３年間の B2C ｅ コマース取引の大部分はマイクロペイメントが占めていることがわかる。２００４年初旬までには B2C ｅ コマース全体に占めるマイクロペイメント取引量は約６０％に増加していた。その間、ユーザーの平均年齢は毎年徐々に低下しており、現在はティーンエイジャーが特にデジタルコンテンツ取引の主流ユーザーとなっている。

マイクロペイメントとは各取引あたり１５ドル未満、各請求期間中あたり１００ドル未満の金額を振替える手段であり、通常の決済システムによる徴収が、徴収額にてらして非実用的もしくは非常に高コストである場合に用いられる。一般的にマイクロペイメントシステムは多くのマイクロペイメントを集積し、集まった金額を取引の前後に通常の決済として徴収する。米国でマイクロペイメントが頻繁に利用される状況の事例としては、公共輸送システム、大学の学生食堂、道路の通行料金がある。これらはサービスが実行される度に消費者からその対価を徴収していたのでは全く非実用的な領域である。インターネット上でコンテンツの有料提供を促進する為に、昨今マイクロペイメントシステムの大幅な革新が行われている。多くの決済はクレジットカードで行われるが、クレジットカード決済の処理には通常、最低およそ２０セントプラス代金の数パーセントの手数料がかかる。明らかに料金よりも安く請求することが不可能である。

マイクロペイメントの根本はコンテンツを極めて小額の料金で提供する事により、大量の視聴者を維持しその利点を生かすことにあるだろう。例えば、ウェブコミックの作者がオンラインコミックブックを２５セントで売る等である。このアイディアの他のバリエーションとしてはセントの端数（最小単位の硬貨よりも小さい額）を同等の端数料金のコンテンツに対して請求する、例えばオンラインマガジンのウェブページ１枚あたり１０分の１セントを請求する等がある。

次の２つのシナリオにおいて、潜在的な顧客としてあなたがどのような行動を取るか想像してほしい。

シナリオ １：

あなたは台湾にいて、韓国にあるホームページ上の韓国ドラマを見たいとする。どのようにそれを入手するか？どのようにそのサービスの料金を支払うか？

シナリオ２：

日本に出張中、仕事が終わって FOMA ワイヤレス LAN が使える公園でくつろいでいると

する。あなたはインターネットにアクセスしたい。あなたはそれをどのように実現しどのような方法で支払いを行なうか？

シナリオ３：

今台湾に滞在していて、ワールドワイドサイトにあるディスカバリー誌を閲覧したいとする。サービスはページ毎に課金される。そのサービスをどうやって受け、どのような方法で支払うのか？

上記で述べたシナリオは我々の日常生活で起こりうる。しかし、クロスボーダー取引シナリオでユーザーが満足できる決済メカニズム、特にティーンエイジャーが使えるものはあまり無い。主な障壁は次のように要約できる。

決済ツールはすべてのユーザーが簡単に利用できるようになっていない。特に主要ユーザーであるティーンエイジャーが使えるようになっていない。

心理的な障壁としては消費者からの信頼の欠如、個人情報漏えいの心配、そしてクロスボーダー取引紛争に対する疑念があげられる。

クロスボーダー取引における発送や処理が未だに整っていない。

運営事業者は国際決済メカニズムに対する投資の有効性について疑いを持っている。

マイクロペイメント取引が取引の主流を占めるに至った一方、特にデジタルコンテンツに関して潜在的リスクが認められる。消費者の心配が実損失や不十分な個人情報保護（データ開示）のインパクトを含む取引リスクとともに増加するにつれ、我々は国際マイクロペイメントの確立と推進が特にデジタルコンテンツについてインターネット上決済よりも受け入れられるだろうと考える。さらに、ユーザーはマイクロペイメントではデータの完全性と認証はあまり重要視しないと考えられる。したがって、一般的なインターネット上の決済環境を導入する前に、まず国際マイクロペイメントの仕組みを確立するほうが良いと思われる。

現在、広く採用され信頼できる国際マイクロペイメントの仕組みは殆どの国で欠如している。本稿ではマイクロペイメントの、現在の発展状況の概要について述べ、市場における差し迫ったニーズが存在する一方で現在のこう着状態が続いている理由を挙げ、最後に諸問題を克服するための方法を指摘する。

現存のマイクロペイメント（メンバー国における発展と応用の現況）

いくつかの国ではマイクロペイメントをデジタルコンテンツ取引、自販機による飲料販売、地下鉄や公共バスの料金支払いといったサービスに応用している。これらの国々では日々の生活に利用できる「デジタル電子財布」の配布を始めている。ほとんどのデジタル電子財布はバーチャル ID 情報が入ったコンタクトレス・カードであり、商業利用だけでなく電子政府サービスにも利用できる。下記にいくつか例を挙げる。

日本

プリペイド方式によるマイクロペイメント（オンライン）：この種のマイクロペイメントに対して顧客は通常現金、クレジットカード、または ATM で事前に支払いを行い、自分のウェブアカウント内で同額のバーチャルマネーに変換する。ウェブマネー、ビットキャッシュ、NTT コミュニケーションズのチョコム、日本信販のデジコイン、C チェック、QQQ カード、クオ、全て同種のマイクロペイメント方式である。

ISP アカウントによるマイクロペイメント： NTT コミュニケーションズは２００４年１０月に CoDen と呼ばれるマイクロペイメント・ソリューションを開始した。CoDen サービスは月々の電話料金請求書を利用した代理収納サービスである。CoDen サービスには A, B, C, D, E の５種類のビジネス・タイプがある。ビジネス・タイプは代理収納の種別により決まる。２００５年５月までには CoDen サービスの利用者は少なくとも３万人存在した。ニフティ、@ペイ、ビッグローブの E マイキャッシュ、OCN のペイオン、ソネットのスマッシュも似たような決済システムである。

IC カードベースのシステム: 日本のマイクロペイメント･システムのうち､ドコモの i-mode 携帯電話の普及が特筆に値する。I モード利用者は４２００万人以上に達している。I モードは既にユーザー認証や端末認証、データ利用に対する利用料金支払いサービスが備わっていたため、音楽ダウンロードなどの著作権保護やコンテンツ請求を実装することは比較的容易であった。故に i モードは携帯電話機能と IC カード決済を組み合わせたマイクロペイメント基盤を構築している。i モードを利用した実際のビジネス取引として、コンテンツ購入で約１５００億円、電子商取引で数千億円の取引が報告されている。しかし、２００４年１０月現在では他社も競合するサービスを提供しているので注意が必要である。

またフェリカと呼ばれる技術プラットフォームを利用したエディとスイカが主流になっている。エディでは、最近エディ機能を搭載した携帯電話が提供されている。エディ機能を搭載したスマートカードや携帯電話の数は７４０万台に達し、エディが利用できる店舗の数は１万４千軒に上ると報告されている(２００５年１月現在)。

スイカは JR 東日本による非接触型の電車定期券として始まったが、現在は電子マネーとしてその機能を大幅に拡大している。電子マネーの利便性に加え、クレジットカード、社員証、学生証等との共用も進んでいる。スイカの発行枚数はおよそ８３０万枚と言われており、スイカが使える店舗数は３万５千軒台と報告されている。（２００４年３月現在）

ピタパ及び JCB のクイックペイも似たような決済ツールである。

その他のマイクロペイメント：二種類のマイクロペイメントが存在する。上記に述べた三種類のマイクロペイメント以外にインターネットバンキング及びクレジットカードソリューションがある。

■　台湾

遊遊カード（ユーユーカード）：２００４年に台北市政府はそれまで地下鉄料金支払いに使えるカードであった遊遊カードをタクシーや公共バスなど他の交通機関にも適用を広げた。このカードは何度もチャージでき、２００４年末には発行枚数が百万枚を超えた。遊遊カードは４つの銀行と提携する予定であり、i-Cash としても利用できる IC カード規格を採用することも検討しているかもしれない。遊遊カードが IC カードになれば、その応用範囲はより広くなることが予想される。

金融 IC カード：台湾で人気のある、IC カードベースの統合決済ツールはその応用範囲が国内アプリケーションに限られている。このカードは台湾国内の全銀行が発行しており発行枚数は４０万枚に達している。その数は今後１５０万枚に増える見通しである。しかし、いくつかの銀行を除き、その応用範囲は国内取引に限られている。また数少ない国外でも利用できるカードについても利用可能な国数、店舗数、設置 ATM 数は限られている。

E コイン：玉山銀行（Yu-San Bank）はティーンエイジャーの利用制限や取引処理コストといった利用障壁を克服するために電子コイン型マイクロペイメントを導入した。２００４年までに３０万加入者を獲得し、そのうち２１万人がアクティブ・ユーザーである。マイクロペイメントの利用は玉山銀行のメンバー店での国内取引に限られている。

I キャッシュ：このマイクロペイメント・ソリューションは大手コンビニエンス・ストア（セブンイレブン）が提供している。I キャッシュはプリペイド型で繰り返しチャージ可能な、IC カードに似た仮想カードである。客はコンビニの実店舗にてカードを購入、チャージする必要がある。取引手数料は i キャッシュ口座から出金があったときのみ請求される。２００４年末までには１７００万枚の i キャッシュ・カードが発行された。

ペイパル(Paypal)：イーベイ(eBay)はすべての入札会員に対してプリペイド型デジタル電子財布を提供している。２００４年末までには３５万人のユーザーがペイパルを利用して応札費用を支払った。

■　韓国

電話料金請求書によるペイメントーテレディット：テレディットマイクロペイメントはダナル社により運営されている。ダナル社は５３％のマーケットシェアを達成しており、韓国最大である。加入しているウェブサイトは６０００サイトにのぼり、利用料金は、２０億ウォンまで上昇している。同様のマイクロペイメントに e-コインがあり、電話料金とのまとめ請求のマーケットでのシェアは約２０％となっている。

■　欧州

口座引き落とし：ドイツには振り込みや自動引き落としが５～２０ユーロセントの手数料

で出来る効率的なバンキングシステムがある。(大企業向けには、5 ユーロセント以下にさえなる) その他の欧州各国でも口座引き落としは、主流の決済方式である。多くの人々は追加料金無しで振り込みが出来る定額料金を使っている。従って振り込みがマイクロペイメントの用途に使われており、例えば通常の自動引き落としによる振込みで私は８９ユーロセントを請求されたし、eBay での購入に対し、私の妻は１～５ユーロを振り込んでいる。
ヨーロッパ中に振込みをする事が可能であるが、(プロジェクト SEPA　－シングル・ヨーロッパ・ペイメント・エリアの略) クロスボーダー振込みの場合、料金は高くなるだろう。 ゲルドカルテやペイセーフカードが一般的なソリューションである。
デビット／クレジットカードベースのシステム：基本的にこの種のマイクロペイメントはプリペイドソリューションである。ファーストゲートクリック＆バイ及びインフィンのマイクロペイメントが典型例である。
電話料金請求書によるマイクロペイメント: 電話会社に関連するサービスが、電話料金の請求書にまとめて請求される（どんなサービスでも)。 更に口座引き落としの形で一定額（例えば１０ユーロ）をチャージするインターネットペイメント（ファーストゲートのクリックアンドペイ等）のアグリゲーターも存在する。これにより、インターネットショップでの小額の買い物ができる。しかしこれらのペイメントプロバイダーは手数料が高く(殆どの場合１０％以上）ニッチ市場でしかその魅力を発揮できていない。T ペイ、モビペイ、Dao ペイは類似のマイクロペイメントである。Dao ペイはクロスボーダー決済が可能である。電話加入者であればこの決済方法が使える。

■　米国

e メールベースの決済システム：ペイパル／X.com やフルーズ等は送信者のクレジットカードもしくは銀行口座に請求するか、小切手やマネーオーダーでプリペイドされた口座から支払いを差し引く。ペイパルの受信者は小切手で支払いを受領するか、もしくは銀行口座に直接振り込みとなる。フルーズの受信者は支払われたものを特定のオンライン商店で使用することもできる。
Q パス：もう一つの財布型システムであり、購入者のクレジットカードに購入額をまとめて請求し、他のクレジットベースのオンラインマイクロペイメントシステムにあるような取引毎の店主の負担をある程度軽減するものである。ニューヨークタイムズの貧窮者救済基金はオンライン上での寄付を受け付ける為に１９９９年１１月に Q パスを利用した。
サイバーコイン：サイバーキャッシュが開発したマイクロペイメントシステム。コンセントリックネットワークのような ISP とのパートナーシップを通じてサイバーキャッシュはマイクロペイメントを含むその他の e コマースパッケージを提供できるかもしれない。
ミリセント：DEC により導入されたマイクロペイメントシステムで、現在はコンパックが所有。１０００円から入れられる財布で、５円（当時およそ０．０４ドル）という小額の決済まで取り扱う。
E ゴールド：手ごろな料金で「E メタル」(金、銀、プラチナ、パラジウム）を購入しアカ

ウントに保有する事により、他のアカウント保有者と、どんな規模の電子決済でも可能。
ビートークン：Bee-Token.com で購入する仮想通貨。ビートークン通貨方式に参加しているウェブサイトで使用できる。各トークンは０．１０ドルに相当する。写真、サイドストーリー、音楽、白書、エッセー、星占い、寄付、その他インターネット販売商品等の支払いに使い勝手がよい。
電話請求書・ISP アカウントによるマイクロペイメント：
Trivnet の WiSP マーチャントサーバーは、購入者が財布をダウンロードせずに、消費者の ISP アカウントに対してマイクロペイメントを請求する。E コマースソリューションはクレジットカードによりまだ使用されており、M コマースソリューションはモバイル ISP アカウントで請求を行っている。
IPIN も購入者の ISP アカウントにデジタルコンテンツ購入の請求を行う。１９９９年９月に、デジタルミュージック会社数社とオンラインミュージックコンテンツに対するウェブベースの決済を取り扱う契約を締結した。

決済がクロスボーダーにまで広がった際に直面する問題

上記で述べたマイクロペイメントシステムの多くは国内取引にのみ利用可能である。国内から、クロスボーダーへと決済が広がったら、我々はどのような課題に直面することになるのか？図１はマイクロペイメントから国際マイクロペイメント（IMP）になった場合のシステムアーキテクチャーを示す。日本とドイツ間のクロスボーダー取引を例に取っている。この図は直面する課題を考えるにあたっての一助となる。ここでは、IMP システムに６種の役割が存在している。即ち販売者（コンテンツプロバイダー)、ユーザー、決済サービスプロバイダー（PSP)、IMP センター、ADR 組織、そして政府である。

マイクロペイメントサービスの大半は MSP（マイクロペイメントサービス事業者)により提供されている。　MSP の役割は支払われた金額を仲介者として中継することである。即ち、支払われた金額は二段階に分け、振替えられる。消費者から MSP に対する支払いと、MSP から店/事業主に対する支払いである。 各段階に関連する実際の代金振替は適用される取引に個別に対応されることもある。どのような場合でも、MSP の役割は二つに分割される。一つは消費者から代金を収納する役割であり、もう一つは店主/事業主に代金を仕向ける役割である。この役割モデルはマイクロペイメントにだけ適用されるモデルではなく、クレジットカードを利用した決済にも適用されているモデルである。クレジットカードをベースとした決済の場合、消費者に対応するサービス提供者はカード発行者であり、店側に対応するサービス提供者は加盟店契約会社である。国際カードのブランドの下、これらサービスプロバイダーは協業して信用決済サービスを行う。同様のビジネスモデルをグローバル規模のマイクロペイメントサービスに適用可能であろう。これは消費者に対応するマイクロペイメントサービス事業者と国外の店舗に対応するマイクロペイメントサービス事業者が協業して決済サービスを提供し、国境を越えた e コマースを行うことが出来る、とい

う意味である。二つのタイプのマイクロペイメントサービス事業者間で、相互運用に関する合意形成が必要であろう。そのような合意内容は IMP の国際連携の（基盤）機能も果たす。

概してクロスボーダーに決済を広げる際に直面する課題として、複数システムの統合、ビジネス上の課題、税法、国ごとの法令の違い、取引上の紛争の取扱い、セキュリティや消費者の信用等がある。これらは以下に詳述する。

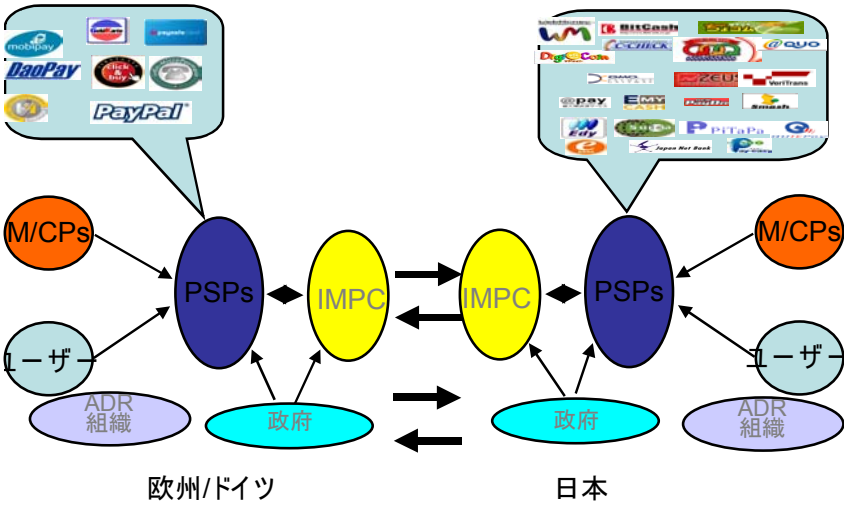

図１：IMP における相互作用モデル

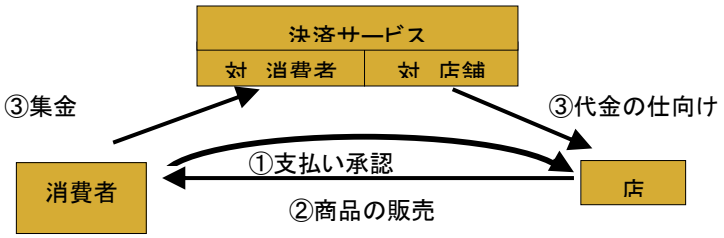

図２：決済サービス役割モデル

■　システム統合の課題 (複数のシステム、複数の技術仕様)

マイクロペイメントがクロスボーダー取引に適用される前に、国内での統合された決済プラットフォームが整備されていなければならない。システムのインターフェースに対する共通プロトコルの存在が複数のマイクロペイメントシステムの統合に必須である。残念ながら現状では殆どのマイクロペイメントは共通のシステムインターフェースを有していない。この現象はクライアント装置、ペイメントワークフロー、もしくはシステムインターフェースのケースにおいて典型的である。技術的な課題が最も難しい部分ではないが、それでも対処が必要である。

IMP に対する様々な技術やビジネスモデルが台北会議にて確認された。例えばスイカやエディのような、金額をチャージしておけるカードをベースとした著名なマイクロペイメントサービスへの言及があった。これらのマイクロペイメントの形態は地域、国内の環境では成功しているが、国際間のスキームには適さないかもしれない。チャージカードベースのマイクロペイメントは、消費者側と店舗側双方が同じ技術を使わねばならない為、ローカル市場では大した問題にはならないかもしれないが、国際市場でグローバルに受入れられるには、著しい障害となるだろう。故に初期段階において IMP を促進する為にはマイクロペイメント技術の一部は、IMP から外す必要があるだろう。

■　ビジネス上の懸念（コスト、マーケティング）

新しいアイディアを実現するには、常にモチベーションが成功への鍵となる。その現象はビジネスとしての意味合いにおいてより顕著である。従って、クロスボーダー取引の取引量や市場の需要は、多くの場合、協業パートナーの最大の関心事となる。現在までクロスボーダー取引の需要がどの位大きく、またどの程度の利益を生むものかを示す客観的な調査は行われていない。IMP（国際マイクロペイメント）の緊急性や重要性を支持するような実データは無いものの、多くのウェブサイトの運営状況を見るとユーザーの２０％が海外からである。一方インターネット上の商取引には国境が無い為、e コマースの発展に伴い IMP に対する需要が大きくなる事が予見される。業者側からの主な懸念は処理コストである。採用されたマイクロペイメントが国内で既に稼動している場合、(国際マイクロペイメントの）コストが増加し過ぎない事が望まれる。業者にとって、うまく機能するクロスボーダーペイメントにより、彼らの市場を海外にまで広げることができるなら、よい動機付けになる。従い e コマースの成長により、IMP は更に重要になって行くだろう。現行の e コマースでは国際取引であっても、クレジットベースの決済サービスが広く普及している。故に、e コマースに適用可能などんなペイメントサービスもクレジットベースの決済と同レベルの競合力をもって提供される必要がある。それが出来なければクリティカルマスを超える

事は難しいだろう。概して、事業者は直接売上に上乗せする分に対してのオペレーションコストを評価するものである。ここでのコストは、不良債権による損失、追加のハードウェア、ソフトウェアの設定、決済事業者との売上配分等が含まれる。

■　税法（付加価値税の違いと各国の課税方針の違い）

世界の殆どの地域では取引毎に付加価値税（VAT）が課せられるのが普通である。各国の税率の違いが著しい。VAT はアジア各国では５％が一般的だが、ヨーロッパ、アメリカではしばしば１０％以上の税率が見られる。異なる税率により、各国の顧客それぞれに対する商品価格が変動することになる。即ち国毎に異なる価格表がある事に対して、顧客側も店舗側も、明確且つ共通の理解を持つ必要がある事を意味する。さもなくば、取引に対する多くの紛争が発生する可能性がある。更に、同じ地域であっても、源泉税の方針も各国毎に異なる。（例：アジア）この問題は代行収納者と店舗間の売上配分プロセスを更に複雑にしてしまう。その上、銀行間での異なる通貨の転換コストを可能な限り削減する事が非常に重要である。これは代行収納者と店舗の間での最終売上配分に影響が出る為である。取引手数料が小口規模である IMP においてその状況は更に顕著になる。言い換えれば、もし代行収納手数料が保持されれば、店舗の利益が減り、それにより店舗が IMP を採用する意欲を削がれてしまうからである。

■　各国の法令の違い　(各国における運営事業者への制約、銀行法、消費者保護法)

上記に述べた税法上の課題に加え、各国の法令の違いも問題である。例えばドイツの"Fernabsatzrichtlinie"（連邦遠隔販売規則)は（確固たる理由がなくても）顧客が契約後２週間以内であれば契約を無効にできる権利を保証している。関連する規則はアジアの各国にもあり、契約後１週間以内であれば取り消せる、というのが一般的である。このような違いは明らかに店舗、顧客それぞれにとって、運営コストの増加や取引紛争の問題の原因となるだろう。その上、銀行法における決済ベンダーの免許制限も国によって違うかもしれない。免許によりベンダーは、交換所の役割は果たせるかもしれないが、法的な決済ベンダーとして許可されないということもある。これら全ての問題の解決策や代替案が、IMP にとっての差し迫った懸念となっている。

■　取引上の紛争の取扱い（問合せや処理を効率よく信頼できる筋を使って行う方法）

取引上の紛争は通常関連する法令規則に従って取り扱われるが、ADR（裁判外紛争処理）は例外的なケースを取り扱う為の備えである。例えば支払いの認証、認可がきちんと行われたにも拘わらず、顧客が期待した商品やサービスを受けられなかった場合。もしくは代金を支払った後で受け取った品物に満足しなかった場合。または思っていた金額とは違う金額で請求が来た場合、等々。取引上の紛争は常に存在するので、IMP の成長を促進する為には便利な仕組みと信頼のおける組織が不可欠である。例えユーザーの損失（支払額の）が

それほど高額はでないとしても。

■ **セキュリティと消費者からの信頼（異なるペイメントルールに対するセキュリティ要件、信頼度の高さ、運営事業者の信用状態、ユーザーのリカバリー）**

セキュリティと消費者からの信頼の問題の大部分は人間の心理的な受け止め方によるものである。法律やセキュリティの規則に準拠した一般的なサービスがより多くのユーザーを惹きつける一方で、過去の経験により顧客はネットワーク上の取引には常にリスクがあると気づいてしまう。顧客に対し、相応の注意義務が常に果たされている事を再度保証される必要がある。　幸運なことに、取引リスクは取引額に比例するので、この問題はそれほど重大ではないだろう。しかしながら、開かれた社会におけるプライバシーは匿名で行なう取引システムを必要とし、これはデジタルコンテンツサービスの取引について特に必要とされる。

eコマースはボーダーレスとはいえ､ほとんどのeコマースは今日国境内におさまっている。最新の統計によると、ドイツではｅコマースの 90%超が国内取引とのことである。理由の一つは、ドイツ語の使用が海外のショップで一般的でないこと、そして（おそらくより重要な）もう一つの理由は、ドイツ国民がドイツのショップを海外のショップより信頼しているということであろう。

ゆえに、マイクロペイメントシステムの開発を促進するための必要事項は以下の点である。

- 追加的な加入等をせずに誰もが利用ができること
- 皆の支払経験を基にしていること
- 取引手数料が小さいこと

IMP 問題解決に向けての世界の現状

実際世界各国政府の多くは ｅ コマースの発展に関心があり、特に金融ビジネスと税制の観点から興味をもっている。eコマースが広範囲に伸びている国においてはその現象はより顕著である。しかしながら、IMP における努力や具体的に採用された成果等は未だ十分とはいえない。

■ システム統合

● 台湾

現在、台湾では、少なくとも 17 のインターネット取引向けマイクロペイメントシステムが稼動している。システム統合とマーケティング調査を通してマイクロペイメントシステム数を減らすことは、すべてのペイメント事業者の常識となっている。
システム統合の前に、クライアント側の環境またはツールを調査しなければならない。たとえば、物理的なカードをベースにしたマイクロペイメントシステムを統合するためには、互換性のあるカード読み取り装置とシステムプラットフォームが必要である。

３G USIM カードのソリューションプランは政府主導のもと、進展してきている。しかし、現在のインターネット上でのマイクロペイメントシステムの進化は、いまだ統合に向う傾向を見せてはいない。電話料金少額課金システムは除き、ほとんどのシステムで取引全体の流れに違いがある。

顧客ベースの原動力の観点からすると、電話料金請求書によるマイクロペイメントシステムとオークションサイト eBay のペイパルシステムが、クロスボーダーペイメントに拡大しても優位､と思われる。台湾の顧客ベースで 95%の網羅率に達する電話料金請求書による統合マイクロペイメントシステムは、中華電信によって 2005 年に稼動を開始している。われわれの経験からすると、電話料金支払に使用可能な一つの IMP に統合すれば、技術的な問題は大きくなく、むしろ税制と規制が大きな問題である。

- 日本

システム統合の観点から、日本は諸外国より良い。スマートカードをベースにしたマイクロペイメントでは、共通のプラットフォーム、Felica が日本のマイクロペイメントシステム市場のほとんどを制覇している。有利な環境として日本政府が共通のシステムインターフェースの設置を命じていることが理由である。　一方、他のマイクロペイメントシステムはたとえば NTT コミュニケーションズの CoDen サービスのように、システム統合に独自のビジネスポリシーをもっている。

- ドイツ

マイクロペイメントシステムは他の国より少ない。この状況は、似たような状況ではクレジットカードでの支払になれているという、ヨーロッパの異なった消費者行動に関係しているだろう。ゆえに、多様なマイクロペイメントシステムの統合ではなく、消費者の信頼を高める為の共通の信頼性あるインフラ構築が、おそらく最優先事項になる。これは、北米の場合にも当てはまる。

■ ビジネス上の問題

IMP の場合、取引額と投資費用の面で、各国間に大きな違いはない。消費者のニーズの研究調査が進展するだろう。しかし、台湾における韓国ファンや日本ファンの存在を考えると、IMP 市場に強い需要が見込まれる。この現象は、共通のアジアの伝統文化を持つ国々で特に明らかである。

■ 税法

e コマースについて、付加価値税が一部の国々のサイバー入札で課税され始めているものの、税は低額化簡潔化の傾向にある。台湾で e コマースが非常に奨励されているが、それでも基本的な付加価値税を避けることは困難である。

源泉徴収税は、将来、デジタルコンテンツ取引に適用可能な IMP には課税されないことが予想される。

日本では、税法が台湾と似ている。台湾と韓国と同じく５％の付加価値税が基本税である。それゆえ、アジア諸国間の差異は、欧米の場合より小さい。この状況は、アジアにおける IMP 具現化を促進するだろう。

■ 法令の違いの縮小

各国間の法制の違いは、消費者保護法、銀行法における決済ベンダーの送金取扱いや営業上の制約に及ぶ。この問題への対応は IMP ワーキンググループの重要な目標である。

■ 取引上の紛争の処理

ADR は、いつも e コマースの主要問題である。IMP だけでなく他のインターネット取引においても同じである。幸運なことに、ADR の連携は近年大きな進展を見せている。地域、さらには地球規模で、BBB on-line や ECOM や SOSA 等のような他の組織とのジョイントベンチャーを通して、連携組織が設立されている。将来、世界にもっと ADR 組織が増えてくるだろう。

■ セキュリティと消費者の信頼

現在、128 ビットトリプル DES 暗号化アルゴリズムを搭載した、セキュアソケットレイヤー（SSL）とよばれる共通の安全取引プロトコルが、インターネット支払において広く採用されている。このプロトコルは、IMP にも適用できる。それでも個人のプライバシーとデータ保護は IMP において主要な問題である。台湾においては、個人のプライバシーデータの保護は法律レベルにまで昇華している。私たちは、関連法令が IMP の進展を促進すると考える。IMP のシステム設計において、注文の情報とプライバシーにかかわる決済の情報が、適切な関係者によって別々に保存され、安全に保護されることを確認しておくことが大変重要である。一方、顧客保護に重点をおいたサービス提供者による取引・決済ポリシーは、特にヨーロッパにおいて消費者の信頼を高める上で積極的に作用する。

提言

明らかに、インターネット決済で生じる問題のほとんどが、IMP においても解決されなければならない。IMP の場合個々の取引額が少額であるため一部の問題はそれほど重要でないにしろ、取引のパフォーマンス、取引ごとの費用と利便性における要件等、もっと深刻な問題もあるだろう。ビジネスの領域を見定め、広く使用されているマイクロペイメントシステムとサービスプロバイダーを相互連結することで、段階的な実施が可能になると私達は考える。例えば、異なった国々のベンダーたとえば中華電信と韓国または日本のベンダー間で小規模なフィールドテストをしてモデルの実行可能性を確かめるべきであろう。
にもかかわらず、IMP だけでは大規模ビジネスに成長せず、サービスプロバイダー間の接続性を確認するための補助金助成は困難であるという問題がある。それゆえ、IMP は「困難な」ビジネスでありデジタルコンテンツのような特定の取引のみ容易に成功するだろう。

マイクロペイメントシステムの具現化は、既存の大手企業（銀行または電気通信会社等）によって推進される場合、成功率が高い。しかし、これでは十分ではないと思われる。IMP を実マーケットで計画するときは以下の内容を考慮すべきである。

－ 現実に使用されてもキラーアプリケーションになるとは限らない、なぜなら人は慣れ

親しんだ支払様式を好むからである。なじみのある取引行動を IMP の実施にあたって軽視してはならない。
－　高価で特別な機器（カード読取装置等）は、広く利用される支払システムを目指すとき障壁となる。
－　IMP の利用が便利である場合（駐車場にいて、十分に硬貨の持ち合わせがないときなど）であっても、購入の前にカードに金銭を補充しておかなければ、IMP システムを利用できない。ゆえに、使いやすい電子財布と金銭のチャージをするためのユビキタス環境の両方が、カードベースのマイクロペイメントに不可欠である。
－　消費者の疑念の除去とショップ側のリスク軽減が、IMP の確立にとって 2 つの重要な要素となる。

二つのマイクロペイメントシステムが一つの適用領域の中に共存することはないことに注意したい。特に、政府が特定の適用領域に対し強制的にマイクロペイメントを発行する場合には、主要な支払システムが構築されるだろう。故に、政府はどの道を行くのか明示することが重要である。さもないと、大手加入者を抱える企業以外の企業は、自社の従業員か限られた顧客に小規模のインフラを構築することしかできなくなるという膠着状況に陥ってしまう。

■結論として、政府への提言を以下にまとめる。
法令と税制の国際格差を是正することが、IMP を提供するにあたっての優先事項であり、政府はこの点にもっと注目すべきである。
各国の法律や税制の違いを撤廃することは、国際マイクロペイメントを導入する前提条件であり、政府として更に注意を向ける必要がある。
IMP を推進するには、（政府による）奨励策と税制の公平性が必要である。
利便性があり信頼出来る国際決済システムの実現に向け、ADR の仕組み構築が、政府の後押しの下、早急に必要とされている。
各国においては、複数のマイクロペイメントシステムをクラス別に単一の決済基盤に統合することが大変重要であり、IMP を定着する上で不可欠と考える。

■特筆すべきこととして
１．政府は急増するサイバー犯罪との戦い、インターネット空間でのプライバシーの確保及び支払いや決済情報の保護推進に積極的な役割を担うべきである。
－　オンラインでの決済情報及び個人情報は官民双方の分野で厳密に保護されなくてはならない。
－　電子決済のアウトソーシングサービスは、今後の成長を確保するためにもセキュリティ手順の徹底が必要。
－　フィッシングやスキミングに代表されるサイバー犯罪に対する意識を高める目的で、

消費者教育を施す。
- 関連分野での法律や規制を現代の事情に合ったものに早急に改定する。

２．政府はオンライン及びオフラインでサービス提供するノンバンクによるマイクロペイメント事業への参入を許可し、規制的制限を撤廃すべきである。政府はまた、金融機関、通信業者、電子財布事業者を含む様々な電子決済サービス事業者間の対話を促進し、業界の安全且つシームレスな連携を確保するべきである。
- セキュリティ問題、個人情報及び情報管理に必要とされる最小限の要件
- 業界の自主規制及び決済ルール、紛争解決等、相互に受け入れられている商慣行
- 革新的なオンライン決済技術の適用とそれに関連する業務契約の設定
- 電子署名、銀行の預金方針問題等、現行の法整備の緩和に向けた検討意見を編纂

３．政府は急成長しているデジタルコンテンツやオンラインメディアサービスなど国境を越えた e コマースの取り組みを支援するべきである。国として国際マイクロペイメントのオンライン対応に向け、利便性・透明性・連携性が更に高められた環境の構築を牽引する役目が求められる。下記項目への対策の検討が要される。
- 政府及び民間の定期進捗会議の開催と対話を通して業界の最新ニーズを討議する。
- 規制の総合的な見直しにより、新技術に適応する。

各国の消費者保護、銀行業務、税制、仕切りに関する方針を調整し、クロスボーダーe コマースや電子決済を推進する。
- デジタル・コンテンツ業界及びオンライン・メディア業界は今日最も利用者が多い国際有料サービスをオンラインで提供していることから本業界に対して優遇策を施す。
- オンライン利用の革新的な電子決済ビジネスモデル開発を奨励し、市場への影響力を高める。
- 各種マイクロペイメントサービスに認定システムを導入し、内外のオンライン決済サービス事業者が提供するサービスの健全性を保証する。

４． 業界への提言
- 民間は業界横断的、且つ業際的な電子決済サービス機関の形成に努めることにより、m コマースや e コマースの振興策を政府に働きかけることが出来る。
- 斯様な業際的機関は商慣習に対し意見の一致を計り、最小限のセキュリティ要件を採用することにより、外国との統合の推進、特にモバイルを利用した決済の促進を図る。
- 電子決済業界の統合努力には、消費者の利便性と信頼を得ることを考慮し、共通のインターフェース構築も含まれなくてはならない。また、ADR、個人情報、セキュリティ等に対し、共通した方針を持つことも必要である。
- 業界は国により文化やビジネスに違いが存在することを認識し、ADR, 信頼マーク、エスクローなどの仕組みを通して、消費者の信頼を構築しなくてはならない。

安全な電子商取引

２００５年１０月１７日

議長：　Dr. Thorsten Demel

COO Global Technology

Deutsche Bank AG（ドイツ銀行）

1. はじめに

法的な拘束力を持つ取引を電子的な送受信で行えることが、電子商取引や電子政府が将来発展してゆくための要と考える。そしてなかでもインターネットによる支払いは極めて重要である。もちろん現在でも、電子政府ベースでの取引で契約に署名がなされればその取引は法的に拘束力を持つ。

GBDe はこれまで数年にわたって信用できる取引のできるインフラ(信用インフラ)の必要性についてたびたび述べてきた。そしてその間多くの政府が、インターネットにおける安全な ID とか認証の問題を取り上げてきており、GBDe としてこの動きを歓迎している。しかしながら、この動きはそれぞれの国単位のものである。　このような状況を踏まえて、GBDe は次の課題について国際的に議論して行くことで貢献を行うことを望んでいる。

―各国内の信用インフラについて、法制度面での調和と国際的なものとしての認識。
―民間と政府それぞれの信用インフラ融合での一般に使われるインフラの実現性。
―新しいインフラが一般に広く受け入れられる方法。

2. 信用インフラを目指しての種々のアプローチ（ケーススタディー）

ドイツ

ドイツはデジタル署名法を施行した最初の国で、1997 年に実施された。電子署名は手書きの署名と同様の効果をもつが、これにはスマートカードと専用の登録手続きが必要である。しかしながら、法制度のほうは PKI の導入という活路を見出すまでには至っていない。期待に反して、この 1997 年の署名法は逆に PKI 導入の障害となった：つまり、高度な安全基準のためマスマーケットを目指すにはこのシステムそのものの投資コストが高すぎた：そしてクリティカルマスは達成されなかった。2005 年 1 月にドイツ署名法の改正がとおり、これによって現在存在するたとえば銀行のカード（スマートカード）のインフラとのコンビネーションが可能となった。

当初ドイツ政府は信用インフラ施行を計画していなかった。しかし、パスポートや ID カードに IC チップが必要となってきて、パスポートや ID カードに PKI を組み入れることが決定した。このデジタルカードの所持が義務付けられそして認証に適合した：電子署名の証明書はカード所有者の費用負担でネットワークからダウンロードが可能である。ID カードの有効期限は 10 年であるから、2007 年にこのカードに切り替えると 2017 年まで有効となる。

官民共同の推進機関“ドイツ電子署名連盟”は 2002 年に設立され、現在国際的に使われている技術に拡大できるような技術基準を明確にする業務をになっている。ドイツ政府はこの電子署名連盟の成果をもって、2004 年に e カード推進を宣言している。電子署名と認証機能を持つデジタル ID やバンクカードが大規模に導入されればカード、認証、アプリケーションのクリティカルマスが創出されることが期待できる。

（同様なデジタル ID プロジェクトがフランス、英国、スペインなどで開始されている。そしてオランダやイタリアなどのほとんどのＥＵメンバー国がこのデジタル ID カードの導入について現在議論しているところである。）

フィンランド

フィンランドは 1999 年の 12 月にＥＵメンバー国として最初にデジタル ID を導入した。このデジタル ID は選択自由であり、これを採用する場合は 3 年で 40 ユーロがかかる。その結果､最初の 3 年で 300 万の人口があるのに 1 万 4 千枚しかカードは発行されていない。このカードは官民どちらでも使えるように作られている。特筆すべきは、このカードがオンラインバンキングや保険サービスにも使用できることである。しかし、アプリケーションの数は市民が喜んでこのデジタルパスポートにお金を支払うほどのレベルに達してはいない。そうこうしている間に銀行はこれに取って代わる認証の仕組みを導入した。
2005 年の 4 月で、6 万 3 千の市民が電子 ID カードや銀行のカードやモバイル SIM カードなどの証明を所持している。

ベルギー

ベルギーでは所有が義務付けられるデジタルパスポートの制度が 2003 年に導入された。デジタル化されていない ID の使用は 2009 年までは可能。デジタルパスポートの有効期間は 5 年間で、これは官民両方に使用できる。このデジタルパスポートはある資格(免許)を伴っている。この資格認定は官の責任であるが、民間機関によって運営されている。

ベルギーのように、エストニアやスエーデンでは義務化されたデジタル ID 制度が始まっている。エストニアではこのデジタル ID が全人口の半分にまで行き渡っている。

台湾

2002 年の署名法に基づき、台湾政府は電子署名カードとなる電子 ID カードを発行してい

る。このカードは電子政府にも使えるし、民間でも使用できる。電子商取引/電子政府のアプリケーションは 353 を超えている。内訳は G2G が 50、G2B が 15、G2C が 288 となっている。これらのアプリケーションのなかでも電子納税が一番魅力的なもので、2004 年には 10 万人、2005 年には 19 万 8 千人の人が利用している。2005 年の 9 月時点で、2 千 3 百万人の国民に対して 88 万 1 千枚のカードが配布されている。

促進の目的で 2004 年末までは電子署名カードは無料で発行されていた。2005 年の 1 月からは 1 枚あたり、275 台湾ドル（8.5 米ドル）となっている。

日本

日本ではこれまで政府のなかでそれぞれの部門の責任のもと別々な認証基盤が使用されていた。すなわち、中央官庁での認証基盤、地方自治体での認証基盤、ビジネスと政府間の認証基盤、政府と市民との間の認証基盤が存在した。2003 年末までに、これらのすべての部門の認証基盤がつながる認証ブリッジが全国で導入された。このような全国ベースでの認証基盤は世界でも一番早い導入である。

日本の一般市民向けの PKI カード（住基カード）はスマートカードベースとなっている。この電子署名カードは義務付けられてはいず、カード発行には 500 円(5 米ドル)がかかり、さらに PKI 機能をつけるにはさらに 500 円(5 米ドル)がかかる。このカードは導入から 2 年で 50 万枚以上を発行しており、これは全人口の 0.4%である。PKI 機能のついているものはこれよりも少ない数と見られる。

市民はこの電子署名カードを公での ID として活用できる。これはパスポートや運転免許を持たない市民にとっては役に立つものである。

他の国と比べて、日本はこの市民の使える PKI を民間の利用に開放していず、このために可能なアプリケーションが制限されている。従って、日本の市民 PKI カードは広範囲な信用基盤というよりはむしろ政府と市民とのコミュニケーションを安全なものにするためのものである。

マレーシア

2001 年 9 月にマレーシア政府は MyKad すなわちスマートカードベースの国民 ID カードを導入した。MyKad は官民のアプリケーションをひとつにまとめている。PKI の機能以外にこのカードは国籍 ID（入国時)、運転免許証、体の健康情報を持ち、電子財布としても使

用できる。この MyKad は現在の銀行口座とつないで ATM カードとしても使用できる。1997 と 1998 年のマレーシア署名法に基づき二つの認証付与機関が MyKad の認証を行っている。しかしながら、この認証はマレーシア以外では受け入れられていない。

MyKad は義務付けられいず、カード発行とその認証には 40RM(10 米ドル)の費用がかかるが、これまでの 4 年で 1000 万枚発行されている。マレーシア政府では 2005 年に人口の 50%の普及の計画である。

USA

米国では他の多くの国と同様に認証インフラの導入は民間セクターに委ねられている。米国にある大手の認証機関は個人と企業むけに認証を販売している。
認証のプロセスとコストは認証機関と認証を受ける側との合意に基づく。署名の法的な効力はケースごとに決められる。この署名の法的効力について高等裁判所からの明確な表明はまだない。

III. ケースから学んだこと

雑多な花園

以上の様々なケースから学んだことは、現在の状況は極めて異なっていることである。一方ではこの状況ゆえに世界ベースのクリティカルマスを獲得できる信用インフラ構築が s またげられていると嘆いている。そして他とはつながらないローカルな信用インフラとかあるいは信用インフラのまったく無い地方ができる結果となるリスクがある。他方では異なるソリューションでの競争が起これば最善の仕組みが広がるチャンスが増えるという意見もある。

現在導入されているものは政府の責任のもの

いろいろなアプローチの最終評価を現時点で下すのは早すぎる。しかしながら、事実として今日うまく行っている信用インフラは政府の責任によって運営されているものである。

米国のように、信用インフラの構築を完全に民間セクターにゆだねている国では、PKI はニッチな存在である。広範囲に法的な枠組みを与えることで法的な確実性を与えられる、しかしこれだけでは（ドイツの例から分かるように）民間のイニシャティブを引き出すには十分とは思えない。

広い範囲で受け入れられている信用インフラが存在しない理由は明らかでない。多くの人にとって証明するということは政府の基本的な機能であって、このようなサービスのために民間の会社に金を支払うことには慣れていないのであるという見方もある。しかし、新しいインフラを構築するにともなう高額な初期投資が民間の信用インフラへの主要な障害となっていると思われる。
(100 年前の電話会社インフラのように)信用インフラの提供者が第 2 フェーズで上場するまでは、新しい信用インフラの導入の初期には政府の参画を必要とするということは考えられなくはない。
それにもかかわらず、政府がこのインフラに責任を持つということでインフラが受け入れられることが保証されるものではない。電子署名カードを与えて市民がこれを使用し、アプリケーションが導入されてゆくのをも待っているのでは十分ではないことはフィンランドの例からも分かる。

ID カードは義務とするかそれとも自由選択とするか

（ベルギーのように）ID カードを義務化することでクリティカルマスの問題を克服する可能性があることは確かである。もし十分に浸透してゆけば、このインフラのうえでのアプリケーションが構築されてゆくことは大いにありうる。義務化には強い政治的なコミットメントが必要である、というのも、多くの市民がその利点がまだ見えていないうちに市民や納税者によってこの初期コストが支払われることになるからである。
電子署名の認証が含まれていなければ義務化された ID カードのコストは削減される。たとえば、ドイツではこのやり方を取っている。この場合、しかしながら、ID カードの使用はアップグレードされない限り限られたものとなる。アップグレードされていないカードの機能はビジネスの活用には不十分であり、義務化されない場合のようにアップグレードされたカードの数は少ないままとなるリスクがある。

義務化された ID カードは移行するのに長い時間がかかり、国の中での ID カードであるというコンセンサスが必要であることは明らかである。米国は英国の例でも分かるようにこれでは明らかに満足できない。（英国ではこのような ID が導入されるべきかどうか政治的な議論がなされている。）

政府のインフラの民間の使用

政府が運営している信用インフラを民間が使用する動きにはいろいろと異なったニュアンスがある。このニュアンスの隔たりの両端に日本とマレーシアがある。日本では民間の使用がみとめられていないし、一方マレーシアでは現存の銀行のカードをリプレースするほ

どである。
民間の企業にとり、政府の信用インフラの活用はきわめて大きなコスト削減になる。これは政府主導のインフラを信用する傾向のある人たちを顧客にもつ企業にとっては特に顕著である。ただし企業側はこのコスト削減効果と、信用インフラを外部に依頼し独立したブランドでなくなることによるインパクトとの比較が必要。また政府のインフラと民間によるアプリはデータ保護や公正な競争の観点からも明確に分けられねばならない。たとえば、政府の信用インフラは認証目的のみとして、すべてのデータは(民間の)アプリの中に保存するなど。
政府の運営するインフラを G2C のアプリに限定することは、市民にとってのインフラの価値を限定したものとし、さらに民間会社がこのインフラを活用することを妨げることになる。

IV. 提言

国際的な調和と国境を越えるという認識

現況は国ごとに極めて異なり雑多；ある国ではデジタルパスポートを義務付けており、それが電子署名にも活用でき、別の国ではこのようなカードを発行中あるいは計画中だが対象は希望者に対してのみ、さらに別の国ではこの信用インフラはまったく民間任せ。
国際標準があるから PKI を基礎的なものとしているのだが、現実には技術面でも法制度の面でも国ごとに多くの相違がある。その結果、ある国で法的に認められている信用インフラも別の国では価値がないと一般的に考えられている。
異なった解決法を競い合うことから最良のものが出きる可能性が増すことは疑う余地はない。ところがそんなことをしていると、ほかの地方や国と互換性のないシステムばかりとか、信用システムそのものをまったく持たないところばかりとなってしまう危険性が増えてゆく。
それゆえ GBDe ではこの信用インフラの開発にあたっては国際協調や国境を越えた認証確立のための政策の必要性を強く提言する。

クリティカルマス問題と政府の役割

インフラ計画実施にあたっては、一般的にクリティカルマス（最低限必要な量）の問題に直面する。ユーザーあたりの使用価格はそのシステムに参加する人の数による。この信用インフラシステムが成功するにはかなりの数のユーザーとアプリケーションが必要。デジタル ID カードを義務付けるような政府の強力な介入はクリティカルマス問題解決のひとつと考える。

しかし、政府の介入があるからといってその信用インフラが国民に受け入れられると保証されるものではない。
GBDe は信用インフラの実現にあたって政府が自らの役目とクリティカルマス問題解決戦略を明確にすることを提言する。そして民間側もこの戦略策定議論に参画することを提言する。

政府インフラの民間活用

民間の企業にとり、政府の信用インフラの活用はきわめて大きなコスト削減になる可能性がある。これは政府主導のインフラを信用する傾向のある人たちを顧客にもつ企業にとっては特に顕著である。ただし企業側はこのコスト削減効果と、信用インフラを外部に依頼し独立したブランドでなくなることによるインパクトとの比較が必要。また政府のインフラと民間によるアプリはデータ保護や公正な競争の観点からも明確に分けられねばならない。たとえば、政府の信用インフラは認証目的のみとして、すべてのデータは(民間の)アプリの中に保存するなど。
政府の運営するインフラを G2C のアプリに限定することは、市民にとってのインフラの価値を限定したものとし、さらに民間会社がこのインフラを活用することを妨げることになる。以上から、GBDe は政府の運営するインフラを民間の使用にも開放すべきと提言する。

民間の信用インフラ

多くの国では銀行や電話会社などによる（スマート）カードの民間の信用インフラが存在している。
GBDe は民間と政府のインフラとアプリに互換性を持たせるよう設計することを提言する。そうすれば民間のインフラを政府向け用途に活用できまたその逆も可能。

信用インフラのためのビジネスケース

信用インフラの開発には実現可能なビジネスケースが必須であるということをすべての利害関係者は認識すべき。この信用インフラが民間によって運営されたり、政府のインフラがあっても使用が義務付けられていなければ、顧客あるいは市民にその民間インフラのコストの一部を負担していただくことを説得しなければならない。顧客や市民は自分たちにとっての利益（金銭的なインセンティブや利便性など）を見出せばこれを活用するだろう。税金の申告のような政府の重要なアプリはキラーアプリとなる可能性がある。このようなキラーアプリこそがクリティカルマス達成へ重要な要素となる。
以上から GBDe は信用インフラの導入計画の要はすべての利害関係者のためのビジネスケ

ースであり、その作成を提言する。

電子大量書類/電子記録

安全な電子決済を見ると、電子商取引や電子政府での個人ユーザーの認証を行うやり方にほとんどの努力が割かれている。そして大量の書類を市民や顧客に電子的に送付したがっている企業や政府のほうにはあまり関心が寄せられていない。この手の書類は銀行口座情報や請求書や納税額評価通知などである。これらの記録はしばしば第三者に提示されることがある。それゆえ、このような記録が完全で認証されていることが保証されねばならない。しかしながら、(銀行口座記録のように) 顧客の要求で作成されるこのような大量の書類や記録に個人の署名が使われるのは適切ではない。
以上から GBDe は大量の電子書類についてはもっと簡単に配布でき、すべての政府機関に認識されるよう電子大量書類への要求を定めるように法的な枠組みの調整を提言する。

以上

サイバーセキュリティ

２００５年１０月１７日

議長：　藤原　武平太

理事長

独立行政法人　情報処理推進機構

1. はじめに

インターネットは、情報通信技術の偉大な進化の賜物であり、個人、家庭、学校、地方自治体から政府、公共機関、法人に至るまで、我々人類にとって、今や必要不可欠なインフラである。

インターネットという考え方は、友人や仲間うちでの善意の通信手段として、研究者達の間で始められた。従い、疑いを知らない側面がある。インターネットが商用的に運用されるようになると、善意に基づく性格は脆弱性へと転化した。インターネットは低コストの即時的通信を可能にし、e コマースに多大な貢献をするが、その匿名性の性格は事業環境に対しては不確実性として機能する。インターネット通信は、ブロードバンドや無線接続によって拡大し、様々な、かつ重大な脅威が急速に浮上している。脅威は、ウイルス、ワーム、悪質な攻撃から詐欺、そしてインターネットの乱用や不正利用など様々である。従って、インターネットのセキュリティ問題は、ネットワーク通信のみならず、インターネット上で行われる様々な社会的経済的活動の障害になってしまう。広範に普及したインターネット・ネットワークの利益を享受する一方で、我々は、異なったふるまいをする者に対するインターネットの耐性を確立しなければならない。

様々な分野、地域、人々によって膨大な努力が重ねられてきた。我々は、こういった努力の結果を活用し、サイバー空間を安全かつ安定したものとするために我々が出来ることを強化し再構築しようとしている。GBDe は、過去の研究結果を踏まえ、有効と思われる対策を講ずることで、インターネットの利益を全面的に享受し、そのマイナス面を緩和するための活動に取組む。

サイバー・セキュリティ・イシュー・グループには、こういった論点を扱い、脅威とは何か、いかに社会に関わっているか、可能な緩和策や解決策は何か、といった研究が委ねられている。こうした議論は、国際的な IT ネットワーク社会へ貢献出来る建設的な提案や提言に結実するものと期待される。

2. インターネット・セキュリティにとっての主な脅威、不正、弱点

2.1 脆弱性

コンピュータ・ソフトウェアが複雑になり相互に連携してくると、些細なバグや欠陥などが、重大な脅威への導火線となる。こういった欠陥は、犠牲となったコンピュータの誤動作や有害な動き、あるいは、貴重なデータや情報の消失につながる。

オペレーティング・システムや、その他のシステム・ソフトウェアが広範に利用される状況では、ひとたびこういった脆弱性が発見され悪用されると、その脅威や起こり得る損害を大きなものにしてしまう。マイクロソフト社は、こうした重大な問題に真摯に取り組んでいる。UNIX や Linux のコンポーネントの脆弱性も報告されている。潜在的な脅威は、携帯電話、自動車や電気製品にも存在する。こういった全ての製品には、組込みソフトウェアが使われている。ユビキタスが実現しあらゆるものがネットワーク化されると、潜んでいる脆弱性とその悪用による同様の脅威が、現実のものとなってしまう。

昨今、我々が遺憾に思うことは、PC における脆弱性がほぼ毎日のように報告されていることであり、適切なパッチを適用する前に、非常に短時間の間に、それに対する攻撃が実

行に移されることである。このことがネットワークを脆弱で有害なものにしている。

2.2 ウイルス及びワーム

コンピュータ・ウイルスやワームは、ネットワークにごく一般的に存在するものとなった。それらの多くが、次のような所作を行うことにより、害を及ぼす。

1）コンピュータの誤動作や機能停止。
2）データや情報の消失。
3）メール送信により、自分自身のコピーをばらまいたり、ネットワーク装置・回線の容量を浪費すること。
4）トロイの木馬やゾンビと呼ばれるプログラムを埋め込み、人知れず重要な情報を送り出したり、指定の標的に向けて指定されたタイミングで攻撃を行わせたりすること。
5）膨大な数のインターネット・パケットを送信すること。

多くの場合、ウイルスやワームは、自身のコピーを、電子メール、共用ファイルや共有記憶装置、ウェブの閲覧、ファイルのダウンロードや転送、といった手段を用いてばらまく能力を備えている。ウイルスやワームの大半は、脆弱性を悪用する。多くの場合、トロイの木馬はバックドアを仕掛け、攻撃者（一般的にはハッカー又はクラッカーと呼ばれる）が標的となったコンピュータに入り込み、操ることを可能にする。

最近行われた IPA（日本の情報処理推進機構）の調査の結果では、2004 年、日本の回答者の 70%が、ウイルスに遭遇（発見／感染）した旨を報告している。同様の調査では、アメリカ、ドイツはそれぞれ 71%、韓国、オーストラリアは 62%、そして台湾は 37%という結果が報告されている。遭遇した回数がもっとも多いウイルスの名称は、W32/Netsky（ネットスカイ）、W32/Mydoom（マイドゥーム）、W32/Bagle（ベーグル）及び W32/Klez（クレッツ）である。これらのウイルスは、調査が行われた国々に共通するものである。

2.3. ハッキング

ハッキングーある定義によればクラッキングーとは、通常、遠隔からコンピュータを攻撃することである。多くの場合、攻撃者は、アイデンティフィケーション（本人確認）やオーセンティケーション（認証）手続きを欺き、コンピュータにログオンする。攻撃者は、ブルート・フォース（総当り攻撃）、パスワード・ファイルを覗き見る、ソーシャル・エンジニアリング（人をだます話法・手法）など、様々な方法でパスワードを見つけ出す。そういった攻撃を自動化するツールの中には、インターネット上で入手可能なものがある。彼らは手動で、多くの場合はこうしたツールを駆使して、他人のコンピュータに侵入する。攻撃者がコンピュータを支配下に置くと、その犠牲となったコンピュータを新たな攻撃の足場として、ネットワークの乱用、悪用、DoS（サービス妨害）攻撃を行う。

このような場合、攻撃者はよく、再侵入のためのバックドア・プログラムを仕掛け、撤収する前にログを消去する。このようにして、不正な攻撃は次から次へと継続され、攻撃者はインターネットの世界で自由にふるまうことが出来る。

不正な攻撃は、情報はもとより、金銭的被害という形で、犠牲となるコンピュータに損害を及ぼす。その他の不正利用の例としては、ウェブ・ページの書き換えや、メッセージの発信や詐欺を行うことがある。別の悪質な利用方法には DoS（サービス妨害）攻撃があ

る。DoS 攻撃は、頻繁なネットワーク・アクセスや、有害なネットワーク・トラフィック（通信往来）を生成する。こういった攻撃は、通常、次の章で触れるトロイの木馬やボットによって行われる。特定のネットワーク・ノードーたとえば政府又は大企業といった有名な、あるいは重要な事業体のサーバやルータなどーに損害を与えようと思えば、彼らは何時でも易々とそれをやってのけられるのである。

2.4. トロイの木馬及びボット・ネット

何らかの形でインターネットに接続されているだけで、さまざまな方法で招かれざるプログラムがコンピュータにセットされる可能性がある。このようなプログラムは、トロイの木馬と呼ばれる。それは通常、ワームによって植え付けられる。トロイの木馬の中には、遠隔操作が可能なものがあり、ネットワーク攻撃を生成することが出来る。これは、一般的に、「ロボット」からの派生語で、ボットと呼ばれる。ボットは、インターネット上にある様々なコンピュータに寄生し、あらかじめプログラムされた、または遠隔から送信されてくるコマンドに従い、あるタイミングで、指定された対象にネットワーク攻撃を行う。ボットは情報を盗み出すエージェントとしても機能する。ボットの脅威は急速に深刻になってきている。

2.5. スパム・メール

スパム又はスパム・メールは、歓迎されない大量送信メールの総称である。スパムの大半は、広告やマーケティングを目的として、無差別に送りつけられる。多くの場合、スパムは好ましくない、あるいは不快な勧誘である。スパム・メールは途方もない数で、ビジネスの効率を阻害し、ネットワーク通信に悪影響を及ぼす。ビジネスマンは、スパム・メールを識別して削除するため、多くの時間を費やさなければならない。ネットワーク・インフラは、無意味なあるいは、有害なメールを扱うため用いられることとなる。ある統計では、一般的にビジネスマンが受け取るメールの半分以上がスパムである。その影響の強さによって、スパムはインターネット社会と、その通常のユーザとってのもうひとつの脅威となっている。

2.6. フィッシング

フィッシングは、インターネット世界に新たに出現した脅威である。典型的な例では、コンピュータ・ユーザは、あるメール、多くの場合スパムであるメールを受け取る。メールは、実存する会社組織を装った偽ウェブ・サイトー一般的には銀行やクレジット・カードの発行元などーへアクセスするよう求める。ユーザは、メールや偽ウェブ・ページによって誘導され、カード番号・口座番号等の識別番号と暗証番号・パスワードなどの個人の重要情報を渡してしまう。一旦そういった情報が犯罪者の手に渡ってしまうと、お金に関するあらゆる不正が即座にできてしまう。

これは、新たなタイプの脅威である。典型的な例では、犯人は、1）スパム・メール、2）URL やウェブ・ページの改竄若しくは偽装、3）ソーシャル・エンジニアリングを組み合わせた技法を用いる。

同様の詐欺が起きだしており、ファーミングと呼ばれている。ファーミングの場合には、対象者が導かれるのは正しい URL で実際のウェブ・サイトであるが、接続が捻じ曲げられ詐欺サイトに接続される。この場合、被害者は自分が行き着いたのが詐欺サイトだと認識することは不可能である。ファーミングはフィッシングと同類の詐欺だが、より巧みな手法のゆえにより深刻な問題である。

このことは、IT を活用し、知識の欠如や適切な注意の不足を悪用する、新手の犯罪の台頭の可能性を意味するものである。

2.7. 情報の盗難

一旦コンピュータが乗っ取られると、コンピュータ上のあらゆる情報は、パスワードや暗号によって適切に保護されていない限り、攻撃者の使用に委ねられてしまう。その多くが、プライバシーの侵害、秘密情報や企業秘密の盗難、金銭的損害、ビジネスの機会損失や、社会的災害の脅威をもたらす結果となる。もっと悪いケースになると、健康や命の危険や、日常社会生活の阻害をもたらすことにもなりかねない。

最近日本では、個人情報の盗難や、個人情報が危険に曝されるといった事件を立て続けに経験した。一つの事件で盗まれた ID の最大数は、ほぼ 500 万人分に上っている。コンビニエンス・ストア・チェーンでは、被害にあった会社が、情報が盗まれたと思われる顧客に対し、一人当たり 500 円（約 5 ドル）を、補償金あるいは謝罪の意味で支払った。この金額が 500 万人分の ID 盗難のケースに適用され、実質的に、同様のケースにおける標準的な水準と見なされることになった。このことは、大量の個人情報の喪失が破産を招きかねないことを意味することとなり、情報の盗難は、企業や公的機関にとって一躍重大な脅威となっている。

3. インターネットの脅威とリスクに対する対策活動

3.1. 脆弱性情報扱取扱い体制

オペレーティング・システム、通信プロトコル、アプリケーション等のソフトウェアにおける脆弱性は、毎日のように発見され、報告されている。こういった脆弱性は、悪意を持ったユーザがそれを悪用することを許してしまう。このような攻撃や悪用を防ぐためには、全てのユーザがパッチを当て、ソフトウェアを最新の状態にしておくことが肝要である。

ここにはいくつかの難問がある。まず初めに、脆弱性情報は、秘密に保たれなければならない。ソース・コードの所有者は、報告された脆弱性を確認し、ハッカーに知られる前にその対抗策を講じなければならない。つまり、これは、静かに、そして慎重に行われるフェーズである。

回避策やパッチの準備が整った時点で、脆弱性やその回避・修繕対策を公開し、全てのユーザが脆弱性を排除するための適切な措置を施すよう促す。こういった対策は、攻撃者が脆弱性を悪用する準備を整える前にすべてのユーザが防御を固められるように、直ちに、広範に渡って伝えられなければならない。ここは、様々な情報が行き交うにぎやかなフェ

ーズである。

全ての手続きは、注意深く、迅速に実施されなければならない。何かを極秘裏に行うことは、常に困難である。全てのエンド・ユーザに対し、速やかに正確で判りやすい情報を伝えることは、また違った困難性がある。

2003 年から 2004 年にかけて、こうした取組みは日本政府によって提起され、IPA のイニシアティブのもと、官民共同スキームとして構築された。この脆弱性情報扱い枠組みは「情報セキュリティ早期警戒パートナーシップ」と名付けられた。IPA は、脆弱性の発見・報告者の窓口として中核的役割を担い、処理過程の中心となっている。JPCERT/CC は IPA と協働し、コーディネータとして、対策の作成に当たってのベンダ間のコーディネータとしての役割を担っている。対策の公表に先立って、IPA、JPCERT/CC、発見者及びソフトウェア・ベンダ間で調整が行われなければならない。ベンダ団体やユーザ団体などのすべての関係機関が、その組織内に情報を広く広めるための取組みをする。その情報に関するデータベースが IPA と JPCERT/CC の協働により作成され公開された。当該データベースは、「JVN」、「JP ベンダー・ステータス・ノーツ（JP Vendor Status Notes）（http://jvn.jp/）」と呼ばれ、脆弱性に関する情報や、ベンダの活動内容を提供している。このデータベースは IPA と JPCERT/CC の共同チームによって運営・維持管理されている。

米国では、US-CERT が同様のサービスをそのウェブ・サイト http://www.kb.cert.org/vuls で提供している。

3.2. CSIRT 及び CSIRT ネットワーク

CSIRT は、「コンピュータ・セキュリティ・インシデント・レスポンス・チーム：（Computer Security Incident Response Team）」の略で、CERT 又は、コンピュータ・エマージェンシー・レスポンス・チームとも呼ばれる。ＣＳＩＲＴは、攻撃やウイルスによって生じたコンピュータやネットワークのトラブルに関する問い合わせに対し、調整、助言及び情報支援を行う非営利組織である。

CSIRT は通常、国ごと、あるいは教育機関、又は業界ごとといった異なる共同体ごとに設立され、緊急援助サービスを提供する。CSIRT の役割は、当初は問い合わせに対し助言するといった受身的なもの、事後的なものであった。次にはネットワーク監視といった同時・即時的なものになり、さらに発展して、「3.1.」に見たように、脆弱性情報取扱い体制といった予防的なものになってきている。

CSIRT は、国や経済圏ごとに設立された CSIRT 間にネットワークを形成し、情報交換や国際調整を行っている。APCERT は、アジア太平洋地域における 14 の経済圏の 17 の CSIRT を結ぶネットワークである。

CERT／CC（CERT コーディネーション・センタ：米国）、NISCC（ナショナル・インフラストラクチャー・セキュリティ協力センタ：英国）、JPCERT／CC（JPCERT コーディネーション・センタ：日本）は、脆弱性情報の取扱いに焦点を当てた別のホットラインを形成している。

CSIRT 及びその協働ネットワークは、ネットワークの脅威とリスクの緩和に寄与している。

3.3. インターナショナル・トラック・バック・ネットワーク

ハッカーの物理的ネットワーク拠点を追跡し、識別することは、攻撃の脅威及び危険性を緩和する有効な方法である。各 SCIRT や SOC（セキュリティ・オペレーション・センタ：Security Operation Center）が、ハッカーを追跡しハッキングの元を識別するための国際的なネットワークを形成している。

トラッキングプロセスはパケットと同じスピードで実施する必要があり、極めて困難な取組みである。パケットは国境を越えて流れるので、作業はまた国際的でなければならない。従い、この仕事は、できるだけ多くの国々の、ネットワーク・サービス提供事業者による協力によって支えられなければならない。

3.4. コモン・クライテリア

コモン・クライテリアは、IT 製品やそのシステムを評価し、認証を行うための国際的な枠組である。コモン・クライテリア(CC)は、国際規格として ISO／IEC15408 を規定している。CC 標準に基づく認証を希望するセキュリティ製品の開発者や製造者は、自社又は第三者によって定められた PP（プロテクション・プロファイル：Protection Profile）に整合する ST（セキュリティ・ターゲット：Security Target）を自社製品のセキュリティ仕様として設定することが求められる。評価され認証された製品は、そのセキュリティ適合レベルが保証される。認証のスキームには、7 つのセキュリティ適合レベルが規定されている。例えば、公的セクタによる調達では、EAL（評価保証レベル：Evaluation Assurance Level）は、通常 EAL3 又は EAL4 が求められる。このようにして、セキュリティ適合レベルの一般的な基準が定義され、保証されるわけである。CC は、セキュリティ・レベルの測定の基準として有効であり、システムインテグレーションや製品調達における共通評価基準を提供する。

3.5. ISMS（情報セキュリティ・マネジメント・システム：Information Security Management Systems）

ISO／IEC17799 は、情報セキュリティの管理枠組に係る国際的な基準である。本基準の原典は、英国基準 7799（以下 BS7799）である。BS7799 は、パート 1「ガイドライン」及びパート 2「要件」から成る。BS7799 パート 1 は 2000 年に国際化され、推奨最善策を規定する ISO／IEC17799 規格となった。BS7799 パート 2 は、ISO／IEC17799 に規定するコントロール（管理策）を用いて ISMS を構成、実装、維持するための仕様としての役を果たす。

ISO／IEC17799 において規定される情報セキュリティ・マネジメント・コントロールは、2005 年 6 月、ISO／IEC17799：2005 と改訂され、以下の分野を包含する：

1） 情報セキュリティ基本方針
2） 情報セキュリティの組織化
3） 資産の管理
4） 人的資源セキュリティ

5） 物理的及び環境的セキュリティ
6） 通信及び運用管理
7） アクセス制御
8） 情報システムの取得、開発及び保守
9） 情報セキュリティ事件・事故管理
10）事業継続管理
11）適合性

全体として、新バージョン(ISO／IEC17799:2005)は情報セキュリティ事件・事故管理の章一つと、従業員・契約社員・第三者下請けの管理に関するコントロールその他を追加した。今回の改訂は、企業における情報セキュリティガバナンスの重要性を強調している。

ISO／IEC17799 及び BS7799 パート 2 は、多くの先進国の国家基準として広く適用され、組織における情報セキュリティ管理枠組みの国際的なベース・ラインとして機能しており、通信や取引における国内・国際間の相互信頼の形成に寄与している。

ISMS 評価及び認証プログラムは、多くの国で導入されている。台湾政府は、民間及び公共セクタ双方に対し、国際基準の ISO17799（前 BS7799）を基準とする ISMS 基準を制定するよう奨励している。日本では、ISMS 評価及び認証プログラムは 2002 年に導入された。日本の認定機関である JIPDEC によれば、全世界で 1,100 以上の認定が交付されているとのことである。JIPDEC の直近の報告書では、上位 5 カ国は、日本（510）、英国（185）、インド（82）、台湾（45）、そしてドイツ（36）となっている。（2005 年 8 月の JIPDEC の最新発表では日本の認証取得企業数は 1014 に達している。）関連情報は、ISO17799 のニュース・サイト（http://www.iso17799-web.com）及びインターナショナル・ユーザーズ・グループ（http://www.xisec.com）から入手可能である。

ISO／IEC17799：2005 を基本とする ISMS は、2005 年の 11 月から 12 月ごろに、ISO／IEC27000 シリーズに再構成される予定である。再構成では、BS7799 パート 2 は ISMS 要件を規定する ISO／IEC27001 に、ISO／IEC17799：2005 は ISO／IEC27002 として、セキュリティ管理を提供する。リスク管理、評価および評価基準、ならびに実装ガイダンスは各々、27000 シリーズ内の独立した基準となる。

3.6. トラストマーク及びプライバシー・マーク

消費者信頼は、GBDe の活動の重要な関心事の一つであり、IT ネットワークにおける商行為の基本である。

1980 年、OECD（経済協力開発機構：Organization for Economic Co-operation and Development）は、プライバシー及び個人データの国際流通に関する保護ガイドライン（http://www1.oecd.org/publications/e-book/930211E.pdf）を発布した。1995 年発布の EU 指令では、個人情報の保護に係る取組みを求めている。この指令がきっかけで日、米、EU 間で個人情報の保護に関する議論が起こり対応策が話し合われた。それに基づく取決めは「セーフ・ハーバー」と呼ばれる。米国では、BBB 及びトラスト e がそれぞれプライバシーおよびサイトの信頼性に関する証明を発行している。日本では、1998 年にプライバシー・マークの認定枠組みが構築され実施に移された。

3.6.1. トラストマーク

トラストマークは、2000 年 9 月 26 日の GBDe 課題ワークショップにおいて議論された。セッションの資料では、その導入部で、以下のようにトラストマークに係る主な要件を定義している：

1） 適用可能性、特に中小企業にとっての。
2） 厳格な強制力。明瞭な監視・報告メカニズムを提供し、適用判断の中立性を保証すること。
3） 広く配布すること。また消費者が商用ウェブ・サイトを評価する時、容易にアクセス可能であること。
4） 全ての関係者との協議された上で策定すること。
5） トラストマークの誤用を回避するため、適切なセキュリティ対策を用いること。
6） GBDe の ADR 提言に沿った消費者救済メカニズムの提供。
7） 商業者は、GBDe 提言に沿った、オンライン商慣行、プライバシー保護、苦情処理に関する取扱い基準を、最低限用意すること。

トラストマークに関する最近の出来事としては、アジア・トラストマーク連盟(ATA)とグローバル・トラストマーク連盟(GTA)の設立がある。GTA の組織委員会は、2004 年 11 月、クアラルンプールの GBDe サミットでスタートした。

3.6.2. 日本におけるプライバシー・マーク・プログラム

日本で用いられる個人情報保護に関する主たるマーク（シール）システムは、JIPDEC（日本情報処理開発協会）が運営管理するプライバシー・マーク（P マーク）である。

P マークの認定基準は、JIS（日本工業規格）Q15001「個人情報保護に関するコンプライアンスプログラムの要求事項」への適合である。P マーク・プログラムの認定を希望する企業は、書類審査及び JIPDEC による実地調査を受け、当該企業体が、適合プログラムを制定し、当該基準に従い個人情報を扱っているかの確認をパスしなければならない。P マークの有効期間は僅か 2 年であり、P マークの所有者は、自社のウェブ・サイトに P マーク表示を継続するためには、2 年毎の書類審査及び実地調査にパスすることが必要である。この基準の要求条件は個人情報保護法による要件よりも厳密であるため、P マークは日本におけるユーザの信頼を集めている。

この認定サービスは 1998 年に開始され、当該マークの認定を受けた事業体の数は、2005 年 7 月現在で約 1,700 件である。個人情報保護法の 2005 年 4 月からの全面施行に伴い、個人情報保護に対する関心の高まりを背景に、P マークの認定を受けようとする企業の数は、急激な上昇を見せた。

P マーク・プログラムは、米国の BBB オンラインのプライバシー・シール・プログラムとの相互承認が可能であり、相互 BBBOL マークと呼ばれる。プライバシー・マークの認定企業は、BBB オンラインによる審査を受けることなく、追加手続きと、僅かな費用で相互 BBBOL マークの認定を受けることが出来る。

BBB オンラインのプライバシー・シール・プログラムによって認定された米国の企業は、自社のウェブ・サイトに相互承認マークを添付し、日本のオンライン顧客に提示することができる。

3.7. 政府及び民間セクタにおけるイニシアティブとその取組み

3.7.1. 台湾

1)　ウイルス、ワーム及び悪質な攻撃

ウイルス、ワーム、そして悪質な攻撃に打ち勝つため、台湾では 2003 年に刑法の改訂を行い、サイバー犯罪の章を追加した。そこでは、4 種の行為を犯罪の対象と見なしている：コンピュータ設備への不正アクセス、不法傍受、不法妨害、及びプログラマーによるこれら犯罪のためのハッカー・ツールの作成である。更に、その標的が政府施設である場合、当該犯罪者の刑期は、1.5 倍重科される。

トロイの木馬及びボット・ネットは、未だに管理課題として捉えられている。台湾政府は、官民双方のセクタに対し、ISMS 国際基準の ISO17799（BS7799）に基づいた内部基準を奨励している。さらに、サービス・プロバイダは一般消費者よりも強固なシステム・セキュリティ防御能力を持つべきであるとの考えから、台湾政府は、サービス・プロバイダの責任をより重く定めたモデル契約を規定した。

2)　フィッシング

インターネットのみならず、携帯電話における SMS（ショート・メッセージ）についても、フィッシング犯罪が悪化していることを受け、台湾政府は、電話通信サービス・プロバイダに対し、詐欺まがいのメッセージを除去する門番としての役目を担うことを要請した。台湾政府は、インターネット・サービス及び電話通信サービス・プロバイダの双方に対し、フィッシング犯罪者のオンライン追跡を支援する能力を備えることを求めるため、政府規定の改訂の準備も行っている。

それに加え台湾政府は、金融サービス・プロバイダに対し、自身の ATM システムの性能を向上させること、磁気カードからスマート IC カードに変更すること、及びカード 1 枚についての 1 回当りの取引金額を 3 万台湾ドルまでとすることを求めている。

3)　情報の盗難

情報の誤利用からユーザを保護するため、台湾政府は、「コンピュータ処理による個人データ保護法改正案」を上程し、2005 年 3 月より議会で討議中である。

同法案によれば、個人情報は、本人の名前、生年月日、個人識別番号及び個人を特定するために十分なその他の情報、と定義している。この法律は、当該データの検索／読み取り、複製（コピー）又は当該データの補足／訂正、当該データ処理／利用の停止、及び、当該データを削除する権利について規定している。重要な変更点には以下が含まれる：

1)　コンピュータ処理されたデータに限らず、個人に関するデータ処理の範囲の拡大。
2)　全ての事業体及び政府機関に適用可能であること。
3)　政府機関は、個人のデータを用いる際、どのような方法で収集されたデータであるかに関わらず、そのデータが属する個人にその旨を通知する。
4)　損害に係る合計補償金額を増額する。
5)　侵害行為を監督する政府機関の権限を強化する。
6)　法的援助を提供する非政府組織を立ち上げる。

3.7.2 マレーシア

マレーシアにおける NISER による情報セキュリティ・イニシアティブ：

1） NISER によって提供されるサービス

NISER（国家 ICT セキュリティ緊急対応センター：The National ICT Security and Emergency Response Center（www.niser.org.my）は、ナショナル・インフォメーション・テクノロジー・カウンシル（国家情報技術委員会：The National Information Technology Council: NITC）によって設立された、技術機関であり、２０００年 11 月よりその業務を開始した。NISER は、特に自国の情報通信技術（ICT）セキュリティ及びサイバー防衛活動を支援し、自国の重要なインフラを脅かす可能性を持つ侵入や不正サイバー行為に対する防衛を任務とする。

NISER によって提供される業務には、事故対応、コンピュータ・フォレンジックス、セキュリティ保証、セキュリティ管理及び実装が含まれる：

a. 事故対応

マレーシア・コンピュータ緊急対応チーム（MyCERT：www:mycert.org.my）は、マレーシアのインターネット・ユーザに対する事故対応業務を提供するため設立された。何年もの間、MyCERT は、不正侵入、DoS 攻撃、ハッキング、悪意的プログラムによる攻撃、電子メールの乱用、ソーシャル・エンジニアリングなど、実に多くの情報通信セキュリティ事象に対する支援を提供してきた。

b. コンピュータ・フォレンジックス

コンピュータ・フォレンジックスサービスは、データ・リカバリ業務及び政府機関や組織体に対する電子挙証サービスを提供する。コンピュータ・フォレンジックス業務には、法執行機関及び他の政府機関に対するトレーニングも含まれる。

c. セキュリティ保証

セキュリティ保証業務は、IT 製品及びそのシステムに対して信頼性評価サービスを提供すると共に、セキュリティシステム監査に携わっており、その対象には、人材管理情報システム、電子予算・財務計画システム及び年金のオンライン・ワークフロー環境（POWER）といった政府機関がある。

d. セキュリティ管理及び実装

セキュリティ管理及び実装業務は、情報セキュリティ管理システム（ISMS）や事業継続管理（BCM）を含め、マレーシアにおける情報セキュリティ基準の開発及び実装にたずさわっている。

2） 国際協力

国際的な舞台では、NISER（MyCERT）は、アジア太平洋地区コンピュータ緊急対応チーム（APCERT）のメンバーである。APCERT を通じ、NISER（MyCERT）は、オーストラリア、日本、シンガポール、タイ、フィリピン、インドネシア、香港、中国、台湾、ベトナム、ブルネイや大韓民国を含むアジア太平洋地区における他国の CERT と協力を行っている。

3.7.3. 韓国

韓国は、インターネット社会の実現や情報セキュリティにおいて、めざましい発展を遂げた。

1)　サイバー社会開発における政府のイニシアティブ

1995 年、韓国政府は、情報社会の促進（1999 年及び 2000 年に改訂）に対する基本法を制定した。同法を基に、1996 年には主軸となる構想が制定され、韓国の内閣府に情報促進委員会が設置された。この年、KISA（韓国情報保護振興院：Korea Information Security Agency）が設立され、KISA 内に設立された CERTCC-KR と共にその業務を開始した。

1999 年に策定されたサイバー・コリア 21 計画は、ブロードバンド・インフラを基本とする独創的な情報国家を目指したものである。2002 年、サイバー・コリア 21 計画は、e－コリア・ビジョン 2006 に改訂された。こうしたイニシアティブでは、3 つの目標が示されている：1）サイバー・テロリズムに対する回避／対応スキーム、2）セキュリティ技術及び人材開発、及び、3）健全かつ倫理的なサイバー空間の構築である。

e－コリア・ビジョン 2006 の構想は、中長期情報セキュリティ・マスター計画であるセキュア e－コリア 2002－2007 という新たなイニシアティブに軌道修正された。同イニシアティブにおいて設定された対象は：1）高度知識化情報社会インフラの強化、2）信頼のおける電子商取引を支える電子署名の促進、3）安全なサイバー環境のための暗号化アプリケーション基盤、4）個人情報の保護及びスパム・メールの制御、5）健全なサイバー世界の開発、及び、6）情報セキュリティ業界の戦略的育成、である。

組織的には複数の政府機関の集合であり、国家安全委員会が司令塔に位置し、国防省（軍部）に帰属する防衛情報センター、国家情報サービス（政府）に帰属する国立サイバー・セキュリティ・センター及び情報通信省（民間セクタ）に帰属する韓国情報保護振興院などにより構成される。

2)　深刻な数々の事故経験

韓国史上最大にして最も注目すべき韓国でのインシデントは、SQL Slammer Worm（スラマー・ワーム）が原因で 2003 年に発生したインターネット・ブラックアウトである。そのインターネット・ブラックアウトは、ユーザによるアクセスのピーク時にぶつかったため、韓国に致命的な損害をもたらし、経済的な損失も莫大なものとなった。この、世界中が知ることとなったインシデントに引き続き、Sobig（ソービッグ）、MS Blaster（ブラスター）や Sasser（サッサー）といった一般的なウイルスによる国民登録番号の盗難、スパム・メール、国立教育情報システムからの重要個人情報の漏洩、47 万人分のクレジット・カード番号と対応する ID 情報の盗難といったインシデントが発生した。

情報通信省は、インターネット・ブラックアウト以降に発生したサイバー攻撃を次のように分析している：1）システム攻撃から、ネットワーク・サービス攻撃へのパラダイム・シフト、2）複雑さや、悪意的要素の増加、及び 3）リード・タイムの短縮化及び被害の拡大の高速化。

3)　サイバー・セキュリティへの取り組み活動

韓国では、官民による協力体制が整えられ、その有効にしているように見える。公的セクタは、政治的なイニシアティブの装備、技術や人材開発を推進する組織の設立、及び情報セキュリティ業界の成長の活性化に積極的に取り組んでいる。一方民間セクタでは、

CERTCC-KR、CONCERT（CERT の共同体）及び ISAC を含む相互協力枠組みの構築に取組んでいる。KISA がこういった活動を先導している。様々なベンチャー企業が、独自開発の IT セキュリティ技術やその製品を提供し、重要な役目を担っている。

3.7.4. 日本

日本政府が 2003 年に導入した個人情報保護法は、2005 年 4 月全面的に施行された。同法では、一定数の個人情報を含む何らかの形のデータベースを所有する事業体は、組織的、人的、物理的、および技術的セキュリティ対策を講ずることを求めている。

プライバシー・マーク認定システムは、電子商取引やインターネットベースの取引の台頭に対応して、個人情報の適切な保護を保証することを目的に、1998 年に日本に導入された。数年の後、プライバシー・マークは、新たに導入された個人情報保護法によって、広く一般に知れ渡ることとなった。プライバシー・マーク制度は見直しが検討されており、完成時には、システムはさらに実効的となるであろう。そうなると、より国際的に整合した基準となるであろう。

日本には、情報処理各社に対する安全対策企業認定制度があった。この認定制度は、2002 年に ISMS 認証枠組に改組された。この変更は、情報セキュリティに係る国際的要件および今日的要求により適合するために行われた。

情報セキュリティ監査制度と呼ばれる、上述と類似の認証システムが、中小企業向けにより柔軟な枠組みを提供するため、2004 年に導入された。この監査システムの目的は、認証されたセキュリティ・レベルの保証を示すことに加え、セキュリティ管理の実践に対する支援や助言を提供することにある。

3.7.5. 米国

CERT／CC へのサイバー攻撃の報告が、近年、幾何学的に増加の一途を辿っている：2000 年には 21,756 件だったものが、2003 年には 137,529 件に拡大した。その攻撃の多くが、ボット又はトロイの木馬と呼ばれる自動化攻撃ツールによるもので、これらのツールは通常ワームによってばらまかれる。ウイルスやワームの大多数は、ネットワークの信頼や性能へ悪影響を及ぼす。最近出現しているネットワーク脅威は、トロイの木馬やボットに留まらず、スパム、スパイウェア、フィッシングやファーミングにも及んでいる。

様々な攻撃や悪意的プログラムに加え、ネットワーク詐欺の被害が拡大している。ハッキングやスパイウェアによる情報の盗難や不正利用が横行し、その被害は甚大である。人々は、自身の ID の盗難や不正利用が与信の崩壊につながり、金銭的な信用の失墜によって社会生活が困難になることを危惧している。

米国政府は、サイバー脅威や犯罪と対峙するため、国土安全保障省の指揮下に、国家サイバー・セキュリティ局（NCSD：National Cyber Security Division）を組織した。NCSD は、商務省の重要インフラ保証部門（CIAO：Critical Infrastructure Assurance Office）、連邦捜査局（FBI：Federal Bureau of Investigation）の国家インフラ保護センター、連邦調達機関の指揮下にある連邦コンピュータ事故対応センター（FedCIRC）及び国防総省の国家通信システム（NCS）を統合して創設された。国土安全保障の守備範囲が広すぎて、NCSD の活動は、その権限や資力の面で限界が見られる。これを補填するため、米国司法省が役割の一部を担っている。連邦捜査局の専門家も、サイバー犯罪に関して NCSD の能

力を補っている。

世界的に知られるように、米国は、高水準の IT セキュリティ技術やその製品を提供する先導国の一つである。従来、米国は主に、アンチウイルス製品、ファイヤーウォール、侵入検知システムを提供して来た。IT セキュリティ技術における最近の展開に、無線 LAN セキュリティ、デスクトップや携帯用デバイスなどを総括的に含めたエンド・ポイント・セキュリティ、そしてトラステッド・コンピューティングがある。トラステッド・コンピューティングはトラステッド・コンピューティング・グループ（TCG : Trusted Computing Group）が推進しており、特定のハードウェアで構成することでより安全なコンピューティング・プラットフォームを目指す、比較的新しい業界の動きである。トラステッド・プラットフォーム・モジュール（TPM : Trusted Platform Module）と呼ばれるハードウェアは、暗号鍵、電子認証書、パスワード及びその他のセキュリティ機能を搭載したものである。こういったセキュリティ機能は、チップの中に安全に保存され、改ざんや悪用に対し十分な耐性を持つ一方、一旦チップから取り出されると、自動的に破壊されてしまう。これは、コンピュータの自由かつ柔軟な利用に対する制限を行うことになるが、インターネットにおけるより安全な演算及び通信環境を提供することができる。

情報やＩＤの盗難による損害の増加及びユーザの懸念の拡大に対応して、連邦や州政府は、法や規制を整備している。このような法や規制の中で現在施行されているものは：連邦レベルではサーベンス・オクスリー法（別名：企業改革法）、健康保険可携責任法（HIPAA : Health Insurance Portability and Accountability Act）、グラム・リーチ・ブライリー法（別名：米金融制度改革法）（GLBA : Gramm-Leach-Bliley Act）及び連邦取引委員会（FTC : Federal Trade Committee）規制などがある。カリフォルニア州で 2003 年に設立されたセキュリティ違反情報法は、典型的な州レベルの法制の例である。いくつかの法案、統括機密法、社会保険番号悪用防止法、個人識別情報盗用防止及び被害者救済法などが、連邦議会で審議中である。

民間セクタもまた、活発に活動し、政府の様々な取組みに協力的である。トラステッド・コンピューティング・グループ以外にも、全米サイバー・セキュリティ・パートナーシップ（NCSP : National Cyber Security Partnership）は、情報セキュリティ統治に向けてのアクションを促すために積極的に活動している。NCSP は、ビジネス・ソフトウェア連盟（BSA: Business Software Alliance）、米国情報技術協会（ITAA : Information Technology Association of America）、テックネット（TechNet）、米国商工会議所、その他で構成される。国家サイバー・セキュリティ連盟（NCSA : National Cyber Security Alliance）は、サイバー・セキュリティ問題の意識を高め、最善の実践を尽くすことを目的とする、ビジネス、ユーザグループ、政府機関、教育機関で構成される、非営利の官民パートナーシップ組織である。NCSA は、ホームユーザ、小規模企業や学校がネット上での安全性を維持する能力を向上するためのツールや装置を提供する。

米国は、サイバー攻撃や不正行為に悩まされ続けつつも、政府、学界、民間セクタをあげて、安全なサイバー・ソサエティの構築に向けて、急速に活動的になり協力的になりつつある。

3.7.6. ドイツ

ドイツの CERT は、ウイルス・ワームの取扱いや不正侵入への対応・調整において非常に積極的と見られる。脆弱性情報取扱い枠組はまだ組織されていない。公的、あるいは非営利組織はまだ積極的にフィッシング対策に取組んでいない。フィッシングに対する公的

規制は実施されていないが、業界では自主的に取組みを始めている。

個人情報およびプライバシーの保護に関する法律はある。その適用範囲は広範囲で、個人情報から、社会的個人特定情報、さらにプライバシーや機微情報までが対象となっている。

4. 将来に向けての課題

大局的な見地では、誰もが頑張っている。しかしながら問題は、もう一方の世界の住人も「頑張って」いることである。従って、我々は、現状の取り組みを一層進めるとともに、更に努力を傾注し、ウイルス、ワームそしてあらゆるサイバー攻撃に脅かされない未来を実現しなければならない。

本章では、インターネット世界とサイバー・セキュリティのより良い将来の構築のために必要な新たな挑戦課題や、取組みを強化すべき領域について概観する。

4.1. セキュリティ文化

IT が社会に浸透し、IT が社会の仕組みや活動の秩序や序列に変化をもたらすに従い、その支配文化も変わらざるを得ない。IT 化された世界にいる誰もが「ユビキタス」の意味するところを理解し、それが利便性に関して意味するであろうものと同時に、脅威について意味するところも知らなければならない。

インターネットに接続した時、それがどういう意味を持っているかを知るべきである。何かの便宜を求めてクリックすることが、何かのリスクに遭遇する可能性を持つことを理解するべきである。こういった類の知識は、自動的に得られるものではない。経験から得られるものは確かにあるが、それは決して十分とは言えない。従って、セキュリティ意識向上の努力が必要であり、そのためにはセキュリティ教育が必須である。セキュリティ能力は、もはや、ユーザ自身のみのセキュリティではなく、サイバー社会のセキュリティにとって不可避なものである。

様々な分野の人々が、そしてインターネットから利益を受ける人々が、行動を起こし始めた。プライバシー保護及びセキュリティの統治管理責任に係る国からの要求は企業の背中を押し、IT 及び情報セキュリティについて一層考えさせるようになっている。現在、多くの企業は、自社従業員のセキュリティ意識の開発や向上に懸命に取り組んでいる。オペレーティング・システムのベンダは、自社製品をより安全にするための、そして自社製品のユーザがよりセキュリティの理解を深めるための努力を続けている。インターネット接続サービス事業者はセキュリティチェックサービスを提供し、ユーザのセキュリティ知識向上を促している。セキュリティツールベンダ、特にアンチウイルス・ベンダは、自社製品のユーザに対し、脅威や損害をより良く理解してもらう機会を提供している。

セキュリティ教育は、ひとつの市場区分として確立している。教育サービス提供事業者は、塾経営者からセキュリティ技術のベンダ、コンサルタントからシステム・インテグレータまでさまざま存在する。セキュリティ文化を取り巻く状況は、著しく改善されている。しかし、ウイルスの発生数とその頻度は留まる所を知らない。情報の盗難や紛失といった事故が、次から次へと発生する。こういった事故や被害の発生の大半は既知又は管理可能

な原因によるものである。つまり、ユーザがセキュリティや防御策について十分なトレーニングを受け、注意をすれば、そういった事故は防げるものである。さらなる知識と対応能力の向上が望まれる。

4.2. 情報セキュリティガバナンス

脅威やリスクは間違いなく存在し、簡単には緩和したり取り除いたりできない。従い、インターネット世界のすべての参加者がリスクを認識することは必須の要素である。しかし、企業の場合、インターネット・セキュリティに係る投資や費用をどの範囲で、どれだけ行うかといった根拠を示し、判断することは容易ではない。

例えば、ネットワーク・セキュリティ支出についてのガイドラインや評価尺度があれば、企業が脅威や想定される損害について準備することは比較的簡単である。日本経団連（日本の経済活動を先導する協会）は、最近、セキュリティ管理に対する共通理解についての報告書を発表した。この報告書によれば、ネットワークや情報セキュリティに係る企業の取組みが、企業統治及び経営評価の観点から測定・査定可能であれば、企業の経営者はたいへん助かるであろう。

日本の経済産業省（METI : Ministry of Economy, Trade and Industry, Japan）は、最近、情報セキュリティのガバナンスに係る研究を実施し、報告を公表した。企業の健全な管理及び社会的サイバー・セキュリティの観点の双方から、METI は、企業のセキュリティ投資を肯定し評価する方法を確立しなければならないと考えている。これは、経団連からの提案と軌を一にするものであり、多くの企業経営者の声を代弁するものである。

上述の METI の報告書では、情報セキュリティガバナンスの実現について、次の 3 つの切り口を指摘している：

a. 情報セキュリティのベンチマーク

これは、企業が情報セキュリティ対策に対してどのような行動をとり、どれだけ資金を使うかを査定する指標又はものさしのようなものである。こういったベンチマーク無くしては、セキュリティ支出に係る基準を設定することは容易ではないため、特に中小企業にとっては有益だろう。

b. 情報セキュリティ報告書モデル

これは、企業の情報セキュリティへの取組みと活動を報告するテンプレート又はガイドラインである。セキュリティ投資に係る公正な評価やお墨付きを得るため、報告書の参照モデルが示されていれば役に立つ。

そういった参照モデルを設定するための取組みが開始される。併せて、セキュリティ会計の方法論が示され、セキュリティ費用及びその期待効果を評価するための書式や方法が開発されることが期待される。

c. 事業継続計画のガイドライン

情報セキュリティは、事業継続計画（BCP : Business Continuity Plan）のプログラムの一環としても定義される。BCP は、企業がセキュリティ投資の重要性を数値化し理由付けをするもうひとつのアプローチ手法である。たとえば IT システムが故障した場合、企業活動は停滞し、事業の中断や、金銭的な損害といった、多大な被害を受ける。

従って、BCP が情報セキュリティを不可欠なものとして位置づけるならば、それは、情報及びネットワーク・セキュリティに係る取組みや支出を評価し正当化する一つの手段となる。

4.3. 次世代ネットワーク（NGN）

インターネットは、ベストエフォートの考え方に基づく通信手段である。遅延、正確性、失敗の排除、セキュリティを保証するものは何もない。不安定で脆弱なインターネットの特性の経験から至極当然に導かれるものが、別の、あるいはもう一つのインターネットである。もう一つのインターネットの構想は 2 つの要素を持つ。信頼のおけるネットワーク、そして信頼のおける参加者である。ネットワーク・サービスは、重要な通信に耐えうるサービス・レベル保証を提供できる、信頼のおける通信事業者によって提供される。こうした信頼のおける世界では、信頼のおける、本人識別が可能なユーザのみが適切なマナーで参加するので、善意の参加者は安心してネットワークを利用できる。

こういったもう一つのインターネットの概念は、次世代ネットワーク、NGN と呼ばれる。NGN の様々な活動は、世界中で行われている。こういった研究例には：米国国立科学財団（NSF：National Science Foundation）が資金を提供するプラネットラボ（PlanetLab）、ネットワークの相互運用性を目指す業界及び大学からの参加者による民間団体、ネットワーク・セントリック・オペレーション・インダストリー・コンソーティアム（NCOISC：Network Centric Operation Industry Consortium）、アビリーン(Abilene)・ネットワークを運営する NSF 後援によるインターネット・プロジェクト、及び欧州連合による FP-IST、FET がある。経済開発協力機構（OECD：Organization for Economic Co-operation and Development）や国際電気通信連合（ITU：International Telecommunication Union）などの国際機関も活発な活動を行っている。これらとは別に日本重要技術協会競争力委員会（COCJ：Committee on Competitiveness of Key Technology Institute-Japan）による研究が日本でも行われている。

こうした活動を概観し、今後の展望を表す報告書は、GBDe 内の NGN ワークグループによって別途作成中であり、本報告書とは別に提出される。

4.4. ユビキタス社会におけるセキュリティ

IT は日々進化を続け、我々の日常生活や活動を構成し動かすすべてのものに IT 装備と実現能力を提供する。こういった方向性や展望は「ユビキタス」と呼ばれ、「どこでも IT」を意味する。「ユビキタス」状態とは、あらゆるもののあらゆる場所でのインターネット接続を実現することである。たとえば、RFID（RFID：Radio Frequency Identification）あるいは IC タグは、世界中のあらゆる対象物に取付けられるようになる。これによって、遠隔地から自宅の電気器具をモニタし操作したり、自宅のセキュリティを確認したりすることが可能となる。すべての食品の個別識別が可能となり、食物の安全の追跡可能性が実現できる。このことは同時に、適切な保護を講じ維持していなければ、悪意を持った人間が、何らかの方法で同様のアクセスを行うことが可能であることも意味する。サイバー攻撃や詐欺がさらに安易に行われる訳である。

情報、特に個人情報のセキュリティも同様の危険にさらされている。世界中の全ての主体と客体は電子的に検索することが可能である。つまり、あなたが、いつ、どこで、何をするかを、知りたい時に誰でも知ることが出来る。これは、重要なプライバシーの問題である。

4.5. セキュリティ・レベルの評価指標化への取り組み

セキュリティとは、技術的、文化的な、ひいては社会的な問題である。個人も企業もすべての参加者がそれぞれの責任を果たさなければならない一方、公共部門もさまざまな面で積極的な役割を果たす必要がある。一つには、研究開発やリテラシー開発への資金提供がある。また別の切り口として、ガイドラインや指標を生み出すということもあろう。日本では、現在、国のセキュリティ・レベルの数量表示手法の導入を目指しているところである。これには、セキュリティの点数評価がある。韓国では、この方法を開発中であり、IPA は KISA と協同でそれを推進している。

情報セキュリティ評価指数は、情報セキュリティ対策状態（例：ファイアウォールの導入率）や、IT インフラ発展状態（例：PC の利用割合）など様々な基本データを基に、一国のセキュリティ・レベルを測定するために開発された。

何年にも渡り、こういった指数を測定し参照データを収集することにより、情報セキュリティ評価指数は、セキュリティ対策を改善していくことに寄与すると期待される。セキュリティ対策ソリューションの変化及びセキュリティ投資の費用対効果の測定値を把握することで、比較及びベンチマークの基本となるデータの蓄積が可能となる。

現在、韓国によって開発された指数を参照しつつ、日本は自国の指数を作成中である。韓国の指標をベースにして世界中に受け入れられるような指標を開発するべく、日韓の共同事業が計画されている。

4.6. ウイルス感染による損害算定モデル

感染被害の査定分野における評価も期待されている。ウイルス感染による被害算定の算式を策定するための取組みが行われている。

IPA では、金銭的な損害を算定するためのウイルス被害額見積モデルを開発した。これは、ネットワークのダウンタイム、システムや事業を回復するために必要な労力、労働コスト及び IT への依存度といったデータを基にはじき出されたものである。パラメータを得るためにアンケートや統計を調査した。パラメータが抽出され算式が確定したら、金銭的な損害は簡単に見積もることができるようになる。

5. 結論（GDBe からの提言）

上に見てきたものは、サイバー・セキュリティに対し、比較的大きな影響をもつ主要なテーマである。これらのテーマは、サイバー・セキュリティ問題をめぐる状況を改善するために IT 先進国が取り組んできた重要分野である。テーマの現在における状況の見直しを行うことは、今日、我々はどこに立っているのだろう、という総合的な見解を得る非常に良い機会となることだろう。そして、そのことは、より良いサイバー社会を築くための将来的な課題に対する視点につながっていく。

サイバー・セキュリティは、単に社会的な問題ではない。社会のあらゆる要素の混合である：技術、科学、工学、ビジネス、文学、教育、文化等々。その意味でサイバー・セキュリティは社会的であり、それがゆえに政治的である。全ての IT 関係者には、それぞれの

役割が期待され、そしてそれぞれの役割が行われなければならない。そうすることによって、サイバー・スペースは、全ての IT 関係者へ最善の利益をもたらすために役立つのである。

こういった見解から、GBDe は、政府及び民間セクタによって実現されるべき取組み、方向付け、そしてリーダーシップの対象とするべき以下の課題を提起する：

5.1. 知識（リテラシー）及び教育

人間は個人レベルでは、インターネット接続の危険性に対する知識が不足する傾向がある。適切なアンチ・ウイルス・ソフトウェアを用いることなくウイルスやワームにあっさりとやられてしまう。その結果がトロイの木馬やボットによる感染である。トロイの木馬やボットが動き出すとネットワークが攻撃されたり、詐欺用ウェブ・サイトに導かれて、銀行口座の番号やクレジット・カード番号などが簡単に盗まれたりしてしまう。

こういった類の危険な状況を回避する唯一の方法は、インターネットの危険性や、適切な保護や予防策を取らずにインターネット上で何かを行うことのリスクを知ることである。従って、教育や知識の開発は、最も重要な課題として着目し実現を図るべきである。リスクの認識度合いが少なければ、人々がリスクに関する知識を得るために支払おうとする金額や、費やそうとする時間も少なくなってしまう。それは、公的リーダーシップの役割が期待されることを意味する。人々がリスクについて認識し、学習する気を起させることが一層重要になっているのである。同時に、インターネット・プロバイダ、PC メーカ及びソフトウェア・ベンダがメッセージを発し、リスクについて知らせ、いかにクライアント環境を守るかを教えることも重要である。

教育が効果を発揮し、一定レベルの知識に到達した時、ボットやゾンビ PC を温存するリスクや、フィッシング、ファーミングによる被害のリスクは著しく軽減されるであろう。従って、政府が IT セキュリティに関する理解を促進し、人々がインターネット利用のメリットとリスクについての知識を得るよう促すように提言する。同時に業界関係者には、ビジネスとしてであれ無償奉仕としてであれ、ユーザにインターネット・セキュリティ教育の機会を提供することを期待する。

5.2. 情報セキュリティガバナンス

情報セキュリティガバナンスとは、セキュリティリテラシーの別の側面である。セキュリティの理解は、個人レベルにおいて最も重要なものである。同様のことが企業市民にも当てはまる。企業の場合は、情報セキュリティガバナンスとして定義される。企業の経営者は、インターネットの利点に加え、その脅威や潜在的な被害についてよく知っていなければならない。情報セキュリティガバナンスのコンセプトは 4.2.セクションで見た。

セキュリティの理解は、企業経営に情報セキュリティガバナンスを組み込むことで実現できる。政府は促進のためにガイドラインやインセンティブの提供を考えるべきである。インセンティブとしては、減税、特別目的基金、政府の要請や推奨、あるいは法による強制などがある。

企業も、情報セキュリティガバナンスについて努力が要求される。企業の社会的責任（CSR：Corporate Social Responsibility）の一部であるセキュリティ報告書が、その例である。事業継続計画はその一部として情報セキュリティガバナンスを組み入れてよく、そ

れは企業経営の改善にも寄与する。証券市場における格付けも、リスク査定要素として情報セキュリティガバナンスを取り入れるべきであり、企業にとって情報セキュリティを考えるインセンティブあるいは圧力として機能させることができる。

従って、情報セキュリティガバナンスは、政府及び民間セクタ双方が、究極のインターネット・セキュリティに向けそれぞれ取り組みを行うことが可能な分野なのである。

5.3. 次世代ネットワーク

インターネットの世界には、検討されるべき問題点が無数に存在する。その内のいくつかは、4.3.において簡単に触れたが、詳細は NGN の報告書に述べられている。GBDe は、近い将来 NGN が実現し、重要通信インフラの基礎を提供することを推奨する。NGN が実現した時、現在のインターネットは、NGN と共存し、全てのネットワークは、政府から個人まで、企業から従業員まで、そしてベンダからユーザまでの全ての利用者の利益となるように働くことだろう。

GBDe は、NGN の推進に注力することとする。そのための具体的な活動が来年に向けて行われ、様々な NGN 開発の取組みに影響を及ぼすことが期待されている。

5.4. 脆弱性情報扱ネットワーク

脆弱性は、インターネット・セキュリティの最懸案項目の一つである。セクション 3.1. で見たように、発見者、製造者及びコーディネータとの間で、潜在的脅威と対抗し、協働枠組みを形成する成功事例がある。この枠組みは、現在、米国及び日本を含む数カ国で取り組み中である。

GBDe は、こういった枠組みが、インターネットの先進各国で構築され、それが相互接続されることを提案する。相互接続が実現し適切に運用されれば、世界中を網羅し、インターネット社会に寄与する多目的・多機能の協働ネットワークのよい基盤となるに違いない。

5.5. ネットワークの追跡可能性

インターネットでのあらゆる通信が追跡可能となった場合、インターネットの世界に様々な利益がもたらされるだろう、という主張が一貫してある。ユーザは、ウイルスやワームへの感染や、知らずにゾンビ・プログラムを飼うことや、ウイルスに感染したメールを発信することについて、より注意を払うようになることだろう。これは、インターネット上における追跡可能性が実現すれば、インターネット攻撃や、有害な通信を知らずにばら撒くのを予防するのに役立つことを示唆している。

一方、追跡可能性は、インターネットの特性の一つであり、参加者の一部が支持するインターネット上における匿名性を危険にすることがある、という議論もある。この特性は、批判、主張、実演、実験のための場を提供する。それは民主主義や創造のゆりかごとして機能し、その意味において多くのインターネット・ユーザの利益に貢献する。

従って、現状のインターネットにおける追跡可能性は検討に値するべきものであると同時に、それによってインターネットの自由に悪影響を及ぼさないように適切な行為がとられるべきものと提言する。

本報告書は、サイバー・セキュリティ上の観点を提供することを意図するものである。推奨・提案項目としていくつかのテーマを取り上げた。ここに掲げた課題やテーマに沿って、サイバー・セキュリティ・イシュー・グループは、サイバー及びユビキタス社会に貢献していく。GBDe は現在、SET、ユビキタス、RFID 及び NGN を含む様々な面においてサイバー・セキュリティにコミットしている。全ての GBDe メンバーが声を大にして、サイバー・セキュリティについて語り、IT セキュリティの安定性に寄与するよう働きかけると同時に、サイバー・セキュリティ・イシュー・グループは、ここに掲げたテーマを推進することを約束する。

次世代ネットワーク

２００５年１０月１７日

議長：　小島　和人

特命顧問

富士通株式会社

I. 総論:

1. 現在のインターネット網に関して多くの問題が指摘されている。第一に指摘すべき弱点は所謂ベストエフォートベースであること、即ち、相手方に届くのか否か、どの程度の時間で届くのか、が全く保証されていない点である。第二に通信の相手方が本当に目指す相手であるのか、或いは送信者が悪意のない信頼できる相手であるのか特定できないことであり、この弱点を悪用した SPAM、フィッシング、ウィルス、ネット詐欺などが現在大きな問題となっている。

2. 勿論これらの問題に対処するため、現在でも様々な対策が取られている。しかし、これらはどれも対症療法的なパッチワークであって完全な防御は不可能であり常にそれを破ろうとする者との絶え間ない戦いとなっている。インターネットはその誕生に於いて限定され信頼できるメンバー間での通信が前提となっていた。しかし、それがひとたび相手の素性も分からない不特定多数の人々の間の通信手段になるに及んで、性善説にたったシステムは重大な弱点をさらけだすこととなった。

3. そこで、この問題を憂慮する研究者の間では、はじめから相手方に一定の時間内に確実に届くことが保証され、また悪意に満ちた犯罪行為を許さない新しいネットワークを構築し、安全な通信・電子商取引の実現を図ろうとする試みが検討されつつある。

4. ただ、現在のネットワークは、既に世界の何億もの人々に日常的に使われている社会的なインフラとして存在し、コスト的にも比較的安価に利用できるものとなっている。従って、もし現在より遥かに安全なネットワークが実現できるとしても、その実現に要するコストが巨額にのぼり、一部の人しか利用できないようなものとなっては意味がない。更に現在のインターネットのトラフィックが爆発的に増大している事から、現在のインターネット回線はいずれ容量不足に陥るおそれが指摘されている。現在のネットワークは従来の電話会社が電話の接続のために敷設した回線がベースとなっているが、今後の需要に応えられる大容量の幹線の新設に伴う莫大な建設費用を一体誰が負担すべきであろうか。インターネットの経済性理論からの検討も必要である。

5. 先に述べた現在のネットワークの弱点となっている匿名性については、それが逆に人々の表現の自由を保証し、デモクラシー確保のために必要であるとの社会学的な見地からの意見がある。相手を常に特定できるシステムは、逆に自由な発言を抑圧し、民主主義の進展を阻害する恐れがあるとも指摘されている。この、人権と安全性とのバランスを我々はどのように取れば良いのか。

6. これらの問題意識を基に、この WG の NGN 研究はスタートした。

7. しかし、次世代ネットワークにかかる問題は社会的にも技術的にも多岐にわたり、各国での検討も端緒についたところである。新ネットワークに関する一定の合意が形成されるのは今後数年から 20 年先になることが予想されている。

8. そこで、この WG では、まず、第一段階として、現在各国でどのような問題意識のもとにどのような組織(政府・民間)が検討を開始し、どのようなものが構想されているかを探ることとした。当然のことに、内容はユビキタス WG その他での検討内容と重なる部分があるが、それは今後の検討のなかで整理されていくものと考えている。

II. 各国の検討情況

1. 日本:

1) COCJ (Committee on Competitiveness of Key Technology Industries-Japan)

日本においては日本の主要企業 24 社と東京工業大学･大阪大学のメンバーにより構成される委員会である重点技術産業競争力委員会(COCJ)の検討項目のひとつとして「安心安全で信頼できる次世代ネットワークシステム開発プロジェクト」の検討が本年一月よりその部会の一つで開始されている。

基本的なコンセプトとしては次のような点を提案している。

a) 高品質通信の提供
   －「高速道路」に相当する高品質な仮想専用回線を実現
   －「救急車」に相当する緊急通信を実現

b) 安全性の提供
   － 車の「ナンバープレート」に相当する信頼できる認証された識別子を転送単位に付与し、誰が・どこから・いつ通信したのかを把握できるようにする。

c) 信頼性の提供
   －「環状道路」に相当する迂回経路の構築と、切替方式･管理機能
   － 災害時の通信ルートを簡便に確保する仕組みを実現

d) 主要テーマ
   － IP ベースネットワークの技術開発
     全体アーキテクチャ、ネットワークの品質・セキュリティ･信頼

性を実現する技術、ルータ・スイッチ技術，耐被災型情報通信技術等

- セキュリティ技術開発
  ネットワーク―端末連携セキュリティ制御技術，セキュリティログ自動分析エンジン等
- アプリケーション技術開発
  情報コンテンツに信頼性を付与するなどの次世代高信頼アプリケーション開発技術
- 素子基盤技術開発
  光集積回路，低消費電力素子等のネットワークを支えるデバイス技術

ネットワークの品質保証，高信頼化、およびセキュリティ関連の現行ナショナルプロジェクトの成果を活用し、さらに発展させる。

（参考）現行のナショナルプロジェクト

- ユビキタスネットワーク技術の研究開発　（総務省）
- 次世代バックボーンに関する研究開発　（総務省）
- 高度ネットワーク認証基盤技術の研究開発　（総務省）
- フォトニックネットワーク　（総務省・経済産業省）
- 次世代高速通信機器技術開発（経済産業省）
- 世界最先端 IT 国家実現重点研究開発プロジェクト
  （文部科学省）
- 安全なユビキタス社会を支える基盤技術の研究開発プロジェクト　（文部科学省）

2）次世代 IP インフラ研究会

2004 年 12 月から総務省では「次世代 IP インフラ研究会」の下に「IP ネットワーク WG」を設置して通信インフラのオール IP 化に伴う課題や課題解決に向けた政策の在り方等について検討を行い、2005 年 8 月 11 日に同研究会の「第三次報告書」として「電話網から IP 網への円滑な移行を目指して」が取りまとめられた。

今回の報告書では IP ネットワークへの移行に関し、安全性･信頼性･相互接続性は維持されること、また安全かつ便利なサービスが提供されることが示されている。また、その移行の推進にあたってはその手順が明確にされ関係者が理解を共有することが不可欠とされている。同省では、この結果を念頭に必要な政

策の実施を進める予定。

3) 情報通信審議会情報通信技術分科会

日本における NGN 標準化は本分科会の ITU-T 部会 NGNWG で行なわれている。また、2005 年 4 月より、NGN の国際標準化関係者が結集する場の整備を目的に、下記 TTC 標準化会議アーキテクチャ専門委員会 NGN アップストリーム SWG と一体となって推進されている。

4) TTC (Telecommunication Technology Committee)

上述の連携が行なわれているほか、NGN アーキテクチャ専門委員会では韓国、中国の国内標準化機関と連携を密にし、CJK NGN-WG を設立している。

2. 米国:

1) NSF (National Science Foundation)

- 2003 年 4 月、ワークショップ(ネットワークの基礎研究)を開催、ネットワーク研究の将来動向とビジョンを抽出した。
- 次世代のサービスとアプリケーションの開発を促進するための新しいネットワーク理論、アーキテクチャと手法を開発
- 新しい課題
  a) 耐性力のあるネットワークの開発: 大規模地震・災害、戦争などによってネットワークの一部が破壊されても自動的に別ルートを組み立て、通信の途絶を起こさないネットワーク。現在のインターネットもそのように機能するとされているとされているが、現実にはそれぞれのオペレータは自身の持っているネットワークの負荷を軽くするため自身のドメイン以外のパケットは他のルートに転送するようにしており、これがボトルネックとなっている。

  また、現在の幹線では、今後爆発的に増加するトラフィックを十分まかなえるとは考えられない。各事業者が過当な競争から十分な利益を上げられないでいる現状では民間がこれを負担するのは不可能に近い。このような幹線を敷設するためには政府レベルでの国際的な資金投入という政策が必要ではないか。(ネットワークの経済理論)

b) オーバレイネットワークの設計: 現在のネットワークにパケットの流通をまかせ、その上にもうひとつのネットワークレイヤを追加。具体的には現在のネットワークのノードに様々な機能を持たす。例えば発信元、中間、および最終ノードでタイムスタンプを押し、その間の所要時間を常に計測することにより、サービスクラス(即時、普通など)の要求に応じることができるようになる。また、様々な実験を行う場合に、各ノードに研究者が実験ソフトをインストールすることが必要になる。これを物理的に行なおうとすれば困難であるが、各ノードに Virtual Machine および VM Monitor 機能を設けることにより簡単に行なうことが可能となる。(これは PlanetLab と呼ばれるプロジェクトとして既に 20(+α)ヶ国 500 サーバで実験中。下記ご参照)

c) 実環境のセンシング: 身近なところでは温度・湿度などのセンサーをあらゆるところに設置し、それを(ワイアレスで)受信することにより、ビル内の環境設定に役立てる。また、センサーが微細な温度変化まで測定できるものとすれば、不審者の侵入の管理ができる。勿論軍事的な応用、例えば戦場に人の動きを感知するセンサーを多数配置することにより、どこで人の動きがあったかの情況把握も可能。更にそれが誰であるかのタグをつければ、倉庫の中で誰がどの棚に最も多くアクセスしたかなども分かり、倉庫内での資材配置なども合理化できる。振動センサーを建築時壁に埋め込んでしまえば、地震の情況把握なども可能。この実現のためには、センサーの小型化、電池の問題、センサーとルータ間のワイアレス通信、等々の課題がある。

d) ワイアレスネットワークの情報通信理論: 上述のようなセンシングネットワークを実現するためには、ワイアレスによるセンサーネットワークが不可欠である。そのための理論・技術の開発が必要。

- **The GENI (Global Environment for Networking Investigations) Initiative**

これは本年 8 月 24 日に明らかになった NSF の CISE(Computer & Information Science & Engineering)総局の計画で、従来の PlanetLab などとの連携を通じ培われた NGN 検討成果の一層の推進を目的とするもの。

この計画は新しいネットワーキングおよび分散型システムアーキテクチャの開発を目指すもので、それにより、セキュリティの確保、モバイル・ワイア

レス・センサーネットワークをも包含したユビキタス環境への対応、簡便な操作性の確保、新しい社会的サービス・アプリの実現などを可能とすることを目標としている。また、その研究のため、米国のみならず、世界各国の研究機関・企業等にも幅広く参加を呼びかけている。実際の研究にあたってはInternet2 などと接続により行われると見られる。

また、新しいネットワークの建設やサービスの創造に関しインターネットの経済性からの検討も行い、ネットワークサービスプロバイダーが健全な経済基盤を確立できるようにすることが重要であるとしていることが注目される。

2) 米国の産官学連携プロジェクト

a) 100x100 プロジェクト:

これは 100Million 家庭に 100Mbit/s の回線が提供されることを目指すプロジェクト。過去 30 年にわたり作り上げられてきたネットワークの限界を認識し、今後どのようなネットワークが必要とされるのか、単に容量だけでなく、サービス内容、基本的アーキテクチャおよびプロトコルまで含めての検討を、科学者、ネットワーク技術者、ネットワークオペレータ、などの関係者を集めて検討し、今日のインターネットを越えるネットワークのブループリントの作成を企図するもの。2003 年から米国の主要大学(カーネギーメロン、スタンフォード、ライス、UC バークレイ、Internet 2 のほか民間から AT&T などが参加して推進中。

b) PlanetLab:

これは現在のインターネットの上に新しいレイヤを追加するオーバレイネットワーク構想を推進するコンソーシャム。2002 年 3 月から活動が開始され、プリンストン大、ケンブリッジ大、MIT、UC バークレイなどの大学と産業界からは INTEL, HP,AT&T, France Telecom, NECLab などが参加している。現在のネットワークにパケットの流通をまかせ、その上にもうひとつのネットワークレイヤを追加。具体的には現在のネットワークのノードに様々な機能を持たせる。例えば発信元、中間、および最終ノードでタイムスタンプを押し、その間の所要時間を常に計測することにより、サービスクラス(即時、普通など)の要求に応じることができるようになる。また、参加の研究者が様々な実験を行う場合に、各ノードに研究者が実験ソフトをインストールすることが必要になる。これを各ノードに Virtual Machine および VM Monitor 機能を設けることにより、リモートに行えるようにな

る。2004 年 12 月の時点で 500 サーバで実験中。日本では東大青山先生などが参加。

EU COST-IST プログラムと交流(2003 年 6 月)

c) NCOIC (Network Centric Operation Industry Consortium)

これは 2004 年 9 月に発足したコンソーシャムで、ボーイングやロッキード・マーティンを含む 28 社により設立された。現在では Johns Hoplins University, Carnegie Melon University などの大学と、Cisco, Oracle, Intel, Raytheon, Sun Microsystems, Northrop Grummann など 50 社以上がメンバーとなっている。
過去 10 年間、ネットワークの性能が飛躍的に向上したにも関わらず、異なるシステムが一つのネットワークとして機能するための共通したアプローチが欠けていたことが原因で、連邦政府ではネットワークの統合が実現されていなかった。そこから連邦政府だけでなく、民間企業も含んだネットワークシステムの相互運用性の推進を目的に NCOIC が設立された。

NCOIC は、産官学の協力により、セキュアで信頼性が高く、相互運用性をもったネットワークの構築に向けた R&D が実施されている。参加企業はオープン・スタンダードやシステム・エンジニアリング・ツールの整備によるジョイント・オペレーションの効率化や、管理費用の節約といったメリットを受けることができる。同コンソーシャムから生まれる情報や新技術に関する知識を、さまざまなイニシャチブを立ち上げて米国内の軍事産業、その後は民間の両市場に普及させることとなっている。

d) Internet2

Internet2 とは、1996 年、NSF による出資と 34 の大学のパートナーシップから発足した次世代インターネットの研究プロジェクトで、現在は 207 の大学と 70 社の企業がメンバーとなっている。

最先端技術の R&D をミッションとする大学機関は、これまで以上に人的交流による知識の共有と、米国各地に位置する施設（ハードウェア）の統合を必要としているが、既存のインターネットにこれを実現できるだけの容量がない。このため、次世代ネットワーキング技術を必要とするアカデミア･研究コミュニティは、自分達で Internet2 の開発に取り組むこととなった。

Internet2 では、教育・研究専用の高速･低コストのネットワークを構築するため超高速ネットワークを利用した次世代インターネットプロトコルなどのネットワーク関連の基礎技術の研究、また高度なアプリケーションに関する R&D 活動が実施されており、多数のメンバー機関によって資金や機器の無償提供が行われている。

Internet2 の活動は、非営利の大学コンソーシャムである UCAID(University Corporation for Advanced Internet Development)によって管理されている。

Internet2 の最大の成果は、1999 年 2 月に運用が開始されたバックボーン・ネットワーク「アビリーン(Abilene)」である。アビリーンは Qwest Communications や Cisco Systems が UCAID に無償で提供した 2 万 km に及ぶ光ファイバー・ネットワークである。2003 年、アビリーン･ネットワークは 10Gbps、国内の接続アクセスポイント合計 47 ヶ所を持つようになった。

アビリーン･ネットワークは IPv4 だけでなく、次世代インターネットプロトコルの IPv6 に適していることから、現在 Internet2 では同ネットワークを利用して IPv6 ネットワークの展開に取り組んでおり、2006 年末までにネットワークのセキュリティを確保するモニタリング・ツールの開発や新しいマルチホーミング方式の検討を実現することが目指されている。

3. 欧州:

1) EU FP-IST FET （Framework Program-Information Society Technologies　Future and Emerging Technologies)

Framework Program は EU が主導で科学技術振興を目的に推進しているプロジェクトで、現在はその 6 段階目(FP6: 2002 年から 2006 年)となっている。情報通信分野が重要テーマの一つとして掲げられており、その中にいくつかの研究分野別カテゴリーに細分されている。 Future and Emerging Technologies はその一つである。これは 2020 年の通信パラダイムをとりまとめようとするもの。2004 年にその概要を示してプロジェクト募集が行なわれ(締め切り 2005 年 3 月)、2005 年秋に採用案を発表予定。

これにもりこまれた内容は、NSF の考え方との共通点も多く、情況変化に応じて自律制御・自己組織化する超分散通信システム[Situated and Autonomic Communication (COMS) -- Communications Paradigm for 2020] の研究 が中心となっている。

これ以外にも以下の 16 の研究分野が次世代ネットワーク関連の研究として立ちあがっている。全て欧州レベルの規模で 3 社（団体）以上の企業または研究機関のコンソーシャムとして構成され、欧州委員会のファンドおよび当該コンソーシャム構成機関からのファンドにより R&D を推進している。
（以下に 16 プロジェクト名称を列記する。）

a) European Research Network on Foundations, Software Infrastructures and Applications for large scale distributed, Grid and Peer-to-Peer Technologies (Code Name: COREGRID)
b) Being on Time Saves energY continuous multimedia experiences on network handheld devices (BETSY)
c) Distributed European Testbed Laboratories (EUROLABS)
d) Mobility and ADaptation enAbling Middleware (MADAM)
e) Access to Knowledge through the GRid in a MObile world (AKOGRIMO)
f) Co-ordination Action for Libre software Engineering for Open Development Platforms for Software and Services (CALIBRE)
g) Understanding Networks of Learning Design (UNFOLD)
h) Flexible Gateways Architecture for enhanced access network services and applications (FLEXINET)
i) Realizing the semantic web (KNOWLEDGE WEB)
j) Digital Switchover, Developing Infrastructures for Broadband Access (ATHENA)
k) Exploring new limits to Moore's law (MOE MOORE)
l) Design and Engineering of the Next Generation Internet towards convergent multi-service networks (EURO NGI)
m) Network of Excellence on Digital Libraries (DELOS)
n) Broadband services for everyone over fixed wireless access networks (BROADWAN)
o) Next generation Optical network for broadband in Europe (NOBEL)
p) Ultra High Bit Rate Over Cooper Technologies for BROADband Multiservices Access (U-BROAD)

なお、フレームワーク・プロジェクトに関しては、既に次期プロジェクトである FP7（2007 年から 2013 年の期間が対象）のスキーム作成が開始されている。2005 年 6 月に欧州委員会の研究･開発総局から FP7 に向けた提言が欧州議会･閣僚理事会に対し提出され、この秋以降審議に入る見込みである。

2) COST - European COoperation in the Field of Scientific and Technical Research

これは 1971 年創設された欧州各国が共同して科学技術分野での優位性を保つべく資金を出し合って研究を進めるもの。情報通信、バイオ、医学、物理学社会科学など多岐に渡る研究分野の研究を行っている。

2003 年 6 月には米 NSF と Exchanges and Trends in Networking (Nextworking '03)をテーマにギリシャにおいてワークショップを開催している。欧米の主要大学のほか民間からは、INTEL, AT&T, Microsoft が参加。目的は、今後ネットワーキングに関し、どのような技術が出てくるのか率直な議論を行い、知識の共有を図るもの。

III. 国際機関での検討情況:

1. OECD

OECD では､その Directorate for Science, Technology and Industry の Committee for Information, Computer and Communications Policy の下に Working Party om Telecommunication and information Policies がおかれ、これが、Next Generation Network Development in OECD Countries というレポートを 2004 年 6 月にまとめ、2005 年 1 月公表したが、これは主として政策面での課題をまとめたもの。

ネットワークが従来の PSTN から IP ベースへ移行することで既存の ICT サービス業者のビジネスモデルが変わる。VoIP など IP ベースのサービスになっていくことを予想しているが、現在のインターネットに関する問題の解決を目指す意味での NGN は企図されていない。

ただ､ユビキタスネットワーク社会の進展などに伴う必要な容量の増大に対応する

ためのオペレータの投資は、ビジネスモデルの不確定性を考えるとき如何にあるべきか、また End-to-end QoS はどう考えるべきか、今は注意深く動向を見つめるべきであるとしている。

2. ITU

ITU-T SG13

ITU では、1995 年からの GII(Global Information Infrastructure) Project に於ける提言を基に、GII の実現を目指して 2002 年 1 月、"NGN 2004 Project"が立ち上げられ、NGN に関する基本的特徴(IP ベース)、持つべき機能(サービスとネットワークの分離)、目的(公正な競争の促進、民間投資の推進)、7 つの研究分野(アーキテクチャ、セキュリティ、モビリティ、ナンバリング、ルーティング等)に関する検討を行うことが決定され、その後の討議を経て 2004 年 6 月に最初の提言が発表された。

それによれば、NGN を今期(2005 年から 2008 年)の標準化重要課題として位置付け、取り組みを強化している。FG NGN による標準作成の加速とともに、NGN 担当の SG(SG13)を設置して対応している。

ITU に於ける議論はキャリアに於ける次世代ネットワークの色彩が濃く、またそこではユニバーサルサービス、インターオペラビリティ、シームレスなアプリサービスの提供、これらに関する標準といった側面が重視されている。

3. ETSI (European Telecommunications Standard Institute)

ETSI では TIPHON (Telecommunication Internet Protocol Harmonization Over Network)プロジェクト と SPAN(Service and Protocol for Advanced Network)プロジェクトを統合した TISPAN プロジェクトが NGN 標準化を積極的にリードしている。NGN 標準 Release1 を 2005 年 6 月に完了予定であったが、進捗に遅れが見られるため、分割リリースされる方向と考えられている。

4. APEC (Asia Pacific Economic Cooperation)

APEC では NGN は情報セキュリティやユビキタス社会の問題とともに、通信情報閣僚会合下の通信情報 WG および ECSG(Electronic Commerce Steering Committee)で取り上げられている。

5. 米国では ATIS(Alliance for Telecommunications Industry Solutions)内に NGN FG を設立し活動を開始している。北米での法規制に関する部分以外は基本的に

ETSI-TISPAN NGN Release1 の要求条件と同じである。

6. 3GPP (3rd Generation Partnership Project)

これは基本的に第三世代携帯電話に関係するフォーラムであるが、ここが開発した IMS (IP Multi-Media Subsystem)が NGN のコアネットワークに流用されている。

6. その他の国際フォーラム

a) IETF (Internet Engineering Task Force)

SIP (Session Initiation Protocol), MPLS (Multi-Protocol Label Switching), GMPLS (Generic Multi-Protocol Label Switching), IPv6 などの要素技術の仕様の作成を中心に活動。

b) MSF (Multi-service Switching Forum)

NGN の実装仕様作成。仕様標準化は ITU-T 勧告、IETF などのフォーラム仕様を採用。

IV. 現在の検討情況から導き出せる結論

1　実現されると予想される時期

安全かつ確実な通信を可能とする NGN については、ある日全てが一斉に開始されるというのではなく、ある程度部分的・段階的に開始されていくことが予想される。従ってどの部分を取り上げるかによってその時期異なるが、標準化については 2008 年、新ネットワークやインフラについては 2010 年から 2020 年をターゲットにしている活動が多い。

2. 利用されるであろう技術

これについては基本的には IPv6 などの技術を用いた IP ベースの超高速オールパケット型ネットワークが目指され、パケットの転送機能レイヤとその管理機能レイヤの分離により様々なサービスが提供でき、またいかなる場合も通信が途絶しない自律制御・自己組織化する分散型システムアーキテクチャが目指されている。ワイアレス、センシングネットワーク技術なども重要な関連技術として開発が進められている。

3. それに向けて政府がなすべきこと

NGN は一事業者、一国家を超えた議論であるため、政府には NGN フレームワーク作成における国家間の橋渡しを行い、R&D やインフラ整備・強化のための投資・支援をお願いしたい。それによりユビキタス社会に向けてのプラットフォームが

形成され、民間セクターによる新たなビジネス創出も可能となる。また匿名性の問題など社会的課題に関する検討を民間とともに行い、一定の合意形成を図る。

4. それに向けて民間がなすべきこと

NGN の全地球的意義に鑑み、各国政府、国際機関、他の民間団体・企業との連携のもと、民間のもつ活力を最大限に活用して技術的発展を目指すとともに、上記の社会的課題に関する合意の形成に協力し、もって世界市民の利便向上・文化的生活の向上に資することを目的として活動する。

V. 結語および来年度検討項目

今回は各国、各国際機関での NGN の検討情況を把握した。これから直ちに分かるように現在の検討情況は、それぞれの機関の目的により、その目指すところが大きく異なっており、我々が期待するあるべき新ネットワーク像が明確に示されているとは言いがたい状況である。即ち電子政府を含む広い意味での電子商取引を対象とするインターネット関連組織(ISP、コンテンツ業者、決済機関、機器メーカーなど)は新しいビジネスモデルとその安全確実なサービスの実現を、電話オペレータは PSTN から VoIP への技術的移行を中心にどのようにそれを実現するか、また ITU や WITSA などを中心とする機関は如何にして適切な技術標準を設定できるか、更にアカデミアでは民衆が直接意見を述べ政治に関与する可能性からのデモクラシーと個人の匿名性のあり方についてなど、対象が幅広いだけにそれぞれが目的とする対象がオーバーラップする部分はあるにせよ異なっている。これらは例えて言えば、自らが動きながら他の Moving target を狙っている状態であり、共通の地平に到達することが極めて難しい。もちろんそれらが他の機関での情況を認識しつつ同時並行的に研究を進めても、結果的に一定の時間ののちにはある種の合意・結論に到達すると楽天的に考えることも可能である。

しかし、我々としては、及ばずながらこれを一歩進めて GBDe の中にこの問題の情況を常にウォッチする組織を来年度以降立ち上げ、政府・民間・学のそれぞれのフォーラと意見交換するとともに可能な提言を適宜まとめて提供し、もって NGN の推進に貢献したいと考える。

また、今後の NGN 建設にあたって、政府が例えば標準や各種制度を決定するに際して、民間の意見を積極的に聴して欲しいということである。電子商取引などについてはこれまでも政府・国際機関は民間の意見を取り上げ、政策に反映して頂いており大変良好な結果を実現している。民間も、それがより良い成果を求める競争の結果として止むをえない面はあるとしても、これまでの映像・情報記録の規格に関する不毛な争いを脱してより建設的な協力体制を築くことが求められるであろう。

この問題に関してさらに言えば、民間といってもPSTNのIP化というキャリア視点での考え方だけではNGNフレームワークを狭いものに限定してしまう恐れがあるため、広くビジネス全体を俯瞰しての対応を期待する。

また、特に標準化推進については、その動きを否定するものではないが、いくつかの機関の考え方の違いの調整のためにNGNの推進が不必要に遅れることがあってはならない。

更に、資金的な面でも政府の役割は極めて大きい。それは、現在のネットワークが機能的・容量的に飽和し、新しいネットワークを開発し、建設するための投資である。従来は主として民間が民間の競争をばねに投資を続けて来た。しかし、今日過激な競争にさらされた民間企業は収益もあがらず、再投資のための資金も十分にまかなえない状態となっている。NGNを世界の巨大インフラとして位置づけるとき、政府による投資が検討されるべきであり、民間もそれに協力する形で参加することを惜しまないであろう。実際米国ではNITRD(Networking & IT R&D)に2004年度$373.3M(約410億円)、欧州もFP6IST(Information Society Technologies)に5年間で3,625MEuro(約5000億円)が予算化されている。

以上