世界情報社会サミット（ＷＳＩＳ）に関する報告

社団法人自由人権協会
世界情報社会サミット（WSIS）プロジェクト

第１　ＷＳＩＳと市民社会

世界情報サミット（ＷＳＩＳ：World Summit on the Information Society）は、「各国首脳レベルで、情報社会に関する共通のビジョンの確立を図るとともに、そのビジョン実現等のための基本宣言及び行動計画を策定する」（総務省）ことを目的とし、２００１年以降、国連及び国際電気通信連合（ＩＴＵ）が主催者となって進めてきた。２００３年１２月にジュネーブでサミット第１フェーズが既に開催され、ＷＳＩＳにおける基本原則の宣言や行動計画が採択された。そして、２００５年１１月１６日から同月１８日まで、チュニジアの首都チュニスで第２フェーズが開催された。

ＷＳＩＳにおいては、南北のデジタル格差、インターネット管理、メディアの取り扱い、セキュリティ確保、知的所有権の確保などがテーマとして取り扱われるが、ネットと表現の自由、プライバシー、南北のデジタル格差など、市民社会の協力と連帯が不可欠な論点につき、NGO 側の問題意識と関与は十分とは言えない状況であり、NGO 側の意見はＷＳＩＳの公式文書に十分に反映されていない状況にある。

現段階で主要な論点となっているのは、主に、インターネットガバナンスの問題、デジタル連帯基金の問題である。前者は、ドメインネームやＩＰアドレスを管理するＩＣＡＮＮ（米国籍非営利民間団体）中心に現行組織で対応していくべきとする立場と、政府間の国際組織で対応すべきとの立場が対立している。また、後者は、デジタル格差解消のためのプロジェクトの実施において、世界銀行、国連開発計画（ＵＮＤＰ）、二国間協力等、既存のスキームを有効活用すべきとの立場と、新規の基金（「デジタル連帯基金」を設立すべきとの立場が対立している。先進国と発展途上国との関係、国家と市民との関係、各国間の関係などが複雑に絡み合う状況の中、これらの論点について議論される。

ＷＳＩＳには、国連、政府、産業界、市民社会の各方面から参加し、情

報社会のあり方について討議するが、市民社会の発言は重要な意味を持つのであり、市民社会ないしＮＧＯからの積極的な参加及び関与がなされるべきである。

なぜなら、一般的に、これまで国家は、産業界の要請を受けて情報流通の枠組を構成するための基礎となるインフラの整備を行うばかりで、市民社会の情報のあり方への積極的参加ないし関与に消極的であったと言わざるを得ず、そのことは、結局、国家・政府・産業界の主導のもとで、市民の関与しないところで情報社会のあり方が決定されてきたことを意味するものである。ＷＳＩＳの目的は、そのような構造を打開すべく、市民社会にとって真に有益な情報社会のあり方、情報流通の中での意思決定過程に市民が主体的に関与できる構造を構築することにこそあるというべきである。

なお、ＩＴ企業もＷＳＩＳに関与しているが、ＩＴ企業の関与だけでは、南北のデジタル格差の根本的解消にはつながらず、かえってその格差を温存させる可能性もあり、場合によっては、人権抑圧的国家に対して国民監視のためのツールを提供することになるおそれさえある。このような点からも、市民社会・NGO のＷＳＩＳへの参加ないし関与が必要である。

また、当然のことながら、情報社会のあり方は表現の自由などの人権にも直接的な影響を及ぼす。２０００年７月に発足した国連グローバル・コンパクトは世界人権宣言など世界的に確立された合意に基づく原則であり、参加する世界各国の企業に対して、人権、労働、環境の３分野で世界的に確立された１０原則を支持し、実践することを求めている。これは、世界中の企業が一致団結して、地球市民としての立場からその責務を推進すべきこと、国家のみならず企業も、人権の促進と確保に対する責務を負っていることを示している。また、２００３年８月２６日に発せられた、「人権に関する多国籍企業および他の企業の責任に関する規範についての注釈」は、社会的機関としての多国籍企業その他の企業もまた、世界人権宣言に規定された人権の促進と確保に責任を負っていることを定めている。このような観点からも、情報社会のあり方が論じられるべきである。

第２　ＷＳＩＳと市民的自由の確保

１　情報化社会と市民的自由

情報化社会、とりわけインターネット技術の利用が可能となることは、市民による情報の発信や表現を格段に容易にする。他方で、そうしたインターネット技術の利用を通じて、他の市民の人格権や名誉、あるいはプライバシーを侵害する行為も存在する。その他、インターネット技術を用いてなされる犯罪行為に対抗する必要性は否定できない。

たとえ情報化社会がもたらす否定的な側面が存在するとしても、そのことを理由に市民が持ちつつある多様な表現手段を国家から奪われることがあってはならない。そのために、インターネット技術に対する管理は、まず、世界人権宣言が普遍的な人権規範として設定する諸基準に依拠してなされなければならない。そのような諸基準には、法の下の平等（７条)、プライバシーや通信に対する侵害の禁止（１２条)、情報及び思想の自由な流通を含む意見及び表現の自由に対する権利（１９条）がある。

そのような普遍的な諸基準のもとで、市民によるインターネット技術の利用については、以下の諸原則が確保されるべきである。

インターネット技術の利用は、それを希望する者すべてに開かれているべきであり、人種、皮膚の色、性、言語、宗教、政治上その他の意見、国民的若しくは社会的出身、財産、門地その他の地位又はこれに類するいかなる事由によっても差別されてはならない。

国家による規制は、インターネット技術の利用が他の者の権利を侵害する場合にのみ許されるものであり、その規制の手段は人権の諸基準や法の支配に合致したものでなければならない。

国家による規制は、市民によって発せられる情報を事前に検閲したり、恣意的に制限したりするものであってはならない。

インターネット技術の利用に関する個人情報は、本人の同意なしに収集、保有、利用または開示されてはならず、本人のコントロールのもとにおかれなければならない。

２　サイバー犯罪防止条約の問題点

以上に述べた諸基準が確立される前に、すでに国際的に進行しているサイバー犯罪条約は、市民的自由にとって多くの問題点を含んでいる。

サイバー犯罪条約は、１９９９年に欧州評議会によって作成され、日本でも２００４年に批准発効するにいたった。

サイバー犯罪条約は、コンピュータ・システムを攻撃するような犯罪及びコンピュータ・システムを利用して行われる犯罪（サイバー犯罪）を国際的に防止・抑制するために、違法アクセスなどの一定行為の犯罪化、サイバー犯罪に関する刑事手続の整備、捜査や犯罪人引渡に関する国際協力などを締約国に義務づけるものである。

問題点として、以下のような点があげられる。

・プライバシーや市民的自由の保護に関する規定を欠いている。

・対象とする犯罪が広範で、コンピュータを用いた犯罪のみならず、コンピュータに証拠がある犯罪すべてに適用されかねない。

・捜査協力において通常要求される双方処罰可能性が、この条約のもとでの捜査協力においては要件とされていない。そのため、他国が政治犯処罰目的で捜査協力を日本に要請した場合でも、日本は政治犯処罰が日本法の下で許されていないことを理由にその要請を拒否できない。

・政治活動への保護が弱い。

・世界的な不均衡のある知的財産権をそのまま保護しようとしている。

・警察に新たな捜査権限を与える。

第３　デジタルでデバイドの克服に向けて

１　デジタルデバイドの現状

現在の国際社会は、アメリカを中心とした情報通信網の中で、「ＩＴ社会の構築」に向けて急速な変化をとげようとしている。

特に、世界情報サービス市場の進展は目覚しく、ブロードバンドの普及により電子商取引の利便性は著しく向上している。

一方、世界の情報サービス市場の地域別シェアーをみると、アジア太平洋・中南米・中東アフリカを合算しても日本一国の１０％にも満たない状態である。（ＷＩＳＴ「Digital Planet 2002」より）

市民社会においてはさらに深刻な格差が存在することは想像に難くない。

諸外国における情報通信の普及率を比較すると、高所得国（国民一人当たりの GNP が９，０７６ドル以上の国）の人口は世界全体の１５．８％に

過ぎないが、世界固定　電話回線数の５１．５％、移動電話加入数の５４．９％、インターネット利用者の６８．７％が高所得国に集中している。

他方、低所得国（国民一人当たりの GNP が７３５ドル以下の国）の人口は、全世界の３９・６％を占めるが、固定電話においては６．３％、移動電話加入数においては３．６％、インターネット利用者においては５．２％を占めるに過ぎない状況にある。（２００４年　情報通信白書より）

特に「ＩＴ社会の谷間」ともいえるアフリカ諸国では「電話回線、ラジオ受信機、テレビ受像機、コンピューター及びインターネット利用者」の数はいずれも世界中で最も少ない。

これらの情報通信技術（ＩＣＴ）を利用できる人とできない人の格差「デジタルデバイド」はアフリカが世界でもっとも大きい。

インターネット普及率を数値的に比較するとアフリカは２５０人から４００人が一台のパソコンを利用していることになり、アフリカを除く世界の普及率は１５人に１人加入、北米とヨーロッパは２人に１人加入している事実と比較するとその差は歴然としている。

また実生活では、ほとんどのアフリカ人は電話をかけることさえままならないのが現状である。

国連のアナン事務総長は「インターネットを通じて時宜を得たニュースや情報を入手することによって貿易，教育，雇用，健康と富を促進することができるが世界にはこの変革から取り残された人々が余りにも多く、この問題は余りにも大きい」と述べている。

２　国際協力の必要性

２００３年１２月にスイスのジュネーブにおいて開催された世界情報社会サミット（ＷＳＩＳ）でも「デジタルデバイド」の解消を重要な論点のひとつとして取り上げた。

「世界の５０％以上のひとびとがネットワークに接続できる環境を整備する、またすべての学校をネットワークに接続する」といった基本宣言・行動計画を採択し２０１５年を目標達成の年度と定め、「デバイド」解消の動きをはじめている。

また、アフリカの指導者達も「デジタル連帯基金」の創設を技術先進国に期待するなど具体的な提案を行っている。

同様に「ＷＳＩＳ」に参加したＮＧＯグループの「アフリカ市民社会コーカス」は「通信の権利は、グローバル情報社会が構築される土台としてみなすべき基本的人権である」と主張すると同時に「開発されている技術のほとんどは価格が高く、基本的通信であっても貧困層には手が届かない」と言っている。

さらに、アフリカの現地で開発援助に取り組んでいる多くの人々は「デジタルデバイド」の解消が優先課題であるとは主張していない。

「飢餓と病気」の撲滅に直接寄与する食料や薬品、医師の派遣などを重要な課題として挙げ、「デジタルデバイド」是正のための施策がさらなる富の偏在を生み、貧困層の拡大を助長するのではないかと危惧している。

１人当たりの GNP と固定電話回線数、移動電話加入者数及びインターネット利用者数の人口比には、高い相関関係がある（２００４年情報通信白書）ことからも、「デジタルデバイド」解消のための国際協力は「貧困」の撲滅を不可欠の課題とした施策であることが重要である。

以上の現状を鑑み、以下の国際協力のあり方を提案する。

① 世銀・ＩＭＦ等の国際機関が共同して「デジタル基金」を拠出し、その使途と効果についての情報公開をし、資金の流れについての透明性を確保する。

② 途上国政府が必要とする技術者を供給するために、国際的な人材バンクを設けると共に国連機関において技術者養成を行う。

③ 多国籍企業等の協力を要請すると同時に、企業利益追求のための安価な労働力の確保、資源の確保等といった発展途上国の人々の生活向上に望ましくない行動を規制する実効性のある法的拘束力を確保する。

④ 援助される国の意思と自助努力を優先した協力の方法について、国連と当該発展途上国による開発マニュアルを作成し、援助は低利子の借款によるものとする手段も含めて、「デジタルデバイド」の解消を希望する全ての国に必要な援助を行えることとする。

⑤ ソフトの開発については，先進国が無償で技術提供を行うのが望ましい。

⑥ 被援助国の一般国民が世界に向けて，自国内の意見，感想を述べることのできる民主的な伝達手段を確保する。

第４　東京ユビキタス会議市民セッションとプライバシー・インターナショナル

ＷＳＩＳでは、政府や業界を中心に、インターネットガバナンスとデジタル格差を中心とした議論が行われているが、その議論の場にＮＧＯや市民社会は、何をもたらす必要があり、またそれは可能なのか。

１　東京ユビキタス会議（２００５年5月１６日及び同月１７日に開催、ＷＳＩＳのテーマ別会議でもあった）のセッションから

情報通信技術（ＩＣＴ）は、それ自体が社会正義、市民の立場強化及び持続可能な発展に寄与するという積極的な面と、市民社会に強い影響があるにもかかわらず市民不参加のまま進められ、市民の自由の脅威となるかも知れないという消極的な側面がある。特に様々な意味で社会の周辺に追いやられた集団が、ＩＣＴの利益を受けることなく放置され、あるいはＩＣＴによってさらなる不利益を被る危険性がある。

このような事態を防止し、政治と市場中心に進められるＩＣＴの発展に対し、カレン・バンクス氏は、その隙間を市民社会が埋めていくために、政治と市場に対し、説明責任、透明性、利潤に対する市民社会の価値の対置を求めていくことが必要だと主張する。その目指すところは、意思決定において多様な利害関係者が参加できるシステムを保障することである。

しかしそれがどのようにして実現可能なのか、政府、業界そして市民社会と多様な利害が錯綜する中で合意形成はできるのか、ということは、国際機関や各国の実践の中で進められていくしかない。そのような観点に立って、実施されているケニアの制度改革は、市民社会の参加を進める好例である。

逆に、市民の情報へのアクセスの障害となっている問題点を指摘したのが、チュンユン・フィー氏である。彼はそうした阻害要因として、以下のようなものをあげた。

- 知的財産権の過度の保障体制
- 人材や投資が流出遍在することによる格差の増大
- 技術発展が旧設備を無効化することによって旧設備に頼らざるを得ない人々や地域に対する格差の増大

・アクセスを可能とする諸技術が監視技術に転化する危険性
・ネットにおける認証技術や発信源特定技術が表現の自由を萎縮させる危険性
・情報内容の規則化が表現の自由を制限する危険性

2　プライバシー・インターナショナルの議論から

プライバシー・インターナショナル（ＰＩ）が市民のプライバシー保護の観点から最も強く懸念を表明しているのは、反テロリズムの対策として各種の情報技術が用いられていることである。

・情報通信に対する監視権限の増大
・データ保護体制を弱体化させる制度
・政府機関でのより広範なデータ共有とそれに伴うプロファイリング機能の増大

その他、ＰＩが懸念を表明している技術としては、以下のようなものをあげている。

・個人認証システム：ＩＤカード、バイオメトリクス（生物的特徴を数値化）とそれに基づくパスポート
・通信の監視、特にインターネット通信監視システム（ブラックボックス、キー・ロジャーズ鍵の運搬器）や取引・発信場所の監視記録
・サイバー犯罪の国際的な規制強化
・安全保障・諜報のための技術：エシュロンなど。
・旅行、出入国記録の政府による収集、旅行者の追跡、モニター
・会話盗聴技術の発展
・ビデオ監視と顔のデジタル認識
・通信衛星による監視
・インターネットコマースの情報記録とプロファイリング
・無線周波個人認証（ＲＦＩＤ）
・行政の個人情報の集積とプロファイリング
・国勢調査
・デジタル権限管理（ＤＲＭ）による情報の匿名利用の困難化
・ＩＣＡＮＮのWHOＩＳ登録データ

・ スパイテレビ：インタラクティブ・テレビ技術
・ 遺伝情報個人認証
・ 病気の探知・治療
・ 職場での監視、捜査、モニタリング、薬物テスト
・ 電子投票制度
・ ナノテクノロジーの監視機器への応用

なお、ＰＩはＷＳＩＳについて、第１フェーズは、あまりにもテロリズム対策と安全保障に議論が引きずられすぎた、行動計画はその実施方法が不明なままである、安全保障とプライバシーの項は対テロ戦争への明示の言及はないものの黙示的にサイバー犯罪条約に言及し、プライバシーに言及した方針は一つだけだったと否定的な評価を下している。それらは第２フェーズの課題であるが、有力なスポンサー国の支援が必要であろうとしている。

以　上