官民連携による健全なインターネット社会の発展に向けて
－第2回 IGF(インターネット・ガバナンス・フォーラム)への日本の経験の発信－

2007 年 9 月 18 日
(社)日本経済団体連合会

Ⅰ．はじめに

インターネットはその普及から１０年余の間に、情報通信や放送のあり方を根本的に変えるとともに、そのボーダレスな影響力を通じて、経済、社会構造にも大きな変革をもたらしてきた。今やインターネットは情報社会におけるインフラとして中核的な役割を果たしており、インターネットを活用したビジネス、行政、サービスの拡充とともに、市民生活や企業活動のインターネットへの依存度は益々高まっている。

一方、インターネットの普及・発展に伴い、サイバー犯罪やデジタル・デバイド拡大といった課題も増加、深刻化の傾向にあり、自由かつ安全なインターネットの利活用を支えるガバナンス、セキュリティの問題が全てのインターネット利用者にとって重要な課題となっている。

インターネットはボーダレスに全世界に張り巡らされているため、このような課題の多くは一国家、一企業のみの努力によって解決できるものではない。そこで国連は、インターネットが抱える諸問題について世界中のステークホルダーが議論する場として、2003 年と 2005 年に世界情報社会サミット(WSIS)を開催した。そして「既存のインターネット・ガバナンスの枠組みが効果的に機能している」ことを確認するとともに、「インターネット・ガバナンス・フォーラム(IGF)を設置し、マルチステークホルダーによる議論を継続する」ことを決定した。

昨年 10 月にアテネにて開催された第 1 回 IGF では、世界各国のマルチステークホルダーが一堂に会し、インターネットのアクセス、開放性、セキュリティ、多様性の４つのテーマについて意見交換を行い、IGF がインターネットに関する世界共通の課題を共有する場として有効に機能した。日本経団連は、第１回 IGF にミッションを派遣し、日本の産業界の立場から、ブロードバンド先進国として他国に先駆けて経験している課題や、携帯電話のスパムメール撲滅等、ベストプラクティスを発信し、インターネットをめぐる国際的な意思形成の場に建設的な貢献をしてきた。

Ⅱ．第２回 IGF への期待

第１回IGFは、世界各国のマルチステークホルダーがインターネットに関する世界共通の課題を議論する画期的な場となり、そこからベスト・プラクティスの共有やダイナミック・コアリッション[1]などの具体的な取り組みが生まれた。IGFは意思決定をしないが、だからこそ全てのマルチステークホルダーが参加し、活発な意見交換がなされているところに意義がある。また、IGFが意思決定をしなくても、そこでの議論を通じて、政府、企業、市民社会等の参加者の今後の行動に影響を与えうることから、インターネット社会をより良い方向へ導くための「種まき」をしていると言える。マルチステークホルダーに対してこのような形で議論の場を提供できるのはIGFのみであり、今後も自由な立場から様々な議論を継続していくことが必要である。

今回は、特に途上国の民間部門により多く参加してもらい、アクセスや、国際的セキュリティ水準の向上における具体的なダイナミック･コアリッションが新たに生まれることを期待したい。

さらに、インターネット・ガバナンスに関する議論が、国際的に一層活性化することを期待する。日本経団連は今年５月、Kummer 国連 IGF 事務局長を始めとする主要関係者を東京に招き、IGF 東京会議を開催した。IGF は年１回の開催で、しかも開催地によって参加者に偏りが生じる。東京会議のように、一定の国や地域内でマルチステークホルダーが議論する場を設けることは、その国・地域における議論の活発化やインターネット・ガバナンスの重要性の認識度向上に繋がり、非常に有意義である。その意味で、東京会議自体が一つのベストプラクティスであり、IGF としても世界各国・地域でのこのような会議の開催を推進し、インターネット・ガバナンスに対する意識を世界的に高めてもらいたい。

日本経団連は、第２回IGFにおいて、特に健全かつ安全なインターネット社会構築に資する日本の取り組み事例として、民間の自主的な取り組みによって違法コンテンツ等を排除することを目的としたプロバイダ責任制限法、及びボット[2]対策としてのサイバークリーンセンターについて説明を行い、参加者の参考に供する予定である。

また、「情報セキュリティに関するキャパシティビルディングのための国際協力」、及び「途上国のインターネット・アクセスの向上に向けた課題」の二つのワークショップを関係団体とともに主催し、具体的な問題の解決に向けた対話を進める予定である。

---

[1] ダイナミック･コアリッション：IGFにおいてマルチステークホルダーによる議論やワークショップ等を通じて、政府、企業、市民社会の枠を超えて具体的なアクションに繋がる連携や協力関係が築かれたことを指す。

[2] ボット：コンピュータウィルスの一種で、ボットに感染したPCはインターネットを通じて特定の”指令者”からの命令に従い遠隔操作を受けるようになる。感染してもPCの処理速度が落ちるなどの兆候が現れないため、ユーザーはボットの感染に気づかないまま、サイバー攻撃等に加担することになってしまう。全世界で発信されているスパムメールの半数以上がボットによるものとの推計もある。

Ⅲ．日本経団連の基本的見解

第１回IGFでは、メインセッションのテーマとして、″アクセス[3]″、″開放性[4]″、″セキュリティ[5]″、″多様性[6]″の４つのテーマが設定された。第２回IGFでは、４つのテーマに″重要インターネット資源[7]″を加えた５つのテーマについて、メインセッションで議論する。これら５つのテーマに関して、日本経団連の基本的見解を以下に述べる。

１．重要インターネット資源

重要インターネット資源の管理運営の在り方に関しては、世界情報社会サミットで十分議論された結果、現行の体制を維持すべきとのコンセンサスに至ったと理解している。また、IGFはICANN[8]に対して勧告等をする立場にはなく、議論の成果を供するという役割にとどまる点に留意すべきである。したがって、IGFの場では、重要インターネット資源について過去の議論を繰り返すのではなく、より建設的な議論が展開されることを期待したい。

現行の体制の下、インターネットは有効に機能し、健全な発展を継続している。様々な課題も発生しているが、課題は発展に伴い必然的に発生するものである。健全な発展の継続には、技術革新や環境変化に柔軟に対応できる民間部門が、インターネットの管理運営を担当していることが大きく貢献している。仮に各国政府が主導する国際機関が管理運営を行うことになった場合、各国政府の政治的な利害対立等により迅速な意思決定が妨げられ、市民生活やビジネスに多大な影響が及ぶ可能性がある。したがって、インターネットの管理運営については、現状の体制を維持していくべきである。

２．アクセス

デジタル・デバイド解消に向けて、途上国におけるインフラ整備に係る技術支援の継続は不可欠である。特に農村部等、十分なインフラが整っていない地域において、地域共同体のパブリック・スペースにインターネット端末を設置するなど、アクセス機会の提供に取り組むことが重要である。

また、インフラ整備と並行して、利用者を対象にインターネットの適切な

---

[3] アクセス(Access)：特に途上国や過疎地域における、インターネットへのアクセス機会の提供等に関する議論を行う。

[4] 開放性(Openness)：表現･言論の自由とプライバシーや知財権の保護とのバランス、有害コンテンツの取扱い等に関する議論を行う。

[5] セキュリティ(Security)：サイバー犯罪やスパム、ウィルス感染への対策や本人確認に係る技術等に関する議論を行う。

[6] 多様性(Diversity)：インターネットサービスの多言語化や、高齢者･身体障害者がアクセスしやすい環境整備等に関する議論を行う。

[7] 重要インターネット資源(Critical Internet Resources)：IPアドレス、ドメインネームの割り当て等、インターネットの管理・運営に関する議論を行う。

[8] ICANN：Internet Corporation for Assigned Names and Numbersの略。インターネット上で利用されている、IPアドレス、ドメインネーム等の標準化や割り当てを行っている民間の非営利団体。

利活用に向けた啓蒙・教育を実施する必要があり、先進国等においては人材・教材・ノウハウ等の支援を行うべきである。

３．開放性

インターネットへのオープンアクセスとインターネットにおける表現･言論の自由は、インターネット社会の発展に不可欠なものであり、最大限尊重されるべきである。

著作権侵害やプライバシー侵害等となりうる違法コンテンツ、わいせつな内容を含む有害コンテンツ等に関しては一定の規制が必要である。コンテンツの規制に関しては、政府主導の規制に頼るばかりではなく、民間部門が主体となって自主規制に取り組むべきである。

自主規制の具体的な手段として、フィルタリングがある。一定のフィルタリングは技術的に可能であり、実際に有償/無償で提供されているフィルタリングソフトもあるが、現状ではユーザーの使用率は低い。事業者はフィルタリング技術の向上に努めるとともに、一層の周知徹底を図るべきである。

また、プロバイダの自主規制も違法コンテンツ等の排除に有効である。日本では、法律によってプロバイダの自主的な取り組みを促進し、著作権やプライバシーの保護と表現･言論の自由のバランスをうまく取っている。日本で実施している具体的事例については、別紙で紹介する。

ネットワーク上で多くの知を結集することにより、新たな創作活動が促進される。著作物の自由な利用や相互連携は産業・文化の発展に寄与することから、権利保護と利活用促進の新たなバランスを構築していくことが必要である。

４．セキュリティ

インターネットは情報社会の基盤であり、誰もが安心して利用できる安全なインターネット環境の実現は最重要課題の一つである。しかし、一般利用者が出所不明メールの添付ファイルを不用意に開けてウイルス感染したり、ボット等により意図せずに犯罪に加担してしまうケースが後を絶たない。このように、セキュリティの教育・啓発が不十分なまま利用者が増えると、インターネットの利用そのものがリスク拡大に繋がることになるため、利用者への啓蒙活動や注意喚起によるセキュリティ意識向上を図ることが急務である。

また、インターネットの世界に国境は無く、サイバー犯罪は国境を越えて行われるものがむしろ一般的であるため、セキュリティ対策においては国・地域ごとの個別対応では十分な成果が出ない。その上、どこか一カ所でも対策レベルの低い国・地域があると、そこが犯罪の温床となりかねない。したがって、国際社会が一致団結し、セキュリティ対策のノウハウやベストプラ

クティスを共有するとともに、協調して対策に当たるための仕組み作りを目指すべきである。

各国のCSIRT[9]は、FIRST[10]を通じてセキュリティ情報の交換を行っており、セキュリティ・インシデントの早期検知、対応と再発防止を目的とした国際的な情報共有のための枠組みとして有効であると思われる。CSIRTが存在しない国・地域は、まずはNational CSIRTの設置を積極的に検討すべきであり、国際機関や先進諸国においては人材やノウハウの提供による支援を推進すべきである。

特に、途上国においては、アクセス機会提供及び利用方法の教育と同時に、セキュリティ面の教育も欠かすことはできない。先進諸国等支援する側としても、この視点を持って"アクセス"と"セキュリティ"の取り組みを並行して推進するべきである。

なお、日本において官民連携で取り組んでいるボット対策の具体的事例を、別紙で紹介する。

５．多様性

言語の違いによるデジタル・デバイド解消に向けて、各種アプリケーションの多言語開発や多言語ドメイン名の開発は今後も継続していかなければならない。

そして、文化・言語の多様性が尊重され、利用者間のコミュニケーションが一層促進される社会の実現に向け、国際的支援を推進すべきである。

また、高年層の利用者や身体障害者がストレス無くインターネットを利活用するための技術やノウハウを、マルチステークホルダーが持ち寄り共有することが重要である。

[9] CSIRT：Computer Security Incident Response Teamの略。コンピュータセキュリティに係る事故や不具合への対応、分析、啓蒙、研究開発等を行っている組織の総称。所属する組織や目的によってCSIRTのあり方も異なる。JPCERT/CC(民間非営利団体)、NTT-CERT(NTTグループ)、HIRT(日立グループ)等、多数のCSIRTが存在する。

[10] FIRST：Forum of Incident Response and Security Teamsの略。世界各国のCSIRTやセキュリティチームが集まり、コンピュータセキュリティ問題について議論する国際的なフォーラム。

Ⅳ．おわりに

インターネットの発展によって、全てのステークホルダーが恩恵を享受すると同時に、様々な脅威に晒されていることは、これまで述べてきたとおりである。インターネット・ガバナンスの重要性は改めて強調するまでもないが、政府による規制が行き過ぎると、検閲によって表現･言論の自由が損なわれたり、インターネットの自由なアクセス機会が奪われるなどの弊害が生じる虞がある。

インターネットの発展は、技術革新や環境変化に最適な民間主導による運営に負うところが大きく、国際機関等の管理によって、その安定性、成長、自由な表現･言論の場としての特徴が失われるようなことがあってはならない。重要なのは、政府、民間、市民社会が互いに連携し、適切なバランスを保ちつつ、それぞれの役割を果たすことである。そのためにも、世界各国のステークホルダーが、インターネットの健全な発展のために、IGF において議論を継続していく必要がある。

なお、本提言は、日本の産業界としてインターネット・ガバナンスについて議論した結果であり、基本的スタンスや主要論点において ICC(国際商業会議所)をはじめとする世界の産業界と意見の多くを共有している。本提言における日本産業界の意見が、IGF の議論に貢献することを強く期待する。

以　上

別紙：健全なインターネット社会の発展に向けた官民連携の取り組み

日本において、健全なインターネット社会の発展のため、インターネット・ガバナンスに関連して実施している取り組みを紹介する。

インターネット・ガバナンスへの取り組みにおいては、政府による規制だけでは迅速性、柔軟性に欠ける一方、民間だけでは法整備、インフラ整備等が困難である。

そこで日本では、政府が法整備、インフラ整備や枠組み作りを担い、中身に関しては民間に委ねて自主規制を促すなど、官民の役割を明確にして連携することにより、対策のスピードアップを図りつつある。

国によって法律や環境等が異なるため、各国の状況に合わせてアレンジする必要はあるが、被害者、加害者がクロスボーダーで存在する場合に各国で対応の窓口をワンストップ化し、対策の足並みを揃えるうえで、下記の事例を参考に供したい。

１．プロバイダ責任制限法と民間協力の事例

著作権やプライバシーの保護と表現･言論の自由のバランス構築において自主規制が有効に機能している例として､2002 年に制定されたプロバイダ責任制限法と民間協力の事例を紹介する。

（１）概要

インターネット上のホームページや掲示板において、名誉毀損、プライバシー侵害、著作権侵害等、特定の者の法益が侵害される書き込みが行われた際に、以下の枠組みを整備。

①どのような場合であれば、掲示板等の運営者(プロバイダ等)が当該書き込みを削除しても(しなくても)免責されるかについての基準を明確化

②被害者が、匿名で当該書き込みを行った者の氏名、住所等の情報の開示を請求する権利を創設

具体例として、インターネット上の掲示板に名誉を損なうような書き込みをされたユーザーが、書き込み情報を削除してほしい場合を想定する。

〔本法施行前〕

①当事者間で問題を解決しようとしても､発信者が情報削除に応じない、または発信者が誰だか分からない場合があった。

②被害者がプロバイダ等に対し、書き込み削除を要求しても、書き込み情報の違法性の判断が困難であり、容易には書き込み削除ができなかった。また、被害者がプロバイダ等に対し、発信者情報の開示を請求

しても、「通信の秘密」の観点から、容易には情報開示に応じてもらえなかった。

〔本法施行後〕

①被害者から書き込み削除の申し出があっても、以下のいずれにも該当しなければ、プロバイダ等は書き込みを削除する必要がない。（責任を問われない）

・他人の権利が侵害されていることを知っていた場合

・他人の権利が侵害されていることを知ることができたと認めるに足りる相当の理由がある場合

②以下のいずれかに該当する場合は、プロバイダ等は書き込み情報を削除することができる。（削除しても責任を問われない）

・他人の権利が侵害されていると信じるに足りる相当の理由があった場合

・削除の申し出があったことを発信者に連絡し、７日以内に反論がない場合

③発信者情報開示請求の要件が明示されるようになり、被害者は開示の要請や、開示請求訴訟を起こしやすくなった。

（２）官民の役割分担

①政府部門

(i)実効性があり、かつ必要最低限のルール策定

「表現の自由」及び「通信の秘密」と「被害者救済」とのバランスを是正するために、必要最低限のルールとしてプロバイダ責任制限法を策定。ガイドライン作成は民間に委ね、自主規制を促進している。

(ii)法制面のフォローアップ

各種ガイドラインを作成する「プロバイダ責任制限法ガイドライン等検討協議会」（以下「協議会」という）は民間主導で組織されているが、政府もアドバイザー・オブザーバーとして参加し、法制面での支援を行っている。

(iii)法務省人権擁護機関による個別フォロー

インターネット上で人権侵犯の事実がありながら、被害者自ら被害の回復予防を図ることが困難な場合には、法務省人権擁護機関が対応。これにより、例えば、犯罪を犯したとされる少年の顔写真等がインターネット上に掲載された場合に、当該機関から削除要請を行うことができる。また、被害者に対して、対応方法に関する助言等も行っている。

②民間部門

(i)民間主導でガイドラインを作成

(社)テレコムサービス協会[11]を中心として、民間が主体となって「協議会」を結成し、実務上の行動指針となるガイドラインを作成。これまでに、以下４件のガイドラインを作成した。

・名誉毀損･プライバシー関係ガイドライン
・著作権関係ガイドライン
・商標権関係ガイドライン
・発信者情報開示関係ガイドライン

(ii)「信頼性確認団体」経由の削除申請スキームを確立

協議会は、著作権と商標権の侵害に関し、ガイドラインにおいて、被害者本人ではない「信頼できる第三者」による削除申請手続きについて明確化した。協議会が、「信頼できる第三者」であると認定した団体を「信頼性確認団体」と呼び、これまで、著作権関係につき 11 団体、商標権関係につき１団体が認定されている。

（３）成果と今後の課題

・これまでは、表現の自由や通信の秘密が憲法によって保障されていることから被害者が泣き寝入りするケースも少なくなかったが、プロバイダ責任制限法施行以降は、被害者の訴訟が認められるケースが増加。
・プロバイダ責任制限法の円滑な運用のため、「プロバイダ責任制限法ガイドライン等検討協議会」を結成し、実務上の行動指針となるガイドラインを作成するなど、民間主導の動きが活発化。
・プロバイダ責任制限法に基づく自主規制により、表現･言論の自由と著作権･プライバシー等保護のバランスを確保。
・信頼性確認団体の中には、これまでに 25 万件を超える削除要請を実施している団体もあり、プロバイダ責任制限法の円滑な運用に貢献している。
・インターネット上の掲示板等書き込みにおける、一般ユーザーのモラル向上が今後の課題。

[11] (社)テレコムサービス協会：電気通信事業者及び情報通信関連事業者を中心とする業界団体。1994 年 8 月に発足し、会員企業数は約 300 社。電気通信及び情報通信関連事業の競争市場における健全な発展や安心･安全なネットワーク社会の実現を目指す。

２．サイバークリーンセンター

ボット対策における官民連携事例として、サイバークリーンセンターを紹介する。

（１）概要

ボット対策を目的とした総務省と経済産業省の連携プロジェクトで、2006年度から5カ年計画で、国内のボット感染者の撲滅を目指している。

〔運営体制〕

①サイバークリーンセンター運営委員会

総務省、経済産業省、Telecom ISAC Japan[12]、JPCERT/CC、IPA[13]等からの委員によって構成され、センターの活動方針や活動内容について総合的な検討を行う。

②ボット対策システム運用グループ

Telecom ISAC Japan、ISP[14]各社の連携により、ボット感染ユーザーへの注意喚起及び対策情報の提供を行っている。

③ボットプログラム解析グループ

JPCERT/CC、トレンドマイクロ社の連携により、ボットプログラムを解析し、駆除ツールを開発する。

④ボット感染予防推進グループ

IPA、及びソースネクスト、マイクロソフト、マカフィー、シマンテック等のセキュリティベンダとの連携により、各ベンダの対策ソフトのパターンファイルに最新のボットプログラムの情報を反映し、一般ユーザーにおけるボット感染予防策の強化及び再発防止を図る。

〔業務フロー〕

①ハニーポット[15]によるボットウィルス検体収集

②収集した検体から未知の検体を選別・解析し、駆除ツールを作成

③駆除ツールをサイバークリーンセンターのサイトで公開

④一方、ボットウィルス感染が認められたユーザー宛てに注意喚起メ

---

[12] Telecom ISAC Japan：コンピュータセキュリティに係る事故や不具合に対処するため、通信業界内での情報共有や連携を目的として、平成14年7月に発足。会員企業は、インターネットサービスプロバイダーを中心に18社。

[13] IPA：独立法人「情報処理推進機構」。1970年10月に情報処理の振興を図ることを目的として、特別認可法人「情報処理進行事業協会」が設立されたが、特殊法人の独立行政法人移行に伴い、2004年1月に解散し、独立行政法人として新たに発足した。

[14] ISP：Internet Service Providerの略。電話回線や光ファイバー等を通じ、顧客である企業や家庭のPCをインターネットに接続するサービスを提供する業者。一般にプロバイダと呼ばれる。

[15] ハニーポット：サイバー犯罪者をおびき寄せる罠としてインターネット上に設置されたPC等の機器のこと。サイバー攻撃を受けたりウィルスに感染したハニーポットを調査することにより、サイバー犯罪の手口やコンピュータウィルスの振る舞いを研究・分析することができる。

ールを送信

⑤注意喚起メールを受信したユーザーは、メールの指示に従い駆除ツールをダウンロードしボットを駆除

⑥駆除ツールの内容を各ベンダ提供対策ソフトのパターンファイルに反映

（２）官民の役割分担

①政府部門

(i)連携プロジェクトの立ち上げ

総務省と経済産業省が共同でボット撲滅を目指したプロジェクトを立ち上げ、サイバークリーンセンターの運営の枠組みづくり、参加の呼び掛けを行った。その結果、プロバイダからベンダー企業まで業界横断的かつボット撲滅のための総合的な運営体制を整えることに成功している。

(ii)運営委員会の設置

総務省と経済産業省が中心となり、民間からも委員を入れて「サイバークリーンセンター運営委員会」を設置。センターの活動方針を決定する、いわば頭の役割を担っている。

②民間部門

(i)実行部隊としての役割を遂行

それぞれのグループ参加企業が、実際の業務フローを回している。

(ii)情報･技術供与

ボットプログラムの分析･駆除ツールの開発などを担当し、ボット対策に不可欠な情報･技術を供与している。

（３）これまでの実績（2007 年 6 月現在）

・ボットの収集検体数は累計約１３７万体
・駆除ツール作成検体数は累計約３，５００体
・サイトに公開している駆除ツールを毎週更新
・発信した注意喚起メールは累計約７２千通
・駆除ツールのダウンロード回数は累計約１３万回
・各ベンダによる自身の取り組みとして、駆除ツールの内容を提供対策ソフトのパターンファイルに１ヶ月以内に反映

（４）今後の課題

・現在の参加 ISP は８社で、国内ユーザーの６割強をカバーしている。今後は参加 ISP を拡大し、カバー率を引き上げる必要がある。

・ボットプログラムはより悪質･巧妙になり、一部ではハニーポットを選別する機能を備えつつある。そのため、ハニーポットの構成も断続的に変更していく必要がある。

以　上