

経済人コーポラ卓会議日本委員会
ニッポンCSRコンソーシャム
2015 Stakeholder Engagement Program

ICT業界と人権課題

2015年6月10日

(株)国際社会経済研究所
代表取締役社長 鈴木 均

(株)国際社会経済研究所の紹介

(IISE : Institute for International Socio-Economic Studies)

- **NECグループのシンクタンクとして、人と地球にやさしい情報社会のあるべき姿を中立的立場から調査研究します。その成果を国内外に向けて発信し、日本および国際社会の持続可能な発展に貢献します**
- **主な調査・研究テーマ：**
情報セキュリティ、国民ID、高齢化・eHealth、都市のスマート化（セーフティ、防災、交通、エネルギーなど）、サイバー空間、新興国・途上国等での社会課題解決に向けたICTの可能性や市場機会、日本企業が目指すべき持続可能な経営など

「ICTビジネスと人権」について

ICT事業は、ハードウェアの製造からソフトウェア開発、システムインテグレーション、サービス事業運営など多様で幅広い事業領域を含む

人権 이슈の捉え方もドメインごとに違いがあるが、ICT事業に共通する特徴的な人権リスクとしては、「個人情報保護・プライバシーに対する侵害」が挙げられる

プライバシー問題が グローバルに拡大する主な背景



- 技術や経済のグローバル化の急速な進展
- 個人の権利意識の向上の拡大



- スマートフォン、監視カメラ、IoT機器(ウェアラブル端末、スマートメーター、車載センサー等)など個人データ収集手段の高度化
- ビッグデータ活用によるデータ価値の高まり



- SNSなど個人によるデータ公開・共有化の拡大
- クラウドコンピューティング等による越境データ流通の増大など

ICTビジネスにおける正の面と負の面 (1)

(1) 社会保障政策などの公平性とプライバシー

- ・ 国民IDに代表される国民基礎情報の整備と管理は、公平で効率的な社会保障政策(生活保護手当、教育手当、健康保険、医療手当、乳幼児向け予防接種管理、選挙権付与など)の実現とその展開という基本的人権に関わる行政サービスの提供には不可欠。特に途上国では一般的に文盲率の高さから指紋認証技術などの生体認証技術を活用した個人(市民)の特定が不可欠
- ・ 一方、その管理に脆弱性があると個人情報やプライバシーが漏えいするリスク、さらには市民の管理につながるリスクがある。国によっては、国家安全保障やテロ、また防犯対策上、個人情報の管理や監視などが優先され、また消費者などの個人情報の提出要求に対応せざるを得ないケースがある。これらの行動によって人権監視団体等から批判等を受けるレピュテーションリスクが通信業者、インターネット関連企業、行政サービス受託企業などで存在

ICTビジネスにおける正の面と負の面 (2)

(2) 市民の安全とプライバシー

- ・ 市民の安全を守る監視カメラネットワーク(顔認証技術の活用も含む)は防犯対策には有効で世界的に導入が拡大する傾向にある
- ・ 一方プライバシー侵害のリスクもある

(3) ビッグデータビジネスとプライバシーなど

- ・ 消費者向けビッグデータ活用による革新的なサービス事業の創出に、別目的で収集した個人情報間接的に活用することにより発生するリスク(例: JR東日本のSuicaを巡るプライバシー問題)
- ・ 最新のハイテク技術を活用したシステム(ドローン、準天頂衛星・GPSなど)やGoogleなどによる情報収集展開事業などもプライバシー侵害リスクが高い

人権リスク(プライバシー問題)を軽減する対策(1)

(1) 政策的展開:ルール作り

- ・ 国家の安全保障とICTによる経済発展は重要なテーマだが、人権(プライバシー権利)は優先されるべき権利
- ・ 企業の自由裁量度を高めることはイノベーション創出に必要な要件だ。一方歴史を見ても、一定のルール化も新事業の発展の基盤となり不可欠(例:自動車における交通ルールなど)
- ・ 政府主導によるルール作りに加え、インターネットの性格から **国際的な共通ルール作り**も必要
- ・ 業界によるイニシャチブやコラボレーション(JEITAなど)

人権リスク(プライバシー問題)を軽減する対策(2)

(2) 企業自身の取り組み: 人権デューディリジェンス

- 基本的には他分野と同様、デューディリジェンスに基づくマネジメント施策展開(方針策定⇒影響評価⇒組織への統合⇒パフォーマンス評価⇒救済措置)が重要
 - 事業の合従連衡が進んでいるので、バリューチェーンへの施策展開は不可欠
- 会社と社員のリスク感度の啓発にあたっては、例えば経営層に加え、行政システムやビッグデータビジネスの開発、マーケティング、サービス事業などに関わっている事業部、関係会社等の関係者(開発、営業、SEなど)をパイロットとして、事業活動や製品・サービスが社会にどのような負の影響を与えるかを検討・抽出する取り組み(影響評価: Impact Assessment)を実施
- 社外有識者、人権関係のNGOなどを交えたステークホルダー・エンゲージメントが効果的

人権リスク(プライバシー問題)を軽減する対策(3)

(2) 企業自身の取り組み: 人権デューディリジェンス

- ・ 特に個人情報等の機微な情報を扱うシステム事業の展開には以下のような取り組みが重要
 - ・ **プライバシー・バイ・デザインの採用**: 設計段階からプライバシー保護を組み込むシステム開発の基本的概念
 - ・ **プライバシー・インパクト・アセスメント(PIA)**: 個人情報収集を伴う情報システムの企画、構築、改修にあたり、情報提供者のプライバシーへの影響を「事前」に評価し、情報システムの構築・運用を適正に行うことを促す一連のプロセス

仕組み構築、社内教育に加え、社内関係部門(事業部、営業、SEなど)と社外ステークホルダー(社外有識者、人権NGOなど)によるPIAのパイロットをワークショップ形式で開催など

プライバシー問題を除いたICT産業に特徴的な人権リスク（ステークホルダー別）

ICT産業に特徴的な人権 이슈(ステークホルダー別)(1)

従業員

(バリューチェーンも含む)

- ・ 労働集約的であるソフトウェア産業やSEに代表されるシステムインテグレーション事業は 超過勤務(労働時間)、残業代不払いなどの労働問題リスクがある
- ・ 長時間労働等がメンタル等の安全衛生にも影響。
- ・ 過度のノルマによる長時間労働が事実上の強制労働となる恐れ。
- ・ データセンター、通信網敷設(アンテナ、タワー等)の設置による労働安全上のリスクなど

お客様・消費者

(製品・サービスの不具合などに関連する人権リスク)

- ・ 通信システムなどICTの不具合による社会生活および身体・生命への悪影響(通信インフラ停止、消防防災等緊急通信網の遮断、停電、交通網の遮断、金融決済、行政サービスの停止など)
- ・ 健康と安全の問題(発火等の製品の安全性問題、ICTパフォーマンスが確保されないために発生するシステムの欠陥や事故・災害など、電子機器不具合を原因とする機械や自動車、またプラントや医療機器の故障や事故など)
- ・ 先進性の高いハイテク製品(ドローン、遺伝子解析技術など)の瑕疵や操作ミスなどによる事故など

ICT産業に特徴的な人権 이슈(ステークホルダー別)(2)

お客様・消費者

(情報の管理、表現の自由などに関連する人権リスク)

- ・ インターネット管理事業者やサービスプロバイダー等で、不正サイトや児童に悪影響を与えるサイト、ヘイトスピーチなどの誹謗中傷に関わる投稿等を放置することによる人権侵害に加担するリスク
- ・ 人権侵害と表現の自由との板挟みになるリスクなど

コミュニティ

(一部、お客様や消費者も対象)

- ・ データセンターによる地域環境への影響(低周波騒音など)
- ・ 電波や放送送信機が発生する高周波による影響
- ・ 電子機器の不適切な廃棄による環境汚染など

ICT産業に特徴的な人権イシュー(ステークホルダー別)(3)

政府

(途上国を中心に)

※加担の可能性

- ・ 賄賂(通信網、政府向け基幹システムなどの受注活動等を通じて、また迂回寄付などにより生じる)
- ・ ミャンマー等の途上国を中心に発生する先住民や少数民族の問題(通信網や携帯基地局等の設備整備に関し少数民族の土地等を強制的に収用する政府に加担など)
- ・ データセンター事業、クラウドサービスなどに関し、国家権力からの個人情報提供要求に抗しきれないリスク
- ・ 国民ID等の行政システムや政府データセンターの構築や運営受託サービス事業における国民監視・管理、および個人情報保護・プライバシーに対する侵害、保安要員による過剰防衛など
- ・ 表現の自由が保障されない国での通信サービスやプロバイダー事業者への表現の自由に関する過度な干渉や制限など
- ・ 労働基準が国際規範から外れているケースでの労働問題(児童労働など)



ICTと人権【まとめ】

- ICT事業は多様で幅広い領域を含んでおり、従業員、お客様・消費者、コミュニティ、政府などステークホルダー別にさまざまな人権リスクが存在
- ここでは、共通する特徴的な人権リスクとしての「個人情報保護・プライバシーに対する侵害」にフォーカス
- 「個人情報保護・プライバシーに対する侵害」は、ICT業界が特に注意を払うべき人権領域ではあるが、ICTは社会インフラのひとつとして、企業、行政を含むあらゆる組織、産業を支えているツールでもあり、同様のリスクはあらゆる組織に共通
- 既存マネジメントシステム等との紐付け
- ステークホルダー・エンゲージメントの有効性(気づきと感度の醸成)