活動報告

パーソナル情報を活用したビジネスの拡大とプライバシー情報保護

インダストリ・システム部

情報・産業社会システム部会　情報セキュリティ調査専門委員会では、国内外のプライバシーを取り巻く法制度やITを活用した社会経済活動の変化について調査・分析活動を行っております。

昨今、日本国内では、事業者の認識不足やセキュリティ対策が不十分なことによるプライバシー侵害事件が発生しており、日本国内企業へのプライバシー保護の底上げが必要であるとの問題意識から、日本国内のサービス提供者の国際競争力の強化及び損失の低減、日本国内のサービス利用者の更なる保護を実現するために、日本国内の関係者が何をするべきかについて検討を行いました。

1. パーソナル情報を活用したビジネスの拡大

クラウドコンピューティングやビッグデータ、スマートデバイスといったIT技術の進展を受け、アメリカを始めとする欧米先進国では、パーソナル情報を集積し、2次利用するビジネスが広がっています。

日本国内におけるプライバシー情報を活用したライフログ市場規模は、2011年度で約10億円と見込まれていますが、サービス自体はまだ浸透しておらず、有料サービスを提供する一部事業者の売上に占められているのが実態となっています[1]。

サービスの提供形態としては、消費者から取得したライフログを使って、その消費者に対して何らかのサービスを行う形態や、ライフログプラットフォーム事業者が消費者から取得したライフログを第三者の事業者に提供し、その事業者が消費者にサービスの提供を行う形態が考えられます。

サービスの分類	事例	サービス事業者
レコメンド／コンテンツ配信	i コンシェル	NTT ドコモ
Web マーケティング	インターネット視聴率調査	ネットレイティングス
オンライン広告	Google Adwords	Google
販売促進／マーケティング支援	おすすめ商品	Amazon.com
販売促進／マーケティング支援	T ポイントサービス	カルチュアコンビニエンスクラブ
SNS 広告	スポンサー広告	Facebook
O2O	Edy	au	KDDI、楽天
PHR (Personal Healthcare Record)	ポケットカルテ	日本サスティナブルコミュニティセンター

国内における個人情報利活用サービス例[2]

2. 増大するプライバシーのリスク

個人のプライバシー情報を活用したビジネスが広がりを見せる一方で、プライバシーを侵害するような事例も発生しています。特にクラウドサービスについては、サービス提供者のデータセンターが国外にあったり、サービス事業者が国外の事業者であったりとボーダレスな特徴を有しています。データセンターの所在する国の法執行機関によって、予期しないデータの捜索や差押え、データ移転の制限等が考えられます。

1 矢野経済研究所 ライフログ市場に関する調査結果 http://www.yano.co.jp/press/pdf/879.pdf

2 IPA パーソナル情報保護と IT 技術の調査より抜粋 https://www.ipa.go.jp/security/fy23/reports/pdata/index.html

例えば、アメリカでは、2001年9月11日の同時多発テロを受け、テロ対策を目的として米国愛国者法が制定されました。同法では、捜査機関が裁判所の命令なしに通信を傍受できるなどの権限拡充が行われており、実際2009年4月に FBI が米国内のデータセンターを捜索して、サーバ等の設備を押収した結果、当該データセンターを利用していた約50社がサービスを利用できなくなる事態に陥りました。

また、EU では EU データ保護指令が発効されています。EU 域外の国にプライバシー情報を含むデータを移転する場合には、移転しようとする国が、EU データ保護指令が要求するプライバシー情報の保護措置を確保している必要があります。2012年3月時点でデータ保護措置の十分性が認定されている国は、スイス・カナダ・アルゼンチンなど9カ国で日本は含まれていない状況です。結果として、例えば、EU 域内のデータセンターにクラウドサービスを通じてプライバシー情報が保管されている場合、十分なデータ保護措置を取っていると見なされていない日本に対してのデータ移転が制限される可能性があります。

また、グローバルに展開されているクラウドサービスの利用にあたっては、準拠法や裁判管轄に関しても留意する必要があります。契約内容によっては、クラウドサービス事業者が存在する国で裁判を起こさざるを得なかったり、判決内容を執行できないことも考えられています。

欧米では、プライバシー情報を扱うための法制度が整備されつつありますが、日本では、個人情報を保護することを目的とした「個人情報保護法（2005年成立、2007年施行）」の規定しかなく、プライバシー情報を適切に取り扱うための法規制は存在していません。このため、プライバシー情報を利用したビジネスを構築しにくい状況になっています。

また、ビジネスが構築されたとしても安全性が担保されなければ、利用者が不安になりプライバシー情報を提供しないことも考えられ、ビジネスが成長しないことも予測できます。日本にとってのプライバシー保護の課題は、下記のように整理されます。

プライバシー保護の課題	放置によるリスク
産業競争力の低下	アメリカの優位拡大
法制度整備の遅れ	他国の産業保護政策による非関税障壁
プライバシー情報活用の遅れ	ビッグデータ活用機会の損失
プライバシー情報の管理コスト増大	利益圧迫に伴う事業収益悪化
利用者の理解不足	本人特定・公開等のプライバシー侵害

プライバシー保護の課題とリスク

3. プライバシー情報活用の遅れを挽回するための施策（プライバシー・バイ・デザイン）

サービス提供者が、プライバシー情報を効率的に管理するためには、企業全体として統合された規範が必要となりますが、日本ではプライバシー保護の課題への反応は鈍く、国際的展開のキャッチアップも不十分でありました。しかし、国際的な動向へのキャッチアップの重要性は高く、その一環として注目されているのが、プライバシー・バイ・デザイン（Privacy by Design: 以下 PbD）の考え方です。

PbD とは、カナダのアン・カブキアン博士が提唱した概念であり、「技術」「ビジネスプラクティス」「物理設計」のデザイン（設計）仕様段階から、予めプライバシー保護の取り組みを検討し、実践することです。PbD は、システムでの情報利用のみならず、それにとどまらないビジネス慣行（事業活動）、ネッ

トワークインフラなどの情報システムが前提とする環境についても、同様に意識しなければならないことを明確にしています。PbD が目指していることを序文から引用すると以下の通りです[3]。

「従来は、プライバシーを守ろうとすると認証情報を収集できなかったり、あるいはそれまでのビジネス慣行と対立してしまうなど、プライバシーとビジネスのどちらか一方を諦めなければならないゼロサムモデルに基づいていた。しかしゼロサムモデルでは、結果的に IT そのものが利用者に受け入れられず、プライバシーも実現されなかった。このパラダイムをポジティブサムに変えることで、プライバシーの未来はより確かなものになる。」

企業が PbD を導入すると、企業活動にどのような効果が期待できるのでしょうか？
PbD では、7つの基本原則を実践することで「プライバシーの確保」「個人の自己情報に対するコントロール」「組織の持続可能な競争的利点の獲得」を達成できるとしています。

【7つの基本原則】
①事後的ではなく、事前的；救済的でなく予防的
②初期設定としてのプライバシー
③デザインに組み込まれるプライバシー
④全機能的－ゼロサムではなくポジティブサム
⑤最初から最後までのセキュリティ－すべてのライフサイクルを保護
⑥可視性／透明性－公開の維持
⑦利用者のプライバシーの尊重

以上のように、プライバシー情報を活用したビジネスの展開とその課題について見てきました。

日本は、携帯電話での各種サービスや SNS 利用、携帯電話内蔵 IC カードによる決済など、他国に先駆けて非常に高度な IT 利用が進んでいる分野があります。プライバシーに対する独特な考え方や法制度をベースに欧米諸国では発想できない新たなサービスを立ち上げる道もあるのではないでしょうか。
企業としては、顧客のプライバシー権に十分配慮した上で、本当に魅力のあるサービスを国内のみならずグローバルに提供して、多くの顧客が利用するようになることで、各国の法制度や運用にインパクトを与えることもできると考えられます。

3　プライバシー・バイ・デザイン（堀部政夫／一般財団日本情報経済社会推進協会（JIPDEC）編）