【講演レポート】JIPDEC連続ミニウェビナー
「ポストコロナのデータプライバシー　社会実装に向けて」（第4回）

日本におけるこれからのデータプライバシー

一般財団法人日本情報経済社会推進協会（JIPDEC）
電子情報利活用研究部　主席研究員　　寺田　眞治

現在withコロナ、アフターコロナ等という言い方がされていますが、この2つは明確に異なります。withコロナはまさに今現在の状況で、治療法やワクチンが開発されるまでの、ある種特殊な状況です。一方、アフターコロナはひと段落した後の状況で、ここでは以前の形に戻ろうとする力、wihtコロナでの対応をそのまま継続する力、そしてこれまでのものを変化させようとする力が入り交じりながら進んでいく段階です。そこでは、今回のことで明らかになったFactに対しての対応が始まり、縮小・消失するものや、さらに拡大するもの、新たに生まれるものも出てくる可能性があります。

もう一つが、非常に難しい問題ではありますが、次に同じような非常事態/緊急事態が発生した際に対応できる制度やシステムを構築することができるか、という点が大きなポイントになると思います。例えば、今回教育に関してはインフラとしてのネット環境が脆弱、必ずしも家庭に環境が整備されていない等が問題となりました。今後、非常時/緊急時の社会対応制度としては、オンラインでできないことを減らす、社会活動の可用性を確保する、そしてどうしても対応できないものに対しての社会保障を考える、といったことが考えられます。

一方で、今回はテレワークやオンライン教育、遠隔医療等が自由な移動の制限の対策として行われましたが、実際に利用してみると非常時以外の日常でも利便性が高いという点が認識され、その結果、DX、デジタルトランスフォーメーションと言われていたものが可視化され実際に進んでいくのではないかと思われます。

Contact Tracing Applicationは何をもたらすのか

現在、新型コロナ感染追跡アプリが新たなプライバシー問題を提起していますが、実際には現在の個人情報保護法には関係しない機能です。利用者がアプリをダウンロードし起動させると、アプリが一定時間ごとに変更される個人に紐づかないランダムな識別子を発行し、一定時間同じ場所にいた相手の識別子をスマホのBluetoothを通じて記録するものです。この段階では、まず個人情報のやりとりは行われません。実際に個人情報となるのは、利用者が陽性判定された際に感染者として感染者等把握・管理支援システムに登録されるときです。その後、感染者はアプリ経由で陽性判定を通知サーバーに送信することになりますが、ここでも送られるのは識別子のみです。アプリは一定時間ごとに通知サーバーに感染者識別子のデータを読みにいき、実際に自分の端末に同じ識別子が存在した場合に感染者と接触したことが通知されます。また、接触が通知された利用者が感染者等把握・管理支援システムに登録するのは個人情報ですが、登録するかどうかは任意となっています。

それでも、多くの方が不安を感じている理由としては、

1)アプリがインターフェースとして動いているので、アプリ自身が個人情報を扱っているように感じられる。

2)近接者とBluetooth通信するため、本人が認識できないまますれ違った人のスマホに個人情報が記録されているように感じられる。

3)接触者であると通知される仕組みが理解しにくく、ずっと監視されているように感じる。

4)接触者となった後、常に追跡されるのではないかという心配。

5)緊急時という説明に対して強制的な圧力や人権を制限されるかもしれないという不安

といった点が挙げられます。しかし、これらの問題に対応することは簡単ではありません。

理由は、これらは法律で解決するような問題ではなく心理的・倫理的な要因なので、例えば説明しようとしても説明量の多さがさらに不安を掻き立てたり、逆に理解を放棄し惰性的になってしまうということが起きてしまいます。今回のアプリに関しては、事細かに説明するよりもいかに信頼されるかに注力する方が理解が得やすく、その方法としては、利用者が納得できるような第三者の関与と透明性が重要なポイントになると思います。

また、今回政府はプラットフォーム事業者に対して情報提供の要請を行っています。これも個人情報の提供ではなく、さらにデータ廃棄も宣言していますが、国家による個人監視ではないか、情報の不正利用ではないかといった不安・不満が払しょくできていないため、要請されたプラットフォーム事業者が協定内容を精査したり、提供の可否を第三者委員会に諮る等、炎上リスク軽減の対策を強いられています。これは、プラットフォーム事業者以上に国、政府が信頼されていないということで、これまで政府がプラットフォーム事業者に対して透明性向上等の規制を課していましたが、今回、政府自身もプラットフォーム事業者に求めてきた規制と同様の対応を迫られることになりました。そして、この一連の問題は、今後プラットフォーム事業者以外の事業者に対しても迫られる問題となってきます。

これまでは個人情報の保護が企業として配慮すべき点でしたが、現在考慮すべき対象として議論になっているのはその外側にあるプライバシーです。しかし、先ほどお伝えした通り、このプライバシーというものは対象、環境によって変化するものなので、個人情報保護のような法令遵守だけではなく、本人の情報を使用した結果として相手に差別や不利益、不安を与えない配慮が求められます。

これからのデータプライバシー

データプライバシーに関する課題としては、

1)　透明性確保が困難（説明が必要な内容や接点が複雑化・多重化し、結果としてわかりにくい。）

2)　同意取得、本人関与の確保が困難（ユーザーが同意内容や問い合わせ先を把握しきれない、パーソナルデータ取得が常態化、IoT等本人が不可知な状況でのデータ取得増大、第三者提供による流通先の増加　等）

3)　プライバシー保護の基準がない

4)　レピュテーションリスク（プライバシー以外の誤解、企業と消費者の意識・感覚のずれ等）

があります。このうち、３、４がいわゆるプライバシーガバナンスの問題です。

１つめの透明性確保に関しては、説明事項の整理・構造化、説明タイミングの標準化が対策として考えられますが、単なる形式化はかえって相互不信を招き、結果として実効性を確保することができません。同意取得や本人関与の確保に関しても同様で、最初に完全な形で同意を取得することは事実上困難という前提で、何か疑問が発生した際に対応できるような体制を作ることが現実的な対策になってきます。さらに、今後考える点として、3~4にあたる個人情報の外側にあるプライバシーへの対応があります。

これに関しては、政府や民間団体等でプライバシーガバナンスをコーポレートガバナンスの１つと位置づけ内部統制の仕組みを構築・運用することも検討されています。具体的には、

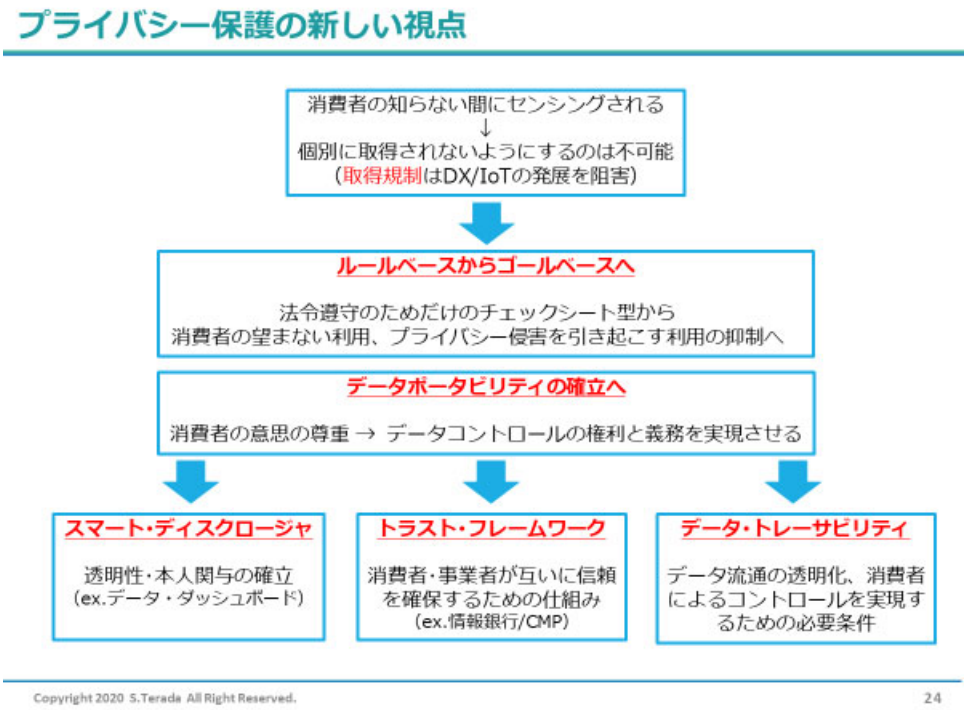
1)プライバシーに対する組織の姿勢を明文化し公表する
2)プライバシーに関する責任者を設置
3)取り組むためのリソース投入

をした上で、プライバシー・バイ・デザインに基づいたリスク管理を行うとともに、従来のコーポレートガバナンスと同様にその取り組みを理解してもらえるようステークホルダーとコミュニケーションを図っていくことが重要となります。このコミュニケーションの部分について、アカウンタビリティという言葉が使われますが、この真の意味は、単に説明をするということではなく、説明した内容を実行していることを証明する、さらに誤りがあれば責任を持って訂正する、というところまでが含まれます。これまでのコーポレートガバナンスでは「Comply or Explain」でしたが、プライバシーガバナンスでは「Comply and Explain」が求められており、実際にNTTドコモ等が組織としての姿勢を宣言し、それに基づいた行動原則を提示しています。

そして、実際にこの原則の下で、事前に企画段階から保守段階までのプライバシー対策を考慮（プライバシー・バイ・デザイン）して設計し、PIA（プライバシー影響評価　GDPRではDPIAにあたるもの）によりリスク管理を行うことで、ステートメントの内容の実効性が確保されることになります。PIAに関してはISOで標準化が進んでおり、年内または年明けにはJIS化されるので、これに基づいて実施することで有効性が認められることになると思います。

PIAの中には、責任者や組織についても規定されているので、組織の中でのプライバシー対応体制を考える際のベースになると思っています。また、コミュニケーションについては、対顧客はもとより、取引先に対してもサプライチェーン全体の信頼を高める上で重要なポイントとなります。

IoTが進展し、消費者が意識しない状況でのセンシング等も行われている中では、ルールベースの事前チェック型からゴールベースで「結果としてプライバシー侵害を引き起こさないために」必要な対策を取れる組織作りを行うとともに、消費者の意思を尊重できるデータポータビリティ等の仕組みも必要になってきます。



すでに民間企業や業界団体、行政等で様々な取り組みが始まっているので、ぜひ参考にして、自組織のこれからのプライバシーガバナンスを検討していただきたいと思います。

JIPDEC電子情報利活用研究部　主席研究員　寺田　眞治

•データ流通における個人情報を含むプライバシー保護に関する政策、法制度
•IoT、ITセキュリティに関する政策・法制度
•インターネット上のマーケティング、メディア、コンテンツビジネス
等に精通。
総務省、経済産業省、消費者庁や関連機関の通信事業、海外進出、消費者保護、個人情報保護、データ流通、セキュリティ関連の有識者会議の委員等を歴任。

本内容は、2020年5月28日に開催されたJIPDEC連続ミニウェビナー「ポストコロナのデータプライバシー社会実装に向けて」「第4回　日本におけるこれからのデータプライバシー」講演内容を取りまとめたものです。