

【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3回)
エストニアにおける新型コロナ対応-官民連携、データプライバシー-

NORDX Legal Partner, Attorney at Law
Risto Hubner氏

エストニアについて

エストニアは、北側はフィンランド、スウェーデン、東側はロシア、南側はラトビア、リトアニアに接する人口約130万人の比較的小さな国です。いわゆる大企業と同じ程度の規模なので、国の様々な取り組みも企業プロジェクトのように迅速に試行することができます。人口は日本の約1/100で、自然が多くオランダとほぼ同じ国土面積です。。

WTOやOECDといった主だった国際機関にも加盟しており、GDPの約6%をICT産業が占めています。また、特長の1つに活発なスタートアップコミュニティがあります。評価額10億ドル以上のユニコーン企業も4社誕生しており、現在1,000以上のスタートアップが活動しています。

1.エストニアの電子政府の仕組み

エストニアの電子政府には、Once Onlyの原則があります。政府機関が市民からデータを収集するのは1回限りとしています。この目的は、煩雑な手続きの排除と時間削減です。エストニア政府のほぼすべてのサービスは、オンラインで可能となっています。。もちろん、希望する人は窓口に行くこともできますが、基本的にすべての人がオンライン上でデジタルに手続きを行うことが優先されています。

ここで重要な点は、「役所の煩雑な手続き」がなく高度にデジタル化されているため、透明性が高いという点です。この透明性によって、一般の人はシステムを本当に信頼できるようになっています。具体的にいうと、公共機関が私のデータを確認した場合、市民である私もシステムで誰が何のデータを調べたのかを確認することができます。例えば、私が医療データを医師に公開する場合は、どの医師がそのデータにアクセスしたかも確認することができます。

現在、エストニアの公共サービスの99%がオンラインで24時間年中無休で利用可能となっています。数回クリックをするだけで、真夜中に約20分で自分の会社を立ち上げることもできるのです。ただし、結婚と離婚の手続きはオンラインではできません。これは技術的な問題ではなく、重要な意思決定だからです。また、不動産取引も公証人の証明が必要だったため、これまではオンラインではありませんでしたが、数か月前にデジタル公証を使ったオンライン手続きが可能となりました。

安全にデータを守る仕組み

この電子政府の仕組みが安全に機能するために重要な要素が、X-Roadと呼ばれる分散型データ連携基盤と、すべての個人に発行されているデジタルIDです。

1) データ取引

X-roadsは、2001年に運用が開始されすでに19年経過しています。オープンソースとしているため、すでに世界の多くの国でも利用されています。エストニアのX-Roadは分散型システムでエストニアに

は集中型のデータベースはありません。それぞれが個別にデータベースを持っており、他のシステムにあるデータが必要になると、X-Road上で他のデータベースの情報を参照できます。これにより、年間約300万時間分の作業が削減できると言われています。現在、X-Road上で年間約13億トランザクションが実行されています。

また、興味深いのは、このX-Roadに接続できるのは公共機関だけではなく電気通信会社や金融機関等の民間企業も含まれている点です。そのため、セキュリティ確保は重要な側面となります。X-Roadではデータ改ざん検知にブロックチェーン技術が用いられています。

2) デジタルID

X-Road運用開始から1年後にデジタルIDの発行が開始されました。ここで重要な点は、このデジタルIDは全国民が取得することが義務付けられている点です。実際に広く使われるまでには数年かかりましたが、普及のためには誰もが実際に使える状態にすることが重要です。

また、デジタルIDは公的機関だけでなく、企業-個人間取引の契約も含め、あらゆる契約で法的拘束力のある電子署名として使用できます。偽造が容易な手書き署名に比較し、非常に安全性が高く、公的機関の作業量を大幅に削減します。デジタルIDはIDカードだけではなく、モバイルID、スマートID等のインフラも整備しており、これらによって安全に個人の識別や手続きでの電子署名を可能としています。

電子政府を推進するための秘訣

しかし、国のデジタル化を成功させるために必要なものは、技術やお金だけではありません。強いリーダーシップが必要になります。政府が、どのようなエコシステムを構築するか明確な戦略を持って、推進していくことが重要です。このため、エストニアでは何年も前に政府CIOが配置され、政府の施策推進化責任者としてデジタル化や新たなオンラインサービスを推進しています。

また、リーダーシップに加えて法制度も、デジタル化を進める上での重要な側面となります。現在のシステムを効率的に変更するためには、まず法令により方向性を示し、その後、新たな技術が登場すれば、法制度も迅速に対応していく仕組みが必要です。

エストニアは高度な技術、強力なリーダーシップ、それを支える法制度により電子政府を推進できましたが、その要因の1つとして、エストニアがソビエト連邦の崩壊により独立したとき、国内にコンピュータもレガシーシステムもなかったことが挙げられると思います。

2. Hack the Crisis、Global Hackから学ぶエストニアでの取り組み

次に、スタートアップと政府との連携の例として、Hack the Crisisについて少し紹介します。Hack the Crisisは、エストニアのスタートアップコミュニティGarage48とAccelerate Estonia（政府運営の新ビジネス創出プロジェクト）が主催したハッカソンです。開催目的は、新型コロナウイルス感染症対策として、対面でミーティングする必要がない新たなソリューションを開発することで、たった6時間で準備されたハッカソンには30チーム、1,400人が参加しました。エストニアでは、以前よりイノベーションプロジェクトにおいて政府とスタートアップが連携しており、今回のHacksonも非常に短期間で連携した好例と言えます。

その後、Hack the Crisis主催者は、Global Hackwoをはじめ世界各地のオンラインハッカソン開催をサポートしてきました。その結果、12,000人が参加し、1,032のアイデアが出され、507のプロジェクトが提供されました。これは、どんな小さなイニシアチブも世界規模でインパクトを与えるものに成長する、そして政府とスタートアップコミュニティが連携できるという素晴らしい見本だと思います。

3. エストニアでコロナウイルス下での官民連携取り組みとデータ保護の関係性

エストニアで、危機的状況での官民パートナーシップにおいて、パーソナルデータの取扱いは、GDPRに照らして非常に関連があります。

通信位置情報を活用した移動履歴の分析

エストニアでは、2020年3月12日から5月17日まで緊急事態宣言が出されていました。当初、新型コロナウイルス感染拡大の懸念が高まった際、政府は通信事業者が持つ通信位置データの利用を検討していました。しかし、GDPRではパーソナルデータの利用に対し非常に厳格で、個人の位置情報が他のデータと組み合わせることは個人のプライバシーに対するリスクが高くなるだけでなく、そのようなデータ使用に対して社会からの反発も起こります。このため、通信位置データを直接政府に提供せずに、専門家である電気通信事業者自身が匿名化し、統計データとして政府に提供することになりました。匿名化データであれば、GDPR適用外なのでより簡単に安全に行うことができます。これはプライバシー保護アプローチの1つであり、結果として、通信事業者は異なる目的で使用される可能性があるデータを制御不能にせずすみずみにすみます。

コロナ対策の移動追跡トレーシングアプリ

新型コロナウイルスのコンタクトトレースアプリケーションについて、エストニアではあまり後半には議論されていませんが、すでにエストニア社会問題省と民間企業9社で開発コンソーシアムがスタートしています。スイスのプライバシー専門家が開発し、非常にプライバシーに配慮した設計となっているDP-3Tプロトコルを使用することが提案されています。iOS、Androidデバイスで採用されている匿名IDをBluetoothで通知するタイプのもので、国境を越えた相互運用性があります。

これはコロナ禍で国または民間企業がアプリ開発をする際の一例ですが、例え誰がどのようなアプローチをとる場合でも、個人のプライバシーを保護し、データ共有に関しては個人がコントロールできるようにして、同意した場合にのみ許可されるということです。一部の調査では、このアプリケーションが効果を発揮するためには人口の60~70%が使用する必要があるそうです。エストニアでは、本人の同意なしにこの種のアプリケーションの使用を人々に要求することはできません。

4. GDPR関連のエストニアスタートアップ動向

GDPRは、エストニアの大企業だけでなくスタートアップビジネスにも大きな影響を与えています。私たちは企業のGDPR対策支援を行っていますが、企業、特にスタートアップがGDPR順守の行動をとっていないこと、施行から2年たってもまだ意識・関心が低いことは大きな課題です。

現在、EUの中でエストニアはGDPR違反に対する制裁金が発生していない数少ない国の一つです。

実際に執行されていないので、企業の意識が高まらないのかもしれませんが。ただ、そのような状況の中で、スタートアップに対する投資に際しては、GDPR対応状況が厳しく問われています。最近の傾向として、GDPR施行以降、ベンチャーキャピタルのスタートアップへの投資は慎重になり、GDPR対応ができていないスタートアップを敬遠する動きも見られます。また、取引先からも非常に強い圧力があり、1つのデータ処理契約を締結するまでに3~4か月を要したケースもあります。スタートアップにとって、GDPR対応は非常に大きな課題です。

5.日本企業のGDPR対策と今後に関して

EU在住の消費者に対してサービスや商品を提供する場合や、EU在住の消費者の行動分析を行う場合、日本企業でもGDPRが域外適用されるため対策が必要となります。例えば、日本のeコマースで、EUへの商品発送に応じていたり、英語やEUの言語で商品紹介を行ったり、日本円以外の通貨での支払いを受け入れていれば、EU在住者を対象としているとみなされ、GDPRの対象となります。また、より多くの日本企業で対策が必要となるケースが、Cookieやそのほかのトラッキング技術を使ってどこの国からのアクセス等をモニタリング、分析している場合です。

私たちの法律事務所の経験に基づけば、日本企業のGDPR対応への関心は高まっています。例えば、GDPRは企業のデータ処理に対して高い透明性を要求するため、EU消費者に対するプライバシーポリシーが必要です。また、EUの消費者や当局との窓口となる担当者も設置する必要があります。これらは主なものですが、まずは自社の活動がGDPRの対象となるかを把握するための分析を行うことをお勧めします。



講師：NORDX Legal Partner, Attorney at Law Risto Hubner氏

特にIT関連、データプライバシーに関する豊富な知識、経験を持つ弁護士として、バルト諸国最大のテクノロジー企業の1つであるNortalをはじめ多くのクライアント企業に対し、ビジネスを取り巻くさまざまな分野についてアドバイスを行っている。また、Legal Hackersのエストニア主導者として、スタートアップ企業の支援等に力を注いでいる。

本内容は、2020年5月25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3回 エストニアにおける新型コロナ対応-官民連携、データプライバシー-」 講演内容をまとめたものです。