感染症対策で問われる個人情報保護

――「プライバシーと公」はデザインできるか

感染拡大防止策とプライバシーのバランスをどうする？
各国やEUのプライバシー規制ばかりではなく、
アプリ配布の媒体となる〝GAFA〟による
「テクノロジーによる法」も大きな課題だ。
両者のバランスをどうデザインするかが、いま問われる。

情報セキュリティ大学院大学副学長
湯淺墾道

ゆあさ　はるみち　一九七〇年生まれ、青山学院大学卒。九州国際大学法学部教授、副学長を経て二〇一一年情報セキュリティ大学院大学教授。二〇年より現職。総務省情報通信政策研究所特別研究員、法務省法制審議会民事訴訟法（IT化関係）部会委員、神奈川県情報公開・個人情報保護審議会副会長、日本データ通信協会電気通信個人情報保護推進センター諮問委員長などを務める。

新型コロナウイルス感染症対策として、各国でスマートフォン用のコンタクト・トレーシング（接触追跡）アプリやコンタクト・コンファーミング（接触確認）アプリが提供され始めている。日本では、厚生労働省が新型コロナウイルス接触確認アプリ（COCOA）を六月一九日にリリースし、七月三日から陽性者がアプリに登録するための処理番号の発行を開始した。イギリス、シンガポールなどにおいても、こうしたアプリの提供が始まっている。しかし、各国で提供されているこれらのアプリは、個人情報やプライバシーをどのように扱うかという点で、国によって基本的な考え方が大きく異なっている。

中国や韓国では、キャッシュレス決済アプリや個人信用アプリなどから収集される各種のデータを突き合わせることによって、感染者や濃厚接触者の移動経路や感染経路が明らかにされた。中国における大量のデータを利用した社会・国民の監視体制は以前から注目されていたが、中国政府は、スマートフォンの位置情報、スマホにインストールする健康アプリ、キャッシュレスサービスや個人信用スコア、街頭の監視カメラなどから、感染者や濃厚接触者だけではなく健康な人も含めて大量のデータを収集し、感染拡大防止対策に活用したとされる。韓国では政府のウェブサイトやアプリの通知により、年齢、性別、職場、おおよそ

の住所、利用したコンビニ、移動手段などが公開された。氏名は非公開とされたものの、SNS上の情報を照らし合わせれば個人を特定することができる場合も多く、顔写真、住所などがインターネット上で晒されてしまった場合もあった。

日本の場合、国民の個人情報保護に対する意識も高まっており、おそらく中国や韓国のように政府が個人に関するデータを大量に収集したり、感染経路特定のために年齢、性別だけではなく移動手段等も公開したりすることには、抵抗が強いであろう。もともと日本では、アプリを通じて各種の情報を収集してそれを分析することや、情報に経済的インセンティブを付与して情報を提供すればするほど有利となるような仕組み自体にアレルギー感のあるユーザーも多く、さまざまな事業者が個人信用スコアに参入しているものの、必ずしも成功していないという実情がある。

しかし、感染者であるか非感染者であるかを問わず、アプリで個人の移動履歴や位置情報などを追跡することによって、感染が発覚した場合にその行動先や接触者を特定して感染経路を明らかにし、感染者と接触した人にはそのことを通知するという感染拡大防止対策は、六割程度のユーザーがアプリをインストールして利用すれば、効果的であるとされる。「アフターコロナ」ではなく、新型コロナウイルスとの長期的な共存の必要性が唱えられる中で、個人に関するデータの収集と利用も長期化する可能性があり、緊急対策としての一時的なものにはとどまらないものとなる。感染症対策と、個人情報やプライバシーの保護とは、どのような条件であれば両立するのであろうか。

コンタクト・トレーシングとGAFAの影

COCOAのようなコンタクト・トレーシングアプリには、感染症対策と個人情報・プライバシー保護を両立させるために、個人の識別や感染者との接触の認識に関する技術的な工夫が埋め込まれている。

感染者が自分で入力する場合を除いて、匿名IDを付与することによって個人を識別はするが、個人を特定する情報は収集しない。つまり、A、B、Cという個人は識別するが、Aが山田太郎でありBが鈴木花子であるという個人の特定は行わない。感染者との接触通知の仕組みは、まず、アプリを端末にインストールしている人同士が一メートル以内で一五分間近接した場合に接触を記録する。GPSによって位置情報を収集することは避け、ブルートゥースによってアプリを端末にインストールしている人同士の接触

を判定する。Aが感染していたことが判明した場合、Aはアプリ上に自分で感染を登録する。そうすると、Aと接触していたユーザーに、感染者と接触していたということが、アプリを通じて通知される。それによって、感染者と接触していたユーザーは自主的に適切な行動を取ることができるようになるというものである。

このように個人情報や、位置情報のようなプライバシー性の高い情報の収集を避けつつ、感染者との接触や感染経路を特定しようとする仕組みは、技術的な手段によって個人情報やプライバシーをできるだけ保護しようとするものであり、あらかじめ保護する技術的方策を組み込む手法は「プライバシー・バイ・デザイン」とも呼ばれる。

ところで、スマートフォンのアプリによってコンタクト・トレーシングやコンタクト・コンファーミングを行う際、スマートフォンの市場がアップルのiPhoneとグーグルのAndroidにほぼ寡占化されている現状では、両者にインストールできないアプリは意味をなさない。政府がスマートフォンのアプリのインストールを要請したり、場合によっては強制したりするときは、そのアプリはアップルによって承認されたものでなければならないという制約が課せられることになる。アプリのダウンロード元が純正ストアに限られるためである。

COCOAは、当初、ボランティア・ベースでエンジニアたちが協力し、無償での開発が進められていた。しかし、後述するEUのガイドラインを受けて、アップルとグーグルが共同で開発・公開したフレームワークでは、かなり厳密なプライバシー保護が求められることになった。コンタクト・トレーシングはボランティア・ベースではなく政府が中心となることが求められており、COCOAも急遽、厚生労働省による調達・リリースとなった経緯がある。

国家同士の協定や条約、国会によって制定された法律だけではなく、テクノロジーが「法」となる。このことは、ローレンス・レッシグが著書『CODE』の中で二〇年前に予言していたことではあったが、新型コロナ対策としてのコンタクト・トレーシング、コンタクト・コンファーミングも、もはや一国の政府だけの判断では実効的な実施手段を決定することはできず、スマホの市場を寡占するアップルとグーグルの意向を無視できない現実がある。

データの「国境」は越えられるか

本稿執筆時点で、日本と海外との往来にはきわめて厳しい制約が設けられている。しかし、経済活動の早期再開の

ために入国規制の緩和を求める声は強く、各国ともに段階的に規制を緩和することによって人の往来を再開することになるであろう。

その際に問題となるのが、感染者の国境を越える移動や接触の追跡のために、感染者や濃厚接触者に関する個人データを国際的に共有したり外国から収集したりすることは可能か、という点である。というのも、近年、個人に関するデータの国境を越える移動や利用を制限しようとする動きが国際的に強まり、個人情報保護が国際的な課題となっているからである。

インターネットは、個人に関する情報の国境を越えた流通を容易にした。しかし近年、中国がサイバー空間の「主権」を主張するなど、それに歯止めをかけようとする動きが顕著になってきている。ボーダーレス社会、グローバル社会の実現とは逆に、サイバー空間における「ボーダー」を画定しようとする動きは、個人データ保護法制やプライバシー保護法制の面で顕著であり、国内で収集されるデータの海外への移転に制約を設けたり国内サーバに保存することを求めたりするデータローカリゼーションが、開発途上国においても強まってきた。

その背景にあるのは、インターネットを利用したサービス提供の高度化と、個人を同定・特定する技術の急速な進化であり、技術進化はプラットフォーマーと呼ばれる特定の巨大インターネット事業者への膨大な個人に関するデータの集積と、データ利用の独占・寡占をもたらし、データの独占的利用とプライバシー侵害の危機が顕在化してきた。このため、EU、中国、ロシアなどは、国内（域内）の個人のデータが国境を越えて流通することに対する規制を強めるようになっている。

世界における個人情報保護、個人データ保護を主導するEUは、二〇一六年四月にEU域内の個人データ保護をさらに強化するため、「個人データの処理に係る個人の保護及び当該データの自由な移動に関する欧州議会及び理事会の規則（一般データ保護規則、GDPR）」を採択し、一八年五月二五日から加盟国への適用が開始された。GDPRは、個人データの保護の強化を図るものではあるが、EU域内国民の個人データの域外への「当該データの自由な移動」を抑止しようとする意図を有しており、EU域内国民の個人データを有する海外企業に対しても、GDPR違反に多額の課徴金を課すこととしている。GDPRは、「健康に対する国境を越える重大な脅威から保護すること、又は、医療及び医薬品若しくは医療機器の高い水準の品質

及び安全性を確保することのような、公衆衛生の分野において、公共の利益を理由とする取扱いが必要となる場合」には健康情報や生体情報を取り扱うことを許容しているものの、今回のようなパンデミックの状況において位置情報を個人の同意なく収集することが許されるのかについては具体的な規定を欠いており、ガイドラインも存在していなかった。

GDPRに関するEUの公的機関である欧州データ保護会議（European Data Protection Board）は、今年四月二一日、新型コロナ対策のためのコンタクト・トレーシングと位置情報の収集に関するガイドラインを公表した。

ガイドラインでは、個人データの収集と利用はGDPRの規定を遵守した上で行うべきであることを強調し、データ利用に関する法的な規制や権限がないまま、新型コロナの感染拡大を追跡するためスマートフォンの位置情報を利用することは認められないという立場を取っている。また、コンタクト・トレーシングについても、個人が特定されないように匿名化して情報を取り扱うべきであるとし、個人ユーザーの位置情報を直接収集することは認められない、収集したデータによって個人が再識別されることがないようにしなければならない、必要最小限の情報のみ収集するようにしなければならないなどの制約を課した。集中型のシステムと分散型のシステムという二つの想定されるシステムについては、分散型を採用すべきであるとした。集中型のシステムを採用した場合、各ユーザーには匿名化された識別子が割り当てられ、ユーザーの行動や人との接触についてのデータが集められる。各ユーザーと接触した人が感染していたかどうかは、識別子を通じて確認することができるが、集中するデータを政府が悪用し、匿名の識別子と個人の名前を突き合わせて、個人の再識別が行われる恐れがある、という懸念があるためである。

さらに、ボランティア・ベースでコンタクト・トレーシングを行う場合について否定的な見解を示し、個人データの取扱いが合法化される要件を定めるGDPR第六条第一項e号の「公共の利益において、又は、管理者に与えられた公的な権限の行使において行われる職務の遂行のために取扱いが必要となる場合」に適合するためには、政府機関が法律の規定に基づきコンタクト・トレーシングを行うことが最も適切であるとした。

またデータの利用についても、接触履歴に関する情報は各国の保健機関が定める時期を経過した後は消去すること、収集された国内だけで使用し、グローバルな感染状況

マップの作成のためなどに使用してはならないことなど、多くの制約を課している。

このような欧州データ保護会議のガイドラインからみれば、EUは新型コロナ対策を理由とした個人データの収集と利活用にはかなり慎重であり、越境利用に対する規制をゆるめるつもりはないように見える。もとよりEU内部にも、このようなガイドラインの立場に対して個人データ保護偏重との批判があるが、新型コロナ対策の場面でも、「データの国境」は簡単に越えられそうにはない。

求められるプライバシー・バイ・デザイン

東日本大震災の後も、日本では大規模な自然災害が毎年のように各地で発生している。このような相次ぐ自然災害への対応で見えてきたのは、災害の現場で救助・救援や復興に当たる自治体職員、消防、警察、自衛隊などの関係者への信頼度が高まる反面で、災害に関する政策決定を行う立場にある政府の対策には批判が集まりがちであるという実態である。このような状況の下で、政府が国民に対してコンタクト・トレーシングアプリのダウンロードを要請しても、不信感はなかなか払拭されないであろう。

欧州データ保護会議がコンタクト・トレーシングと位置情報の収集に関するガイドラインで規制をゆるめないという姿勢を堅持しているのも、規制を緩和した場合、新型コロナ対策を口実として政府が情報を収集し、監視国家化していくのではないかという懸念が人々の間に生じ、アプリをインストールするユーザーの数が減る恐れがあるからである。実際に、シンガポールでは三月二〇日に「トレーストゥギャザー（Trace Together）」というコンタクト・トレーシングアプリがリリースされたものの、四月末の時点でインストールしたユーザーは二五％程度にとどまっているという。バッテリーの消耗が速くなる、高齢者はスマートフォンを持っていないなどの技術的な課題もあるようだが、やはり個人の行動履歴や人との接触履歴を逐一収集されることには、管理国家といわれるシンガポールですら抵抗感が強いということであろう。

テクノロジーの進化により個人情報やプライバシーの侵害が発生している面は、確かにある。しかし、コンタクト・トレーシングアプリのように、適切に設計すれば、テクノロジーは逆に個人情報やプライバシーを守りながら感染症対策を進めることに貢献する。プライバシー・バイ・デザインは、個人情報やプライバシーの保護と感染症対策とを両立させるために、欠かせないものとなるだろう。●