コロナ追跡とプライバシー　―韓国と日本の対極的手法

市原麻衣子

（一橋大学法学研究科准教授）

本エッセイは 2020 年 7 月 27 日にアジア民主主義研究ネットワーク（Asia Democracy Research Network）から発表されたものを日本語訳したものです。
原文 URL
http://adrnresearch.org/publications/list.php?cid=1&sp=%26sp%5B%5D%3D1%26sp%5B%5D%3D2%26sp%5B%5D%3D3&pn=1&st=&code=&at=view&idx=89

新型コロナウイルスという目に見えない敵が現れた。誰が感染しているのか、どこにウイルスが付着しているのか分からない中でこの敵と戦い続けることは容易ではない。各国政府が次から次へと IT を用いた感染者追跡を開始したのは、この目に見えない敵をできるだけ可視化し、管理可能にするためであった。

IT を用いた監視の手法は、コロナ発生以前から用いられていた。契機は 2001 年の 9・11 テロにあった。テロ対策として生体認証や顔認証などの技術が開発され、出入国管理を中心に幅広く使用されるようになった。さらに、AI の進展によって個人の識別や予測も可能となり、GPS、インターネット、スマートフォン、監視カメラ、IC カード利用などの普及と相まって、個々人を監視するベースが築かれてきた。中国、シンガポール、マレーシアのペナンなど、様々な国と地域でこうした技術を駆使したスマートシティの構築が行われてきていた。しかし、民主主義国においては今日に至るまで、個々人の大規模な監視は基本的にほとんど行われてこなかった。

1.　韓国によるコロナ追跡

こうした中、韓国政府が早期にコロナ追跡を開始したことは注目を集めた。韓国政府の早期対応を可能にしたのは、2015 年に流行した MERS の経験である。MERS を受けて韓国では感染症予防管理法が改正され、感染者や感染が疑われる人の個人情報の提供を通信会社などの関係機関に要請できるようになっていたのである。同法に基づき韓国疾病管理本部（Korea Centers for Disease Control and Prevention: KCDC）は、クレジットカードの利用履歴、防犯カメラ記録、スマートフォンの GPS 機能、交通カードの利用状況などを用いて感染者の行動履歴を追跡し、感染者と接触した可能性のある人々に警告を発信してきた。感染者の行動履歴は、名前こそ開示されないものの、性別、年代、国籍などの個人情報とともにウェブサイト上で公開されてきた。海外からの入国者に対しては、入国管理事務所で自己診断アプリをインストールさせ、パスポート番号、滞在国、

健康状態に関する情報を 14 日間登録させる。入力は毎日行わなければならず、入力忘れが 4 日続くと警察に通報される。

3 月下旬には、都市計画に関わる情報を集めたスマートシティデータプラットフォームをベースとして、韓国電子技術研究院、KCDC、および韓国国土交通部が開発した疫学調査支援システム（Epidemic Investigation Support System: EISS）が構築された。スマートシティはもともと 2020 年 2 月に実証実験を予定していたものであったが、これをコロナ対策に運用したのである。KCDC が感染者情報を入力すると、権限を持った捜査官が EISS を通じて通信事業者とクレジットカード会社に対し、追跡に必要な個人情報の要求をする。これに応じて企業側は、自動または手動で EISS への情報アップロードを行う。

EISS を用いた追跡とホットスポット分析が可能となったことにより、それまで感染者追跡データの収集・分析に 2-3 日掛かっていたところが、1 時間以内に短縮されたという。個人追跡を迅速に行えるようになった結果、韓国では感染が疑われる者の検査や隔離を迅速に実施することが可能となった。そして感染者と接触した可能性がある人たちにもメッセージが共有され、自分自身の感染可能性に関する認識を高めることにも成功した。初期に大邱において大規模な感染が発生したにも関わらず、今日に至るまで感染者数・死亡者数ともに抑えられ、ロックダウンを行わずに日常生活を続け、4 月には総選挙も実施することができたのは、個人追跡システムの貢献も大きい。

EISS ではプライバシー侵害を最小限に抑え、ハッキングによる個人情報流出への対策も行っている。EISS 上で閲覧可能な感染者個人情報は、コロナの潜伏期間である過去 14 日間に限定されているほか、アクセス権限を持つ調査員も、同調査員が情報にアクセスできる時間も限定されている。アクセス可能なデータは感染経路に関するもののみで、監視カメラ映像や顔認証システムの情報は連携していない。また、ハッキング防止のため調査員は VPN を介してログインするほか、二要素認証が行われているという。データベースは暗号化されている。

ただしこの手法は、それでもプライバシー侵害を完全に排除することはできない。人々の同意なく、裁判所の同意も得ることなく個人情報を取得するやり方には問題があるほか、悪用の懸念もある。特に、監視権限に明確な時限が設定されておらず、個人情報へのアクセスがいつまで行われるのか分からない。パンデミック自体長期化が予想される上に、今後異なる用途に利用される可能性も完全に排除することができない。

この懸念は、2015 年の MERS 感染者に関する個人データを韓国政府が現在も保持し続けていたことが発覚したことで、さらに深刻さを増した。韓国国立保健研究院のクォン・ジュヌク院長は、6 月初めに行われた記者会見において、MERS 感染者データを永久に保存することとしたと述べている。これは感染者個人のデータを遅滞なく消去するよう求めた個人情報保護法に違反する動きである。政府はコロナ感染者の情報をパンデミック終了後に削除すると述べているが、MERS の先例に基づけば、政府発言の信憑性は低いと見られている。

また、感染者に関して得られた個人情報を公開している点についても、公開情報が多過ぎるとして、国際的にも国内的にも問題視されてきた。SNS では感染者探しや感染者のプライベートに関する詮索が行われ、個々人の尊厳が侵害され、感染者の差別が行われてきた。韓国進歩ネットワークセンターのオ・ビョンイル氏は、感染者と接触があった可能性を指摘する上で感染者の性別、国籍、年齢といった個人情報は不要であると指摘する。さらに、症状のある人々がプライバシー侵害を恐れた場合、検査をためらう可能性もあり、韓国の国家人権委員会が警鐘を鳴らす。それでも個人追跡が行われているのは、プライバシー侵害をある程度許容してコロナを抑制する政府のやり方を韓国世論が概ね支持しているためである。

2. 個人情報入手を躊躇する日本

これに対し日本では、元来プライバシー侵害に対する忌避感が強く、保健当局者の個人情報アクセスを認めて感染拡大を防ぐというやり方は取られてこなかった。韓国同様、感染者の行動を辿ってクラスターの発生を防ぐという手法が取られてきたものの、感染者の行動に関する情報は聞き取りで行われてきた。

感染者との接触をトラッキングするアプリの導入についても慎重な検討が続き、日本全体で用いるアプリ「COCOA」が導入されたのは、最初の感染者発覚から 5 か月後の 6 月 19 日であった。韓国のシステムが個人情報にアクセスしているのに対し、COCOA はグーグル社とアップル社が開発したシステムを用い、ブルートゥース相互の接触情報を明らかにするものとなっている。1 メートル以内の距離に 15 分以上あった端末を、10 分ごとに発行されるランダムな ID で自分の携帯内に記録する。個々人のスマホに保存された ID 情報は中央サーバーには送られないが、コロナの陽性判定を受けた人は、厚生労働省から発行される番号を自らアプリに入力すると、ID 関連情報が中央サーバーに送られる。そしてその人の端末と近くにいた可能性のある人に通知が届くこととなっている。位置情報を含めた個人情報とは紐づけされておらず、政府が COCOA を通じて個人情報にアクセスすることはできない。

しかし個人情報の流出に対する忌避感から、発表から 1 か月でのダウンロード数は 769 万件に留まる。特に若年になればなるほど浸透していないという。また、感染しても感染の事実を登録しない可能性も高く、実際 1 か月間での陽性登録者数は 27 人だった。利用者が増えなければ本システムの実効性は上がらない。

政府が個人情報への不正アクセスを行わないという信頼感が必ずしも高くない点も、ダウンロードが伸びない原因となっている可能性として指摘する声もある。アプリ会社による情報の不正利用などに対する懸念も社会に広く見られる。

こうしてプライバシー侵害の懸念から、日本では政府による個人情報管理型監視は導入されなかった。しかし、政府がこうしたアプローチを採用したことで人権が保護されたとは言えない部分もある。政府による強制的な管理の不在は、社会における人々の自主的な相互監視を引き起こした。周囲の人々の外出、マスク無着用、営業継続などを問題視し、抗議、警察への通報、脅迫などを自主的に行う「自粛警察」と呼ばれる人々が多く出現し、社会問題となった。政府がプライバシーと市民的自由を尊重する手段を選択したにもかかわらず、人々が相互に市民的自由を抑圧する行動に出たのである。

3. 結語

生命なくして人権保護が無いのは確かだ。しかし我々は、コロナ後の社会構築を見据えて動く必要がある。政府による過度なプライバシー侵害を許容することは、権威主義的監視社会の土台となる可能性があり、危険である。EISS に内包された様々な制限措置は望ましいものである。これに加え、韓国政府は個人情報アクセスへの期限設定とパンデック後の個人情報削除を約束し、国民による監視が可能な形でこれを行う必要がある。日本においては、相互監視が市民的自由をいかに抑圧しているかについて、アドボカシーを継続していく必要がある。今後教育の一環としてコロナ禍で起こった自粛警察の問題を反面教師として教育していくことも望ましい。

コロナ禍によりインターネット上でのインタラクションが拡大し、今後はさらに個々人の監視がしやすい社会となるであろう。我々は今からこの問題に向き合い、オンラインにおいてもオフラインにおいても、プライバシーと自由を維持する動きを取っておく必要がある。