翻訳：ロブ・キッチン「市民的自由と公衆衛生のどちらか一方かそれとも双方か？COVID-19の蔓延に対処するための監視技術の利用」

中　村　　努

要旨

COVID-19の蔓延に対処するため，さまざまな監視技術（スマートフォンアプリ，顔認証カメラ，赤外線カメラ，生体認証ウェアラブル，スマートヘルメット，ドローン，予測分析）が急速に開発，利用されている。接触者履歴，強制隔離や移動許可，社会的距離や移動の監視，症状の追跡に利用された監視技術の急速な展開は，ウイルスを抑制するのに不可欠であり，公衆衛生のために市民的自由を犠牲にしなければならないという議論によって正当化された。筆者はこうした主張に対して，監視技術の技術的，実際的な有効性に疑問を呈し，市民的自由，統治性，監視資本主義，公衆衛生の意味を考察する。

はじめに

COVID-19パンデミックが世界を支配して以降，その効果に対抗し，軽減させる戦略や方策が提示されてきた。伝統的な公衆衛生アプローチは，概して封じ込めの段階（ウイルスの拡大を防止する段階），先延ばし（ピークを減少させる方法），軽減（保健システムに必要な支援を行う），研究（追加の効果的な方法や治療の追求）を実行してきた。先延ばしや封じ込めの段階で採用された典型的な方法は，積極的な個人衛生の推奨，防護服の着用，ソーシャルディスタンスと自主隔離の実践，懇親会の禁止，移動制限，隔離の強化やロックダウン，検査体制である。

既存と新規のデジタル技術はこれらの伝統的方法を増強したり，補完したりするために利用されている。同時に，個人や集団レベルにおけるリアルタイムの大衆監視を通じて，効果を改善し，ひいては人口抑制を最適化するという議論が生ずる。実際に，多数の国が比較的早期に技術主導のソリューションを利用して，以下の５つの目的でコロナウイルスへの対応に役立てた。それは，①隔離の強化／移動の許可（人々がどこにいるべきかを知ること，感染者か濃厚接触者のために

自主隔離を強制すること，非感染者の移動を可能にすること），②接触者履歴（人々がどこですれ違ったかを知ること），③パターンとフローのモデリング（疾病とその広がりの分布や，どれぐらいの人が場所を通過したかを知ること），④社会的距離と移動監視（人々が推奨された安全な距離と循環流動の制限を順守しているかどうかを知ること），⑤症状の追跡（人々がどんな病気の症状をもっているかを知ること）である（Economist, 2021）。加えて，国家や超国家（たとえば，EU）は，受託研究や企業プログラム[1)]およびスポンサー付きのハッカソン[2)]を通じて，積極的に新技術の即座の試作と開発を推進している。

隔離の強化／移動許可に関して，中国の一部の市民は，電話にアプリをインストールし，公共空間（たとえば，ショッピングモール，オフィスビル，共同住宅，地下鉄）へアクセスする際にはQRコードをスキャンすることを要求される。その目的は，感染状況と入室許可を証明し，もし隔離すべき場合には地元警察に通報するためである（Goh, 2020）。モスクワ当局は移動やルートを事前承認するアプリシステムを公開し，隔離を強化している。登録には，個人のスマートフィンと都市のeガバメントシステムとの紐づけが要求され，個人のID，被雇用者の納税者番号，自動車のナンバープレートがアップロードされる（Ilyushina, 2020）。台湾は義務的な電話位置追跡システムを活用して隔離を強化している（GPS機能付き[3)]電話を非所有者に支給）。すなわち，ロックダウンの範囲を超えた人にテキストメッセージを送信し，違反の罰金を公表する（Timberg and Harwell, 2020）。ポーランド政府は自宅隔離アプリを導入して，隔離している人々にSMSを受信して20分以内にジオロケーション付きの自撮りを要求し，そうでなければ警察による訪問のリスクを負う（Nielsen, 2020）。香港は電子追跡リストバンドを支給して，強制自宅隔離を観察できるようにした（Stanley and Granick, 2020）。

イスラエルは反テロ対策に通常利用される先進デジタル監視ツールを再利用して，濃厚接触をたどるために検査で陽性となる前の14日間におけるコロナウイルス保有者の電話の動きを追跡する（Cahane, 2020）[4)]。韓国では，政府が監視カメラの映像，スマートフィンの位置データ，クレジットカードの購入記録を利用して，陽性者とその接触者を追跡している（Singer and Sang-Hun, 2020）。4月中旬現在，28カ国が接触追跡アプリを制作し，他に11カ国が緊急に開始する計画をもつ（Linklaters, 2020）[5)]。米国では，航空会社が24時間以内に着陸する乗客および乗務員の氏名と接触情報を，アメリカ疾病管理予防センターに伝達する（Guarglia and Schwartz, 2020）。

他国では生体情報を計測するように設計された技術を利用している。たとえば，携帯型サーモグラフィは，多くの国で公共空間での移動の確認や，職場への入退出確認に利用されている（Nellis, 2020）。イタリアはドローンに搭載されたサーモグラフィを利用して，公共空間における体温を監視すると同時に，ロックダウン規制の違反を取り締まっている（Url, 2020）。アラブ首長国連邦の警察は200人までの体温を1分でスキャンするため「スマートヘルメット」を利用している（Reuters, 2020）。リヒテンシュタインは生体ブレスレットを試験的に運用して，数カ月内の全

市民への展開を目的として，着用者の皮膚温，呼吸，心拍数といったリアルタイムの生命にかかわる身体指標をモニターしている（Jones, 2020）。

多数の会社が自社のプラットフォームやデータをウイルスへの対処を支援する手段として別の用途に利用する提案や保証をしている。注目すべきは，iOS とアンドロイドスマートフォンに基本ソフトを提供する Apple と Google が，接触者追跡を支援するソリューションを開発していることである（Brandom and Robertson, 2020）。また，Google は世界の都市，地域において，介入測定効果をモニタリングしている[6]。ドイツではドイツテレコムが，集約して匿名化された人口流動に関する情報を政府に提供している。テレコムイタリア，Vodafone，WindTre もイタリアにおいて同様の行為をしている（Pollina and Busvine, 2020）。イスラエルの接触者追跡ソリューションを支援する NSO Group は，多数の政府にサービスを提供している（Martin, 2020）。Cellebrite, Intellexa, Verint Systems, Rayzone Group, Cobwebs Technologies and Patternz といった他のサイバーインテリジェンス企業も同様である（Schectman et al., 2020）。位置データ仲介業者の Unacast はスマートフォンにインストールされたアプリから収集した GPS データを用いて，ソーシャルディスタンスが行われるかどうかを判定する（Fowler, 2020）。米国全郡で社会的距離のスコアカードを作成し，各州と提携して実行された対策が機能するかどうかを判定するのに役立てられる（Hoonhout, 2020）。

Palantir は警察や諜報機関と協業する評判のある極秘データ分析企業である（MacDonald, 2020; Sadowski, 2020）。同社はアメリカ疾病管理予防センターやイギリスの NHS に対して，必要な保健サービスの対応を予測するために疾病の拡大のモニターとモデリングを実施しており，他国にも売り出している（Hatmaker, 2020）。米国では，Clearview AI が公共空間およびプライベート空間で相互に濃厚接触した人を認識するため，CCTV カメラ映像の顔認識サービスの利用を売り込んでいる（NBC News, 2020）。イギリスでは，Onfido が移動を規制する「免疫パスポート」を作成するため，検査結果と顔認識とのリンクを提供している（Proctor and Devlin, 2020）。巨大なグローバルデータ仲介業者かつ信用スコア企業である Experian は，３億人の消費者プロフィールを組み合わせてパンデミックに影響されそうな人を識別し，その情報を医療提供者，連邦機関，NGO といった「必要不可欠な組織（essential organizations）」に提供している（Wodinsky, 2020）。Facebook，小規模位置追跡企業の Cuebiq と Camber Systems は，移動データを感染症研究者と共有し，米国内全域の社会的距離を監視している（Paul et al., 2020）。Wolfie Christl による Twitter のスレッドには，コロナウイルスの分析やデータをパンデミックに取り組む政府や研究者に提供している位置追跡企業のリストが掲載されている。そこには，Foursqure, SafeGraph, Placer, Umlaut, Gravy Analytics, PlaceIQ が含まれる[7]。

多くの政治家，政策決定者，市民が，プライバシーや統治性に関する懸念にもかかわらず，監視技術はウイルスの拡大を抑え，生命を救うのに役立つなら合法的に配備されるものと信じてい

るかもしれない。実際に，利用を促進する人々は，公衆衛生の要件は市民的自由についてのいかなる懸念にも勝ると主張する。しかし，公衆衛生か市民的自由のどちらか一方しか選べないのであろうか。それともこれは誤ったトレードオフなのだろうか。または，これらの技術の有効性や効果がまだ証明されていないとしたら，虚偽のトレードですらあるのだろうか。市民的自由，市民権，監視資本主義に関する即時かつ付随した結果をもたらす侵襲的な監視に，見返りがほとんどないままわれわれは突き進むのであろうか。この問題は，注意深く考察する価値があり，本稿で筆者はこれらの技術が実際にどのように展開しているのか，統治性やより広範な政治経済にどのように影響しているのか実証するための最初の回答を示し，課題を概説する（論点整理は表1を参照のこと）。

表1 COVID-19の蔓延に対処するための監視技術の利用から生じる問題

技術的／実務的	市民の自由と統治性	監視資本主義
●技術解決主義	●個人の権利と公共の利益との対立	●国家公認の監視資本主義
●安定したドメイン情報に基づく設計	●プライバシー，データ漏洩，再識別	●新市場の機会
●パイロットテストと品質保証	●データ最小化と同意	●公衆衛生やその他の国家データへの入り口
●目的適合的	●統治性	●深まるデータシャドー
●規則の設定とパラメータ	●社会的／空間的仕分け，線引き	●新規スマートフォンの所有者登録
●潜在的に断片化したデータソース	●人口プロファイリング	●コロナ洗浄の活動
●データの範囲と解像度	●コントロールクリープ	●株主の価値や利益の増加
●代表性とデジタル・デバイド	●規格化	
●データの質，信頼性，偽陰性／偽陽性	●権威主義	
●重複と偽装	●適正手続き，監視，是正	
●効果的なウイルス検査と証明への依存	●情報監視に関する国家の記録	
●60％の参加率に依存する接触者追跡	●国民の信頼と萎縮効果	
●隔離／移動許可のために追加のインフラが必要となる		
●企業の法的根拠		
●従来の接触者追跡より効果的である証拠		

技術ソリューションは効果的か？

執筆時点（2020年4月）において，COVID-19の拡大に対する潜在的なデジタルソリューションが急に現れ始め，急速に展開した。限られた検査が技術の大規模な投入の前に行われる。検査は出回るというよりはむしろ，実験室ベースかシミュレーションによるもので，効果的なソリューションかその他の効果があるかどうかというよりもむしろ，技術が機能するかどうかにかかわる。そこで，ウイルスの拡大を遅らせたり，抑制したりする適切かつ実行可能な手段であるかどうか明確にならないまま，監視技術が採用される。実際に，技術主導のソリューションを推進する誇大広告で見落とされる重要な問題は，それらが目的にかなっているかどうか，意図した結果

を生み出すのかどうかである。ここで，筆者はスマートフォン中心の接触者追跡と隔離強化（デジタルフェンス）／移動許可（デジタルの鎖）に関するこれらの問題を考察する。

技術的実現可能性と有効性

携帯電話の技術によって自動化された接触者追跡を利用する論理的根拠は，従来の接触者追跡の量と範囲を著しく拡大することを可能にすることである。それは時間と費用のかかる労働集約的な作業であり，記憶に依存し，近くの他人を見分けることができない（Stoke-Walker, 2020）。電話の近接を計算することによって，後の検査陽性者との接触を含む多数の人々の交点が自動で追跡される。近隣の電波塔への接続に基づく基地局位置情報（cell-site location information=CSLI）は粗すぎで，Wi-Fi 接続は密集した都市以外のカバー範囲が狭すぎるため，GPS で共有位置を監視し，Blootooth で濃厚接触を記録することが中心となっている（Stanley and Granick, 2020）。ただし，GPS も Bluetooth も空間的精度は高くない。

行政勧告のほとんどは，他人との濃厚接触や長時間の接触を回避し，２m 以上離れるというソーシャルディスタンスを維持することである。２m 未満の近い距離の違反を正確かつ確実に決定するのは不可能である。GPS は１m までの精度であるが，より一般的には５－20m であり，技術は屋内で機能せず，高層ビルの影や激しい雷雨や吹雪では十分に機能せず，デバイスのスイッチを最初に入れるか，屋外へ出ると，位置の確定には数分を要する（Shwartz and Crocker, 2020; Stanley and Granick, 2020）。Bluetooth は位置を計算できないが，他のデバイスとの通信を30m の範囲まで可能にする。他の電話との近さは受信信号強度インジケーター（Received Signal Strength Indicator=RSSI）を用いて推定されるが，精確さに欠け，条件によって変化する（バッグかポケットにある場合など）（Leith and Farrell, 2020）。さらに，すべての電話が初期設定で Bluetooth を内蔵しているわけではなく，利用するとバッテリー寿命がかなり短くなる（Stanley and Granick, 2020）。GPS も Bluetooth も人々の間に壁か窓があるかどうか，同じ空域を共有しているかを判定できない。刹那的で無意味にみえる出会いを排除するため，システムには時間的要素が取り入れられている。提案されたイギリスのアプリでは，あるデバイスが他のデバイスと15分以上２m 以内に近づいた場合のみ濃厚接触と記録される（Kelion, 2020）。しかし，短時間を排除する効果があるが，ある人がスーパーの通路でくしゃみをして通り過ぎたり，バスで10分間誰かのそばで席をしながら座ったりすることが重大になる可能性がある。

デジタルのフェンスや鎖を利用する論理的根拠は，堅牢で迅速に拡張可能な個別移動管理手段を提供することである。移動を防止するためのデジタルフェンスを実行するには２つの主な方法がある。第１に，GPS の追跡によって携帯電話か電子タグが移動しているかどうかを監視することである。第２に，短時間でジオロケーションメッセージ付きの返答を回答者に求める自動化メッセージを利用することである。限られた移動許可を提供するデジタルの鎖は，アクセスポイ

ントでスキャンして照合される QR コードを発行することによって実行される。そのため，ビル，公共空間，公共交通にまたがるチェックポイントインフラの高密度ネットワークを公開する必要がある。こうしたインフラは現在，大部分の法域で確立していない。別の方法は，検温して発熱していないことが確認できれば空間に入ることである。しかし，サーモグラフィの精度は低く，業界大手の FLIR によると，人の体温の誤差を華氏3.6度程度に抑えられると報告している（Gershom, 2020）。

ほかにも，技術による接触者追跡やデジタルフェンスおよび鎖を利用した有効性に関して疑問を抱く技術的問題点が存在する。たとえば，データの質をめぐる一般的な懸念がある。膨大な量のリアルタイムデータであるビッグデータは，たびたびノイズが入り乱雑で，精密さ（正確性や精度）や信頼性（経年的な一貫性）に疑問が生じる欠落，エラー，バイアス，不一致がみられる（Kitchin, 2014）。個人の自由を制限するかもしれない不正確で信頼性に欠くデータに基づいて決定がなされる場合，できる限り高い質を保証するプロセスが導入されなければならない（McDonald, 2020）。こうしたプロセスが積極的に実行された証拠はほとんどない。また，いくつかのシステムデザインの要素は，質を低下させる可能性を生む。たとえば，自己診断の主観的性質は，疑わしいものの陽性ではない事例に基づいた偽陽性を生むであろう。さらに，関連データが省略されたり誤ったデータが追加されたりして，システムをだます可能性がある。人々は電話の位置機能の無効を選択できるし，Bluetooth も切断でき，自宅に電話を置いておくことも，二台目のデバイスを利用したり，誰かの電話を借りたりもできる（Stanley and Granick, 2020）。その代案として，人々は症状を経験したら情報を共有しないか，検査を受けることを回避することに決めるかもしれない。Teresa Scassa が指摘するように，

> 日常に戻ろうとすると，アプリを操作するインセンティブが生じる。あなたは仕事に戻って家族をサポートしなければならない。咳が出るアプリを教えようとしていますか？（Patriquin, 2020）。

加えて，Bluetooth 信号はなりすましに脆弱であるため，誰かが識別コードを取り上げて別の位置に送信することができる（Angwin, 2020）。

データの受信圏や代表性はさらなる問題を惹起する。もし重要でなければ，あらゆる接触者追跡が起こる単一のアプリ，特に GPS やアプリが収穫したデータに基づく際の位置データは，通信業者か位置追跡企業によって断片化され，異なるフォーマットで巧妙に結合して蓄積されている。これはとりわけ米国とその他の国における問題であり，民間企業は接触者追跡やフローモデリングを実行する提案をしている（Stanley, 2020）。Apple と Google による構想の場合，データは携帯電話を除く Android や iOS を用いたスマートフォンのみに関係する。19％のアメリカ人に挙げられる問題は，スマートフォンを所有しておらず，コロナウイルスの高リスク群である65歳以上の非所有者は47％にまで増加する（Pew Research, 2019）。階層や人種によっても差異がある。年収３万ドル未満のアメリカ人の29％はスマートフォンを所有しておらず（Pew Research,

2019），このグループ内の接触者追跡の効率を悪くし（Schwartz and Crocker, 2020），移動を承認するための QR システムの導入によって，スマートフォンを購入していなければ約 3 分の 1 の低収入労働者がデジタルフェンスに囲まれることを意味する。そしてある宗教グループ，たとえば，ユダヤ教やアーミッシュ派はスマートフォンの利用を中止している（Ems, 2015）。加えて，効率的に働くため，技術はすべてのスマートフォンユーザーに常時の充電と起動と所持を求める。

データの質と範囲の問題を超えて，データに基づく解釈と決定に用いられるアルゴリズムやルールセットについての問題がある。Julia Angwin（2020）が述べるように，システムは感染の可能性を特定するための堅牢で信頼できる手段を実装する必要があり，誤報でユーザーに負担をかけるようなトリガーハッピーなものであってはならない。同時に，真の陽性のリスクが無視されることに慎重であるに越したことはない。濃厚接触にとっての陰性という結果以外に，偽陽性もまた検査体制に負荷をかけすぎるリスクがあり，とりわけその検査体制が接触者追跡を通じて課された措置を解除する唯一の手段である場合である。それはシステムへの信頼を低下させ，利用者が指示を無視する可能性がある（Angwin, 2020）。イスラエルでは，検査を受けずに強制隔離された人が，誤りを訂正してもらうことが困難であるとして，接触者追跡に基づくシステムの利用に抗議した（Linder, 2020）。そのため，米国自由人権協会が主張するように，

> 不適切な技術を用いて感染したかもしれない人について結論を下すことによって，実際には無防備ではなかった人に，おそらく医療従事者や初期対応者でさえ，2 週間の労働，友人，家族からの隔離といった大きな損害をもたらすであろう（Stanley and Granick, 2020）。

危篤状態

現在追求され展開されている技術ベースのソリューションは，理想からは程遠く，目的には適さない可能性を示唆する多くの問題点を抱えていることは明らかである。しかし，それが適切でも実際のところは，以下の仮定にのみ有効かもしれないと留意しておくことは重要である。

（1） 人がウイルスに感染したことを確認する認証を受けた大規模検査のプログラムがある場合，また追跡かデジタルフェンスや鎖が必要な場合（Angwin, 2020）。
（2） 症例数が少なく，実行再生産数（R）＜ 1 であり，（多数の隔離とは対照的に）選択的な隔離の場合は急拡大を制限するのに効果的である。
（3） 60％の人口が接触者追跡に参加している（Stokel-Walker, 2020; Kelion, 2020）；そこには隔離や移動許可の完全な順守と適切な警備が存在する。
（4） 技術主導のソリューションの利用に関する確固たる法的根拠が存在する（Ada Lovelace Institute, 2020）。

認証をともなう大規模な検査体制がなければ，特定できる既知の確認された症例は存在しない。また，未知数の未確認病原体保有者が行き交い続け，追跡や隔離の効果を減らすであろう。多数の症例がある状況において，アプリに基づく接触者追跡は，実行再生産数（R）が1未満でゼロに近い時点で，追加の感染の波を潜在的に抑える目的でのみ有効である。イギリスは質問票で自己診断できる大規模検査がなく，指導医に話したり，検査結果を入手したりする必要がない解決策を提案した（Kelion, 2020）。その結果として，大規模な偽陰性や偽陽性を生んだようである。

開発者は，電話ベースの接触者追跡システムが効果的であるためには，人口の約60％が参加する必要があると示唆している（イギリスではスマートフォン保有者の約80％に相当する）（Kelion, 2020; Stokel-Walker, 2020）。シンガポールでは，TraceTogether というアプリを無償で利用でき，1カ月後に人口の17％しかインストールしていないことは（Vaughan, 2020），別の場所における60％の普及率を実現することが課題となっていることを示唆する。例外状態における緊急権限を行使して，従来の抑制措置を講じてきたものの，アプリを義務化する（たとえば，ロックダウンの免除を受けるために必要とされる）ことで法的挑戦を受け（Stanley, 2020; Stokel-Walker, 2020）や，民主国家では抵抗と破壊に会う可能性がある。同様に，隔離強化や移動許可技術は権威主義的でない国家の人々の抵抗にあう可能性があり，企業がそれを労働者や訪問者のために政務に組み込み，利用を標準化し始めるものの，必要なインフラの整備を義務付けるかもしれない。

市民的自由，統治性，監視資本主義

技術的，実用的実現可能性を超えて，こうした技術を利用する結果は試験運用の前にはほとんど考えられず，より大きな利益のために苦慮すべき許容できる欠点とみなされるようである。

技術は移動，社会的ネットワーク，健康状態についての詳細な知識を求めることから，最も批判的な論評が焦点を当てる議論はプライバシーである（Angwin, 2020; Schwartz and Crocker, 2020; Stanley and Granick, 2020）。接触者追跡が，位置マーケティング会社やアドテックなどの民間企業による既存の位置追跡を活用し，同意を伴わないイニシアチブの場合，データ最小化原理の明確な違反がある。最小化原理とは，業務を遂行するのに関連する必要なデータのみが作成され，その目的にのみ利用されることである（OECD, 1980; Information Commission's Office, n.d.）。オプトイン（訳者注：本人から自らの個人データの第三者への提供について同意を得ること）の同意に基づくイニシアチブでは，匿名の ID を利用して，開発者は利用者にいかなる位置追跡や接触者追跡もデータを収集せず，身元を共有しないよう努める。集中システムでは，データは政府のサーバーに蓄積され，サイバーセキュリティ対策によって保護される。分散システムでは，ほとんどのデータはそれぞれの電話に蓄積され，プライバシー擁護派はこのアプローチを支持している。いずれのアプローチも，データが漏洩したり利用者の電話内の他のアプリに透過したり，近

くの利用者の電話の他のアプリや中央サーバーとの通信によってIDが取得される可能性がある（Angwin, 2020）。そしてこれらのデータは第三者に共有されうる（Patriquin, 2020）。さらに，GPSやBluetoothで位置データを開放することによって，デバイスは他のアプリに埋め込まれた広範なアドテックによって追跡可能となり，位置に基づくデータブローカーのエコシステムに登録される（Angwin, 2020）。Palantirのような政府のために接触者追跡データを利用してモデリングを行う企業にとって，データはすでに大規模なデータバンクや個別プロフィールに加えられ，別の用途で再利用されているかどうかは明らかではない。

加えて，匿名化のプロセスを取り消してデータが再識別される懸念がある[8]。ビッグデータの文献において，もしデータが完全に再識別されないならば，データセットを徹底的に探して結合することによって，エンジニアの匿名化戦略を覆しうるという見方が確立している（de Montjoye et al., 2013; Narayanan and Shmatikov, 2010）。たとえば，韓国では初期の患者を再認識しやすくなった（Singer and Snag-Hun, 2020）。シンガポールでも同様に，性別，年齢，職場，他の症例との関係といった検査陽性者の詳細な個人情報が保健省のウェブサイトで公表されている（Singer and San-Hun, 2020）。香港も同様に，年齢，居住者の状態，ウイルスの発症日と検査によって確認された日付，海外感染か市中感染か，入院している場合は病院を作成，一覧表示することによって，すべての症例を表示するインタラクティブマップを提供している[9]。脱認証には，（固有の識別子と大いに関係する）直接識別子と準識別子の双方を慎重に排除しなければならない（Cavoukian and Castro, 2014）。これが生じる程度や可能性は明らかではない。

プライバシーに対する影響は多くの人にとって心配することが多くある。しかし，その結果は（たとえプライバシーが保護されていても）統治性や市民的自由により一般的に拡張する。接触者追跡や移動監視はわれわれがどのようにその生活を営んでいるか記録し，社会的接触や移動を作り変えるように設計されている（Aouragh et al., 2020）。それらは社会的，空間的に分類し，空間やサービスを混合，移動，アクセスできる人とできない人に線を引く。Aouragh et al.（2020）が述べるように，接触者追跡アプリは，

> 現実の規範的条件を提示し，決めるか決めないかの選択の自由を持つ人の決定に貢献し，誰が生存し，生活を営み，世界それ自体を認識する可能性をもつか共同で定義するであろう。

活用されたさまざまな監視技術が，統治の一形態である，訓練（人々をナッジして濃厚接触の結果を恐れるためにソーシャルディスタンスを順守させる）や管理（選択の余地がほとんどないが順守すべき空間行動を積極的に規定する）を実行するように設計されている。そのため，従来の封じ込め措置，共同のまなざし（communal gaze）やさらしあげに加えて，技術は素直で従順な身体を生み出そうとする（Foucault, 1991）。しかしそれ以上に，その技術的なアルゴリズムで自動化された性質は，統治論理を監視や規律から捕獲や制御へとシフトしうる（Deleuze, 1992）。そこでは，人々は，行動が（自己）規律ではなく明示的または暗黙的に操縦されるデータ駆動型

システムを通じて絶え間ない変調の対象になる（Kitchin, 2018）。この生政治的権力は現在の例外状況を通じて深刻化する（Agamben, 2005）。そこでは，通常の権利は停止され，集団的利益のための優れた政府の正当な行動として，慣習的な抑制と均衡なしに措置が課される（Avila, 2020）。

この現れつつあるパンデミックの生政治は身体の緊密な管理と制御，およびそれらの循環と接触におもに関係している。それは，その表現において完全に空間的であり，公共および私的空間，空間的アクセスおよび行動を規制し，特定の空間性を生み出す。重要なことは，構築された決定要因（制度，官僚主義，インフラ，規制，法律，言説体制；Foucault, 1977）は公共空間を超え，職場の特徴となっている（例えば，検温，認証ステータス，または職場にアクセスするための接触者追跡アプリの使用，キー入力，送信メール，在宅勤務者のステータス更新などさまざまなパフォーマンス指標を監視するなど）（Mosendz and Melin, 2020）。さらに，米国自由人権協会や電子フロンティア財団，その他団体が指摘しているように，特に小売り，サービス，流通業や公衆衛生，より広い公共部門における「エッセンシャルワーカー」の人口動態を考えると，暴露のリスクと政務の適用は集団間で不均等である。一般的にアルゴリズムのガバナンスのように，この不均等と不公平は，階級，人種，エスニシティ，ジェンダー（Benjamin, 2019; Eubanks, 2018; Noble, 2018）をめぐるデータ公正の問題を再生産し（Dencik et al., 2016; Taylor, 2017），致命的な結果をもたらす可能性がある。

この新しい生政治的構造を実現するため，スマートフォンのインフラのような既存の技術がコントロールクリープ（統制の漸進）の対象となっている（Innes, 2001）。すなわち，その本来の目的は監視やガバナンスの業務に拡張されつつある。ある症例では任意（たとえば，接触者追跡アプリの使用）であるものの，クリープによって（必ずしも義務ではないが）強制になりつつある。たとえば，ある会社は職場へのアクセスにアプリの利用を求めたり，ある国はアプリの利用を制限の除外の条件にしたりしている（Weaver, 2020）。インドではすでに Aarogya Setu という接触者追跡アプリが封じ込め地帯の居住者と，官民部門の従業者に義務となっている（Sircar and Sachdev, 2020）。アプリのインストール漏れは罰金刑または懲役刑となる。過去20年間，特に9.11以後，コントロールクリープがネットワーク化されたシステムで発生している。特定のサービスを提供するために設計された技術が，警察やセキュリティ機器に登録されるようになった（Kitchin and Dodge, 2011）。現在の危機において，コントロールクリープは公衆衛生の目的で発生し模索されているが，その利用は政府の追跡とデジタルフェンス／鎖を常態化し，その後開発された設計概念は，継続的な健康監視に関して，警察，緊急管理対応，国家安全保障といった他の問題に軸足を移す危険性を孕んでいる（Sadowski, 2020）。たとえば，インドのアプリは特定の人々を監視し差別する政治的な目的のために再利用される恐れがある。確かに，9.11以降に起こったコントロールクリープは，縮小することがなかった（McDonald, 2020; Sadowski, 2020）。

正当な理由があって，パンデミックに対応するために利用されたシステムは危機の後に止

められずに，社会を監視し統治するニューノーマルの一部となる恐れがある（Sadowski, 2020; Stanley and Granick, 2020）。監視技術がいかにして歴史的に疾病管理に登録されてきたかについて French and Monahan（2020）が概観したように，技術ソリューションは持続する傾向がある。言い換えれば，現在実装されているあらゆる技術は，新しいタイプの社会的・空間的仕分けを日常化する新しいタイプの管理へのゲートウェイとして機能する可能性が高い。これは，統治性の本質を恒久的に変化させる可能性があり，また，テクノロジーを使って国家の意思を積極的に市民に押し付ける権威主義的な統治形態への道筋として作用する可能性がある。移動，他者との近接性，（たとえば健康状態を超えた）何らかの状態に対する知識をきめ細かく大量に追跡することで，より厳しい形態の管理が可能になり，抗議行動や民主主義に萎縮効果を与える可能性がある。こうした経路が正当化されるのは，Jathan Sadowski が指摘するように，「権威主義が『正しい』理由のために唯一の選択肢に見えるため，許容可能，さらには優れたものにさえみえ始めるからである」。スノーデン，ウィキリークス，その他多くの調査が明らかにしているように，このような懸念に正当性を与えているのが，データ監視の実践に乏しい国家である（Lyon, 2015）。

中国とロシアは，これが何を意味するのかを知る手掛かりとなる。コロナウイルスに対する技術的解決策が一見うまくいった例として中国を挙げる擁護者がいる一方で，警鐘を鳴らしているのも事実である。権威主義国家として，中国は技術支援なしに社会的，国家的取り締まりによって，ロックダウンをうまく行うことができた。しかし，中国は技術ソリューションを即座に動員できた。というのも，中国はすでに社会的信用度の評価や数百万台の顔認識カメラ，自動ナンバープレート認識カメラを含むスマートシティ技術の普及を通じて，ビッグ・ブラザー（訳者注：ジョージ・オーウェル作の SF 小説『1984』に登場する支配者）式の監視装置を導入する道を進んでいるからである（Keegan, 2019; Lee, 2019; Liang et al., 2018）。スマートフォンは，キャッシュレス社会に移行にともなって，仮想の財布となり，あらゆるデジタル取引を追跡するための手段として，日常生活に欠かせない技術になった（Mozur, 2017）。2019年12月以降，中国では新しい SIM カードを登録したすべての携帯電話ユーザーが，顔認証スキャンを行う必要があり，個人と携帯電話の間に直接の生体認証の連携ができた（Kuo, 2019）。パンデミック危機は，国家にとって，監視技術の本格的な展開を促進し標準化する機会となり，そこで実施された追跡が危機後に元に戻ることはほとんどない。言い換えれば，技術は自宅に待機させるという社会的，統治的措置が実施された以上の効果は限定的であったかもしれないが，下流では大きな影響を及ぼした。アプリで承認された公共空間やプライベート空間への入場による空間の仕分けが，ニューノーマルになるかもしれない。ロシアでも同様のことが懸念されており，評論家はモスクワのロックダウン強制アプリを「サイバー収容所」と呼んでいる（Ilyushina, 2020）。

加えて，システムの合法性，勧告や強制的な命令，適正手続きや監視，救済やオプトアウト（訳者注：第三者が本人から個人データの提供の許可をとらないものの，本人が求めれば第三者提供

をやめること）の権利などの慣行をどの程度伴うかについても懸念される（McDonald, 2020）。接触者追跡アプリの使用を選択した場合，アプリを通じて陽性検査結果を共有することは義務になるのだろうか。あるいは，陽性反応が出た人と近くにいたことをアプリが知らせた場合，その人は診断された対策を行わなければならないのだろうか。指示を無視した場合の罰則はあるのだろうか。検査や自己診断に基づく指導に違いはあるのだろうか。特に，強固で広範な検査体制と認証が運用されていない状態で，指示された措置に従うことを正当化しようとするのは困難であろう。指示が強制される場合，それを不服として訴える手段はあるのであろうか。一度登録した体制から脱退することは可能か。その場合，何か罰則があるか。新しい技術開発の実施と運営を監督し，既存の規制と法律を遵守し，イニシアチブに与えられた権力を乱用しないようにするための正式な仕組みはあるのだろうか。不正行為や悪用に対する罰則はあるか。これらの疑問が熟考され，適正なプロセスと監視が行われていることを示す証拠はほとんどない（McDonald, 2020）。

また，調達やパートナーシップを通じて，産業界と協力して監視ベースのソリューションを追求することで，監視資本主義（Zuboff, 2019）の手法と論理が正当化され，再生産される。過去20年の監視研究の文献でよく言及されるように，個人レベルのきめの細かいデータ収集とプロファイリングが大きく変化し，データブローカーとその利益が大きく拡大した（Kitchin, 2014）。とりわけ，2000年代半ばのスマートフォンの登場によって，位置情報を記録，送信するアプリを通じて，インデックス化されたリアルタイム位置情報データが大量に取得され，2014年には米国内だけで58社の位置情報専門企業が事業を展開しており（Angwin, 2014），以来成長している。さらに，通信事業者，Facebook（Whatsapp や Instagram を含む）のようなソーシャルメディア企業，スマートフォンの OS を提供している Apple，Google，Microsoft は，リアルタイムの位置情報や移動情報を生成，蓄積している。これらの企業がこのようなデータを作成していることは多くの人が知っていたが，COVID-19の流行によって，これらの企業が接触者追跡を支援するためにデータおよび分析ツールを共有し，社会的距離の影響を監視し，移動監視を実施していたことが露呈した。

こうした企業の多くがパンデミック危機に協力したという動機があったことは間違いないが，このような動きには他の効果や動機があることも明らかである。第1に，監視資本主義が正当化され，利益のために人々のデータの侵略的な収集，利用が助長される。実際に，これらの活動は，特に無償で提供される場合，評判のロンダリングを通じて監視資本主義の「コロナ洗浄（covidwashing）」[10] を可能にする（McDonald, 2020; Stanley, 2020）。意図的でないせよ，国家による企業ソリューションの採用は，株主価値と投資家の利益を高めることにもつながっている。第2に，これらの企業は，自社の活動やサービスを宣伝，マーケティングする機会を得て，将来のビジネスを呼び込む可能性をもつ。第3に，新しい製品や市場の可能性が広がる。投資家への呼びかけで，Phunware（トランプ氏の2020年再選キャンペーンの一翼を担うスマートフォン追跡会

社）は，パンデミックにかかわる動機を明らかにし，ソーシャルディスタンス政策の執行など，いくつかの潜在的な新製品と市場を売り込んだ（Biddle and Fang, 2020）。公衆衛生データのさらなる民営化だけでなく，COVID-19への取り組みにも貢献することで，公衆衛生やその他の政府との契約への入り口として機能することを望む企業も間違いなく存在するであろう（Sadowski, 2020）。第 4 に，新たなデータへのアクセスを獲得したり，スマートフォンの新規所有者の登録を促したりすることで，データの影をさらに拡大，深化させている。そのため，COVID-19パンデミックが，プライバシー，社会的，空間的仕分け，プロファイリングに関する市民的自由を損なうような監視資本主義の実践を定着させ，正常化することに明らかな懸念がある。

市民的自由と公衆衛生のどちらか一方か，あるいは双方か？

これまでの議論で強調したのは以下である。使用されている監視技術は急いで導入され，その目的適合性が確立していない。これらの技術を利用することで，市民的自由，統治性，市民権に大きな影響がある。市民は証明されていない，あるいは間違いが発生しやすい監視技術の使用によって，市民的自由と公衆衛生を交換することを要求されている。事態の緊急性と病気の深刻さによって，公衆衛生が市民的自由に優先することが求められ，その代償として監視の強化，統治性の変化，監視資本主義の強化が必要と主張する人もいるかもしれないが（Tony Blair Institute for Global Change, 2020），これは 3 つの理由からあまりに単純である。

第 1 に，監視技術が期待された公衆衛生上の利益を提供できない場合，すなわち，その利用から生じる相応の利益がない場合，その交換は誤りとなる可能性がある（Stanley and Granick, 2020）。これは，米国自由人権協会（Guarglia and Schwartz, 2020）とエイダ・ラブレス研究所の結論であり，後者は接触者追跡に関して，「現在，その利用を支持する証拠は不十分であり，技術的な限界，効果的な展開への障壁，社会的な影響などをより検討する必要がある」と結論付けている。

第 2 に，公衆衛生と市民的自由を交換する考え方は，技術的解決主義に基づいており，技術は付随するコストに関係なく問題を解決する唯一の有効な解決策とみなされ，政策は技術によって導かれるのではなく，むしろその逆である（Morozov, 2013）。多くの国家は，ハイテク企業によるロビー活動の相次ぐ展開，自国の技術主義への転向，経済のハイテク部門におけるイノベーションを刺激したいという願望によって，技術的解決主義を追求する素地ができた。そのため，大衆監視や技術を介した管理が病気を克服するための主要な手段であるべきだという解決主義的な命題に従順であった（Aouragh et al., 2020）。このようなシステム思考的，決定論的アプローチは，社会技術的な見方というよりも，それが最も適切または効果的な解決策で，その予期せぬ効果やより広範な費用対効果がどうであるかという，さらなる考察を差し控えるものである。その代わりに，欠点が強調されると，その対応は次のように組み立てられる。「たとえ欠陥があったり適さないものであっても，その技術を使うことは，使わないよりはましだ」ということになり，外部

性の有無や，その技術をうまく導入するための重要な条件が存在するかどうかは関係ないのである。その結果，真っ先に導入が急がれ，欠点が明らかであっても導入が推進し続けられることになる。

第3に，プライバシーやコントロールクリープなどの問題を尊重し，市民的自由と公衆衛生の双方を保障した展開を推進することが可能である（Goldenfein et al., 2020）。実際に，市民的自由を保障しないことは，信頼を損ない，反対意見を助長することによって，公衆衛生の取り組みを台無しにする可能性がある（Ada Lovelace Institute, 2020）。韓国やシンガポールでは，初期の患者が再識別されると，公然と追い回され，恥をかかされ，検査に萎縮効果が生じた（Singer and Sang-Hun, 2020）。追跡者接触アプリの導入率が低いのは，人々が個人情報に関する政府の過去の記録を信用していないことも一因である（Patton, 2020）。もし，人々が自分の権利が侵害されていると感じたり，自分が好まない，あるいは信頼できない方法で管理されたり，ターゲットにされていると感じたら，人々は技術の利用を中止するか，回避や破壊する方法を見つけるか，検査を避けたり，医療を求めたりするであろう（Schwartz and Crocker, 2020）。これは社会的に孤立した状態を維持するための手段や国からの社会的支援が得られない人々に特に当てはまるであろう。Anna Johnston（2020）の述べる通り，国の威信に訴えたり，規制解除や利用義務化を阻止するために脅したり，国家やGoogle，Facebookなどがあらかじめわれわれのすべてを知っていると軽率に主張したりすることは，逆効果になる可能性が高い。むしろ，公衆衛生問題への取り組みには，法執行のアプローチよりも，公教育と自主的な対策や遵守が効果的であり（Stanley and Granick, 2020），強引な対策は，「信頼が最も重要なときに市民と政府の関係を悪化させる」（Schwartz and Crocker, 2020）可能性が高い。そのため，技術は期待した効果と逆の効果を生む危険がある。

市民的自由が公衆衛生と不必要に引き換えられないようにするため，多くの法域で組織や学者が活発な運動を展開している。その中心的なメッセージは，監視技術を導入するのであれば，適切でバランスがとれ，既存の法律を遵守し，市民的自由を保護するものでなければならないということである。たとえば，電子フロンティア財団，米国自由人権協会，エイダ・ラブレス研究所[11]，欧州データ保護委員会[12]は，以下のように要求している。

・データの収集と利用は科学と必要性に基づいて行わなければならない。
・技術には目的，意図，仕組みが透明でなければならない。
・技術やより広範なイニシアチブは有効期限がなければならない。
・匿名化，強力な暗号化，アクセス制御を含むプライバシー・バイ・デザイン・アプローチ（訳者注：エンジニアリングプロセス全体にわたってプライバシーを考慮するシステムエンジニアリングのアプローチ）を利用すべきである。
・ツールは理想的にはオプトアウトではなく，オプトインで同意を求め，オプトインの利点，運

用，寿命について非常に明確に説明する必要がある。
・仕様とユーザー要件，データ保護とプライバシーへの影響評価，およびソースコードを公開する必要がある。
・データはイニシアチブを超えて共有したり，再利用や収益化したりできない。
・匿名データを再識別するためのいかなる努力も行ってはならない。
・技術や広範なイニシアチブは，使用に対する適切な監視，行動に対する説明責任，確固たる法的根拠，そして誤用に異議を唱えるための適正な手続きを備えていなければならない。

これらの要求が意味するのは，ウイルスの拡散を抑え，遅らせる目的で公衆衛生の専門家が必要と判断した場合にのみツールを使用し，危機が去った後はその使用を中止しなければならないということである。市民はその技術が何を実現しようとしているのか，自分のデータに何が起こるのかを正確に知るべきである。また，コントロールクリープや，技術が一般的または国家安全保障，予測的な取り締まり，その他の統治または商業目的のために再利用されることを阻止するための保護措置も必要である。さらにその開発は，公衆衛生やプライバシーの専門家が設定した詳細なユーザー要件によって導かれるべきであり，アマチュアや民間企業による設計や生産の主導に委ねるべきではない。この点において，参加者に専門知識がないハッカソンで開発された技術は，その後，法的，社会的，政治的な期待に応えるために再構成されたとしても，利用されることはまずない。このようなロビー活動の結果，多くの国では，プライバシーやデータ保護に関する懸念に対処するため，接触者追跡アプリの開発中に設計仕様や基本設計概念を変更し，集中型から分散型のアプローチに切り替えている（Busvine and Rinke, 2020; O'Brien, 2020）。同様に，ドローン，顔認識カメラ，生体情報モニタリングなどの監視技術についても，その侵略的な性質や，社会的距離を置くといった従来の対策以上の効果的なパフォーマンスを示す証拠がほとんどないことから，その利用に対する反発がある。

結論

本稿で筆者が目的としたのは，COVID-19に取り組むための遅延，封じ込め対策としての監視技術の開発と展開に関する技術的，実際的，倫理的問題を比較的幅広く概観することであった。筆者は主にスマートフォン技術を用いた接触者追跡，隔離強制，移動許可に注目してきたが，社会的距離／移動の監視や症状の追跡，顔認識やサーモグラフィ，生体認証ウェアラブル，ドローン，予測分析などの活用に，より徹底した分析を加える必要がある。この分析では，迅速に行動することを急ぐあまり，提案された解決策の技術的な実現可能性，実際に機能するかどうか，従来の介入策よりも効果的な結果をもたらす程度について十分な検討と評価が行われていないことが強調される。また，市民的自由，生政治，監視資本主義に対する影響，想定される利益が相応の悪影響を上回るかどうか，市民的自由を守りながら公衆衛生の野心を実現できるかどうかについて

も，十分な検討がなされていない。

現在提案，導入されている技術ソリューションの初期評価では，その有用性が過大評価されていることが示唆される。スマートフォンによる接触者追跡は，自己診断ではなく大量検査を行わなければ効果がなく，理想的には感染者数が非常に少ないときに導入する必要があり，60%のオプトイン率が必要なものの達成される見込みはない。隔離強制や移動許可技術は，多くの市民が受け入れられず，不本意ながら使用され，不快に思われ，抵抗され，覆されるであろう。政府や企業は，こうした解決主義的な技術が市民的自由に及ぼす影響について安心させようとしているが，こうした技術がプライバシー，政府性，コントロールクリープ，市民性に重大な影響を及ぼし，監視資本主義の論理を強化することは明らかである。

危機への対応が展開されるにつれて，地理学者らは，政府の統制と監視資本主義の連携，そしてさまざまな技術の利用を通じて，新しい監視と生政治体制がどのように生み出されるかを記録する必要がある。この作業では，形成されつつある知識共同体や擁護連合（Kitchin et al., 2017），技術主導の解決策を推進するために構築し動員する生政治と決定要因を解明し（Avila, 2020），技術が実際にどのように展開され，公衆衛生や市民的自由，統治性や市民権にどの程度の影響を与え，技術がどの程度まで浸透し，強制となり，利用が中止になるサンセット法に反するか描き出す必要がある。重要なことは，この作業において，政治経済や体制が異なる中で，技術主導の解決策が法域を超えてどのように展開しているかを検証する必要がある。実際に，北半球で展開されている技術主導の解決策は南半球とは種類が異なる。南半球では，従来の公衆衛生対策でさえパフォーマンスや経済コストの課題を考えると実践が困難な場合がある（Taylor, 2020）。また，こうした新たな監視体制がさまざまなコミュニティに及ぼす影響，階級，人種，民族，ジェンダー，その他の社会集団にまたがる影響を検証し，人々がどのようにデータの正当性の形態に抵抗し，破壊し，制定しようとしているかを描き出す必要がある。さらに，公共の場だけでなく，職場における監視技術の利用や新たな行政のあり方にまで分析のレンズを広げる必要がある。

パンデミック後の公正で公平な社会をつくるためには，市民的自由と公衆衛生は互いにやり取りされる必要はなく，調和して機能しなければならないことを，われわれはこの研究を行う中で粘り強く訴えていく必要がある。

注

1）たとえば，アイルランドでは，アイルランド科学財団，アイルランド企業庁，アイルランド政府産業開発庁が共同で，ウイルス対策に実証的な効果をもたらすソリューションを開発するための研究，イノベーション活動への資金提供を目的とした緊急対応要請を開始した。https://www.irishtimes.com/news/science/urgent-call-out-for-irish-scientists-to-help-global-coronavirus-response-1.4217710

2）たとえば，EU 対ウイルスハッカソン，https://euvsvirus.org/; The Global Hack, https://theglobalhack.com/; an example of more bottom event is the Codevid Hackathon, https://codevid19.com/

3）Global Positioning System ＝全地球測位システム

4）４月下旬，イスラエル最高裁判所は，新法が制定されるまで情報機関がCOVID-19感染者の電話の位置を追跡することを禁じた。https://www.bbc.com/news/technology-52439145
5）以下も参照のこと。https://en.wikipedia.org/wiki/COVID-19_apps
6）https://www.google.com/covid19/mobility/
7）https://twitter.com/WolfieChristl/status/1246079249544630279
8）この方法の例として，以下を参照のこと。 https://twitter.com/ashk4n/status/1250071326372638736
9）https://chp-dashboard.geodata.gov.hk/covid-19/en.html
10）https://twitter.com/WolfieChristl/status/1242956802930683913
11）Ada Lovelace Institute (2020); Guarglia and Schwartz (2020); Stanley (2020)
12）https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf

付記

本論文の初期の草稿について，Alistair Fraser，Tracey Lauriault，Sophia Maalsen，および２名の匿名の査読者からご意見をいただいたことに感謝いたします。

利益相反の開示

著者による潜在的な利益相反は報告されていない。

資金

この研究はアイルランド科学財団［助成金番号15/IA/3090］の支援を受けた。

寄稿者の注記

Rob Kitchin は，アイルランド・メイヌース大学の人文地理学教授。デジタル技術，社会，空間の関係を研究している。30冊の学術書，多数の論文や章の（共）著者または（共）編者であり，雑誌「Dialogues in Human Geography」の編集者でもある。https://www.maynoothuniversity.ie/people/rob-kitchin

ORCID

Rob Kitchin http://orcid.org/0000-0003-4458-7299

文献

Ada Lovelace Institute. (2020). *Exit Through The App Store*, April 20. https://www.adalovelaceinstitute.org/wp-content/uploads/2020/04/Ada-Lovelace-Institute-Rapid-Evidence-Review-Exit-through-the-App-Store-April-2020-1.pdf

Agamben, G. (2005). *States of exception*. University of Chicago Press.

Angwin, J. (2014). *Dragnet Nation*. St Martin's Press. ジュリア・アングウィン著・三浦和子訳（1995）.『ドラグネット　監視網社会―オンライン・プライバシーの守り方』祥伝社.

Angwin, J. (2020). Will Google's and Apple's COVID Tracking Plan Protect Privacy? *The Markup*, April 14. https://themarkup.org/ask-the-markup/2020/04/14/will-googles-and-apples-covid-tracking-plan-protect-privacy

Aouragh, M., Pritchard, H., and Snelting, F. (2020). The long tail of contact tracing. D3PT (Decentralized Privacy-Preserving Proximity Tracing). *GitHub*, April 10. https://github.com/DP-3T/documents/issues/118

Avila, K. (2020). Coronavirus as a dispositive. *Open Democracy*, May 4. https://www.opendemocracy.net/en/

democraciaabierta/coronavirus-dispositive/

Benjamin, R. (2019). *Race after technology*. Polity Books.

Biddle, S., and Fang, L. (2020). Location-Tracking Firm Helping Trump Get Reelected Now Wants to Cash In on Coronavirus. *The Intercept*, April 9. https://theintercept.com/2020/04/09/coronavirus-trump-smartphone-tracking/

Brandom, R., and Robertson, A. (2020). Apple and Google are building a coronavirus tracking system into iOS and Android. *The Verge*, April 10. https://www.theverge.com/2020/4/10/21216484/google-apple-coronavirus-contract-tracing-bluetooth-location-tracking-data-app

Busvine, D., and Rinke, A. (2020). Germany flips to Apple-Google approach on smartphone contact tracing. *Reuters*, April 26. https://www.reuters.com/article/us-health-coronavirus-europe-tech/germany-flips-on-smartphone-contact-tracing-backs-apple-and-google-idUSKCN22807J

Cahane, A. (2020). The Israeli Emergency Regulations for Location Tracking of Coronavirus Carriers. *Lawfare*, March 21. https://www.lawfareblog.com/israeli-emergency-regulations-location-tracking-coronavirus-carriers

Cavoukian, A., and Castro, D. (2014). *Big data and innovation, Setting the record Straight: De-identification does work*. Information and Privacy Commissioner Ontario. www2.itif.org/2014-big-data-deidentification.pdf

Deleuze, G. (1992). Postscript on the societies of control. *October*, 59, 3–7.

de Montjoye, Y. A., Hidalgo, C. A., Verleysen, M., and Blondel, V. D. (2013). Unique in the Crowd: The privacy bounds of human mobility. *Nature, Scientific Reports*, 3, 1–5. Article 1376. https://doi.org/10.1038/srep01376

Dencik, L., Hintz, A., and Cable, J. (2016). Towards data justice? The ambiguity of anti-surveillance resistance in political activism. *Big Data and Society*, 3(2), 1–12. https://doi.org/10.1177/2053951716679678

The Economist. (2020). Countries are using apps and data networks to keep tabs on the pandemic. *The Economist*, March 26. https://www.economist.com/briefing/2020/03/26/countries-are-using-apps-and-data-networks-to-keep-tabs-on-the-pandemic

Ems, L. (2015). Exploring ethnographic techniques for ICT non-use research: An Amish case study. *First Monday*, 20(11). https://doi.org/10.5210/fm.v20i11.6312. https://journals.uic.edu/ojs/index.php/fm/article/view/6312/5139

Eubanks, V. (2018). *Automating Inequality: How high-tech tools Profile, police, and Punish the poor*. St Martin's Press. ヴァージニア・ユーバンクス著・ウォルシュ・あゆみ訳・堤　未果解説（2021）：『格差の自動化―デジタル化がどのように貧困者をプロファイルし，取締り，処罰するか』人文書院.

Foucault, M. (1977). The confession of the flesh. In C. Gordon (Ed.), (1980) *power/knowledge* (pp. 194–228). Pantheon Books.

Foucault, M. (1991). Governmentality. In G. Burchell, C. Gordon, and P. Miller (Eds.), *The Foucault effect: Studies in governmentality* (pp. 87–104). University of Chicago Press.

Fowler, G. A. (2020). Smartphone data reveal which Americans are social distancing (and not). *Washington Post*, March 24. https://www.washingtonpost.com/technology/2020/03/24/social-distancing-maps-cellphone-location/

French, M., and Monahan, T. (2020). Dis-ease surveillance: How might surveillance studies Address COVID-19? *Surveillance Studies*, 18(1), 1–11. https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/13985 doi: 10.24908/ss.v18i1.13985

Gershom, D. (2020). Infrared Cameras Could Be the New CCTV. *OneZero*, April 24. https://onezero.medium.com/infrared-cameras-could-be-the-new-cctv-b4c79ede310e

Goh, B. (2020). China rolls out fresh data collection campaign to combat coronavirus. *Reuters*, February 26. https://www.reuters.com/article/us-china-health-data-collection/china-rolls-out-fresh-data-collection-campaign-to-combat-coronavirus-idUSKCN20K0LW

Goldenfein, J., Green, B., and Viljoen, S. (2020). Privacy Versus Health Is a False Trade-Off. *Jacobin*, April 17. https://jacobinmag.com/2020/04/privacy-health-surveillance-coronavirus-pandemic-technology

Guarglia, M., and Schwartz, A. (2020). *Protecting civil liberties during a public health crisis*. Electronic Frontier Foundation, March 10. https://www.eff.org/deeplinks/2020/03/protecting-civil-liberties-during-

public-health-crisis

Hatmaker, T. (2020). Palantir provides COVID-19 tracking software to CDC and NHS, pitches European health agencies. *Tech Crunch*, April 1. https://techcrunch.com/2020/04/01/palantir-coronavirus-cdc-nhs-gotham-foundry/

Hoonhout, T. (2020). Kansas Says It's Using Residents' Cell-Phone Location Data to Fight Pandemic. *National Review*, April 1. https://www.nationalreview.com/news/coronavirus-kansas-using-resident-cell-phone-location-data-fight-pandemic/

Ilyushina, M. (2020). Moscow rolls out digital tracking to enforce lockdown. Critics dub it a 'cyber Gulag'. *CNN*, April 14. https://edition.cnn.com/2020/04/14/world/moscow-cyber-tracking-qr-code-intl/index.html

Information Commission's Office. (n.d.). *Principle (c): Data minimisation*. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/

Innes, M. (2001). Control creep. *Sociological Research Online*, 6(3). http://www.socresonline.org.uk/6/3/innes.html

Johnston, A. (2020). Should I download the COVID-Safe app? The privacy pros and cons. *Salinger Privacy*, April 29. https://www.salingerprivacy.com.au/2020/04/29/covidsafe-app-blog/

Jones, S. (2020). Liechtenstein rolls out radical Covid-19 bracelet programme. *Financial Times*, April 16. https://www.ft.com/content/06b7e6f3-a725-4eda-9153-e0af48040e30

Keegan, M. (2019). Big Brother is watching: Chinese city with 2.6 m cameras is the world's most heavily surveilled. *The Guardian*, December 2. https://www.theguardian.com/cities/2019/dec/02/big-brother-is-watching-chinese-city-with-26m-cameras-is-worlds-most-heavily-surveilled

Kelion, L. (2020). Coronavirus: NHS contact tracing app to target 80% of smartphone users. *BBC News*, April 16. https://www.bbc.com/news/technology-52294896

Kitchin, R. (2014). *The data Revolution: Big data, Open data, data Infrastructures and their consequences*. Sage.

Kitchin, R. (2018). Governance. In J. Ash, R. Kitchin, and A. Leszczynski (Eds.), *Digital Geographies* (pp. 238–249). Sage.

Kitchin, R., Coletta, C., Evans, L., Heaphy, L., and Mac Donncha, D. (2017). Smart cities, urban technocrats, epistemic communities, advocacy coalitions and the 'last mile' problem. IT – *Information Technology*, 59(6), 275–284. https://doi.org/10.1515/itit-2017-0004

Kitchin, R., and Dodge, M. (2011). *Code/space: Software and Everyday life*. MIT Press.

Kuo, L. (2019). China brings in mandatory facial recognition for mobile phone users. *The Guardian*, December 2. https://www.theguardian.com/world/2019/dec/02/china-brings-in-mandatory-facial-recognition-for-mobile-phone-users

Lee, C. S. (2019). Datafication, dataveillance, and the social credit system as China's new normal. *Online Information Review*, 43(6), 952–970. https://doi.org/10.1108/OIR-08-2018-0231

Leith, D. J., and Farrell, S. (2020). Coronavirus contact tracing: Evaluating the Potential of using Bluetooth received signal strength for proximity detection, April 6. https://www.scss.tcd.ie/Doug.Leith/pubs/bluetooth_rssi_study.pdf

Liang, F., Das, V., Kostyuk, N., and Hussain, M. M. (2018). Constructing a data-driven society: China's social credit system as a state surveillance infrastructure. *Policy and Internet*, 10(4), 415–453. https://doi.org/10.1002/poi3.183

Linder, R. (2020). Quarantined After Waving at Coronavirus Patient: How Accurate Is Israel's 'Terrorist-tracking' Tech? *Haaretz*, March 22. https://www.haaretz.com/israel-news/.premium-isolated-after-waving-at-corona-patient-is-israeli-phone-tracking-tech-accurate-1.8698946

Linklaters. (2020). 28 countries race to launch official Covid-19 tracking apps to reduce the spread of the virus, April 16. https://www.linklaters.com/en/about-us/news-and-deals/deals/2020/april/28-countries-race-to-launch-official-covid-19-tracking-apps-to-reduce-the-spread-of-the-virus

Lyon, D. (2015). *Surveillance after Snowden*. Polity Press. デイヴィッド・ライアン著・田島泰彦・大塚一美・新津久美子訳（2016）.『スノーデン・ショック―民主主義にひそむ監視の脅威』岩波書店.

Martin, A. (2020) Coronavirus: NSO Group attempting to woo west with COVID-19 tracking software. *Sky News*,

April 4. https://news.sky.com/story/coronavirus-nso-group-attempting-to-woo-west-with-covid-19-tracking-software-11966961

McDonald, S. (2020). The Digital Response to the Outbreak of COVID-19. *Centre for International Governance Innovation*, March 30. https://www.cigionline.org/articles/digital-response-outbreak-covid-19

Morozov, E. (2013). *To save everything, Click here: Technology, solutionism, and the Urge to Fix Problems that Don't exist*. Allen Lane.

Mosendz, P., and Melin, A. (2020). Bosses are panic-buying spy software to keep tabs on remote workers. *Los Angeles Times*, March 27. https://www.latimes.com/business/technology/story/2020-03-27/coronavirus-work-from-home-privacy

Mozur, P. (2017). In urban China, cash is rapidly becoming obsolete. *New York Times*, July 16. https://www.nytimes.com/2017/07/16/business/china-cash-smartphone-payments.html

Narayanan, A., and Shmatikov, V. (2010). Privacy and security: Myths and fallacies of 'personally identifiable information'. *Communications of the ACM*, 53(6), 24–26. https://doi.org/10.1145/1743546.1743558

NBC News. (2020). Controversial tech company pitches facial recognition to track COVID-19, April 28. https://www.nbcnews.com/now/video/controversial-tech-company-pitches-facial-recognition-to-track-covid-19-82638917537

Nellis, S. (2020). As fever checks become the norm in coronavirus era, demand for thermal cameras soars. *Reuters*, April 9. https://www.reuters.com/article/us-health-coronavirus-thermal-cameras-fo/as-fever-checks-become-the-norm-in-coronavirus-era-demand-for-thermal-cameras-soars-idUSKCN21R2SF

Nielsen, M. (2020). Privacy issues arise as governments track virus. *EU Observer*, March 23. https://euobserver.com/coronavirus/147828

Noble, S. U. (2018). *Algorithms of Oppression: How Search Engines reinforce Racism*. New York University Press.

O'Brien, C. (2020). HSE Covid-19 tracing app data will be stored on individual devices. *Irish Times*, April 29. https://www.irishtimes.com/business/technology/hse-covid-19-tracing-app-data-will-be-stored-on-individual-devices-1.4240304

OECD. (1980). *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

Patriquin, M. (2020). Montreal computer scientists expect to launch contact-tracing app in less than a week. *The Logic*, April 9. https://thelogic.co/news/montreal-computer-scientists-expect-to-launch-contact-tracing-app-in-less-than-a-week/

Patton, L. (2020). Oh really? Our data is secure in government hands? *The Mandarin*, April 23. https://www.themandarin.com.au/131542-oh-really-harry-our-data-is-secure-in-governments-hands/

Paul, K., Menn, J., and Dave, P. (2020). In coronavirus fight, oft-criticized Facebook data aids U.S. cities, states. *Reuters*, April 2. https://www.reuters.com/article/health-coronavirus-facebook-location/in-coronavirus-fight-oft-criticized-facebook-data-aids-u-s-cities-states-idUSKBN21K3BJ

Pew Research. (2019). Mobile fact sheet, June 12. https://www.pewresearch.org/internet/fact-sheet/mobile/

Pollina, E., and Busvine, D. (2020). European mobile operators share data for coronavirus fight, March 18. https://www.reuters.com/article/us-health-coronavirus-europe-telecoms/european-mobile-operators-share-data-for-coronavirus-fight-idUSKBN2152C2

Proctor, K., and Devlin, H. (2020). Coronavirus UK: health passports 'possible in months'. *The Guardian*, May 4. https://www.theguardian.com/politics/2020/may/03/coronavirus-health-passports-for-uk-possible-in-months

Reuters. (2020). Emirati police deploy smart tech in coronavirus fight. *Reuters*, April 24. https://www.reuters.com/article/us-health-coronavirus-emirates-smart-hel/emirati-police-deploy-smart-tech-in-coronavirus-fight-idUSKCN2260YJ

Sadowski, J. (2020). The Authoritarian Trade-Off: Exchanging privacy rights for public health is a false compromise. *Real Life Magazine*, April 13. https://reallifemag.com/the-authoritarian-trade-off/

Schectman, J., Bing, C., and Stubbs, J. (2020). Cyber-intel firms pitch governments on spy tools to trace coronavirus. *Reuters*, April 28. https://www.reuters.com/article/us-health-coronavirus-spy-specialreport/

special-report-cyber-intel-firms-pitch-governments-on-spy-tools-to-trace-coronavirus-idUSKCN22A2G1

Schwartz, A., and Crocker, A. (2020). Governments haven't shown location surveillance would help contain COVID-19. *Electronic Frontier Foundation*, March 23. https://www.eff.org/deeplinks/2020/03/governments-havent-shown-location-surveillance-would-help-contain-covid-19

Singer, N., and Sang-Hun, C. (2020). As Coronavirus Surveillance Escalates, Personal Privacy Plummets. *New York Times*, March 23. https://www.nytimes.com/2020/03/23/technology/coronavirus-surveillance-tracking-privacy.html

Sircar, S., and Sachdev, V. (2020). Not Just Red Zones, New Rules Make Aarogya Setu Mandatory For All. *The Quint*, May 2. https://www.thequint.com/tech-and-auto/aarogya-setu-app-mandatory-for-containment-zone-red-zone-orange-zone-all-employees

Stanley, J. (2020). How to Think About the Right to Privacy and Using Location Data to Fight COVID-19. *Just Security*, March 30. https://www.justsecurity.org/69444/how-to-think-about-the-right-to-privacy-and-using-location-data-to-fight-covid-19/

Stanley, J., and Granick, J. S. (2020). The limits of location tracking in an epidemic. *ACLU*, April 8. https://www.aclu.org/sites/default/files/field_document/limits_of_location_tracking_in_an_epidemic.pdf

Stokel-Walker, C. (2020). Can mobile contact-tracing apps help lift lockdown? *BBC Future*, April 16. https://www.bbc.com/future/article/20200415-covid-19-could-bluetooth-contact-tracing-end-lockdown-early

Taylor, L. (2017). What is data justice? The case for connecting digital rights and freedoms globally. *Big Data and Society*, 4(2), 1–14. July–December. https://doi.org/10.1177/2053951717736335

Taylor, L. (2020). Discussion comments, Webinar: Data, Ethics and the Covid-19 crisis, April 23. https://mooreinstitute.ie/2020/04/24/video-of-the-covid-19-response-webinar-data-ethics-and-the-covid-19-crisis/

Timberg, C., and Harwell, D. (2020). Government efforts to track virus through phone location data complicated by privacy concerns. *Washington Post*, March 19. https://www.washingtonpost.com/technology/2020/03/19/privacy-coronavirus-phone-data/

Tony Blair Institute for Global Change. (2020). A Price Worth Paying: Tech, Privacy and the Fight Against Covid-19, April 24. https://institute.global/policy/price-worth-paying-tech-privacy-and-fight-against-covid-19

Url, S. (2020). Drones take Italians' temperature and issue fines. *Arab News*, April 10. https://www.arabnews.com/node/1656576/world

Vaughan, A. (2020). There are many reasons why covid-19 contact-tracing apps may not work. *New Scientist*, April 17. https://www.newscientist.com/article/2241041-there-are-many-reasons-why-covid-19-contact-tracing-apps-may-not-work/

Weaver, M. (2020). Don't coerce public over contact-tracing app, say campaigners. *The Guardian*, April 26. https://www.theguardian.com/law/2020/apr/26/dont-coerce-public-over-coronavirus-contract-tracing-app-say-campaigners

Wodinsky, S. (2020). Experian Is Tracking the People Most Likely to Get Screwed Over by Coronavirus. *Gizmodo*, April 15. https://gizmodo.com/experian-is-tracking-the-people-most-likely-to-get-scre-1842843363

Zuboff, S. (2019). *The Age of surveillance capitalism: The Fight for the future at the New Frontier of power*. Profile Books. ショシャナ・ズボフ著・野中香方子訳（2021）.『監視資本主義―人類の未来を賭けた闘い』東洋経済新報社.

訳者謝辞

本稿は，Kitchin, R. 2020. Civil liberties *or* public health, or civil liberties *and* public health? Using surveillance technologies to tackle the spread of COVID-19. Space and Policy24, 362–381. を訳出したものである。翻訳にあたって，Rob Kitchin 先生には突然のご依頼にもかかわらず，本稿の掲載を快諾いただきました。ここに記して感謝の意を表します。