COVID-19 追跡アプリについての倫理的ガイドライン

デジタル技術を用いた接触追跡において、鍵となる問いによって、プライバシーや平等性、公平性を守る

J. モーリー、J. カウルズ、M. タッデオ、L. フロリディ

凡例

特殊な用語や注意すべき表現については、元記事における英語表記を（）で示した。また、要約文中の特に注意すべき部分については下線で示した。

概要

本記事は、情報哲学と倫理学の教授であるフロリディをはじめとする、オックスフォード大学のインターネット研究所(Oxford Internet Institute)に所属する四人の研究者によって執筆されたものであり、ネットで閲覧することが可能である（URL は以下に記載の通り）。彼らは、英国国民保健サービス（NHS）に関連する技術開発を手掛ける政府機関である NHSX が設立、開催した「COVID-19 アプリ倫理諮問委員会（NHS COVID-19 App Ethics Advisory Board）」（すでに終了済み）に参加しており、本記事は、そこでの議論を受けて彼らが提示した、アプリが満たすべき倫理的ガイドラインについて紹介するものである。
（URL: https://www.nature.com/articles/d41586-020-01578-0）

要約

コロナウイルスの感染者と接触した人に速やかに警告する技術が、パンデミック制御の方法の一つになってきている。記事執筆現在、全世界で少なくとも 47 の接触追跡アプリ（contact-tracing apps）が使用可能であり、例えばオーストラリアや韓国、シンガポールをはじめとする国で運用段階に入っている。他の多くの政府機関も検討を行っている。
これらデジタル技術による介入には代償が伴う。個人的なデータを収集することはプライバシーや平等性、公平性の侵害につながり得るからだ。たとえアプリ運用が一時的であっても、追跡技術を拙速に運用開始してしまうことには、人々の健康や移動、社会的交流につい

ての永続的かつ漏洩しかねない記録を作り出してしまうというリスクがある。

従来、倫理的関心は主にプライバシーに関して向けられていたが、他の倫理的・社会的考慮も見過ごされてはならない。倫理的・社会的影響を考慮せずアプリの運用を開始することは危険かつ高コストで無益なことになりかねない。

筆者らは、ある接触追跡アプリが倫理的に正当化可能か否か、可能であるとすればどの程度までかを評価する 16 の質問を提示した。これらの質問は政府機関や公衆衛生を担当する機関、サービス提供者に倫理的に妥当なアプリを開発する助けとなり得る。これらは既にフランスやイタリア、イギリスにおけるアプリ開発に活用されている。また、監視機関などがこれら技術を精査するのにも役立つだろう。

接触追跡アプリを倫理的に正当化するために必要な 16 の質問

諸原則：「これは開発するべき正しいアプリですか？」（Is this the right app to develop?）**という問いについて**[1]

1. これは必要ですか？
   - はい、これは人々の命を救うという目的のため、開発されなくてはなりません（＋）。
   - いいえ、もっと良い方法があります（－）。
2. これは状況の深刻さに見合ったものですか？
   - はい、状況の重大さは、アプリが潜在的に持つ否定的インパクトを正当化します（＋）。
   - いいえ、好ましくない影響は状況に見合いません（－）。
3. それは十分に効果的で、時宜を得ており（timely）、一般の人向けに制作されていて、精確ですか？
   - はい、エビデンスによって、それが機能すること、それが時宜を得ていること、十分な数の人に採用され、正確なデータと洞察を生むことが示されています（＋）。
   - いいえ、それはうまく機能しませんし、利用可能になるのが早すぎるないし遅すぎますし、広範には用いられませんし、偽陽性や偽陰性を含むデータを集めてしまう

[1] ここでは、まず、「これは開発するべき正しいアプリですか？」という問いに関する「4つの原則」が挙げられ、その次に、「このアプリは正しい仕方で開発されていますか？」という問いに関する「12 の要求」が掲げられる。フロリディによる、「接触追跡アプリへの注意：COVID-19 追跡アプリの倫理的リスクの考慮」という別稿に従えば、前者の問いは、アプリの「妥当化（validation）」に関わるもの、後者の問いは、アプリの「正当化（verification）」に関するものとして解説されている。詳細については、高木博登らによる本稿の紹介をご参照頂きたい。

可能性があります（－）。

４. それは一時的ですか？

- はい、それが終了する明確かつ合理的な日付が決まっています（＋）。
- いいえ、定められた終了の日付はありません（－）。

諸要求：「このアプリは正しい仕方で開発されていますか？」（is this app being developed in the right way?）**という問いについて**

５. それは任意ですか？

- はい、ダウンロードやインストールするかどうかを選択することが可能です（＋）。
- いいえ、それは強制的で、人々は従わない場合罰則を受けることがあり得ます（－）。

６. それには同意が必要ですか？

- はい、どのデータがいつ共有されるかについて人々は完全な選択権を持ち、その選択をいつでも変えることが出来ます（＋）。
- いいえ、デフォルト設定では全てが常に共有されることになっていて、変更は不可能です（－）。

７. データはプライベートなままであり、利用者の匿名性は保存されますか？

- はい、データは匿名で、利用者の端末でのみ保存されます。接触した人には、感染のリスクがあるということのみが知らされ、誰からとかどこでといったことは知らされません。差分プライバシー[2]のような手法が用いられこれを保証します。サイバ

---

[2] Differential privacy の訳語。サイバー攻撃などに対するデータの安全性指標として近年新たに注目されている概念である。以下その概略を説明する。

データの安全性を評価する際には、たとえ単一の攻撃のみを想定した安全性指標の値が高くとも、他の手法の攻撃、あるいは他の背景知識を持った攻撃者に対しては脆弱であるということがありうる。たとえば、男女 10 人ずつの計 20 人からなるクラスで試験を実施し、その結果から受験者の性別と合否のみを抽出し公開したとする。このとき、クラスにいる A 君（男性）は自分の試験結果というデータを知られたくない。A 君の合否自体は公開されないから、彼のデータは守られるように思われる。しかし、たとえ公開されるのは受験者の合否・性別の人数だけであり、個人名に紐づけられた試験結果の情報は秘匿されているとしても、A 君が不合格であったという情報は守られない場合がある。たとえば女子 10 人が合格し男子 10 人が不合格であったという情報が公開された場合、攻撃者が A 君は当該クラスに所属する男性である、といった背景知識と、公開された 20 人がクラス全員の人数と一致すると判断する攻撃能力さえ備えていれば、A 君が不合格であったことは知られてしまうのである。このように、特定の背景知識や攻撃能力を持つ攻撃者のみを想定した安全性指標は、想定外の攻撃に対しては脆弱であり、また、さらに別の攻撃者を想定して改善しても、さらなる想定外が生じうるという問題がうまれる。そこで、特定の攻

ーレジリエンス[3]は高い水準にあります（＋）。

- いいえ、データは収集されたデータレベルのために（再）特定が可能であり、中央のサーバーで集中的に管理されます。接触の場所（に関する情報）も利用されます。サイバーレジリエンスは低い水準にあります（－）。

８. 利用者はデータ消去が出来ますか？

- はい、望んだ時にデータ消去が可能です。すべてのデータはアプリの運用終了時点で消去されます（＋）。
- いいえ、データが消去されるという見込みはありませんし、消去されうるという保証もありません（－）。

９. データ収集の目的は確定（define）していますか？

- はい、明確に定まっています。たとえば、感染の可能性がある人と遭遇したということを利用者に警告する、といったことです（＋）。
- いいえ、データ収集の目的は明確には定まっていません（－）。

１０. その目的は限定（limit）されていますか？

- はい、それは COVID-19 の追跡のためだけに用いられます（＋）。
- いいえ、その機能を拡張する追加要素を加えるために定期的にアップデートされます（－）。

１１. それは感染予防のためのみに用いられますか？

- はい、それは人々が自発的に感染拡大を抑制できるようにするためだけに用いられます（＋）。
- いいえ、それは人々が利益を主張したり仕事に戻ったりすることを可能にする、パスポートとしても用いられます（－）。

１２. その利用は、遵守すべき法令（compliance）となりますか？

- いいえ、それは人々に行動を強制するためには用いられません（＋）。
- はい、アプリを利用せず法令を遵守しないことは、罰金や懲役といった罰則に帰結し得ます（－）。

１３. それはオープンソースですか？

- はい、ソースコードは調査、共有、共同的な改善のために公的に利用可能です（＋）。
- いいえ、ソースコードは私有物であり、それに関するどんな情報も与えられません

撃者による攻撃に対してのみ安全性を保証する指標ではなく、任意の攻撃者による攻撃に対して同時に安全性を保証できる指標が必要とされる。この指標を差分プライバシーと呼ぶ。（寺田雅之 「差分プライバシーとは何か」、『システム/制御/情報』、2019 年 63 巻 2 号 pp. 58-63　を参考にした。また、上述の A 君の例も当論文に登場したものを一部簡略化したものである。）

[3] システムがサイバー攻撃を受けた際の回復力の高さ、復旧速度などを表す用語。

（－）。

１４.それは平等に利用可能ですか？

- はい、それは無料でありあらゆる人に分配されます（＋）。
- いいえ、それは恣意的に一部の人にのみ与えられます（－）。

１５.それは平等にアクセス可能ですか？

- はい、それはデジタル機器に慣れていない利用者にも使いやすく、可能な限り最も広範な種類の携帯端末で機能します（＋）。
- いいえ、それは特別な機器を持ち、デジタル機器を利用するための教育を十分に受けた人々にのみ使用可能です（－）。

１６.終了手続きは存在していますか？

- はい、シャットダウンの手続きが存在します（＋）。
- いいえ、適切な方針はありません（－）。

多くのアプローチ

アプリが倫理的に正当化可能かどうかはアプリの有効性や追及される目的、システムの種類やそれが運用される文脈に大きく依存する。

国や地域によってさまざまに異なるアプローチが取られている。

情報送信に用いられる方法の違い

- 中国（Alipay Health Code）：利用者それぞれに QR コードを割り当て、利用者の隔離状態を色別に示す。
- 香港：アプリを通して地方当局に位置情報を送信する電子腕輪の装着を義務化。
- ポーランド：海外渡航からの帰国者に 14 日間の自己隔離と、家にいることを証明するために位置情報付き自撮り写真の提出を義務化。

データを収集・保管する方法の違い

- シンガポールやオーストラリアの集中型（centralized）システムと、ドイツやイタリアにおいて用いられているような非集中型（decentralized）システムの違い[4]。

[4] 集中型アプリは利用者の端末に保管された匿名のデータを中央のデータベース（たとえば国家運営の保健機関などが運営している）に送り、データベースで接触が照合される。非集中型アプリは利用者の端末で照合を行う。https://www.nature.com/articles/d41586-020-01514-2 を参照すると、両者の違いは以下のようになる。まず、両者とも各利用者（端末）にユーザーコード（pseudonym）を割り当て、各端末が接近した際に Bluetooth を用いてお互いのコードを交換（これが接触を示すことになる）するという点は同じである。違

- アプリの使用が任意である場合（欧州議会が推奨している）と、強制的である場合（インド）場合の違い。
- アプリが利用者に症状を自己申告するよう要請する場合（アルゼンチン・英国）と、医師による正式な診断を課す場合（ノルウェー）の違い。

様々な超国家的な取り組みもある。WHO は資源の不足した国で、症状のチェックに加えて接触追跡も行えるアプリを開発中だ。欧州データ保護監督機構（European Data Protection Supervisor）は、欧州全土で使える接触追跡アプリの必要を呼び掛けた。欧州議会は EU 内で運用される、データ保護やプライバシーの観点から、追跡システムが満たすべき要件の大枠を定めた。

コロナ禍のプレッシャーを受ける政府機関や開発者に、プライバシーのみならず平等性や公平性も含めた広範な倫理的関心を考慮するのは難しいかもしれない。フランスやイタリア、英国におけるように、専門家グループが設立されアドバイスを行うべきかもしれない。

4 つの原則

ある接触追跡アプリが倫理的であるためには、以下の 4 原則を満たさねばならない。即ち、必要であること、状況の深刻さに見合ったものであるということ、科学的に妥当であること、運用期間が定まっていることだ。

アプリの使用がこれらの 4 原則を満たすものとなるために、我々は設計者や開発者や評価者が守るべき 16 の質問を作り上げた。そして、それぞれの質問に対して、アプリのデザインや使用が倫理的に正当化される場合（＋）、あるいは、倫理的に正当化されない場合（－）についての、典型例を提示した。これらの質問は既にリリースされたアプリにも開発中のアプリにも適用される。

理論的には、倫理的なアプリは 16 の要素全てを満たすべきだが、実践的には、様々なトレードオフがあるだろう。それらは地域毎の状況や規範、価値観によって左右されるし、ウ

いはある利用者が陽性判定を受けた後の手順にある。集中型の場合、陽性判定を受けた利用者の端末が、接触した相手のユーザーコードのリストを接触場所の位置情報などとともに中央のデータベースへ送り、中央でその情報を分析した結果、感染の可能性がある利用者を特定し警告を中央から送ることになる。これに対し非集中型は、接触相手のリストは端末自体に保存され、陽性者リストとの照合を端末が行うというものである。
非集中型アプリに比べ集中型はプライバシー保護の観点からの懸念が大きい。集中型の提唱者は、集中型ならばクラスターやスーパー・スプレッダーの発見が可能であると主張している。しかし集中型には、システムがハッキングを受けた場合にすべての情報が危険に晒されるという指摘もなされている。

イルスの感染状況や利用可能な技術の時間的変化の影響も受ける。時間経過とともにかつて正当化可能であったものがそうでなくなることもある。また、アプリの実装戦略やそれが与える影響も考慮されるべきだ。計画上は上手くいくはずだったことが実用段階では上手くいかないということもある。

アプリが失敗すると、それは不必要で、非倫理的なものとなってしまう。そうしたアプリは改善されるか運用を停止されるかするべきであり、そのような判断を行うためにも、独立機関による定期的な検証が行われるべきだ。

たった一つのチャンス

たった一度の失敗が、予見される未来への公共的な信頼を台無しにしてしまう可能性があるので、介入を適正なものにするチャンスは、政府機関には一度しかないかもしれない。政府機関や開発者、運用者は、彼らの COVID-19 接触追跡アプリが我々の定めた倫理的質問を満足に扱っていることを保証しなくてはならない。考慮なしにアプリを実用段階に持って行くことを容認するべきではない。

（吉田隼大、三上航志）