



大阪大学
社会技術共創研究センター

ELSI NOTE

No. 04

接触追跡技術と ELSI に関する 10 の視点

Ver.0.8

2020 年 4 月 30 日

Authors:

岸本 充生 大阪大学 データリテリフロンティア機構 教授
社会技術共創研究センター センター長
工藤 郁子 PHP総研 主任研究員
大阪大学 社会技術共創研究センター 招へい教員(5/1 着任予定)

※ 本ノートは、ドラフト版です。5 月半ばに Ver. 1.0 に向けて更新される予定です。ご意見や提案を募集しています。kishimoto@elsi.osaka-u.ac.jp までご連絡ください。

はじめに

新型コロナウイルス対策として、様々なデジタル技術の利用が提案されている。その中でも特に、感染者との濃厚接触の可能性を検出・追跡・通知する技術である「接触追跡(contact tracing)」技術、「曝露通知(exposure notification)」技術に、注目が集まっている。

このような技術はすでいくつかの国で利用されている。オーストラリアでもアプリのダウンロードが始まった。欧州では、研究者等が参加する PEPP-PT (Pan-European Privacy-Preserving Proximity Tracing) がアプリの開発を進め、各国が採用する方向で進んでいる。英国では国民保健サービス(NHS)が独自にアプリを開発している。また、Apple と Google が連携してアプリの開発を進めている。日本でも、5月上旬に民間団体の「Code for Japan」がアプリの提供を開始し、政府も後押しする予定である。

他方で、こうした技術は監視技術としての側面もあわせもつことからプライバシーやセキュリティといったリスクへの懸念、すなわち、倫理的・法的・社会的課題(ELSI)も指摘されている。データ保護機関等も関わり始めた国や地域もある。例えば、欧州では、ガイドラインが策定されツールボックスが提供されている。技術開発や社会的取組みによって、トレードオフではなく両立が目指されている。

先行する国や地域では、どうすればアプリの利用率をあげられるのかが大きな課題になっている。日本でもアプリの提供が開始されれば、インストールするかどうか多くの人々が悩むだろう。かく言う我々自身もそうである。そこで、「自分だったらどういう視点から判断するか」を、参考までにまとめることにした。一見遠回りに見えるかもしれないが、悩みや不安の要因を把握し、納得した上で選択することが重要であると考えます。

接触追跡技術は、新型コロナウイルス対策の選択肢を増やしてくれるものだ。各人がアプリをインストールするかどうか選べる(新しい選択肢を考案することもできる)。そして、当事者としてどう行動するか判断の集積が、今後を決する面がある。希望の持てる未来に向けて、各自、行動を選んでほしい。

10 の視点

1. 何のためのアプリか、目的を確認する

a. 目的がきちんと明示されているか？

- i. それは、感染状況の把握なのか、外出の制約を緩和していく「出口戦略」の一環なのか
- ii. 公衆衛生上の戦略の中にきちんと位置づけられているか
- iii. 目的に応じて、必要な普及率（人口に対するアプリのダウンロード率）が異なってくるだろうが、それはどの程度か

b. 自分に生じるベネフィットが、あるかもしれないリスクを上回っていると思えるか？

c. 社会全体のベネフィットが、あるかもしれないリスクを上回っていると思えるか？

2. アプリの利用は自発的なものであることを確認する

a. 「事実上ダウンロードしなければいけない」状況になっていないか？

- i. 例えば、アプリの提示をしないと、外出できない、入店できないなど事実上の制約が生じているか
- ii. それは、海外渡航時などに予防接種を要請されるなど、従来許容されてきた規律レベルと同視できるものか

b. アプリをダウンロードしても、また OS に組み込まれたとしても、機能のオン・オフを自ら選べる設定になっているか？

- i. 逆に、アプリを起動しつづけてもよい場合、他のアプリの使いやすさやバッテリーの持続性が十分担保されているか

3. 「接触可能性」「曝露可能性」の意味や精度を知る

a. 距離や接触期間などの設定の根拠は明確であるか？それらは疫学的知見に基づいているか？

b. 接触検出できる精度はどれくらいか？誤って通知される、または通知されない可能性はどれくらいか？

- i. 保健所等のスタッフが、陽性者に「最近どこに行ったか」「誰と接触したか」などをヒアリングした上で、濃厚接触者を追跡・通知するためのしきい値

(陽性者との「距離」「曝露時間」)を分析・設定すれば、濃厚接触判定の精度が高まるが、プライバシーリスクは高まるだろう

- c. **接触可能性の有無は自動的に判断・通知されるのか、それとも最終判断において人がチェックする仕組みがあるのか？**
 - i. 保健所等のスタッフが、濃厚接触者に対して助言や適切なケアを提供することは望ましいが、プライバシーリスクは高まるだろう
- d. **変わりゆく状況の中で、専門家からの助言を受けて設定を再調整する仕組みがあるか？再調整した場合に、利用者に通知されるか？その根拠は示されるか？**

4. アプリにできることとできないことを把握する

- a. **アプリで追跡できる「接触可能性」は、感染可能性のうちの一部であることが説明されているか？**
- b. **アプリをインストールしたスマートフォンを持っている人の割合によって、接触可能性の把握度合いが変わってくるかが説明されているか？**
- c. **接触可能性の通知がないことが感染可能性がないことを意味しないことが説明されているか？**
- d. **アプリの相互運用性(interoperability)はあるか？また、将来、別のアプリ(例えば、位置情報を利用したもの)や、医療健康データベース(例えば、PHR(Personal Health Record))と紐付けられる可能性はありそうか？**
 - i. 例えば、自治体ごとにバラバラのアプリを採用した場合、接触判定できないとなると、対策として意味をなさなくなるのではないか
 - ii. 濃厚接触判定の精度が低いとすれば、位置情報や PHR とデータ連携させないと、対策として意味をなさなくなるのではないか

5. データの使われ方を把握する

- a. **端末に蓄積されるデータや、感染が判明した際にサーバに提供される行動ログは、〈視点1〉の目的に照らして必要最小限であるか？**
- b. **アプリ利用者の身元はわからないようになっているか？**
 - i. 他のデータと突合させた場合の再識別のリスク評価を含む、個人の特定を回避するための措置はとられているか？
 - ii. 端末の一時的 ID は疑似ランダムに生成され定期的に変更されているか？

- c. 陽性者と接触があったことが通知される場合、誰が陽性なのかが分からないようになっているか？
- d. 行政に連絡先等を提供可能とする場合、その都度同意がとられる仕組み(オプトイン)になっているか？
- e. 端末のデータやサーバに提供されたデータがどのタイミングで削除されるか明記されているか？感染症の終息後は、アプリは無効化されるか？OS から削除されるか？

6. データが安全に管理されているか確認する

- a. どういう場合に端末のデータが、サーバに提供されるのか？
- b. ライフサイクル全体にわたりセキュリティ対策が講じられているか？
 - i. データの可用性、信頼性、機密性を守るための効果的なサイバーセキュリティは担保されているか？
 - ii. サイバーセキュリティの確保は第三者によって検証されているか？

7. 誰が、どんなデータにアクセスできるのかを知る

- a. アプリの開発・運用の責任者は誰か？
- b. アプリの承認は、誰がどのような手続きで行っているのか？
- c. 陽性者のパーソナルデータを取り扱う上での政府や行政の役割は？
 - i. 陽性者が確実に陽性であることを担保し、虚偽の通知(「いたずら」や「詐欺」)を防ぐには、保健所等との連携が必要だろう
- d. それは、目的に限定したデータの取扱いになっているか？
 - i. 例えば、虚偽の通知を防ぐために、保健所等と連携する際も、陽性申告のワンタイムパスワードを陽性者に送るなどの配慮がされているか
- e. 第三者へのデータ共有はされるか？共有される場合、その都度同意がとられる仕組み(オプトイン)になっているか？
 - i. 捜査関係事項照会書や弁護士会照会等により情報が提供されることはありうるのか？
- f. 誤って処理されたデータの即時的かつ不可逆的な消去方法は用意されているか？

8. アプリを使えない人や陽性者への配慮の有無を確認する

- a. アプリを使えない人たち、例えば高齢者や子供に対する代替措置はあるのか？彼らが不利益を被らないような配慮が可能か？
- b. 職業上、感染可能性のある人たちとの接触を避けられない人たち（医療・福祉従事者、流通・小売事業者等）に対する代替措置はあるのか？きちんと防護していた場合に通知をなくすような設定は可能か？
- c. 使いたくない人たちへの配慮はどうか？大きすぎる不利益などは生じていないか？（〈視点 2〉とも関連）
- d. 陽性者、濃厚接触者、接触地で生活や経済活動を行う人々などへの偏見の防止を確保するセーフガードがあるか？

9. 自身の「接触可能性」を知った後、とるべき行動を把握する

- a. 虚偽の通知（「いたずら」や「詐欺」）を防止する仕組みはあるか？
- b. 接触可能性の通知があった場合にとるべき行動が明確になっているか？通知があった人がみな医療機関に向かうことで医療資源を圧迫することはないか？
- c. 疑問がある場合に相談できる窓口はあるか？

10. 第三者がチェックする仕組みがあるか確認する

- a. アプリ開発・運用について、第三者の立場から監督・助言する専門家組織が設置されているか？
- b. 第三者からの助言に対して、どう対応したか・しなかったかについて記録を残し、公開されているか？
- c. 監査可能性（auditability）があるか。一定の情報開示を通じて、利用者本人や専門家（研究機関や NPO 等）が、定期的（例えば、3 か月に 1 回等）、プライバシーへの影響などを評価・検証する仕組みがあるか？
- d. 事態の終息後に、第三者による事後的な評価・検証が実施され、評価結果が公表されることになっているか？

アプリの仕様が判明した暁には、上記視点に基づいて、ダウンロードするかどうかを考えた。

最後に、10個の視点を考えるのは「しんどい」という人もいるだろう。その際は、信用できそうな組織や信頼できそうな専門家の判断に託すというのも、ひとつの対応だ。

例えば、普段でも、医薬品の作用機序を十分に理解できなくても、医師や薬剤師の勧めに従って服薬している。これは、高い能力・専門性を備えた医師等に任せた方が合理的であるという考えや、国家資格による認証や専門職集団の行動規範 (code of conduct) による制約などが制度的に担保されているから信じるに足るとの考えが背景となっている。今回も、このような「信頼 (trust)」「信認 (fiduciary)」があればよいだろうし、さらに言えば、信頼の仕組みを構築する一助になればとも考えている。その意味で、開発者・運用者には、少なくとも〈視点 10〉だけは、ぜひとも担保してほしい。

逆にもっと詳しく知りたい人は、アプリのリリースに合わせて「データポリシー」「プライバシーガイドライン」「プライバシー影響評価書」などが公表されるかもしれないので、チェックしよう。

参考資料

接触追跡技術/曝露通知技術

- <https://www.apple.com/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/>
- <https://www.blog.google/inside-google/company-announcements/apple-and-google-partner-covid-19-contact-tracing-technology/>
- <http://news.mit.edu/2020/bluetooth-covid-19-contact-tracing-0409>
- <https://www.politico.com/news/2020/04/07/kushner-coronavirus-surveillance-174165>

- <https://www.pepp-pt.org/>
- https://edpb.europa.eu/news/news/2020/statement-edpb-chair-processing-personal-data-context-covid-19-outbreak_en
- https://ec.europa.eu/commission/presscorner/detail/en/ip_20_626
- https://ec.europa.eu/commission/presscorner/detail/en/ip_20_670
- https://ec.europa.eu/commission/presscorner/detail/en/IP_20_680
- https://edpb.europa.eu/news/news/2020/european-data-protection-board-twenty-third-plenary-session-edpb-adopts-further-covid_en
- <https://www.reuters.com/article/us-health-coronavirus-europe-telecoms/european-mobile-operators-share-data-for-coronavirus-fight-idUSKBN2152C2>

- https://edps.europa.eu/sites/edp/files/publication/2020-04-06_eu_digital_solidarity_covid19_en.pdf
- <https://www.tracetgether.gov.sg/>
- https://www.mois.go.kr/frt/bbs/type010/commonSelectBoardArticle.do?bbsId=BBS_MSTR_000000000008&nttlId=76366
- <https://www.itmedia.co.jp/news/articles/2004/15/news148.html>
- <https://k-tai.watch.impress.co.jp/docs/news/1247495.html>
- <https://xtech.nikkei.com/atcl/nxt/column/18/01279/041700002/>
- <https://www.nri.com/jp/keyword/proposal/20200326>
- <https://www.shojihomu-portal.jp/nbl1137pc>
- <https://thinktank.php.co.jp/voice/6142>
- <https://www.web-nippy.jp/17671/>
- <https://gendai.ismedia.jp/articles/-/71248>
- <https://note.com/inflorescencia/n/n6d1de663948c>

詐欺やフェイクニュースへの注意喚起

- https://www.caa.go.jp/policies/policy/consumer_policy/information/notice_200227.html
- <https://www.caa.go.jp/notice/entry/019433/>
- https://www.mhlw.go.jp/stf/newpage_09393.html
- <https://www.europarl.europa.eu/news/en/headlines/society/20200327STO76003/how-to-protect-yourself-from-cybercrime>
- <https://about.fb.com/news/2020/04/covid-19-misinfo-update/>
- <https://thehill.com/policy/technology/491338-youtube-to-reduce-spread-of-videos-falsely-linking-5g-to-the-coronavirus>
- <https://www.fcc.gov/document/fcc-warns-covid-19-robocall-text-scams>

COVID-19 関連の偏見・差別、ヘイトクライム

- <https://ag.ny.gov/press-release/2020/ag-james-launches-hotline-combat-coronavirus-hate-crimes-and-xenophobic-rhetoric>
- <https://www.mhlw.go.jp/content/10900000/000624048.pdf>

ELSI NOTE No. 04

接触追跡技術とELSIに関する10の視点

Ver.0.8

2020年4月30日

大阪大学 社会技術共創研究センター

〒565-0871 大阪府吹田市山田丘2-8

大阪大学吹田キャンパステクノアライアンス C棟 6階

TEL 06-6105-6084

<https://elsi.osaka-u.ac.jp>