日本型セルフケアへのあゆみ

児玉龍彦
東京大学先端科学技術研究センターがん・代謝プロジェクトリーダー
日本セルフケア推進協議会業務執行理事

人生において，元気でいることは誰にとっても大事なことである．自分の健康と病気に関わることは正確に知りたい．さまざまな薬や治療法があるなら，自分の希望で決めたい．そうした願いをもとに，大きな転換がはじまろうとしている．インターネットの普及により，医薬品・健康食品・病院に関する情報に誰でも容易にアクセスできるようになったが，正確性に欠けた情報も溢れかえっている．本シリーズでは，地に足をつけた“日本型セルフケア”へのあゆみを提唱していく．

第8回 コンタクトトレーシングと個人情報

POINT

- **新型コロナウイルスの陽性者ならびに濃厚接触者の行動を追跡するために，スマートフォンを用いる取り組みが世界各国で進められている．諸外国では，スマホから取得した位置情報や通信情報が分析され，追跡に用いられている．**
- **位置情報やスマホ決済アプリの履歴をもとに行動を追跡できれば，誰と会い，どこで飲み食いし，どんな趣味があるかといった情報まで取得が可能となる．こうした情報はきわめてプライバシー性が高いため，データを収集する公衆衛生上の必要性と個人情報の権利をめぐって議論が巻き起こっている．**
- **そうした背景から，日本の新型コロナウイルス接触確認アプリ「COCOA」ではプライバシーの保護が重視されている．このアプリで収集された接触情報は本人のスマホ内にのみ暗号化して記録され，行政機関や第三者が接触記録や個人情報を利用・収集することはないとされている．どういった仕組みで運用されているのかを解説する．**

※本稿は2020年10月8日時点の情報に基づいて書かれたものです．

新型コロナ対策を目的とした個人情報の利用

PCR検査で陽性となった者の行動履歴を追跡することは，感染経路の特定，ひいては感染拡大の防止において重要な手立てとなる．これを徹底して行っているのが，韓国の追跡方式である．しかし，そのやり方には個人情報保護の観点で懸念もある．まずは韓国での状況をみてみよう．

1. 韓国での感染拡大の経緯

新型コロナウイルスの発生地である中国に隣接する韓国では，2月にキリスト教系新興宗教団体「新天地イエス教会」の集会において集団感染が発生した．教祖の兄が1月末に死亡し葬儀を行った病院で，当時に中国からきた教徒も多数出入りしたことで院内・市中感染が発生し，2月25日時点で韓国の感染者893人のうち，半数以上がこの教団の信徒とその関係者であった[1]．この集団感染を発端として大邱（テグ）市は同国におけるウイルス流行の中心地となった．ソウル市は「感染拡大を防ぐための積極的な措置を講じなかった」として，この教団の教祖や教団幹部らを“殺人罪”で刑事告発している．教団は，濃厚接触者の把握するための正確な参加者名簿の提出などを拒んだといわれる．

2. 韓国における追跡方式

2013年の中東呼吸器症候群（MERS）発生時に対応が十分でなく多数の死者が出た反省から，韓国での追跡方式はかなり“強権的”なものとなっている．

GPSで取得した感染者の移動履歴だけでなく，カード会社からクレジットカードの決済情報，市

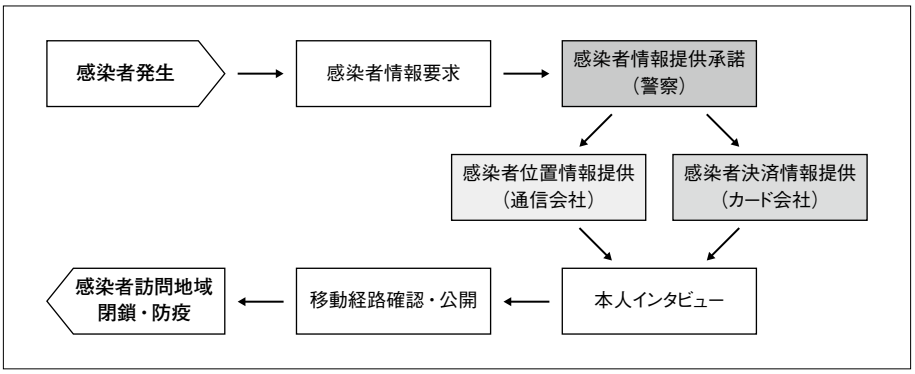

図 1　韓国における個人情報を駆使した追跡体制

中の防犯カメラでの映像など使える情報をすべて収集し，行動と接触の履歴を網羅的に把握することが特徴である（**図 1**）．

このように徹底して行政が個人情報を収集・利用することは防疫上有効ではあるだろうが，第三者への情報漏洩や，監視社会化といったリスクも懸念される．次項では，それについて検討したい．

位置情報から個人は特定できる？

GPS 位置情報から，個人に関する情報はどれくらい入手できるのだろうか．匿名の GPS 情報を公開しているスマホ用アプリ「EveryPost」（※現在は非公開となっている）に登録されたデータから，どの程度まで個人を特定できるかを検証した試みを紹介する[2)]．

この試みでは特定する対象として，国外の移動が多い人物が選ばれた．頻繁に出入りしている場所をもとに大学関係者であると推測し，また海外への移動履歴をもとにその時期に開催された国際学会を検索し，その学会に出席しそうな分野の研究者のなかから候補者をリストアップした．さらにその人物が頻繁に行く場所を Google のストリートビューで見るとそこには一軒家があり，その表札を見るとリスト中の 1 人の人物の名字と一致した．この間わずかに 10 時間であった．

GPS 情報の精度は 10 メートル程度の場合が多く，どこへ行ったかを正確に追跡するのは難しい．しかし行動履歴からその個人の職業などの特徴をつかむことができれば，行った場所がどこであるかの類推ははるかに容易になる．

個人情報保護法では，匿名の位置データは個人情報に該当しないため，本人の同意を得なくても企業間で共有することさえできる．個人情報を提供した覚えのない第三者から本人が特定され，行動が筒抜けになる可能性もあるということになる．位置情報をもとに，趣味，通っている病院，よく行く飲み屋，宗教団体など，隠しておきたいさまざまな秘密が知られかねない．

ネットを覗くとき，ネットもまたこちらを覗いている

インターネットであるワードを検索したり，画像や動画を見たり，商品を買ったりするとき，自分側だけでなく相手側にも履歴が残る．ブラウザのシークレットモードを使うと履歴は残らないが，それは自分のコンピュータ上のみの話であり，匿名でインターネットを利用できるわけではない．アクセス先のサイト管理者やプロバイダが解析を行えば，閲覧した内容や使用者の身元を調べることも可能である．

米国プリンストン大学のコンピュータサイエンス学部のブライアン・カーニハン教授は，「インターネットを見つめれば，インターネットも等しくお前を見つめ返すであろう」と授業で教える．カーニハン教授によると，車を買おうと自動車メーカーのサイトにアクセスしたところ，初回の訪問で 79 の異なるサーバーから 200 を超えるクッキーなどがダウンロードされたという[3)]．

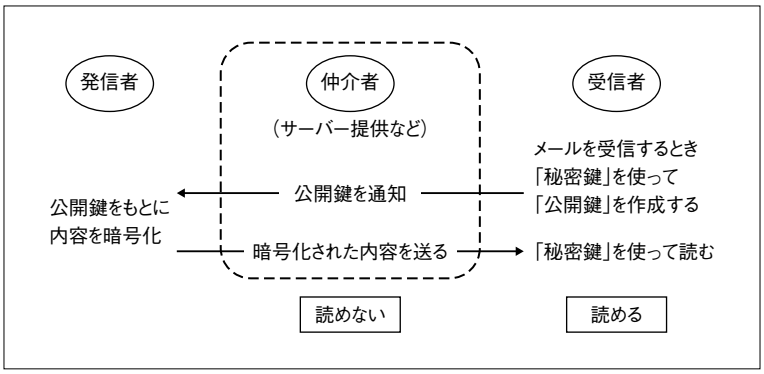

図 2　公開鍵方式による情報の保護

このように，ユーザーのクッキーをもとにあらゆる情報が分析・集計され，企業活動に利用されている．代表的な例としては，検索履歴を活用することでユーザーの趣向や関心事を分析し，より訴求力のある広告を表示させる“ターゲティング広告”があげられる．そのデータが，ユーザーの十分な同意を得ずに企業間で取引されることもある．大手就活情報サイトの「リクナビ」を運営するリクルートキャリアが，クッキーや閲覧履歴などの情報をもとに応募者の“内定辞退率”を予測し，そのデータを顧客に販売していたニュースは記憶に新しい[4]．

街中を移動しているときも，あなたの情報はさまざまなことに活用されている．日本交通系のタクシー会社・ジャパンタクシーは，タクシー内に設置されたカメラで乗客を撮影して性別を自動で判定し，車内のタブレット端末に表示する広告の内容を選定している．顔画像の利用用途や方法に関して乗客への事前説明が不十分だったとして，ジャパンタクシーは個人情報保護委員会から指導を受けることとなった[5]．

こうして得られる情報を，企業のみならず政府がチェックしているケースもある．公共サービスに活用するという名目で，人口 14 億人のビッグデータを管理している中国がその象徴である．また米国では，国家安全保障局(NSA)が「XKeyscore(エックスキースコア)」というプログラムを用いて，あらゆるデータ通信の検索・分析を行っていたことが，元CIA 職員のスノーデン氏の告発に記されている[6]．

情報を保護するためには

先述したカーニハン教授のコンピュータサイエンスの教科書[3]によると，こうした懸念への対策として有効なのが，データの暗号化だという．

・データの暗号化

ここでは“共通鍵”と“公開鍵”の 2 種類の暗号方式について述べたい．共通鍵は古典的な暗号方式で，暗号化と解読で同じキーを使用する．発信者と受信者で同じパスワードを共有するため処理が高速だが，鍵さえ分かってしまえばだれでも解錠できてしまうため，いったん漏洩すると不特定多数に開かれるリスクがある．共通鍵が複雑であるほど解読に必要な労力(計算機の演算能力)増えるが，それでも完璧に安全とは言えない．

共通鍵暗号に生じる安全性のリスクは，発信者と受信者が同じ鍵を用いるために起きる問題である．そのため，両者が異なる鍵を用いる暗号方式が考案された．今日主に用いられるのはこの“公開鍵”方式である(**図 2**)．

公開鍵は，誰でも自由に利用できるように公開されていて，“閉める専用の鍵”である．対して秘密鍵は，受信者だけがしっかりと管理をしている“開ける専用の鍵”である．共通鍵方式と違い，閉める鍵と開ける鍵が異なるため，開ける鍵(秘密鍵)さえしっかり管理しておけば情報は秘匿される．公開鍵方式を用いた運用は以下のようになる．

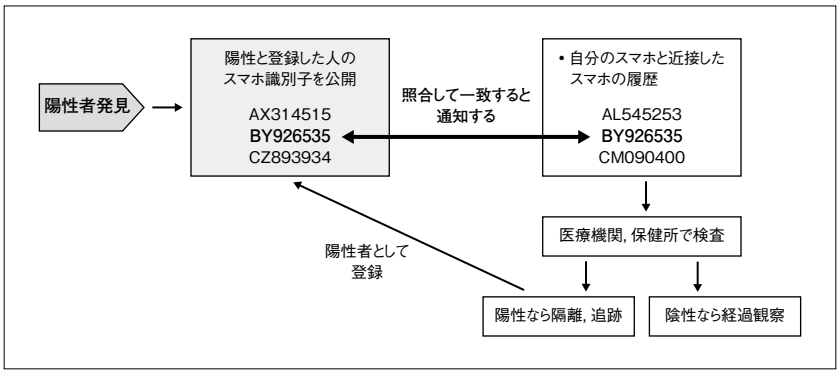

図 3　接触確認アプリ「COCOA」の仕組み

① 受信者が秘密鍵から公開鍵を作成し，あらかじめ発信者に渡す
② 発信者は，その公開鍵を使って通信内容を暗号化し，受信者に送る
③ 暗号化された文書を受信者が受け取る
④ 受信者は秘密鍵を用いて暗号化を解除し，中身を確認する

公開鍵方式の代表的な例がRSA暗号である．これは，素因数分解の困難さを利用したアルゴリズムにより安全性を高めるものである．その解読には膨大な時間と労力を要するため，公開鍵方式で広く使われている．

公開鍵方式はインターネット通信においても活用されているが，デメリットとして共通鍵方式よりも非常に多くの処理時間がかかる点があげられる．共通鍵方式の処理速度と公開鍵方式のセキュリティを兼ね備えた通信方法がSSLサーバー証明書を用いた暗号化通信であり，「HTTPS」とよばれる．これはブラウザのURLに表示されるので，お馴染みの方も多いだろう．

「COCOA」で行われている情報の保護

この公開鍵方式と似た仕組みで，情報が漏れないように，陽性者との接触(コンタクト)を当事者が把握できるように考えられたのが，日本の接触確認アプリ「COCOA(ココア)」である．

このアプリをダウンロードして接触通知を有効にすると，ランダムに生成された識別子がスマホから定期的にBluetoothで発信される．この識別子は頻繁に更新され，ユーザーの個人情報と紐付けられることはない[7]．他のアプリユーザーと“1 m以内の距離を保ち，15分以上の時間が経過したとき”，相手の情報をスマホの中だけに記録する．「相手の名前やID」「相手といた場所」「相手といた時間」などは記録されず，識別子を持つ人と濃厚接触したという情報のみが記録されている．もちろん自らの個人情報はネットワークに公開されず，位置情報を含む行動履歴も記録されていない．サーバーで公開される「COVID-19陽性と登録した人の識別子」とスマホ内の「接触した識別子」を照合し，一致するとアプリ上で濃厚接触の可能性が通知される(**図3**)．なお，保存された識別子は2週間で自動的に消去される．直近2週間の接触した識別子の記録のなかに，陽性登録者の識別子があれば，濃厚な接触があったとして，検査を受けることが推奨される．そして陽性が確認された場合は，今度は自らがアプリに陽性を登録する．

この仕組みの要点は，ユーザーの情報が公開鍵方式と同様の方法で管理されているところにある．陽性者の識別子はアプリの機能により暗号化され，サーバーに公開される．対して，ユーザーのスマホに保存された接触履歴は秘匿されており，第三者に閲覧されない．厚労省が提供するのはサーバーだけであり，**図3**でいう仲介者の位置づけである．サーバーに多数の人がアクセスしても，その人たちの位置情報も接触情報もサーバー側には残らない．

本アプリは，AppleとGoogleの共同開発による技術が基盤となっている．ターゲティング広告に代表されるように個人のデータ活用に積極的なGoogleと，プライバシー保護を最重要理念に位置づけているAppleの異色のタッグが実現したことも特筆すべきことである．彼らは，個人にかかわる情報をデバイス内に留めることで，データの利活用と保護の両立をめざした．ユーザーのプライバシー保護を表明することが，利用率の向上につながるという点で2社の方向性が一致した．

アプリの公開にあたり，AppleとGoogleは以下の共同声明を発表している[8]．これを引用して本稿の締めくくりとしたい．

「このシステムの成功は，ユーザーが使ってくれるかどうかにかかっている．われわれは強力なプライバシー保護が，システム利用を促進するための最善のアプローチだと考えている．」

*　　*　　*

文献/URL

1) AFPBB News．韓国，新型コロナ集団感染の新興宗教「新天地イエス教会」とは？　2020年3月1日．(https://www.afpbb.com/articles/-/3270907?pid=22183421)
2) 日本経済新聞．10時間で本人特定，スマホ位置から出張・実家も筒抜け．2019年3月25日．(https://www.nikkei.com/article/DGXMZO42770850S9A320C1000000/)
3) ブライアン・カーニハン著，酒匂　寛訳．教養としてのコンピュータサイエンス講義．日経BP；2020，p.380.
4) 日経クロステック．不十分な同意で個人情報を販売　リクナビ，就活生の辞退予測中止．2019年8月22日．(https://xtech.nikkei.com/atcl/nxt/mag/nc/18/020800017/080900265/)
5) 日本経済新聞．ジャパンタクシーを再指導，個人情報保護委改善遅れに．2019年9月17日．(https://www.nikkei.com/article/DGXMZO49896420X10C19A9TJ1000/)
6) Wikipedia. Xkeyscore. (https://ja.wikipedia.org/wiki/XKeyscore)
7) 厚生労働省．COCOA-新型コロナウイルス接触確認アプリ．App Store．(https://apps.apple.com/jp/story/id1517366013)
8) Google. Exposure Notification API launches to support public health agencies. May 20, 2020. (https://blog.google/inside-google/company-announcements/apple-google-exposure-notification-api-launches/)