「接触確認アプリ及び関連システム仕様書」に対する
プライバシー及びセキュリティ上の評価及びシステム運用上の留意事項

2020年5月26日

接触確認アプリに関する有識者検討会合

はじめに

本「『接触確認アプリ及び関連システム仕様書』に対するプライバシー及びセキュリティ上の評価及びシステム運用上の留意事項」（以下、「本評価書」という。）は、新型コロナウイルス感染症（以下、「本感染症」という。）への対策として厚生労働省が運営する予定の接触確認アプリ及び関連システム（通知サーバーを含む。以下、「本アプリ」と総称する。）が、プライバシー及びセキュリティ等の観点から安全なものであるかどうかを評価すると共に、その運用段階における留意事項を指摘し、もって本アプリが広く国民に信頼され、社会に普及することを後押しすることを目指すものである。

本評価書の**第１**では、「接触確認アプリ及び関連システム仕様書」（2020 年 5 月 26 日付テックチーム作成。以下、「本仕様書」という。）に記載された本アプリの仕様について、主にプライバシー及びセキュリティの観点からのリスク分析及び評価を行う。続く**第２**では、そのようなアプリ及びシステムを運営するにあたって、本アプリの運営者たる厚生労働省（以下、「本アプリ運営者」という。）及びその業務委託先である民間事業者（以下、「委託先事業者」といい、本アプリ運営者と合わせて「本アプリ運営者等」と総称する。）が留意すべき点を指摘する。

本評価書は、2020 年 5 月 26 日付の仕様書を対象としている。今後、本アプリの機能が大幅に変更される場合には、改めて当該変更に係る仕様書について、本検討会その他の中立な専門性のある有識者委員会等による検討が行われるべきである。

また、陽性者の状況の把握や濃厚接触に関する調査等を目的として別途厚生労働省が構築している感染者システムについては、本評価書の対象としていない。

なお、本評価書で用いる用語は、特段の断りがない限り、本仕様書の定義を引用する。

第１　本アプリのプライバシー及びセキュリティ上の評価

１．プライバシー

＜サマリー＞

本アプリ運営者は、個人に関する情報として、通知サーバーにおいて、感染者システムから発行される処理番号及び登録した陽性者の端末から送信される診断キーを取り扱う。

まず、これらの情報に対する、行政機関の保有する個人情報の保護に関する法律（以下、「行個法」と略す。）及び個人情報の保護に関する法律（以下、「個情法」と略す。）の適用関係を整理する[1]。

[1] 但し、現時点では、実際のシステム開発が完了した段階ではないため、一定の幅を持って適用関係を整理するものである。

行個法の適用について、処理番号は、同法の定める「要配慮個人情報」[2]に該当するため、処理番号について行個法上の義務を負う。また、委託先事業者も、行個法に基づく安全管理措置に関する義務を負う。

他方、診断キーについては、原則として個人情報に該当しないと考えられる。もっとも、本アプリ運営者が、診断キーと個人情報である処理番号を紐づけることによって、診断キーから特定の個人を識別することができる場合には、診断キーも要配慮個人情報に該当し、行個法の適用対象となる。

次に、個情法の適用については、委託先事業者において、処理番号から特定の個人を識別できる場合（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなる場合を含む。）には、処理番号は（診断キーと処理番号を紐づける場合には診断キーも）、「要配慮個人情報」[3]に該当することになり、委託先事業者が同法に基づく義務を負うこととなる。

こうした行個法及び個情法に基づく義務に加え、本アプリは、ユーザーが陽性者や接触者であるかどうかという機微な情報を取り扱うものであり、その上で広くユーザーに信頼されるものである必要があることから、行個法及び個情法の適用関係にかかわらず、サービスの利用開始及び陽性者登録等の重要な局面において、ユーザーの同意を取得することを原則とすると共に、情報のライフサイクル（取得、保管、利用、移転、削除）の各過程において、プライバシーに対する十分な配慮がなされる必要がある。本仕様書によれば、本アプリは、そうした配慮が十分になされているものと考えられるが、一定の事項については運用にあたって留意する必要がある。

（1）行個法及び個情法の適用の有無

(i) 行個法

本アプリ運営者は厚生労働省であることから、本アプリが取得する情報に行個法の定める「個人情報」が含まれる場合、行個法に基づく義務を負う可能性がある。

行個法上、生存する個人に関する情報であって、①特定の個人を識別することができるもの（他の情報と照合することができ、それにより特定の個人を識別することができることとなるものを含む。）、及び②個人識別符号が含まれるものは、「個人情報」に該当する[4]。

本仕様書によれば、本アプリ運営者が取り扱う個人に関する情報は、陽性者が登録を行った場合に通知サーバーに送信される(a)処理番号及び(b)診断キーである[5]。これらの情報には、個人識別符号は含まれないことから、以下では上記①の要件について検討する。

(a) 処理番号

[2] 行個法2条2項、4項
[3] 個情法2条1項、3項
[4] 行個法2条2項
[5] ①登録した陽性者以外のユーザー端末の日次キー、及び②ユーザー間で交換される接触符号は、各端末内でのみ保存されるため、本アプリ運営者等が取り扱う情報には含まれない。

処理番号とは、陽性者からの要求を受けて感染者システムから発行する無意かつ一次的な番号である。感染者システムの管理者でもある厚生労働省では、どの処理番号がどの陽性者に割り当てられているかを把握していることから、処理番号によって特定の個人を識別することが可能である。したがって、処理番号は行個法の定める個人情報となると考えられる。さらに、処理番号は、陽性者であると医師等に診断された個人にしか発行されない番号であるから、当該処理番号によって特定される個人は、陽性診断を受けた者であることが明らかである。したがって、処理番号は行個法の要配慮個人情報に該当するといえる[6]。

(b) 診断キー

診断キーとは、端末につき毎日異なるものが１つランダムに生成される日次キーと、時刻情報を基に作成される識別子である。陽性者が、処理番号による認証を経て、自身の情報を感染者システムに登録する場合には、この診断キーが通知サーバーにアップロードされることになる[7]。

診断キーを構成する要素は、Apple-Google Exposure Notification Framework (AGF) の API で提供されるものであり、それ自体では、特定の個人や端末を識別することはできないと考えられる。

もっとも、(a)の処理番号と、上記の診断キーがサーバー内で紐付けられることにより、本アプリ運営者等において、(処理番号を介して) 診断キーがどの陽性者に割り当てられたものであるかを把握できるような場合には、診断キーも個人情報となる。さらにこの場合、個人の診断キーが通知サーバーに送信されるのは、当該個人が陽性者であると医師等に診断され、感染者システムから発行された処理番号をアプリ上で適切に入力した場合のみであることから、当該診断キーを鍵として、陽性診断を受けた特定の個人を識別できることとなる。したがって、診断キーが行個法の個人情報にあたる場合には、当該診断キーは要配慮個人情報に該当すると考えられる。本アプリでは、処理番号を陽性者の認証終了後直ちに通知サーバーから削除することとしていることから、本アプリ運営者等が、処理番号を介して、通知サーバー内で陽性者と診断キーを結びつけることは困難と考えられるが、もしこれが可能である場合には、診断キーについても行個法上の義務が及ぶ。

以上より、本アプリ運営者が通知サーバーにおいて取り扱う情報のうち、少なくとも処理番号は要配慮個人情報に該当するといえる。したがって、本アプリ運営者は、処理番号について行個法上の義務を負うものと考えられる。また、委託先事業者も、行個法上、個人情報に関する安全管理措置を行う義務を負う[8]。

他方、診断キーについては、原則として個人情報に該当しないと考えられるが、本アプリ運営者が、診断キーと個人情報である処理番号を紐づけることによって、診断キーから特定の個人を識別することができる場合には、診断キーも要配慮個人情報に該当し、行個法の適用対象となる。

---

[6] 行個法２条４項、同施行令４条２号

[7] 本仕様書第２編第１章 1.5)

[8] 行個法６条２項

なお、かかる処理番号は（診断キーが個人情報に該当する場合には、診断キーも）、行個法上の「個人情報ファイル」[9]として管理されるものと考えられる。但し、処理番号は陽性者の認証終了直ちに削除され、診断キーも取得から 14 日の経過後に削除されることから、一年を超えて記録される情報に適用される総務大臣への通知や、個人情報ファイル簿の作成及び公表を行う義務はない[10]。

（ii）個情法

本アプリの委託先事業者における処理番号及び診断キーの取扱いが、個情法上、個人情報取扱事業者[11]による「個人情報」の取扱いと評価される場合には、当該事業者に別途個情法が適用される。

本アプリの委託先事業者が、個人情報取扱事業者に該当するか否かは、当該事業者が確定した後に、個別具体的に評価する必要があるが、個人情報取扱事業者に該当する可能性は高いと考えられる。

そこで、委託先事業者が取り扱う情報が個情法の「個人情報」に該当するかどうかを検討する。個情法上、「個人情報」とは、生存する個人に関する情報であって、①特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）、及び②個人識別符号が含まれるものをいう[12]。

委託先事業者が取得する個人に関する情報は、処理番号及び診断キーである（個人識別符号は含まれない）。当該事業者は、これらの情報からだけでは、特定の個人を識別することができないと考えられるが、委託先事業者が別途感染者システムの運営も行っている等の事情により、処理番号と他の情報とを容易に照合し特定の個人を識別することができる場合には、処理番号は（診断キーと処理番号を紐づける場合には診断キーも）、個人情報に該当すると考えられる。

さらに、処理番号や診断キーが委託先事業者の通知サーバーに送信されるのは、これらの情報に係る本人が陽性者であると医師等に診断された場合に限られることから、処理番号（診断キーと処理番号を紐づける場合には診断キーも）が個情法の個人情報に当たる場合には、これらの情報は要配慮個人情報に該当すると考えられ、委託先事業者は、個情法に基づく義務を負うこととなる。

（iii）運用及びシステム設計におけるプライバシーへの配慮の必要性

上記のとおり、本アプリ運営者等には、行個法及び個情法に基づく義務が課される場合があるが、本アプリ運営者等は、こうした法令上の義務のみを遵守すればよいわけではないと考えられる。

すなわち、本アプリはユーザーが陽性者や接触者であるかどうかという機微な情報を取り扱うものであり、これらの情報が第三者に知られれば、特定のユーザーやその家族の差

[9] 行個法 2 条 6 項
[10] 行個法 10 条 2 項 6 号、11 条 2 項 1 号
[11] 個情法 2 条 5 項
[12] 個情法 2 条 1 項

別につながる等、個人の人格的利益を損なうおそれがある。こうしたリスクを考慮した上で、本アプリが国民に広く信頼され利用され、本アプリに期待される公衆衛生上の目的を達成するために、本アプリ運営者等は、法令上の義務の有無にかかわらず、ユーザーのプライバシー情報（個人に関する情報であって、行個法や個情法の「個人情報」に該当するものに限らない。）の取扱いに十分に配慮する必要がある。

そのため、本アプリ運営者は、アプリの利用開始や陽性者登録等の重要な局面において、ユーザーの同意に基づく運用を原則とすると共に、情報のライフサイクル（取得、保存、利用、移転、削除）の各過程においてもユーザーのプライバシーが確保されるようなシステムを設計しなければならない。また、委託先事業者との間の契約によって、当該事業者がそのような運用やシステムを実現することを確保しなければならない。

このような観点から、以下で、本アプリが満たすべきプライバシー上の配慮について検討を行う。

（2）ユーザーの同意の取得

本アプリにおいて、ユーザーの重要な意思決定の局面は、①アプリの利用開始の決定、及び、②自らが陽性者と診断された場合に、その旨を感染者システムに登録し、自己の診断キーを他のユーザーに発信する決定であり[13]、これらの場面において、ユーザーの正しい理解と自由な意思に基づく同意を取得するべきである。そのため、ユーザーに対してはあらかじめ、感染症対策全体の仕組みの中でのアプリの位置づけ、プライバシー情報を取得する目的、データ項目ごとの利用目的や利用方法等について十分な説明を尽くすべきである（本評価書第２ 1(1)も参照)。

本仕様書によれば、本アプリのインストール及び利用開始にあたっては、利用規約やプライバシーポリシー等をわかりやすく表示した上で、ユーザー本人の同意を取得する（同意しない場合にはアプリを利用できない）ことされる[14]。また、インストール及び利用開始に関する同意の撤回はいつでも可能であり、同意を撤回した場合は、利用時にユーザー本人のアプリに記録された接触に関わる情報は削除され、以後は当該撤回者の情報取得は行わないものとされている。

本アプリ運営者は、こうした同意及び同意の撤回の判断が、ユーザーの正しい理解に基づく任意の判断によって行われることを確保するため、利用規約やプライバシーポリシー等において、プライバシー情報の利用目的やデータフローについて、ユーザーに対して具体的に分かりやすく明示すると共に、端末の画面上でも概略を分かりやすく説明し同意を取得するべきである。

次に、陽性者が感染者システムへ登録を行う際には、処理番号（要配慮個人情報である）及び診断キー（要配慮個人情報となる場合がある）を通知サーバーに送信することに加え、自己の診断キーが通知サーバーから他のユーザーに発信されることになるが、これらの点に

[13] これらに加え、接触者が感染者システムに登録する際の意思決定も重要であるが、この点については、本アプリではなく感染者システムの問題と整理されるため、本評価書のスコープに含まない。

[14] 本仕様書第２編第１章 1.1）

ついても本人の同意を取得することとされている[15]。その際には、改めて処理番号及び診断キーの利用目的について陽性者に明示すべきである[16]。この段階での同意については、撤回が認められていないが、これは、一旦陽性者として登録された者が同意を撤回することによって、本アプリのシステム及びその後の接触者の取扱い全般に混乱が生じることを避けるためであり、やむを得ないものといえる。また、陽性者の診断キーが他のユーザーに送信されても、他のユーザーからは、当該診断キーがどの個人のものであるかを特定することは通常できないから、同意が撤回できないことによる陽性者のリスクは小さいといえる。

このように、ユーザーが本アプリの利用を開始する際及び接触に関する情報をアップロードする際には、その都度同意を取得することとされている点については評価できる。その上で、こうした同意を実質的なものとするために、上述のとおり、ユーザーに対してはあらかじめ、プライバシー情報の利用目的や取扱方法等について十分な説明を尽くすべきである。

（3）取得するプライバシー情報が最小限であること

本アプリの目的は、陽性者と接触した者に対して通知メッセージを表示するというものであり（以下、「本目的」という。）、本アプリを通じて取得されるプライバシー情報は、その目的を達成するために必要最小限である必要がある。

(i) 本アプリ運営者等が取得する情報

本アプリ運営者等が本アプリを通じて取得する情報は、上記（1）のとおり、①陽性者の処理番号及び②その陽性者の診断キーである。

このうち処理番号については、陽性である旨の虚偽申告を防ぐために、感染者システムから陽性者のみに発行される番号を通じて認証を行う目的のものであり、本目的を達成するために必要な機能であると評価できる。また、診断キーについては、各端末内で陽性者のマッチングを行うために不可欠の情報である。諸外国では、診断キーに加えて、陽性者の接触履歴をサーバーにアップロードするシステムも存在するが、本目的を達成する上ではそのような情報は不要であるから、取得することとしていない。

以上より、本アプリを通じて本アプリ運営者等が取得する情報は、本目的達成のために最小限のものであるといえる。

(ii)本アプリのユーザーが取得する情報

本アプリを使用するユーザーの端末が本アプリを通じて取得する情報は、①自身の端末に割り当てられる日次キー及びそれを基に生成される接触符号、②自身が接触したユーザーの端末の接触符号、及び③陽性者の診断キーである。名前、性別、住所、生年月日、位置情報、電話番号、メールアドレス等の個人が識別され得る情報については、本目的を達成するのに不必要と考えられることから、本アプリで取得することとはしてしない[17]。

[15] 本仕様書第2編第1章1.3)
[16] 処理番号については、行個法4条によって利用目的の明示が義務づけられている。
[17] 本仕様書第1編2.3)

①日次キーは、端末につき毎日ランダムに生成される識別子であり、接触符号は、日次キーをもとに 10 分ごとに生成される符号である。これらの識別子及び符号は、いずれもそれ自体で個人を特定して識別することはできない。

②の他のユーザーの接触符号は、それによって特定の個人を識別することは困難である上、接触符号から日次キーを計算することはできないとされる点で、プライバシーに十分に配慮がなされたものであるといえる。

③の診断キーも、上記（１）のとおり特定の個人を識別することができない情報であり、また、ユーザーがこれを受信することは、陽性者を自己の接触履歴とマッチングするために不可欠である。

以上より、本アプリを通じてユーザーが取得する情報は、本目的達成のために必要最小限のものであるといえる。

（４）プライバシー情報の適切な管理

本アプリ運営者等は、通知サーバーで保管するプライバシー情報について、十分なセキュリティ措置を行うことで、データの安全を確保しなければならない[18]。

本仕様書では、下記２．のとおり、通知サーバー及びアプリの双方について、本アプリの運営上に必要と考えられるセキュリティ基準を満たすことが求められているため[19]、これを満たす限りにおいて、十分なセキュリティ措置が行われるものと評価できる。

本アプリがこれらの基準を満たしているかどうかについては、システム導入時の脆弱性検査を行うことに加え、本評価書第 2.4 に示す検証を継続的に行う必要がある。

また、本アプリに係るサービスは、国内のクラウドサービスを使って行うとされている[20]。本アプリ運営者がクラウド事業者にデータ保存を再委託等する場合には、クラウド内に保存する情報の取得・アクセス・変更等に係る権限を本アプリ運営者のみが有すること、本アプリに関する契約の終了後は、クラウド事業者においてクラウド内に保存されている本アプリに関するデータを速やかに削除すること等を、確認すべきである。

（５）プライバシー情報の移転

本アプリ運営者等が取得するプライバシー情報（処理番号及び診断キー）のうち、診断キーについては、通知サーバーで取得された後、他のユーザーの端末に発信されることになる。本アプリ運営者等は、上記（２）のとおり、この点についてユーザーに対してあらかじめ十分な説明を尽くすべきであり、その上で、①ユーザーがアプリの利用を開始する前、及び、②陽性者となったユーザーが感染者システムに登録する前に、各ユーザーの同意を取得すべきである。

（６）利用する必要がなくなったプライバシー情報の消去

[18] 行個法 6 条 2 項により、個人情報については、委託先にも本アプリ運営者同様の安全管理義務が課されている。

[19] 本仕様書第 2 編第 2 章 11.

[20] 本仕様書第 2 編第 2 章 12.

本仕様書によれば、端末内の日次キー及び接触符号、並びに通知サーバー内の診断キーは、それぞれ取得から 14 日間の経過後に消去することとされている。また、通知サーバー内の処理番号は、陽性者の認証直後に削除することされている[21]。

日次キー、接触符号及び診断キーを 14 日間とするのは、コロナウイルスの潜伏期間を考慮した上で必要とされる合理的な期間である。処理番号は、もっぱら認証目的で発行されるため、認証後ただちに破棄することに合理性がある。

以上より、本アプリでは、不要となったプライバシー情報は速やかに削除するものとされていると評価できる。

２．セキュリティ

本アプリは、厚生労働省が構築し、運用管理する情報システムである。そのため、本情報システムは、政府機関が遵守すべき情報セキュリティ対策を実施することが必要である。政府機関の情報システムでスマホ端末のアプリを提供していることは少なく、スマホ端末のアプリに関するセキュリティ対策については、特に留意するべきである。

（１）政府機関のシステムが遵守すべきセキュリティ対策

本アプリは、国の行政機関等が遵守すべきセキュリティポリシーである「政府機関等の情報セキュリティ対策のための統一基準」（サイバーセキュリティ戦略本部決定）に基づきセキュリティ対策を行うことが示されている。「政府機関等の情報セキュリティ対策のための統一基準」は、情報システムが遵守すべき一般的なセキュリティ対策項目が網羅されている。

クラウドサービスの利用に関しては、認証制度や監査フレームワークの活用を含めた「政府情報システムにおけるクラウドサービスの利用に係る基本方針」（各府省情報化統括責任者（CIO）連絡会議決定）に従った利用検討と利用方針が示されている。

本アプリの委託先事業者が、クラウドサービス事業者にデータ保存を再委託等する場合には、当該クラウドサービス事業者において適切な安全管理措置が講じられることを担保する必要がある。

（２）スマホ端末のアプリに関するセキュリティ対策

スマホ端末のアプリに関するセキュリティ対策としては、スマホの OS である iOS 及び android に組み込まれた仕組みを利用することが重要である。本仕様では、スマホの OS のセキュリティ機能を利活用することが示されている。スマホ OS のセキュリティ機能は、OS に最適化されており、かつ、信頼のあるセキュリティ機能である。

これらは信頼のあるセキュリティ基準・機能であり、セキュリティ対策方針としては妥当である。但し、実際に本アプリがこれらの基準を満たすかどうかについては、運用段階で適切に検証する必要がある（本評価書第２．４）。

---

[21] 本仕様書第 1 編 7.

第２　本アプリの運用上の留意点

１．透明性

本アプリの仕組み、及び本アプリが本評価書の記載事項を遵守していることを、ユーザー及び第三者が客観的に確認できるよう、本アプリ運営者等は、本アプリの設計及び運用に係る透明性を確保すべきである。

＜具体的な対応方法＞

（１）仕様書等の公開

本アプリに係る仕様書及びそれに付随する文書は、公表すること。

（２）ユーザーへの通知公表

本アプリ運営者等は、感染症対策全体の仕組みの中でのアプリの位置づけ、本アプリの仕組み及びプライバシー情報の取扱い等の事項について、利用規約やプライバシーポリシー、厚労省や委託先事業者のホームページ等において、ユーザーに対して具体的にわかりやすく明示すること[22]。また、本アプリを初めて起動する際に、上記の事項について、視覚的に理解しやすい方法で概要を表示すること。

2. インクルーシブネス（包摂性）

本アプリ運営者等は、本アプリがより多くのユーザーが利用できるようなデザインとすると共に、本アプリを使用することでユーザーが不当に差別されることが無いように十分留意すべきである。

＜具体的な対応方法＞

（１）分かりやすい操作

高齢者等、スマートフォンの操作に慣れていない者であっても問題なく利用できるような、分かりやすく使いやすいユーザーインターフェースとすること。

（２）多言語対応

日本語を理解しない者であっても仕様できるよう、少なくとも英語など、多国籍の言語で表示できるようにすること。

（３）同意の判断を行うことが困難なユーザーの代理登録

16 歳未満の者や成年被後見人など、自身で本アプリの陽性者登録に関する同意の判断を行うことが困難なユーザーや自らによる操作が困難なユーザーについては、代理人が本アプリ

[22] その際、本アプリが使用している Bluetooth 技術がユーザー間の距離測定を信号強度に依存するものであり、Bluetooth 信号が通過する可能性のあるバリア（ガラス窓や薄いアパートの壁など）があるかどうかは考慮されない場合があるといった、本アプリの性能の限界についても記述することが重要である。

の使用や陽性者登録に関する同意を与えることができるようなインターフェースとすること。

（4）ユーザーの差別の防止

本アプリを使用することによって、陽性者、接触者、その家族等が差別を受けないよう、本アプリのシステム全体の設計運用上、十分に配慮すること。

とりわけ、接触者に表示される接触通知は、その記載内容によっては、誰が陽性者であるかという機微な情報の特定につながるものであることから、そうした特定ができない内容とする点に特に留意する必要がある。具体的には、接触者に対し、接触の回数、日、時間帯等を通知することが考えられるが、これらのうちどのような情報を通知するかは、本アプリの利用者数も踏まえながら、慎重に検討すること[23]。

また、自らが陽性者又は接触者であることを画面に表示するかどうかを、ユーザー自身が選択できるようにする等の配慮を行うこと。表示自体についても、画面の色や構成を工夫して、陽性者又は接触者であることが他人から肩越しに見えること等のないように配慮を行うこと。

（5）相談窓口の設置

本アプリに関する苦情・相談のための窓口を設置すること。

3．使用目的の限定

本アプリは、本仕様書第1編1.に記載の公益的目的の下に、国民に対してその使用を呼びかけるものである。そのため、本アプリ運営者は、本アプリを上記以外の目的以外に使用し、又は第三者により使用されることを避けるべきである。

＜具体的な対応方法＞

（1）目的外利用の禁止

本アプリ運営者等は、本アプリ及び本アプリの運用によって得られたデータを、上記の目的以外のいかなる目的（刑事及び民事事件の証拠収集、ユーザーの行動把握、委託先事業者における商業目的等）でも使用し、又は第三者に使用させないこと。

（2）本感染症終息後のサービス停止

本感染症が終息したと厚生労働省が判断した場合には、アプリ運営者は、速やかに本アプリのサービス提供を停止すること。

4．検証

本アプリ運営者は、上記の原則を遵守していることを自ら継続的に検証し、中立かつ専門の有識者による検討会に報告するとともに、その評価を受けるべきである。

---

[23] たとえば、「〇月〇日午前」のように接触の日時が接触者に判明すると、「その時に一緒にいたのはあの人だ」ということで、陽性者が特定できてしまうことがある。

＜具体的な対応方法＞

（1）内部検証

本アプリの運用開始前及び運用開始後、上記の項目が満たされていることについて、定期的に検証を行うこと。その際、プライバシーについてはプライバシー影響評価を、セキュリティについては、脆弱性などのセキュリティに関するテストを行うこと。

（2）有識者検討会等の評価

上記の検証結果を含む本アプリの運営状況について、本検討会その他の中立かつ専門性のある有識者委員会等に対し、定期的に報告し、その評価を受けること。

（3）仕様書の大幅な変更

本仕様書を大幅に変更する場合には、事前に本検討会その他の中立かつ専門性のある有識者委員会等に報告し、その意見を尊重すること。

5．調整事項に関する留意事項

① 仕様書に記載の「各端末内で全接触回数を記録し表示することを可能にする」という調整事項については、基本的には、ユーザー本人に自分の他者との接触回数を表示するだけなので、プライバシー上の問題はないと考えられる。

② 他者との接触回数をアプリ上で表示・確認することにより、接触回数を減らし、感染リスクを減らそうという行動変容を促す上では、当該機能の実装が必要と考えられる。

③ 本機能の搭載にあたっての具体的な仕様は現時点で不透明であることから、今後機能を固めていく過程で、適時評価を行っていくことが求められる。

以上