資料６

「接触確認アプリ　実施処理のログ蓄積・送信に関する仕様」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 9 月 18 日
接触確認アプリに関する有識者検討会合

はじめに

本会合は、新型コロナウイルス感染症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し、2020 年 5 月に「『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、「原評価書」という。）をまとめた。

その後、原評価書による評価の対象となった「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）及び原評価書に基づき、厚生労働省（以下、「本アプリ運営者」という。）が本アプリの開発をすすめ、2020 年 6 月 19 日にリリースした。リリース以降、様々な障害が見つかり、これまでに三度、本アプリのバージョンアップを行っている。また、これまで[1]に約 1698 万件のダウンロードがなされるとともに、785 件の陽性登録に基づいて接触者に通知が行われている。

今般、本アプリ運営者より、本アプリについて、障害の疑いのある事象が起きているが、利用者による誤認との切り分けや原因の特定に至っていない事象があること、これらの事象により、陽性者と接触があった可能性がある利用者に対していち早く通知を出し、検査等の適切な対応につなげ、感染拡大防止を図るという本アプリの目的が十分に達成できていない可能性があることが報告された。また、利用者からの意見・情報を踏まえて速やかに本アプリの機能等の改善を行い、より多くの利用者に安心して利用いただくため、本アプリが実施した処理のログを端末内で保存し、本アプリの障害の可能性等を感じた利用者本人の同意の元で送信する機能を本アプリに追加することについて提案がなされ、その仕様（以下、「本仕様」という。）が示された。

本会合は、本アプリが引き続き広く国民に信頼され、公衆衛生上の役割を適切に果たすことを後押しすることを目的として、本仕様について、主にプライバシー及びセキュリティの観点からの評価を行う（本評価書第１）とともに、本アプ

[1] 2020 年 9 月 16 日 17 時現在

リの実施処理のログを取得して本アプリの機能等の改善を図るにあたって本アプリ運営者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（本評価書第２）の検討を行った。厚生労働省においては、本仕様及び本評価書に則って当該機能の実装を進め、利用者からの意見・情報を踏まえて速やかに本アプリの機能等の改善を図り、真に新型コロナウイルス感染症の感染拡大防止に資するものとしていくことを期待する。

第１　本仕様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

（１）行個法[2]及び個情法[3]の適用の有無[4]

まず、本アプリ運営者である厚生労働省が、本仕様に基づき新たに取得することとなる情報が、行個法上の「個人情報」に該当するかどうかを検討する。本仕様によれば、本アプリ運営者が新たに取得することとなる情報は、本アプリで実施した処理のログ（実施した処理の内容、処理が行われた時点、処理の成功/失敗、処理の実施にあたり参照した情報、処理の結果として出力した情報、実施時の状態等。API の処理結果として本アプリが受け取る情報を含む。）に加えて、本アプリの利用環境に関する情報としてアプリのバージョン、利用端末の OS、OS バージョン及び端末機種としている。これらの情報だけでは特定個人を識別することはできないと考えられる。

ただし、送信された実施処理のログを、ログ ID 等を介してヘルプデスク等で受け付けた問い合わせ事象と紐付けて管理する可能性があるとしている。このような場合において、仮に、ヘルプデスク等で問い合わせを受け付けたメールアドレス等が個人情報に該当し、これと紐付けが可能な状態となるのであれば、紐付けられた実施処理のログも行個法上の個人情報に該当し、本アプリ運営者等は、新たに取得する情報についても行個法上の義務を負うこととなる。

委託先事業者への個情法の適用の有無については、委託先事業者が本仕様に基づき新たに取り扱うこととなる情報だけで特定の個人を識別することはできないが、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ような状態で管理・運用を行う場合には、個情法の個人情報に該当し、委託先事業者が、新たに取り扱うこととなる情報についても個情法上の義

---

[2] 行政機関の保有する個人情報の保護に関する法律

[3] 個人情報の保護に関する法律

[4] 現在の本アプリの運用状況に鑑みると、本アプリ運営者等はすでに行個法及び個情法上の義務を負っていると考えられる。

務を負うこととなる。

（２）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

本アプリは、利用者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ることに鑑み、本アプリが国民に広く信頼され利用され、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、利用者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べきであることは、原評価書で指摘したとおりである。本アプリ運営者は、引き続き国民・利用者から疑念を抱かれることのないよう、実施処理のログの蓄積・送信機能の設計及び委託先事業者による運用において、以下のとおりプライバシー面の配慮がなされることを確保しなければならない。

（３）利用者の同意の取得

実施処理のログの蓄積・送信にあたり、利用者が意思決定をする場面としては、不具合等を感じた際に、実施処理のログを本アプリ運営者等が管理するサーバーに送信する場面がある。この際に利用者が、送信対象となる情報の性質、利用目的や利用方法について正しく理解した上で送信されるよう、適切な情報提供がなされるべきである。

本仕様によると、改正するプライバシーポリシーを、本アプリアップデート後の最初の起動時に表示し、利用者本人の同意を得た上で利用を開始できるようにするなど、利用者に改正内容をわかりやすく知らせる仕組みを実装することとしている。また、実施処理のログの送信にあたっては、利用目的等を画面にわかりやすく明示し、本人同意を得た上でサーバーに送信される仕組みにすることとしている。これらに加え、本アプリ運営者は、本アプリのホームページ等でプライバシーポリシーの改正内容等について周知を行うなど、利用者が安心して使い続けられるよう、配慮すべきである。

（４）取得するプライバシー情報が最小限であること

現在、報告されている障害疑い事象の中には、本アプリに正しい処理番号を入力しても陽性者としての登録ができない、接触が OS 上で検知されているにもかかわらず接触があった旨が本アプリに表示されない等、本アプリの感染拡大防止の目的を十分に果たせていないことが疑われるものも含まれている。また、スマートフォンアプリケーションの特性として、頻繁な OS や API のアップデートや、利用している機種によって障害が発生する場合があり、現在報告されているもの以外の障害の疑いが、今後報告されてくる可能性もある。そのため、継続的

に利用者からの声を集め、それを元にアプリの改善を図っていく必要がある。利用者の端末から実施処理のログ等を収集して分析・活用していくことはスマートフォンアプリケーションの保守運用において一般的に行われていることであり、かつ、上述のようなアプリの継続的な改善に必要なものであると言える。

本アプリで実施した処理のログ以外に取得する、本アプリの利用環境に関する情報としては、利用しているアプリのバージョン、利用端末の OS 及び OS バージョン、端末機種のみとしており、これらは本アプリの障害発生時に原因等を特定する上で不可欠な情報であると考えられる。

実施処理のログの収集の目的は、利用者からの意見を踏まえ、障害事象の原因特定の可能性を上げ、速やかに本アプリの機能改善につなげることにより、より多くの方に安心して本アプリをご利用いただくこととしている。本仕様に基づき新たに取得する情報は、その目的を達成するために必要最小限であると言える。

また、本アプリのヘルプデスクでは、メールにより様々な不具合事象やログ ID を含む問い合わせを受け付けることとなるが、その際に氏名等の個人情報がメールに記載されないよう、利用者に対する案内において留意すべきである。

（５）実施処理のログの適切な管理

本アプリ運営者等は、原評価書「第１．１．（４）プライバシー情報の適切な管理」に記載の留意事項に加え、本評価書「第１．１．（１）」で指摘しているとおり、本アプリの実施処理のログが、仮に、ヘルプデスク等で問い合わせを受け付けたメールアドレス等が個人情報に該当し、これと紐付けが可能な状態となるのであれば、紐付けられた実施処理のログも行個法及び個情法上の個人情報に該当することとなるため、行個法・個情法上の義務を遵守し、十分なセキュリティ措置等を講ずる必要がある。

（６）実施処理のログの移転

本アプリの実施処理のログについては、本アプリ運営者等が本アプリの改善のために取得するものであり、本アプリ運営者等以外の第三者に移転しないことについては、プライバシーポリシー等に明記し、利用者の理解を得るべきである。

（７）利用する必要がなくなった実施処理のログの消去

本仕様によれば、実施処理のログが発生した場合には端末内で 14 日間保持した後、端末から削除することとしている。また、利用者の同意に基づいてサーバーに送信された実施処理のログについては、本アプリ運営者等において管理プ

ロセスを定義し、障害調査終了後に当該管理プロセスに従い適切に削除することとしている。また、この削除までの期間は長くとも 60 日までとしている。

特定の障害事象の調査に必要な期間として 60 日以上保持されることは想定し難く、障害調査終了後に適切に実施処理のログが削除されるよう、管理プロセスの定義及び運用にあたり十分に留意すべきである。

２．　セキュリティ

本アプリのセキュリティ面の評価については、原評価書「第１．２．セキュリティ」で示したとおりであるが、原評価書で示される基準の遵守の検証にあたっては、実施処理のログの蓄積・送信の機能についてもあわせて検証を行うべきである。また、利用者からの安心と信頼に資するよう、脆弱性等のセキュリティに関するテストの実施状況についてもホームページ等で公表を行うべきである。

第２　実施処理のログの収集及び活用にあたっての留意点

１．　透明性

本アプリ運営者等が本アプリを通じて仕様外のプライバシー情報を収集しているのではないかとの疑念を国民・利用者に持たれることがないよう、本アプリ運営者は、実施処理のログの蓄積・送信の機能について、そのメリットとあわせてホームページや本アプリの画面等でわかりやすく明示することが必要である。特に、引き続き本アプリで特定の個人を識別しうる情報等を取得するものではないことについて、国民・利用者の理解を得るよう、丁寧に説明すべきである。送信された実施処理のログ情報は、本アプリの保守運用の委託先事業者のみが取り扱うこととなるが、取り扱うことができる者の範囲を明確に示し、利用者が安心してこの機能を利用できるようにすることも必要である。

また、引き続きソースコードを公開し、第三者が客観的に確認できるようにすることや、サーバーに送信する前の実施処理のログ内容を利用者本人が確認できるような仕組みを装備することも透明性確保の上で有効であると考えられる。

２．　利用者及び保健所の業務負荷への配慮

本アプリの不具合を感じている利用者が、実施処理のログ情報を送信するに当たり誘導が不十分であった場合には、利用者が困惑するとともに、保健所に追加的な相談等の負荷が生じることも想定されるため、ヘルプデスクや本アプリの画面において、利用者に対して適切な誘導をするよう、最大限の配慮をすべきである。

３．　インクルーシブネス（包摂性）

本アプリは、幅広い国民が利用することで感染拡大防止の効果が期待されるものであることに鑑み、利用者がヘルプデスクへの問い合わせに際して実施処理のログの送信に同意をしなかったとしても、本アプリの通常の利用に関し支障が生じないよう、ヘルプデスクではその時点で明らかになっている情報に基づいて適切な対応が行われるようにすべきである。また、実施処理のログの送信手順についても、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、わかりやすいユーザーインターフェースとすべきである。

４．　利用目的の限定

実施処理のログの収集は、利用者からの意見・情報を踏まえて速やかにアプリの機能等の改善を行い、より多くの利用者に安心して利用いただくことを目的として行うものである。従って、本アプリ運営者等は、新たに収集される情報を、この目的以外のいかなる目的でも使用しないことが重要であり、その旨をプライバシーポリシー等にも明記すべきである。

５．　検証

原評価書で求めたとおり、本アプリ運営者は、原評価書に記載した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。この検証及び評価の実施にあたっては、実施処理のログの収集等に係る追加機能についてもあわせて行い、適切な運用を確保するとともに、利用者からの信頼の醸成に努めるべきである。