資料５－２

接触確認アプリ　実施処理のログ情報蓄積・送信に関する仕様

１．　背景・目的

接触確認アプリ（以下「本アプリ」という）は、「接触確認アプリ及び関連システム仕様書」（2020 年 5 月 26 日新型コロナウイルス感染症対策テックチーム。以下「仕様書」という。）に則って厚生労働省が開発し、2020 年 6 月 19 日にリリースした。これまでに約 1700 万件ダウンロードされており、利用者からメールのヘルプデスク等に、本アプリの障害の可能性も含めた様々な意見・情報が寄せられている。

これまでに 3 度、本アプリのアップデートを行い、機能の改善を図ってきたが、現在の本アプリには、実施処理のログを蓄積・送信する機能が実装されていないため、再現確認できない事象については、利用者へのヒアリングとソースコード解析以外の調査方法がなく、原因を特定することが困難な場合がある。

そこで、プライバシーに最大限配慮した本アプリの特徴を尊重しつつ、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ご利用いただくことを目的に、実施処理のログ情報を蓄積し、利用者本人の同意・協力のもとで送信する機能を実装する。

そのための仕様を以下に示す。なお、本仕様に特段の記載のない限り、本仕様で用いる用語の定義は仕様書によることとする。

２．　仕様

２．１　対象データ

（１）蓄積・送信する情報

本アプリで実施する一連の処理の中で、様々な障害が発生しうることから、利用者からの障害に関する情報を踏まえ、速やかに本アプリの機能改善につなげるために必要な処理の情報を蓄積・送信の対象とする。

以下の情報を蓄積・送信の対象とする。

・本アプリで実施した処理の内容
・処理が行われた時刻
・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。

本アプリの実施処理のログ以外に本アプリの利用環境に関して、以下の情

報を蓄積・送信の対象とする。（以後、ログ関連情報と記載）

・利用しているアプリのバージョン
・利用端末の OS
・OS バージョン
・端末機種

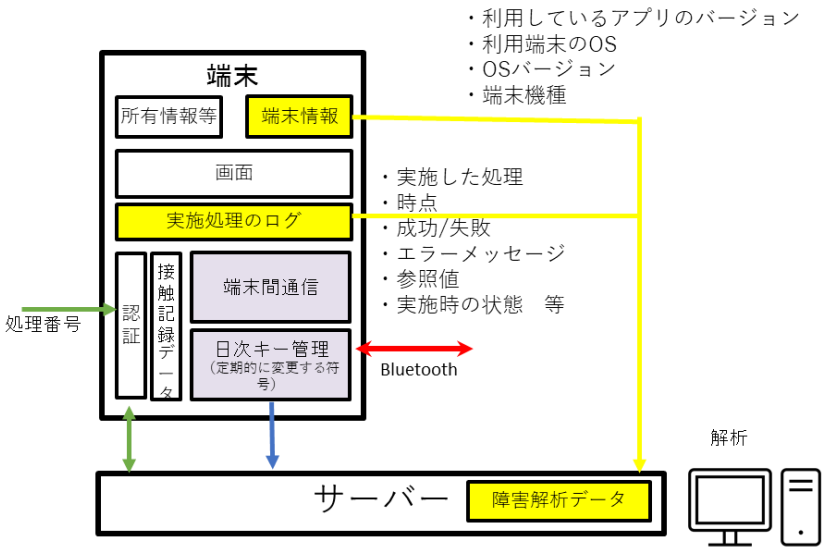
以下の情報は蓄積・送信の対象としない。

・処理番号
・日次鍵（TEK）
・接触符号（RPI）
・診断鍵（Diagnosis Key）

プライバシーに最大限配慮した本アプリの特徴に鑑み、本アプリで取得しない以下の情報は、当然、蓄積・送信の対象としない。

・利用者の氏名、電話番号、メールアドレス等の特定個人を識別しうる情報
・位置情報
・ＩＰアドレス、MAC アドレス、ホスト名等、当該情報だけで端末を特定しうる情報

整理すると以下の流れになる。



２．２　蓄積・送信等の機能

（１）端末内での情報収集と蓄積

本アプリが何らかの処理を実施し、実施処理のログが発生したときに、実施処理のログ情報を本アプリのデータ層に蓄積する。

１．利用者が操作もしくは本アプリが自動で蓄積

２．実施処理のログ情報を端末内に記録する

※　端末内の実施処理のログ情報は、取得から１４日後に順次削除する

（２） 蓄積した実施処理のログ情報の送信

利用者本人が、本アプリの障害の可能性を感じた場合等に、任意で送信ボタンを押すことで、蓄積された実施処理のログを送信する。

この際に、送信される実施処理のログ情報の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。

１．利用者が障害の可能性を認識

２．利用者が報告を希望する場合は、任意で送信機能を選択

３．実施処理のログ情報の利用目的などを端末画面に表示

４．利用者が同意した上で送信ボタンを押下

５．実施処理のログ情報及びログ関連情報をサーバーに送信

また、実施処理のログを送信する前に、利用者本人が実施処理のログ内容を確認することができる仕組みを設ける。

（３）機能追加アップデート時のプライバシー確認

接触確認アプリの更なる普及に当たっては、接触確認アプリがプライバシーに最大限配慮した仕組みであることについて、透明性を確保しながら説明責任を果たし、それにより利用者・国民からの信頼を得ることが重要である。

そのため、この機能の実装に伴い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。

１．アプリアップデート（自動処理）

２．新プライバシーポリシーの表示（アップデート後初回起動時）

３．新プライバシーポリシーへの同意

２．３　実施処理のログ情報を活用した障害調査

（1）送信された実施処理のログ情報の管理・活用・削除

利用者から送信された実施処理のログ情報の管理プロセスを厚生労働省と協議の上、定義する。

障害調査のための利用が終了した時には、ただちに当該管理プロセスに従い適切に削除する。なお、削除までの期間は、サーバーでの受信から最大60日とする。

一旦サーバーで受信した実施処理のログ情報は、利用者の任意により削除されず、上記の管理プロセスに則って障害調査及びサーバーからの削除を行う。

（2）ヘルプデスクでの対応とデータの紐付け

ヘルプデスク等では障害の疑いのある問い合わせを受け付ける。必要に応じて、障害解析のための実施処理のログ情報送信の案内を行う。なお、ヘルプデスクに問い合わせを行った利用者が、実施処理のログの送信に同意をしなかったとしても、継続して本アプリをご利用いただけるよう、最大限のサポートを行う。

実施処理のログは、ヘルプデスク等で受け付ける障害の疑いのある問い合わせ事象と紐付けて管理することにより、原因の特定とアプリの改善により有効に役立てることが可能になると考えられる。

このため、利用者から送信された実施処理のログは、ログID（アプリ又はヘルプデスクで実施処理のログに対して振り出すランダムな番号で、問い合わせ事象と実施処理のログとの紐付けのみに利用）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。

このような紐付けを行う場合には、偽のログID等を用いたなりすましやプライバシー保護の観点から適切な対策を講じること。

2．4　情報セキュリティに関する扱い

サーバーはクラウドサービスを利用し、仕様書 P22 に記載のとおり、厚生労働省が管理し、国内のリージョンとする。

実施処理のログには、当該情報だけで個人や端末、所在地を特定しうる情報は含まれていないが、仕様書 P22 に示す情報セキュリティに関する事項を遵守し、適切な安全管理措置を講ずる。

3．　その他

実施処理のログを蓄積・送信する機能の実装にあたっては、本仕様によるほか、仕様書及びこれに対する「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）にも準拠する。

また、本仕様に関して接触確認アプリに関する有識者検討会合から示されるプライバシー及びセキュリティ上の評価及び留意事項も遵守し、必要な内容に関しては明示的に利用者に伝わるような手段でコミュニケーションする。