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

目次

第１編　総論

１．目的

本アプリケーション（以下「本アプリ」と記述）は、スマートフォンの近接通信機構（Bluetooth）を利用し、人と人との接触したことを検知、記録する。新型コロナウイルス感染症の陽性診断が確定した者（以下「陽性者」と記述）であることが判明した場合に、その本人の同意のもとで、その陽性者と一定期間内に接触が確認された者に対し通知を行う。

※本仕様書では、「本人」とは本アプリが入った端末を操作する利用者を表す

利用者は、スマートフォンを活用して、①日常において自らの行動変容を意識できると共に、②互いに誰とどこで接触があったのかは分からないよう、プライバシー保護と本人同意を前提に、自らが陽性者と接触した情報について、通知を受けることが可能になる。

（利用者におけるメリット）

・利用について本人の同意のもと、自分が感染者と接触が確認された者かどうかを知ることができる

（公衆衛生当局、保健所等におけるメリット）

・個人が自らの行動変容を意識するとともに、接触確認後の適切な行動等を実施できることにより、感染拡大の防止につながる

２．前提条件

1)　本アプリの接触者の定義

本アプリにおける接触者の定義は、陽性者との接触に関する情報が利用者本人に通知される者として、陽性者との接触により感染のおそれがある期間に、陽性者との間で概ね 1m 以内の距離で継続して 15 分以上の近接状態が続いたもの（案）（以下「接触確認者」と記述）と定義する。また、プライバシーの保護と潜伏期間等を考慮して、過去に遡って利用者が自らの接触の情報を確認できるのは、14 日間までとする。（14 日経過後のデータは削除する）

2)　AppleとGoogleが提供するAPIの活用

本アプリは、以下の理由により、公衆衛生当局（厚生労働省）において、Apple と Google が共同で提供する Exposure Notification Framework （以下「AGF」と記述)を利用して構築し、サービスを提供する。

・AGF では、利用者間の接触に関する情報の管理や照合を個人の端末内で行う方式としており、陽性者と接触確認者のそれぞれの情報は、本人自らが申告しない限り、公衆衛生当局では把握できない仕組みとしている。アプリでは、利用者のプライバシーを保護するための厳格な対応が講じられている（仕様の詳細は後

述）

・多数のスマートフォン利用者がBluetoothにより効率的にサービスを利用するためには、iOSとAndroidの共通仕様で、OSで提供される機能が利用できることが合理的であり、国民への普及推進にも不可欠である。

※　BluetoothをOS上でコントロールすることで、他のアプリを利用中でも、バックグラウンドで利用可能となる。

・AppleとGoogleから共通仕様で提供されるAPIを利用してアプリを構築することで、効率的な開発が可能となる。

3)　個人情報保護

本アプリでは、個人のプライバシーに配慮し、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特定の個人が直接識別される可能性のある情報は取得しない。より詳細な個人情報保護及びプライバシー等の評価については、別途「接触確認アプリに関する有識者検討会合」における評価を踏まえ、実装を進める。

4)　AGFとの調整事項

本仕様では、現在、技術、規約面から実現可能か精査している部分がある。その部分は、文字色を変えて調整事項であることを明記する。

調整事項：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。

この仕様調整項目に関しては、調整項目の機能の目的を達成するために、仕様の画面やフローを変更する場合もある点に留意が必要である。

３．システムの基本的な考え方

前提条件を基に、システムの基本的な考え方を以下のように整理する。

- BluetoothをOS上でコントロールすることで、他のアプリ利用中でもバックグラウンドで利用可能となることから、AppleとGoogleから提供されるAPI（AGF）を利用して構築する。
- アプリ間で交換される識別子は周期的に変更されるものであり、個人や端末を特定できない。
- 接触の記録は全て端末で管理され、陽性者との接触の照合も各自の端末内で行う。
- 接触を検知するための端末間の通信や、個人を特定できない識別子の管理は、AppleとGoogleが提供する機能により実現する。
- 通知サーバーでは、本人同意のもと、陽性者の識別子のみが管理される。
- アプリと通知サーバーは、情報漏洩や侵入を防ぐために十分なセキュリティ上の措置を講じる。

４．概要

1)　関係者

主なユーザーは日本国内居住者・滞在者である。

主な関係者は以下のとおりである。

保健所	：新型コロナウイルス感染者等情報把握・管理支援システム（以下「感染者システム」と記述）を用いて陽性者等の情報を把握・管理し、健康観察等を行う。
厚生労働省	：アプリケーションの開発、運用・保守のオーナー。
受託者	：オーナーとの契約に基づきアプリケーションの開発、運用・保守を行う民間事業者。
利用者	：端末を保有し、本アプリの利用について同意し、インストールする。
陽性者	：PCR 検査で陽性診断が確定した者
接触確認者	：本アプリにより陽性者との接触が確認された者

日本語以外の言語を使う利用者がいることも想定している。

2)　本アプリの概要

本アプリは、スマートフォンの Bluetooth を利用し、人と人の接触を検知、記録し、自らの行動変容を確認できるようにする。陽性者であることが判明した場合、その本人の同意のもとで、その陽性者と一定期間内に接触が確認された者に対し通知を行う。以下の流れを本アプリで実現する。

接触確認アプリの仕組み

<通常時>

- 他者との接触についてアプリの端末に**相手の識別子（個人に紐付かない）**が記録される。
- 識別子の記録は、一定期間経過後に順次削除されていく。

接触の条件ををを満たしたら識別子を記録

<陽性確認時>

- 保健所で感染者システムに陽性者が登録される。
- 登録された陽性者は保健所の通知を受けて、自分が陽性者であることをアプリ上で入力。
- アプリユーザーに対して、陽性者との接触歴がある場合に**接触者アラートが通知され、これを確認**。（**接触した個人が特定できない形で通知**）
- 接触が確認された者には、メッセージにより、**適切な行動と帰国者・接触者相談センターへの相談方法等をガイダンス**。

具体的な流れ（現時点の想定）

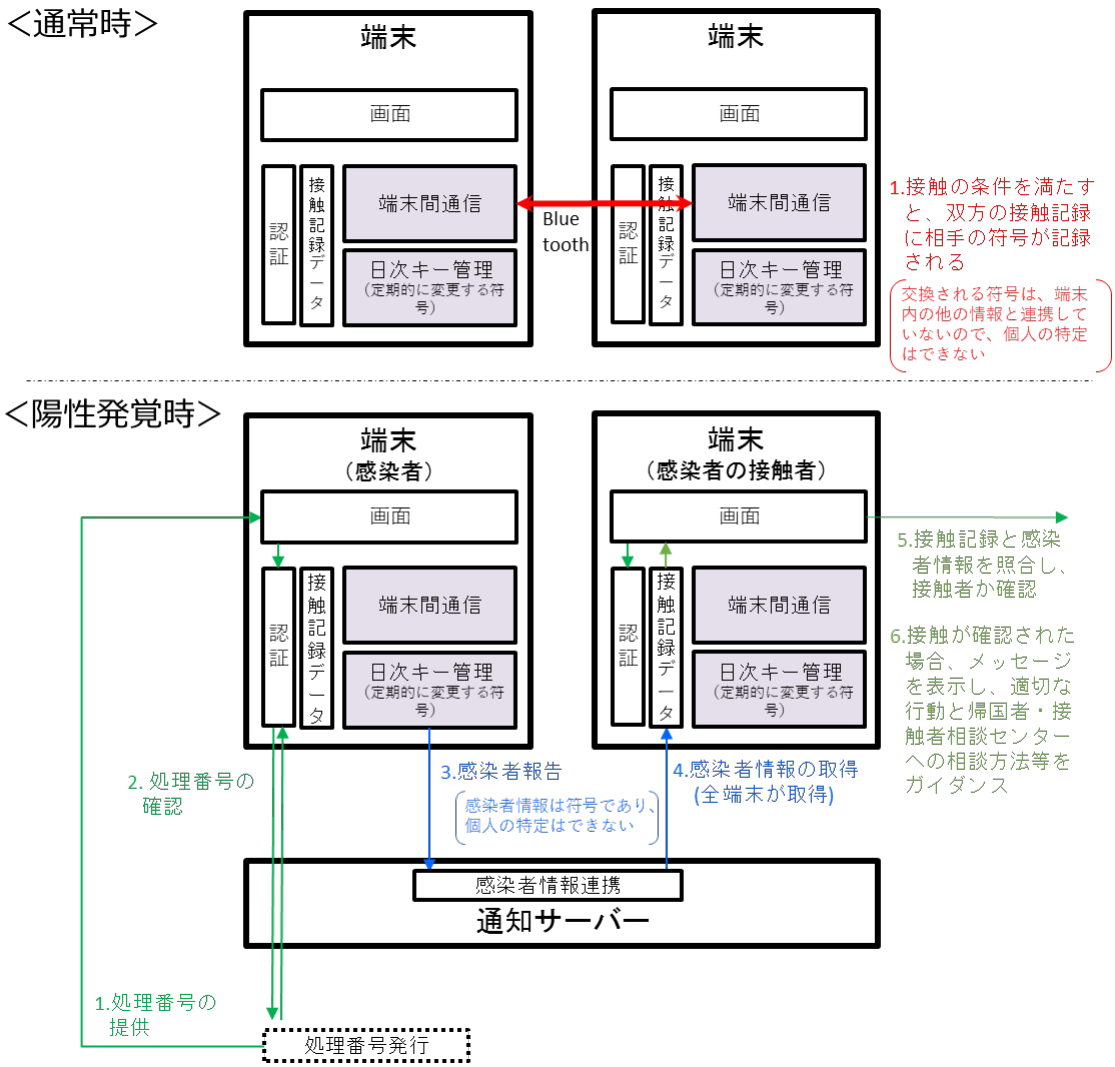
① 利用希望者が、本人同意の上で、本アプリをインストールする。
② 本アプリを導入した利用者は、接触時に接触相手の交換用キーを取得し、接触者データとして自端末内に記録する。（交換用キーは、端末内で一定期間毎に変更される匿名化されたキーである。アプリ利用者からは見えず、バックグランドで処理される）
③ 本アプリを導入した利用者は、日常的に本アプリの導入からの日数や日々の全接触回数（相手が陽性者か否かにかかわらず接触した回数）を確認ができ、行動変容のための情報として活用する。
④ 本アプリを導入した利用者が、感染者システムの登録を経て、新型コロナウイルス感染症の PCR 検査を受け、陽性診断の確定がされた場合、同システムからその陽性者に対し、アプリに登録する処理番号が通知される。
⑤ 陽性者は、本人同意の上で接触者に通知することを選択する場合、本アプリで処理番号を入力する。
⑥ 本アプリから通知サーバーを経て感染者システムに処理番号が送信され、感染者システムが正当な処理番号であるか照合したうえで、確認結果が通知サーバーを経て本アプリに戻される。
⑦ 陽性者本人の端末から、感染が疑われる期間の識別子（診断キー）が抽出され、通知サーバーに送信される。
⑧ 全ての端末において、陽性者の識別子（日次キー及び日次キーが発行されたタイミングに関する情報（上記「診断キー」））の情報を通知サーバーから取得し、自端末内にある接触に関する情報と照合して、過去 14 日間において陽性者と接触したかどうかを確認する。
⑨ 陽性者との接触が確認された場合には、その接触確認者に対し、適切な行動と帰国者・接触者相談センターへの相談方法等をメッセージによりガイダンスする。

新型コロナウイルス感染症対策の基本的対処方針（令和２年５月 21 日改正新型コロナウイルス感染症対策本部決定）では、「接触確認アプリについて、接触率の低減及び感染の拡大防止に寄与すること等の国民理解を得つつ、新型コロナウイルス感染者等情報把握・管理支援システム（ＨＥＲ-ＳＹＳ）及び保健所等と連携することにより、より効果的なクラスター対策につなげていく」としている。

本アプリと感染者システムとの連携について、アプリの運営者（厚生労働省）が陽性者と接触確認者との関係を把握することのないようプライバシーを確保しつつ、接触確認者本人が申告した場合に陽性者との関係が保健所で把握できるようにする方法として、①接触確認者本人からの要求を受けて、感染者システムにおいて陽性者に発行した処理番号と１対１の対応関係を持つ別の処

理番号を接触確認者に対し発行し、アプリで表示する、②接触確認者本人が感染者システムにアクセスし、接触確認者としての申告と本人の情報、当該別の処理番号の入力を行う、という方法が現時点で考えられるが、実装するためには、アプリにおける AGF の利用の条件、技術的な解決方法等について、引き続き調整・検討する必要がある。このため、本アプリと感染者システムとの連携については、本仕様書の範囲には入れずに、別途これらの利用の条件、技術的な解決方法等について調整・検討していく中で、仕様を整理することとする。

本アプリの機能構成と主な情報の流れ。



端末内の接触記録及び通知サーバー内の陽性者情報一覧は、暗号化したうえで格納され、一定期間（14 日を想定）終了後に廃棄する。

アプリ起動時の画面のイメージ

① 導入から、自らの陽性の確認も陽性者との接触も確認されていない場合
導入からの日数もしくは導入日と当日・前日等の全接触回数が表示される。

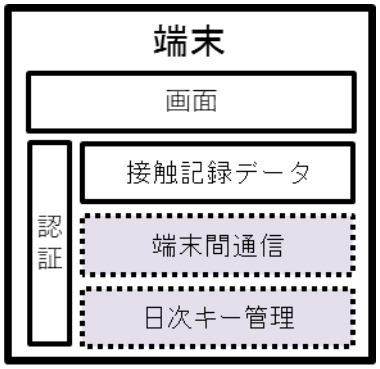
② 陽性診断が確定され、本人の同意のもとで通知した後
陽性者報告済みの画面が表示される。

③ 接触確認者の通知がされた後
初期画面に戻る方式、もしくは、初期画面に戻れない方式が考えられる。厚生労働省との協議の上で決定し実装する。

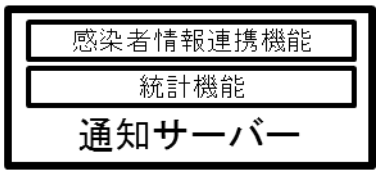
注：①は調整事項が実現可能な場合に実施

５．アーキテクチャと本仕様の範囲

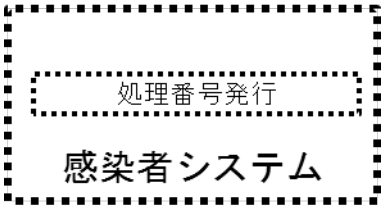
本アプリケーションは、以下のアーキテクチャで構成される。



端末は、業務層（画面）、データ層（接触記録データ）、通信層（端末間通信、日次キー管理）からなる。
通信層の機能は、AGF で実現される。



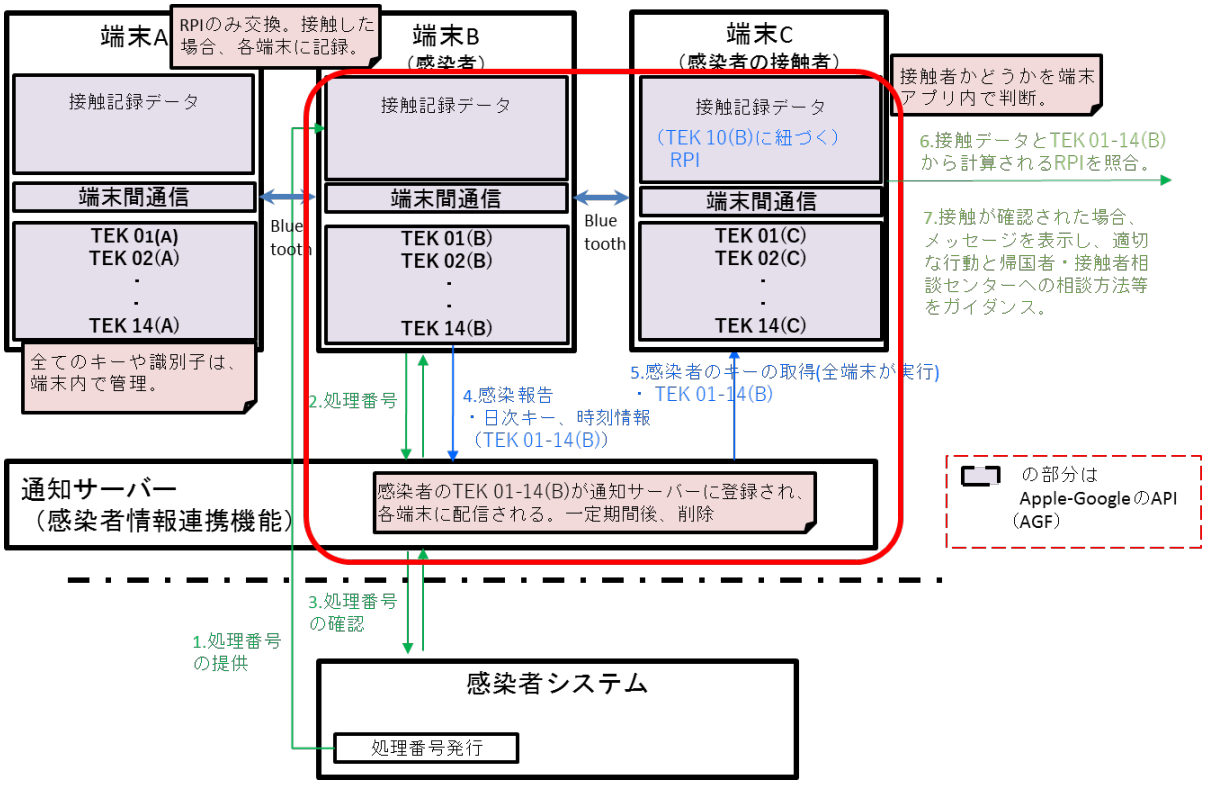
通知サーバーは、陽性者情報の通知機能、陽性者数・接触確認者数の統計等の機能のみ持つ。
クラウドサービスを使って整備される。



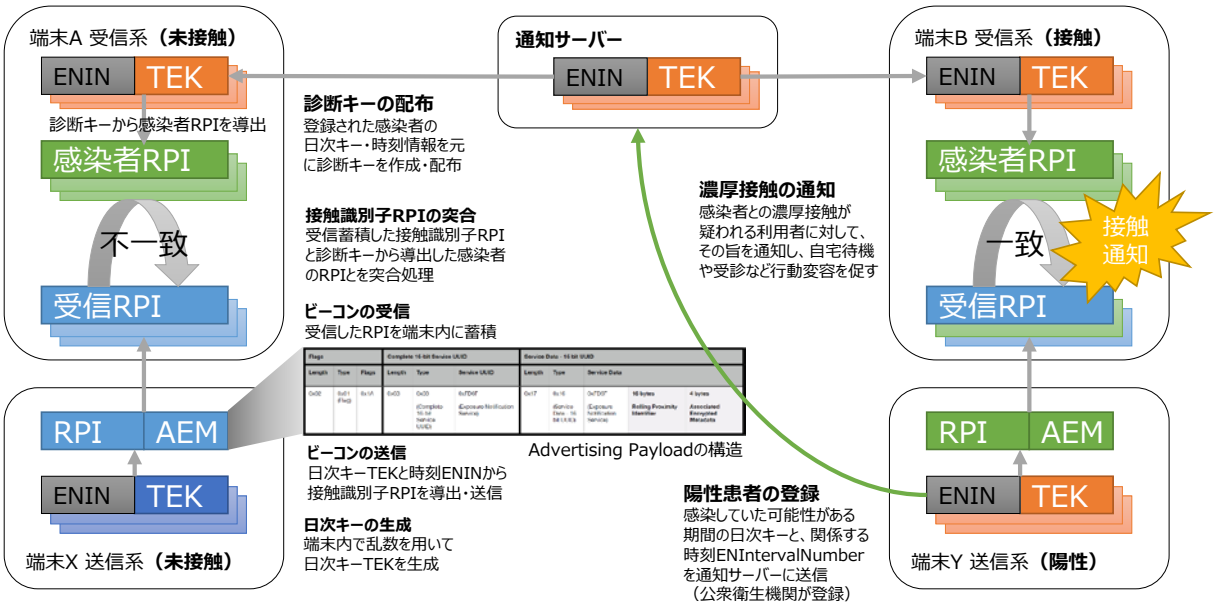
陽性者に処理番号を発行し、端末側アプリと連携させる機能は、感染者システムとして別システムとして構築され、アプリと連携を図る。（本仕様の範囲外）

６．アプリケーション詳細

本アプリは、AGF により OS の中で実施される事項と、アプリ部分で実現する部分により構成される。以下の赤線で囲われた部分が AGF により実行される。AGF で提供する機能については、当該機能を採用する。



キーや符号を使った接触確認者の照合プロセスは以下のとおりである。日次キーの TEK と時刻 ENIN から接触符号 RPI を生成しその RPI の照合で、接触確認者を発見する。このプロセスは OS の中で実行される。



７．本アプリで定義、使用する識別子

識別子名	説明	付与タイミング	削除タイミング
日次キー TEK（Temporary Exposure Key）	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。	アプリケーション導入時(端末)	14 日間の経過後(端末)
接触符号 RPI（Rolling Proximity Identifier）	TEK から RPI を作成。RPI から TEK は、計算できない。	10 分ごとに作成（端末）	14 日間の経過後(端末)
診断キー （Diagnosis Key）	陽性者の日次キー・時刻情報を基に作成	本アプリでの陽性者の登録時(端末)	14 日間の経過後(通知サーバー)
処理番号	感染者システムが陽性者に対し、アプリでの陽性者本人の確認をするために発行する番号	陽性者から感染者システムへの要求時（感染者システム）	端末の本人確認の終了時 （端末）

８．スケジュール

本アプリの開発スケジュールは、以下のとおりとする。調整事項については、開発スケジュールは未定である。

６月中（予定）　　リリース　　※調整事項を除いた機能のみ

９．体制

本アプリの開発及び運用は、厚生労働省がプロジェクトオーナーであり、受託者が実務を担う。

本アプリの仕様は、内閣官房新型コロナウイルス対策テックチームの下に設置した「接触確認アプリに関する有識者検討会合」で確認を行った上でテックチームとして策定する。また、運用開始後は、必要に応じて、厚生労働省が同会合に運用状況の報告を行い、同会合で評価・検証を実施する。

１０．用語集

用語（略称）	解説
接触	概ね 1m 以内の距離で継続して 15 分以上の近接状態が続いた状態
全接触回数	相手が陽性者か否かにかかわらず接触した回数
陽性者	PCR 検査で陽性診断が確定された者
接触確認者	接触確認の条件に該当した者
接触確認アプリ（本アプリ）	接触確認に必要な情報を収集し、陽性者の同意に基づき、接触確認者に対し接触確認された旨を通知するスマートフォン用アプリ
通知サーバー	端末の接触確認アプリと連携し、陽性者の日次キーを配信する受託者が再委託等するクラウドサービス事業者が保有するサーバー。
新型コロナウイルス感染者等把握・管理支援システム（仮称）（感染者システム）	厚生労働省が運用する新型コロナウイルスの感染者等の情報を管理するシステム。陽性者、接触確認者の健康観察等に用いる。
Apple-Google Exposure Notification Framework （AGF）	Apple-Google が、スマートフォンの OS レベルで提供する接触確認を通知するための機能
端末間通信機能	AGF の機能であり、Bluetooth で他端末との通信を行う機能
符号管理機能	AGF の機能であり、「日次キー」と日次キーから生成する「接触符号」を発行・管理する機能
接触記録データ	各端末に記録される、他者との接触情報。
処理番号	感染者システムが、陽性者からの要求を受けて１対１で発行する無意かつ一次的な番号。接触確認アプリへの陽性者の登録の真正性の確認に利用する。
接触符号	端末内で接触記録データとして記録され、陽性者との接触を照合するための符号

※AGF 内の識別子は別途定義する。

注：全接触回数は調整事項で実現可能な時の仕様

第２編　仕様（要件定義）

第１章　機能要件の定義

１．機能に関する事項

本アプリは、以下の機能で構成する。灰色は AGF で実現する機能である。

基本機能	本アプリのインストールや情報提供などを行う
認証機能	感染時に、感染者本人から入力かどうかを確認する
全接触回数 カウント機能	一日の相手が陽性者か否かにかかわらず接触した者をカウントして表示する。
日次キー管理機能	自分の端末で発行された日次キーを管理する
端末接続機能	Bluetooth を使って、端末間の接近距離や接触時間を測定する
接触記録データ管理	IT 管理機能と Bluetooth 接続機能を使い、接触した記録を管理する
接触確認判定	感染者状況を通知サーバーから取得し、接触しているかどうかの判定を行う
通知	接触が確認されたことが判明した人に、接触が確認されたことの通知を行う。

注：全接触回数カウント機能は調整事項が実現可能な時に実現

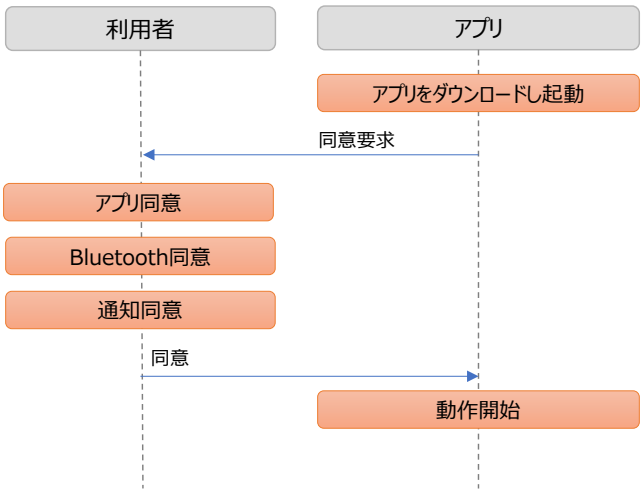
1)　基本機能（アプリのインストール）

a)　機能概要

本機能は、アプリのインストール及び利用にあたってのプロセスを実現する。本アプリや OS の提供する機能に対する本人同意のプロセスを含む。本人同意にあたっては、別途「接触確認アプリに関する有識者検討会合」で定めるプライバシーやセキュリティに関する留意事項を遵守する。

また、アプリに関する設定やアプリのバージョンなどの基本情報の提供などを行う。

b)　機能の基本フロー



アプリの利用に同意しなかった場合は、同意しない場合には利用できない

旨を表示し、次処理に移行しない。

c) 画面遷移

以下に画面遷移を示す。

1. ダウンロード完了画面
2. 利用規約等
3. Bluetooth 利用の案内
4. OS からの Bluetooth 利用の確認
5. OS からの通知機能利用の確認
6. 準備完了案内

2) 基本機能（基本設定等）

a) 機能概要

本機能は、アプリの基本設定情報と問い合わせなどの情報の提供などを行う。登録画面、通常運用画面左上のメニューから提供され、各 1 画面で構成される。

① 設定

機能の設定がある場合に設定の On/Off やパラメータの設定を行う。
同意撤回の意思の表明も本設定画面で行う。(同意を撤回した場合、本アプリのトップ画面では動作が停止していることを表示する。)

② バージョン表示

アプリケーションのバージョンを表示する。

③ 利用規約等

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のわかりやすい説明や、本アプリ導入時に同意を求める利用規約等を表示する。

④ お問い合わせ先

問い合わせの送信フォーム等、問い合わせ方法を表示する。

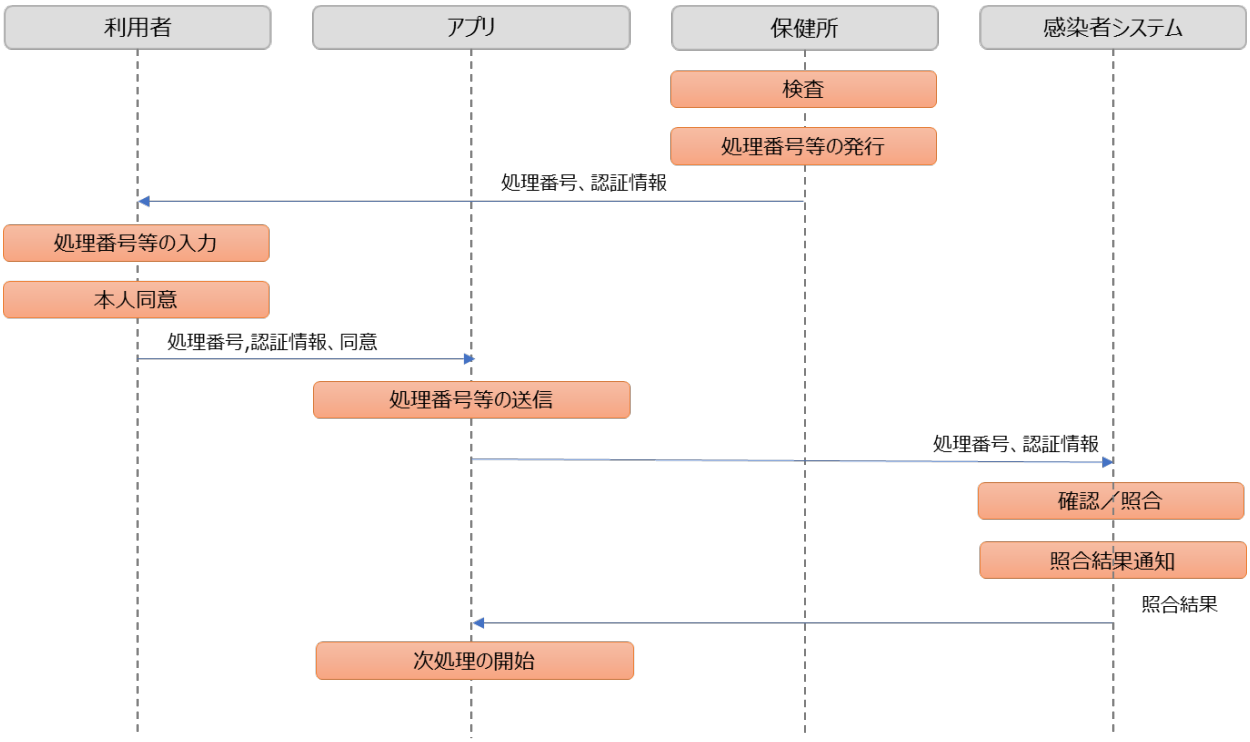
3) 認証

a) 機能概要

本アプリ利用者が新型コロナウイルス感染症の陽性診断の確定がされ、感染者システムに陽性者の登録がされ、その陽性者の要求を受けて、感染者システムから陽性者に、処理番号を通知する。陽性者はこの処理番号をアプリで入力

し、端末から通知サーバーを経由して感染者システムに処理番号の確認を行うことで、いたずらの陽性者の通知を防止する。

b) 機能の基本フロー



処理番号及び認証情報の照合結果が True であれば次処理に進む。照合結果が Fault であれば、エラーメッセージを画面に表示する。

また、本仕様の対象外の機能であるが、感染者システムでは、通知サーバーから処理番号をセキュアに受け付け、照合結果を通知サーバーに返戻する機構を設ける。

c) 画面遷移

以下に画面遷移を示す。

1. アプリを起動すると、導入してからの日数等と、行動変容を自ら確認するための当日・前日の接触状況を表示する。
2. 陽性者であると判明し、過去に接触した人にアプリから通知する場合、感染者システムから受け取った処理番号を入力する画面を表示する。
3. 送信確認画面を表示し、本人同意を行う。
4. 処理番号の認証に失敗した場合には、エラーメッセージを表示する。
   - 入力した番号が違います
   - センターとの通信ができません
5. 処理番号の認証に成功した場合は、バックエンド処理で通知サーバーに診

断キーが送信されるため、登録のお礼のメッセージを表示する。本画面はその後変更されず、アプリ起動時には、本画面が表示される。

※陽性者が陰性になり完治した後は、本アプリを利用する場合、一回削除し、再インストールする必要がある。

4) 全接触回数カウント機能

a) 機能概要

1 日単位での相手が陽性者か否かにかかわらず接触（1m 以内の距離で継続して 15 分以上の継続的な近接状態（案））した人数の総計を画面に表示する。あらかじめ設定した時間に、スマートフォンの通知機能で、当日及び前日の全接触回数の通知を行う。この通知は、設定画面により、通知の有無及び通知時間を設定できる。

過去 14 日間の全接触回数の状況を把握することも可能とする。

注：調整事項が実現可能な時に実現

5) 日次キー管理、接触記録データ管理、接触確認判定

a) 機能概要

接触管理を行うための日次キー、接触符号の発行・管理と、Bluetooth を使った接触確認管理を行う。本機能は、AGF の API で提供される。

詳細情報

１．接触通知アプリ関連のポータル

https://www.google.com/covid19/exposurenotifications/

https://www.apple.com/covid19/contacttracing/

２．開発者に向けたコードの公開

https://github.com/google/exposure-notifications-android

https://developer.apple.com/documentation/exposurenotification

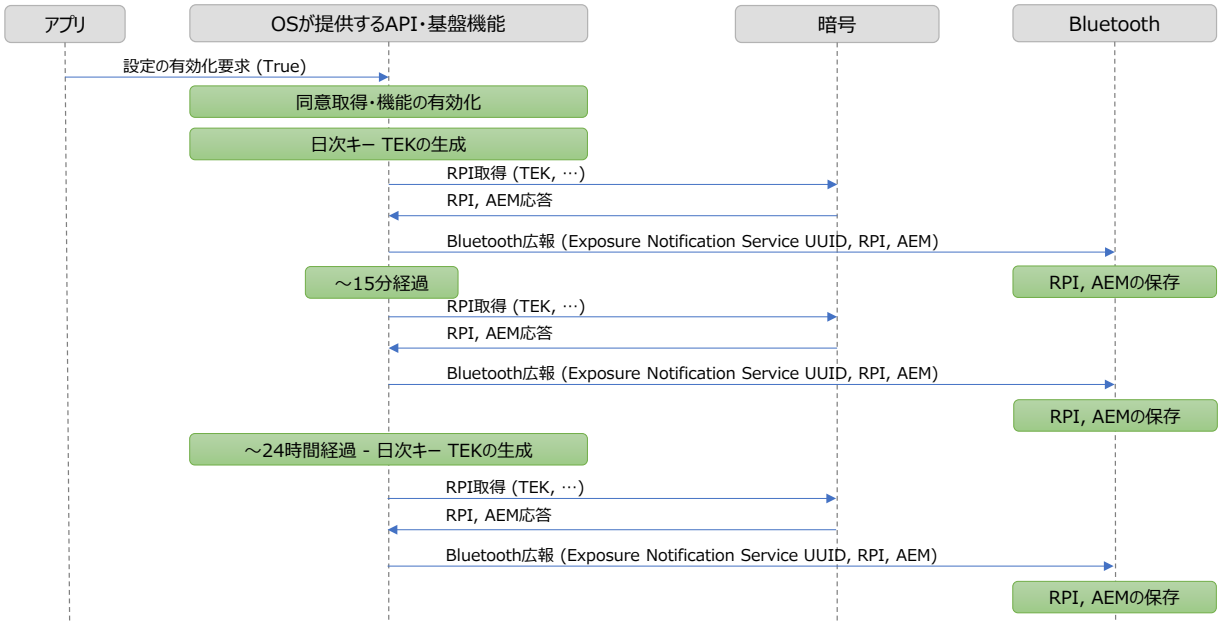
https://developer.apple.com/documentation/exposurenotification/building_an_app_to_notify_users_of_covid-19_exposure

３．ユーザーインターフェースのサンプル画像

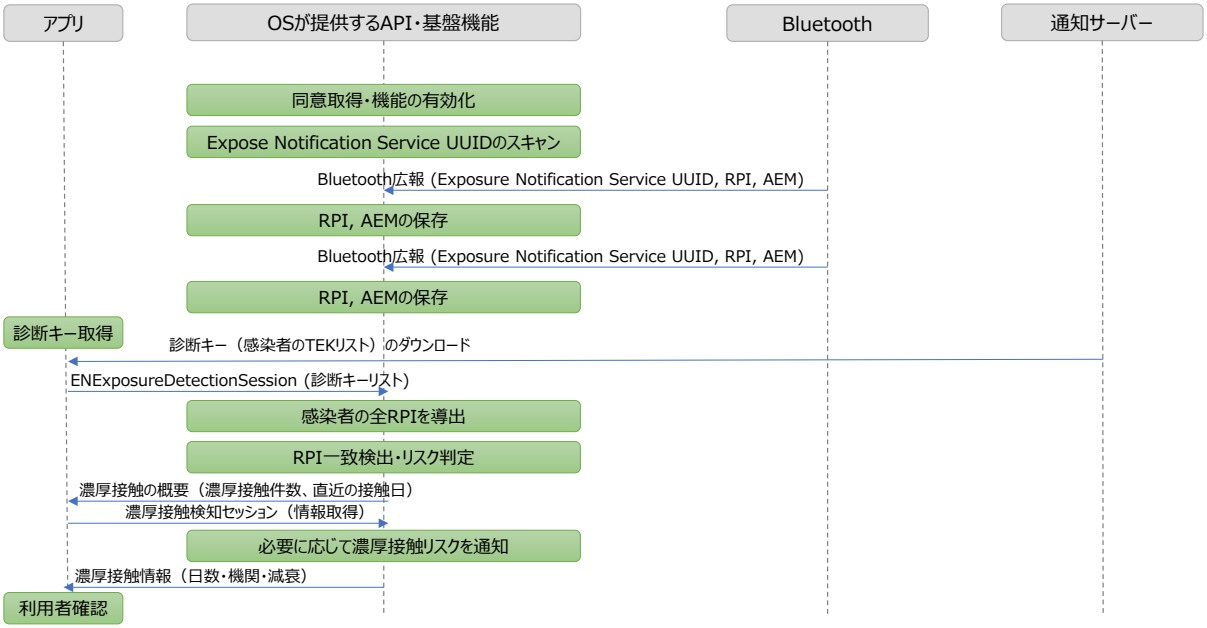
https://apple.ent.box.com/s/sv3cop1slwt57p2pkl11a4p6f44hsicl

b)　機能の基本フロー

（日次キーと接触識別子の作成、変更、送信）



（日次キーと接触符号の受信、接触判断）



Exposure Notification Bluetooth Specification Preliminary – Subject to Modification and Extension April 2020 v1.2 Information を元に作成

c)　OS で行う機能と本アプリで行う機能の分担

本機能の大部分は、OS により行われる。

本アプリが活用できるデータは、OS から提供される API を通じてのみである。

OS で行われる機能

・日時キー（TEK）の発行、時刻（ENIN）の発行
・接触符号（RPI）の管理
・接触符号（RPI）の照合

アプリで行われる機能

・診断キーの API からの取得と通知サーバーへの送信
・接触確認情報の取得

通知サーバーで行われる機能

・陽性者から感染のおそれがある時刻（ENIN）と日次キー（TEK）により生成された診断キーついて陽性者の端末から配信を受け、診断キーを各端末に配信

6) 接触確認結果の受領と接触確認者へのの案内

a) 機能概要

端末で RPI の一致が確認されると API で接触確認の検知が報告される。報告を受け、アプリの通知機能で、画面上に接触確認アプリの画面を確認するように案内される。(他のアプリケーション利用時にも表示される)

接触確認アプリの画面では、利用者に陽性者との接触が確認されたことを通知する。

b) 機能の基本フロー

※アプリから接触確認フラグの送信と接触確認者数カウントの機能は、実装可能な場合実施。

c） 画面遷移

以下に画面遷移を示す。

1. 接触確認が判明した場合には、スマートフォンの通知機能を使用して画面に接触確認通知が表示される。
2. 本アプリを起動すると、接触確認の通知が表示。適切な行動と帰国者・接触者相談センターへの相談方法等をメッセージによりガイダンスする。

通知メッセージの条件

・通知受領者に心理的な負担を与えないように配慮する
・通知結果により、陽性者と接触確認者が特定されないように、適切な表示を行う。

7） 通知サーバー統計機能

a） 機能概要

陽性者数の報告通知数と接触確認者の報告通知数等の AGF の API から取得できるデータを 00:00-2400 までの 1 日単位で集計する。

b） 機能の基本フロー

「6） 接触確認結果の受領と接触確認者への案内」の接触確認者フラグをカウントしたもの等、AGF の API から取得できるデータを集計する。

c） 画面遷移

画面の指定はない。コンソール表示も可能である。

8） その他機能

セキュリティ確保の観点から以下の機能を実装する。

・ユーザーからデータ提供を受ける I/F の保護機構
・ユーザーの同意撤回に基づくデータ削除機構
・通知サーバーと感染者システムとの通信内容を保護するための認証機構

ユーザーが本アプリ使用開始後に同意を撤回した場合の機能を実装する。

・同意の撤回時点で接触確認機能を停止し、機能停止の画面を表示する。
・同意の撤回時点までに、通知サーバーに送信されたデータは削除されない。

2．ファイルに関する事項

1） 端末

a) **接触記録データ**

AGF の機能として提供される。

内部データは API が提供しているデータのみ取得できる。

b) **日次キー**

AGF の機能として提供される。

内部データは参照できない。

2) **通知サーバー**

a) **診断キー**

AGF の機能として提供される。

診断キーを保存する。本アプリを導入した全端末から参照を可能とする。

b) **統計データ（陽性者数、接触確認者数）**

日付、通知サーバーに報告された陽性者数、接触確認者数を記録する。

本サービス開始時から終了時まで継続的に記録する。

３．外部インタフェースに関する事項

整備する情報システムと他の情報システムとの連携（外部インタフェース）について、外部インタフェース一覧、相手先の情報システム、送受信データ、送受信タイミング、送受信の条件の基本的な考え方等を記載する。

外部インタフェースは、なりすまし等を防止する適切な対策を実施すること。

ア　感染者システムとのインタフェース

a) **陽性通知**

感染者システムから通知された処理番号を、アプリの陽性情報入力画面から入力する。

	発出者	受信者	方法	タイミング	暗号化
処理番号	感染者システム	陽性者	メール（陽性者が感染者システムにメールアドレスを登録）	陽性確定後に本人が通知のための処理番号の発行を要求した時	なし
処理番号	アプリ（通知サーバー）	感染者システム	API	アプリ利用者の入力時	なし
確認フラグ	感染者システム	アプリ（通知サーバー）	API	処理番号到達後、確認終了時	なし

機能要件の機能の基本フロー参照

b) 陽性者の日次キー送出時

陽性者の端末から通知サーバーに日次キー（TEK）と時刻（ENIN）による診断キーが送信される。

c) 全端末からの陽性者の日次キー等の取得

通知サーバーに保存されている日次キー（TEK）と時刻（ENIN）による診断キーを各端末が取得する。

CDN（Contents Delivery Network）の活用等、アクセス集中を防止する手段を提供する。

第２章　非機能要件の定義

１．ユーザビリティ及びアクセシビリティに関する事項

- 本アプリは、操作する部分が少ないが、プライバシーなどの同意事項が多いのが特徴である。
- アプリケーションは、誰でも直感的に操作できるよう、構築する。
- 利用者が分かりやすい文章や図で説明するとともに、誤操作時に適切なガイダンスが出せる設計に配慮する。また、本アプリを初めて起動する際に、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、視覚的に理解しやすい方法で概要を表示すること。
- スマートフォンが持つ基本的操作性に可能な限り準拠する
- 日本語に加え、英語の画面を整備し、iOS 又は Android 端末の OS の言語切替機能で選択可能にする。
- 未成年者及び成年被後見人など自ら登録の判断を行うことが困難なユーザーのための代理登録を可能にする。

２．システム方式に関する事項

- システムは、クラウドサービスを活用する。
- 端末は、iPhone または Android 端末を対象とする。
- OS は、Exposure Notification API に対応した iOS および Android（本仕様書の執筆時点では iOS 13.5 以上および Android 6 以上）。

３．規模に関する事項

- スマートフォンの国民の個人保有率が 64.7%（令和元年版情報通信白書）であるので、最大で国民の６割以上が導入することを目指す想定で基盤等の拡張性を確保する。
- 端末は、最大で過去 14 日分の接触に関するデータを蓄積する。
- サーバーには、陽性者の最大 14 日分の日次キーが端末から提供される。
- １週間単位での新規陽性者数が最大 4200 人とする。
  ※令和２年４月 6 日週（4/6～12）の陽性者数約 3500 人×1.2（システム上の安全率）＝約 4200 人

４．性能に関する事項

- 端末の応答は 3 秒以内とする。
- 全ての端末で陽性者の日次キー等の取得をする時には、コンテンツデリバリーネットワーク等を活用し、通信回線の輻輳を避けるとともに、効率的にすべての端末がデータを取得できるようにする。

・ 接触の測定にはBluetoothを活用するが、電波干渉や障害物により正確に測定できないことがあるのでパラメータ設定に留意すること。

５．信頼性・可用性に関する事項

・ 端末での稼働率は98%以上とし、サーバーの稼働率は95%以上とする。

６．拡張性に関する事項

・ 処理能力の拡張が容易にできる設計にすること。
・ 機能ごとにモジュールで設計し、機能拡張時の影響範囲を最小限にとどめる設計にする。
・ 接触カウント機能、接触確認時の機能で機能拡張が検討されている。機能拡張に配慮した設計にし、厚生労働省と緊密に連携をとるようにする。
・ 将来、海外でAGF対応のアプリが提供されたときに相互運用性の検討が行われる可能性があることに留意すること。

７．上位互換性に関する事項

・ OSが提供するAGFの機能改修に柔軟に対応できるように、APIによる接続を原則とする。

８．中立性に関する事項

・ いわゆるベンダーロックインの解消等による調達コストの削減、透明性向上等を図るため、市場において容易に取得できるオープンな標準的技術又は製品を用い、特定のハードウェア又はソフトウェアに依存しない仕様とする。
・ 本アプリへの信頼を高めるため、開発ドキュメント等の透明性の確保に配慮する。

９．継続性に関する事項

・ 本システムは、一時的な停止により社会的に大きな社会的混乱を引き起こすものではない。障害時には72時間以内の復旧を目標とする。大規模災害におけるシステム停止時には、システム運用者と相談の上、1週間以内の復旧を行う。
・ 緊急性の高い開発であるから、端末の機種変更時（故障や紛失を含む）のデータの引継ぎは考慮しないこととする

１０．個人情報保護に関すること

・ AGFの示すプライバシー保護の方針を遵守する。また、別途「接触確認アプリに関する有識者検討会合」で定める個人情報保護に関する留意事項を遵守する。

１１．情報セキュリティに関する事項

- 「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）に準拠してセキュリティ対策を進める。また、別途「接触確認アプリに関する有識者検討会合」で定める情報セキュリティに関する留意事項を遵守する。
- アプリのセキュリティ機能は、スマホの OS によって標準機能として提供される機能を最大限活用する。
- システム導入時には脆弱性検査を実施する。

１２．情報システム稼働環境に関する事項

- サービスは、クラウドサービスを使って行う。個人を特定する情報を持たないが、厚生労働省が通知サーバーを管理し、公衆衛生に用いられる情報であるので、国内のリージョンとする。

１３．テストに関する事項

- 短時間開発であることから、開発者のテストに加え、ベータ版でのテストも検討する。（ベータ版：検証であることの同意を得た利用者に試行検証してもらうための最終試行版アプリ）

１４．運用に関する事項

- 通知サーバーの運用は、自動化することを可能とする。
- 異常発生時にはオペレータにメッセージが届くなどの工夫を行う。
- メッセージには、ユーザーからの問い合わせのメッセージも含むこととする。
- 問い合わせに対応するため、FAQ を整備する等の利用者への支援体制を用意する。
- アプリ利用規約、同意事項等の内容については、別途「接触確認アプリに関する有識者検討会合」で定める留意事項を遵守し、必要なものに関しては明示的にユーザーに伝わるような手段でコミュニケーションする

１５．保守に関する事項

サーバーに機能追加するなど保守を行う場合には、信頼性、継続性に配慮するとともに、サーバーの停止時間ができるだけ短期になるよう配慮する。ただし、緊急を要するメンテナンスの場合はその限りではない。

１６．関連ドキュメントの整備

本アプリの提供にあたり、以下のドキュメントを整備すること。

・本アプリケーションの利用規約等

　－　本アプリ導入時や感染者登録時の本人同意確認等の文面を含む

　－　作成に当たっては、法律専門家による確認を行うこと

- 利用規約や本人同意内容、同意撤回状況は、本アプリ内から容易に確認できるようにする

・設計書及び関連ドキュメント（ソースコード、通知サーバーの運用マニュアル含む）
・簡易説明および FAQ