

接触確認アプリ及び関連システム仕様書（案）〔概要〕

2020年5月17日

新型コロナウイルス感染症対策テックチーム

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。

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確認できると共に、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。

接触が確認された旨の通知を受けた者自らが、国の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）（以下「感染者システム」と記述）に登録することで、健康観察への円滑な移行、自らが接触通知を受けた際の行動変容、保健所の負荷の軽減等も期待できる。

なお、陽性者の状況の把握や濃厚接触に関する調査等については、別途厚生労働省で構築中の感染者システムで行われる。

（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、自分が陽性者と接触が確認された者かどうかを知ることができる
- ・接触が確認された旨の通知を受けた者は、自らの申告による感染者システムへの登録と健康観察等への円滑な移行ができる

（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確認するとともに、接触確認後の行動変容を実施できることにより、感染拡大の防止につながる
- ・利用者自らの申告により、濃厚接触者等の把握に関わる業務の軽減が期待できる

2. 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、個人に紐づか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、個人の特定はできない。
- 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。

(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。

調整事項1：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機能

調整事項2：保健所による健康観察等に円滑につながる補助をする機能

3. 概要

本アプリは、スマートフォンのBluetoothを利用し、人と人との接触したことを検知、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（検討中・未定稿）

<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。



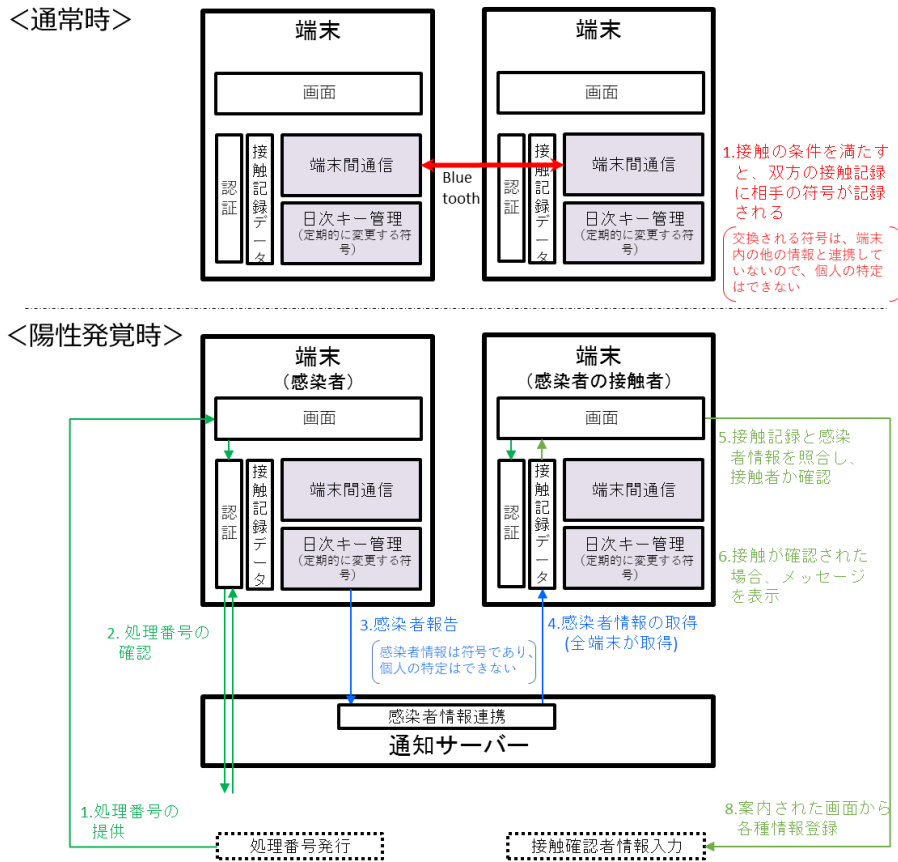
接触の具体的な定義については、技術的なAPIを検証の上整理

<陽性確認時>

- 保健所で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）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は陽性者と接触したことを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）上で**登録**。



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。

目次案

第1編 総論

1. 目的
2. 前提条件
3. システムの基本的な考え方
4. 概要
5. アーキテクチャと本仕様の範囲
6. アプリケーション詳細
7. 本アプリで定義、使用する識別子
8. スケジュール
9. 体制
10. 用語集

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
2. ファイルに関する事項
3. 外部インタフェースに関する事項

第2章 非機能要件の定義 22

1. ユーザビリティ及びアクセシビリティに関する事項
2. システム方式に関する事項
3. 規模に関する事項
4. 性能に関する事項
5. 信頼性に関する事項
6. 拡張性に関する事項
7. 上位互換性に関する事項
8. 中立性に関する事項
9. 継続性に関する事項
10. 個人情報保護に関すること
11. 情報セキュリティに関する事項
12. 情報システム稼働環境に関する事項
13. テストに関する事項
14. 運用に関する事項
15. 保守に関する事項
16. 関連ドキュメントの整備