新型コロナウイルス接触確認機能付き

GPSトラッカーシステム仕様書

　 Ver 1.0 2020.12.10

Ver 1.1 2020.12.16

Ver 1.2 2020.12.23

Ver 1.3 2020.12.25

Ver 1.3.1 2021.01.11

株式会社アイルソフト

市川満之

目次

[1. 目的 3](#_Toc61300667)

[2. 前提条件 3](#_Toc61300668)

[3. 機能概要 4](#_Toc61300669)

[3.1. 接触確認機能 4](#_Toc61300670)

[3.2. GPSトラッカー機能 8](#_Toc61300671)

[4. 基本シーケンス 12](#_Toc61300672)

[4.1. 基本機能 12](#_Toc61300673)

[4.2. 接触確認機能 13](#_Toc61300674)

[4.3. GPSトラッカー機能 15](#_Toc61300675)

# 目的

本システムは、２つの目的を持つ。

１つ目はスマートフォンを持っておらず、新型コロナウイルス接触確認アプリ（COCOA)（以降COCOAと記述）を使えない子供やお年寄りに対して、本システムのデバイス（以降「デバイス」と記述）がBLEを利用したCOCOAと同じ機能を持ち、人と人との接触したことを検知、記録する。記録を管理者のスマートフォンの本システムのアプリケーション（以降「アプリ」と記述）に移し、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およびその陽性者と濃厚接触があった場合に、その管理者および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。（以降接触確認機能と記述）

２つ目はGPSトラッカーとして本デバイスから本アプリに対してLTE-Mを利用してMQTT通信で緯度経度を通知し、子供やお年寄りがどこにいるか分かるようにするためである。また、緊急時にボタンを押下することで本デバイスから近辺にいる不特定多数の本アプリに対してアラートによる緊急通知を行う。（以降GPSトラッカー機能と記述）

# 前提条件

接触確認機能は、接触確認者としての定義および接触の情報を確認できるのは14日間までとし、COCOAに準ずる。また、個人情報保護の観点からGPSトラッカー機能の名前、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関係性を持たない。

GPSトラッカー機能は、互助の考えから身元保証と管理する意味で名前、電話番号、メールアドレス、パスワードを入力する。デバイスには緊急通知のために、性別、生年月日を記録する。また、デバイスを使用するためには、認証コードによる有効期限をアプリからBLEを利用して保存する必要がある。

# 機能概要

## 接触確認機能

* デバイス（写真は試作品）

他者との接触について、デバイスに1メートル以内で１５分以上接触した相手のスマートフォンのCOCOAの識別子が記録される。同様にCOCOAにもデバイスの識別子が記録される。また、デバイス同士でもデバイスの識別子が記録される。

デバイスに記録された識別子は、管理者のアプリにBLEに転送する。転送された識別子から濃厚接触したかを確認する。確認した内容は学校もしくは会社にスマホのインターネットを利用して暗号化したMQTT通信で配信することができる。デバイスおよび管理者のアプリの識別子の記録は、14日間経過後に削除される。

BLE（ペアリングおよびボンディング）

記録された識別子を転送

新型コロナウイルス接触確認アプリ 厚生労働省Bluetoothのアイコン, ブルートゥースのロゴ, ブルートゥース, ロゴ, アイコンを, 青Bluetoothのアイコン, ブルートゥースのロゴ, ブルートゥース, ロゴ, アイコンを, 青Bluetoothのアイコン, ブルートゥースのロゴ, ブルートゥース, ロゴ, アイコンを, 青Bluetoothのアイコン, ブルートゥースのロゴ, ブルートゥース, ロゴ, アイコンを, 青

濃厚接触を確認

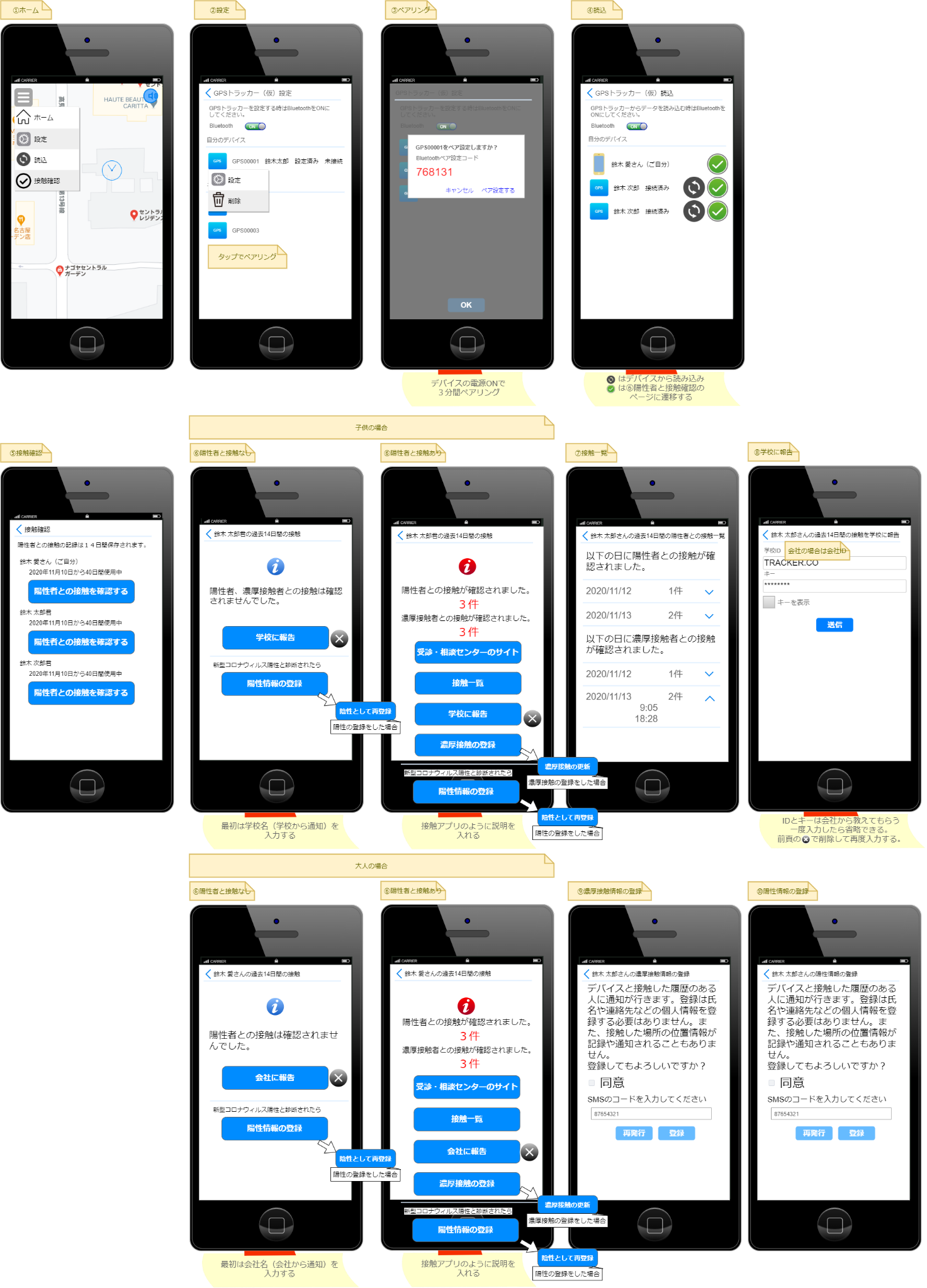
BLEで識別子を送信、記録

アプリおよびCOCOAと通信する

BLEで識別子を送信、記録

通知サーバ

* 管理者のアプリ画面　marmo(マーモ)　 　　（仮アイコン）



* 濃厚接触情報、陽性情報はローカルに保存する。
* デバイスとのペアリング

セントラル：スマートフォン、ペリフェラル：デバイス

表示は「marmo」とし、IDはスマートフォンから設定できるものとし、設定されたIDに５桁のランダムで生成された数字を付与する。

最初と２回目の接続時はデバイスとペアリングする。

３回目に同じデバイスと接続する時は交換した鍵を保存しておくボンディングを使用する。

　　詳細は新型コロナウイルス接触確認機能付きGPSトラッカー\_通信仕様書を参照

* GPSトラッカーの読み込み処理

BLEのGATT通信でTEK、ENIN とRPI、AEMを読み込む(read)

詳細は新型コロナウイルス接触確認機能付きGPSトラッカー\_通信仕様書を参照

* 濃厚接触者の判定

サーバからWeb APIを使用して情報の送受信を行う。

詳細は新型コロナウイルス接触確認機能付きGPSトラッカー\_通信仕様書を参照

* + - アプリを起動していなくても定期的に判定し、アプリのアイコンに通知バッジ（濃厚接触者の合計数）を表示する。
* COCOAからの情報の移行は検討中
* 学校のアプリ画面

管理者のスマートフォンから配信された接触情報を表示する。



※内容はローカルに保存する。学校IDとキーを登録時にブローカにユーザ登録する。

詳細は新型コロナウイルス接触確認機能付きGPSトラッカー\_通信仕様書を参照

## GPSトラッカー機能

* デバイス（写真は試作品）

電源を入れてから3分間、デバイスとアプリをペアリングできる。  
ペアリング後、アプリで名前、性別、生年月日、キー、位置の送信間隔、有効期限、緊急ボタン押下時間を入力し、BLEを利用してデバイスに保存する。デバイスからの情報はデバイス番号と共に緯度経度、温度、湿度、歩数をLTE-Mを利用して暗号化したMQTT通信でアプリに配信する。中央のボタンを指定時間押下すると、LTE-Mから暗号化しないMQTT通信で近辺のアプリに緊急通知を行い、近辺の登録している方に助けてもらう。



LTE-M(MQTT通信)

緯度経度、温度、湿度、歩数

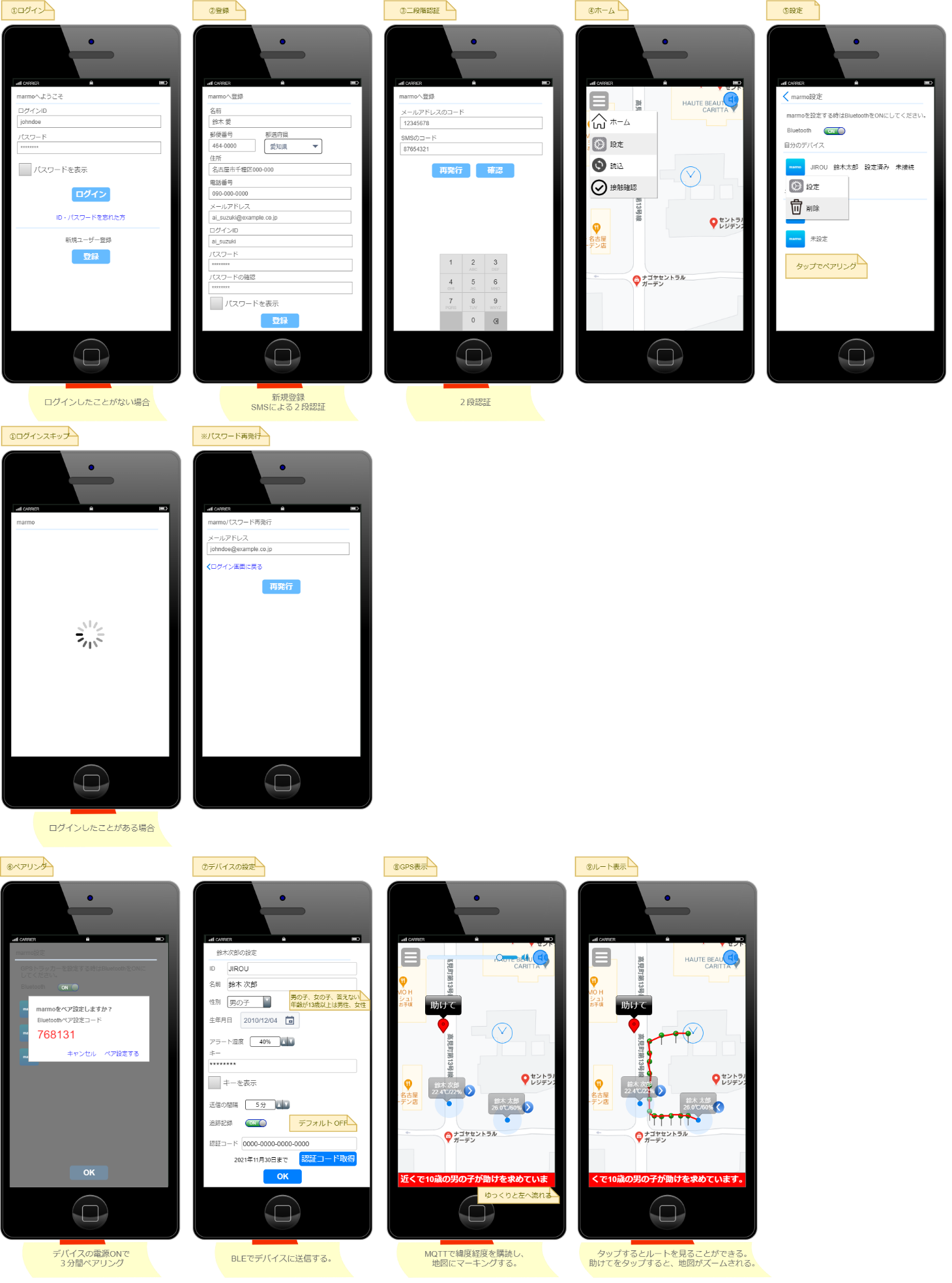


LTE-M(MQTT通信)

緊急通知、緯度経度、特徴



* 管理者のアプリ画面



※ログイン情報はサーバ上のプリザンターに保存／読込する。

　スマートフォンは登録時にブローカにユーザ登録する。

※緊急通知が複数存在する場合は、複数の内容をロールして表示する。

　ルートの２４時間経過したものは削除する。

* GPSトラッカーの設定処理

ペアリングした後にBLEのGATT通信で現在の設定値を読み込み(read)、設定ボタンで設定(write)する。

詳細は新型コロナウイルス接触確認機能付きGPSトラッカー\_通信仕様書を参照

* MQTTによるデバイス暗号配信、デバイス情報配信

デバイスから暗号化して配信（パブリッシュ）する。購読（サブスクライブ）する管理者アプリ側は複合化してデータを抽出する。

詳細は新型コロナウイルス接触確認機能付きGPSトラッカー\_通信仕様書を参照

* MQTTによるデバイスからの緊急通知配信

デバイスで３秒間ボタンを押した場合、近辺の管理者の方に購読してもらうために平文で緯度経度、性別、年齢を配信する。

詳細は新型コロナウイルス接触確認機能付きGPSトラッカー\_通信仕様書を参照

緊急通知中はデバイス、スマートフォン共にブザーを鳴らす。

スマートフォンに関してはブザーと共にプッシュ通知を行い、プッシュ通知の内容をタップすると、アプリのホームが表示される。

【プッシュ通知の例】

アプリ名：marmo

Title：近辺でSOSあり

Body：近くで10歳の男の子が助けを求めています。

※　同じMQTTの配信がなくなったら、そのプッシュ通知を削除する。

17歳まで男の子、女の子で、18歳から男性、女性とする。

性別不明な方は男の子、男性の性別は入れない。

性別不明の場合、

「近くで10歳の子が助けを求めています」

「近くで70歳の方が助けを求めています」

18歳以上の場合、

「近くで70歳の女性が助けを求めています」

* MQTTによる学校への濃厚接触数の配信

管理者アプリから濃厚接触数を暗号化して配信（パブリッシュ）する。購読（サブスクライブ）する学校アプリ側は複合化してデータを抽出する。

詳細は新型コロナウイルス接触確認機能付きGPSトラッカー\_通信仕様書を参照

# 基本シーケンス

基本のシーケンスを記述する。

## 基本機能

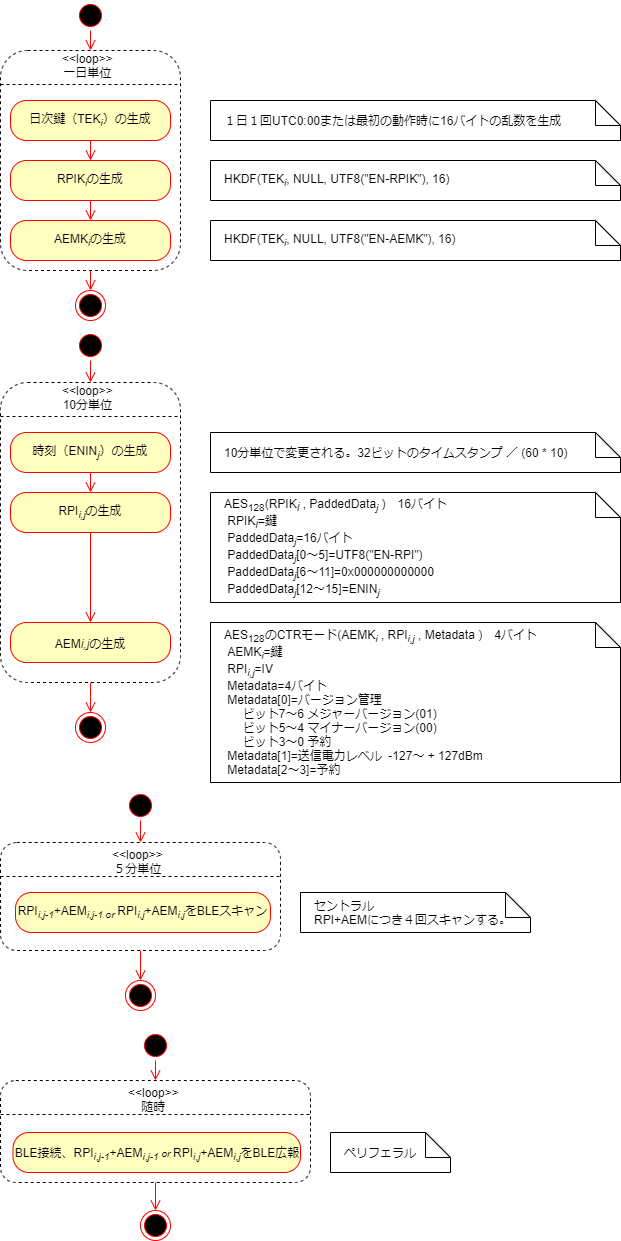
アプリおよびデバイスを動作するにあたっての基本機能のプロセスの流れを示す。



デバイスはアプリと接続し、有効期限を含んだ設定を書き込まれ、有効であれば接触確認機能およびGPSトラッカー機能を動作させる。３分経っても接続しなかった場合、有効期限が有効でない場合は、終了する。

## 接触確認機能

接触確認機能が起動してからのプロセスの流れを示す。



タイムスタンプはUTCを使用

セキュアな乱数を使用

３回以上受信した場合、RPIとAEMを保存する。

スマートフォン、デバイス共常時動作するようにする。スマートフォンは定期的に濃厚接触者の判定も行い、通知バッジ表示を行う。

生成したTEK、ENIN、RPI、AEM、受信したRPI、AEMを14日間保存する。14日間を超えた場合、削除する。

15分以上接触しているかはRPI+AEM※が３回以上一致していることと信号の強さ(RSSI>=-55)で判定する。

* + - RPI+AEMは10分間隔で変更されるが、BLEの送受信は平均１５分となっているため、内部でRPI+AEMが変更されても５分間隔で同じデバイスでスキャンする。

## GPSトラッカー機能

GPSトラッカーが動作開始してからのプロセスの流れを示す。

