# 【調査】感染症の接触段階における有効な追跡技術

山下 尚彦

2020 年 4 月 16 日

## 1　はじめに

2020 年、特に 3 月以降から新型コロナウイルス (COVID-19) の脅威が世界中に広まり [1], その特徴として潜伏期間が長いことが挙げられる．そのため, その間に接触した人が感染する可能性があり, 今日のような COVID-19 感染者が爆発的に増えていると考えられる．そこで, 欧州の 8 大学を中心としたアカデミアグループが進めるプロジェクト DP-3T[2] では, スマートフォンなどのデバイスを利用して感染者と接触した可能性のある人を追跡し, 接触者に対する通知プロセスを迅速・簡略化することで新型コロナウイルスの拡散を遅らせる技術を提案した．また, CoEpi, CovidWatch, Zcash Foundation の 3 グループが実装した TCN Protocol[3] や MIT が提案した PACT Protocol[4] のいずれも Bluetooth の機能を利用して感染者との接触した人の特定を行っている．これらの技術ではデバイスやユーザ, 位置などのセンシティブな情報は利用しないため, プライバシーの問題を解決する事ができる．次の章から TCN Protocol を例にその仕組みを説明する．

## 2　概要

TCN Protocol は Temporary Contact Numbers の頭文字から由来しており, 一時的な疑似乱数値を用いることでプライバシーに配慮して接触者を追跡するプロトコルである．

### 2.1　プライバシーとセキュリティの保証

感染者を追跡する情報を扱ううえでプライバシーなどの課題が挙げられる．TCN Protocol のプロジェクトでは, 追跡技術のプロトコルにおけるプライバシーとセキュリティを保証するには以下の性質が望ましいとしている．

- **サーバに対するプライバシー**
  サーバはユーザの位置情報などの個人情報を取得しない
- **ソース情報の完全性**
  ユーザは接触していないユーザにレポートの送信や, 他のユーザの代わりにレポートを送信しない
- **ブロードキャストにおける完全性**
  ユーザーは自身が生成していない擬似乱数値をブロードキャストしない
- **ソース情報のセキュリティ**
  悪意あるユーザがレポートを送信していないユーザに関する情報を取得できないようにする
- **レポート受信者に対するプライバシー**
  レポートを受け取ったユーザが第三者にその情報を公開できないようにする
- **レポート送信者に対するプライバシー**
  レポートを送信するユーザは接触者にのみ接触した時間の情報を開示する

### 2.2　接触者の追跡方法

接触者の追跡は以下のフェーズによって行われる．

- **ブロードキャスト**
  疑似乱数値を生成して近くのデバイスにブロードキャストする
- **レポート**
  COVID-19 に感染した場合, 潜伏期間中に接触した可能性のあるユーザを把握するためにサーバにレポートを送信する
- **スキャン**
  COVID-19 の感染者に接触した可能性があるかサーバに問い合わせる

疑似乱数値のブロードキャストには Bluetooth Low Energy(BLE) を利用できる iOS および Android OS の機能を用いるため, 異なる OS 間であっても疑似乱数値の送受信は可能である．感染者は潜伏期間の範囲と疑似乱数値を計算するための鍵, 署名の検証鍵をサーバに送信することで, サーバは感染者が潜伏期間中に他ユーザにブロードキャストし

た疑似乱数値を計算する．他ユーザは，感染者から受け取った疑似乱数値を保持していないかサーバに問い合わせることで，自身が接触者か確認できる．

# 3　TCN Protocol による追跡

接触者の追跡には，疑似乱数値を生成して近くのデバイスにブロードキャストするブロードキャストフェイズ，感染者がサーバにレポートを送信するレポートフェイズ，自身が接触者になっているかを確認するスキャンフェイズがあり，それぞれの詳しい仕組みを次の節より示す．以下は TCP Protocol で登場する鍵と擬似乱数値を表す用語である．

- RAK(Report Authorization Key)
  レポートの署名を行う秘密鍵
- RVK(Report Verification Key)
  レポートの検証を行う公開鍵
- TCN(Temporary Contact Number)
  Bluetooth でブロードキャストされる疑似乱数値
- TCK(Temporary Contact Key)
  TCN を計算するための値

## 3.1　ブロードキャストフェイズ

ブロードキャストフェイズの初期段階として，署名に使用する鍵ペア RAK, RVK の作成と疑似乱数値 TCN を計算する TCK の初期値 $TCK_0$ の作成がある．その後，$TCK_0$ と RVK のハッシュ値から $TCK_1$ を求め，$TCK_1$ から $TCN_1$ を計算し，その値を Bluetooth を介して他ユーザにブロードキャストする．$TCN_1$ 以降の TCN($TCK_n(n>0)$) は，$TCN_{n-1}$ と RVK のハッシュ値から計算される．実際の実装での TCK は，自身のインデックスを表す $index$ と RVK を保持する $rvk$，$TCK_{n-1}$ と RVK のハッシュ値から求められた $bytes$ を持つ構造体である．$TCK_1$ のそれぞれの値の計算式を以下に示す．また，**図 1** は疑似乱数値 TCN を計算する手順を表したものである．

$$index = TCK_{n-1}.index + 1$$
$$rvk = TCK_{n-1}.rvk$$
$$bytes = H(TCK_{n-1}.rvk, TCK_{n-1}.bytes)$$

## 3.2　レポートフェーズ

RVK と $TCK_i$ をレポートとしてサーバに送信することで，$TCK_i$ 以降の $TCK_j$ と $TCN_j(j \geq i)$ を計算することができるので，すべての TCK を送信する必要はない．感染者の潜伏期間と思われる期間を $(j_1, j_2)$ とする．ユーザはレポートを送信する際に，$RVK$, $TCK_{20}.bytes$, $j_1$, $j_2$ の 4 つの情報を送信することで，サーバ側で $RVK$ と $TCK_{20}.bytes$ から $(TCN_{20}..TCN_{90})$ を計算できる．

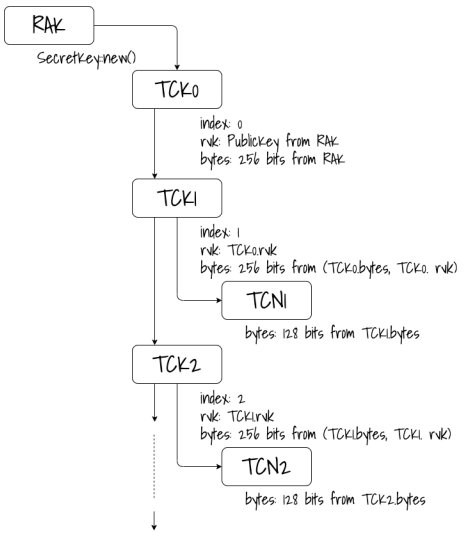


図 1　TCN を計算する手順

## 3.3　スキャンフェーズ

他ユーザはサーバにアクセスすることで，自身が感染者の TCN を保持していないかを確認することで感染者と接触したかを判断できる．

# 4　おわりに

TCN Protocol を利用することで位置情報などの個人情報を必要としないで接触者を追跡でき，感染経路の特定が容易にできると考えられる．ただし，このプロジェクトでは TCK の更新タイミングなどを言及していなかったため，どの程度の間隔で TCN をブロードキャストすることで追跡に有効なのかはわからなかった．また，完全な乱数を生成することができないため接触者でない場合でも接触者と判断される可能性がある．さらに，保健所が実際にこのような技術を導入した際には時間や個人を特定するために個人情報等をサーバに送信する必要があるため，新たにプライバシーの問題が発生すると考えられる．

# 参考文献

[1] 外務省 海外安全ホームページ | 各国・地域における新型コロナウイルスの感染状況. https://www.anzen.mofa.go.jp/covid19/country_count.html. (Accessed on

04/15/2020).

[2] Dp-3t/documents: Decentralized privacy-preserving proximity tracing – documents. https://github.com/DP-3T/documents. (Accessed on 04/15/2020).

[3] Tcncoalition/tcn: Specification and reference implementation of the tcn protocol for decentralized, privacy-preserving contact tracing. https://github.com/TCNCoalition/TCN. (Accessed on 04/15/2020).

[4] The-pact-protocol-specification-ver-0.1.pdf. https://pact.mit.edu/wp-content/uploads/2020/04/The-PACT-protocol-specification-ver-0.1.pdf. (Accessed on 04/15/2020).