準同型暗号によりプライバシー保護を実現する接触確認アプリケーション

2019SE028 熊崎廉真
指導教員：沢田篤史

1　はじめに

近年，COVID-19 の感染拡大に伴い，接触確認アプリケーションが世界中で使われている．接触確認アプリケーションを大別すると，分散型と中央集権型の 2 つに分けることができる．分散型接触確認アプリケーションは，アプリケーションをインストールした端末間で通信をすることによって，接触確認を行う．利点は，個人のプライバシーに配慮しやすいという点である．中央集権型接触確認アプリケーションは，アプリケーションの利用者の位置情報をもとに，中央サーバが距離計算をして接触確認を行う．利点は，感染拡大防止効果を高めやすいという点である．

2 つのタイプの接触確認アプリケーションには，それぞれに問題がある．分散型接触確認アプリケーションは感染拡大防止効果が低く，中央集権型接触確認アプリケーションはプライバシーへの配慮が不足する．

本研究の目的は，2 つのタイプの接触確認アプリケーションが抱える問題を同時に解決する接触確認アプリケーションのアーキテクチャを考案することである．

目的を解決するために，中央集権型のアプリケーションを前提としたアーキテクチャを設計することと，その妥当性を確認することという 2 つの技術課題を設定する．

本研究では，準同型暗号を使った中央集権型の接触確認アプリケーションのためのアーキテクチャを提案する．中央集権型を採用することによって，感染拡大防止効果を高めることができる．また，準同型暗号を採用することによって，十分にプライバシーへ配慮することができる．

2　背景と問題点

1 章で前述した通り，接触確認アプリケーションには，次のような問題点がある．

- 分散型：感染拡大防止効果を得にくい
- 中央集権型：プライバシーへの配慮が不足する

分散型接触確認アプリケーションは，アプリケーションの利用者間でしか接触確認ができない． また，感染者であったとしても陽性登録をしていない場合，アプリケーションから感染者として認識されない．

中央集権型接触確認アプリケーションには，個人のプライバシーへの配慮が不足する．中央集権型接触確認アプリケーションは，中央サーバが国民の位置情報などを収集し，それらを分析することによって，接触確認を行う．それゆえ，中央サーバから個人情報が漏洩したり，管理者によって，個人情報が接触確認以外の不当な目的に利用される可能性がある．

3　研究目的と技術課題

2 章であげた問題点を解決するために，本研究では，中央集権型を前提に，個人のプライバシーへの配慮を達成することを目的とする．この研究目的を達成することによって，中央集権型の利点である高い接触確認防止効果を得ながら，プライバシーへの配慮を実現することが可能となる．

目的を解決するために，次の技術課題を設定する．

- 中央集権型の接触確認アプリケーションにおいてプライバシーに配慮するためのアーキテクチャを明らかにする
- 中央集権型アプリケーション基盤としてのアーキテクチャの妥当性を確認する

4　プライバシーに配慮した中央集権型接触確認アプリケーションのアーキテクチャ設計

本研究では次の方針で設計を進める．

- アプリケーションのタイプとして中央集権型を採用することによる感染予防効果の獲得
- 準同型暗号の採用による個人情報保護の実現
- 医療分析，電子投票という 2 つの分野における先行研究成果を採用

本研究では，準同型暗号計算を実現するライブラリをアーキテクチャに組み込んでいる．準同型暗号とは，暗号文に対して加算や乗算ができるという性質を持つ暗号化方式である．準同型暗号を採用することによって，ユーザや感染者の位置情報を秘匿したまま接触確認を行うことができる．

また，本研究では，医療分析，電子投票という 2 つの分野における先行研究成果を採用した．医療分析については，Aloufi らの研究 [1] を参考にした．電子投票については，Yang らの研究 [2] を参考にした．

本研究で考案した接触確認マップというデータ構造について説明する．接触確認マップは，感染者の位置情報が六角形格子上に黒い点として表されたものである．六角形格子の採用は An らの研究 [3] を参考にした．

アプリケーションの静的構造を図 1 に示す．アプリケーションのクラスとして，ユーザ，感染者，医療機関，サーバ，位置情報，接触確認マップ，暗号機，復号機，鍵，鍵束，計算結果，判定結果がある．

本研究で提案する接触確認アプリケーションでは，接触確認マップを用いて接触確認を行う． 接触確認マップを用いた接触確認の流れは，図 2 のようになる．

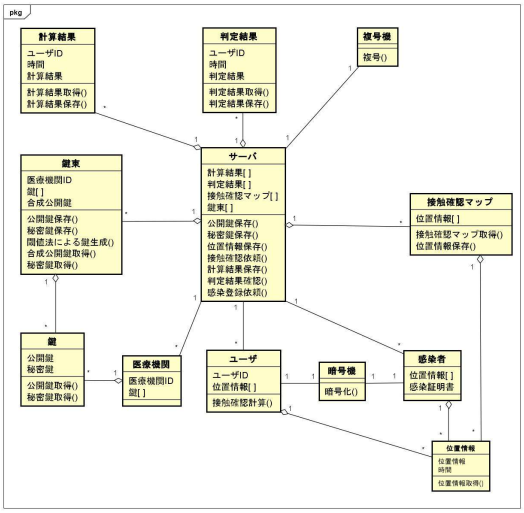

図 1　接触確認アプリケーションのアーキテクチャ

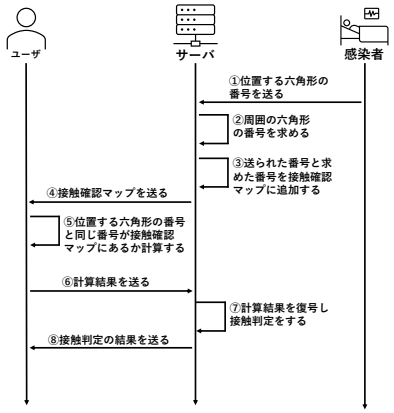

図 2　接触確認マップを用いた接触確認の流れ

接触確認マップを使った接触確認と従来の接触確認には 2 つの違いがある．1 つ目の違いは，接触確認を行う対象である．2 つ目の違いは，濃厚接触の定義である．

5　シミュレーション

提案する接触確認アプリケーションで接触確認が行えることを確認するために，簡単なシミュレーションを行った．シミュレーションは，感染者 1 人とユーザが 1 人いる場合を考え，決められた移動経路についてとランダムに設定した移動経路についての 2 通りを行った．

2 通りのシミュレーションの結果，提案する接触確認アプリケーションで接触確認が行えることを確認できた．

6　考察

アーキテクチャの妥当性確認では，ユーザ，感染者の立場から，次の考察を行った．

- プライバシーへの配慮という観点から，従来の中央集権型接触確認アプリケーションと提案する接触確認アプリケーションとを比較
- 情報がプライベートであるか

妥当性の確認の結果，従来の中央集権型接触確認アプリケーションと比べ，個人のプライバシーへ配慮されることが示された．

接触確認計算，接触判定という 2 つのユースケースについて，アルゴリズム記述を作成し，計算量を見積もる．

考察の結果，接触確認計算の計算量は $O(n)$，接触判定の計算量は $O(n)$ と見積もることができた．

7　おわりに

分散型と中央集権型という 2 つのタイプの接触確認アプリケーションにはそれぞれ問題がある．すなわち，分散型で感染拡大防止効果を得にくく，中央集権型でプライバシーへの配慮が不足する．

これらの問題点を解決するために，本研究では，中央集権型のアプリケーションに準同型暗号を組み込んだアーキテクチャを提案した．

本研究では，中央集権型を採用することにより感染拡大防止効果を得た．準同型暗号によって，個人のプライバシーへ配慮した．妥当性確認によって，従来の中央集権型の接触確認アプリケーションと比べて，個人のプライバシーへ配慮されることを示した．

今後の課題は 3 つある．1 つ目の課題は，物を介した二次接触による感染を判定できるように拡張することである．2 つ目の課題は，人流モデルを用いたシミュレーションを行うことである．3 つ目の課題は，ブロックチェーンの採用による感染者の情報の保護である．

参考文献

[1] Asma Aloufi, Peizhao Hu, Harry WH Wong, and Sherman SM Chow. “Blindfolded evaluation of random forests with multi-key homomorphic encryption”. *IEEE Transactions on Dependable and Secure Computing*, Vol. 18, No. 4, pp. 1821–1835, 2019.

[2] Xuechao Yang, Xun Yi, Surya Nepal, Andrei Kelarev, and Fengling Han. “A secure verifiable ranked choice online voting system based on homomorphic encryption”. *IEEE Access*, Vol. 6, pp. 20506–20519, 2018.

[3] Yongdae An, Seungmyung Lee, Seungwoo Jung, Howard Park, Yongsoo Song, and Taehoon Ko. “Privacy-oriented technique for COVID-19 contact tracing (PROTECT) using homomorphic encryption: Design and development study”. *Journal of medical Internet research*, Vol. 23, No. 7, p. e26371, 2021.