コンタクトトレーシング（接触追跡）アプリとクラウド

高橋郁夫

駒澤綜合法律事務所

KOMAZAWA LEGAL CHAMBERS

コンタクトトレーシングの概念

- 概念(Concept)
  - コンタクトトレーシング
    - ワクチン接種や健康モニターなどの感染拡大防止・公衆衛生対応を行うために、伝播する可能性のある感染症の感染者から、感染した可能性のある人をたどる調査手法
    - 感染源となりうるウイルスに感染した患者本人の行動を調査し、濃厚接触者を特定し、それぞれ診断・カウンセリング・治療を提供することにより、感染拡大を予防する一連のプロセス
- 「積極的疫学調査」
  - 積極的疫学調査とは、今後の感染拡大防止対策に用いることを目的として 行われる感染症などの色々な病気について、発生した集団感染の全体像や病気の特徴などを調べることをいいます

KOMAZAWA LEGAL CHAMBERS

出口戦略（Exit strategy)と コンタクトトレーシング（Contact tracing)

- 例　EU 「COVID-19　封じ込め手段の緩和のための共通ロードマップ」（Joint European Roadmap towards lifting COVID-19　containment measures）
  - クライテリア
    1. 疫学的基準
    2. 医療のキャパシティ
    3. 適切なモニタリングのキャパシティ
       1. 大規模な検査能力
       2. **コンタクトトレーシング**
       3. 再発症および感染拡大防止のための隔離設備

KOMAZAWA LEGAL CHAMBERS

コンタクトトレーシングの基礎

- 大きな種別
  - データ把握モデル
    - 位置情報利用
  - 匿名化されたデータアプローチ
  - データ収集を最小限におさえるアプローチ
    - ブルートゥース技術利用
      - 中央処理モデル
      - 分散処理モデル

      - PEPP-PTのホワイトペーパーによる

SingaporeのTrace Together

- GovTech Agency（政府技術庁）
  - TraceTogether
  - VigilantGantry(自動体温スクリーニングシステム)
  - Self-help Temperature Scanner(自主的体温スキャナー)
  - Travel and Health Declaration System(旅行健康申告システム)
  - Ask Jamie chatbot(チャットボット)

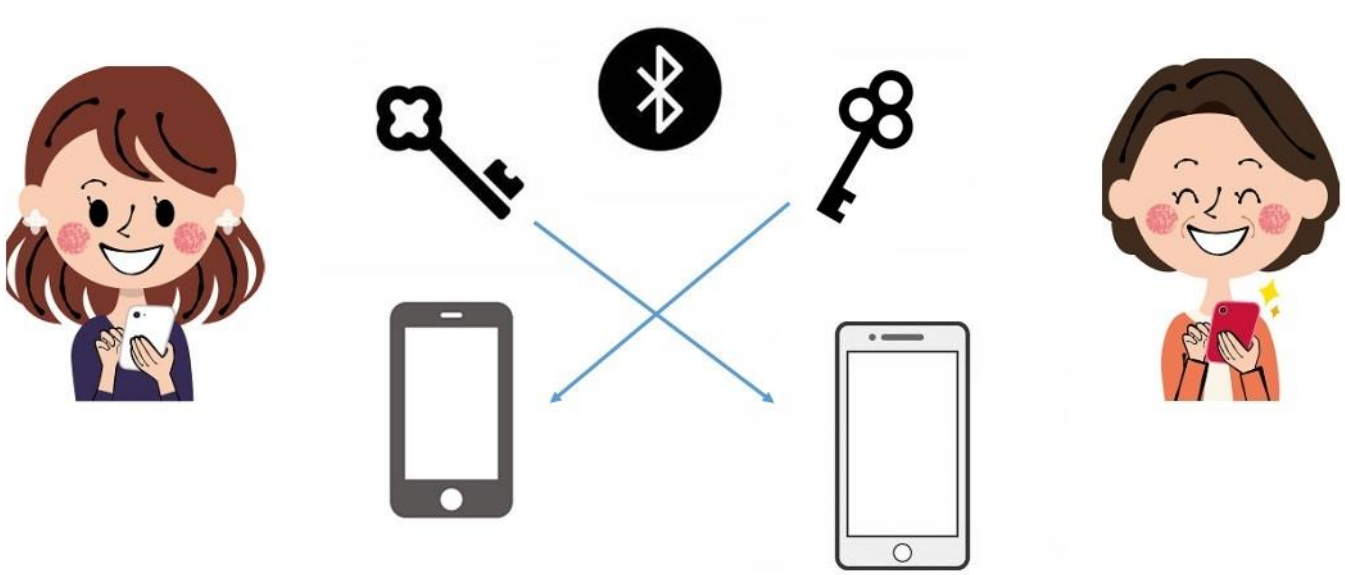
TraceTogetherを支えるもの

- GovTehAgency（政府技術庁）
- プロトコルとしてのBlueTrace
  - ポリシードキュメント
  - ホワイトペーパーとして、根拠となっている論文が公表

- ４つのフェーズ
  - （1）アプリのダウンロード・登録
  - （2）利用とデジタルシェークハンド
  - （3）陽性判定によるデータのアップロード
  - （4）近接接触者への通知のプロセス

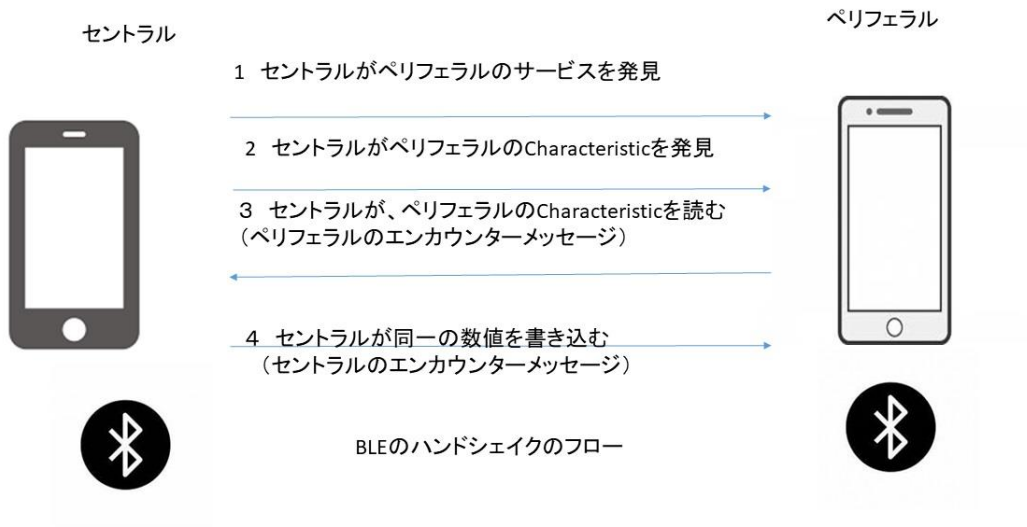
フェーズ1　アプリのダウンロード・登録

- 利用者は、アプリをインストール
- ユーザーはシンガポールの携帯電話番号を使用して登録
- ランダムなユーザIDとともにサーバーに保存される



フェーズ2　利用とデジタルシェークハンド

- 一時的IDの生成
  - ユーザーID、作成時刻、有効期限
  - 保健当局のみが暗号化・復号化
  - 短期的に消滅
- ハンドシェイク
- 接触履歴の保存
  - 特定の日数（OpenTraceは、21日）



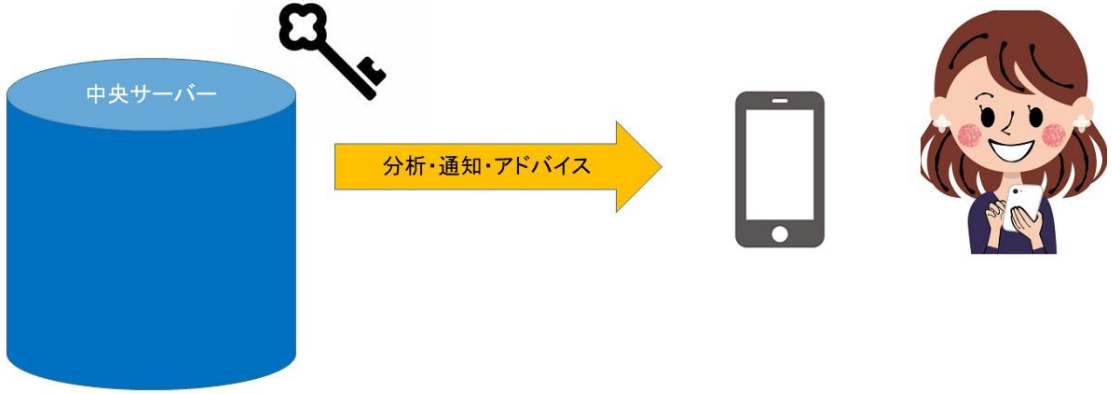
フェーズ3　陽性判定によるデータのアップロード

- 陽性判断を受けた利用者
  - 接触履歴を自らの端末から、第三者に渡すことを要求される
- 接触追跡者のみがユーザーにデータのアップロードを要求できる
  - 認証メカニズムを導入

KOMAZAWA
LEGAL CHAMBERS

フェーズ４　近接接触者への通知のプロセス

- 保健当局
  - アップロードされた接触履歴の中から、各接触のためのTempIDを解読
  - UserID と有効期間を取得
  - 各 TempID の出会いのタイムスタンプが　有効期間内であることを確認
- ばく露時間（遭遇の連続したクラスターの長さで測定）と距離（測定、受信した信号強度の読み取りによる)の疾患の疫学的パラメータに基づいて、フィルタリング
- 接触追跡者が接触の可能性の高い人のリストを手に入れたら、その人にコールドコールをする必要



KOMAZAWA
LEGAL CHAMBERS

日本の選択と今後の議論すべき課題

Challenges as “Wrap up”

KOMAZAWA
LEGAL CHAMBERS

KOMAZAWA
LEGAL CHAMBERS

日本は、何を選んだのか？（テック会議　5/8資料）

- 正確な事実認識？
- トレードオフは意識されているのか？

接触確認アプリ主要類型の特徴

日本案

類型	位置情報型	Bluetooth型		
		個人特定型	匿名型 (EU提案)	
		中央サーバ処理型	中央サーバ処理型	スマホ端末処理型
特徴	・位置情報を用いて、感染者と接触のあったアプリユーザを当局が特定。 ・位置情報精度補完のために、インド等はbluetoothも併用	・電話番号等の個人情報により、当局が接触者を特定し、連絡が可能。	・各ユーザの接触者データは、当局が保有するサーバーで管理。	・各ユーザの接触者データは、各ユーザの端末で管理
実施国	インド、イスラエル等	シンガポール、オーストラリア	（検討中）英国、フランス	（検討中）ドイツ、スイス、エストニア 等
Google・AppleのAPIとの関係 （API接続のメリット） ①低電力での相互互換性 ②常時記録が可能 ③プライバシー保護	活用せず （独自開発によりアプリをリリース済、Google-Appleは位置情報を活用せず）	不明 （これまでは活用せず独自開発によりアプリをリリース済。今後の対応は不明）	検討中 （英国は独自の開発により、一部地域で実証開始したところ。）	活用する方向 （APIの公開後アプリをリリース予定）

日本の仕組み

接触確認アプリの仕組み（検討中・未定稿）

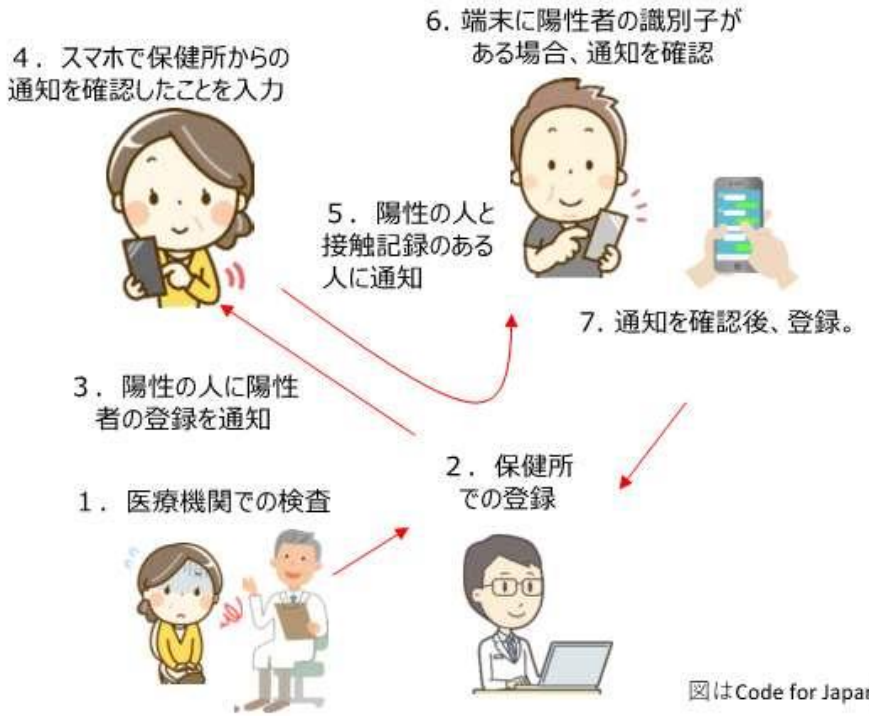
＜通常時＞

- 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。**



図はCode for Japan提供

KOMAZAWA LEGAL CHAMBERS

仕様書とプライバシー等評価書・

- 公表（5月26日）
  - 「接触確認アプリ及び関連システム仕様書」
  - 「「接触確認アプリ及び関連システム仕様書」に対するプライバシー及びセキュリティ上の評価及びシステム運用上の留意事項 」
- クラウドとの関係
  - 民間による業務委託がなされることが明らかになった

KOMAZAWA
LEGAL CHAMBERS

日本の接触確認アプリのプロセス

自主的なインストール
携帯電話は接触識別子を生成し、端末に保存

利用者Aは新型コロナウイルスに感染／利用者Aは、利用者BやCと接触
利用者Dとは、社会的距離を維持

利用者AがCOVID－19検査で陽性判定
利用者Aは、匿名データの送信に同意、Aは、隔離

主体Aの接触識別子が中央サーバーに送信される

主体Aの診断キーのブロードキャスト

接触確認アプリを通じて受信
端末で分析・利用者B&Cへの通知
利用者B&Cは、行動変容・保健所（？）

KOMAZAWA
LEGAL CHAMBERS

接触確認アプリおよび
HER-SYS

接触
ユーザー

民間委託
事業者

取
扱

接触確認アプリ
中央サーバー

④接触確認

③診断キー
ダウンロード

②診断キーのアップロード

①登録キー

⑤（必要に応じて）連絡

保健所

陽性登録

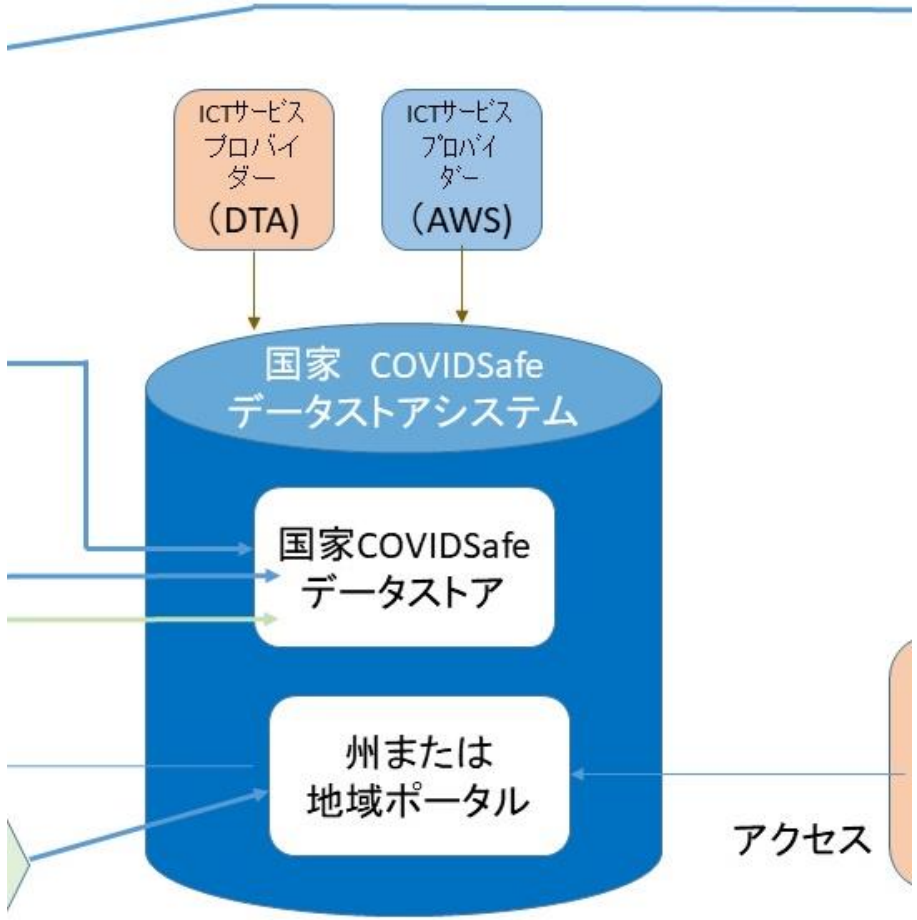
感染者システム

検査陽性

KOMAZAWA
LEGAL CHAMBERS

COVIDSafe(オーストラリア)のデザインとクラウド

- COVIDSafeの国家COVIDSafeデータストアシステムは、AWS が実際の運営を担っている。
- 留意すべき事項
  - 法的論点
    - 第三者提供となるのか、どうか。
    - 国家(保険省とデジタルトランスフォーメーション庁)とアマゾンとの契約の問題点



KOMAZAWA
LEGAL CHAMBERS

第三者提供となるのか、どうか。

- オーストラリアでの解釈
  - サービスを提供する契約者への開示は、契約者という（第三者への）開示／収集ではなくて、関連するプライバシー組織による利用
  - 無条件にこのように考えられるわけではなく、拘束力のある契約があること、そして、同等の義務を負うことが要件である
- 日本ではどうか
  - 利用目的の達成のために必要な範囲であれば、同意がなくても個人データの取り扱いの全部又は一部を委託することが可能（同法23条5項1号）。
  - 委託先の監督
    - 「取扱いを委託する個人データの内容を踏まえ、個人データが漏えい等をした場合に本人が被る権利利益の侵害の大きさを考慮し、委託する事業の規模及び性質、個人データの取扱状況（取り扱う個人データの性質及び量を含む。）等に起因するリスクに応じて」とされる
  - 個人情報の保護に関する法律についてのガイドライン （通則編）」の3-3-4「委託先の監督（法第 22 条関係）」（42頁以下）
  - 仕様書では、明確に委託としている
  - 行政機関等個人情報保護法では同意が必要となる

KOMAZAWA LEGAL CHAMBERS

契約による担保（なお、DTAとAWSについて）

- PIAの項目をみる
  - デジタルトランスフォーメーション庁が、アクセス、変更、検索の権利／力を維持すること、情報へアクセスしうる者の目的、セキュリティ措置、情報が検索しうるのか、永久に消去されるのか、などが考慮されて判断されること（10.2.3）
  - デジタルトランスフォーメーション庁とアマゾンとの契約が含むべき事項(10.4)
  - その契約によるとき、コモンウエルスによる利用と認識されること(10.5)
  - 保健省は、AWSとの契約を精査すること(10.7)

具体的な契約事項

- アプリの詳細な機能要件と非機能要件、および 全国COVIDSafeデータストア・ インフラストラクチャ上のセキュリティ、機密性、およびプライバシー要件（インフラストラクチャ、アプリ内の情報の保存に関する詳細なセキュリティ要件と暗号化を含む）
- 全国 COVIDSafeへのアクセスを制限する詳細なサポート要件
- クラウドベースのインフラストラクチャの提供における契約に一般的に見られる条項
- AWSに課せられた義務は、AWSの下請け業者および/またはそのサービスプロバイダのいずれかにも課せられることを保証するために必要な下請け業者への要求事項
- ユーザー が個人情報へのアクセス権、訂正権を有する場合の情報へのアクセスに関する要求事項
- 国立COVIDSafeデータストアからの移転に関する詳細な要求事項（国外への持ち出し等の禁止）

KOMAZAWA
LEGAL CHAMBERS

クラウドベースのインフラストラクチャの提供における契約に一般的に見られる条項

- AWS は、全国 COVIDSafeデータストアに保存されたデータコンテンツの管理に責任を負わないこと
- オーストラリア連邦に、アクセス、変更、取得を制御するために必要な権利と権限が与えられていること
- 連邦政府がAWS契約の終了後、全国 COVIDSafe データストアに保存されているデータコンテンツを削除することをAWSが許可すること（削除されない場合についても同様）

最後に

- 新型コロナウイルス対プライバシー: コンタクトトレーシングと法 （Kindle版）
- 高橋郁夫 有本真由 黒川真理子 (著)

- ご購入ください。

KOMAZAWA
LEGAL CHAMBERS