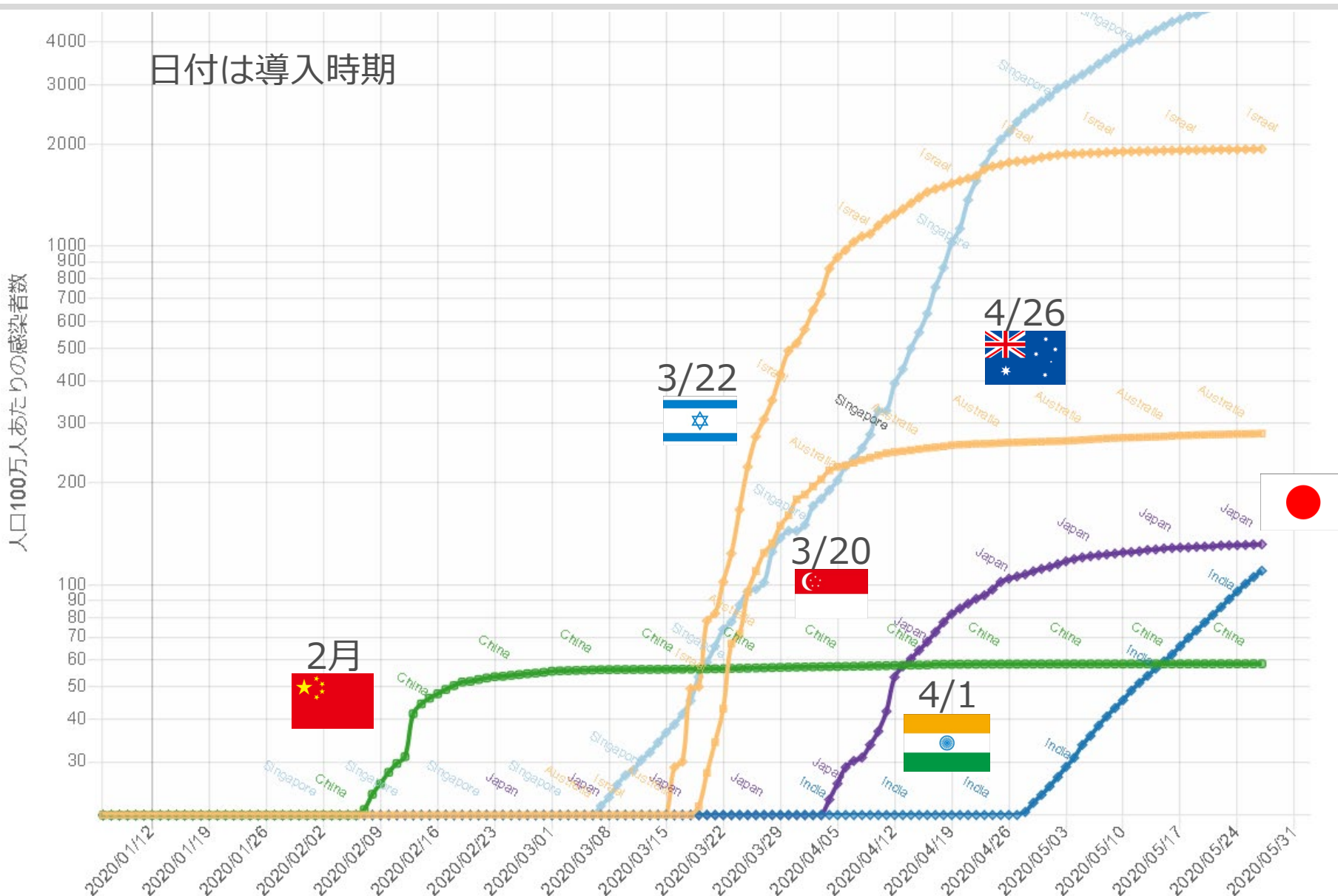


プライバシー保護に配慮した追跡システム AI for Good Global Summit より

2020年6月1日
一般社団法人情報通信技術委員会 (TTC)
金子 麻衣

コンタクトトレーシングアプリを導入した国と日本の感染者数の比較（人口100万人当）



出典：札幌医科大学医学部 附属フロンティア医学研究所 ゲノム医科学部門ホームページより筆者加工

Copyright © 2020 TTC. All Rights Reserved

Contact Tracing（接触者追跡）とは

- 接触可能性に基づき、感染リスクの高い人を予防的に発見・通知し、必要ならば隔離することによって、ウイルスの蔓延防止に役立てるための仕組み
- 諸外国で開発されているTracingには3つのアプローチがある
- Bluetoothはデータの収集方法で、サーバ集中型と分散型に分かれる

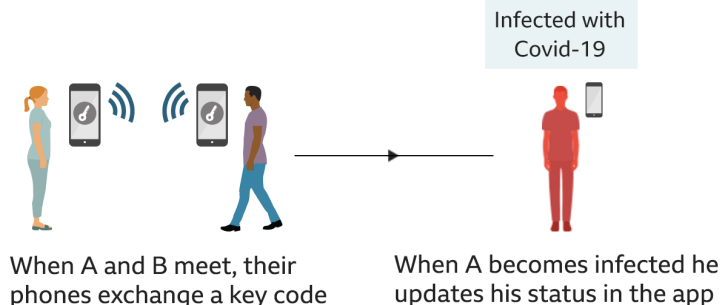
表 Tracingアプリの主な分類

①ロケーション	②Bluetooth	③両方
<ul style="list-style-type: none">• 携帯電話のGPSデータを活用、幅広く検討	<ul style="list-style-type: none">• ほぼリアルタイムで接触した人の記録が取得可能• プライベート端末に情報を保持	<ul style="list-style-type: none">• GPSやBluetooth等の技術を両方活用
<ul style="list-style-type: none">• Duality SecurePlus™ プラットフォーム• Hamagenアプリ（イスラエル政府）• 通信ビッグデータ旅程カード（中国政府）	<p>ランダムに変わるBluetoothのID等を記録</p> <ul style="list-style-type: none">• PEPP-PT（欧州8カ国）両方• AGF※分散型 <p>電話番号・郵便番号を記録</p> <ul style="list-style-type: none">• Trace Together（シンガポール政府）集中型• COVID Safe（オーストラリア政府）集中型	<ul style="list-style-type: none">• Aarogya Setuモバイルアプリ（インド政府）集中型

※正式名称はAppleとGoogleが共同で提供するExposure Notification Framework、略してAGF

集中型VS分散型アプリ

感染しなければ接触したスマホのIDは各自のスマホに蓄積されたまま



感染が発覚

(集中型)

感染者のスマホからID及び蓄積した他のスマホのIDがサーバに送られる

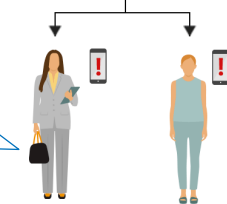
集中型



Phone provides own anonymised ID plus codes gathered from other phones to centralised database

(集中型)

サーバでマッチング、感染のリスクがある連絡先にアラートを出す



Computer server uses database to do contact matching and risk analysis, plus sends alerts

分散型



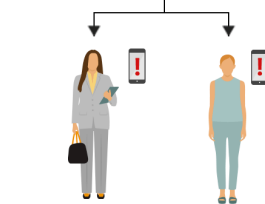
Phone provides own anonymised ID only to centralised database

(分散型)

スマホから感染者のIDだけがサーバに送られる

(分散型)

スマホにデータベースをダウンロード、リスクが高い連絡先を照合し、アラートを出す



Phone downloads database, does contact matching and risk analysis, plus sends alerts

出典：BBCNews「Coronavirus contact-tracing: World split between two types of app」

(参考) Bluetooth (集中型) の基本的な仕組み

- ユーザ毎にTempID (暗号化されたトークン・15分有効) を発行、保健機関で集中管理
- スマホが接近するとTempIDを交換し、各自のスマホに接近したIDを記録
- 陽性と判定された患者のスマホから全TempIDが保健機関にアップロード
- 保健機関から接触したと思われるスマホに通知

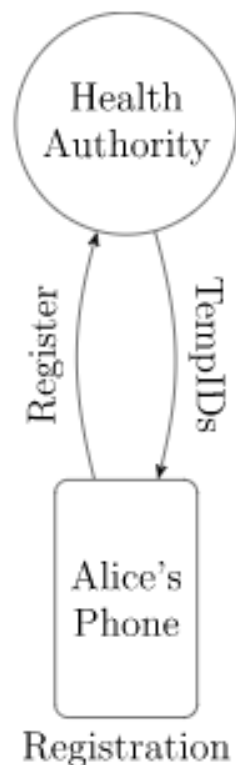
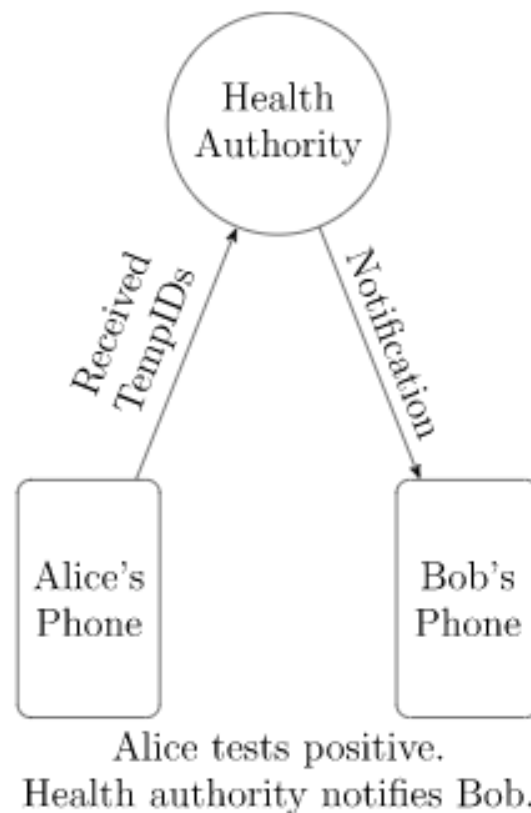
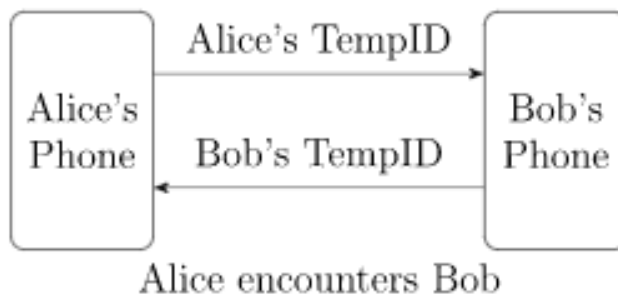


図 オープンソース「BlueTrace」の仕組み
(シンガポールTraceTogetherとオーストラリア
COVID safe で採用)



①ロケーション

- **Duality SecurePlus™** プラットフォーム
- **Hamagenアプリ** (イスラエル政府)
- **Rilevatore terremotoアプリ** (イタリア)
地震対策で開発したアプリを活用
- **マルチソース** (韓国) 防犯カメラ・クレカ記録も含む
- **通信ビッグデータ旅程カード** (中国)
- **GH COVID-19 Tracker** (ガーナ政府)
- **CovidApp** (イタリア)

③両方 (Bluetooth・GPS等併用)

- **Aarogya Setuモバイルアプリ** (インド政府)
- **NOVID20** (オーストリアのデジタル専門家等の団体)
- **Corona-Datenspende** (ドイツ公衆衛生研究所)
リストウォッチ対応
- **Institute of Public Health**
(ノルウェー公衆衛生研究所)
- **Open Coronavirus** (スペイン)

②Bluetooth

BluetoothのID等ランダムに変わるIDを記録

- **PEPP-PT** (欧州8カ国) Ephemeral Bluetooth識別子
- **DP-3T** (スイス等欧州のアカデミア等)
- **Private Tracer** (オランダのMILVUM) DP-3Tプロトコル
- **TCNプロトコル** (米国欧州のTCN連合) 一時的なTCN番号
- **Covid Watch** (米スタンフォード) TCN連合・CoEpiと連携
- **CoEpi** (米国)
- **Ketjuプロジェクト** (フィンランド)
- **HSEアプリ** (アイルランド政府)
- **WeTraceアプリ** (スイス)
- **AGF**

電話番号・郵便番号も記録

- **Stopp Corona** (オーストリア赤十字)
- **Trace Together** (シンガポール政府)
- **COVID Safe** (オーストラリア政府)

出典：GDPR HUB・各サービスサイトより金子が編集・分類

AI for Good Global Summitとは

- 国際連合のAIプラットフォームで毎年5月にジュネーブで開催するイベント、今年は12月までデジタルプログラムに移行
- COVID-19対策などグローバルな課題に関するAIの最新の開発や有望なユースケースを共有

開催概要	3/27～毎週1or 2回 3～4月 COVID-19対策 5月～ スタートアップ紹介など幅広い分野に拡大
開催方法	Zoom
主催	ITU XPRIZE※
内容	60分～90分程度/回 モデレータ+講演者数名
概要	<ul style="list-style-type: none">• Zoomチャット機能を使って質問を受付• 当日のセミナー動画が大体が後日公開• セミナーによっては資料も共有

※ 世界中のイノベーターを支援する非営利団体の財団、賞金レースを運営

3/27 : COVID-19 : 韓国における感染者数曲線平坦化のためのICTとAIの活用事例

講演者 :

- 韓国厚生省健康福祉部疾病予防管理センター (KCDC) リスク評価部門のディレクター
- 成均館大学校 (ソウルの私立大学) のインタラクシオンサイエンス学部教授

4/3 : COVID-19 : プライバシーを尊重しながら、携帯電話とAIで接触者追跡

講演者 :

- テクノロジ新興企業Dualityの共同創設者兼CTO
- FG-AI4H議長、ベルリン工科大学教授、フラウンホーファーハインリッヒヘルツ研究所の事務局長

4/9 : COVID-19:世界的大流行に対する中国のデジタル保健戦略

講演者 :

- 政府の情報通信分野主管庁MIITの直属組織、中国情報通信研究員 (CAICT) のスマートヘルス部門の技術者
- 中国電信 (チャイナテレコム) のマシンビジョンの研究開発・標準化担当のディレクター

4/17 : COVID-19 : 誤情報(misinformation)と偽情報(disinformation)に対して何をすべきか (動画未公開)

講演者 :

- 410LabsのCEO (ユーザインタフェースの開発、メッセージを効率的に整理するメーラー等を開発)
- Bodacea Light Industries (情報セキュリティ関連企業) の創設者
- Stanford Internet Observatoryの技術マネージャ (SNS上の悪意ある情報の広がりを調査)
- EEAS (EUの関係機関) のメンバー (欧州委員会等と連携し外交・安全保障対策を実施)

4/24 : COVID-19 : 自動運転車はどこにありますか? モビリティの未来について

講演者 :

- Roborace (AI自動運転マシンによるモータースポーツ) とADA (Roboraceを推進する非営利団体) の創設者
- 世界経済フォーラム 自動車・自動車関連事業本部長
- デューク大学電気情報工学科教授

- 1 Duality SecurePlus™ プラットフォーム
- 2 PEPP-PTプロジェクト
- 3 欧のコンタクトトレーシングアプリの動向
- 4 まとめ

プライバシーの保護に配慮した追跡システム

- Duality社は、生データを公開することなく暗号化した状態で共有できるAIベースのDuality SecurePlus™ プラットフォームを開発
- キーテクノロジーは準同型暗号、最大の特徴は暗号化したまま計算できること、電子投票、電子マネーなどの暗号プロトコルとして利用

Schematic of data flow: データフロー図



準同型暗号化: ライフサイクル全体を通じてデータを保護
Homomorphic Encryption secures data throughout the entire lifecycle

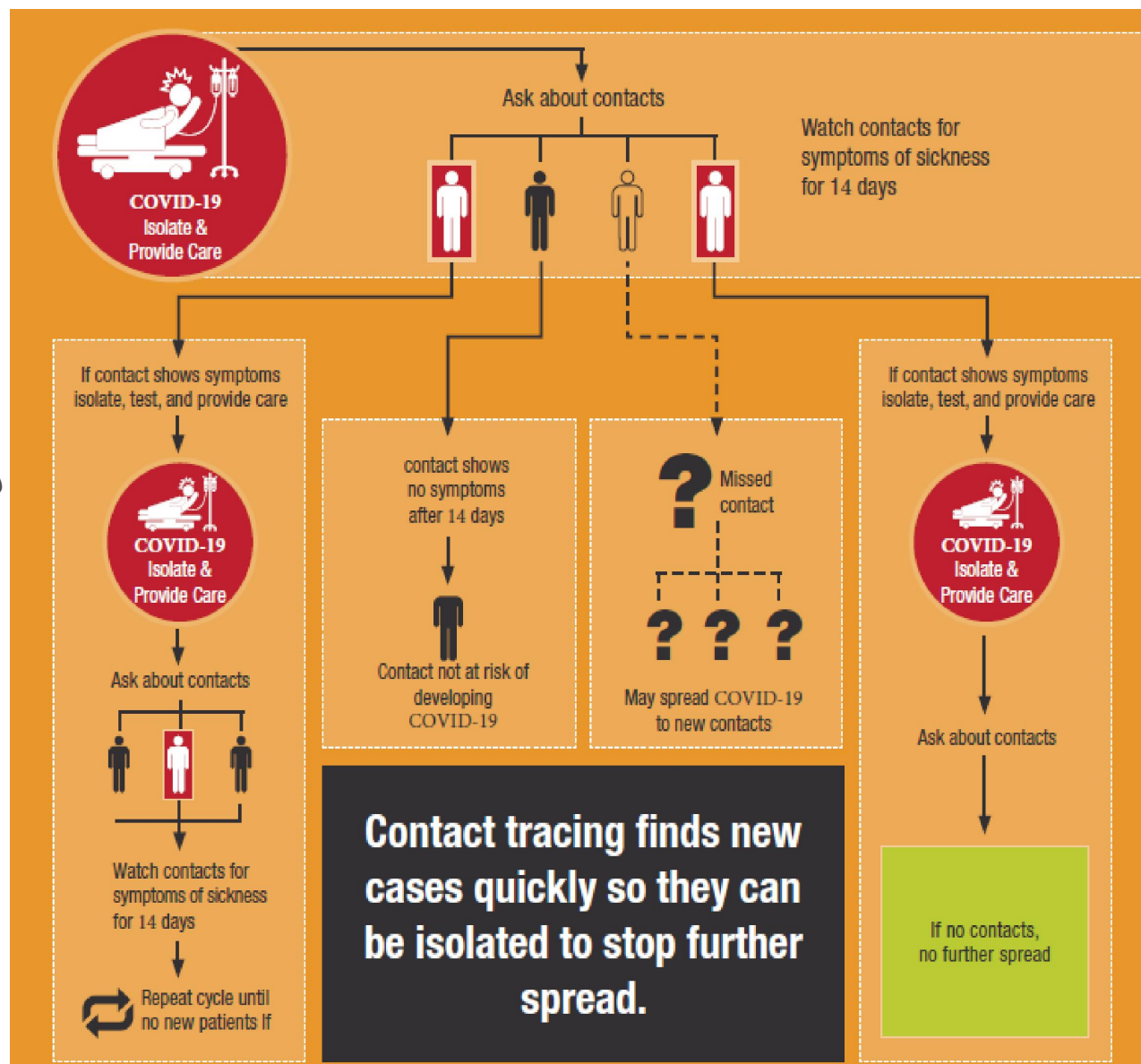
感染状況を確認し、14日間病気の症状が見られないか監視

(左)
症状がある場合は検査・隔離
→接触者に患者がいなくなるまで
サイクルを繰り返す

(中左)
感染者と接触して14日経過しても
症状がない
→感染リスクはないか注意

(中右)
連絡先・消息不明
→感染拡大の可能性あり

(右)
症状がある場合は検査・隔離
→接触者がいない場合はそれ以上
広がらない



Secure Query1

- (入力)医療機関で感染者の**ID（電話番号・電子メール等）**と日付
- （出力）スマホ等が確認された**場所・日付・時刻**

Secure Query2

- (入力)スマホ等が確認された**場所・日付・時間**
- （出力）同日同時刻に同じ場所にいた**個人の情報**

Action

- 医療機関は感染可能性がある**接触者、企業等のリスト**を入手し、連絡を取ることが可能
- 地域の医療機関、自治体、政府関係機関と連携

プライバシー保護

- 位置情報を提供するプロバイダは医療機関が入力した**個人情報**を閲覧することはできない（**出入力情報は全て暗号化**）
- 医療機関であっても開示を拒否している**個人の情報は閲覧できない**

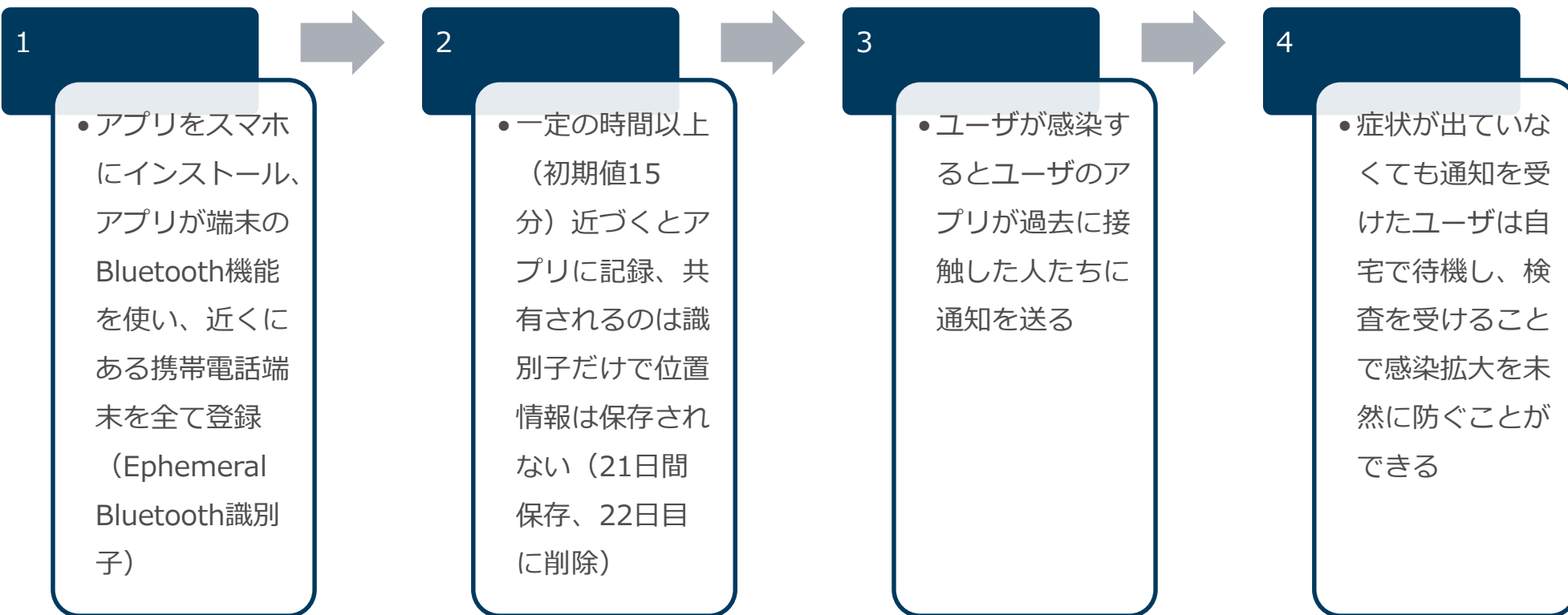
- **汎用オープンソースの暗号化ライブラリ** <https://palisade-crypto.org>
2条項BSDライセンス※に基づくオープンソース
- Duality、ニュージャージー工科大 (NJIT)、MIT、BBNテクノロジーズ (アメリカのハイテク企業)、Lucent Govt、インテル等からなるコンソーシアム
- **アメリカ国防総省 (DoD)、アメリカの諜報活動を支援するインテリジェンスコミュニティ (IC)、アメリカ国立衛生研究所 (NIH) から多額の資金提供**
- **業界国際標準コンソーシアム** <https://homomorphicencryption.org/>
参加企業 : Microsoft, Samsung, Intel, Duality, IBM, Inpher, Google, SAP, Mastercad, Mercedes Benz, Alibaba Group, LinkedIn, 政府機関、アカデミア多数etc
参加国 : USA, Canada, Korea, Japan, China, Singapore, Australia, UK, Ireland, Italy, Israel, Germany, Egypt, Brazil, UAE, etc
- 2020年秋、EPEL (スイス連邦工科大学ローザンヌ校)、Inpher (米国とスイスに拠点をおく機械学習を使ったセキュアなソフトウェアを開発)、**ITUと共同で HomomorphicEncryption.org ワークショップを開催予定 (バーチャル予定)**

※フリーソフトウェアで使われるライセンス体系の一つ、書面上の許可なく開発者の名称を販売促進に使用しないという項目を削除したもの

- 1 Duality SecurePlus™ プラットフォーム
- 2 PEPP-PTプロジェクト
- 3 欧のコンタクトトレーシングアプリの動向
- 4 まとめ

- **PEPP-PT (The Pan European Privacy-Preserving Proximity Tracing) プロジェクト**は、ドイツのフラウンホーファー・ハインリッヒヘルツ研究所が主導し、欧州8カ国の研究機関・130名の研究者が参加するスイスの非営利団体 (Foundation Botnar (スイス慈善団体) から寄付)
- EUの厳しいプライバシー規則である**一般データ保護規則 (GDPR) に準拠**し、個人のプライバシーを侵害することなく、感染者を追跡できるデジタルプラットフォームを開発
- **通信プロバイダのデータを必要としない**、AGFと技術的には類似しているが別物で特に連携はしていない
- **ドイツはPEPP-PTのアプリ採用する予定**で国内のサービスプロバイダーに互換性を持たせるよう要請していたが、**中央集中型に反対する世論によりAGFを採用**→中央集中型・分散型が可能とアピール
- スイス連邦工科大学チューリッヒ校 (ETHZ)、同ローザンヌ校 (EPFL) も本プロジェクトに参加していたが、当初の中央型に懸念を示し**DP-3Tの開発に移行、スイス政府も支援**
- フランス政府はこのプロジェクトに参加しているINRIA※に協力、PEPP-PTのプロトコルを使う予定 (国民の参加は任意)

※フランスのコンピュータサイエンスの国立研究所



その他

- 接触者の識別子は個人のスマホにローカルで記録、感染すると情報をサーバにあげる
- 識別子は擬似的にランダムに生成され、定期的に変更されるため個人を特定することはできない
- Bluetoothが発信するブロードキャストは4, 5mの短距離
- 国別コードが埋め込まれていて、国境を越えた移動にも対応
- プロトコルやコードは[GitHub](#)で公開中

- 1 Duality SecurePlus™ プラットフォーム
- 2 PEPP-PTプロジェクト
- 3 欧のコンタクトトレーシングアプリの動向
- 4 まとめ

主な欧諸国の追跡システム動向

- 英には内閣府デジタルサービスが支援するBlueTraceもある
- 導入後も他方式を検討する国も（フィンランド：DP-3T、オーストリア・アイルランド・イタリア：AGF）
- その他AGFを支持する国：独、ラトビア、スイス、エストニア
- スイス・エストニアはDP-3Tも検討

国	システム（主体）	仕組み
イギリス	NHS COVID-19 app （NHSX：国民保険のデジタル部門）	Bluetooth・集中型
ポーランド	ProteGo	
オーストリア	STOPP CORONA （赤十字）	Bluetooth・分散型
フィンランド	Ketju	
イタリア	Immuni	
ノルウェー	Smittestopp	ロケーション
ブルガリア	Virusafe	
アイスランド	Rakning C-19	
アイルランド	HSE Covid-19 App	

出典：MIT Technology Review 「A flood of coronavirus apps are tracking us. Now it's time to keep track of them.」
 BBCNews 「Coronavirus contact-tracing: World split between two types of app」等より筆者作成

ETSIによる標準化の動き

- **ETSI（欧州電気通信標準化機構）**は、ヨーロッパにおける電気通信産業に関する標準化機関
- **スマホをベースにした近接追跡システムの標準化フレームワークの開発を行うグループ「INDUSTRY SPECIFICATION GROUP EUROPE FOR PRIVACY-PRESERVING PANDEMIC PROTECTION（ISG E4P）」の発足を発表（5/12）**
- グループには通信事業者、ベンダ、研究関連組織など10以上が参加、キックオフミーティングが5/26に開催
- **主なメンバー：BT（英通信事業者）、Telekom Deutschland（独通信事業者）、Orange（仏通信事業者）、フラウンホーフアーハインリッヒヘルツ研究所、INRIA、HUAWEI、サムソン、エリクソン、クアルコム、NECヨーロッパ**
- **本標準化フレームワークにより、ユーザのプライバシーを保護し、関連するデータ保護規制に準拠しながら、潜在的に感染したユーザを自動的に追跡して通知するシステムの開発や、異なる近接追跡システム間の相互運用性を可能にすることを目指す**

- 1 Duality SecurePlus™ プラットフォーム
- 2 PEPP-PTプロジェクト
- 3 欧のコンタクトトレーシングアプリの動向
- 4 まとめ

まとめ

- 新型コロナウイルスの感染拡大に伴い、世界各国でICTを活用した対策を講じており、一部の事例については、ITUが主催するAI for Good Global Summit Programme 2020（無料のWebセミナー）で紹介されている。
- 接触追跡システムは①ロケーション（GPS）②Bluetooth③①②を併用の3種類。
- ①の事例：Duality SecurePlusプラットフォームはデータを暗号化したままやりとりでき、位置情報を提供するプロバイダに個人情報が開示されないことが特徴。アメリカ国防総省も多額の資金提供しており、業界国際標準コンソーシアムで検討されている。②の事例：PEPP-PTは、EUのGDPRに準拠したプライバシー侵害に配慮したシステムで、15分以上接触した相手を端末内に登録し、感染すると相手に通知される。
- PEPP-PTは当初導入を予定していたドイツが断念、スイスは別の仕組みを開発するなど検討しているのはフランスのみ、EUでは足並みが揃わず結果的にAGFを採用する国が多くなりそう。

ウィルスは国境を関係なく危機をもたらし、COVID-19対応にも国境はない。グローバルな視点でICTを活用した取り組みを推進する必要がある。

- **国際標準等国際協調・議論の場への参加**

PEPP-PTプロジェクト、準同型暗号型国際標準コンソーシアム、ETSIの標準化フレームワークの検討は**全て欧米が主導**し、彼らにとって有利な方向に議論が進むことが懸念される。ITUの関連の会合や、準同型暗号型国際標準コンソーシアム、ETSIのISG E4P等**各国が議論する場に日本企業やアカデミアが参加**する必要があるのではないか。

- **接触追跡アプリの早期実用化**

コロナとの闘いが長期化する中で、**接触・追跡アプリを導入することは適切な予防と対策を講じるために重要な手段**である。内閣府テックチームの専門家会議でAGFを前提としたアプリの導入が議論されているが、プライバシーの保護に配慮した仕組みであることを検証した上で、国民に誤解を与えないよう安全な仕組みであることに十分な理解を得ながら、早期導入が必要である。

本スライド内に出典の記載がないものはAI for Good Global Summitからの引用であるが、本日紹介したプロジェクトやサービスの最新の状況等については海外の様々なメディアを調査し追記した。全て書き切れないため省いているがソースが気になる方は連絡をいただきたい。

その他、サミットのプログラムについて興味のある方は問い合わせください。

■ 問い合わせ先

TTC企画担当 金子 kaneko@s.ttc.or.jp



■ AI for Good Global Summit関連

- 2020年度のProgramme（日々更新中）
<https://aiforgood.itu.int/programme-2020/>
- スタートアップ募集中（～6/30）！
<https://aiforgood.itu.int/start-up-and-ideas-application-form/>
- Webinar企画募集
<https://aiforgood.itu.int/webinar-proposal/>