【講演レポート】JIPDEC連続ミニウェビナー
「ポストコロナのデータプライバシー　社会実装に向けて」（第2回）

ドイツにおける感染者追跡アプリに関する議論とGDPRへの対応

株式会社Enobyte　代表取締役
Dr. Hermann Gumpp氏

追跡の仕組み

新型コロナウイルス感染追跡アプリ（以下、コロナアプリ）に関しては、現在（2020年5月21日時点）、様々な議論・開発が行われ、状況も刻々と変化しているため、ここでは基本的な追跡の仕組みだけを説明します。

日本も含め、すでにいくつかの国で様々なアプローチでコロナアプリの開発・実用化が進められていますが、いずれの仕組みにも共通する4つの重要なデータポイント（個人と他の人に対する距離、そこにいた日時と期間、誰がコロナに感染したか、その一人一人を追跡するためのID）があります。このアプリの目的は感染拡大防止なので、アプリは１）誰が誰の近くにいつ、どのくらいいたか、２）誰かがコロナに感染したらどうやって近くにいた人に警告を送るか、３）よりセンシティブな情報を含む個人のIDをどのように守るか、について処理する必要があります。

ドイツでは、アプリはスマホの近距離無線通信Bluetoothを使い、一定時間近距離にあったスマホ端末のIDを登録します。アプリ利用者が咳・発熱等の症状が出て医療機関を受診し新型コロナ感染が確認されると、感染者に対し暗号が与えられ、その暗号をアプリに登録すると、接触が記録されていた他の端末に「新型コロナ感染者と接触したので、感染の可能性がある」と接触者への注意喚起が行われます。ここで使用される端末のIDは個人プライバシーのために仮名化されます。

集中型vs分散型

ドイツでは、集中型か分散型、どちらのアプローチにするかという議論がありました。この２つのプライバシーへの影響の違いを説明したいと思います。

ドイツのコロナアプリはまだ完成していません。当初、ドイツでは集中型システム（PEPP-PT）を支持していましたが、４月、セキュリティの観点から分散型アプローチのシステム（DP-3T）に切り替えることになりました。

集中型システムのコロナアプリでは、アプリが取得したデータはすべて中央サーバに送られ、その後仮名化処理や各種処理が行われるため、ハッカーやその他障害によりデータ漏えいが発生すると、アプリ利用者のデータプライバシーが侵害されます。また中央サーバに障害が発生すれば、アプリそのものが機能しなくなってしまいます。

一方、分散型システムでは、アプリの中でデータの仮名化も行われるため、データセキュリティは向上します。現在ドイツでは、アイデンティティを遡って調べられないようにするため、仮名化を30分毎に変更することが提案されています。また、分散型では感染者データのみが中央サーバに送られ、それをもとに仮名化されたIDパターンが配信され、一定期間にそのIDの近くにいた人たちに注意喚起するため、接触機会のなかった人たちのデータは集積されません。中央サーバで持つデータは最小限となるた

め、データ侵害リスクが低く、中央サーバに障害が起きてもアプリそのものは機能します。ただし、分散型においても感染の可能性が高いというセンシティブな情報が中央サーバに蓄積されるので、リスクは存在します。

GDPRからの観点

2016年にEUでGDPRが成立し、無責任なクラウドコンピューティングの時代は終わりました。ITが企業の基礎といっても過言ではない現代社会において、企業や政府はデータ処理を行う責任を取り、データ主体である個人に説明しなければなりません。

また、インターネット、ビッグデータ、AI、IoTがもたらす利益は非常に大きなものですが、そのリスクに対しても目を向けなくてはなりません。ミュンヘン再保険の研究論文によれば、企業にとってサイバー犯罪リスクは債務リスクに次いで2番目に大きいそうですが、それに対する規制がこれまでほとんどありませんでした。そういう点で、GDPRは非常に重要な法律です。

コロナアプリの集中型アプローチと分散型アプローチを、GDPRの観点から見ると、

- GDPR第5条1(c)　個人データの最小化の点からは分散型アプローチの方が有利
- GDPR第25条　データ保護バイデザインおよびデータ保護バイデフォルトの点からも、分散型アプローチの方が適切

と整理することができます。

リスクとメリットの評価

コロナアプリのようにセンシティブ情報を収集する場合は、リスクとメリットをしっかり評価する必要があります。コロナアプリが効果的であれば、ハイリスクなデータの取り扱いも許容されます。しかし、オックスフォード大学ビッグデータ研究所の研究では、全国民の56%がアプリを使用しないとあまり効果が得られないという結果があります。また、先週ドイツで行われたアンケート調査では、アプリを使いたいという回答は44%に留まっています。

ただ、新しい技術に関しては、「危ないから使わない」ではなく、「安全に活用するための方法を議論する」ことが本来の健全的な姿だと思います。ドイツのコロナアプリも、潜在的リスクと安全に使用するための方法をしっかりと調査しながら改善されることを望んでいます。

ドイツのカオスコンピュータクラブ（CCC）は、コロナアプリに完全性を求めるのではなく、社会的および技術的に容認されるために最低限達成されなければならない条件を提言しています。

I　社会的要件（1.疫学的意義と目的適合性、2.任意性と差別の排除、3.基本的プライバシー、4.透明性と検証可能性）

II　技術的要件（5.中央への依存の排除、6.データの最小化、7.匿名性、8.移動および接触プロファイルを中央で構築することの禁止、9.unlinkability、10.通信の観察不能性）

参考資料：https://www.enobyte.com/ja/news/ccc-corona-app/

コロナアプリを入れるスマホは、小型ですがスーパーコンピューター並の計算力を持ち、カメラやマイク、WiFi、Bluetooth、RFID、GPS、運動センサ等複数のセンサを装備して、インターネットに接続しています。サイバーセキュリティの観点では、このような複雑なプラットフォームを使用すると、デ

ータ漏えいのリスクはとても高くなります。特に健康データはセンシティブなデータなので、しっかりとしたサイバーセキュリティが必要です。

現在、コロナアプリについてはAppleとGoogleの共同プロジェクトが分散型システムでAndroid用およびiOS用APIを開発し、アプリ開発者にそのAPIと開発キットを提供しています。iOS（13.5）にコロナAPIがあります。基本的にオフになっていて、ユーザーが同意の上オンにして使用することになります。

まとめ

これまでの内容を簡単にまとめると3つのポイントがあります。

・ 集中型は危ないので、分散型システムの方が有利
・ コロナアプリは厳しいGDPR上でも可能だが、しっかりとした技術的および組織的対策が不可欠。
・ ドイツではユーザー数が少ない可能性があるので影響はあまりないと思われる。

すべてのアプリは必ずしも安全ではないので、インストールの際は注意が必要です。利便性の裏には必ず落とし穴があります。無料アプリというものはなく、お金で払わないということは自分のデータで払うということです。今もあなたが使ってるアプリの中にトラッキングが仕組まれていて、あなたの大事な情報が盗まれている可能性があります。ただ、そのことにはほとんどの人が気にしていません。人気アプリの付録としてコロナ追跡アプリをつければいつのまにか普及するかもしれません。皆様はどうお考えになりますか？

株式会社Enobyte　代表取締役（CEO）　Dr. Hermann Gumpp氏
•日独産業協会ITワーキンググループ議長
•バイエルン州独日協会ボードメンバー
•JETRO中小企業海外展開現地支援プラットフォームにおいて日本企業の技術導入アドバイザーとして、データ保護のITソルーションズを共同開発中
•東京国立情報学研究所での研究開発経験あり
•Enobyte GmbHでCEOとして企業の一般データ保護規則(GDPR)対応をサポートするGDPR Toolboxを開発中

本内容は、2020年5月21日に開催されたJIPDEC連続ミニウェビナー「ポストコロナのデータプライバシー社会実装に向けて」「第2回　ドイツにおける感染者追跡アプリに関する議論とGDPRへの対応」の講演内容を取りまとめたものです。