
位置情報等のプライバシー情報の利活用モデル実証事業 －報告書の概要－

2019年3月

株式会社野村総合研究所

内容

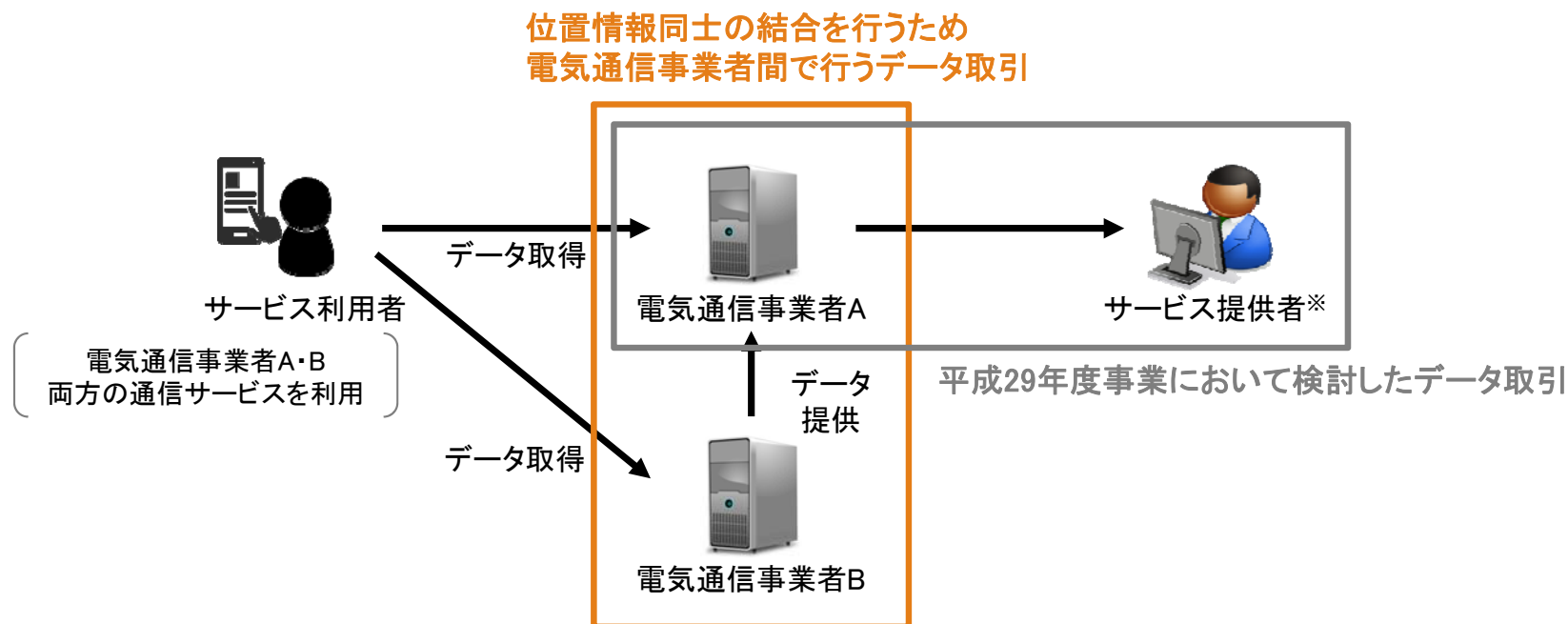
1. 事業の趣旨
2. 実施概要
3. 検討項目
 - ① 国内外におけるパーソナルデータ活用に係るプライバシー保護に関する調査・分析
 - ② 複数事業者間のデータ流通を前提とするモデルケースによる実証
 - ③ その他IoTの進展に伴う新たなプライバシー上の課題
4. 契約書サンプルの改定

1. 事業の趣旨

データの利活用とプライバシー保護の両立を目的に、平成30年度は、電気通信事業者間で行う位置情報等に係るデータ取引を円滑に進めるための検討を実施した。

- データの利活用とプライバシー保護の両立を目的に、位置情報等のプライバシー情報について、本人関与や、データ流通に係る情報の権限、データの管理責任に関する関係者間の責任分担等について平成29年度から継続的に検証してきた。
- 平成30年度は、電気通信事業者が取り扱う位置情報について、複数事業者間における位置情報の共有・提供時のルール、すなわち、電気通信事業者が電気通信役務を提供する中で取得した位置情報等を別の電気通信事業者第三者提供して、提供を受けた事業者が自ら取得した位置情報と結合して、活用するデータ取引を想定し、検討を実施した。
- 事業の実施にあたっては、本事業の理念、社会的価値に共感する事業者の協力を得ながら検討を進めた。

本事業の検討対象としたデータ取引



2. 実施概要

検討は有識者・事業者により構成される協議会を設置して実施した。

1. 検討項目

- ① 国内外におけるパーソナルデータ活用に係るプライバシー保護に関する調査・分析
- ② 複数事業者間のデータ流通を前提とするモデルケースによる実証
- ③ その他IoTの進展に伴う新たなプライバシー上の課題

2. 協議会の設置

- 個人情報保護・通信の秘密を専門分野とする有識者及び情報セキュリティを専門分野とする有識者8名を委員として、個人情報保護委員会事務局、電気通信事業者、関連団体及びモデル実証協力事業者をオブザーバとして、協議会を設置し、4回会議を開催した。

協議会の構成

<委員> ◎は主査

◎森 亮二	英知法律事務所 弁護士
井上 由里子	一橋大学大学院国際企業戦略研究科 教授
木村 たま代	主婦連合会
佐藤 一郎	国立情報学研究所 副所長／教授
高橋 克巳	NTTセキュアプラットフォーム研究所 主席研究員
寺田 眞治	慶應義塾大学SFC研究所上席所員／ 一般社団法人 モバイルコンテンツフォーラム 常務理事
疋田 敏朗	トヨタIT開発センター シニアリサーチャー
山本 龍彦	慶應義塾大学法科大学院 教授

<オブザーバ>

個人情報保護委員会事務局
一般社団法人電気通信事業者協会
一般財団法人日本データ通信協会
株式会社NTTドコモ
KDDI株式会社
ソフトバンク株式会社
エヌ・ティ・ティ・ブロードバンドプラットフォーム株式会社
株式会社ワイヤ・アンド・ワイヤレス
三井不動産株式会社
小田急電鉄株式会社

<事務局>

総務省総合通信基盤局電気通信事業部消費者行政第二課
株式会社野村総合研究所

3. 検討項目 ①国内外におけるパーソナルデータ活用に係るプライバシー保護に関する調査・分析

国内外におけるプライバシー保護に関するルールを調査し、電気通信事業者間のデータ取引を実施するにあたり、参考とすることが考えられる箇所を確認した。

- 文献調査の結果、電気通信事業者間の契約を検討するにあたり、経済産業省「AI・データの利用に関する契約ガイドライン」において示された、データ提供型契約において検討することが望ましい事項について参照することが考えられることが確認された。

調査対象文献

国	法令・政策文書等	概要	主な調査のポイント
EU	ePrivacy規則(案) ※2018年9月時点修正案	EEA※内で共通的に適用される電気通信分野におけるプライバシー保護法。	<ul style="list-style-type: none"> ・ 位置情報の取扱い ・ IoTデータの取扱い
米国	カリフォルニア州消費者プライバシー法(CaCPA: The California Consumer Privacy Act)	米国カリフォルニア州で成立した消費者を対象とするプライバシー保護法。州法ではあるものの、全米や米国外にも影響がある。	<ul style="list-style-type: none"> ・ 位置情報の取扱い ・ 消費者からの開示請求・利用停止の申出対応ルール
韓国	情報通信網法及び同法に紐づくガイドライン	韓国の情報通信サービス全般について個人情報保護などを規定する法であり、個人情報非識別措置ガイドラインなどが紐づく。	<ul style="list-style-type: none"> ・ 規制対象 ・ 事業者間のデータ提供についての契約書の規定
韓国	位置情報保護法	位置情報の収集、利用に関する個別法。	<ul style="list-style-type: none"> ・ 位置情報の取扱い ・ 規制対象
EU	Communication towards a common European data space	B2Bにおけるデータ共有の在り方等について、欧州委員会がデジタル単一市場戦略で示した政策文書。	<ul style="list-style-type: none"> ・ 非個人データの契約取引における重要原則
日本	経済産業省 AI・データの利用に関する契約ガイドライン	データ利用に係るB2B間の契約上の考慮要素を提示。	<ul style="list-style-type: none"> ・ 事業者間のデータの権限の考え方 ・ 責任分担

契約書サンプルの改定を行うにあたり 追記・参照が考えられる箇所(オレンジの網掛け)

経済産業省 ガイドライン データ提供型契約	平成29年度事業において 作成した契約書サンプル
(1) データ等の定義	1条 用語の定義
(2) 提供データの内容・提供方法	2条 対象とするデータの特定 3条 データの提供等
(3) 提供データの利用許諾等	4条 データの利用目的に係る制限 5条 データの識別行為の禁止
(4) 対価・支払条件	
(5) 提供データの非保証	
(6) 責任の制限等	6条 第三者提供に係る制限
(7) 利用状況	8条 安全管理措置
(8) 提供データの管理	8条 安全管理措置
(9) 損害軽減義務	
(10) 秘密保持義務	13条 秘密保持
(11) 派生データ等の取扱い	
(12)有効期間	16条 契約期間
(13) 不可抗力免責	
(14) 解除	
(15) 契約終了後の措置	7条 データの保存期間・消去
(16) 反社会的勢力の排除	
(17) 残存条項	
(18) 権利義務の譲渡禁止	
(19) 完全条項	
(20) 準拠法	
(21) 紛争解決	18条 合意管轄

3. 検討項目 ②複数事業者間のデータ流通を前提とするモデルケースによる実証

複数の電気通信事業者が位置情報を連携・結合して活用する具体的なモデルケースを設定して消費者の受容性等を検証した。

- 本事業における位置情報の連携とは、第三者提供を意味する。
- また、位置情報の結合とは、同一の消費者に係る位置情報を複数の電気通信事業者が取得し、一方が他方にデータを提供し、他方において、提供を受けた位置情報と自身が取得した位置情報とを識別子を共通キーにして、同一のサービス利用者に係る位置情報として取り扱うことを指す。

位置情報同士の結合イメージ

例) 商業施設と駅において提供されるWi-Fiサービスを通じて取得された位置情報

識別子を共通キーに位置情報同士を結合する

Wi-Fiエリア	時間	識別子	識別子	Wi-Fiエリア	時間
ショップA	14:15:53	7a-bb-2d-51-43-11	7a-bb-2d-51-43-11	駅 #1	12:04:01
ショップA	14:15:56	c6-28-66-35-0c-97	8c-cd-11-a7-18-ec	駅 #2	12:04:06
ショップB	14:15:59	d8-88-23-a0-01-87	1c-8a-c9-21-5d-57	駅 #2	12:04:11
ショップB	14:16:00	d6-ad-33-46-43-91	c6-28-66-35-0c-97	駅 #2	12:04:18
モール入口	14:16:25	8e-25-56-62-4a-9a	1b-2b-86-73-15-dd	駅 #1	12:04:30
ショップB	14:16:34	3e-6e-82-ae-7d-d3	3e-6e-82-ae-7d-d3	駅 #1	12:04:32
ショップA	14:16:41	83-21-a3-5d-4d-d2	8e-cd-11-a7-18-ec	駅 #1	12:04:06
ショップA	14:16:50	c0-44-0e-da-0a-98	1c-8a-c9-21-5d-57	駅 #2	12:04:11
モール入口	14:17:07	8e-cd-11-a7-18-ec	8e-cd-11-a7-18-ec	駅 #1	12:04:06
モール入口	14:17:16	c6-28-66-35-0c-97	c6-28-66-35-0c-97	駅 #2	12:04:18
モール入口	14:17:29	5a-34-90-26-a1-27	c6-28-66-35-0c-97	駅 #1	12:04:18

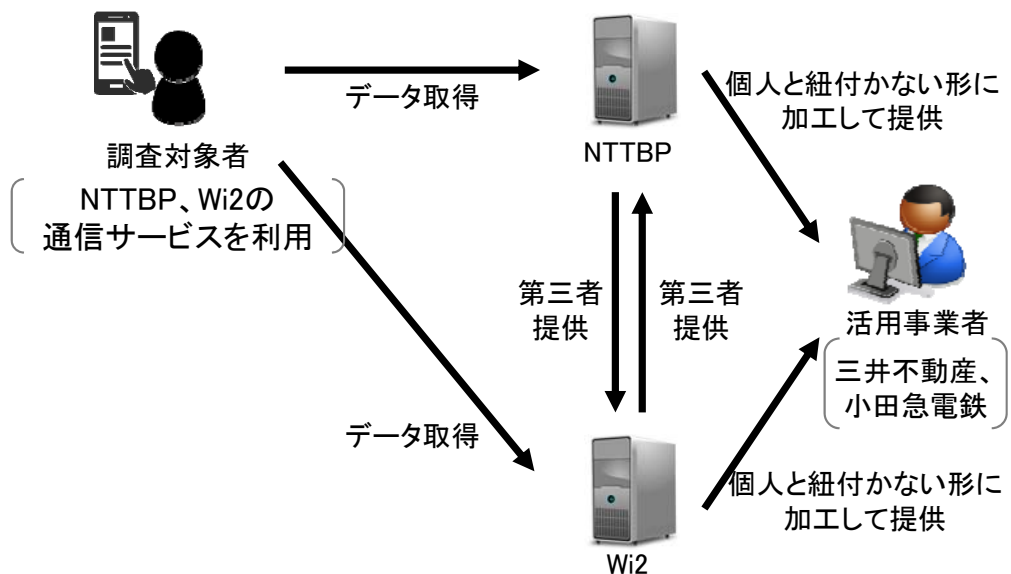
識別子	時間	Wi-Fiエリア	時間	Wi-Fiエリア
7a-bb-2d-51-43-11	12:04:01	駅 #1	14:15:53	ショップA
c6-28-66-35-0c-97	12:04:18	駅 #2	14:15:56	ショップA
3e-6e-82-ae-7d-d3	12:04:32	駅 #1	14:16:34	ショップB
8e-cd-11-a7-18-ec	12:04:06	駅 #1	14:17:07	モール入口
c6-28-66-35-0c-97	12:04:18	駅 #2	14:17:16	モール入口

3. 検討項目 ②複数事業者間のデータ流通を前提とするモデルケースによる実証

モデルケース(実証実験)の概要

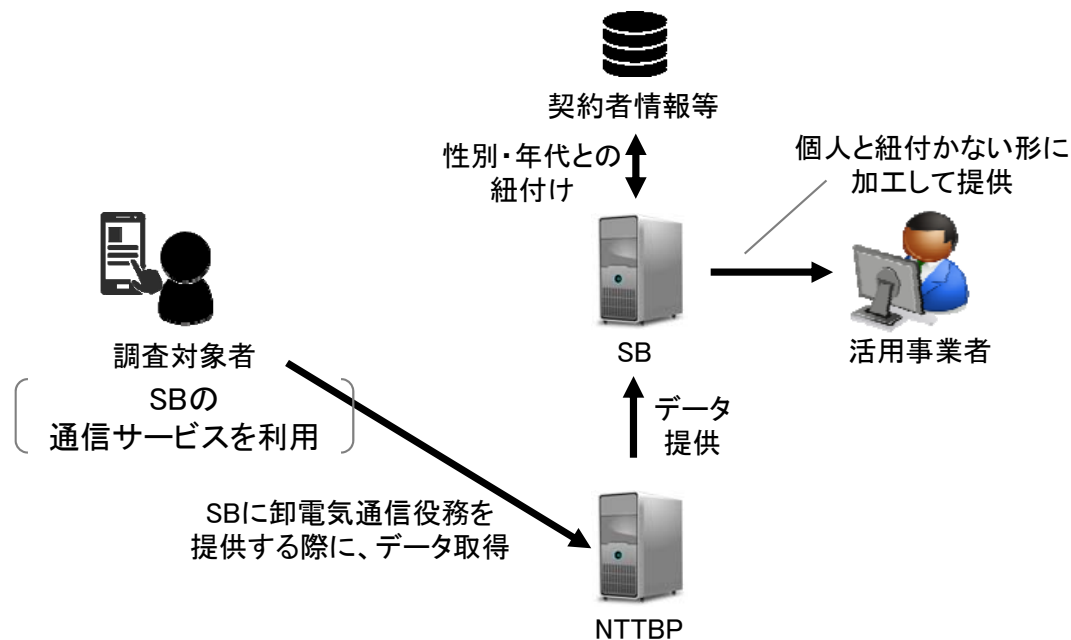
ケース1 第三者提供を受けた位置情報の活用

※ 契約者情報との紐付けは行わない



- 調査対象者はエヌ・ティ・ティ・ブロードバンドプラットフォーム株式会社（以下「NTTBP」という。）及び株式会社ワイヤ・アンド・ワイヤレス（以下「Wi2」という。）のWi-Fiサービスを利用する。
- Wi-Fiサービスの提供を通じて、調査対象者の位置情報を取得した2社は取得した位置情報を互いに第三者提供し合い、自社で取得した位置情報と第三者提供を受けた位置情報とを結合して、調査対象者に関する、より広範囲※の位置情報を把握する。結合した位置情報は個人と紐付かない形に加工を行った上で、施設や交通機関の利用状況を分析する目的で活用する。
- なお、位置情報の連携、結合にあたっては秘密計算と呼称される先端技術も併用して、その有用性を検証した。

ケース2 卸電気通信役務の提供元から受領した位置情報を契約者情報(性別・年代)と紐付けた活用



- 調査対象者はソフトバンク株式会社（以下「SB」という。）の契約者である。SBがNTTBPから卸電気通信役務の提供を受けてWi-Fiサービスを提供している範囲※において、調査対象者がSBのWi-Fiサービスを利用した際、NTTBPが取得した調査対象者の位置情報をSBに提供し、SBにおいて契約者情報(性別・年代)と紐付けを行った上で、個人と紐付かない形に加工し、交通機関の利用状況を分析する目的で活用する。

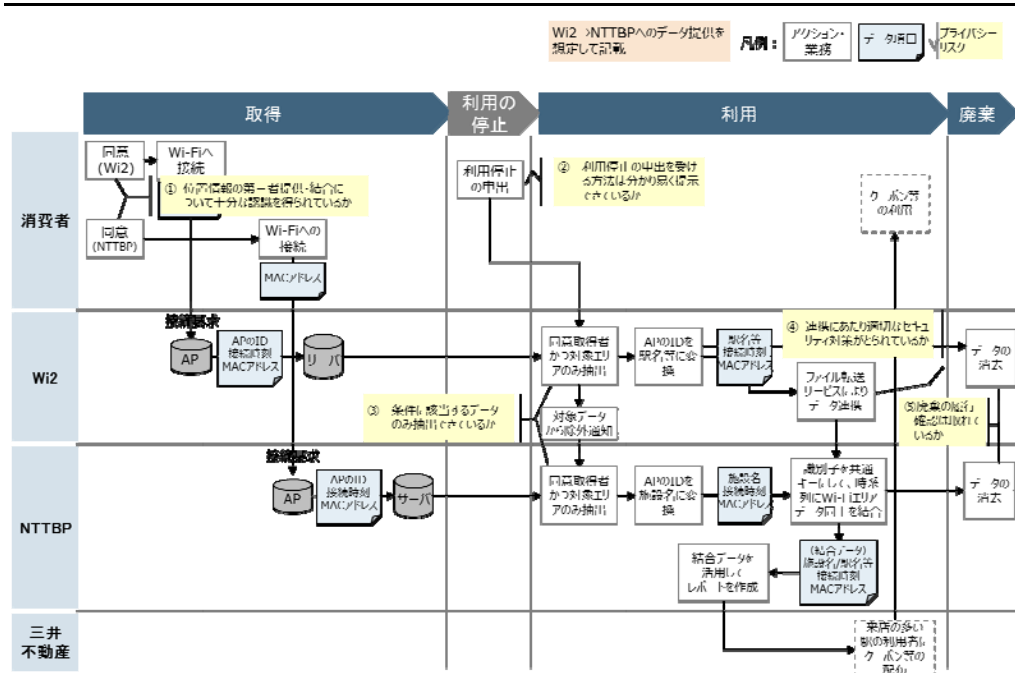
※ 本実証の対象エリアに限る

3. 検討項目 ②複数事業者間のデータ流通を前提とするモデルケースによる実証

モデルケースで想定する各データフローにおいて、プライバシーリスクの所在を特定し、本事業における対応内容と一般化を検討する際の対応方針・課題を整理した。

- 本実証では、調査対象者の対象エリアにおける位置情報を複数の電気通信事業者が取得し、取得した位置情報を電気通信事業者間で連携・結合した。
- 位置情報に含まれるデータ項目及び各項目の形式は、本実証に協力した電気通信事業者間で特に大きな差異がなかったため、技術的な理由により結合できないデータは生じなかった。
- 協議会では委員から、連携する位置情報についてハッシュ化※1することは、データ形式が揃い、結合がし易くなるだけでなく、より安全管理措置に配慮した処理を行うことに資する点で望ましいとの意見があった。

データフローと所在するプライバシーリスク(ケース1)※2



プライバシーリスクの詳細と対応方針(ケース1)※2

リスクの所在するアクション・業務	プライバシーリスク	対応方針 (上段：本実証実験における対応 下段：一般化する際の対応・課題)
取得	Wi-Fiサービスの利用に関する消費者の同意	① 位置情報を他の電気通信事業者に第三者提供し、提供を受けた事業者が自身で取得した位置情報と結合して活用することについて、消費者が十分に認識できているか。 ③ モデルケースの内容の表示に基づいて、説明を実施。受容性調査回答者の約9割は認識できると回答した。 ✓ 説明内容の理解はできるが、多くの消費者が詳細な利用規約を常に確認していないと思われる点は課題と考える。
利用の停止	消費者からの利用停止の申出	② 消費者に対して、利用停止の申出を受けやすい方法が示されているか。 ✓ 調査対象者のリコレーティングを行った調査会社（マコミ社）が窓口となる旨を示して対応した。 ✓ データを取得する電気通信事業者が対応する必要があると考えられる。申出を受けた事業者が、データの提供先に当該消費者の識別子等の情報を伝え、提供先でも同様に利用を停止する対応が必要になる。
利用	同意取得者が対象エリアのみのデータ抽出	③ 位置情報のログデータから、対象エリアの同意取得者のデータのみを抽出し、非対象のデータ（エリア、同意未取得者）のデータが混入することはないか。 ✓ 同意取得者のリストを事前に作成し、2社間で共有してデータ抽出した。 ✓ データの取得を行う電気通信事業者は、自社のサービスを利用する消費者がデータの連携・結合に同意しているか、峻別するリスト等を整備する必要がある。
	他の電気通信事業者へのデータの第三者提供	④ 他の電気通信事業者にデータを提供する際に、適切なセキュリティ対策を講じているか？ ✓ 自社で規定する情報セキュリティ対策に則り、ファイル転送サービスを利用して、データを提供した。 ✓ 提供するデータ量等に応じて、適切なセキュリティ対策が講じられるデータ提供手段（専用線等）を利用することが考えられる。
廃棄	利用目的の達成や消費者からの申出に基づくデータの消去	⑤ データの提供先においてデータを消去したことが担保できるか。 ✓ 本事業終了後にデータは各社が消去し、その旨事務局が報告を受ける。 ✓ データの消去を履行した旨の書面等をデータの提供元に提出等の方法が必要になると考えられる。

※1 ハッシュ化とは、元のデータから一定の計算手順や関数にしたがって「ハッシュ値」と呼ばれる規則性のない固定長の計算結果を得て、元のデータとハッシュ値を置き換えることを指す

※2 ケース1において秘密計算を実施した場合及びケース2については報告書を参照のこと

3. 検討項目 ②複数事業者間のデータ流通を前提とするモデルケースによる実証

位置情報を連携・結合して活用するビジネスモデルに対する受容性及びそうしたビジネスを行う際に消費者に対し通知・同意取得する方法について確認した。

ビジネスモデルに対する消費者の受容性

- 位置情報を連携・結合して活用するビジネスモデルに対して、消費者の受容性は一定程度認められる。本調査ではDM・クーポンの配布、案内等の複数の位置情報を活用したサービスを想定して、質問を実施した。いずれのサービスについても3～6割のアンケート回答者がサービス提供のための位置情報を活用してもよいと思うと回答した(下図)。
- 他方で、調査対象者のリクルーティングにあたっては、当初、目標数を獲得することが難しかったことから、その背景には、位置情報の取得・活用全般に関し、消費者の受容性が必ずしも高くはない状況があることが考えられる。そこで、受容性については、限定されたエリアとはいえ、一定期間位置情報を提供することに対して、忌避感のある消費者がいることを踏まえつつ、解釈すべきとの意見が委員から指摘された。

■ 下記のようなサービスの提供を受けられる場合、各施設で提供されているWi-Fiサービスを通じて取得された位置情報を事業者間で共有して、活用してもよいと感じますが、最もあてはまるものをお答えください。

設問番号	サービス(ビジネスモデル)概要	消費者の受容性
#10	ある商業施設において特定の地域からの来訪客が多いと判定し、場合、同じ地域に住む人に商業施設で使えるクーポンを配布します。	1% 39% 50% 10% N=431
#11	洋服を売るショップAと化粧品を売るショップBの両方を訪れる客が多いと判明し、場合、ショップAの利用客にショップBのセールのお知らせを配布します。	2% 35% 47% 16% N=431
#12	災害や突発的な事故の発生時に鉄道やバスなど事業のエリアを越え、車両の混雑状況や振替輸送を待つ人の状況を駅のディスプレイやあなたのスマートフォン等で表示します。	0% 59% 36% 4% N=431
#13	C駅で降車した人は高確率でショップDを訪問していることが判明した場合、あなたがC駅で降車した際、あなたのスマートフォンにショップDの案内が表示されます。	4% 30% 45% 22% N=431

■ 活用してもよいと思う ■ あまり活用してもよいと思う ■ あまり活用してもよいとは思わない ■ 活用してもよいとは思わない

消費者に対し通知・同意取得する方法

- 位置情報を他の電気通信事業者第三者提供し、データ同士を結合することについて、利用規約等を通じた説明により大部分の消費者は認識することができる。本実証における説明表示※について、約9割の調査回答者が認識できると回答した。
- ただし、多くの消費者が詳細な利用規約を常に確認していないと思われる点は課題と考える。

本実証における通知内容(ケース1)※

実証実験 参加のご案内

本調査は、データの自由な流通とプライバシー保護の両立を目的に、スマートフォン等から取得される位置情報の活用を検証する総務省の調査事業です。

■ 調査期間中、対象エリア(①)でWi-Fiサービスを利用された場合、調査の協力事業者(②)があなたのスマートフォンに関する位置情報(③)を取得します。

①対象エリア	②調査の協力事業者	③取得する位置情報の内容
<ul style="list-style-type: none"> ・ ららぽーと海老名※、ららぽーと横浜 ・ 小田急線、相鉄線の駅構内 	<ul style="list-style-type: none"> ・ NTTブロードバンドプラットフォーム ・ ワイヤードワイヤレス 	<ul style="list-style-type: none"> ・ Wi-Fi後利用した施設名、駅名(位置情報) ・ 利用したスマートフォンの端末ID(MACアドレス) ・ Wi-Fiの利用時刻

※「ららぽーと海老名」では、周辺施設の「ピナウォーク」でも同様に位置情報を取得する可能性があります

■ 取得した位置情報は協力事業者間で共有し、個人と紐づかない形に加工した上で、施設や交通機関の利用状況を分析する目的で活用します。

加工後のデータ例)

12/10(月) ららぽーと海老名 訪問者20人 訪問者の経路(小田急線 町田-海老名15人、厚木-海老名5人)

- なお、加工方法の1つとしてデータを暗号化したまま計算する技術(学術的には秘密計算と呼ばれるもの)を採用します。
- 取得した位置情報は本事業終了(2019年3月末終了予定)後、速やかに消去します。
- 一度、調査協力の表明をいただいた後、調査から離脱される場合は、マクロミルアンケート事務局までご連絡ください。離脱表明された方のデータは分析実施前に限り、分析対象から除外いたします。

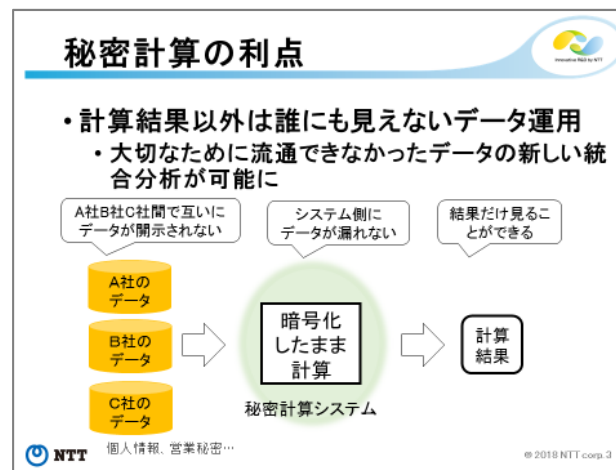
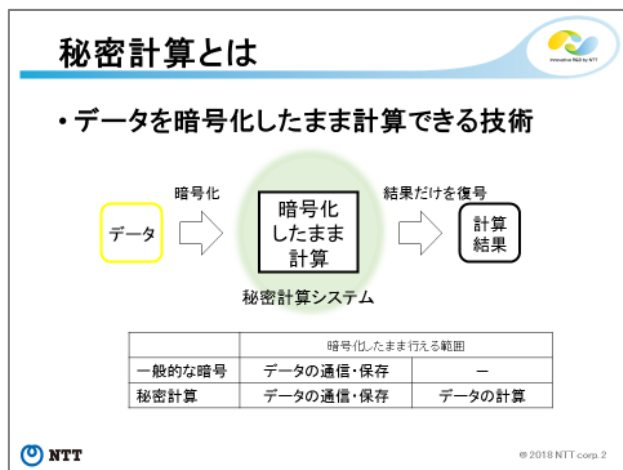
※ 上記の通知内容を調査対象者のスマートフォンに表示して通知したスマートフォン画面上での表示状況の詳細は報告書を参照のこと

3. 検討項目 ③その他IoTの進展に伴う新たなプライバシー上の課題

位置情報のプライバシー保護を目的に、 安全管理措置に係る先端データ分析技術の有効性の検証を行った。

■ 検証技術の概要

- 暗号化したままデータ分析を可能とする秘密計算について検証を行った。
- 本事業では、NTTセキュアプラットフォーム研究所の協力の下、ISO/IEC 19592-2に基づく秘密分散をデータ形式とする秘密計算を利用した。



(出所) 日本電信電話株式会社 NTTセキュアプラットフォーム研究所 「秘密計算のシステムとその原理」

■ 本事業における検証結果

- 秘密計算を用いて、位置情報を連携・結合するデータ処理を行うことが確認できた。
- 同処理で、データは秘密分散で暗号化されているので、データの連携に際し、安全管理措置として有益であることが確認された。
- また、秘密計算データのまま、データの結合、分析を行うため、その過程においてデータ内容が不用意に作業員の目に触れることがなく、データ最小化の観点における貢献も期待される。
- ただし、上記検証結果は本事業において利用した秘密計算について確認されたものであり、秘密計算の安全管理措置に係る有効性は個々の技術に応じて判断されるべき点に留意が必要である。

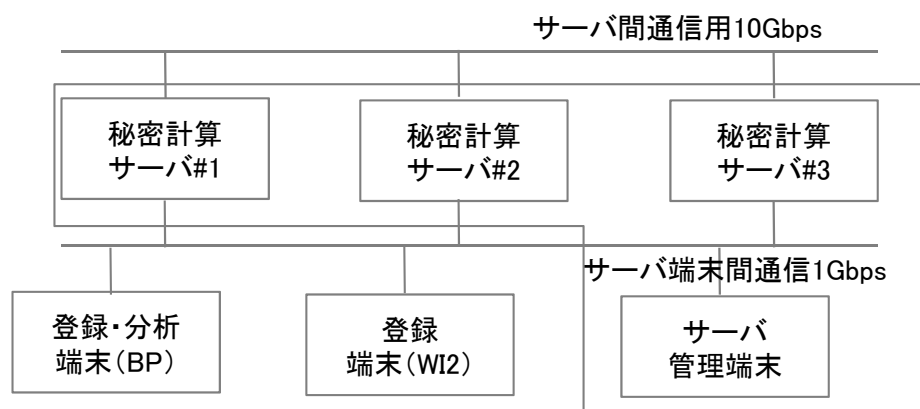
3. 検討項目 ③その他IoTの進展に伴う新たなプライバシー上の課題

秘密計算の実施状況

- 本実証の協力事業者が一般的な表計算ソフトを用いて作業した位置情報に係るデータの集計結果について、秘密計算を用いて同様の集計結果を再現した。
- 以下の実験環境の下、表計算ソフトによる集計結果と同様の結果を得た。処理時間は2.7秒(試行回数5回の平均値)である。
- なお、処理に供したデータは約1.5万レコードである。

実験環境

< システム構成 >



サーバ、登録・分析、サーバ管理端末の環境

OS	RHEL 7.2
CPU	Xenon 4コア 3.5GHz 2ソケット
メモリ	64GB
HDD	SSD 200GB
NW	10Gbps(サーバ間)

登録・分析/サーバ管理端末の環境

OS	Windows7
CPU	Core I 5 2.3GHz
メモリ	16GB
HDD	450GB
NW	1Gbps

4. 契約書サンプルの改定

本事業における検討を踏まえ、電気通信事業者が位置情報等に係るデータ取引を行う際に、参考となる契約書サンプルの改定を行った。

- 電気通信事業者が電気通信役務を提供する中で取得した位置情報等を別の事業者第三者提供して、提供を受けた事業者が自ら取得した位置情報と結合して、活用するデータ取引を想定し、契約書サンプルの改定を行った。
- なお、本サンプルは電気通信事業者が扱う位置情報等に係るデータ取引に関する契約を締結する際に、条項として検討される可能性のあるものについて提示するものである。契約書サンプルで提示する条項は、例示であり、想定事例に類似するデータ取引の場合には、適宜修正の上、用いることができる。
- また、卸電気通信役務の卸元から卸先へ位置情報を提供し、卸先が受領した位置情報を契約者情報と紐付けた活用を行うケースについては、サンプルに加えて、報告書記載の留意点についても参考とすることが考えられる。

契約書サンプルの想定するデータ取引

