Vol.2018-DPS-176 No.8
Vol.2018-EIP-81 No.8
2018/9/13

位置情報利用サービスに関する個人情報保護の各国比較

小向太郎[†1]

コンピュータ処理能力の向上とデータ収集可能な情報の増大を背景に，大量のデータが分析・利用されるようになっている．ビッグデータ，IoT，AI といった技術が高度化している要因の一つは情報収集量の爆発的な増加であり，こうした情報のなかで，特に重要視されているものの一つが，位置情報である．位置情報については，それを利用したさまざまなサービスが考えられている．一方で，人の行動と密接に結びついている場合も多く，これらの情報が本人の望まない使われ方をされるとプライバシーや個人情報保護上の問題を生じることが懸念されている．本稿では，こうした位置情報を利用したサービスについて，我が国における法的位置付けや，欧米における保護の動向を比較し，位置情報に関するプライバシー・個人情報保護制度のあり方について検討を行う．

The Comparative Study on Data Protection for Location Data

TARO KOMUKAI[†1]

This paper focuses on data protection for location data, which is one of the essential elements of rapid development of new technologies such as bigdata, IoT and AI. Location data would be a curse to serious privacy concern because it could be collected, used or disclosed while data subject does not recognize it. The aim of this paper is to compare the relevant discussions in the EU, the U.S. and Japan, and reach a suggestion for appropriate solution.

1. 検討対象

最近注目を集めている IoT（Internet of Things）やビッグデータ技術において利用されるデータのなかでも，特に位置情報を含む情報に対する期待は大きく，具体的な利用分野も幅広い．さまざまな機器がネットワークで接続されるようになり，情報が大量に収集処理されることで，従来はあまり意識されなかった POS レジや IC カードリーダによって収集される情報や，監視カメラによって撮影される影像を処理したデータも，位置情報としての意味を持つようになってきている．こうした情報取得には，個別には意識されにくいものも多いということがある．いつどんな情報がとられているか意識されずに，自分についての収集されることが増えており，それをもとにして，さらに情報を生成することも容易になっている．人の行動と密接に結びついている場合も多く，これらの情報が本人の望まない使われ方をされるとプライバシーや個人情報保護上の問題を生じることが懸念されている[1][2]．本報告では，こうした位置情報に関連する制度の各国の近時の動向を比較し，今後の課題を提示する．

2. 個人情報保護制度と位置情報

2.1 日本

位置情報のなかには単独では個人情報に該当しないものもあるが，個人に関連して収集されることも多い．わが国の個人情報法保護法においては，「生存する個人に関する情報であって，当該情報に含まれる氏名，生年月日その他の記述等により特定の個人を識別することができるもの」や「個人識別符号」が含まれている場合や，そうした情報と「容易に照合することができ，それにより特定の個人を識別することができることとなる」場合には，個人情報となる（個人情報保護法 2 条 1 項）．そして，2015 年の法改正によって，個人識別符号を含む情報も個人情報になることが明確化されている．個人情報取扱事業者は取扱う個人情報について，利用できる目的をできる限り特定し（15 条），公表等することと（18 条）その目的の範囲で利用すること（16 条）等が求められる．

†1 日本大学
Nihon University

現行法上は，利用目的を特定・公表して，その範囲で利用するのであれば，本人の同意等は求められていない．ただし，2015 年の法改正によって，「要配慮個人情報」に関する規定が設けられ，「本人の人種，信条，社会的身分， 病歴，犯罪の経歴，犯罪により害を被った事実その他本人に対する不当な差別， 偏見その他の不利益が生じないようにその取扱いに特に配慮を要するものとして 政令で定める記述等が含まれる個人情報（第 2 条第 3 項）の取得には，法令に基づく場合等の正当な理由がある場合を除き，本人の同意が求められることになっている．

個人情報保護法は，個人データ（電子化または体系化された個人情報）の第三者提供には原則として本人の同意が必要であるとしており（23 条），本人の同意がなくても第三者に提供できるのは，法令に基づく場合や緊急性等がある場合（23 条 1 項）のほかに，オプトアウト（23 条 2 項），委託先への提供（23 条 4 項 1 号），事業承継（23 条 4 項 2 号），共同利用（23 条 4 項 3 号）のいずれかに該当する場合に限られる．さらに，2015 年の個人情報保護法改正によって，適正な匿名加工を行うことによって，一定の条件のもとで本人の同意がなく第三者提供等ができる制度が整備されている．

以上のように，通常の個人情報に該当する位置情報については，事業者が自ら収集して利用する場合には，利用目的を特定・公表して，その範囲で利用するのであれば，本人の同意等は求められていない．また，本人が事後的に利用の停止を求めることができるのは，目的外利用や不適正取得がされた場合に限られる（30 条）[3]．

2.2 EU

EU では，1995 年に採択された「個人データ処理に係る個人の保護および当該データの自由な移動に関する欧州議会および理事会の指令（EU 個人データ保護指令）[4]」に基づいて個人情報保護に関する制度が各構成国で整備されてきた．2018 年 5 月には，EU 域内の個人情報保護をさらに確保するために，「個人データの取扱いに係る個人の保護および当該データの自由な移動に関する欧州議会および理事会の規則（GDPR）[5]」が発効している．

GDPR が保護の対象とする個人データは，「識別（identify）された，または識別可能な自然人に関するあらゆる情報」と定義されている．ここでいう識別可能な自然人とは「直接的であるか間接的であるかを問わず特に識別子を参照することで，識別されるもの」をいう．そして，識別子には「名前，識別番号，位置情報，オンライン識別子や，その人物の物理的，生理的，遺伝子的，精神的，経済的，文化的または社会的な固有性として，単独または複数組み合わせによって特定される要素」が該当する（第 4 条（1））．したがって，位置情報を含む情報は，個人データとして GDPR の保護を受ける．

個人データに該当する位置情報を取扱うことができるのは，データ主体（本人）の同意がある場合や，その他の正当化自由がある場合（データ主体との契約の履行等に必要な場合，データ管理者が法的義務を果たすために必要な場合，人の生命に関する利益を保護するために必要な場合，公共の利益や公的な権限の行使のために行われる職務の遂行に必要な場合，legitimate interests の目的のために必要となる場合等）に限られる（第 6 条）．

2.3 米国

米国では，連邦取引委員会（FTC: Federal Trade Commission）が，消費者プライバシーを所轄しており，2012 年 3 月に「急変する時代の消費者プライバシー保護[6]」という報告書を取りまとめている．この報告書が提示するフレームワークでは，本人意思の反映を重視しており，プライバシー・バイ・デザイン，シンプルで分かりやすい消費者の選択，透明性を重要な要素としてあげている．さらに，消費者が自分のデータに関する決定を行うような状況では選択の機会が与えられるべきであり，（1）データが収集される際に示された方法と大きく異なる方法で利用される場合と，（2）ある目的のためにセンシティブ情報を収集する場合には，積極的な同意の表明を得るべきである」としている．そして，「子供に関するデータ，金融情報と健康情報，社会保障番号，および一定の位置情報は，少なくともセンシティブ・データ」として扱うという考えが示されている（47 頁，注 214）．ただし，これらは事業者に対するベストプライティスを示したものであり，執行の指針を直接示したものではない．

一方で，FTC は，FTC 法違反に対する法執行も，積極的に行っている．FTC 法 5 条は「商業活動に関わる不公正な競争手段と，商業活動に関わる不公正または欺瞞的な行為または慣行は，違法であることがここに宣言される（15 U.S.C. § 45(a)(1).）」と規定しており，この規定が執行の根拠となっている．実際に対象となっているのは，自社のプライバシー・ポリシーや利用規約で個人情報の利用を拒否できるかのように記述しているにもかかわらず，対応を十分にしていなかったこと

などが，欺瞞的とされているケースが多い[7].

3. ネットワーク事業者と位置情報

3.1 日本

電気通信事業法は，「電気通信事業者の取扱中に係る通信の秘密」に関して，特別の保護を規定している（第４条，第 179 条）．また，電気通信事業者が取り扱う情報は，通信の秘密に当たらなくてもプライバイシーの保護が必要とされる場合が多いと考えられてきた．総務省「電気通信事業における個人情報保護に関するガイドライン（平成 29 年総務省告示第 297 条）」では，電気通信事業者による個人情報の取得・利用について，次のような考え方を示している．

・個人情報の取得について，できるだけ通信サービスを提要するために必要な場合に限るよう務めなければならず（第 6 条），利用目的を特定する際に，電気通信サービスを提供するため必要な範囲を超えないように努めらければならない（第 4 条第 3 項）
・通信の秘密については，利用者の同意がある場合その他の違法性阻却事由がある場合を除いては，利用してはならない（第 5 条）

携帯電話事業者が取扱う位置情報のなかで，「個別の通信を行った基地局の位置情報」は，通信の秘密であるとされる．通信の秘密として保護される情報としては，通信内容以外に，個別の通信の通信当事者がどこの誰であるかということや，いつ通信を行ったかということも含まれると考えられており，「個別の通信を行った基地局の位置情報」は，こういった情報に該当する．そして，通信の秘密に当たる情報の取得は，電気通信サービスの提供に必要な範囲で利用できるほかは，正当防衛や緊急避難などの違法性阻却事由が認められる場合にのみ許される[8].

携帯電話事業者が取扱う位置情報としては，この他にも「位置登録情報（端末所在地を基地局単位等で把握する情報）」と「GPS 位置情報（GPS 機能により取得する情報）」がある．総務省のガイドラインではこれら「位置登録情報」「GPS 位置情報」についても，「ある人がどこに所在するかということはプライバシーの中でも特に保護の必要性が 高い上に，通信とも密接に関係する事項であるから，通信の秘密に準じて強く保護することが適当である」と位置づけ，情報の取得に際して利用者の同意を取得すること等を求めている．つまり，携帯電話事業者が取扱う位置情報を利用するためには，その他の位置情報（個人情報）とは異なり，利用者の同意が必要となる．

一方で，位置情報の利活用を求める声もあがっており，2017 年に改正された総務省ガイドラインでは，「通信の秘密に係る位置情報について十分な匿名化を行った上で他人への提供その他の利用を行う場合」について，約款等に基づく包括同意でも一定の要件のもとでは有効な同意となりうるという考え方が示されている ．

なお，GPS 情報は，例えばスマホアプリを利用したサービスでも利用されている．これに関しては，総務省が 2012 年 8 月に，「スマートフォン プライバシー イニシアティブ」を公表し，アプリが利用者情報を外部送信したり蓄積したりしている場合には，どのような情報が取得・利用されているかを分かりやすく記述したプライバシー・ポリシーを公表することや，電話帳・位置情報・通信履歴等のプライバシー性の高い情報を取得する際の利用者の同意を取得することを推奨している．ただし，このような取り組みを法的に求めるものではなく，事業者の自主規制を促すものである[2].

3.2 EU

EU では，「個人データの保護および電子通信分野のプライバシー保護に関する欧州議会および理事会の指令（電子通信プライバシー指令）[9]」が 2002 年に採択され，2006 年および 2009 年に改正されている．この指令において位置情報は「電気通信網または電子通信サービスにおいて処理される情報であり，公衆電気通信サービスのユーザ端末機器の地理的な位置を示す情報」と定義され，匿名化されている場合か，（通信サービス以外の）付加価値サービスの提供のために必要な範囲及び期間に関して，利用者が同意をしている場合に限って，処理することができるとされている．サービス提供者は，位置情報の種類，利用目的，処理期間，データの第三者提供の有無について，同意取得に先立って，利用者・加入者に知らせなければならない（第９条第１項）．また，同意が得られている場合には，利用者・加入者に対して，シンプルな手段によって無料で，当該ネットワークへの接続や電子通信の伝送が行われるたびに，これらの情報の処理をいつでも拒否することを常に可能にしておかなければならない（第２項）．付加価値サービスを提供するための権限を付与された者は，当該付加価値サービスの提供目的に必要なものに限られている場合に，

限定されなければならない（第３項）.

電子通信プライバシー指令は，GDPR の成立をうけた改正が検討されており，欧州委員会は，これに代わる規則の提案を，2017 年 1 月 10 日に公表している[10]．この規則提案では，位置情報やトラフィック・データのようなメタデータを取扱うことができるのは，次の場合に限られるとしている（第６条第２項）.

1. EU の法令に基づいて要求されているサービスの品質水準を満たすために必要な場合
2. 電気通信サービスに関する，料金請求，相互接続料金支払いのための計算，詐欺的行為や不正利用の検知と停止，加入等に必要な場合
3. その情報に関する利用者が当該利用者のメタデータを，特定のサービスを当該利用者に提供するなどの特定の目的のために取扱うことについて同意を与えている場合であって，匿名化された情報では目的を達成することが出来ない場合

また，サービス提供や課金等のために必要がなくなった場合に，本人の同意がなければ匿名化か消去をしなければならないとされており（第 7 条第 2 項，第 3 項），ネットワーク側だけでなく，ユーザが利用する端末やそれに関連して保存される情報に関しても保護の規定が置かれている（第 8 条）．また，適用対象を電子メールやオンラインメッセージング・サービスに拡大しており，WhatsApp，Facebook Messenger，Skype，Gmail，iMessage，Viber のような新しい電子通信サービスの提供事業者についても，適用される可能性がある．

3.3 米国

米国の連邦通信法は，「顧客情報のプライバシー」に関する規定を定めており，「全ての電気通信事業者は，他の電気通信事業者（電気通信事業者が提供する通信サービスを再販売する電気通信事業者を含む），機器製造事業者，および顧客に関連する情報であって，これらの者に帰属する情報の秘密を，保護する義務を負う（47 U.S. C. § 222(a)）」とされている．特に，電気通信サービス提供を提供するために取得した CPNI（顧客に帰属するネットワーク情報）は，「(A) そのような情報が生成された電気通信サービス，(B) そのような電気通信サービスの提供に必要であるか，提供の過程で利用されるサービス（電話帳の発行を含む），のいずれかを提供するためである場合」にのみ利用することができる（47 U.S. C. § 222(c)）．ただし，個々の顧客の識別子および特性が当該データから除去した顧客統計情報（「顧客統計情報」とは，「サービスまたは顧客のグループまたは属性に関する集合体のデータであり，個々の顧客の識別子および特性が当該データから除去されているもの」をいう（47 U.S. C. § 222 (h)(2).））は，これらの目的以外にも利用，開示，またはアクセス可能にすることができる．なお，顧客からの要望にも続いて開示する場合も，「顧客からの明示的な書面による要求」が必要である．

特に，商用携帯電話や IP 音声電話の位置情報を利用するための同意については，事前かつ明確に表明される必要があるとしている（47 U.S. C. § 222(f)）．また，商用携帯電話の位置情報については，公共の安全や緊急事態のための必要な場合に利用できることが，例外規定として明示されている（47 U.S. C. § 222(d)）.

電気通信事業者に対する規制を所轄する連邦通信委員会（FCC: Federal Communications Commission）は，2012 年に，「ロケーション・ベースド・サービス[11]」という報告書を公表している．この報告書は，位置情報を利用したサービスの重要性と今後の可能性について検討を行っており，特にプライバシーに対する懸念がこの分野での最重要課題の 1 つであるという認識を示している．そして，ロケーションテストサービスを提供する事業者に，①製品の開発段階開発初期段階でのプライバシーの配慮，②データのセキュリティ，③通知の時期と内容の充実，④データの最小化，といった取り組みを求めている．そして，政府と産業が合意して位置情報利用ビジネスとプライバシーの問題とのバランスを最適化していくべきだとする一方で，FCC としてはあわせて監視も続け，さらに次のステップが必要かどうかについても検討する可能性があることを表明していた（40-41 頁）.

2016 年 10 月 27 日には，ブロードバンドサービスを始めとする電気通信サービスに関する新たなルールとして，「ブロードバンド顧客プライバシー保護規則[12]」が採択されている．従来，BIAS（Broadband Internet Access Service）提供事業者は，通信法の規制を受ける電気通信事業者に当たらないとされてきたが，2015 年に FCC が採択した「オープンインターネット規則」によって，BIAS 提供事業者が通信法による規制を受けることとなり，通信法が定める顧客情報のプライバシー保護の規定（47 U.S.C. § 222.）が，適用されることになったため，それに対応した規則を策定したのである．この規則では，「正確な地理的位置情報」

をセンシティブな情報と位置付け，その利用・提供に際しては「オプトイン」を求めていた．

ISP 等のインターネット・アクセスを提供する事業者に規制対象を広げるこの規制は，Google などのいわゆるプラットフォーム事業者が対象外とされているため，バランスを欠くという批判も強かった．政権交代によってこの規制に反対していた共和党が政権をとったこともあり，前提となる「オープンネットワーク規制」が撤回された．この規則も議会審査法（the Congressional Review Act, 5 U.S.C. §802）に基づく撤廃決議が連邦議会の上下院で可決され，2017 年 4 月 3 日には正式に撤廃されている．

これらによって，FCC のプライバシーに関するルール全体が失効した状態となっていたため，FCC は 2017 年 6 月 29 日に，従来の電気通信事業者に対する 222 条の適用について，従来のルールを復活させるための命令を出している[13]．位置情報に直接関係する規定としては，顧客からの要請に応じて通話詳細情報（これには位置情報が含まれる）を開示する場合に，顧客に提示を求めるパスワードの取扱いを厳格にすべきとするものがある（§64.2010（b））．

4. 今後の課題

以上のように，位置情報の取扱いについては各国で規制の整備や議論が行われている． そして，いずれの国においても，伝統的な電気通信事業と新しく急成長しているネットワーク関連ビジネスにおけるプライバシー保護のギャップが顕在化しつつあるといえる．

従来から，電気通信事業者の取扱う情報は，通信の秘密に代表されるセンシティブなものが多く，どの国でも特別な規制が課せられていることが多い．しかし，EU の電子通信プライバシー指令改正の議論では，位置情報等の保護がネットワーク関連事業者により処理される情報に限定されていることが実情にそぐわないことが指摘され，現在提案されている規則案では保護すべき情報の対象が拡大されている．米国では ISP 等の位置情報について厳格な保護を求める規則が施行に至らず撤廃されているが，この背景にもネットワーク事業者以上に大量の情報を収集しているプラットフォーム事業者との不均衡についての指摘があった．

現在，インターネット上で利用者に関する情報を利用しているのは電気通信事業者だけではなく，プラットフォーム事業者を始めとして様々な事業者が，顧客に関する大量の情報を収集・利用している．

わが国では，現在のところ携帯電話事業者に関する位置情報に関しては厳格な配慮が求められているが，それ以外の分野に関しては，その他の一般の個人情報と同様の保護がされており現在のところあまり議論がされていない．そういう意味では，①どのような事業者が取扱う，②どのような情報に対して，特別な保護が必要になるか，について検討を行う必要性が諸外国と比べても高い状況にあるといえる．

（図表 1）位置情報に関する規制（概要）

	個人情報取扱事業者	ネットワーク事業者	その他
EU	本人の同意または正当化事由（法定の利用，公共の利益，適法な利益等）同意の撤回等を保障	サービス提供や課金等のために必要がなくなった場合の匿名化または消去の義務	ユーザが利用する端末やそれに関連して保存される情報に関しても保護の規定
米国	不公正または欺瞞的な行為または慣行の禁止	法に基づく要請または顧客の同意	FTC レポート（位置情報全般に同意取得を推奨）
日本	利用目的の通知・公表，適正取得，本人同意なき第三者提供の原則禁止等	本人の同意または正当化事由（正当業務行為，緊急避難等）	スマホアプリ事業者に対するガイドライン（同意取得等の推奨）

謝辞

本研究は，電気通信普及財団の研究助成による研究費を得て実施した．

参考文献

[1]小向太郎「ライフログの利活用と法律問題」ジュリスト 1464 号（2014）53-58 頁．
[2]小向太郎「ネットワーク接続機器の位置情報に関するプライバシー・個人情報保護制度の動向」情報処理学会研究報告電子化知的財産・社会基盤（EIP） 2016-EIP-74，2016-11-17.
[3]小向太郎，『情報法入門（第 4 版）デジタル・ネットワークの法律』NTT 出版(2018) 193-218 頁．
[4] 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
[5] Regulation (EU) 2016/679 of the European Parliament and

of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.
[6] FTC, Protecting Consumer Privacy in an Era of Rapid Change (2012).
[7] 小向太郎，「米国 FTC の消費者プライバシーに関する法執行の動向」，堀部政男編『情報通信法制の論点分析』商事法務(2015)151-162 頁.
[8] 多賀谷一照他編著『電気通信事業法逐条解説』（財団法人電気通信振興会，2008）37-41 頁参照.
[9] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.
[10] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications).
[11] FCC Wireless Communications Bureau, Location-Based Services - An overview of opportunities and other considerations, May 2012.
[12] FCC, Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, Report & Order, FCC16-148 (2016), https://apps.fcc.gov/edocs_public/attachmatch/FCC-16-148A1.pdf.
[13]FCC, Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, FCC17-82 (2017).