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

研究代表者　　小　向　太　郎　　日本大学危機管理学部教授

1 はじめに

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は、一つはコンピュータ処理能力の向上である。しかし、高度な処理能力も利用できる情報があってこそ役に立つ。つまり、もう一つの要因は、情報収集量の爆発的な増加である。スマートフォンに代表される携帯端末は、持ち主の行く先々でネットワークにアクセスしている。そして、各種センサーが内蔵されており、様々な情報を取得可能である。SNS では利用者が大量の情報を発信しており、インターネット上にこれらの情報が蓄えられている[1]。自動車の情報化も進展が著しく、カーナビや制御装置がネットワークに接続しつつある。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。例えば、都市計画に利用して、交通システムを最適化したり、防災時の避難経路を補強したりすることも可能になる。日常的に、公共交通機関の混雑状況や渋滞情報など、便利な情報の提供にも役に立つ。さらに、目的地への経路情報や地域案内、障害者等への移動支援のような行動支援型サービスにも、位置情報が不可欠である。犯罪やテロの予防や捜査活動などの治安維持のための利用も現実的なものになっている。ビジネス面では、例えば、所在エリアに応じた広告や割引クーポンの提供やレコメンデーションやサービスのカスタマイズを実現することができる。しかし、位置情報は、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。

本研究は、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った。

2 収集技術とわが国における法的位置づけ

2-1 収集技術

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。大規模かつ広範囲に収集される主要な位置情報としては、表１のようなものが考えられる。

（表 1）位置情報収集技術の例

端末等種別	ネットワーク接続機器（例）	収集情報（例）
インターネット端末	PC、スマートフォン、タブレット端末、ゲーム機	GPS 位置情報、基地局情報、WiFi アクセスポイント
自動車、重機	カーナビゲーション・システム、自動運転や電気自動車の制御装置､遠隔操作システム	GPS 位置情報、走行情報
カメラ	監視カメラ、デジタルカメラ	顔認識等によるトレース情報､GPS による撮影地情報
ID カード等	POS レジ、IC カードリーダ、RFID リーダ、自動改札	購買場所と登録住所、交通機関の利用経路

出典：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

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。こうした情報の取扱についても、今後は注意が必要になってくるであろう。

留意すべき点として、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。

2-2 個人情報保護法上の義務

上記のような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。しかし、多くの位置情報は個人に関連して収集されることが多い。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。

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、今回の法改正では､「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。

一方で、情報の性格によってはできるだけ本人の意思を反映させるべきではないかという意見はあり、例えば総務省「パーソナルデータの利用・流通に関する研究会報告書」では、パーソナルデータのなかでも慎重な取扱いが求められるものについては取扱に際して同意を得るべきであるとしている。そして、そうした情報の例として「継続的に収集される購買・貸出履歴、視聴履歴、位置情報等」があげられている[2]。なお、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、わが国の個人情報保護法においては、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、要配慮個人情報以外については、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 携帯電話事業者と通信の秘密

携帯電話事業者が取扱う位置情報は、特別な法的制約を受けると考えられている。携帯電話事業者が取得する位置情報には､「個別の通信を行った基地局の位置情報」「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)」「GPS位置情報（GPS機能により取得する情報)」の3種類がある。このうち「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[3]。さらに、総務省のガイドラインでは「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[4]」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。

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 。

以上のように、携帯電話事業者が取扱う位置情報については、一般の個人情報とは異なり、利用者の同意が必要となる。

また、携帯電話事業者に限らず、公衆無線 LAN（Wi-Fi）へのアクセスを提供している事業者は、利用者がどのアクセスポイントを利用したかという情報を取得しうる。Wi-Fi の設置者は、各アクセスポイントが設置されている場所を通常把握しているので、端末利用者がアクセスポイントにどのアクセスポイントにアクセスしたかが分かれば、利用者がそのアクセスポイントのカバーエリアにいた事がわかる。これも端末利用者の位置情報であるといえる。こうした情報については、携帯電話事業者の基地局情報と同様に、端末利用者が通信を行っている場合のアクセスポイントは通信の秘密、端末利用者がアクセスポイントにアクセスしているだけの場合に取得される情報はその他の位置情報であると考えられている[5]。

なお、GPS 情報は、電気通信事業者以外の者によっても利用されることがある。例えば、一部のスマホアプリでは利用者の情報を同意なく送信していることや、情報を取得・利用する旨の同意をとっている場合でも、どのような情報を何に利用するのかは詳しく表示されていないまま、利用者は反射的に同意ボタンを押してしまっていることが、問題として指摘されていた。

この問題については、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[5]。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。

3 欧米の動向

3-1 欧州の動向

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）」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。2012 年 1 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案（GDPR）」が提案され、2016 年 5 月に発効し、2018 年 5 月に施行されている[6]。これによって、構成国に立法を求める「指令」から、直接適用される「規則」に変更されるとともに、環境の変化に対応するための数多くの保護規定が追加されている。

EU 個人データ保護指令では、個人データ（personal data）の処理に本人の同意を求めることが基本的な枠組みとして採用されていたが、GDPR では、有効な同意とみなされるための要件が明確化されるなど、さらに本人によるコントロールが重視されている。

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。

また、2002 年に採択され、2006 年および 2009 年に改正されている「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）」には、位置情報に関する特別の規定がある[7]。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）[8]。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 の成立をうけて改正が検討されており、データ保護指令第 29 条に基づいて設置され他諮問機関である 29 条作業部会が、改正のあり方について意見書を公表している[9]。この意見書なかで 29 条作業部会は、現行の位置情報に関する規定が通信事業者や通信サービスのプロバイダに限られており、例えばアプリケーション開発事業者が対象になっていないことなどを指摘し、規定の整理に合わせて対象を拡大することが望ましいとしている。そのためにも、現在別々のものとして規定されているトラフィック・データと位置情報に関する規定を統合し、全ての関係者に向けた規定であることを明確にするとともに、「これらのメタデータの処理に対して同意を要求することによって、改正電子プライバシー規定は、GDPR の第６条が定めるデータ主体の同意と同等の強い法的基準に基づくハイレベルな保護を提供することになる」としている。また、「通信の秘密は、民主主義社会の核心的な権利である」として、特に、現代の通信技術は、表には現れない方法や少なくとも人々が完全には気づかない方法で、度を超えた大量のデータの収集を可能にしていることから、通信およびそれに関連するメタデータにはより厳格なルールが求められることを示唆し、次のような提言をしている。

「通信を提供するという特別な利用目的を超えて、これらのデータを収集、処理、および利用を行うことは、利用者が適切な情報提供を受けたうえで同意をした場合にのみ許される。以上のような理由から、本作業部会は欧州委員会に対して、電子通信のより良いセキュリティ保護のために、トラフィック・データと位置情報のようなメタデータの処理に対して調和の取れた同意取得を義務付けることを勧告する。この同意取得義務は、全てのトラフィック・データと位置情報について適用されるべきであり、ユーザ端末のセンサーによって生成される場合も含むとすべきである。この新たなルールは、これらのデータを収集・処理する全ての者に対して適用されなければならない（14 頁）[10]」

こうした検討を受けて、現在公表されている規則提案[11]においては、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、規則が成立すれば、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、適用されることになる。そして、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）。

(a) 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
(b) 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
(c) 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）。

3-2 米国の動向

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」という報告書を取りまとめている[12]。この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と位置づけられ、執行の指針を直接示したものではない。

一方で、FTC は法執行についても多くの実績がある。FTC 法 5 条の「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)。）」と規定している。この規定が FTC による法執行の根拠となっており、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[13]。

また、電気通信事業者に対する規制を所轄する FCC は、2012 年に、「ロケーション・ベースド・サービス」という報告書公表している[14]。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うらやましいでも入る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）。

そして、2016 年 10 月には、「ブロードバンド顧客プライバシー保護規則 」を採択して、「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」を求めている。ただし、この規制全体が、ISP 等のインターネット・アクセスを提供する事業者だけが対象で、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。そして、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、この規則は議会審査法（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た[15]。今後、ISP やプラットフォーム事業者に対して新たなプライバシー保護のための規制が求められるかどうかは、現在のところ不明である。

4 考察

以上のように、位置情報に関するプライバシー・個人情報保護のあり方について、各国で検討が行われている。EU では、GDPR の制定を踏まえて、電子通信プライバシー指令の改正が検討されており、位置情報については、より広い範囲の保護をすべきではないかという意見が出されている。米国でも、消費者プライバシー政策を担当する FTC と、電気通信に関する規制を所掌する FCC が、ともに位置情報に関するプライバシー保護について検討を行っている。

IoT やビッグデータ技術によって、位置情報を始めとするさまざまな情報が、当初予想されていなかった利用が発生する懸念が高まっている。こうした懸念を考慮に入れた場合に、本人のコントロールをどのように及ぼすべきかという議論が、各国で進んでいる。特に、本人の同意が、有効な同意であるかどうかということや、どのような射程で同意がなされているかを、新たな状況のもとでどのように考えるべきかが焦点になっている。

位置情報に関して、とくに議論になっているのは、①本人意思の反映方法と、②ネットワーク事業者規制との関係の２点である。

まず、「①本人意思の反映方法」については、本人の意思反映自体が難しいとされている情報の保護について、本人から同意を取得する方法や、取得した同意の範囲をどのように考えるべきかが議論になっている。

我が国でもこうした議論が行われてはいるが、わが国の議論は基礎となる法律上の根拠に欠ける面があるのは否めない。EU の制度は、本人の同意を原則として、その同意をいつでも撤回できる権利を認めており、本人の意志の反映を保障している。 米国の制度は、消費者保護をベースに、不公正または欺瞞的行為または慣行を禁止するという形をとっており、他国の個人情報保護制度とは体系が異なる。しかし、消費者の期待を裏切る悪質な行為は FTC 法５条に基づき執行が可能であり、積極的な法執行と相まって、実質的に事業者

に消費者の意思の反映を求めることに実効を挙げていると評価してよい[16]。これに対して、わが国の個人情報保護法においては、個人情報の収集前に利用目的を特定・公表して、その範囲で利用するのであれば、利用一般について本人の同意やプライバシーへの配慮を求める規定がない。要配慮個人情報以外の情報については、情報の利用目的が情報主体の意思に反するものであっても、個人情報を収集した事業者の内部利用については、法律に基づいて利用自体を止めさせる事ができる場合はかなり限定されている。

次に、「②ネットワーク事業者規制との関係」については、ネットワーク事業者のメタデータとして取り扱われる位置情報に対する規制と、その他の位置情報に対する規制について、どのようにバランスをとっていくべきかが議論されている。

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。我が国では、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おり、電気通信事業者以外の者が取扱う位置情報に対して特別な保護が必要かどうかに関する議論は行われていない。我が国では、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おり、この点では欧米と比較してもより保護されているとも言える。しかし、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。つまり、位置情報に関しては、電気通信事業者が取扱う場合と、それ以外の事業者の場合では、規制の厳格さの落差が大きい。

位置情報に関する規制について、EU，米国、日本の状況の概要をまとめたものが、（表２）である。

（表 2）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	不公正または欺瞞的な行為または慣行の禁止	不公正または欺瞞的な行為または慣行の禁止
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）

位置情報のように、本人の意思反映自体が難しいとされている情報の保護について議論を進める場合でも、そもそも本人意思の反映について、さらに法的な保障が必要かどうかについて、まず議論される必要がある。個人情報保護制度の主要な目的の一つは、個人に関する情報の扱いに対してルールを定めて本人の意思に反する利用を抑制することで、弊害を予防したり解消したりすることにある[17]。わが国においても、こうした情報の取扱について本人の意思を反映させる制度をどのように考えるべきかを議論する必要がある。

また、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。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。位置情報を収集・利用するのも、もちろん電気通信事業者だけではない。我が国においても、どのような事業者が取扱うどのような種類の位置情報に規制を課すべきか、収集・利用される位置情報の拡大も視野に入れて、引き続き検討していく必要がある。

【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 年 3 月）53-58 頁。
[2] 総務省「パーソナルデータの利用・流通に関する研究会報告書　パーソナルデータの適正な利用・流通の促進に向けた方策」（2013 年 6 月）28-30 頁。
[3] 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。
[4] 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 16 年総 務省告示第 695 号。最終改正平成 27 年総務省告示第 216 号）の解説」46-48 頁。
[5] 藤波恒一「位置情報に関するプライバシーの適切な保護と社会的利用の両立」ジュリスト 1484 号（2015 年 9 月）87 頁。
[6] 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.
[7] 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.
[8] 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.
[9] Article 29 Data Protection Working Party, Opinion 03/2016 on the evaluation and review of the ePrivacy Directive (2002/58/EC), Adopted on 19 July 2016, WP 240.
[10] 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。
[11] 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).
[12] FTC, Protecting Consumer Privacy in an Era of Rapid Change (2012).
[13] 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, pp. 151-162(2015)。
[14] FCC Wireless Communications Bureau, Location-Based Services - An overview of opportunities and other considerations, May 2012.
[15] 小向太郎「米国連邦取引委員会のプライバシー政策」情報法制研究第 1 号（2017）36 頁以下。
[16] 小向太郎「データ集積の急増と個人情報の利用目的規制」電気学会論文誌 C 電子・情報・システム部門誌第 137 巻 6 号 790-795 頁（2017 年 6 月）。
[17] 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』215-218 頁, NTT 出版(2018）。

〈発　表　資　料〉

題　　名	掲載誌・学会名等	発表年月
Japan’s National Report for “Data Protection in the Internet”	International Academy of Comparative Law	2018 年 7 月（予定）
「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」	情報処理学会 EIP 研究会	2018 年 9 月（予定）