



利用者情報の適切な取扱いの確保に向けた検討課題

2021年3月18日
事務局

- 利用者の利便性と通信の秘密やプライバシー保護とのバランスを、どのように確保していくか。プラットフォーム機能が十分に発揮されるようにするためにも、プラットフォーム事業者がサービスの魅力を高め、利用者が安心してサービスが利用できるよう、利用者情報の適切な取扱いをどのように確保していくか。
- スマートフォンやタブレットなどの通信端末の位置情報や、ウェブ上の行動履歴、利用者の端末から発せられ、または、利用者の端末情報に蓄積される端末IDやクッキーなどの端末を識別する情報等の実態はどのようなになっているか。
- 当該実態を踏まえ、スマートフォンやタブレットなどの通信端末の位置情報や、ウェブ上の行動履歴、利用者の端末から発せられ、または、利用者の端末情報に蓄積される端末IDやクッキーなどの端末を識別する情報等については、通信の秘密やプライバシー保護の関係で、その適切な取扱いの確保のために、どのように規律すべきか。
- 今後のAIの活用やIoT化の進展に伴い、データ流通環境等が大きく変化することが想定される中で、これまで総務省において策定してきた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、位置情報プライバシーレポート、スマートフォン・プライバシー・イニシアティブ等の指針等については、どのように見直していくことが適切であるか。
- 国内外のプラットフォーム事業者、電気通信事業者など関係者による継続的な対話を通じた自主的な取組を促し、その履行状況をモニタリングするという共同規制的なアプローチを適切に機能させるために、どのようなアプローチをとり具体化させていくことが適切か。

【電気通信事業法の射程】

- 競争ルール等の包括的検証の報告書等でしばしば電気通信事業法の役割の変化について言及があった。設備が一方においてソフトウェア化することとサービスがグローバルになるということを通じて、電気通信事業法が電気通信事業者規制法から電気通信サービス利用者保護法に転換を迫られざるを得ないのではないかというところから、各論を検討しなければならないのではないか。【森構成員・第21回】
- プラットフォームの自由と規制の在り方をめぐってEU等で様々な動きがある中で、日本の関係法・政策形成の意義・重要性をよりグローバルな規模でこれまで以上に可視化していくために、従来よりももう一步踏み込んだ、シンプルかつより包括的なコンセプトないしは規範的な基軸を打ち出していくのも、政策戦略の将来構想としてあり得るのではないか。【山口構成員・第21回】

【個人情報とプライバシー保護】

- 端末の中のデータを個別に分類して、個人情報の該当有無を判断するのではなく、もう少し全体でそういった情報は必ず何かにひもづく可能性があるということを前提にした上で考えていく必要があるのではないか。古くて新しい問題としてフィンガープリントとか、駄目だと言っているにも関わらず検知されないからということでDPIのようなこととか起こり始めているとも聞いており、もう少し大きな枠組みで、やっていいこと、いけないことといった概念の方からもう少し考えていく必要があるのではないか。【寺田構成員・第21回】
- 個人情報保護法の令和2年改正において個人関連情報の規制が導入されたが、個人情報になる前、特定の個人を識別することができるものになる前の部分の扱いが、通信の秘密のみなのか、もう少し通信関係プライバシーのようなものを考えて保護しなければならないのか、日本の場合はGDPR等に比べると個人情報の範囲が狭いということがあり、それにより穴になっているところを考えていかなければならないのではないか。【森構成員・第21回】

【個人情報とプライバシー保護（つづき）】

- 個人関連情報が個人情報になる前のウェブの閲覧履歴とその分析の情報等について、個人情報保護法、取引透明化法、消費者優越、電気通信事業法等のうちどれでカバーするかという話について検討が必要。

【森構成員・第22回】

- 個人情報になっていないものは個人情報保護法でというわけにはいかない。個人情報保護法は、令和2年改正で個人関連情報を導入しており行けるところまで行っており適切な改正がされている。取引透明化法は、取引透明化法の枠組みがあり、閲覧者の閲覧履歴を収集する、取得する場面において、消費者・閲覧者に対して一定の何か表示をしたり同意を取る等について義務づけられるような立てつけの法律ではない。消費者優越についてはまだなかなか具体的な法執行の段階に至っていないということもあり、やはりここをカバーできるのは電気通信事業法だけであると改めて認識する。ウェブサイト、ファーストパーティーのところでクッキーやフィンガープリントやそういったものについて情報を取得する行為、タグを設置して情報を取得する行為等については、それをカバーして規律するのは電気通信事業法であるのだと考えられる。【森構成員・第22回】

【ウェブサイトにおけるCookie等の実情について】

- First Party CookieとThird Party Cookieがあり、Third Party Cookieには、SNS事業者、広告事業者、アクセス解析事業者、データ仲介事業者等に情報を送信するものが多く見られる。SNSのIDが付番されSNSアカウント情報と紐付けられ、取得されたデータは個人データになる可能性があるため、設置サイトの運営者が利用者に周知する必要があることが個人情報保護委員会から注意喚起されている。【太田氏・第22回】
- Third Partyによる情報取得の方法として、従来はイメージタグ（イメタグ：1ピクセルの見えない画像）をウェブサイトに貼ってCookie、IPアドレス、閲覧ページURL等を取得していたが、今はJavaScriptのタグ（JSタグ）が主流。イメタグより多くの情報取得（ページに表示される情報や入力される情報等も取得可能）やページ操作、他のJSタグの強制的読み込み等も可能となっている。ウェブサイト運営者も知らないうちにJSタグがどんどん増えて制御困難な場合もあり、事業者間でID連係（Idsync）等がされる場合もある。【太田氏・第22回】

【プラットフォーム事業者の最近の動きと対応】

- プラットフォーマーの提供するブラウザでThird Party Cookieによるトラッキングが制限され、2021年以降アプリにおけるIDFAの利用に同意が必要となり、Privacy Sandbox等の提案もある。一方、Canvas Fingerprinting等の別の手法や、同意を取得した上でメールアドレスに基づく情報やIDによるトラッキングを検討する動きもある。業界としてフィンガープリントやメールアドレスベースのトラッキングについてはオプトアウトの仕組みを準備することにより対応しようとしていると認識しているが、オプトアウトの信頼性の問題はある。【太田氏・第22回】
- Third Party Cookieはセキュリティやプライバシーを守るために使われる例もあるが、プライバシーを侵害する使い方が注目され全部やめるという風潮になっており、この辺りは結構慎重に扱うべきなのかと思う。Cookie等についてもプラットフォーム事業者が大きな力を持ってしまっており、競争法的な考え方というのも頭の片隅に入れておく必要がある。【崎村構成員・第22回】
- メールアドレスベースのIDについては、メールのリサイクル問題があり、間違ったプロファイリングがされてしまう可能性があることをちょっと危惧している。【崎村構成員・第22回】
- 固定的IDは問題という議論を経てリフレッシュできるIDFA等が導入された流れがある。一方、ブラウザーフィンガープリントやUnified ID2.0等がメールアドレスベースという時に簡単に変えられないと思うが、それは業界的に許容されるのか。そのようなIDを作ることをオプトインで同意する人が想定されるのか。色々なところで使っているものを一斉にオプトアウトすることは難しいのではないか。【森構成員・第22回】
- Unified ID2.0等についての一番根本的な違いは、最初に同意を取るか取らないかということ。本当にこれが業界でちゃんと話しをして、同意を取るということを誰でも分かるような仕組みとか形にすれば、ある意味理想的な最初の入り口になると思う。オプトアウト系の問題は、データが流通していく中で、CMPといった仕組みで最後まで徹底的にトラッキングできるのかとのせめぎ合いが起きる。徹底的なトラッキングができれば、ちゃんと仕組みを作れば、オプトアウトとかも必要なところできるということになるが、もう一方で、徹底的なトラッキングができてしまうことがいいのか・悪いのかという問題も起きているのは事実。業界だけではなく、消費者などの中でも、何が許され、どこまでは危ないか等の一種の線引きをしないと難しいと思う。【寺田構成員・第22回】



【プライバシー・ポリシーについて】

- プライバシー・ポリシーをめぐる大きな課題としては長文化が進んでおり非常に分かりづらい。長文のポリシーと、短いステートメントなどもあるが、ポリシーの分かりやすさと、分かりやすく見せるための仕組みや工夫というものを今後検討する段階に来ているのではないか。特にユーザーインターフェースのデザインや工夫による見やすさを考えるべきではないか。【新保座長代理・第21回】
- プライバシー・ポリシーを読まない、見ない、あるいはそもそも理解できない人も存在することも含めた対策を考えるべきではないか。分かる方には当然ちゃんとした説明が必要であるが、プライバシー・ポリシーを読ませることだけに専念するのではない別の対策というものをそろそろ考えないといけないのでは。【寺田構成員・第21回】
- プライバシー・ポリシーに関し、全部読めと言われても多分無理ではないか。普通というのが何かあって、普通と違うところを見せる形だと非常にシンプルになる。例えば、アプリケーションの種別のようなものを考えてそのスタンダードを作り、差分を一番最初に表示する方法を考えていくと効果的ではないか。【宮内構成員・第21回】
- 同意を求められる事項、その中でもアプリの情報、利用者情報がどこでどのような目的で使われているのかといった事項については、レッドやグリーンなど何らかのカテゴライズできないものか。特に第三者に提供されるもの、かなり微妙な機微情報や健康情報が提供されるなど一定のカテゴリーのものについて、特に注意喚起をするような仕組みでプライバシー・ポリシーや簡略化されたステートメントに注意喚起するというような仕組みをどこかに導入できないか。【大谷構成員・第21回】
- コロナ禍での接触確認アプリなどツール導入においても、誤解に基づき導入に慎重になる個人や自治体もあったため、そのアプリが利用する個人データや境界領域にある情報の取扱いについて、正確な情報に基づき導入可否の判断ができるよう分かりやすさを重視した仕組みを導入することが必要ではないか。【大谷構成員・第21回】
- ウェブサイト管理者が実情を把握しにくく、プライバシー・ポリシーをきちんと書けていないサイトが多い。例えばSNSのIDは個人データと紐付く場合も多いが、多くのサイトでcookieが個人情報と紐付くことはないと記載している。また多数の事業者がデータを送付しているがその旨の記載がない事例も多い。【太田氏・第22回】

【プライバシー・ポリシーの公表意義】

- プライバシー・ポリシーの公表意義が社会的、制度的に大きく変化している。企業のアカウントビリティを果たす上での公表事項の要素として投資判断の指標としても用いられつつある。プライバシー・ポリシーをスコアリングするサイトも出てきている。個人情報やプライバシー保護は、企業のアカウントビリティの観点から定着しつつある。また、法定公表事項について、改正個人情報法を踏まえ保有個人データに関する事項の公表等を積極的に行うことが期待される。【新保座長代理・第21回】

【プライバシーポリシーの工夫（簡略版・レイヤードアプローチ等）】

- 簡略版を載せない理由として、法務部がプライバシーポリシーは自組織を守るためであって、個人を守るためではないとして強く拒否する事例を聞いている。【崎村構成員・第21回】
- 簡略版については義務化されていないので作成しない側面と、一部しか見ないことによる苦情の可能性などを法務からリスク増ととらえられる側面がある。利用者が構造を理解してくればやりやすくなるが、現状はリスクマネジメントの観点からやらないというのも結構ある。【寺田構成員・第21回】
- 分かりやすいポリシー、プライバシーノティスの事例として、ISO/IEC29184で実際に求められているレイヤードアプローチにより、簡単なものを出し、詳細はこっちを見て下さいという形を推奨している（NTTドコモの事例）。EDPB（European Data Protection Board）やプラットフォーム事業者も検討に参加しており今後の変化に期待。【崎村構成員・第21回】
- CNILのGoogleに対する制裁の中でも透明性ある情報提供という中で、プライバシーポリシーの仕組みとしてレイヤードアプローチがアグリーメントの中に含まれていた。GDPRの透明性のガイドラインの中に、レイヤードプライバシーポリシーのアプローチに関する在り方がかなり詳細に記述されており、やり方として参考になると思われる。実装例もあると思われ、国際的なベストプラクティスを見るとよい。【生貝構成員・第21回】

【海外におけるプライバシーポリシーや同意取得に係る工夫】

- GDPRの通知・同意取得に当たって推奨される方法や留意すべき事項は、透明性と同意のガイドラインにおいて解説されている。GDPR第12条「簡潔で、透明性があり、理解しやすく、容易にアクセスできる方式」の実現のためにガイドラインで示された推奨される通知方法・工夫の例として、階層的なプライバシーステートメント、丁寧な説明、公開討論・消費者テストの実施、トップページからのタップ数等がガイドラインで示されている。ICOにおいて推奨される通知・同意取得における工夫は、①階層的アプローチ、②ダッシュボード（この延長としてCMP等もある）、③ジャストインタイム、④アイコン、⑤モバイル及びスマートデバイスの機能性の5つの手法である。【NRI南島氏・第22回】
- 欧州においてGDPR及びePrivacy指令に基づきCookie取得に際して同意が求められている。ICOガイドラインにおいて、Cookie取得に同意しないとウェブ画面を閲覧できない同意画面（クッキーウォール）や黙示の同意、デフォルトオンは認められないとされている。CNILガイドラインにおいても、階層的な表示が有効とされ、同意取得に当たり個人を誘導することがない形が推奨されている。【NRI南島氏・第22回】
- CCPA規則においては個人情報の収集やオプトアウト権に関する消費者への通知はプライバシーポリシーとは別に消費者への通知が必要とされる。例えば、個人情報の収集に係る通知内容は、収集する個人情報の種類、利用目的、オプトアウトページのURL、プライバシーポリシーへのリンク等とされる。【NRI南島氏・第22回】
- NIST Privacy Frameworkに係るSP800-53文書において、同意や通知に関する具体的に推奨される手法として、Tailored Consent、ジャストインタイムの同意、同意の撤回などICOやCNILと同様の工夫が示されている。【NRI南島氏・第22回】
- CPRAにおいて「共有するな」ボタンの義務化があり、Do not tracking2.0という言われ方をしている。そういう仕組みの提案がある。【寺田構成員・第22回】

【同意の位置づけ】

- ISO/IEC29184の議論の中では以下のようにされた。同意の取得には考慮点と限界が多く、可能ならば、他の適法な根拠を使った方が良い。そうすることにより、同意によらなければならないものは、同意を求める事自体が例外的なものとして個人に対する注意喚起になる。一方、通知は、処理の根拠に関わらず常に必要であり、その内容は第三者にも示されるべき。【崎村構成員・第21回】

【同意の位置づけ（つづき）】

- スマートフォンが使われ始めた頃に総務省の会議でどれだけ情報取得がされているかという発表を聞き大変驚いたが、その実態がほぼ変わっていない状況で、利用者にとって何となく情報が取得されているのかなと思いつつそうしないと使えないというはかりにかけたようなバランスで使っている。同意画面については、とにかく分かりにくい。消費者としては使いたいほうが先で、細かくて分からないだろうしと思い、そのまま同意してしまうというのが正直な気持ちである。Consent Reciptのように、自分が何に同意しているか分かることは大変大切だと思う。【木村構成員・第22回】
- プラットフォーム研で通知と同意の検討をすることは非常に重要であり、世界的にもそういう認識があるから色々なところで同意に関するガイドラインが出てきて同意の有効性が厳しく検討されている。しかし、事柄が複雑になればなるほど、同意の果たす役割は少なくならざるをえず、ユーザーが同意したからよいではなく、そもそもの仕組みから話しをする必要がある。例えば、本日のJavaScriptの話も、同意は2段階目の話で、まず1段階目としてどういう情報取得・情報提供が発生するウェブサイトにするのかファーストパーティーがまず検討しなければならないのか。【森構成員・第22回】
- 同意をどのように取得するのかという手続、同意の取得の対象範囲、個別同意か包括同意か等は、様々な場面で検討されている。クッキー取得時の同意やユーザーインターフェース等も精緻な検討が進められている。一方、同意の効力については、法律行為か事実行為かも意見がある。今後同意取得が更に重要になる中で、同意のそもそもの効力、本人の同意による責任や事業者側への法的効力等もなども少し整理する場があってもよいのではないか。【新保座長代理・第22回】
- 同意についてどんどん細かくなり手続関係の話になるが、そもそもの同意の目的が忘れられ形骸的なものになってきつつあると感じる。同意を取るのに必要などんなデータ（位置情報等）か、利用目的か、第三者に提供・加工する等かなにが重要なのか考えている。本当に重要なのはその結果利用者に与える影響、アウトカムではないか。手続論・ルールベースの話になってしまうが、アウトカムベースでもう一度見直してどう整理するか考える必要がある。グローバルの流れも、リスクマネジメントの考え方で（SP800-53等も）少しずつアウトカムベースに変わりつつあり、そのような視点を持つ必要がある【寺田構成員第22回】

【同意の位置づけ（つづき）】

- 寺田構成員の意見に大賛成。アウトカムをしっかりと一度整理していく必要があると強く感じる。それと併せて、今までやってきている内容・手続論とどうやってそれらが結びつくかという点を最後はゴールとして考えて整理していくというのを一度やるべきかなと思っている。【手塚構成員・第22回】
- アウトカムベースに賛成。手段を規制するのは限界があり、いたちごっこになるので、どういうアウトカムになってはいけないのかというアウトカムベースでやるように規制対象を変えていかなければいけない。【崎村構成員・第22回】
- ISOの通知・同意取得に関する標準規格において、レイヤードアプローチやジャストインタイムの通知とともに、有効な同意を高める手法として同意の証跡（Consent Receipt）がある。【NRI南島氏・第22回】
- ウェブサイト上における利用者の同意管理ツール（CMP）において、同意前から情報取得、取得拒否しても取得が継続されるなど、正しく動作していない場合也多みられる。提供先は包括同意を取られると実効性はほぼないと思われる。提供元（ウェブサイト・アプリ側）で、どういう事業者がどういう情報を取得しているか公表を明確化しちゃんと拒否できるとよいのではないか。【太田氏・第22回】
- アドブロッカーについては物にもよるが、ほとんどのサイトにおいては非常に有効なものだと思う。一方、広告がブロックされてしまうと、メディアとして収益をどう確保するかという問題がある。ドラスティックに広告のエコシステムが変わることがないので、広告を表示して収益を発生させることと、個人が広告をブロックできることをどう両立するかは非常に難しい問題かなと思う。【太田氏・第22回】

【スマートフォン プライバシー イニシアティブ、スマートフォン・プライバシー・アウトLOOK】

- スマートフォン・プライバシー・アウトLOOKについて、2010年代から継続的な検討がなされていることそのものが非常に大きな意義があり、総務省の取組として引き続き継続してほしい。2014年以降の調査により、プライバシーポリシーの掲載率が顕著に向上しているということが非常に分かりやすい調査結果として出ており、継続性の意義がある。【新保座長代理・第21回】
- モバイル・コンテンツ・フォーラムがSPIの内容を受けてガイドラインを作成し会員に広めており、一部の情報収集モジュールはSPIの内容を踏まえてプライバシーポリシーへの記載方法を周知している動きもある。【日本総研小竹氏・第21回】
- 広告代理店において、ガイドラインを作り会員会社に対してそれを守るように促している。モバイル・コンテンツ・フォーラムのガイドラインは地方公共団体のアプリでも利用例がある。【寺田構成員・第21回】
- スマートフォンのアプリについては、広告ID（iOS：IDFA, アンドロイド：AAID）があるが、アプリを起動するとニュース等を閲覧するだけでも広告やトラッキング系の情報提供が数多く行われていた。調査した結果、位置情報を取得するアプリのうち半数はプライバシー・ポリシーにその旨記載がなかった。【太田氏・第22回】
- 太田氏の説明を伺い、やはりこれは木村構成員からもお話があったがスマートフォン プライバシー イニシアティブの話だと改めて思う。スマートフォン プライバシー イニシアティブは、ユーザーに対する情報提供にフォーカスしているが、状況は変わらず、深刻な問題状況にある。アプリのプライバシー・ポリシーの掲載率は上がったが、書かれたとおりになっていなかったり、IDが固定的なものとなったり、事態がよくなったとはいえない。やはりもう一段階踏み込んだことをしないとイケない状態であることがはっきりしたのではないか。【森構成員・第22回】

【利用者情報を取扱う事業者の取組み】

- NIST Privacy FrameworkのCoreにおいて、8つ定められており、1-5がPrivacy Framework独自で通知・同意取得に当たりプロセスをきちんと確立し社内で浸透させようという形の規定がされている。6-8はCybersecurity Frameworkと重複。【NRI南島氏・第22回】

【共同規制的なアプローチ】

- 我が国で同意は個人情報保護法だとすごくあっさりした書き方であり、通信の秘密に関する場合は非常に重くなっている。GDPRで言うように、透明性があり十分情報を提供した上で同意を取るということについて、法令レベルではないとしても、電気通信ガイドライン等を書くことにより、ある種の共同規制的な、インセンティブをつくるのが考え得る。【生貝構成員・第21回】

【検討の視点】

- 「同意」の在り方、ユーザーのモラル、プラットフォーム事業者の自主的取組・透明性・アカウントビリティに関する施策を基盤とした上で、これらと相互排他的な代替措置としてではなく、さらなる実効性の確保に向けた追加的な担保措置を促すものとして、例えば以下の3点が挙げられる。
 - ①プラットフォーム上での言論・表現の送り手と受け手が相互に互換的な存在となるユーザーの、モラル・倫理・責任に加えて、その「権利」の視点もより前面に打ち出すユーザーライツの観点
 - ②AI実装も進むユーザーコンテンツ監視・削除等のシステムに関して、公的部門での規律が必ずしも及ばないブラックボックスの事実状況を把握し、より開かれた検証可能性を確保
 - ③事前ないしプロアクティブに公正性、公平性などの社会的価値を、システムのデザインに積極的に組み込んでいくこと。【山口構成員・第21回】

参考資料

- 「通信の秘密」は、通信が人間の社会生活にとって必要不可欠なコミュニケーション手段であることから、表現の自由の保障を実効あらしめるとともに、個人の私生活の自由を保護し、個人生活の安寧を保障する(プライバシーの保護)ため、憲法上の基本的人権の一つとして、憲法第21条第2項において保障されている。
- 日本国憲法の規定を受け、電気通信事業法第4条、第179条等において、「通信の秘密」は罰則をもって保護されており、電気通信事業法上「通信の秘密」は厳格に保護されている。

通信の秘密の範囲

通信の秘密とは、①個別の通信に係る通信内容のほか、②個別の通信に係る通信の日時、場所、通信当事者の氏名、住所、電話番号等の当事者の識別符号、通信回数等これらの事項を知られることによって通信の存否や意味内容を推知されるような事項全てを含む。

※ 東京地裁判決H14.4.30は、「電気通信事業法第104条【注:現行法では第179条】の「通信の秘密」には、通信の内容のほか、通信当事者の住所・氏名・電話番号、発受信場所、通信の日時・時間・回数なども含まれると解する。」と判示している。

通信の秘密の侵害

通信の秘密を侵害する行為は、以下の3類型に大別されている。なお、通信の秘密の保存自体も侵害に該当し得る。

- 知得＝「積極的に通信の秘密を知ろうとする意思のもとで知ること」
- 窃用＝「発信者又は受信者の意思に反して利用すること」
- 漏えい＝「他人が知り得る状態に置くこと」

通信当事者の有効な同意がある場合

- 通信の秘密の侵害について通信当事者の有効な同意がある場合は、通信の秘密の侵害にあたらない。

通信当事者が侵害される通信の秘密について個別具体的かつ明確に同意した場合でなければ原則として有効な同意があるとはいえない。

ただし、通常の利用者であれば承諾することが想定される場合であって、利用者が随時不利益なく同意を撤回でき(オプトアウト)、それらが十分に周知されるなどしている場合は、約款等による包括的な同意でも有効な同意といえる場合がある。

違法性阻却事由がある場合

- 通信当事者の同意がない場合であっても、下記のような違法性阻却事由がある場合には、通信の秘密の侵害が許容される。

(1) 法令行為に該当する場合

電気通信事業者として、刑事訴訟法第100条に基づく通信履歴の差押えなど、他の法令の規定に基づき正当に行う行為は、法令に基づく行為として違法性が阻却される。

(2) 正当業務行為に該当する場合

電気通信事業者として電気通信役務の提供等の業務を遂行するために必要であって、①目的の正当性、②行為の必要性、③手段の相当性の要件を満たす行為については、正当業務行為として違法性が阻却される。

(3) 正当防衛、緊急避難に該当する場合

通信施設に対する現に生じている攻撃に対応したり人の生命身体に対する危険を避けたりするために通信の秘密を侵す場合等、正当防衛の要件(①急迫不正の侵害、②自己又は他人の権利を防衛するため、③やむを得ずした行為)又は緊急避難の要件(①現在の危険の存在、②法益の権衡、③行為の補充性)を満たす行為については、違法性が阻却される。

日本国憲法

第二十一条

2 検閲は、これをしてはならない。**通信の秘密はこれを侵してはならない。**

電気通信事業法

第三条 電気通信事業者の取扱中に係る通信は、検閲してはならない。

第四条 **電気通信事業者の取扱中に係る通信の秘密は、侵してはならない。**

2 電気通信事業に従事する者は、在職中電気通信事業者の取扱中に係る通信に関して知り得た他人の秘密を守らなければならない。その職を退いた後においても、同様とする。

第百七十九条 **電気通信事業者の取扱中に係る通信（中略）の秘密を侵した者は、二年以下の懲役又は百万円以下の罰金に処する。**

2 電気通信事業に従事する者（中略）が前項の行為をしたときは、三年以下の懲役又は二百万円以下の罰金に処する。

3 前二項の未遂罪は、罰する。

※「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の解説」（抜粋）

通信の秘密（通信内容にとどまらず、通信当事者の住所、氏名、発信場所、通信年月日等の通信構成要素及び通信回数等の通信の存在の事実の有無を含む。）に該当する個人情報の取扱いについては、通信の秘密の保護の観点から、原則として通信当事者の個別具体的かつ明確な同意が必要

- 個人情報の保護に関する法律(平成17年4月全面施行・平成29年5月改正法全面施行)

公的部門

民間部門

独立行政法人等法律）
独立行政法人等の保有する個人
情報の保護に関する法律

地方公共団体等（条例）
各地方公共団体において制定さ
れる個人情報保護条例

個人情報取扱事業者の義務等(第4章～第6章)

個人情報保護委員会 ガイドライン等

電気通信業

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

他に、金融分野、信用分野、医療分野等におけるガイドラインがある。

認定個人情報保護団体の指針等

- 分野横断的に適用される個人情報保護委員会ガイドラインの内容を反映させ統一性を図る一方、**通信の秘密等の電気通信事業法に基づく規律や、プライバシー保護の観点からの規律等、電気通信分野に特有の規律を追加。**

個人情報保護委員会ガイドライン

(通則編)

1. 目的及び適用対照
2. 定義
3. 個人情報取扱事業者等の義務
 - 3-1 個人情報の利用目的
 - 3-2 個人情報の取得
 - 3-3 個人データの管理
 - 3-4 個人データの第三者への提供
 - 3-5 保有個人データに関する事項の公表等、保有個人データの開示・訂正等・利用停止等
 - 3-6 個人情報の取扱いに関する苦情処理
 - 3-7 匿名加工情報取扱事業者等の義務
4. 漏えい等の事案が発生した場合等の対応
5. 「勧告」、「命令」及び「緊急命令」等についての考え方
6. 域外適用及び適用除外
7. ガイドラインの見直し
8. (別添) 講ずべき安全管理措置の内容

(外国にある第三者への提供編)

(第三者提供時の確認・記録義務編)

(匿名加工情報編)

個人情報の保護に関する法律に係るEU域内から十分性認定により移転を受けた個人データの取扱いに関する補完的ルール

電気通信事業分野ガイドライン

(ガイドライン) 第1条
第2条
§

(ガイドライン解説)

1. 目的及び適用対象
2. 定義
3. 電気通信事業者の義務
 - 3-1 個人情報の利用目的
 - 3-2 個人情報の取得
 - 3-3 個人データ等の管理
 - 3-4 プライバシーポリシー
 - 3-5 個人データの第三者への提供
 - 3-6 保有個人データに関する事項の公表等、保有個人データの開示・訂正等・利用停止等
 - 3-7 個人情報の取扱いに関する苦情処理
 - 3-8 匿名加工情報取扱事業者等の義務
4. 漏えい等の事案が発生した場合等の対応
5. 各種情報の取扱い
6. ガイドラインの見直し
7. (別添) 講ずべき安全管理措置の内容

共通の規律については内容を反映し統一性を確保

これらを準用する旨をガイドライン解説に追記。(3-5、3-8)

条項	内容
1 目的及び適用対象	
第1条 (目的)	● 電気通信事業者が扱う個人情報においては、通信の秘密やプライバシー保護の観点から個人情報を保護する必要性が大きいことを解説で言及。(解説1-1) ● 電気通信事業法は、外国法人等が日本国内で電気通信役務を提供する場合及び外国から日本国内にある者に対して電気通信役務を提供する場合に適用されるため、当該外国法人等に本ガイドラインが適用されることを解説で言及。(解説1-2) ※令和3年4月1日施行 ● 「個人情報の保護に関する法律についてのガイドライン(個人情報保護委員会)」に準拠しつつ、通信の秘密その他の電気通信事業者に特有の事情等を鑑み必要となる規定も併せ、電気通信事業者に適用される規律を一元的に示すことを解説で言及。(解説1-3)
2 定義	
第3条 (電気通信事業者等)	● 電気通信事業者として、手続の有無にかかわらず電気通信事業法上の電気通信事業を行なう者を対象とし、電気通信事業法の適用除外とされている同法第164条第1項各号に定める事業を営む者も同法第4条(秘密の保護)の規定の適用があり個人情報保護の必要性に差はないことから本ガイドラインの対象とすることを解説で言及。(解説2-1) ● 電気通信サービスとして、電気通信事業者が他人の需要に応じて提供する電気通信役務及びこれに付随するサービスも含み、電気通信役務に係る個人情報と同じIDで紐付けを行なう場合についても電気通信サービスに該当することを解説で言及。(解説2-1) ● 本人の同意に関して、通信の秘密(通信内容、通信当事者の住所、氏名、発信場所、通信年月日等の通信構成要素及び通信回数などの通信の存在の事実の有無を含む)に該当する場合には、原則として通信当事者の個別具体的かつ明確な同意が必要となることを解説で言及。(解説2-13)

条項	内容
3 電気通信事業者の義務	
第5条 (利用目的による制限の例外)	● 個人情報保護法 第16条第3項 は同意を得ずに利用目的を超えた個人情報の取扱うことが可能な場合を挙げているが、 通信の秘密に係る個人情報 は同条同項は適用されない(同意または違法性阻却事由が必要)旨規定。(GL第5条第4項)
第7条 (適正な取得)	● 個人情報保護法 第17条第2項各号 は同意を得ずに要配慮情報を取得することが可能な場合を挙げているが、 通信の秘密に係る個人情報 は同条同項は適用されない(利用者の同意または違法性阻却事由が必要)旨規定。(GL第7条第3項)
第10条 (保存期間等)	● 個人情報保護法において、利用する必要がなくなった個人データ消去の努力義務が課されているが、電気通信事業分野ガイドラインでは 個人データ(通信の秘密に係るものを除く) に保存義務の設定に係る努力義務を課するとともに、 通信履歴等の通信の秘密に係る個人情報 は、同意又は違法性阻却事由がある場合を除いて記録を最小限にとどめるとともに、 利用目的を達成した際は速やかに消去する義務 を規定。(GL第10条第2項)
第12条 (従業者・委託先の監督)	● 個人情報保護法が定める安全管理措置の他、 従業者先及び委託先に対し必要な教育研修を実施する努力義務 を規定。(GL第12条第2項)
第13条 (個人情報保護管理者)	● 個人情報保護管理者(当該電気通信事業者の個人データ等の取扱いに関する責任者)を設置し、ガイドラインを遵守するための内部規定の策定、監査体制の整備及び個人データ等の取扱いを監督する努力義務を規定。(GL第13条) ● 電気通信事業者内部における責任体制を確保するため、個人データ等の適正な取扱いの確保について必要な権限を有する役員等の組織横断的に監督することのできる個人情報保護管理者を置き、必要な監督等を行なわせよう努める旨を解説に記載(解説3-3-7)。

条項	内容
3 電気通信事業者の義務(つづき)	
第14条 (プライバシーポリシー)	● プライバシーポリシー(個人情報保護を推進する上での考え方や方針)を公表する努力義務を規定。(GL第14条第1項) ● 電気通信事業者の個人情報保護についての社会的信頼を確保するため、電気通信事業者は自らの個人情報保護を推進する上での考え方や方針についての宣言をプライバシーポリシーとして公表することが適切であるとした上で、プライバシーポリシーに記載すべき事項について、具体的に解説で言及。(解説3-4-1) ● アプリケーションソフトウェアを提供する場合、当該アプリケーションの情報取得等に係るプライバシーポリシーを公表する努力義務を規定。(GL第14条第2項) ● アプリケーションを提供するサイトを運営する場合、当該サイトにおいてアプリケーションを提供する者に対して、当該アプリケーションの情報取得などに係るプライバシーポリシーを公表するよう促す努力義務を規定。(GL第14条第3項) ● アプリケーションのプライバシーに記載すべき事項について具体的項目を示し、スマートフォン プライバシー イニシアティブ等によるものと解説で言及。(解説3-4-2)
第15条 (第三者提供の制限)	● 個人情報保護法第23条は第三者提供時に同意を不要となる場合(同条第1項)やアウトアウトによる第三者提供(同条第2項)を規定しているが、通信の秘密に係る個人情報にこれらは適用されない(利用者の同意又は違法性阻却事由が必要)旨を規定。(GL第15条第8項)
第28条～第31条 (匿名加工情報取扱事業者等の義務)	● 匿名加工情報取扱事業者等の義務は「個人情報の保護に関する法律についてのガイドライン(匿名加工情報編)」に準じる。電気通信事業者が取扱う位置情報は、通信の秘密に該当する個人情報を含む場合があるほかプライバシーの観点から保護が必要とされるため、適切な加工手法及び管理運用体制が求められ、認定個人情報保護団体の個人情報保護指針等の自主的ルールに委ねられる旨を解説で言及。(解説3-8)

条項	内容
5 各種情報の取扱い	
第32条 (通信履歴の記録)	● 電気通信事業者が取り扱う通信履歴は一般に通信の秘密に該当することから、以下を規定。 ・ 課金・料金請求・苦情対応・不正利用の防止その他の業務遂行上必要な場合に限り記録し、最小限の範囲内で保存期間を設定した上で、当該保存期間経過したとき又は記録目的を達成後は速やかに削除。(GL第32条第1項、解説5-1-1) ・ 利用者の同意又は違法性阻却事由がある場合以外、通信履歴を他人へ提供はできない。(GL第32条第2項、解説5-1-2)
第33条 (利用明細)	● 利用明細の内容は、通信の秘密に属する通信履歴にほぼ等しいため、通信の秘密やプライバシーに対する配慮が必要なことから、以下を規定。 ・ 利用明細に記載する情報の範囲は、利用明細の目的を達成するために必要な限度を超えてはならない。(GL第33条第1項、解説5-2-1) ・ 利用明細を加入者その他の閲覧しうる者に閲覧・交付する場合には、利用者の通信の秘密及び個人情報を不当に侵害しないよう必要な措置を実施。(GL第33条第2項、解説5-2-2)
第34条 (発信者情報)	● 発信者情報通知サービスを提供する場合には、発信者情報を通知するかどうかの判断を発信者に委ねる観点から、通信ごとに、発信者情報の通知を阻止する機能を設けなくてはならない。(GL第34条、解説5-3-1)

条項	内容
5 各種情報の取扱い(つづき)	
第35条 (位置情報)	● 位置情報は、個々の通信に係る場合は通信の秘密であること、通信の秘密に該当しない場合であっても、プライバシーの中でも特に保護の必要性が高く、通信とも密接に係る事項であることから、以下を規定。 ・ 電気通信事業者は、あらかじめ利用者の同意を得ている場合、正当業務行為その他の違法性阻却事由がある場合に限り、取得可能。（GL第35条第1項、解説5-4-1） ・ あらかじめ利用者の同意を得ている場合、令状に従う場合その他の違法性阻却事由がある場合に限り、他人への提供その他の利用可能（通信の秘密に該当する位置情報について匿名化して他者へ提供等を行なう場合には利用者の同意を得る必要があること、通信の秘密に該当しない位置情報について他者へ提供等を行なう場合には利用者の同意又は違法性阻却事由がある場合に限定することが強く求められる旨を解説で言及）。（GL第35条第2項、解説5-4-2） ・ 位置情報サービスの提供にあたっては、利用者の権利が不当に侵害されることを防止するために必要な措置（※）を講ずることが適切（※①利用者の意思に基づく提供、②利用者の認識・予見可能性の確保、③適切な取扱い、④提携に関する約款等への記載について解説で言及）。（GL第35条第3項、解説5-4-3） ・ 捜査機関からの要請により取得を求められた場合は、令状に従う時に限り、取得可能。（GL第35条第4項、解説5-4-4） ・ 救助を行う機関からの要請により取得を求められた場合は、生命又は身体に対する重大な危険が切迫し、早期発見のために不可欠であると認められる場合に限り、取得可能。（GPS位置情報は通信の秘密ではないが、基地局の位置情報よりも高いプライバシー性を有する旨解説で言及）（GL第35条第5項、解説5-4-5）

5 各種情報の取扱い(つづき)

第36条
(不払い者等情報)

- 電気通信役務に係る料金不払い又は携帯音声通信役務の不正な利用を防ぐために特に必要かつ適切であると認められるときは、**以下の者の情報（氏名、住所等）を電気通信事業者間で交換することができる**旨を規定。(GL第36条、解説5-5)
 - ・ 支払期日経過後も電気通信役務に係る料金を支払わない者
 - ・ 携帯電話不正利用防止法第9条に基づく契約者確認に応じない者

第37条
(迷惑メール等送信に係る加入者情報)

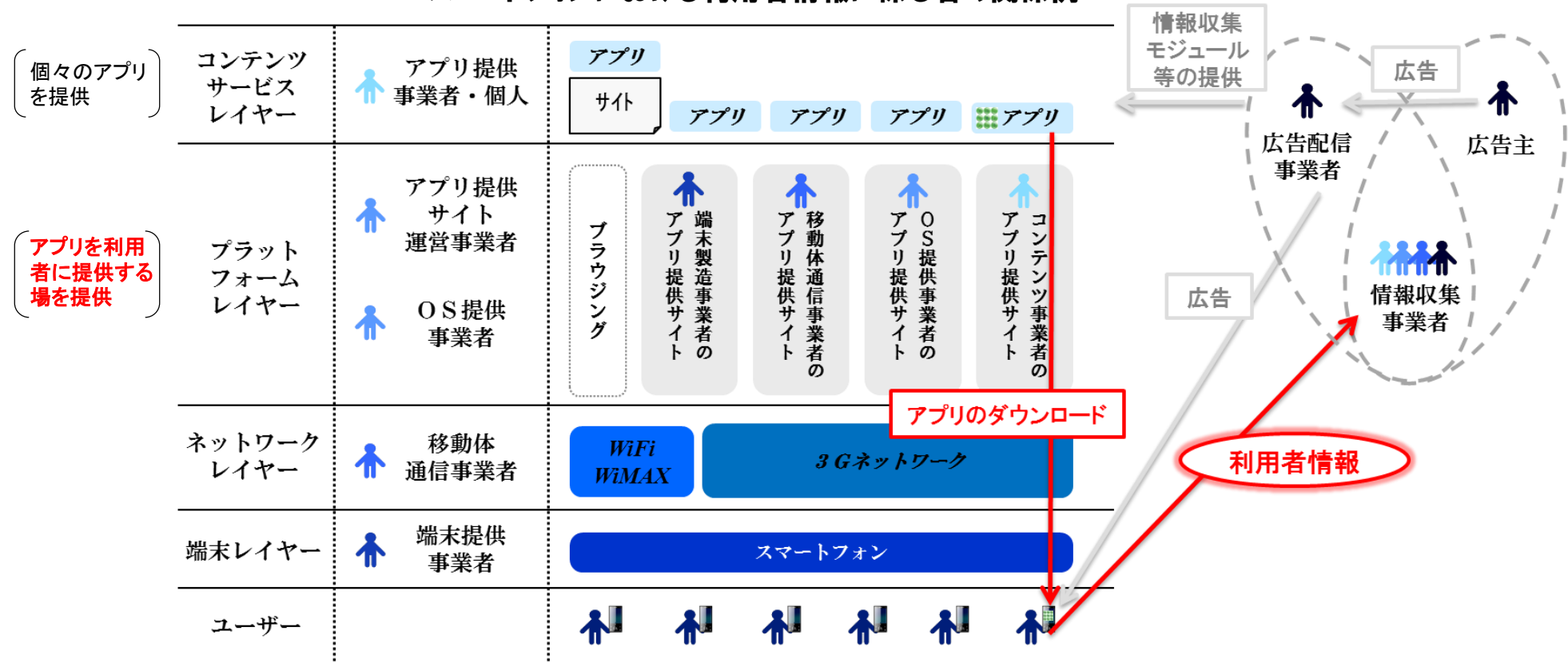
- 電気通信事業者は、一時に多数の者に対してされる電子メールの送信による電子メールの送受信上の支障を防止するため特に必要であり、かつ適切であると認められるときは、他の電気通信事業者との間において、加入者情報（電気通信事業者が迷惑メール送信に関する利用停止措置を講じ、又は契約を解除したものに限る）を交換することができる。（交換することについて契約約款に明記すること等により加入者の同意を得る旨を解説で言及）（GL第37条、解説5-6）

第38条
(電話番号情報)

- 電気通信事業者が電話番号情報を用いて電話帳を発行し又は電話番号案内を行なう場合には、加入者に対し、電話帳への掲載又は電話番号の案内をしないことについての選択の機会を与えることが適切である。（GL第38条、解説5-7）

- スマートフォンにおいては、携帯電話事業者がインフラからコンテンツまでサービス全体を提供する従来の携帯電話と異なり、**サービスのレイヤー(層)ごとに多様な事業者がそれぞれの役割を持ってサービスを展開。**
 - **スマートフォンに搭載されるオペレーティングシステム(OS)を提供する事業者は、一般にアプリ提供サイトの運営を行っており、端末開発、通信ネットワーク利用、アプリ提供、課金・認証等、各レイヤーに影響力を有している。**
 - 広告配信事業者が提供する情報収集モジュールをアプリに組み込むことで、アプリケーション開発者が一定の対価を得、さらに、その情報収集モジュールを通じ、利用者情報が情報収集事業者等へ送信される場合があると指摘される。

スマートフォンにおける利用者情報に係る者の関係例



- 常に電源を入れてネットワークに接続した状態で持ち歩くスマートフォンは、PCに比べて利用者との結びつきが強く、利用者の行動履歴や通信履歴等の多種多様な情報を取得・蓄積することが可能
 - 電話番号及びアドレス帳で管理されるデータ、GPS等による高精度の位置情報

スマートフォンにおける主な利用者情報



～スマートフォン プライバシー イニシアティブ（スマートフォン利用者情報取扱指針）～

- 利用者情報に係る利用者の不安解消は、一義的に関係事業者の役割と責任においてなされるべき。
- 業界団体未加入のアプリ提供者も含め多様な関係事業者が直接参照できる指針を提示。各業界団体が業界の実情を踏まえ、追加的事項を盛り込んでガイドラインを作成することも期待される。

6つの基本原則

- | | | |
|--------------|------------------|------------------|
| ① 透明性の確保 | ② 利用者関与の機会の確保 | ③ 適正な手段による取得の確保 |
| ④ 適切な安全管理の確保 | ⑤ 苦情・相談への対応体制の確保 | ⑥ プライバシー・バイ・デザイン |

利用者情報取得者における取組

(アプリ提供者、情報収集モジュール提供者等による取組)

(1) プライバシー・ポリシーの作成

☞ アプリケーションや情報収集モジュールごとに分かりやすく作成。(簡略版も作成。)

- ① 情報を取得するアプリ提供者等の氏名又は名称
- ② 取得される情報の項目
- ③ 取得方法
- ④ 利用目的の特定・明示
- ⑤ 通知・公表又は同意取得の方法、利用者関与の方法
- ⑥ 外部送信・第三者提供・情報収集モジュールの有無
- ⑦ 問合せ窓口
- ⑧ プライバシーポリシーの変更を行う場合の手続

(2) 適切な安全管理措置

(3) 情報収集モジュール提供者に関する特記事項

(4) 広告事業者に関する特記事項

関係事業者における取組

(1) 移動体通信事業者・端末提供者

- ☞ スマートフォン販売時等
- ☞ 移動体通信事業者のアプリケーション提供サイト

(2) アプリ提供サイト運営事業者、OS提供事業者

- ☞ アプリケーション提供サイト

(3) その他関係しうる事業者

- ☞ アプリケーション推薦等



スマートフォン プライバシー イニシアティブ（平成24年8月公表）

総務省研究会が、「スマートフォン利用者情報取扱指針」（6つの基本方針、アプリごとのプライバシーポリシー（明示すべき8事項を含む）の作成・掲載、適切な安全管理措置等、関係事業主体が取り組むべき事項）等を中心とする提言を取りまとめ。

6つの基本原則

- ① 透明性の確保
- ② 利用者関与の機会の確保
- ③ 適正な手段による取得の確保
- ④ 適切な安全管理の確保
- ⑤ 苦情・相談への対応体制の確保
- ⑥ プライバシー・バイ・デザイン

明示すべき8事項

- ① 情報を取得するアプリ提供者等の氏名又は名称
- ② 取得される情報の項目
- ③ 取得方法
- ④ 利用目的の特定・明示
- ⑤ 通知・公表又は同意取得の方法、利用者関与の方法
- ⑥ 外部送信・第三者提供・情報収集モジュールの有無
- ⑦ 問合せ窓口
- ⑧ プライバシーポリシーの変更を行う場合の手続

スマートフォンの利用者情報等に関する連絡協議会（SPSC）
（平成24年10月設置）

スマートフォン プライバシー イニシアティブⅡ（平成25年9月公表）

総務省研究会が、プライバシーポリシーの作成・掲載を一層推進するとともに、利用者情報の適正な取扱いの実効性を確保するため、運用面・技術面から第三者がアプリを検証する仕組みを民間主導で推進すること等の提言を公表。

スマートフォン プライバシー イニシアティブⅢ（平成29年7月公表）

スマートフォン プライバシーイニシアティブを、策定当時の環境変化や、その後の検討内容を踏まえ、関係事業者等の役割分担の明確化や取組の具体化等を目的として改訂。

電気通信事業者における個人情報保護に関するガイドライン

（個人情報保護管理者）

第十三条 電気通信事業者は、**個人情報保護管理者**（当該電気通信事業者の個人データ等の取扱いに関する責任者をいう。）を置き、本ガイドラインを遵守するための**内部規程の策定、監査体制の整備及び当該電気通信事業者の個人データ等の取扱いの監督**を行わせるよう努めなければならない。

（プライバシーポリシー）

第十四条 電気通信事業者は、**プライバシーポリシー**（当該電気通信事業者が個人情報保護を推進する上での考え方や方針をいう。）を公表することが適切である。

2 電気通信事業者は、**アプリケーションソフトウェア**（以下「アプリケーション」という。）を**提供する場合**において、当該**アプリケーションによる情報の取得等について明確かつ適切に定めたプライバシーポリシー**を公表することが適切である。

3 電気通信事業者は、**アプリケーションを提供するサイトを運営する場合**において、当該**サイトにおいてアプリケーションを提供する者に対して、当該アプリケーションによる情報の取得等について明確かつ適切に定めたプライバシーポリシー**を公表するよう促すことが適切である。

スマートフォン アプリケーション プライバシーポリシー普及・検証推進タスクフォース
（平成25年12月設置）

スマートフォン プライバシー アウトルック

SPI IIで提言されたアプリ検証の推進に向けて、プライバシーポリシーの掲載状況について調査を実施し、スマートフォン上のアプリにおける利用者情報の取扱いの現況等を取りまとめ、報告。

- スマートフォン プライバシー アウトルック（平成26年5月公表）
- スマートフォン プライバシー アウトルックⅡ（平成27年4月公表）
- スマートフォン プライバシー アウトルックⅢ（平成28年4月公表）
- スマートフォン プライバシー アウトルックⅣ（平成29年7月公表）
- スマートフォン プライバシー アウトルックⅤ（平成30年10月公表）
- スマートフォン プライバシー アウトルックⅥ（令和元年5月公表）
- スマートフォン プライバシー アウトルックⅦ（令和2年11月公表）



I 論点

■ 位置情報の加工 (いわゆる匿名化) について

位置情報を加工した上で利活用するため、加工方法、その加工の程度に応じた取扱い、加工後の情報の適切な取扱いについて整理。

■ 通信の秘密に該当する位置情報について

通信の秘密に該当する位置情報について、加工した上で利用・第三者提供することについての有効な同意取得の在り方について検討。

II 検討結果

■ 位置情報の加工 (いわゆる匿名化) について

その時点での技術水準では再特定化・再識別化が不可能又は極めて困難と言える程度に加工(「十分な匿名化」)された場合には、個人を特定されるリスクが大きく低減されており、利用者の同意なく利用・第三者提供が可能である。

■ 通信の秘密に該当する位置情報について

通信の秘密に該当する位置情報を加工した上で利用・第三者提供することは、利用者の有効な同意がない限り、通信の秘密の侵害に該当し得る。通信の秘密に係る位置情報を「十分な匿名化」をした上で利用・第三者提供することについて、

- ① 情報の範囲が、通信内容以外の通信の構成要素のうち、通信の場所、日時及び利用者・端末識別符号に限定されること、
- ② 加工の手法・管理運用体制が適切であること及びそれについて適切に評価・検証が行われていること、
- ③ 利用者がいったん契約約款等に同意した後も、随時、同意内容を変更できる契約内容であって、同意内容の変更の有無にかかわらず、その他の提供条件が同一であること、
- ④ 契約約款等の内容等について利用者に対する相応の周知が図られていること

の全ての要件を満たしている場合であれば、契約約款等に基づく事前の同意であっても、有効な同意といえることができると考えられる。

III 今後の取組み

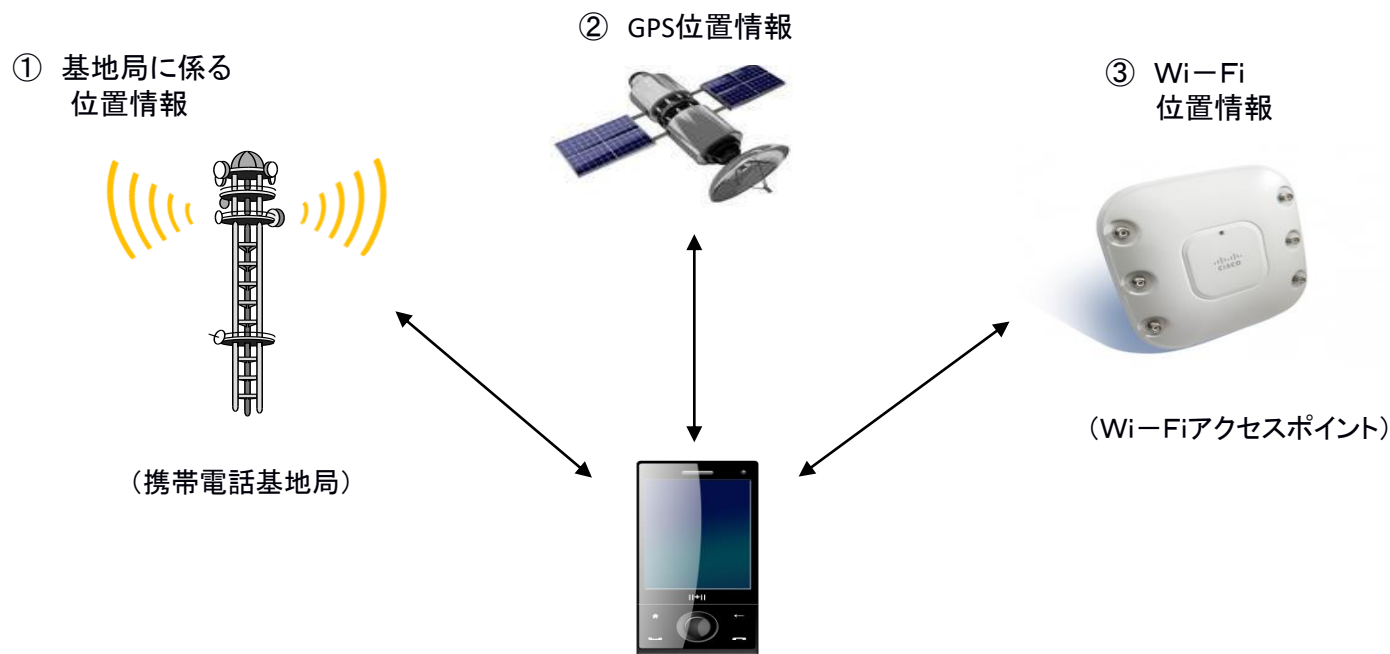
「十分な匿名化」の水準については、通信の秘密に該当する位置情報を含む位置情報について、総務省及び関係事業者において引き続き検討をしていくことが必要である。

加工の方法・管理運用体制(「十分な匿名化」をする過程で作成される情報の管理体制を含む。)の適切性についての評価・検証の在り方について、総務省及び関係事業者において引き続き検討していく必要がある。また、総務省及び関係事業者において、具体的な加工の方法・管理運用体制の在り方について、安全性を確保するための技術等も含め、実証・検証も進めていくべき。

「位置情報」の種類

- ◆ 電気通信事業者が取り扱う「位置情報」(※)は「基地局に係る位置情報」、「GPS位置情報」、「Wi-Fi位置情報」の3つ。
- ◆ 基地局に係る位置情報とは、携帯電話事業者が通話やメール等の通信を成立させる前提として取得している情報のこと。
- ◆ GPS位置情報とは、複数のGPS衛星から発信される電波を携帯電話端末が受信して、電波の発信時刻と受信時刻の差から計算される衛星と携帯電話端末の距離等から当該携帯電話端末の詳細な位置を示す位置情報のこと。
- ◆ Wi-Fi位置情報とは、Wi-Fiのアクセスポイントと携帯電話端末との間の通信を位置情報の測位を応用することによって、利用者によるインターネット接続の前後を問わず取得される位置情報のこと。

※「位置情報」とは、「移動体端末を所持する者の位置を示す情報」をいう(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解説)。



位置情報の取得

○業務上の必要に応じた取得(正当業務行為)※1

○他の機関からの要請に応じた取得

➤捜査機関の要請(裁判官の発付した令状)の場合

➤緊急避難の要件充足する場合(救助を行う機関)※2

※1 携帯電話で通信を行うために基地局の位置情報を取得する行為

※2 警察、海上保安庁又は消防その他これに準ずる機関からの客観的事実に基づく相当な理由のある要請

① 要救助者の生命又は身体に対する重大な危険が切迫

② 要救助者を早期に見つけるためにその者に係るGPS位置情報を取得することが不可欠

平成25年「緊急時等における位置情報の取扱いに関する検討会」において、「人命救助等におけるGPS位置情報の取扱いに関するとりまとめ」を公表し、ガイドラインを改正

位置情報の利用

○利用者の同意

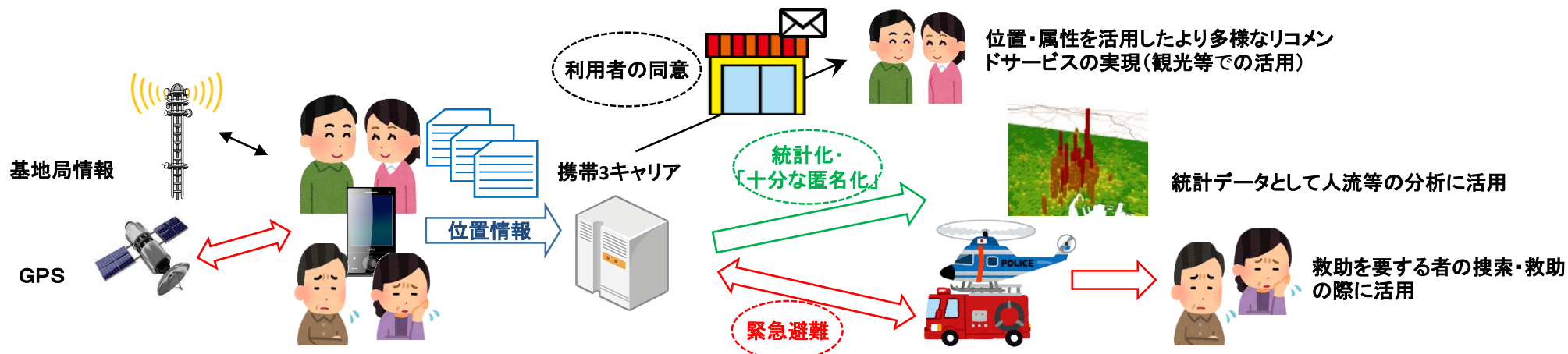
➤「十分な匿名化」※3の枠組み

契約約款等に基づく事前の包括同意であっても、有効な同意といえる。

※3 加工方法の組合せにより、その時点での技術水準では再特定化・再識別化が不可能又は極めて困難といえる程度に加工すること

○違法性阻却事由(緊急避難等)がある場合

平成26年「位置情報プライバシーレポート」での検討を受け、ガイドラインを改正
平成27年度・平成28年度に実施した調査研究において「十分な匿名化」の加工基準等の内容がまとめられ、それを受け民間ガイドラインの作成



位置情報に関するプライバシーの適切な保護と 社会的活用の両立に向けた実証実験等

31

概要

- 電気通信事業者が取り扱う位置情報等のパーソナルデータについては、高い機微性を有する一方で、防災・減災、街づくりなどに係る具体的需要が顕在化。
- パーソナルデータを適切に保護しつつ利活用を行う方策として、匿名化処理を施すことで、プライバシー上安全なデータに加工することが想定されているが、加工の過程で生じる中間データについて、漏えいリスクへの対応や、匿名化後の加工データとの突き合わせによる再識別化、再特定化を不可能とするため、事業者による適切な管理運用体制の構築が必要。
- このため、データの処理・加工・保存における安全確保技術を実証し、その成果をガイドライン等において示す。



スケジュール

平成27年度総務省実証実験

十分な匿名化の基準の検討・実証 等

平成28年度総務省実証実験

・匿名加工基準の検討・実証
・多様な利活用形態の検討・実証 等

民間ガイドライン策定

・認定個人情報保護団体(データ通信協会)
による個人情報保護ガイドライン策定 (H29.5)
・十分な秘匿化に関するガイドラインの策定
(H29.10 ※)

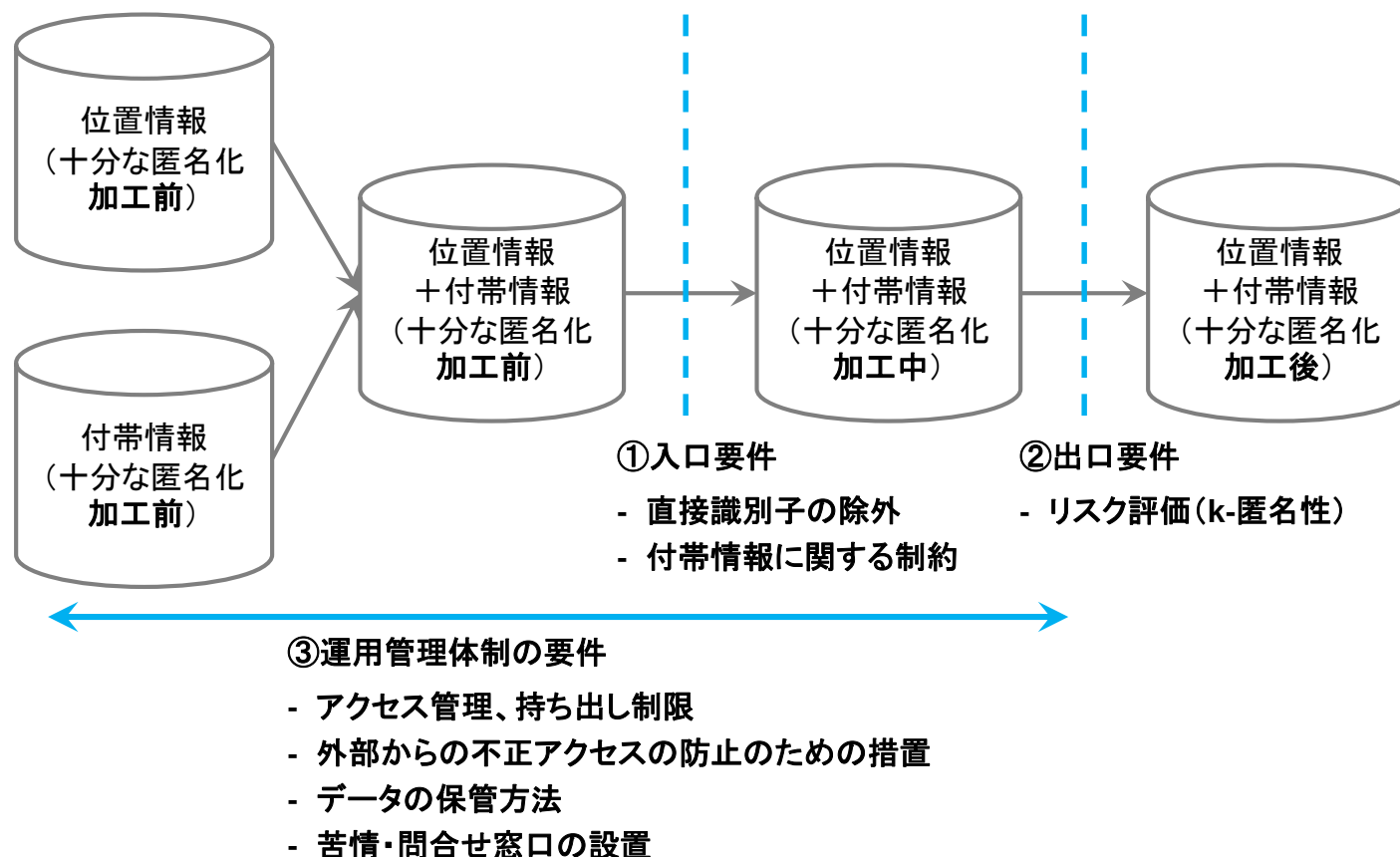
※ 通信4団体及びデータ通信協会による共同ガイドライン(次項参照)

概要

平成27、28年度「位置情報に関するプライバシーの適切な保護と社会的活用の両立に向けた調査研究」における報告書を踏まえ、データの利活用を推進するに当たって利用者の権利を害さないよう、位置情報を加工(「十分な匿名化」)して利活用する際に必要な措置に関する自主的なガイドラインを策定(平成29年10月)。※

※通信関連4団体(電気通信事業者協会、テレコムサービス協会、日本インターネットプロバイダ協会、日本ケーブルテレビ連盟)及び日本データ通信協会が策定。

データの加工プロセスにおける「十分な匿名化」を行うための要件 ①～③



「十分な秘匿化」に関するガイドライン

1. 趣旨
2. 用語の定義
3. 適用範囲
4. 「十分な秘匿化」に係る取扱い
 - 4.1. 「十分な秘匿化」による加工
 - 4.1.1. 位置情報と付帯情報との結合
 - 4.1.2. 入口要件
 - 4.1.3. 出口要件
 - 4.2. 安全管理措置
 - 4.2.1. 加工方法に関する情報
 - 4.2.2. 「十分な秘匿化」による加工途中の位置情報
 - 4.2.3. 「十分な秘匿化」がされた位置情報
 - 4.3. 通知及び同意・選択
 - 4.3.1. 通知及び同意の取得
 - 4.3.2. 苦情・相談窓口
 - 4.4. オプトアウト
 - 4.5. プライバシー影響評価(PIA)－管理運用体制の適切性の評価・検証－
5. 本ガイドラインの見直し