参考資料８

同意取得の在り方に関する参照文書

目次

はじめに

電気通信事業法（昭和 59 年法律第 86 号。以下「法」という。）は、第１章総則で秘密の保護（第４条）を規定し、第２章電気通信事業では、電気通信事業者に対して、業務の停止等の報告（第 28 条）、業務の改善命令（第 29 条）等の規律を、また、第６章罰則では、通信の秘密侵害罪（第 179 条）の規律等を定めている。

通信の秘密を侵害する行為は、「知得」（積極的に通信の秘密を知ろうとする意思の下で知ること）、「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）の３類型があるとされるが、通信の秘密を取得等する場合であっても、利用者[1]の有効な同意がある場合又は違法性阻却事由がある場合には、通信の秘密の侵害に当たらないとされている。このため、どのような場合であれば、利用者の有効な同意があるか又は違法性阻却事由があると判断できるかは極めて重要な事項である。

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[2]（以下「ガイドライン」という。）第３条の解説（２-13「本人の同意」）において「通信の秘密……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」とされており、利用者の同意や違法性阻却事由は、実務上の運用事例を中心に検討が深められてきた。

今後、規律を明確化することで事業者における予見可能性を高めるとともに、必要とされる場合には事後的に行政が機動的に業務改善命令等を発動する観点から、本文書は、その中でも重要な要素となる利用者に対する「同意取得の在り方」に関する論点[3]について主に検討して整理をした上で、公表するものである。

１　通信の秘密における「同意」取得の意味

１）通信の秘密の保護趣旨（保護法益）と「利用者の同意」の関係

通信の秘密を保護する趣旨は、①表現の自由を実効あらしめること、②プライバシー（私生活の秘密）を保護すること及び③安心・安全な通信（通信制度）に対する利用者の信頼・期待を保護することにある[4]。この趣旨の下、法第４条[5]、第 28 条、第 29 条、第 179 条等の規定により通信の秘密は保護が図られている[6]。

---

[1] 「利用者」とは、電気通信事業法上は、電気通信事業者との間に電気通信役務の提供を受ける契約を締結する者をいうが、加入電話にみられるように契約者でなくても電気通信役務の利用は可能であることから、これらの者の通信の秘密を保護するため、単なる電気通信役務の利用者を以下では「利用者」とする。

[2] 平成 29 年４月 18 日総務省告示第 152 号

[3] 「同意」に関する検討は様々な法領域で国内外問わず検討が深められているが、「同意」は各法領域においてその意味づけが異なり保護法益に照らして個別に検討する必要があるところ、本検討は、通信の秘密や通信に関連するプライバシー領域における利用者の同意に対する考え方を整理するものである。本検討においては、従来検討がなされてきた、法第 179 条における通信の秘密侵害罪における利用者の同意の解釈論を参考としている。

[4] 多賀谷一照ほか「電気通信事業法逐条解説改訂版」35 頁、総務省「プラットフォームサービスに関する研究会中間報告書」８頁

[5] 法第４条は、「通信の秘密」の保護（第１項）に加え、「通信に関して知り得た他人の秘密」の保護を規定（第２項）する。同項は、電気通信事業に対する利用者の信頼保持の観点から、電気通信事業に従事する者に対し、第１項より広い範囲の守秘義務を、職務上の義務として課している。

[6] 刑罰における一般論として、同意（承諾）は自ら処分し得る法益（個人的法益）に関するものでなければならない。通信の秘密侵害罪では、国家的・社会的法益とも言える③通信制度に対する信頼という保護法益のみならず、①表現の自由

個々のユーザの通信情報の取得・利用等については、通信当事者である利用者の「有効な同意」又は違法性阻却事由がある場合によって適法化される。この場合の利用者の「有効な同意」は、憲法上の重大な権利である通信の秘密についての権利放棄としての同意であるから、利用者がその意味を正確に理解した上で真意に基づいて同意したことが、利用者の「有効な同意」と評価されるためには求められている[7]。

２）利用者の「有効な同意」のために必要とされる「同意取得の在り方」

ア　法第 179 条における利用者の同意

法第 179 条は、「電気通信事業者の取扱中の通信の秘密……を侵した者は」処罰すると規定する。通信の秘密を侵害する行為は、通信当事者以外の第三者による行為を念頭に、知得（積極的に通信の秘密を知ろうとする意思の下で知ること）、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）を意味する。この場合、通信当事者である利用者の「有効な同意」がある場合には、通信当事者の意思に反しない利用であるため、通信の秘密の侵害に当たらないと解されている[8]。

利用者の「有効な同意」であるか否かは最終的には個々の事例に応じて司法判断に委ねられるものであり、また、それは利用者の内心に関わる主観的なものである。そこでこれまでの検討の中心は、事業者側の手続的・客観的な「同意取得の在り方」の適正性として「個別具体的」な同意、「明確」な同意であるか否かを類型的な分析により検討を加え、それを一般的に言い表す表現として通信の秘密に係る情報の取扱いについては各種報告書やガイドラインの第３条解説（２-13「本人の同意」）等において「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」であると示してきた。一方、通信当事者である利用者との間で本来的に求められているのは「有効な同意」であり、外形的な「同意取得の在り方」が適正か否かは厳密には異なる概念であることに留意が必要である（それぞれの解釈の詳細については「３「有効な同意」・「同意取得の在り方」」に後述）。

なお、法第 179 条は「電気通信事業者の取扱中の通信の秘密……を侵した」ときを対象とする。法は過失犯処罰を規定しないため、故意ではなく過失（重過失を含む。）の場合には規律の対象とならない[9]。

や②プライバシー保護といった個人的法益も重要としてこれまで考えてきたものといえる。保護法益に国家的法益や社会的法益が含まれる場合、通信当事者（本人）の同意のみでは不十分との指摘もありうるが、個人的法益の側面もそれら国家的法益・社会的法益同様に重要であると考えられる場合には、いずれか一方の法益侵害性が否定されるとして犯罪の成立を否定するとの見解もある（西田典之ほか「注釈刑法第１巻総論§１～72」349 頁）。

[7] 「有効な同意」であるためには通信当事者がその意味を正確に理解した上で真意に基づいて同意したといえなければならないことから、そもそものサービスの仕組みやデータ活用の在り方によっては、利用者の認知限界を超え、同意取得したとしても適法化できない場合も存在することに留意が必要である。

[8] 知得や窃用には、機械的・自動的に特定の条件に合致する通信を検知し、当該通信を通信当事者の意思に反して利用する場合のように機械的・自動的に処理される仕組みであっても該当し得る（電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会第一次とりまとめ（平成 26 年４月））。

[9] ただし、第 28 条にいう「通信の秘密の漏えい」には当たると解される（「電気通信事業法逐条解説改訂版」37 頁）。

イ　法第 29 条における「同意取得の在り方」

他方、法第 29 条は、「業務の方法に関し通信の秘密の確保に支障があるとき」等を対象とする電気通信事業者の業務の方法に対する規律であり、業務の方法として外形的に示される「同意取得の在り方」（事業者の手続的な担保の点）を直接的な対象とする。ここでは、「同意取得の在り方」そのものをまずは対象とし、当該サービスにおける通常人（一般的な理解力の利用者）を基準とし、当該同意取得手続が一般的な理解力の利用者により認識し十分理解した上で判断可能なものであるかどうかについて評価する。例えば、「個別具体的かつ明確な同意」が取得されているかどうかを確認する方法などがある。ここでの「同意取得の在り方」は従来検討されてきた法第 179 条における検討状況が基本的には妥当するものであり、「有効な同意」すなわち、利用者から見て真に理解して同意しているかにつながるものといえる[10]。

なお、法第 29 条は「電気通信事業者の業務の方法に関し通信の秘密の確保に支障があるとき」を対象としており、過失（重過失を含む。）の場合であっても対象となり得るため、例えば、事故や犯罪被害（例えば、サイバー攻撃など）等の電気通信事業者及びその従事者に故意がない事由により漏えいした場合であっても法第 29 条にいう「通信の秘密の確保に支障」がなかったか否かが問題となると考えられる。

3）法第 29 条第 1 項第 1 号に関する執行指針の効果

ア　執行指針の適用範囲

法第 29 条第 1 項第 1 号が導入された際には、「通信の秘密の確保に支障がある」とは、伝統的な電話交換機を要する電気通信サービスを想定して、「例えば、機械室への入退室の記録の管理を怠るなど設備の管理運用がずさんであり、通信の秘密が漏えいしているときをいう。」[11]とされており、通信の秘密に係る情報に対する安全管理措置[12]を念頭に置いたものであると考えることができる。

これとともに、「業務の方法」とは、業務の管理運営の方法、窓口業務等の日常業務の取扱方法をいうとしているところ、通信の秘密に係る情報の取得・利用・提供の方法の全ての場面が「業務の方法」に該当するため、当該取得・利用・提供の方法において事業者の「同意取得の在り方」が適切であることは、利用者の通信の秘密に係る情報の取得等を正当化するための一つの根拠として意味を持つ。したがって、通信の秘密に係る情報の取得等に関する「同意取得の在り方」が不適切な場合は、「業務の方法に関し通信の秘密の確保に支障がある」に該当し、法第 29 条の対象となり得ると考える。

---

[10] 通信の秘密侵害罪（法第 179 条）は刑法の一般的な考え同様に、構成要件該当事実が認められたとしても、利用者の同意又は違法性阻却事由がある場合には、通信の秘密に係る情報の取得・利用等を適法化してきた。これまで、行政的な規律においても通秘侵害罪における考え方を借用し、基本的には同様の枠組みで検討が行われてきている。

[11] 「電気通信事業法逐条解説改訂版」154 頁

[12] 現在の電気通信サービス（電話、インターネット接続等）に照らして考えると、①通信を成立させるためのサーバ等の物理的な設備に対する安全管理措置、②当該サーバ等で管理・保存されている通信の秘密に係る情報に対するアクセス権限等が適切に行われているか否か等を意味する技術的安全管理措置、③通信の秘密に係る情報を取り扱う従業員等に対する教育を施す等を意味する人的安全管理措置、④あらかじめ整備された規律や漏えい等の対応をするための体制整備等を意味する組織的安全管理措置をも包含するもの

イ　法第 29 条第 1 項第 1 号に関する執行指針との関係

通信サービスの急速な技術革新や多様化が進み、通信サービスを中核とした多角的・複合的サービスが台頭するとともに、電気通信の社会経済活動の中における役割や位置づけが増して、社会全体が電気通信に依存する度合いが高まり、電気通信が単なる情報インフラではなく社会インフラとして更に重要度を高めている。このため、通信の秘密の保護に関しても、様々なステークホルダーが相互に関係をもった複雑な構造の中で、柔軟な履行の確保や正当業務行為の見直し、さらにはこれまで以上に事業者側の自己責任による判断での通信の秘密保護を図る機会が増加し、事業者の側における自律的な判断の必要性も拡大している。

これまで、通信の秘密に係る情報の取扱いについては、事前に事業者による個別の相談が行われ、その適正な取扱いが確保されることが多く見られた。また、通信の秘密に関する規律について行政の執行場面を定める法第 29 条と罰則を定める法第 179 条の違いが明確に意識されて議論されるよりもむしろ、法第 179 条の罰則適用の可能性の有無の観点から包含的に解釈検討が行われる場面が多く見られたものと思われる。しかしながら、今後各事業者側における自律的な判断の重要性が高まる中で、刑罰を中心とした厳格な規律のみではなく、事業者判断と行政規律における柔軟な執行を組み合わせる場面も増えるものと想定される。

このような状況を踏まえ、事業者の予見可能性や透明性を高め、通信サービスのスピード感ある柔軟な事業展開を更に可能とし後押しする観点から、今回初めて、法第 29 条第１項第１号に基づく「通信の秘密の確保に支障があるときの業務の改善命令の発動に係る指針」が公表されたものである。この中でも、利用者の「有効な同意」に関する判断に関わる項目も示されているところである。本参照文書は、この執行指針と組み合わせて参照することが有効である。

（参考）通信の秘密の確保に支障があるときの業務の改善命令の発動に係る指針（抜粋）

（１）通信の秘密に係る情報の取扱いを示したポリシー・方針等が不適切な例

ⅰ．通信の秘密に係る情報の取扱いを示したポリシー・方針等（以下「ポリシー等」という。）が平易で分かりやすく記載されていないなど、利用者利便を損なっていること[18]。
ⅱ．ポリシー等へのアクセス方法が不十分であること。
ⅲ．サービス利用の許諾条件として、サービス提供などに係る業務上の必要以上に通信の秘密に係る情報の利用を可能としていること。
ⅳ．サービス利用の許諾条件として、通信の秘密を取り扱うために必要とされる利用者による同意やオプトアウト等の関与の機会を与えないままに、事実上、利用者に通信の秘密を放棄させていること。
ⅴ．通信の秘密の漏えい等の事故が発生しても、電気通信事業者が一切の責めを負わないとしていること。

（２）通信の秘密の取得・利用等が不適切な例

ⅰ．利用者からの通信の秘密の取得や利用等に当たって、合理的な理由なく約款等による同意プロセスを恒常的に採用していること。
ⅱ．通信の秘密の取得・利用等が法令行為・正当業務行為などに該当しない場合に、取得・利用目的を明示して適切に同意取得をしないままに通信の秘密を取得・利用し、又は同意取得時に明示した取得・利用目的を超えて通信の秘密を利用していること。
ⅲ．法令行為・正当業務行為として想定された範囲を超えて、通信の秘密の取得・利用等を利用者から適切な形で同意を取得するなどの正当化根拠もなく行っていること。
ⅳ．取得した通信の秘密について、利用者による通信の秘密の取扱いに関して必要とされる同意やオプトアウト等の関与を妨げ、事実上、通信の秘密を無制限に利用していること。

（４）苦情・相談等対応態勢が不適切な例

ⅰ．通信の秘密に係る苦情・相談対応の社内規則等の不備などが原因で、その苦情・相談窓口が機能せず、苦情等が頻発していること。
ⅱ．通信の秘密に係る苦情・相談窓口が形骸化し、通信の秘密の漏えい等の事故の端緒となる重要情報の見落としが常態化していること。
ⅲ．通信の秘密の漏えい等の事故が発生した場合において、利用者への説明や情報提供等の措置が不十分なため、利用者に対する救済措置が適切に機能せず、被害拡大を招いたこと。
ⅳ．利用者の多様性に配慮したアクセス時間・アクセス手段（例えば、電話、手紙、FAX、電子メールなど）の設定が不十分であり、通信の秘密に係る苦情等の受付態勢が不適切なこと。

18　電気通信事業者の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）の公表等については、「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」第 14 条第１項等を参照のこと。

２　「通信の秘密」の侵害を防止する観点からのリスク分析（特定・評価・管理）の重要性

１）「通信の秘密」におけるリスク分析と「同意取得の在り方」

ア　リスクベースアプローチによる事業者の自律的な対応の重要性

リスクベースアプローチは、デジタル化の進展に伴い、様々な技術やサービスが新たに創出され、それに呼応してプライバシーリスクも多様化しているため、政府・事業者においてもそれらの予測・把握が困難となっている点を踏まえ、新たに発生するリスクにも対応可能な枠組みとして推奨される考え方である[13]。

事業者においてあらかじめ潜在的に高リスクの特定・発見とこれに対する柔軟・迅速な対応を実現することで、基本的権利を確保することに主眼を置くもので、進化・競争の激しい情報通信社会における法による事前規制の限界を解消する一つの方法論として機能することが期待され、事業者の責任による自律的な自己評価・自己管理と政府による柔軟な事後規制と相互補完することにより実効性を持つことが期待される。

リスクベースアプローチにおいては、『リスク』の概念が曖昧であることからそれぞれの場面における『リスク』の中核が何かについて、検討することが必要となる。この際、考慮すべきリスクとして、対象となり得る利用者に対するリスクとともに、サービスの性質に応じて社会的影響が大きいものである場合には社会的側面についても考慮に入れることが考えられる。このリスクベースアプローチは、プライバシー影響評価（PIA）及びデータ管理者の体制等と一体的に検討されることが一般的である[14]。

イ　プライバシー影響評価（PIA）の「通信の秘密」への応用

プライバシー影響評価（PIA : Privacy Impact Assessment）[15]は、新たなサービス等を提供する際における情報処理等でのプライバシーに対する潜在的な影響を特定・評価するための手段であり、プライバシーリスクを予め把握し適切な対応方法を設計[16]するために行われるものであり、特に利用者に係るプライバシー性が高い重要なデータを扱う際（すなわちリスクが高い場合）に利用者の権利や自由に対する影響やリスクを適切に把握し管理する観点から有用性が高いと考えられる。一般に、PIA の公開は義務づけられるものではないが、事前協議の場合や監督機関から求められたときには通知しなければならないとされている。このような PIA は事業者の信頼性の醸成や、説明

---

[13] 例えば、欧州の GDPR や、米国の NIST（アメリカ国立標準技術研究所）が民間事業者向けに公表している「プライバシー・フレームワーク」（2020 年 1 月 16 日：NIST PRIVACY FRAMEWORK: A TOOL FOR IMPROVING PRIVACY THROUGH ENTERPRISE RISK MANAGEMENT）においてもリスクベースアプローチの考え方が見られる。この「プライバシー・フレームワーク」と「サイバーセキュリティ・フレームワーク」（2018 年４月：Framework for Improving Critical Infrastructure Cybersecurity）をより実践的な内容としたものとして「SP800-53Revison5」（2020 年９月 Security and Privacy Controls for Information Systems and Organizations）がある。

[14] リスクベースアプローチには、リスクが低いものに対して、利用者の権利が軽視される可能性があること、また、データ管理者の心の中に利用者の権利保護の意識がない場合全く機能しない可能性があること等の問題点も指摘される。

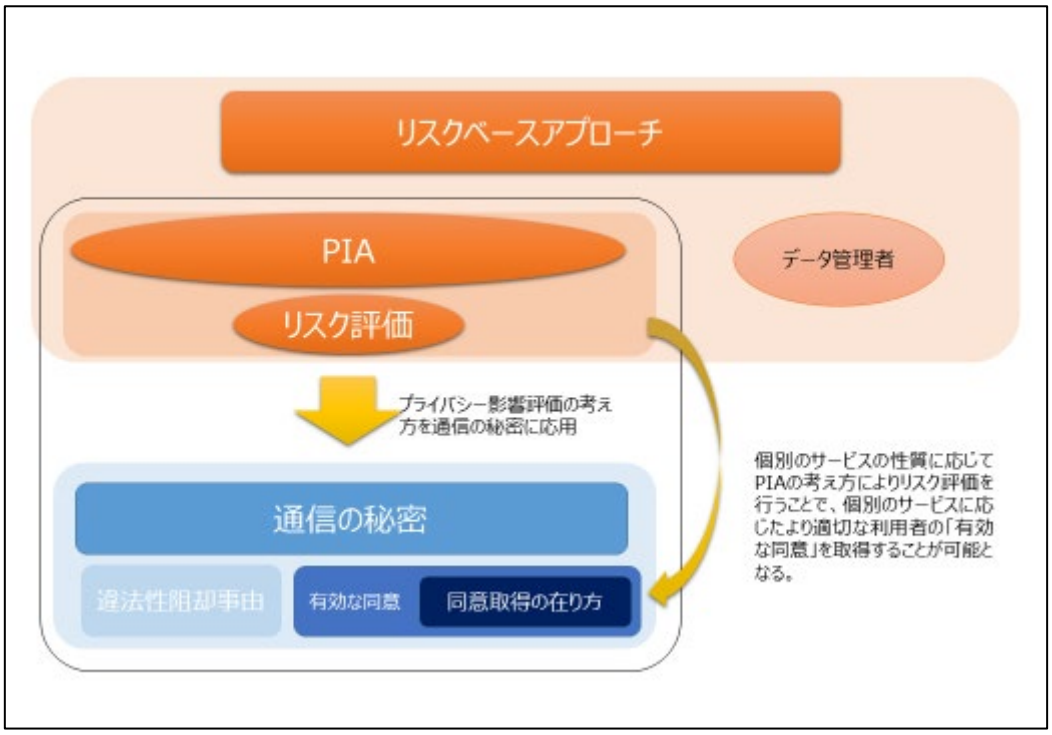
[15] PIA は米国、カナダ、オーストラリア等で行われてきたものであり、GDPR においては、DPIA（Data Protection Impact Assessment : データ保護影響評価）として同種の規律があり、特にプライバシーへの重大な影響が想定される情報を取り扱う場合に導入が義務付けられている。また、日本においてもいわゆるマイナンバー法に導入されている。

[16] 新たなサービス提供等を検討する場合にも、可能な限り早い段階から PIA を検討することにより、予め適切な取り扱いを組み込むプライバシー・バイ・デザインを実現することが望ましいと考えられる。

責任及び透明性の確保に役立つものと考えられる[17]。

一般的に、PIA を導入する際には、①処理される情報は何か、②処理の目的は何か、③情報の処理によって情報主体又は社会全体にもたらされる便益は何か、④情報受領者は誰で、情報をどのように扱うのか、⑤情報のこの処理によって実行されるビジネスプロセスは何か、⑥どの情報主体がこの処理の影響を受けるか、⑦プライバシープロセスはどのように実行されるか（同意、拒否、アクセス、修正及び削除等）、⑧情報主体はどのように通知されるか及び同意は求められるか。プロセスはその状況と一致するか、などを要素として検討することが適切であると考えられる[18]。

※　リスクに応じた「有効な同意」の取得のイメージ



PIA はプライバシーリスクを特定・評価・管理するための手法であるところ、一般に「通信の秘密」に関する情報は、電気通信役務の利用者にとって、プライバシー性が高い重要なデータであり、PIA を応用することで、通信の秘密に係る情報の主体の権利や自由に対する影響やリスクを適切に把握し管理することが可能となる。さらに、PIA の考え方を応用することで、「表現の自由」に対する脅威・リスクや「安心安全な通信網」への利用者の信頼・期待といった社会的側面も一定程度加味して検討し得る。PIA の考え方を「通信の秘密」に対して応用する（以下「リスク評価」という。）有用

[17] GDPR 第 4 章第 3 節参照
[18] ISO/IEC29134：2017

性は高いものと考えられる[19]。

通信の秘密との関係で考えると「リスク評価」は、事前にリスクを特定・評価し、①当該通信の秘密に係る情報の取得・利用等によるユーザのプライバシーや表現の自由、安心・安全な通信への信頼の確保に対するリスク（行為の性質、結果の重大性及び結果発生の蓋然性等）、また、②当該リスクを軽減するために求められる同意の取得方法その他の適切な措置等について、より具体的に検討を加えることができる。「リスク評価」は正当業務行為として適法化される行為についても適用可能なアプローチであるが、本文書では「同意取得の在り方」に着目して検討を行う。

ウ　リスク評価を応用した「有効な同意」の取得の在り方

通信の秘密は、重要な権利であることから、その権利放棄に係る「同意取得の在り方」については原則として「個別具体的かつ明確な」同意が必要とされる厳格な解釈がされてきた。しかしながら、従来から、個別の事例を詳細に検討し、各事例において通信の秘密の侵害により実現する法益（目的の正当性）の検討に加えて、ここでのリスク評価を行うことにより、「同意取得の在り方」についても事前の包括同意を許容するなど、原則としての「個別具体的かつ明確な」同意手続を事例に応じて柔軟に解釈する対応も行われており、その際の検討事項などは参考になる[20]。

「リスク評価」は、リスクに合わせたルール作りを試みるもので事業者の側で適切な「同意取得の在り方」を決定する際の検討に資するものといえる。「リスク評価」は、当該行為の性質、当該行為から発生する結果の重大性及び結果発生の蓋然性などの要素を分析することでそのリスクに応じた対応を行うものである。また、それを公表することで利用者に対する透明性・信頼確保を担保する意味もある。

「有効な同意」であるか否かは様々な要素を考慮に入れることが考え得るものであり、同意の形式面のみに偏重[21]する必要はなく、事業者によるリスク評価の結果、利用者の「有効な同意」が取得されていると実質的に評価できる場合には、「同意取得の在り方」についても厳格な同意手続から一定のリスク評価結果に応じた手続とすることもあり得る。特に、リスク評価で考慮すべき点としては、同意手続を簡素化するとともに代替的な利用者保護が図られている必要があり、全体としての利用者保護が低下すること

---

[19] 社会的法益・国家的法益との関係で影響が大きい場合にはより慎重な検討を要する。

[20] 例えば、「マルウェアに感染している可能性が高い端末の利用に対する注意喚起」について、通信の秘密を侵害することなく本件対策を実施するためには、個別具体的かつ明確な同意の取得ではなくとも一定の場合には電気通信役務提供契約の締結時又は契約条件変更時に、契約約款等に基づく包括的な同意を取得することで足りるとされている。具体的には、a　注意喚起を希望しない者（オプトアウトした者）の利益が侵害されないような態勢を整えること、b　利用者が一旦契約約款等に同意した後も、随時、同意内容を変更（設定変更）できるようにすること、c　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、d　本件取組の内容とともに、注意喚起を望まない利用者は随時同意内容を変更（設定変更）できること及びその方法につき利用者に相応の周知を図ること、といった条件が満たされている場合には、契約約款等に基づく事前の包括同意であっても、当該注意喚起を行うための通信の秘密に属する事項の利用等について有効な同意があるといえるものとする（電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会　第三次とりまとめ（平成30年９月））。

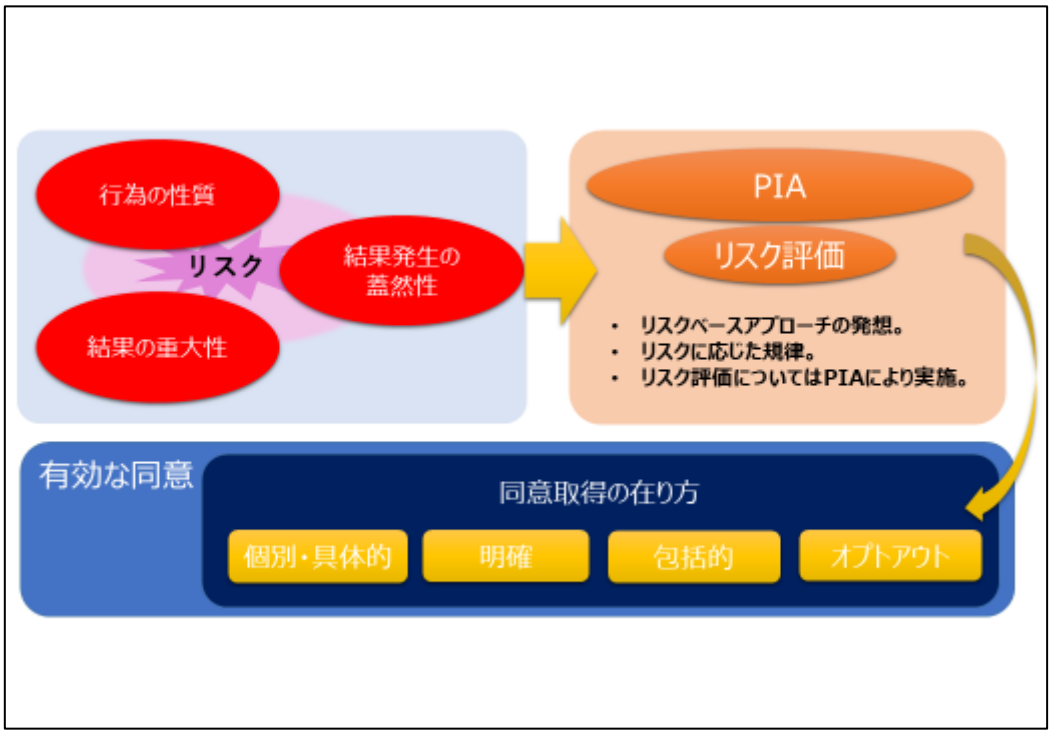
[21] 同意の形式面のみに偏重することにより、利用者が同意の意味を十分理解しないままクリックしてしまういわゆる「同意疲れ」が生じている問題があり、利用者の立場に立った検討が求められる。

がないように配慮する必要がある。代替的な利用者保護としては例えば、対象となる通信の秘密に係る情報及びその具体的な取得・利用等の取扱いについて利用者にわかりやすく説明し、また、利用者における事後の情報コントロールが仕組み上も容易であること等により利用者に対する透明性が確保されていること等が考えられる。

「リスク評価」についてその検討プロセス全ての公開を義務づけるものではないが、これまで厳格性が要求されていた同意手続に対する判断を事業者側が行った際にはそのサービスインの時点（又はそれ以前の時点）[22]で、その概要等を分かりやすく利用者に対して公開することが適当と考えられる。また、事前に総務省と協議する場合や総務省が求めた場合には「リスク評価」を提出できるよう準備することが望ましい。

「同意取得の在り方」を検討するに当たり、「リスク評価」はサービス提供前に実施することが必須であるが、サービス提供中においても定期的な見直し・点検が必要である。そのため、事前に「リスク評価」の更新にかかるルールを明確化することが望ましい。

※　リスク評価を応用した「有効な同意」の取得のイメージ



エ　「同意取得の在り方」に係る「リスク評価」を各事業者の対応によらずに行う場合

「リスク評価」は、評価する行為及びその適切な管理そのものにも「同意取得の在り

[22] なお、通信の秘密に係る情報の取得や利用が、正当業務行為等を理由に正当化されていた場合において、当該情報について新たな目的のための利用を開始しようとする場合等については、その開始前であれば足りる。この際、個人情報の保護に関する法律（平成 15 年法律第 57 号。以下「個人情報保護法」という。）など他の法令についても必要とされる対応を確認することは言うまでもない。

方」を決定する根拠となる性質を有すると考えられる。業界団体等の場において、「リスク評価」等も行った上で、同種サービスにおける業界ルールのような形で取扱いを検討した場合には、それを導入することも想定し得る。

２）「リスク評価」のプロセス

「リスク評価」において、①評価対象となるサービス、②通信の秘密に係る情報の取得・利用等の必要性及び比例性の評価、③リスクの特定・評価、④対策の決定・リスクの管理、のプロセス等を考えることができる。そのプロセスにおいていかなる要素が「同意取得の在り方」に対していかなる影響を与えるか等について検討が必要である[23]。

①　評価対象となるサービス

-利用目的は何か
-それにより得られる利用者又は社会の便益は何か
-関係者及び責任主体は誰か。各関係者においてどのように扱われるか
-新しいサービスか、あるサービスに対する付加的なサービスか
-利用者はどのように関与するのか（同意・透明性・修正及び削除等）
-利用者のリテラシーはどの程度か

②　通信の秘密に係る情報の取得・利用等の必要性及び比例性の評価

-①評価対象となるサービス（利用目的）において、通信の秘密に係る情報の取得・利用等の必要性はあるか（他の情報により代替して目的を達成できるのではないか）
-利用目的に照らして、サービスにおいて利用する情報は適切な形で利用（その質・量・期間等）され不必要な利用をすることなく比例性を満たしているか

③　リスクの特定・評価

-①においていかなる通信の秘密及びプライバシーリスク等があり、結果の重大性及びその発生の蓋然性はどの程度か。
-それぞれのリスクに対して、利用者はどのような影響を受けるのか。
-その評価について、対外的に公表できるものが作成されているか。

④　対策の決定・リスクの管理

-それぞれのリスクに対して、どのような対策を講じるか。
-評価対象となるサービスは、ⅰ当該通信の秘密に係る情報の取得・利用等によるユーザのプライバシーや表現の自由、安心・安全な通信への信頼の確保に対するリスクが大きいか、小さいか、また、ⅱ当該リスクを軽減するために、どのような同意

[23] 例えば、事業者側がこれまで様々なサービスにおいて利用者が同意するように画面設計を検討してきた蓄積（ABテスト）や、利用者においてある事項に同意するか否かの意思決定においてどのような要素をどのように評価しているか、またどのような情報をどう認知しているのかといった点の実証を行うなど引き続き検討が必要である。

の取得方法が適当か、また、その他どのような措置が適当か。

３　「有効な同意」・「同意取得の在り方」

１）概要・定義

「有効な同意」の有無は個別的ケースにおいて判断されるべきであるところ、総務省ではこれまで、「有効な同意」について、一般に「個別具体的かつ明確な同意」[24]であることが必要と解し、事業者が利用者との関係で手続的に一定の担保がとれていることをもって「有効な同意」と解してきた。すなわち、同意の有効性の判断を、手続的な要素である「個別具体的」な同意か。「明確」な同意か。という２つの観点から「同意取得の在り方」を定式化し、類型的な検討により分析的なアプローチをしてきた。

もっとも、「有効な同意」と評価できるか否かは本来、当該要素のみにとどまるものではなく、例えば、同意の任意性についても個別ケースでは検討を要する場合があるなど、上記２要件が「有効な同意」における必要十分条件でないことにも留意が必要である。

また、「有効な同意」であるか、「同意取得の在り方」として適切か否かは本来、個別事例におけるリスクに比例して評価が変わり得るという特徴もある。加えて、利用者が理解することが困難なものについてはそもそも、「有効な同意」として利用者の同意を正当化根拠とすることができないものもあるのではないかとの指摘もあるところである。

２）「個別具体的」・「明確」

ア　「個別具体的」とは

「個別具体的」とはサービスごとに通信の秘密の取扱いについての同意であることを本人が認識した上で行うことを意味すると解し、①「個別」のサービスごとに同意を取得するという意味、②契約約款事項としての包括的な同意（契約締結時の約款同意や約款変更による同意）ではなく、通信の秘密に関する特定の事項を本人が「具体的に」認識した上で同意を取得するという意味、の２つの意味を含み使用されてきた[25]。

「具体的」については、当該同意においてどの程度の情報を、どのように利用者に対して説明して同意を取得するか、また、同意範囲の明確性という意味でも検討が必要であって、利用者が具体的に通信の秘密に関する事項について認識していない契約約款[26]

---

[24] なお、当初は、「個別かつ明確な同意」であることが必要である（例えば、「位置情報プライバシーレポート」等）としており、「具体的」との要件はなく「具体的」の意味するところが不明確であるとの指摘も事業者よりなされている。

[25] なお、「個別」については個別の通信ごとの「都度」同意を意味すると考えることもできるが、「通信の秘密」の取得等における「同意」では都度同意を求めるものではない。

[26] 契約約款は、一人一人との細かい交渉を省き、取引の画一的処理をすることで経済合理性を高める等の理由により類型化して行うためのツールである。このため一人一人との「個別」の合意形成のプロセスは想定されていないところ、両当事者において、取引内容が画一であることが合理的であると客観的に評価される場合に認められるものである。このため、同様の趣旨で、例えば、位置情報サービスを受けるために、利用者の位置情報を取得することについては、契約約款等の記載でも両当事者にとって合理的であると想定され、そこでの合意事項が、位置情報（通信の秘密に該当するものも含む。）の取得・利用に対する「有効な同意」であると評価し得る。もっとも、位置情報以外の通信の秘密に関する事項を取得することは適当でなく、位置情報についても広告目的等で利用することは目的外の利用であるし、そのことを契約約款で記載したとしても、利用者がそのことを認識する特段の事情が認められない限りは、「有効な同意」とは評価できない。

等による包括的な同意（契約締結時の約款全体に対する抽象的な同意や約款変更時の変更の事実のみに対する同意）ではなく、通信の秘密に関する事項を利用者が「具体的」に認識した上で同意を取得することを意味する[27]。

同意が「具体的」であることを求める趣旨は、通信当事者がその同意の内容及び意味を正確に認識し、十分に理解した上で、真意に基づいて行った同意でなければ、通信の秘密についての有効な同意（法益の放棄）をしたものとは評価できないためである。

そして、同意する上で認識する必要のある事項としては、一般的に、

- ✓ 取得される情報の内容
- ✓ 取得及び利用の主体
- ✓ 取得される情報の利用目的
- ✓ 取得される情報の利用態様
- ✓ 取得される情報の利用期間
- ✓ 取得される情報に関する問合せ窓口等
- ✓ 同意を撤回できること及び撤回の方法

等が考えられるところ、これらの事項について何を、どのように利用者に提示し同意を取得するか。特に利用目的については、その全てを明示すべきか。明示するとしてどの程度詳細に明示すべきかについては個別のサービスごとに検討の余地がある。

これらの事項については、各種サービスに照らして、利用者がその内容を十分に理解できるように説明する必要があり、その内容及び量等に応じて、分かりやすい説明を行う必要がある。そして、説明に当たっては、利用者が必ずしも説明される事項の全てを注意深く読み込むとは限らないことから、利用者に対して複数回の画面遷移やスクロールを求める場合には、利用者が必要な情報を認識できるよう特に留意すべきである。

この点、当該情報が一定のサービス類型に照らして通常想定され得る利用にとどまる場合においては、個別の利用目的を詳細に明示する代わりにサービス類型ごとに共通する利用目的を明示した上で当該利用目的について同意を取得することも可能であると考えられる。これは利用者において、通常想定され得る利用にとどまる場合は、個別の利用目的の明示がなくとも、その意味を理解できる場合があると想定できるためである。

もっとも、「一定のサービス類型に照らして通常想定され得る利用」か否かについては、一般論としては通常人の認識を基準として判断すべきであるが、技術の進展・時代の変化等に伴い利用者のリテラシーが変化することから同じサービス類型であってもその時点によって異なり得るものであり、また、当該企業の提供するサービス内容やそれに対して利用者が期待する情報の取扱いによっても「通常想定され得る利用」の範囲は異なることが想定されるため、同じサービス類型であってもそれを提供するサービス主体によってその結論が異なることが生じ得る。

また、通信の秘密の取得・利用に関する同意については、当該サービスにおいて、サ

[27] なお、電気通信事業者はプライバシーポリシーを公表することが適切であるとされる（「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解説」第 14 条参照、スマホアプリ事業者については、「スマートフォン・プライバシー・イニシアティブⅢ」参照）。

ービス類型ごとの同意のみならず、利用目的ごとの同意をも取得する必要があるか否かは各事業者において判断を要するものと考える。その際の検討の一つの資料として、「リスク評価」を用いることが考えられる。

もっとも、通信の秘密に係る情報については、そもそも電気通信サービスの役務提供以外の目的で通信当事者以外の第三者へ提供されることを前提とする情報ではなく、また第三者への提供後、当該情報が拡散し得ることから、第三者提供を伴う態様での利用目的の場合においてはその旨を利用者が明確に認識できるようにする必要がある[28]。

イ 「明確」とは

「明確」とは画面上でのクリック、チェックボックスへのチェックや文書による同意など外部的に同意の事実が明らかな場合を意味している[29]。もっとも、事前にチェックされたデフォルトオンによることや当該サービスの利用を開始すること、ウェブサイトやアプリケーション上の画面をスクロールするだけでは「明確」な同意とはいえない。

なお、利用者の同意においては、同意範囲の明確性も重要な要素であるが、ここは、意思表示が明確か否かという点を評価し、範囲の明確性については前述のとおり「具体的」か否かで考慮するものとする。

3）その他

「有効な同意」の存在時期は、通信の秘密に係る情報の知得、窃用、漏えい（取得、利用、提供）それぞれの時点で必要（なお、情報取得の時点でその後の利活用を含めて同意取得することは可能）であり、利用者の同意行為は、情報取得等の時点以前になされる必要がある（すなわち事後的な同意は認められない）[30]。

「有効な同意」は、判断能力のある利用者の真意に出たものでなければならない。このため、幼児や高度の精神障害者の同意、強制や錯誤に基づく同意は「有効な同意」とは言い難い。未成年者、成年被後見人、被保佐人及び補助人など、同意したことによって生ずる結果について、判断できる能力を有していないなどの場合には、親権者や法定代理人等から同意を得る必要がある。

また、事業者は一度同意を取得したとしても、利用者に対し、情報利活用の透明性を確保し、利用者の同意撤回が容易となるようなサービスの仕組みにしなければならない[31]。

---

[28] 位置情報の利活用の有用性や要望に鑑み整理したものとして「位置情報プライバシーレポート」や、「電気通信事業における「十分な匿名化」に関するガイドライン」がある。それらにおいて、一定の要件の下「十分に匿名化」された位置情報については、契約約款等に基づく事前の包括的同意に基づいて利用・第三者提供できると整理されている。

[29] 「位置情報プライバシーレポート」（2014年7月）27頁

[30] 電気通信事業者は、電気通信役務の提供に「通信の秘密」に係る情報を取得・利用する場合がある。その場合は、当該行為については正当業務行為として整理できる場合があり、この際「有効な同意」は目的外の利用や提供の時点で必要となる。

[31] もっとも、サービス提供上必要不可欠な「通信の秘密」の取得・利用・提供については、その取得等について正当業務行為として適法化できる場合があり、利用者の同意を正当化根拠としないものについては同意撤回の仕組みは不要である。

４　個別ケースの検討

以下では、事業者より質問等をよく受けるものの代表例を検討する。もっとも、前述のとおり、通信の秘密に係る情報の利活用に対する利用者の同意が「有効な同意」であるか否かは、各事例における「リスク評価」との関係にも留意が必要である。

１－１）ユーザアカウント作成時における一括同意

前述のとおり、通信の秘密に関する有効な同意とは、通信当事者がその意味を正確に理解した上で真意に基づいて同意したと評価できる必要がある。

他方、利用者から取得される利用者情報が増えるにつれて、累次の同意取得手続が繰り返され、かつ、その活用の方法が複雑になり多岐にわたるにつれて、同意取得時の説明も複雑でわかりにくくなる結果、かえって利用者が十分に理解しないままに同意してしまう、いわゆる「同意疲れ」が課題になっている[32]。

このため、サービスが複数ある場合に、全ての場合に個別サービスごとの同意をその都度取得する場合もあるものの、適切なリスク評価プロセスを行った上で、当該サービス群において通信の秘密に係る情報の活用方法が複雑になり多岐に渡らない範囲において、それらを束ねて一括で説明して同意取得することについても、そのことを利用者が明確に認識及び理解した上で、真意に基づいた同意であると評価できる場合には、「有効な同意」として認められ得ると考えられる。一括同意が「有効な同意」たり得る場合であっても、後に個別のサービスごとに同意撤回できるようにするとともに、かつ撤回するためのページへのアクセスが容易である等の対応が求められる。

なお、複数のサービスについて、複数の利用目的を一括して同意を取得することは、一般的に利用者にとってその説明は理解し難いものとなっており、その説明・同意取得のプロセスに相当の注意・丁寧さが必要である。

[32] 総務省「プラットフォームサービスに関する研究会最終報告書」（2020 年２月）12 頁

※　同意プロセスの全体（イメージ）

１－２）２階層による同意取得

ア　許容性

前述のとおり、通信の秘密に関する「有効な同意」と評価するためには、通信当事者がその同意の内容及び意味を正確に認識し、十分に理解した上で、真意に基づいて行った同意と言える必要がある。

他方、利用者から取得される利用者情報が増えるにつれて、累次の同意取得手続が繰り返され、かつ、その活用の方法が複雑になり多岐にわたるにつれて、同意取得時の説明も複雑で分かりにくくなる結果、かえって利用者が十分に理解しないままに同意してしまう、いわゆる「同意疲れ」が課題になっている。

このため利用者に対して、同意事項を詳細に全て示すだけでは逆に不適切であり、適切なリスク評価プロセスを行った上で、明確かつ平易な言葉を使用した分かりやすい概要版を第１階層に提示し、関心がある利用者がクリックした場合にのみ詳細な情報が示されている第２階層（又はそれ以降の階層）へ誘導する仕組みで同意を取得する方法についても、以下の点に留意した上で、かつ、後に個別のサービスごとに同意撤回でき、かつ撤回するためのページへのアクセスが容易であるなどの措置を講じた上であれば、許容され得ると考える。

イ　第１階層で示す事項は何か。

通信当事者がその内容及び意味を正確に理解した上で真意に基づいて同意したといえるために、第１階層において概要版を示す趣旨に照らすと、前記のとおり、説明に当

たっては、端末における１、２画面程度で（複数回の画面遷移やスクロールを行うことなく）同意事項の説明を収めることが望ましい。

その上で、第１階層に掲載すべき事項として、①取得される情報の内容、②取得される情報の利用目的のうち重要なもの、③取得される情報の利用態様・取得主体等が主に考えられる。なお、前述のとおり、当該情報がサービス類型に照らして通常想定され得る利用にとどまる場合においては個別の利用目的を詳細に明示する必要はなく、一定のサービス類型ごとに同意を取得すれば足りると考えられる。もっとも、第１階層でどのような事項を説明し同意を取得する必要があるかについては個別ケースに基づく判断となるため、どのような事項を示すかについては各事業者での判断が必要である[33]。

１－３）既存サービスに付加的サービスを追加する場合の同意取得の在り方

ア 新たな同意が必要か否か

当初のサービスでは提供していなかった付加的なサービスを追加で提供する場合は、付加的なサービスが当初サービスから通常想定され得る利用といえない限りは、新たな利用目的についての同意が追加で必要になるものと考える。

例えば、メールサービスを提供していた事業者がメール本文を新たに分析することで、メールサービスを含む各種サービスをパーソナライズすることを付加サービスとする場合は、当初サービスから通常想定され得る利用とはいえないと考えられるので、当該サービスに対する新たな同意が追加で別途必要になる。

他方で、当初サービスについて「有効な同意」を取得しており、付加的なサービスも当初サービスから当然に想定され得る利用の範囲である場合等については、当初サービスにおける「有効な同意」の範囲内であるとして、新たな同意は不要と整理することもあり得る。

イ 必要であるとして約款等の変更で足りるか

事業者からの声として、既にサービスインしている利用者から再度同意を取得するのは困難が伴うとの声がよく聞かれる。そこで改めての「同意」が必要であるとしても、約款、利用規約やプライバシーポリシー等の変更で足りるか否かが論点となる。

契約約款等による同意が「有効な同意」として認められるためには、利用者の利益に資するものであって、かつ、通常の利用者であれば同意することが合理的に推認される必要がある。例えば、迷惑メールフィルタリングサービス等の機能追加の場合にも一定の条件を満たした場合には約款等の変更で足りると考えられる[34]。他方で利用

---

[33] 「リスク評価」との関係で、１階層目に複数のサービス類型（利用目的）を包括的に示し、必ずしも「具体的」に認識していない状態で同意を取得することが「有効な同意」と評価される場合、２階層目（又はそれ以降の階層）で個別サービス類型ごと（利用目的ごと）にオプトアウト手続が担保されていれば許容されると考えることはできる場合も可能性としてはあり得る。また、通信の秘密との関係で特に明示すべきサービス類型（利用目的）はあるか等については引き続き検討を要する。

[34] 迷惑メール等のフィルタリングについて、①利用者がいったんフィルタリングサービスの提供に同意した後も、随時、任意に同意内容を変更できる状態（設定変更できる状態）であること、②フィルタリングサービス提供に対する同意の

者の利益につながるとしても、通常の利用者が同意することが合理的に推認するとまでいえない場合、又は、そもそも利用者の不利益になるようなサービス提供に関するものについては改めて「個別具体的」な同意が必要と考えられる。

２）同意の管理について

ア 同意管理と「有効な同意」の関係

プライバシーダッシュボード等の仕組みは、事業者の透明性を確保し利用者の同意撤回等を容易にするものとして推奨される。また、「リスク評価」によって「同意取得の在り方」を検討する際、利用者が容易に同意管理をできる仕組みを有していることは、同意手続を簡素化させる一事情として評価され得る。

デフォルトオフで各種サービスが管理ツール上表示されている場合には、新サービス追加時にタブを利用者が自ら「オン」にする動作を行うことは「明確」な同意としての意味を持つ。

イ 新サービス追加時に、ダッシュボード（デフォルトオン）で代替できるか

ⅰ）「明確な」同意

デフォルトオンによりプライバシーダッシュボードに新規サービスを追加することで利用規約やプライバシーポリシー上の同意を擬制することは「通信の秘密」に関して求められる「明確」な同意とは言えない。

他方、一般的な利用者がその都度その情報の利用が想定できる場合であって随意オプトアウトの手段も用意されている場合などについては「リスク評価」を実施し、このような条件を踏まえると「有効な同意」といえる場合もあり得る[35]。

ⅱ）ダッシュボードにおける選択の粒度

利用者にとって、ダッシュボードにおける選択の粒度がどの程度が適当であるかは人によって感じ方が異なる。詳細なコントロールを求めるユーザ、簡単なコントロールで納得するユーザのそれぞれが存在するため、適当な粒度といえるか否かは事案によらざるを得ないが、同意取得時点で一括して同意を取得している場合は、同意撤回は個別サービスごとでできる等の仕組みが通常求められると考えられる。

有無にかかわらず、その他の提供条件が同一であること、③フィルタリングサービスの内容等が明確に限定されていること、④通常の利用者であれば当該サービスの提供に同意することがアンケート調査結果等の資料によって合理的に推定されること、⑤利用者に対し、フィルタリングサービスの内容等について、事前の十分な説明を実施すること（法第26条に規定する重要事項説明に準じた手続により説明する場合でも、利用者の有効な同意に基づくフィルタリングと解することが可能であると考えられている（電気通信事業分野におけるプライバシー情報に関する懇談会資料18-1「フィルタリングと通信の秘密について」（2006年1月23日）。

[35] 電話における発信者情報通知サービスについては、発信者が発信者情報の通知を防止しない場合（184番号を押さない場合等）には、発信者が発信者情報を相手方に対して秘密にする意思がないと認められる（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解説第34条参照）。

ウ その他

ⅰ）同意管理についての定期的なリマインド

ある時点において「有効な同意」を取得した場合であっても、将来にわたり継続的に当該同意の意思を利用者が有しているとも限らない。このため、定期的に利用者にリマインドすることで利用者の同意の意思を確認することは、望ましい取組として評価される。また、その際、プライバシーダッシュボード等へのアクセスを容易にする等透明性にも配慮した仕組みが重要である。

（別紙）

参考

【電気通信事業法（抜粋）】

第一章　総則

（秘密の保護）

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。

第二章　電気通信事業

（業務の停止等の報告）

第二十八条　電気通信事業者は、第八条第二項の規定により電気通信業務の一部を停止したとき、又は電気通信業務に関し通信の秘密の漏えいそのほか総務省令で定める重大な事故が生じたときは、その旨をその理由又は原因とともに、遅滞なく、総務大臣に報告しなければならない。

（業務の改善命令）

第二十九条　総務大臣は、次の各号のいずれかに該当すると認めるときは、電気通信事業者に対し、利用者の利益又は公共の利益を確保するために必要な限度において、業務の方法の改善その他の措置をとるべきことを命ずることができる。

一　電気通信事業者の業務の方法に関し通信の秘密の確保に支障があるとき。

（以下略）

第六章　罰則

第百七十九条　電気通信事業者の取扱中に係る通信（第百六十四条第三項に規定する通信並びに同条第四項及び第五項の規定により電気通信事業者の取扱中に係る通信とみなされる認定送信型対電気通信設備サイバー攻撃対処協会が行う第百十六条の二第二項第一号ロの通知及び認定送信型対電気通信設備サイバー攻撃対処協会が取り扱う同項第二号ロの通信履歴の電磁的記録を含む。）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（第百六十四条第四項及び第五項の規定により電気通信事業に従事する者とみなされる認定送信型対電気通信設備サイバー攻撃対処協会が行う第百十六条の二第二項第一号又は第二号に掲げる業務に従事する者を含む。）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。

第百八十六条　次の各号のいずれかに該当する者は、二百万円以下の罰金に処する。

一・二（略）

三　第十九条第二項、第二十条第三項、第二十一条第四項、第二十九条第一項若しくは第二項、第三十条第五項、第三十一条第四項、第三十三条第六項若しくは第八項、第三十四条第三項、第三十五条第一項若しくは

第二項、第三十八条第一項（第三十九条において準用する場合を含む。）、第三十九条の三第二項、第四十三条第一項（同条第二項において準用する場合を含む。）、第四十四条の二第一項若しくは第二項、第四十四条の五、第五十一条、第七十三条の四又は第百二十一条第二項の規定による命令又は処分に違反した者
（以下略）

【GDPR(ePR)との比較】

・ ePrivacy 規則案は、通信内容やメタデータの処理に係る「同意」の定義や取扱いは、GDPR の規定を引用している。
・GDPR の同意の定義(第４条(11))は、「データ主体の『同意』とは、自由に与えられ(freely given)、特定され(specific)、事前に説明を受けた(informed)上での、不明瞭ではない(unambiguous)、データ主体の意思の表示を意味し、それによって、データ主体が、その陳述又は明確な積極的行為により(by statement of by an affirmative action)、自身に関連する個人データの取扱いの同意を表明するもの（を意味する）。」とする（なお、有効な同意の条件について第７条）
・2017 年 11 月「同意に関するガイドライン」が第 29 条作業部会によって策定（2020 年５月 EDPB により一部改訂）されており、同ガイドラインにおいて、「自由に与えられ(freely given)」「特定され(specific)」「事前に説明を受けた上で(informed)」「不明瞭ではない(unambiguous)」「その陳述又は明確な積極的行為により(by statement of by an affirmative action)」等の詳細について記述がなされる。また、「透明性に関するガイドライン」も策定されており、これによってデータの取扱い等についてのユーザへの情報提供の在り方についても示している。
・GDPR は同意の定義における「特定され(specific)」の要件で、「一つ又は複数の特定の」目的に関しての同意を要求している。

【個人情報保護法との比較】

・個人情報保護法で「本人の同意」に関する規定は、利用目的による制限（第 16 条）、適正な取得（第 17 条）、第三者提供の制限（第 23 条）、外国にある第三者への提供の制限（第 24 条）の４カ所である。
・同法において、「本人の同意」とは、「本人の個人情報が、個人情報取扱事業者によって示された取扱方法で取り扱われることを承諾する旨の意思表示をいう」とし、「事業の性質及び個人情報の取扱状況に応じ、本人が同意に係る判断を行うために必要と考えられる合理的かつ適切な方法」での同意取得が認められており（個人情報の保護に関する法律についてのガイドライン（通則編））、契約約款による同意も必ずしも否定されていない。そして、総務省のガイドライン解説では「個別の同意がある場合だけでなく、電気通信役務の提供に関する契約約款において、個人情報の第三者提供に関する規定が定められており、当該契約約款に基づき電気通信役務の提供に関する契約を締結し、かつ当該規定が私法上有効であるときは、「本人の同意を得（る）」又は「本人の同意がある」場合と解される」としている。
・他方で、通信の秘密に該当する個人情報については、その権利の重大性を理由に「個別具体的かつ明確な同意」が必要であるとし、原則として契約約款による同意を認めていない。

・法定代理人等から同意を得る必要がある子供の具体的な年齢は、同意の対象となる個人情報の項目や事業の性質等によって、個別具体的に判断されるべきであるが、一般的には 12 歳から 15 歳までの年齢以下の子供について、法定代理人等から同意を得る必要があると考えられる[36]。

[36] 「個人情報の保護に関する法律についてのガイドライン」及び「個人データの漏えい等の事案が発生した場合等の対応について」に関する Q&A（Q1-58）