総務省 学術雑誌『情報通信政策研究』 第５巻第１号
Journal of Information and Communications Policy Vol.5 No.1

立案担当者解説

「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」及び「同意取得の在り方に関する参照文書」

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課長補佐　丸山　和子
同課課長補佐　伊藤愉理子
同課専門職　　呂　　佳叡

要　旨

「プラットフォームサービスに関する研究会」の最終報告書（令和２年２月）において、電気通信事業法第 29 条第１項第１号に基づく業務改善命令の発動に際する一定の基準や事例を法執行に係る指針を策定・公表することが適当である、とされたとともに、有効な同意の取得やその際の説明の在り方について、さらに検討を深めることが必要であるとされたことを踏まえ、「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」及び「同意取得の在り方に関する参照文書」を令和３年２月 25 日に策定・公表した。

同指針においては、電気通信事業者、業務の方法、通信の秘密の確保に支障があるとき等の考え方を示すとともに、通信の秘密の確保に支障があるときとして想定されるケースを類型化した上で例示している。

同文書においては、通信の秘密における同意取得の意味、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、個別具体的かつ明確な同意等について説明した上で、通信の秘密の侵害を防止する観点からのリスク分析についても触れつつ、個別ケースの検討を行っている。

キーワード：電気通信事業法、通信の秘密、業務改善命令、有効な同意、個別具体的かつ明確な同意

１．はじめに

令和２年５月 22 日に公布された電気通信事業法及び日本電信電話株式会社等に関する法律の一部を改正する法律（令和２年法律第 30 号）では、外国法人等（外国の法人及び団体並びに外国に住所を有する個人をいう。以下同じ。）が電気通信事業を営む場合の規定の整備等が行われ、当該整備に係る改正については、令和３年４月１日に施行された。

改正の経緯の一つとして、「プラットフォームサービスに関する研究会」[1]における検討がある。令和２年２月に出された同研究会の最終報告書[2]においては、我が国の利用者に電気通信サービスを提供する国外事業者に対し、「通信の秘密」の保護をはじめとする電気通信事業法（昭和 59 年法律第 86 号。以下「事業法」という。）の規律を及ぼすよう、所要の措

[1] プラットフォームサービスに関する研究会
https://www.soumu.go.jp/main_sosiki/kenkyu/platform_service/index.html
[2] 「プラットフォームサービスに関する研究会　最終報告書」
https://www.soumu.go.jp/main_content/000668595.pdf

置を講ずることが適当とされたものである。また、事業法第 29 条第１項第１号に基づく業務改善命令の発動に際しては、どのような場合に、各事業者の取組が十分機能していないとして、行政当局が業務改善命令を発動できるのか等についての一定の基準や事例を法執行に係る指針として策定・公表することが適当である、とされたとともに、いわゆる「同意疲れ」は、より多くの利用者情報が利用者から取得されるようになり、また、その活用の方法が複雑かつ多岐にわたるようになり、さらに、その結果同意取得時の説明も複雑で分かりにくくなるといった事情が相まって生じているものと考えられることから、こうした事情を踏まえて、有効な同意の取得やその際の説明の在り方について、さらに検討を深めることが必要であるとされたものである。

当該最終報告書を踏まえ、総務省においては、令和３年２月 25 日に「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」及び「同意取得の在り方に関する参照文書」を策定し、公表したものである。

なお、同指針及び同文書は上述の事業法の外国法人等が電気通信事業を営む場合の規定の整備等の施行に向けて策定したものであるが、当然のことながらその適用は当該外国法人等に限るものではなく、国内事業者にも適用されるものである。

本稿では、まずは通信の秘密について概説した上で、同指針及び同文書の概要等について解説することとしたい。なお、本稿中意見にわたる部分は筆者らの個人的見解であることをあらかじめお断りしておきたい。

２．通信の秘密について

「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」及び「同意取得の在り方に関する参照文書」については、いずれも「通信の秘密」に関するものであるため、「通信の秘密」について概説する。

日本国憲法第 21 条は、基本的人権の一つとして表現の自由を保障し（同条第１項）、検閲の禁止とともに通信の秘密の保護について規定している（同条第２項）。憲法における通信の秘密の保護は、国民のプライバシー保護にとどまらず、通信の秘密が侵害されないことを通じて国民の表現の自由や知る権利を保障するために重要なものと位置付けられている。

事業法第４条第１項において、「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」と規定されている。これは、通信の秘密に関して上記憲法上の要請を担保するために法律レベルで具体化している[3]もので、電気通信事業者を含めて何人も電気通信事業者の取扱中に係る通信の秘密は、侵してはならないとすることにより、電気通信役務の利用者の通信を保護し、もって利用者が安心して電気通信サービスを利用できるようにすることで、表現の自由や知る権利を保障するものである。これは、電気通信ネットワークや通信制度そのものへの利用者の信頼を確保し、多様なサービスやビジネスの実現による電気通信の健全な発展と国民の利便の確保を図ることにも資するものであると考えられる。

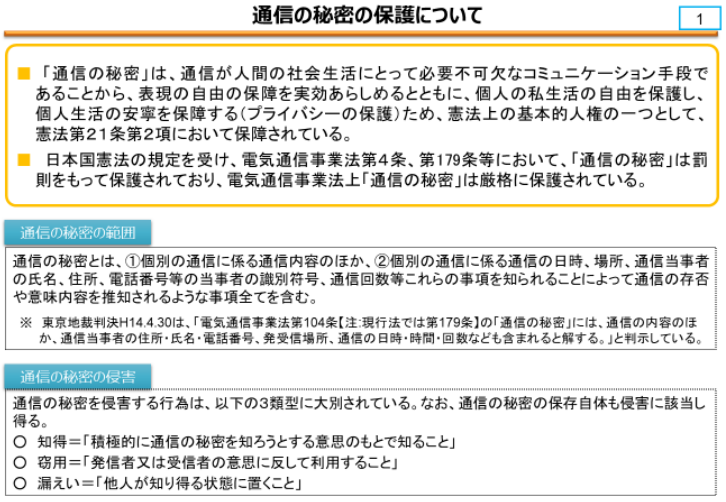
[3] 検閲の禁止については、郵便法（昭和 22 年法律第 165 号）第７条及び事業法第３条において規定されている。また、通信の秘密の保護については、郵便法第８条、電波法（昭和 25 年法律第 131 号）第 59 条及び有線電気通信法（昭和 28 年法律第 96 号）第９条においても規定されており、その罰則は郵便法第 80 条、電波法第 109 条、同法第 109 条の２及び有線電気通信法第 14 条において規定されている。

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。

通信の秘密に係る情報を取得等する場合であっても、通信当事者の有効な同意がある場合には、通信の秘密の侵害に当たらない。また、正当行為（刑法（明治 40 年法律第 45 号）第 35 条）、正当防衛（同法第 36 条）、緊急避難（同法第 37 条）に該当する場合等には例外的に違法性が阻却されると解されている。例えば、通信履歴については、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（以下「ガイドライン」という。）第 32 条第１項において「電気通信事業者は、通信履歴……については、課金、料金請求、苦情対応、不正利用の防止その他の業務の遂行上必要な場合に限り、記録することができる。」と規定されており、これらは正当業務行為[4]と位置付けられている。

通信の秘密を保護する趣旨に鑑み、「通信の秘密」の範囲には、個別の通信に係る通信内容のほか、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・居所、電話番号など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意味内容を推知されるような事項すべてが含まれると解されている。これを踏まえ、ガイドラインの解説においても「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。）[5]」と規定されている。

図１．通信の秘密の保護について

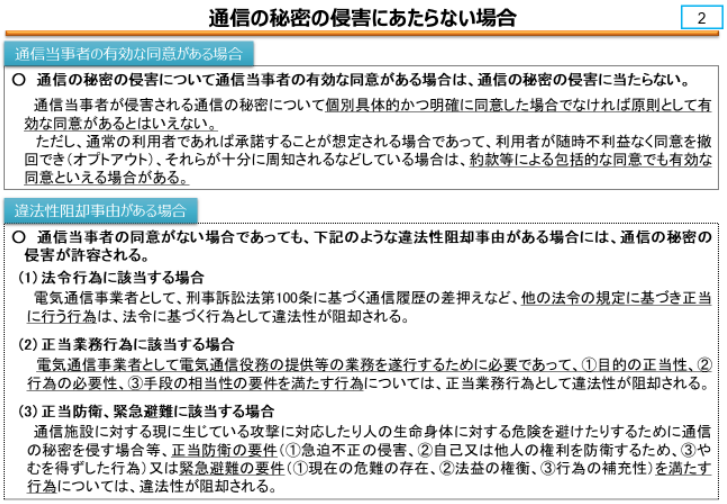


（出典）総務省資料

[4] ガイドライン第 32 条第１項の解説 5-1-1 において「課金、料金請求、苦情対応、自己の管理するシステムの安全性の確保その他の業務の遂行上必要な場合には、必要最小限度の通信履歴を記録することは、少なくとも正当業務行為として違法性が阻却される」と記載している。

[5] ガイドライン第２条の解説 2-13「本人の同意」

図２．通信の秘密の侵害にあたらない場合



（出典）総務省資料

３．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

３．１．背景

情報通信分野においては、新たな技術の進展や市場構造の変化等により電気通信事業者が提供するサービスの多様化や複雑化等が進み、通信の秘密に係る情報を含む利用者情報を活用した様々なサービスが、電気通信事業者によって次々に提供されることが想定される。各電気通信事業者がこれらのサービスの提供に当たって取り扱うこととなる通信の秘密に係る情報については、個々の事業者によって提供するサービスの形態、取り扱う通信に係る情報の種類や規模、利用形態等が異なることから、各事業者において、それぞれの状況に応じて自律的に適切な対応が図られることが必要である。

電気通信事業者による適切な対応が図られることを担保するために、各事業者による自律的な対応が十分に機能せず、当該事業者の業務の方法に関し通信の秘密に係る情報の取扱いが不適切であるなど、通信の秘密の確保に支障があると認められる場合には、総務大臣が事業法第 29 条第１項第１号の規定に基づく行政処分である業務の改善命令（以下「業務改善命令」という。）を機動的に発動することにより、利用者が安心して電気通信サービスを利用できるようにすることが重要である。

このような背景を踏まえ、通信の秘密の確保に関する考え方を明らかにし、総務大臣が各事業者の取組が十分に機能していないとして、業務改善命令を発動する基準や事例を指針として類型的に示すことにより透明性・予見可能性を高めることを目的として、業務改善命令の発動に係る指針（以下「執行指針」という。）を策定したものである。

３．２．概要

３．２．１．考え方

事業法第 29 条第１項第１号においては、「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。」を業務改善命令の要件として定められており、同号に該当し利用者の利益を阻害している場合、総務大臣が当該事業者に業務の方法の改善その他の措

置をとることを命ずることにより、当該事業者に適切な通信の秘密の保護に係る取組・対応を促し、利用者の利益の保護を図ろうとしている。

業務改善命令は、「電気通信事業者」を対象とする規律であり、電気通信事業を営むことについて事業法第９条の規定に基づく登録又は同法第 16 条第１項の規定に基づく届出の対象となる者を対象とするものであり、当該登録又は届出の対象とならない者（事業法第 164 条第１項）の場合には直接的には業務改善命令の対象とはならない[6]。

事業法第 29 条第１項における「業務」とは、事業法第２条第６号に規定する電気通信業務、すなわち電気通信事業者が他人の需要に応じて電気通信役務を提供すること（電気通信サービスを提供すること）を主に想定するものであるが、それ自体に限られるものではなく、電気通信役務と一体的に提供されていて切り離すことができないサービスや電気通信事業者が提供する電気通信役務の利用を前提としているサービス、また、当該業務に関連して行う契約事務や料金収納事務、電気通信設備の保守などの業務を含むより広義なものである[7]。

「業務の方法」は、業務の管理運営方法、窓口業務等の日常業務の取扱方法など「通信の秘密」に係る情報を取り扱う場合の業務全般に及ぶものであり、その業務の方法は電気通信事業者の社内規則等のみで形式的に評価されるものではなく、業務の実情に照らして客観的に評価されるものである。また、その取扱いが人によるか機械によるかは問わないものである。

「通信の秘密」の範囲には、２で述べたとおり、個別の通信に係る通信内容のほか、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・居所、電話番号など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意味内容を推知されるような事項全てが含まれると解されている。「通信の秘密の確保に支障があるとき」は、業務上「通信の秘密」の取扱いが不適切な場合や「通信の秘密」を保護するための態勢が不十分である場合などに該当するものであり、「電気通信事業者の取扱中に係る通信の秘密」を侵した場合（事業法第４条第１項、第 179 条第１項）は、原則として「通信の秘密の確保に支障があるとき」に該当すると考えられる。

３．２．２．「通信の秘密の確保に支障があるとき」として想定されるケース

事業法第 29 条第１項第１号に規定される「通信の秘密の確保に支障があるとき」に該当し、「業務改善命令が発動されるおそれのある場合」について、①通信の秘密に係る情報を含む利用者情報の取扱い等の方針等が不適切な例[8]、②通信の秘密の取得・利用等が不適切

---

6 ただし、「電気通信事業者」が登録・届出の対象外である適用除外となる電気通信事業も併せて提供した場合において、当該適用除外となる電気通信事業における「通信の秘密の確保に支障」が生じていることが間接的に、登録・届出の対象となっている電気通信事業における「通信の秘密の確保に支障」が生じていると評価できる場合には、業務改善命令の対象となり得る。

7 これら業務等の例は、ガイドライン第３条の解説を参照。

8 「通信の秘密」に係る情報の取扱いについて、「知得」「窃用」「漏えい」等の行為すべてが原則違法な行為であり、利用者の有効な同意又は違法性阻却事由がある場合に当該行為が正当化されるものである。このため、「通信の秘密」に係る情報の取扱いについて、個人情報の保護に関する法律（平成 15 年法律第 57 号）上の「個人情報」の取扱いで規定されているように、取得行為について利用目的の通知・公表のみで足りるものではない（同法第 18

な例、③情報管理態勢が不適切な例、④苦情・相談等対応態勢が不適切な例、の４つに類型化して例示しているが、ここでは割愛したい。

なお、執行指針の中で例示していない行為であっても、事業法第 29 条第１項第１号の規定に照らし、個別の事案ごとに「通信の秘密の確保に支障があるとき」の該当性が判断されるものであり、また、例示されているものであっても、一の該当行為をもって必ず業務改善命令が発出されるものでもない。

４．同意取得の在り方に関する参照文書

４．１．背景

電気通信サービスは、５Ｇの普及に伴い、今後さらに AI や IoT などの最新技術を駆使したものに変遷・進化していくとともに、電気通信事業者とプラットフォーム事業者との協業や連携・融合が進み、市場環境も一変していくことが想定される。こうした変化に伴い、多様な電気通信サービスを通じて取得・活用される通信の秘密に係る情報を含む利用者情報についても、例えば、より多くの種類の情報が、より頻繁に、かつ、より多くの事業者間で共有・活用されるようになるなど、その取扱いが質・量ともに深化・拡大していくことが想定される。

通信の秘密に係る情報の取扱いに当たっては、法令行為や正当業務行為、緊急避難等違法性阻却事由に該当する場合を除いて、通信当事者の有効な同意を取得することが必要とされており、また、当該同意は、原則として通信当事者の「個別具体的かつ明確な同意」でなければならないとされているところ、ネット環境の進化に伴って多様なサービスが展開される中、累次の同意取得が繰り返され、かえって利用者の理解が不十分となる、いわゆる「同意疲れ」が課題となりつつある。

こういったいわゆる「同意疲れ」は、より多くの利用者情報が利用者から取得されるようになるとともに、その活用の方法が複雑かつ多岐にわたるようになり、さらに、その結果同意取得時の説明も複雑で分かりにくくなるといった事情が相まって生じているものと考えられることから、こうした事情を踏まえて、有効な同意の取得やその際の説明の在り方について、参照すべき文書を策定したものである。

４．２．概要

４．２．１．通信の秘密における同意取得の意味

個々の利用者の通信情報の取得・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ため、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ものである。

４．２．２．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

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

条参照）点に注意が必要である。

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。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について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、各種報告書や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第３条の解説（２-13「本人の同意」）等において、通信の秘密に係る情報の取扱いについては「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」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」が適正か否かとは、厳密には異なる概念である。

４．２．３．個別具体的かつ明確な同意とは

「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」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について、手続的な要素である「個別具体的」な同意か、及び「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、当該要素のみによるものではなく、例えば、個別ケースでは同意の任意性についても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、すなわち「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場合については、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可能性もあるのではないかとの指摘もあるところである。

（１）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同意を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[9]ものである。

「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。

---

[9] 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。

（２）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。他方、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。

４．２．４．　通信の秘密の侵害を防止する観点からのリスク分析

（１）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[10]。

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もつことが期待される。

（２）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）[11]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

---

[10] 例えば、欧州の GDPR（一般データ保護規則）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。

[11] 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、行政手続における特定の個人を識別するための番号の利用等に関する法律（平成 25 年法律第 27 号。いわゆるマイナンバー法）に導入されているとともに、ISO/IEC29134 が令和３年１月に JISX9251:2021（情報技術―セキュリティ技術―プライバシー影響評価のためのガイドライン）として JIS 規格化され、個人情報保護委員会が令和３年６月 30 日に、「PIA の取組の促進について-PIA の意義と実施手順に沿った留意点-」を公表している。
個人情報保護委員会「PIA の取組の促進について -PIA の意義と実施手順に沿った留意点-」：https://www.ppc.go.jp/files/pdf/pia_promotion.pdf
個人情報保護委員会「PIA の取組の促進について -PIA の意義と実施手順に沿った留意点-（概要）」：https://www.ppc.go.jp/files/pdf/pia_overview.pdf

めの手段であり、プライバシーリスクをあらかじめ把握し適切な対応方法を設計[12]するために行われ、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 の実施結果の公表は義務付けられてはいないが、自主的に公表を行うことは、事業者の信頼性の醸成や、説明責任及び透明性の確保に役立つものと考えられる。

（３）リスク評価を応用した有効な同意の取得の在り方

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」に対して応用する有用性は高いものと考えられる。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ものである。

当然のことながら、リスク評価を行えば、通信当事者の個別具体的かつ明確な同意を取得しなくてもよくなるということではない。

４．２．５．個別ケースの検討

事業者より同意取得の在り方等について質問等をよく受けるものの代表例として、①ユーザアカウント作成時における一括同意、②２階層による同意取得、③既存サービスに付加的サービスを追加する場合、④同意の管理等について検討しているが、ここでは割愛したい。

５．おわりに

本稿が「通信の秘密」に対する考え方等への一助になれば幸いである。

なお、本稿では「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」及び「同意取得の在り方に関する参照文書」の概要等について解説したものであるため、詳細については、実際の同指針及び同文書を参照されたい[13]。

（オンライン掲載日：令和３年９月 14 日）

---

[12] 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、あらかじ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。

[13] 「電気通信消費者情報コーナー」及び「個人情報保護」において同指針及び同文書を掲載しているとともに、英語版も掲載。
https://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/privacy.html