Cookie 事例を通じた「通信の秘密」の再考

今井　達也

はじめに

１．デジタル化した社会における通信

2000 年に情報通信技術戦略本部が設置され、IT 基本法が制定されて以降、日本では、インフラ整備、ICT 利活用やデータ利活用の推進等を通じて、デジタル化が進められてきた[1]。その基盤となるインターネット通信は、携帯電話やスマートフォンの普及もあり、多くの人々に利用されるものとなっている[2]。インターネットを利用したサービスは、インターネットショッピング、クレジットカード等による決済、地図・ナビゲーション、情報検索・ニュース、動画配信、SNS[3]等多岐にわたり、日常生活の様々な場面に浸透している[4]。インターネットを利用したサービスは、AI[5]やVR/AR[6]といった新たな技術と結びついた通信や IoT[7]による通信が増えること等から、今後ますます増えていくものと思われる[8]。

インターネット通信の重要性は、個人の日常生活以外でもしばしば見受けられる。例えば、働き方改革の一環として多くの企業が取り入れているテレワーク[9]ひと

---

[1] 総務省『令和３年版情報通信白書』＜https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r03/pdf/01honpen.pdf＞（2021 年）２頁。なお、同 80 頁では、デジタル化を「デジタル技術を用いた単純な省人化、自動化、効率化、最適化」としている。

[2] 総務省・前掲注１）50 頁参照。

[3] Social Networking Service(Site)の略。個人間の交流を支援するサービス（サイト）で、参加者は共通の興味、知人等をもとに様々な交流を図ることができる。例えば、友人・知人間のコミュニケーションを円滑にする手段や場を提供したり、趣味や嗜好、居住地域、出身校、「友人の友人」といったつながりを通じて新たな人間関係を構築したりする場を提供する（政府 CIO ポータル「世界最先端デジタル国家創造宣言・官民データ活用推進基本計画用語集」(2020 年) ３頁)。

[4] 総務省・前掲注１）54 頁参照。

[5] Artificial Intelligence の略。「人工的な方法による学習、推論、判断等の知的な機能の実現及び人工的な方法により実現した当該機能の活用に関する技術」（官民データ活用推進基本法第２条第２項）のことをいう（政府 CIO ポータル・前掲注３） １頁)。

[6] AR とは、目の前にある現実世界にコンピュータで作られた映像や画像を重ね合わせ、現実世界を拡張する技術のことである。また、VR とは、現実にない世界又は体験し難い状況を CG によって仮想空間上に作り出す技術のことである（総務省・前掲注１）42 頁)。

[7] Internet of Things（モノのインターネット）の略。自動車、家電、ロボット、施設などあらゆるモノがインターネットにつながり、情報のやり取りをすることで、モノのデータ化やそれに基づく自動化等が進展し、新たな付加価値を生み出すというコンセプトを表した語を指す（政府 CIO ポータル・前掲注３） ２頁)。

[8] これらのサービス提供を円滑に提供できる基盤として、超高速通信、超低遅延通信、多数同時接続という特徴を持つ第５世代移動通信システムの商用サービスが、2020 年３月から国内において開始されている（総務省・前掲注１）13 頁参照)。なお、IoT デバイスの急速な普及について、同 43 頁において言及されている。

[9] 総務省・前掲注１）96 頁。

つとっても、社外から社内の情報にアクセスできる仕組みや遠隔会議システムの導入率が比較的高いこと等から[10]、企業活動においてもインターネット通信が重要な役割をはたしていることがうかがえる。また、公的分野においてもデジタル化が推進されており[11]、政府や地方自治体における手続のオンライン化が進められる等、インターネット通信の重要性が高まっていることがわかる。

さらに、近年の新型コロナウイルス感染症の流行拡大を受け、インターネット通信の重要性は、より一層増しているといえる[12]。例えば、オンライン消費の増加[13]、オンライン番組・イベント配信の増加[14]、企業や行政職員によるテレワークの増加[15]、オンライン教育[16]やオンライン診療[17]の実施等が挙げられる。

以上を踏まえると、インターネット通信は、もはや国民の生活や企業活動等に必要不可欠なものになっていると言っても過言ではないと考える。

２.「通信の秘密」不可侵規制

「通信の秘密」は、日本国憲法第 21 条第２項後段において、その不可侵が定められている[18]。また、電気通信事業法、電波法[19]、有線電気通信法[20]、郵便法[21]も、それぞれ「通信（信書）の秘密」を保障している。本稿では、前記１で掲げたサービス等の利用に必要なインターネット通信に関係する電気通信事業法の「通信の秘密」について論じる。

電気通信事業法は、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」の侵害を禁じ、第 179 条に罰則を設けている[22]。これらの規定は、それぞれ公衆電気通信法の規定を受け継いだものである[23]。公衆電気通信法の「通信の秘密」

---

[10] 総務省・前掲注１）97 頁。
[11] 2021 年９月１日、デジタル庁が発足した（デジタル庁「デジタル庁のミッションとビジョン」＜https://www.digital.go.jp/about/organization＞参照）。
[12] 2020 年は対前年比５割以上の増加となっている（総務省・前掲注１）166 頁）。
[13] インターネットショッピングの利用世帯割合は、2020 年３月以降に急速に増加し、二人以上の世帯の約半数以上が利用する状況が続いている（総務省・前掲注１）156 頁）。
[14] 総務省・前掲注１）157 頁。
[15] 総務省・前掲注１）172、194 頁。
[16] 総務省・前掲注１）178 頁。
[17] 総務省・前掲注１）184 頁。
[18] なお、いわゆる３月５日案第 19 条では「……通信手段ノ秘密ハ之ヲ侵ス可カラス」とされているのに対し、憲法改正草案要綱第 19 条では、「……通信ノ秘密ハ之ヲ侵スベカラザルコト」とされており、表現に変遷がみられる。
[19] 電波法第 59 条。また、同法第 109 条に罰則規定が設けられている。
[20] 有線電気通信法第９条。また、同法第 14 条に罰則規定が設けられている。
[21] 郵便法第８条。また、同法第 80 条に罰則規定が設けられている。
[22] その他、「通信の秘密」の漏えい等が生じた際の報告義務（同法第 28 条）、「通信の秘密」の確保に支障がある場合の改善命令（同法第 29 条第１項第１号）等の定めがある。
[23] 公衆電気通信法第５条、第 112 条及び第 113 条。林秀弥ほか『オーラルヒストリー電気

不可侵規定は、憲法第21条第２項後段の規定を受けて定められたものであることから[24]、電気通信事業法における「通信の秘密」不可侵規制も、憲法第21条第２項後段の規定を受けて定められたものであるといえる[25]。

以上からわかるとおり、「通信の秘密」不可侵規制それ自体は、インターネット通信が普及する前から存在するものである。また、電気通信事業法における「通信の秘密」不可侵規定は、主に通話による通信を念頭に置いて定められたものであり、これがそのままの形で存続している。そして、その内容については、必ずしも活発な議論が行われてきたわけではないとされており[26]、「通信によって伝送される情報やその利用の方法が複雑多様になっているのに対し、通信の秘密の規定があまりにも簡素である」との指摘も存在するところである[27]。

３．本稿の目的

本稿の目的は、２つある。１つ目の目的は、Cookieの利活用と「通信の秘密」の関係の明確化である。Cookieは、インターネット通信において広く用いられているところ、Cookieの利活用が「通信の秘密」の侵害に当たるか、いかなる措置を講じれば、「通信の秘密」不可侵規制違反とならないか等については、必ずしも明らかにされていない。本稿では、これらを明らかにすることを試みる。

２つ目の目的は、「通信の秘密」不可侵規制に関する諸論点の再考である。筆者は、近年の電気通信実務に係る「通信の秘密」不可侵規制について、従前の議論では必ずしも説明しきれない点や、未だ明確に整理されていない点があると考える。本稿では、これらの点について、実務に整合的な解釈ができるか検討する。

通信事業法』（勁草書房、2015年）213頁、髙嶋幹夫『実務電気通信事業法』（NTT出版、2015年）767頁参照。

[24] 金光昭ほか『公衆電気通信法解説』（日信出版、1953年）23頁では、「本条は憲法21条の規定を受けて電気通信による通信の秘密の確保を規定したものである」とされている。

[25] 「一般には、①憲法上の規定を受け、これを拡充・確認する意味を持ち、②憲法がもっぱら公権力からの侵害に対応するものであるのに対し、法律上の規定は通信事業者・私人からの侵害を対象に含むと考えられている」とされる（神足祐太郎「通信の秘密をめぐる議論の諸相」レファレンス834号（2020年）46頁）。

[26] 神足・前掲注25）45頁、曽我部真裕「通信の秘密の憲法解釈論」Nextcom16号（2013年）14頁参照。なお、Cookieが「通信の秘密」に当たるとする見解が見当たらないことを指摘するものとして、森亮二「ターゲティング広告と利用者情報」ジュリスト1564号（2021年）39頁。他方、Cookieは、個人情報保護法制との関係では、例えば、「個人関連情報」（個人情報の保護に関する法律（以下「個人情報保護法」という。）第26条の２第１項柱書）にこれが含まれ得るとする等、一定の整理がなされている（佐脇紀代志編著『一問一答令和２年改正個人情報保護法』（商事法務、2020年）64頁、石井夏生利ほか編著『個人情報保護法コンメンタール』（勁草書房、2021年）424頁〔森亮二執筆〕）。

[27] 曽我部真裕「情報法ナビゲーション（第４回）通信の秘密」法学セミナー786号（2020年）68頁。

第１部　Cookie と「通信の秘密」に関する考察

第１章　Cookie とは

１．Cookie の意義

Cookie とは、ウェブサーバーにアクセスするウェブブラウザを識別するために、ウェブサーバーの指示によってコンピュータに保存される一定のデータのことをいう[28]。Cookie の仕組みは、HTTP（Hyper Text Transfer Protocol）[29]の性質から生じる不都合を解消するために開発されたとされる。HTTP は、ウェブブラウザからのリクエスト及びこれに対するウェブサーバーからのレスポンスによって構成されるところ、これらのリクエスト及びレスポンスによって生じた状態は、ウェブサーバーにおいて維持・管理されない。したがって、ウェブブラウザが以前やり取りしたことがあるウェブサーバーに対して新たなリクエストをしたとしても、ウェブサーバーは、当該やり取りによって生じた状態を参照することができないこととなる。

Cookie は、このような不都合を解決する方法として利用される。ウェブサーバーが新たなリクエストを受けた際、先立つ通信に係る情報を記録している Cookie を参照することで、先立つ通信を前提にしたレスポンスが可能となる[30]。

---

[28] 総務省情報通信政策研究所「行動ターゲティング広告の経済効果と利用者保護に関する調査研究報告書」＜https://www.soumu.go.jp/iicp/chousakenkyu/data/research/survey/telecom/2009/2009-I-16.pdf＞（2010 年）12 頁では、「『クッキー』とは、Web サーバーから利用者のパソコンに送られ保存される情報のことであり、クッキーには利用者に関する番号や最後にサイトを訪れた日時、そのサイトの訪問回数などを記録しておくことができる。クッキーによって、利用者を識別することができ、Web サービスを利用者ごとにカスタマイズすることが可能になる」と説明されている。また、総務省プラットフォームサービスに関する研究会「プラットフォームサービスに関する研究会中間とりまとめ」＜https://www.soumu.go.jp/main_content/000769270.pdf＞（2021 年）75 頁では、「ウェブサイトを訪問した際、ブラウザ上に一時的に情報を保存する仕組み」と説明されている。

[29] ウェブブラウザとウェブサーバー間で、ハイパーテキストを送受信するために使用されるプロトコルのことをいう。

[30] その具体的方法は、概ね次のとおりである。①特定のウェブページを表示させるリクエストがウェブブラウザからウェブサーバーに対して送られる。②当該ウェブサーバーは、当該ウェブブラウザに対し、一定の情報が記録された Cookie を発行しつつ、リクエストに対するレスポンスをする。③レスポンスを受けた当該ウェブブラウザは、発行された Cookie を保存する。④その後、当該ウェブブラウザは、特定のウェブページの表示をリクエストする際、当該 Cookie をウェブサーバーに送る。⑤当該ウェブサーバーは、送られてきた Cookie に記録された情報を参照したうえでリクエストに対するレスポンスをする。

２．Cookie の種類

Cookie のうち、その発行元ドメインとユーザーが閲覧するウェブページのドメインが同一であるものをファーストパーティ Cookie という。

これに対し、その発行元ドメインとユーザーが閲覧するウェブページのドメインが異なるものをサードパーティ Cookie という。その発行方法については、特定のウェブページの HTML（Hyper Text Markup Language）上に JavaScript を記述することで、当該ウェブページを表示させたウェブブラウザを広告事業者のウェブサーバー（以下「広告事業者サーバー」という。）にアクセスさせ、サードパーティ Cookie の発行を受けさせるといったものがある[31]。

サードパーティ Cookie を複数のウェブサイト間で横断して利用した場合、当該サードパーティ Cookie の発行元事業者は、その活用方法次第では複数のドメインに対するユーザーのアクセス情報を取得できることとなる。そのため、ユーザーが自らアクセスしたことのないウェブサーバーに、ユーザーのアクセス情報が広く収集されるおそれがあるとする指摘がある[32]。

３．Cookie の利活用

前述のとおり、Cookie は、元々は HTTP の性質から生じる不都合を解消するために開発されたものであるが、現在では様々な場面において利用されている。

例えば、「オンラインショッピングサイトにおいて、商品を商品かごに入れ、購入する」という流れの中で行われる一連のアクセスを、関連性あるものとして扱いたい場合に Cookie を用いてセッション管理が行われることがある[33]。

---

[31] 若江雅子ほか「オンライン広告におけるトラッキングの現状とその法的考察―ビッグデータ時代のプライバシー問題にどう対応すべきか」『情報通信政策研究』第２巻第２号（2019 年）Ⅱ－６頁参照。

[32] 若江ほか前掲注 31）Ⅱ－７頁参照。その他、サードパーティ Cookie については、それが設置されるウェブサイト管理者が実情を把握しにくく、そのためプライバシーポリシーがきちんと書けていない場合も多いとの指摘がある。また、利用者にとってもプライバシーポリシーが分かりにくく、自分のデータがどう扱われているか把握することが難しいという課題があるとされる（以上について、総務省・前掲注 28）76 頁参照）。

[33] その一例は、次のとおりである。①まず、ウェブブラウザがウェブサーバーに対し、特定のウェブページの表示をリクエストする。②リクエストを受けたウェブサーバーは、個人を識別するセッション ID（例：abc123）及び当該セッション ID を記録した Cookie（例：session-id=abc123）を発行しつつ、当該ウェブページを表示させるレスポンスを行う。③レスポンスを受けたウェブブラウザは、当該 Cookie を保存する。④その後、当該ウェブブラウザは、対象となるウェブページの表示をリクエストする際、当該 Cookie をウェブサーバーに送る。⑤これを受けた当該ウェブサーバーは、当該 Cookie に記録されたセッション ID を参照したうえで、これに応じたウェブページを表示させるレスポンスができる。

また、Cookie は、行動ターゲティング広告の配信に利用されることがある。行動ターゲティング広告とは、利用者のインターネット利用上の行動履歴（ウェブサイトの検索や閲覧の履歴等）に着目した広告手法であり、利用者の興味関心にあった広告を適切なタイミングで配信することによって、広告の効果を高めようとするものである[34]。例えば、「ペット関連のウェブサイトを閲覧した後に、旅行関連のウェブサイトを閲覧したところ、ペットと泊まれるホテルに関する広告が表示された」といったものがこれに当たる[3536]。

---

[34] 以上について、総務省・前掲注 28）９頁。なお、個人情報保護委員会は、「いわゆるターゲティング広告」について、「ユーザーがあるウェブサイトにアクセスした際に、当該ユーザーの PC やスマートフォン等のブラウザごとのクッキー等を通じてユーザー一人ひとりの趣味嗜好・性別・年齢・居住地等に関するユーザーデータを取得し、それを活用して当該ユーザーに狙いを絞った広告」と説明している（個人情報保護委員会「個人情報保護法いわゆる３年ごと見直し制度改正大綱」＜https://www.ppc.go.jp/files/pdf/200110_seidokaiseitaiko.pdf＞（2019 年）23 頁参照）。

[35] Cookie を用いる行動ターゲティング広告の大まかなイメージは、次のとおりである。まず、①ウェブブラウザは、ユーザーが閲覧しようとするウェブページのウェブサーバー（以下「コンテンツ事業者サーバー」という。）に対し、当該ウェブページの表示をリクエストする。②当該コンテンツ事業者サーバーは、広告事業者サーバーにアクセスするよう指示を出しつつ、当該ウェブページを表示させるレスポンスを行う。③レスポンスを受けたウェブブラウザは、前記②の指示に従って広告事業者サーバーにアクセスする。④これを受けた当該広告事業者サーバーは、Cookie を当該ウェブブラウザに対して発行しつつ、当該ウェブブラウザの当該コンテンツ事業者サーバーへのアクセス情報を保存する。⑤その後、当該ウェブブラウザが対象の広告枠に広告を表示させるに当たって、当該広告事業者サーバーに当該 Cookie を送信する。⑥これを受けた当該広告事業者サーバーは、当該 Cookie 等を参照することで、ユーザーの興味関心に応じた広告を配信することができる。

[36] 近年、オンライン広告におけるプライバシー侵害への危機感が高まり、欧米において利用者情報の取扱いに関する透明性やアカウンタビリティを高める法制度の適用が見られることも背景とし、プラットフォーム事業者等関係事業者においてクロスサイトトラッキング等をブロック又は抑制する方向で様々な検討が行われている（総務省・前掲注 28）76 頁）。例えば、2020 年３月に Apple が Safari におけるサードパーティ Cookie をブロックしたり（＜https://www.apple.com/jp/privacy/features/＞参照）、2020 年１月に Google が Chrome におけるサードパーティ Cookie のサポートを段階的に廃止する計画を発表したり（なお、2021 年６月に廃止延長の発表をしている＜https://japan.googleblog.com/2021/06/cookie.html＞参照）している。

第２章　Cookie 利活用と「通信の秘密」侵害との関係

第１節　「通信の秘密」の範囲

１．問題の所在

電気通信事業法第４条第１項は、電気通信事業者の取扱中に係る「通信の秘密」の侵害を禁止している。Cookie は、個々の通信に関する情報を記録することができるため、同項に定める「通信の秘密」に当たるようにも思われる。

もっとも、電気通信事業法は、「通信の秘密」の範囲について、条文上明らかにしていない。そこで、本節では、Cookie の「通信の秘密」該当性の検討に先立って、「通信の秘密」の範囲について検討する。

２．「通信の秘密」の範囲

（１）学説

ア　通信内容に限定する見解

「通信の秘密」の範囲については、以下のとおり、通信内容に限定されるとする見解が存在する。

（ア）表現の自由の一環として保障したものであると解する説[37]

この学説は、直接的には憲法上の「通信の秘密」について説いたものであるが、前述のとおり、電気通信事業法上の「通信の秘密」不可侵規制は、憲法上の「通信の秘密」不可侵規制を受けて制定されたものであるため、本稿においても触れることとする。

この学説は、憲法第 21 条第２項後段の規定を、表現の自由の一環として定められたものであると解するものである[38]。すなわち、自己の思想や感情（両者合わせて表現内容となる）をどの範囲で他人に表示するか決定する権利を有することを保障したものが「通信の秘密」不可侵規制であるとする[39]。

（イ）第１項・第２項分離保障説[40]

---

[37] 高橋郁夫・吉田一雄「『通信の秘密』の数奇な運命（憲法）」情報ネットワーク・ローレビュー第５巻（2006 年）66 頁。高橋らは、上記見解が憲法起草者意思であると分析している。

[38] 高橋らは、GHQ 草案について、「『……意思伝達の機密性は、侵されない。』とそもそも訳されるべきであったのではないか」としている（高橋ら・前掲注 37）66 頁）。

[39] 高橋らは、ここでいう「通信」とは、隔地者間での連絡に限られず、意思伝達の表現のうちの特定の者に対して伝えることをいうと解している（高橋ら・前掲注 37）67 頁）。

[40] 情報セキュリティ大学院大学「インターネットと通信の秘密」研究会「インターネット時代の『通信の秘密』再考」（2013 年）29 頁。なお、学説の名称は、筆者が便宜上定めたものである。

この学説は、電気通信事業法第４条第１項が「通信の秘密」について規定しており、また、同条第２項が「通信に関して知り得た他人の秘密」について規定していることに着目し、前者が「通信の内容の秘密」を、後者が「通信の外形的事項の秘密」を保障していると解するものである。

イ　通信の外形的事項も含まれるとする見解

前記アの見解に対し、電気通信事業法第４条第１項の「通信の秘密」の範囲には、通信内容のみならず、通信の構成要素（通信日時、場所、通信当事者の氏名、住所・居所、電話番号、メールアドレス）や通信の個数といった通信の外形的事項も含まれるとする見解が存在する[41][42]。

（ア）通信内容の探知可能性に着目する説

この学説は、通信の外形的事項が知られることによって通信内容が探知される可能性があることから、通信の外形的事項も保障の対象に含まれると解するものである[43]。

（イ）プライバシー保護主眼説

この学説は、「通信の秘密」不可侵規制の趣旨がプライバシー保護にあるとしたうえで、通信の外形的事項にもプライバシー性が認められるから、「通信の秘密」不可侵規制による保障の対象に含まれると解するものである[44]。

この学説を採る場合、通信の外形的事項に係る情報の「通信の秘密」該当性判断に当たって、通信内容の探知可能性は必要ないこととなる。もっとも、（ア）及び（イ）の考え方は、互いを排斥するものではないため、双方をその根拠と

---

41 曽我部真裕ほか『情報法概説 第２版』（弘文堂、2019 年）53 頁〔曽我部執筆〕、宍戸常寿「通信の秘密に関する覚書」長谷部恭男ほか編『現代立憲主義の諸相（下）』（有斐閣、2013 年）508 頁等。

42 なお、金光昭ほか・前掲注 24）23 頁では、公衆電気通信法第５条の「通信の秘密」について、「本条は前条と同じく思想表現の自由を絶対的に保証しようという民主主義の理念に基づくものであつて、公社又は会社の機関等……の取扱中にかゝる通信の秘密を侵害することを禁止し、以て確実なサービスを提供して公衆電気通信業務の信用を維持しようとするものである」としたうえで、「『通信の秘密』とは通信の内容は勿論、誰から誰への通信であるかと云う事実又は場合により単に通信の存在の事実をも意味」するとされている。

43 曽我部ほか・前掲注 41）53 頁〔曽我部執筆〕。もっとも、曽我部・前掲注 27）63 頁では、「通信の構成要素を通じて通信内容が推知される可能性があることなどから、これらも『秘密』に含まれるとされる」（下線は筆者による）としていることから、必ずしもその根拠を通信内容の探知可能性に限定しているわけではないと思われる。

44 高橋正俊「通信の秘密」小嶋和司編『ジュリスト増刊 法律学の争点シリーズ２ 憲法の争点（新版）』（有斐閣、1985 年）104 頁、芦部信喜『憲法Ⅱ人権（１）』（有斐閣、1978 年）641 頁。ただし、いずれも憲法第 21 条第２項後段の「通信の秘密」に関する議論である。

するものもある[45]。

（２）裁判例等

ア　「通信の秘密」不可侵規制の趣旨

（ア）最二小決 2004 年４月 19 日刑集 58 巻４号 281 頁

本件は、電気通信事業者が現に取り扱っていた通信の際に盗聴録音された通話内容を再生して十数名の第三者に聞かせる等した行為は、たとえ自らは盗聴録音に関与していないとしても（改正前）電気通信事業法第 104 条第１項の罪を構成することを明らかにした事例である。したがって、「通信の秘密」の範囲が直接問題となったわけではない。そのため、同決定では、「通信の秘密」の範囲について判断は示されていない。

もっとも、当該決定の調査官解説では、電気通信事業法研究会編著『電気通信事業法逐条解説』を引用して、「通信の秘密」不可侵規制の趣旨を説明している。具体的には、「『電気通信事業者が取扱中に係る通信の秘密』は、いったん通信当事者の手から離れ電気通信事業者に託されるものであるから、通信当事者が秘密を保護するための自衛措置を講じる余地がなく、また、秘密が侵害される危険にさらされやすいことにかんがみ、電気通信事業に対する利用者の信頼を保護するため、その秘密を侵すことを禁止したものであると解されている」としている[46]。

（イ）東京地判 2002 年４月 30 日裁判所ウェブサイト

本件は、被告人 A らが共謀して電気通信事業者 D 社のコンピュータシステムから H ら７名名義の加入電話７台に関する「基本情報照会」及び「料金基本情報」に係るデータを出力し、これが印字された文書を社外に持ち出した事例である。そのため、前記各データが「通信の秘密」の範囲に含まれるか否かが問題となっている。同判決は、その判断の前提として、「通信の秘密」不可侵規制の趣旨について、「個人のプライバシーの保護、ひいては個人の思想、表現の自由の保障を実効あらしめることにある」としている。

イ　「通信の秘密」の範囲

まず、大阪高判 1966 年２月 26 日高刑集 19 巻１号 58 頁は、郵便法の「信書の秘密」の範囲について、「信書の内容のほか、その発信人や宛先の住所、氏名等も含まれると解すべきである」としている。また、大阪高判 1967 年 12 月 25 日判時 514 号 82 頁は、公衆電気通信法の「通信の秘密」の範囲について、「単に通話

[45] 電気通信事業法研究会編著『電気通信事業法逐条解説 改訂版』（一般財団法人情報通信振興会、2019 年）36 頁。

[46] 山田耕司「判解」最高裁判所判例解説刑事篇平成 16 年度（2007 年）239 頁。

内容だけでなく誰と誰が通話したかという事実をも指」すとしている。

さらに、前掲東京地判 2002 年４月 30 日は、(改正前) 電気通信事業法第 104 条第１項の「通信の秘密」の範囲について、「通信内容のほか、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」とし、その理由として、「通信の相手方の住所・氏名・電話番号などを人に知られることによっても、個人の思想、表現の自由が抑圧されるおそれがあるからである」と述べている。

（３）総務省見解

総務省は、通信の秘密を保護する趣旨を、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としている[47]。また、総務省は、「通信の秘密」の範囲について、「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」としている[48][49]。

（４）検討

これまでみてきたそれぞれの見解に対する指摘や問題点等を確認したうえで、いかなる見解が妥当か検討する。

ア　通信内容に限定する見解

（ア）表現の自由の一環として保障したものと解する説（前記（１）ア（ア））

この学説に対しては、通信の外形的事項が他人に知られることで表現行為に対する萎縮効果をもたらし得ることから、通信の外形的事項にも「秘密」が及ぶと解する余地があるという指摘が存在する[50]。

また、「通信」でやり取りされる情報の中には「表現」とは言えないものも含

---

[47] 総務省プラットフォームサービスに関する研究会「同意取得の在り方に関する参照文書」＜https://www.soumu.go.jp/main_content/000734954.pdf＞（2021 年）１頁。

[48] 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解説」＜https://www.soumu.go.jp/main_content/000735774.pdf＞（2021 年）30 頁。

[49] なお、総務省電気通信事業ガバナンス検討会「電気通信事業ガバナンス検討会報告書（案）」＜https://www.soumu.go.jp/main_content/000787584.pdf＞（2022 年）21 頁において、「通信の秘密」の保護が「災害発生時等の非常事態における国家機能の維持及び国民の生命・財産の安全にとって不可欠な重要通信の確保など、国のインフラとして中枢神経的な機能を果たすものであ」るとされているが、これは、本文の見解と矛盾するものではなく、両立するものであると解する。

[50] 海野敦史『「通信の秘密不可侵」の法理－ネットワーク社会における法解釈と実践』（勁草書房、2015 年）150 頁。

まれるという指摘がある。例えば、機器間の通信においてやり取りされる情報は、「精神活動の表出」とは認めがたい場合が大半であるとされる[51][52]。

（イ）第１項・第２項分離保障説（前記（１）ア（イ））

この学説に対しては、そもそも実務上の解釈と異なるという指摘がある。

また、①通信の秘密と他人の秘密の区別は必ずしも明確ではないこと、②両者は多くの部分で重畳することを指摘したうえで、「個々の通信の外形的事項とはいえないが、それを推知させる可能性のあるもの」についてのみ、電気通信事業法第４条第２項の「他人の秘密」に当たると解すべきとする意見がある[53]。

イ　通信の外形的事項も含まれるとする見解

（ア）通信内容の探知可能性に着目する説（前記（１）イ（ア））

この学説に対しては、通信の外形的事項が一律に「通信の秘密」に当たるとする結論を直ちに導けるわけではないといえると考える。なぜならば、通信の外形的事項には、通信内容を探知できる可能性がないものも存在し得るからである。

（イ）プライバシー保護主眼説（前記（１）イ（イ））

この学説に対しては、プライバシー性の低い情報が「通信の秘密」に含まれないという結論が導かれ得るとする指摘がある[54]。

また、「通信の秘密」の範囲に通信の外形的事項が含まれるとする根拠をプライバシー保護のみに求めた場合、法人の「通信の秘密」が保障されると解する実務上の取扱いを直ちに説明できない[55]。

ウ　私見

以上のとおり、「通信の秘密」の範囲の解釈には、「通信の秘密」不可侵規制の趣旨が密接に関わる。そこで、「通信の秘密」不可侵規制の趣旨を再考したうえ

---

[51] 以上について、海野・前掲注 50）105 頁。

[52] なお、当該学説の当否とは別に、「原意」であるとする高橋らの理解に対する疑問を示すものとして、宍戸・前掲注 41）494 頁以下がある。

[53] 以上について、海野・前掲注 50）138 頁。加えて、「通信の秘密」の範囲が通信内容に限定されるとする見解全般に対して、個々の通信において、その内容と構成要素は密接に関わっており、これらは基本的に不可分のものとして捉えることが妥当であり、また、通信内容の秘密が通信の外形的事項の秘密よりも秘匿性、要保護性が高いとは限らないとの指摘がある（同 138 頁以下）。

[54] 海野・前掲注 50）137 頁。ただし、単独ではプライバシーとの関わりが低い情報であっても、それが他の（通信に関する）情報と結びついて新たなプライバシーを構成することもあり得るということには留意が必要であるとする（同 150 頁）。

[55] 同様の問題意識を示すものとして、神足・前掲注 25）47 頁。

で、「通信の秘密」の範囲について検討する。

(ア)「通信の秘密」不可侵規制の趣旨

「通信」は、もともと特定者間の閉鎖的コミュニケーションを想定しており、当該コミュニケーションの存在や内容が無断で知得されるのであっては、その存在価値が低下してしまう。それゆえ、「通信の秘密」不可侵規制は、当該価値を守るため、言い換えるならば、通信に対する「コミュニケーションの存在及びその内容を無断で他人に知得されない」という通信当事者の信頼・期待を守るためにあると考える[56][57]。ここでいう「コミュニケーションの存在及びその内容を無断で他人に知得されない」という通信当事者の信頼・期待には、通信を用いて自己の思想や感情を表出する際にその機密性が害されないことや、自己のプライバシーが害されないことへの信頼・期待が含まれていると解する。

したがって、電気通信事業法の「通信の秘密」不可侵規制の趣旨は、前述の総務省見解と同様、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というべきである。

以上のように解した場合、「通信の秘密」の範囲に含まれ得る情報について、逐一、「表現」に当たるか否か、プライバシー性が認められるか否か等を検討することなく「通信の秘密」に当たるとする実務上の取扱いと整合する。また、法人であっても安心・安全な通信（通信制度）に対する信頼・期待を持ち得るから、法人の「通信の秘密」を認める結論と親和的である。

(イ)「通信の秘密」の範囲

前記（ア）を前提にすると、「通信の秘密」の範囲には、以下のとおり、通信内容のみならず、通信の外形的事項も含まれると解するのが妥当であると考える。

まず、通信を用いた表現の自由の実効性を確保し、また、プライバシーを保護するためには、通信内容のみを「通信の秘密」とするのでは足りないと解する。なぜならば、通信の外形的事項が無断で知られることによって、通信を用いた表現活動に萎縮効果が生じたり、プライバシーが害されたりすることがあ

---

[56] 石井徹哉「通信の秘密侵害罪に関する管見」千葉大学法学論集 27 巻 4 号（2013 年）124 頁参照。また、電気通信事業法研究会・前掲注 45）35 頁では、「電気通信事業者の取扱中に係る通信」は、いったん通信当事者の手から離れ電気通信事業者に託されたものであり、通信当事者が秘密を保護するために自衛措置を講じる余地がなく、また、秘密が侵害される危険にさらされやすいことに鑑み、電気通信事業に対する利用者の信頼を保護するため、その秘密を侵すことを禁止しているとする。

[57] なお、公衆電気通信法における「通信の秘密」侵害未遂罪について、金光ほか・前掲注 24）292 頁では、「保護される法益が一般公衆の通信であり、これを侵害する危険性のあるものを排除して一般公衆に対して信頼できる通信手段を提供しようとする趣旨に基づくものである」としている。

るからである。

また、電気通信業務においては、通信内容のみならず、通信の外形的事項も取り扱うため、両者が「通信の秘密」として保護されることによってはじめて安心・安全な通信（通信制度）に対する利用者の信頼・期待を守ることができると考える。

したがって、「通信の秘密」は、通信内容又は通信の外形的事項をいうと解するべきである[58]。

第２節　「通信の秘密」に該当し得る情報と個々の通信の関係

１．問題の所在

前節のとおり、筆者は、「通信の秘密」を、通信内容又は通信の外形的事項であると解する。それゆえ、Cookie が通信内容又は通信の外形的事項に当たらない場合、Cookie は、「通信の秘密」に該当し得ないこととなる。

ところで、電気通信事業法は、いかなる情報が通信内容又は通信の外形的事項に当たるのか明示していない。したがって、特定の情報の「通信の秘密」該当性を判断するためには、これを明らかにしておく必要がある。

ここで、特に問題となるのは、対象となる個々の通信によって伝送されない情報（以下、「非伝送情報」という。）である。例えば、通話中の発信者を目撃した第三者がその場所を他人に伝えた場合、通信の外形的事項たる発信場所の漏えいが生じた（つまり、「通信の秘密」の侵害があった）とは評価しないことに違和感はないと思われる。もっとも、電気通信事業法が保障しているのは、「通信の秘密」であり、「通信」そのものではないことから、非伝送情報であることをもって直ちに「通信の秘密」該当性を否定できるわけではないと考える。例えば、ある電気通信事業者が提供する電話サービスにおける特定の通信の発信者氏名を明らかにすることを目的とした照会に対し、当該電気通信事業者がその目的を知ったうえで照会された電話番号に対応する加入者氏名を回答することは、実質的には当該通信の発信者氏名を回答することと同義であり、「通信の秘密」の問題となるように思われる。

そこで、本節では、まず、個々の通信といかなる関係があれば、通信内容又は通信の外形的事項に当たると評価できるか検討する。そのうえで、Cookie が「通信の秘密」に該当し得ることを確認する。

---

[58] 海野・前掲注 50）138 頁では、憲法第 21 条第２項後段の「通信の秘密」に関する議論ではあるが、通信当事者の公権力及び通信管理主体に対する「信頼」については、通信の内容たる情報の取扱い（保護）のみならず、その構成要素たる情報の取扱いにも及んでいるものと考えることが合理的であるとしている。

なお、後述のとおり、Cookie は個々の通信によって伝送される情報（以下、「伝送情報」という。）の側面を有するから、少なくとも通信内容であることが明らかであるため、Cookie の「通信の秘密」該当性判断との関係において、前記検討の必要性は必ずしも高くない。しかし、前述のとおり、本稿は、「通信の秘密」不可侵規制に関する諸論点の考察も目的としているため、これを検討することとする。

２．個々の通信との関係

ある情報について、個々の通信といかなる関係があれば、通信内容又は通信の外形的事項に当たると評価できるかという点について、これを正面から論じている学説は見当たらない。もっとも、これに関連する総務省資料及び裁判例が存在するため、これらを参照したうえで検討する。

（１）総務省見解

ア　一般

総務省は、法律上の照会権限を有する者からの照会等がなされた場合において、「通信の秘密」に属する事項を提供することは原則として適当ではないとしつつ、「個々の通信とは無関係の加入者の住所・氏名等は、通信の秘密の保護の対象外であるから、基本的に法律上の照会権限を有する者からの照会に応じることは可能である。」とする。もっとも、これに続けて、「個々の通信と無関係かどうかは、照会の仕方によって変わってくる場合があり、照会の過程でその対象が個々の通信に密接に関係することがうかがえるときには、通信の秘密として扱うのが適当である」（下線は筆者による）としている[59]。

したがって、加入者の住所・氏名等の情報は、それが「個々の通信に密接に関係する」ことがうかがえるか否かによって、「通信の秘密」として取り扱うべきか否か結論が変わるといえる。もっとも、総務省は、「個々の通信に密接に関係する」といえるか否かの判断方法について、具体的には明らかにしていない。

イ　開示された発信者情報を用いた電話会社への弁護士会照会

総務省は、特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律第４条に定める発信者情報開示請求により、権利侵害情報が書き込まれた場・サービスを提供していた事業者が保有する電話番号が請求者に開示された後、当該請求者の代理人弁護士が、権利侵害情報の発信者を特定する目的で、当該電話番号により電話サービスを提供する電気通信事業者（以下「電話会社」という。）に対して、弁護士法第 23 条の２第２項に基づく照会（以下「弁護士会照会」という。）により、当該電話番号に対応する加入者の住所・氏名の提出

[59] 以上について、総務省・前掲注 48）61 頁。

を求める場合について、「当該電話会社にとって、権利侵害情報の投稿通信は自ら提供する電話サービスの個々の通信ではなく、また、当該弁護士会照会は 当該電話会社が提供する電話サービスの個々の通信の発信者を明らかにするためのものではないため、これに応じることは通信の秘密を侵害するものではない」（下線は筆者による）としている[60]。

したがって、以上の場合における加入者の住所・氏名という情報は、「個々の通信に密接に関係する」ことがうかがえない無関係なものであると判断されたといえる。

（２）裁判例

前掲東京地判 2002 年４月 30 日は、前述のとおり、「通信の秘密」の範囲について判断を示しているところ、これに続けて、「例えば電話番号については、通信履歴（利用者が電気通信を利用した日時、当該通信の相手方その他の利用者の通信に係る情報であって通信内容以外のものをいう）や利用明細（利用者が電気通信を利用した日時、当該通信の着信先、これらに対応した課金情報その他利用者の電気通信に関する情報を記載した書面）におけるそれのように、個々の通信を取り扱った電気通信事業者のもとで、当該個々の通信に関係するものであることが分かる形で保管されている場合には、『通信の秘密』として保護されるが、電話番号情報（電気通信事業者が電話加入契約締結に伴い知り得た加入者名又は加入者が掲載、案内を希望する名称及びこれに対応した電話番号その他の加入者に関する情報をいう）におけるそれのように、個々の通信とは無関係に蓄積されたものである場合には、たとい電気通信事業者のもとで管理されていても、また、個人情報として保護する実際上の必要性の高いものであっても、『通信の秘密』の保護の対象外である」としている（下線は筆者による）。

よって、特定の事項について、「個々の通信を取り扱った電気通信事業者のもとで、当該個々の通信に関係するものであることが分かる形で保管されている」場合には「通信の秘密」に該当するといえることとなる。

（３）検討

まず、筆者は、前述の総務省見解や前掲東京地判 2002 年４月 30 日と同様、個々の通信に無関係な情報は、「通信の秘密」に該当しないと考える。なぜならば、個々の通信に無関係な情報を「通信の秘密」として取り扱ったところで、通信（通信制度）に対する利用者の信頼・期待等を保護することにはならないからである。

ここで、非伝送情報は、個々の通信によって伝送されないというその性質上、基本的には個々の通信と無関係なものである。したがって、非伝送情報は、原則とし

[60] 総務省・前掲注 48）62 頁。

て「通信の秘密」には該当しないというべきである。例えば、前記１で掲げた通話中の発信者を目撃した事例における「通話中の発信者の位置に関する情報」は、確かに通話に係る通信の発信場所と合致する情報ではあるものの、前記情報それ自体は、当該発信者が当時行っていた通信によって伝送されたものではない無関係なものであるから、「通信の秘密」には当たらないこととなる。

もっとも、非伝送情報であっても「個々の通信に密接に関係する」といえる情報は、「通信の秘密」に該当し得るというべきである。ここで、「個々の通信に密接に関係する」か否かの判断をどのように行うか明らかでなく問題となるが、「通信の秘密」の範囲が不当に広くなることを防ぐため、「通信の秘密」不可侵規制の趣旨に適合するか否かによるべきであると解する。

以上を前提にすると、前記（１）イで示した弁護士会照会事例における加入者住所・氏名は、当該電話会社が提供する電話サービスに係る契約の締結・履行によって生じたものではなく、これを保護しても安心・安全な通信（通信制度）に対する利用者の信頼・期待の保護等に資するものではないため、「個々の通信に密接に関係する」とはいえず、「通信の秘密」に当たらないこととなる[61]。

他方で、着信履歴に残された電話番号に対応する加入者氏名について、当該電話番号に対する電話サービスを提供する電気通信事業者が弁護士会照会を受けた場合における当該加入者氏名は、「個々の通信に密接に関係する」といえ、「通信の秘密」に当たると解する。なぜならば、当該電話番号に対応する加入者氏名が発信者氏名と同一であることが強く推認されるため、これを保護しなければ安心・安全な通信（通信制度）に対する利用者の信頼・期待の保護等に支障が生じるからである。

なお、電気通信事業者が電気通信役務とは別のサービス（例えば、会員ポイントサービス等）を提供していたとき、当該サービスに係る契約者氏名等の情報を電気通信役務に係る加入者氏名等の情報と明確に分けて管理しているのであれば、当該サービスに係る契約者氏名等の情報は、直ちには「個々の通信に密接に関係する」ものであるとはいえず、原則として、「通信の秘密」には当たらないこととなると解する[62]。

---

[61] 同様の理由で、あるコンテンツ事業者が有する特定の電話番号に対応する契約者氏名情報も基本的には「個々の通信に密接に関係する」とはいえないと考える。

[62] もっとも、実務上、当該サービス自体が電気通信役務と密接に関係していることが多い（例えば、電話サービスに係る契約者と非契約者とで当該サービスで受けられる特典等が異なっていたり、電話サービスに係る契約者にとっては当該サービスが当該電話サービスのオプションとして位置付けられたりすることが考えられる）ため、仮にそれぞれのサービスに係る氏名等の情報を別々のウェブサーバーで管理しているとしても、その事実をもって直ちに明確に分けて管理しているとは言い難いと考える（なお、前掲東京地判 2002 年４月 30 日参照）。

３．Cookie は「通信の秘密」に該当し得るか

Cookie は、これを伝送する通信（以下「Cookie 送信通信」という）の通信内容（伝送情報）である。したがって、Cookie は、Cookie 送信通信に「密接に関係する」といえる。

また、Cookie は、Cookie 送信通信に先立って行われた特定の通信（以下「記録対象通信」という。）に関する情報を含む。当該情報は、まさしく記録対象通信が行われた際に発生し、Cookie に記録されるものであるから、これを保護することは、安心・安全な通信（通信制度）に対する利用者の信頼・期待の保護等に資するといえる。したがって、Cookie は、記録対象通信に「密接に関係する」といえる[63]。

よって、Cookie は、Cookie 送信通信及び記録対象通信いずれの関係においても「密接に関係する」といえ、「通信の秘密」に当たり得るといえる。

第３節　「秘密」性の個別評価の可否

１．問題の所在

前節までみてきたとおり、筆者は、Cookie が「通信の秘密」に該当し得ると解するところ、一定の場合、事業者による Cookie の利活用について、ユーザー自身がこれを期待することが考えられる[64]。そのような場合、Cookie がそもそも「通信の『秘密』」に当たらないこととならないか。個別事例における通信内容又は通信の外形的事項に係る情報の取得・利用等の目的が何か、取得主体が誰であるか等の事情が「秘密」性の有無の評価を左右することがあるのか、条文上明らかでなく問題となる。

そこで、本節では、通信の「秘密」性を個別評価することの可否[65]について検討する。

２．「秘密」性の個別評価

（１）通信の「秘密」の意義

一般的に、「通信の『秘密』」とは、一般に知られていない事実であって、他人に知られていないことにつき本人が相当の利益を有すると認められるものをいい、

---

[63] なお、記録される情報によって、通信内容となる場合もあれば、通信の外形的事項となる場合もあると解する。

[64] 例えば、会員制ウェブサイトでログイン状態を維持することやオンラインショッピングサイトにおいて買い物かごに入れた商品を保持することは、そこでのサービスを利用するうえで必須であり、通常のサービス利用者であれば前記維持等を期待することが想定される。

[65] 通信の「秘密」性の推定の排除について、正面から論じているものはほとんどないとされている（曽我部・前掲注 27）63 頁参照）。

「相当の利益」の有無の判断は一般人を基準に行うものとされている[66]。

なお、特定者へ向けた「電気通信事業者の取扱中に係る通信」に係る情報には「秘密」性が推定されると説明されている[67]。

（２）「秘密」性に関する具体的事例

ア　発信者情報通知サービス

総務省は、発信者情報通知サービス[68]における発信者情報[69]について、「発信者が発信者情報の通知を阻止しない場合には、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から、通信の秘密侵害には当たらないこととなる」としている[70]。

発信電話番号について、学説からは、「従来、電話をかけるものとしての発信者の利益は、発信電話番号が秘密とされることにより、受信者の利益よりも、より強く保護されてきた。しかしながら、そのことは技術的に発信電話番号が受信者に表示され得なかったということに基づく事実上の既得権益にすぎず、発信者を受信者よりもより保護する積極的な法益があるわけではない」、「発信電話番号が秘密として保護されたのは、電話交換が自動化されてから後のことにすぎない。……交換手は受信者と発信者をつなぐに先立って、受信者に対し、発信者が誰であるか(時として電話番号が何番であるか)をあらかじめ通知していたのであり、その当時は発信電話番号はオープンになるのが当然であった。」との指摘がある[71]。

また、「少なくとも通信の当事者間では、発信電話番号を『通信の秘密』として保護する必要はない」という見解が存在する。この見解は、「通信の秘密」不可侵

---

66 電気通信事業法研究会・前掲注 45）35 頁参照。

67 電気通信事業法研究会・前掲注 45）36 頁。また、「当事者にとって、或いは客観的に秘密を要するものか否かを問わない」とする見解として、伊藤榮樹ほか編『注釈特別刑法第６巻Ⅱ交通法通信法編〔新版〕』（立花書房、1994 年）376 頁〔河上和雄執筆〕。

68 総務省「『発信者情報通知サービスの利用における発信者個人情報の保護に関するガイドライン』の解説」＜https://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/money/d_guide_04.html＞参照。

69 「発信者情報」とは、発信者に関する情報であって、当該情報に含まれる電話番号、氏名、住所、生年月日その他の記述、個人別に付された番号、記号その他の符号、映像又は音声により当該発信者を識別できるものをいう。これには、発信電話番号通知サービスによって通知される発信電話番号や発信者名通知サービスによって通知される発信者名等が該当し、発信者の顔写真や発信者の位置等の情報が伝達される場合には、これらも含まれる（総務省・前掲注 48）111 頁)。

70 総務省・前掲注 48）112 頁。

71 堀部政男編『発信電話番号表示とプライバシー』(NTT 出版、1998 年）56 頁〔多賀谷一照執筆〕。

規制を「通信当事者以外の第三者が通信の存在・内容を探知することを禁止することにより、通信の自由やプライバシーを確保するもの」と解したうえで、「通信当事者間では、通信の存在・内容は明らかであるから、発信電話番号を通信の秘密として保護する必要はない」とするものである[72]。

さらに、「通信の秘密」の保護範囲を、通信当事者に対するものと第三者に対するものとを区別し、「通信当事者間に自明の事実は通信相手に対しては秘密として保護されない」としたうえで、「ただし、発信者が受信者への通知を望まず、必ずしも受信者が知り得ない発信電話番号などの発信者情報は、通信相手に対しても保護すべき通信の秘密に該当することがある」とする見解もある[73]。

イ　公然性を有する通信

前述のとおり、一般的には、特定者へ向けた「電気通信事業者の取扱中に係る通信」に係る情報には「秘密」性が推定されると理解されている。これは、「通信」がもともと特定者の間の閉鎖的なコミュニケーションを想定しており、通常であれば秘匿性を有することに基づくものと考える。

これに対して、電子掲示板への投稿やウェブサイトへの掲載のように、不特定多数へ向けて表示されることを目的とした通信は、「公然性を有する通信」として、「通信の秘密」の保護の対象外と解されている（なお、インターネットとの情報の送受信行為に対しては、なお秘密の保護が及ぶとされている）[74]。これは、公然性を有する通信が前記想定の外の行為であり、通信内容等の情報に関して秘匿性が認められないことに基づくものと考える。

（３）検討

まず、通信内容又は通信の外形的事項に係る情報の取得・利用等の目的は、当該情報の客観的性質を左右するものではない[75]。同様に、通信内容又は通信の外形的事項に係る情報の取得者が誰（通信の相手方当事者又は第三者）であるかも、当該情報の客観的性質を左右するものではない[76]。したがって、通信内容又は通信の外形的事項に係る情報の取得・利用等の目的や取得者に着目して「秘密」性の有無を

---

[72] 以上について、堀部・前掲注 71）51 頁〔斉藤啓昭執筆〕。

[73] 間形文彦・高橋克己「ハニーポッドによる通信役務の提供と電気通信事業者の通信の当事者性に係る通信の秘密の問題に関する一考察」情報ネットワーク・ローレビュー第９巻第１号（商事法務、2010 年）105 頁。

[74] 宍戸・前掲注 41）510 頁、太田洋ほか編著『個人情報保護法制大全』（商事法務、2020 年）414 頁〔太田洋執筆〕参照。

[75] 取得・利用等の目的は、正当業務行為や緊急避難の成否の検討において問題となり得る。

[76] 取得者が誰であるかは、「通信の秘密」に対する侵害の有無の評価において影響し得る事実である（詳細は、第４節）。

個別評価することは不適切であるといえる。

この点、通信が一般的に秘匿性を有するものであることに鑑みると、通信内容又は通信の外形的事項に係る情報は、その取得・利用等の目的や取得主体にかかわらず、原則として、「他人に知られていないことにつき本人が相当の利益を有すると認められるもの」として、「通信の秘密」に当たるというべきである。

もっとも、公然性を有する通信において伝送された通信内容等については、秘匿性が認められない以上、「相当の利益」があるとはいえず、例外的に「秘密」性が否定されるというべきである。

３．Cookie の「通信の『秘密』」該当性

Cookie 送信通信は、そこで伝送される Cookie の存在及び内容を不特定多数へ向けて伝達することを目的としたものではない。したがって、Cookie は、「通信の秘密」に当たるというべきである。

第４節　侵害の意義

１．問題の所在

前節までみてきたとおり、Cookie は、「通信の秘密」に当たると解するところ、いかなる利活用が「通信の秘密」の侵害となるのかについては、別途検討を要する。

例えば、Cookie は、コンピュータによって自動的に処理されており、その送受信の都度、人間によってその存在及び内容が確認されているわけではないところ、コンピュータによる自動的な処理が「通信の秘密」の侵害となり得るのかについて、電気通信事業法は必ずしも明らかにしていない。また、ファーストパーティ Cookie の利活用において、ウェブブラウザからこれを受信するのは、一般的にはコンテンツ事業者サーバーであるところ、「通信の秘密」を通信の相手方当事者が取得・利用等することが侵害となり得るか否かについては、条文上明らかにされていない。

そこで、本節では、「通信の秘密を『侵（す）』」ことの意義を明らかにしたうえで、Cookie の利活用が「通信の秘密」を侵害し得ることを確認する。

２．侵害の意義

（１）一般

一般に、「秘密を侵す」とは、一定の範囲にとどまっている他人の「秘密」を、故意にその範囲の外に出るようにすることであり、「通信の秘密を侵す」ことには、知得、漏えい及び窃用の３類型があるとされている。

「知得」とは、通信当事者以外の第三者が積極的に「通信の秘密」を知ろうとい

う意思のもとでなされる行為であるとされる。また、第三者にとどまっている「通信の秘密」を、他人が知り得る状態にすることを「漏えい」といい、本人の意思に反して自己又は他人の利益のために用いることを「窃用」というとされる。なお、漏えい及び窃用の対象となる「通信の秘密」を当該第三者が知る意思があったか否か、知ったことが適法であるか否かは、漏えい及び窃用の有無の判断に影響しないとされる[77]。

（２）裁判例

裁判例には、知得及び漏えいの既遂時期について判断したものが存在する。

まず、盛岡地判 1988 年３月 23 日判時 1269 号 159 頁は、「電話の通話内容を録音すれば、すなわち通信の秘密の侵害になる」として、被告人がその録音内容を聞いたか否かは、本罪の成否には関係しないと判断している。

また、東京高判 1977 年９月 14 日判タ 364 号 301 頁は、電波法違反が問題となった事例ではあるものの、「電波法 109 条１項の無線通信の『秘密を漏らす』とは、無線通信が誰から誰宛に行なわれたかという事実、またはその行なわれた通信の意味内容を他人に漏らし、または他人が知りうる状態に置くことを指すものと解するのが相当である」とし、他人が知ったか否かは問題にならないことを明らかにしている。

（３）検討

ア　自動処理による侵害可能性

「通信の秘密」の主体によって設定された「秘密」の共有範囲の外にいる者が「通信の秘密」を知り得る状態にあるならば、現にこれを知っていなくとも、安心・安全な通信（通信制度）に対する利用者の信頼・期待は損なわれるといえる。ゆえに、「通信の秘密」の主体によって設定された「秘密」の共有範囲の外にいる者が「通信の秘密」を知り得る状態にあるならば、現にこれを知っていなくとも侵害になり得るというべきである[78]。

したがって、以上のような状態を作出できるのであれば、自動的な処理によってでも「通信の秘密」の侵害は生じ得ると解する。

イ　通信の相手方当事者による侵害可能性

（ア）知得

前述のとおり、一般的な説明では、「通信の秘密」の知得の主体は、通信当事

[77] 以上について、電気通信事業法研究会・前掲注 45）36 頁及び 37 頁参照。
[78] 以上の結論は、前掲盛岡地判 1988 年３月 23 日及び前掲東京高判 1977 年９月 14 日の判断と整合的であるといえる。

者以外の第三者であるとされる。これは、多くの場合に、通信の一方当事者から他方当事者に対して「通信の秘密」に係る情報が共有され、その結果、通信の両当事者の「秘密」となることに由来すると思われる。

確かに、「通信の秘密」に係る情報が通信の両当事者間で共有されることによって「秘密」の範囲が当事者間に設定されるのであれば、通信の一方当事者が当該情報を知ろうとしても、設定された共有範囲の外に「通信の秘密」が流出することにはならない。以上を前提にすれば、知得の主体は、第三者に限られるように思える。

しかし、「通信の秘密」は、必ずしも通信の両当事者の「秘密」ばかりではない。例えば、発信者氏名等の情報は、発信者のみの「秘密」である。したがって、受信者に共有されていない発信者のみにとどまる「通信の秘密」に係る情報を知ろうとする行為は、設定された共有範囲の外に「通信の秘密」を流出させることを意味し、第三者の場合と同様、知得に当たるというべきである。

（イ）漏えい及び窃用

前述のとおり、一般的な説明では、「通信の秘密」の漏えい又は窃用の主体は、通信当事者以外の第三者であるとされる。しかし、「通信の秘密」不可侵規制の趣旨が安心・安全な通信（通信制度）に対する利用者の信頼・期待の保護等であることに鑑みれば、通信の相手方当事者がこれを他人が知り得る状態に置いたり、本人の意思に反して自己又は他人の利益のために用いたりすることも電気通信事業法は禁じているというべきである。したがって、通信の相手方当事者であっても漏えい又は窃用をし得ると解する。

３．Cookie の取得・利用等による「通信の秘密」侵害

以上を前提にすると、まず、Cookie がコンピュータによって自動的に処理され、その存在や内容を人間が送受信の都度確認しているわけではない点は、「通信の秘密」に対する侵害可能性を否定する根拠にはならないと解する。

また、通信の相手方当事者によるファーストパーティ Cookie の取得・利用等の行為が「通信の秘密」の侵害に当たるか否かについては、そこに含まれる「通信の秘密」がどの範囲で共有されているかに左右されることとなるが、一般に Cookie に記録される情報には様々な情報が含まれるため、通話における通信内容のように、通信の両当事者が共有する「秘密」であるとは必ずしもいえない。特に、HTTP による通信がステートレスなものである以上、ある通信（Cookie 送信通信）と別のある通信（記録対象通信）が同一ウェブブラウザによって行われたという情報（及びこれに付随する情報）は、ユーザー側のみの「秘密」であるというべきである。したがって、ファーストパーティ Cookie の取得・利用等であっても「通信の秘密」の侵害に当たり得るというべきである。

なお、サードパーティ Cookie の利活用の場合、当該サードパーティ Cookie の発行者は、記録対象通信との関係で無関係な者であるから、当該発行者が当該サードパーティ Cookie を取得・利用等する行為は、「通信の秘密」の侵害に当たり得るというべきである。

以上より、Cookie の利活用は、形式的には「通信の秘密」の侵害となり得るため、これを適法に行うためには、ユーザーの「有効な同意」等が必要となる。そこで、第２部では、「有効な同意」を得るための適正な「同意取得の在り方」について検討する。

第２部　「有効な同意」の取得に関する考察

第１章　「有効な同意」の意義

１．問題の所在

「通信の秘密」の侵害については、「通信の秘密」侵害罪（電気通信事業法第 179 条）として禁じられているところ、総務省は、「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……適法化される」と説明している[79]。

もっとも、総務省は、その理由を必ずしも明確に説明していない。例えば、総務省利用者視点を踏まえた ICT サービスに係る諸問題に関する研究会「利用者視点を踏まえた ICT サービスに係る諸問題に関する研究会第二次提言」11 頁では、「当事者の同意により秘密性が解除される」ことから「侵害に当たらない」としているが、この記述からは、「有効な同意」がいかなる機能を有するのか直ちに判別することができない。すなわち、「有効な同意」があることによって、①「秘密」性が否定されることとなる（それゆえに、「通信の秘密」に対する侵害が認められない）のか、②「侵して」いないこととなるのか、③「通信の秘密」の侵害に関する違法性が阻却されるのか、適法化される理由が明らかでないのである。

そこで、いずれの考え方が妥当か検討する。

２．検討

まず、前述のとおり、筆者は、通信内容又は通信の外形的事項に係る情報は、公然性を有する通信の場合を除き、「秘密」性が認められると解している。そのため、当該情報に対する「通信の秘密」の主体たる通信当事者の主観は、「秘密」性の有無の判断に影響を与えないと考える。

また、前述のとおり、「知得」とは、積極的に『通信の秘密』を知ろうという（知得者の）意思のもとでなされる行為であり、当該情報に対する「通信の秘密」の主体たる通信当事者の主観を問題にしていない。ゆえに、「有効な同意」があることによって「侵して」いないことになると解することは、その定義との関係で困難であると考える。

他方、「有効な同意」により違法性が阻却されると解した場合、「秘密」や「知得」の定義と矛盾することはない。

したがって、「有効な同意」は、「通信の秘密」の侵害に関する違法性を阻却するも

---

[79] 総務省・前掲注 47）２頁。

のであると解するべきである[80]。

[80] なお、電気通信事業法研究会・前掲注 45）37 頁では、誰の承諾を要するかという文脈ではあるものの、被害者の承諾によって違法性が阻却されることを前提にしていることがうかがえる。

第２章　「有効な同意」の取得について

第１節　「有効な同意」の取得に関する従前の整理

１．原則：個別具体的かつ明確な同意

総務省は、従前、「有効な同意」について、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うえで真意に基づく同意であることが求められるとし、「有効な同意」であるといえるためには原則として「個別具体的かつ明確な同意」であることが必要であるとしてきた[81]。

「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うえで行うことを意味し、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」認識したうえで同意を取得するという意味の２つの意味を含むとされている[82]。なお、「具体的」とは、「通信の秘密」に関する事項を利用者が「具体的」に認識したうえで同意を取得することを意味するとされている[83]。

また、「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等外部的に同意の事実が明らかな場合を意味するとされている。ただし、事前にチェックされたデフォルトオンによることだけでは「明確」な同意とはいえないとされている[84]。

２．例外的な判断がなされた事例

前記１のとおり、総務省は、「有効な同意」について、原則として「個別具体的かつ

---

[81] 総務省・前掲注 47）２頁。また、総務省・前掲注 48）30 頁では「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」としている。

[82] 総務省・前掲注 47）11 頁。なお、同頁では、「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ことを確認している。また、総務省緊急時等における位置情報の取扱いに関する検討会「位置情報プライバシーレポート～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活用の両立に向けて～」＜https://www.soumu.go.jp/main_content/000303636.pdf＞（2014 年）27 頁では、「個別」同意について、位置情報の取扱いについての同意であることを本人が認識したうえで画面上でのクリック等により行う同意であると説明している。

[83] 総務省・前掲注 47）12 頁。

[84] 総務省・前掲注 47）13 頁。また、総務省・前掲注 82）27 頁。

明確な同意」であることを必要であるとしてきた。他方で、総務省は、いくつかの事例において、「個別具体的かつ明確な同意」でない同意が例外的に「有効な同意」となる余地があることを示してきた。本項ではその内容を確認する。

（1）迷惑メール等のフィルタリング[85]（デフォルトオン）

総務省は、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親会（第18回会合）において、電気通信事業者が管理するウェブサーバー等で行う電子メールのフィルタリングサービス[86]の提供に関し、いかなる同意が「有効な同意」となるか見解を示している[87][88]。

まず、初期設定をフィルタリングオフとし、利用者から申込みを受けてフィルタリングを提供する場合について、総務省は、一般的に「有効な同意」があると考えられると判断している。

他方で、初期設定をフィルタリングオンの状態で提供する場合、すなわち、事前

---

[85] 一般に、電子メールのフィルタリングとは、特定の電子メールに関して、その内容等を機械的に検索し、あらかじめ設定した一定の条件に合致する電子メールを検知してブロック等することをいう。例えば、電子メール本文中のキーワードフィルタリング（事前に設定したキーワードが、受信した電子メールの本文中に含まれているかどうかを検索し、キーワードが含まれている電子メールをブロック等するもの）等がある（以上について、総務省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親会（第18回会合）資料「電気通信事業者が行う電子メールのフィルタリングと電気通信事業法第４条（通信の秘密の保護）の関係について」＜https://warp.da.ndl.go.jp/info:ndljp/pid/283520/www.soumu.go.jp/joho_tsusin/d_syohi/060123_1.html#b＞（2006年）第１参照）。

[86] 主に、利用者が市販のフィルタリングソフトを購入したりインターネット上からダウンロードしたりして、自己の端末にインストールして利用する方法と、電気通信事業者が、その管理するウェブサーバー等において行う方法がある。総務省・前掲注85）では、このうちの後者と「通信の秘密」の関係について整理している。

[87] なお、電子メールのフィルタリングは、受信者のために行う行為であるから、原則として正当業務行為に該当しないとされる（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「DMARC等の送信ドメイン認証技術の導入に関する法的な留意点」＜https://www.iajapan.org/anti_spam/event/2017/conf_16-17th/pdf/OD-09_D3-10.pdf＞（2017年）５頁）。

[88] こうした整理が求められた背景としては、迷惑メールや有害情報のウェブ閲覧に対するフィルタリングにおいては、送信者から同意を得ることが期待できないといった事情があったとされる（総務省利用者視点を踏まえたICTサービスに係る諸問題に関する研究会「利用者視点を踏まえたICTサービスに係る諸問題に関する研究会第二次提言」＜https://www.soumu.go.jp/main_content/000067551.pdf＞（2010年）９頁）。なお、この判断の前提として、①電気通信事業者の取扱中に係る電子メールの内容又は構成要素が「事業者の取扱中に係る通信の秘密」に当たり、②電気通信事業者がその取扱中に係る電子メールの内容又は構成要素についてフィルタリングを行い、あらかじめ設定した条件に該当する特定の電子メールを検知して、通信当事者の意思に反して利用する行為が「通信の秘密」の侵害に当たるものと整理している（総務省・前掲注85）第２）。

の包括的同意による場合については、同意の対象となる事項が将来の事実に及ぶため予測に基づく不確実な同意になる等、同意の対象・範囲等が不明確になりやすく、同意主体が正確に同意の対象・範囲を理解したうえで同意していないことが想定されること等から、一般的には適当とはいえないとしている。

もっとも、総務省は、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（電気通信事業法第 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こと）という５つの要件を満たす場合には、事前の包括的同意であっても、例外的に利用者の「有効な同意」に基づくフィルタリングと解することができると判断している[89]。

（２）CGM サイト運営者によるミニメールの内容確認（デフォルトオン）

総務省は、「利用者視点を踏まえた ICT サービスに係る諸問題に関する研究会第二次提言」において、ミニメール[90]を提供する CGM 運営者が自ら管理するウェブサーバー上で行うミニメールの内容確認[91]について、いかなる同意が「有効な同意」となるか見解を示している[92]。

まず、総務省は、CGM 運営者が通信当事者とならないミニメールについて、CGM 運

---

[89] 総務省・前掲注 85）第３（２）イ。

[90] いわゆる「ミニメール」は、CGM サイトに会員登録を行っている利用者の間でメッセージを交換するサービスであり、発信者が CGM 運営者の管理するウェブサーバーにメッセージを発信・記録し、受信者が当該記録されたメッセージを閲覧（受信）することによって通信が行われるものである（総務省・前掲注 88）９頁）。

[91] ミニメールを契機とする被害への対策として、一部の CGM 運営者や運営者から委託を受けた監視事業者は、ミニメールの通信内容を確認し、規約違反内容の削除等を実施している。内容確認の手法としては、発信時（ウェブサーバーへの反映以前）にはあらかじめ設定された一定のキーワードを含む内容を機械的に検知して発信を防止し（ベイジアンフィルタリング）、発信後（ウェブサーバーへの反映以後）は目視を含めた内容確認に基づき規約違反メッセージの削除等を行うというのが一般的であるとされている（以上について、総務省・前掲注 88）９頁）。

[92] この判断の前提として、①ミニメールの内容が「通信の秘密」の対象に含まれること、②ミニメールを提供する CGM 運営者（又は業務委託を受けた者）が自ら管理するウェブサーバー上で内容確認を行っている限りにおいては、原則として「電気通信事業者の取扱中に係る通信」に該当すること、③ミニメールの内容確認は、CGM 運営者が積極的意思に基づいて通信内容を検知し、通信当事者の意思に反して処理（利用規約に基づく削除等）を行おうとする限りにおいては、知得ないし窃用に該当するといえるのであって、通信の秘密の侵害に該当することを判断している（総務省・前掲注 88）９頁）。

営者が内容確認を行うことに関する発信者等の「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としている。また、ミニメール利用者の明示的な意思表示に基づいて行う必要があるため、デフォルトオフで個々の同意（発信時の画面表示での確認）を得ることを条件として内容確認を行うことが望ましいとしている。

そのうえで、総務省は、デフォルトオンでのミニメールの内容確認については、前記（１）の迷惑メール等のフィルタリング事例に関する検討内容を参照したうえで、前記５要件とほぼ同様の要件を掲げ、その実施が認められる余地があることを示している。

もっとも、総務省は、当該５要件のうち、④「通常の利用者であれば同意することがアンケート結果等により合理的に推定されること」という要件について、「CGM運営者が通信当事者とならない場合の『ミニメール』内容確認について、利用者の包括同意は推定されにくいため、個別のサービスについて利用者啓発等を通じて、同意が合理的に推定される環境を整備していく必要がある」としている。したがって、総務省は、少なくとも 2010 年当時、デフォルトオンでのミニメールの内容確認が直ちに実施可能であると判断したわけではないといえる[93]。

（３）マルウェアに感染している可能性が高い端末の利用者に対する注意喚起

総務省は、「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」（以下「第三次とりまとめ」という。）において、ISP がマルウェアに感染している可能性が高い端末の IP アドレス、ポート番号及びタイムスタンプに関する情報を、ISP の保有する契約者情報、通信履歴等と照合し、当該端末に係る通信回線の契約者及び連絡先を特定したうえで、当該契約者に注意喚起することについて、いかなる同意が「有効な同意」となるか見解を示している[94]。

まず、総務省は、「第三次とりまとめ」10 頁において、「有効な同意」があるとは、原則として、「通信の秘密」を侵すことに対する認識、認容がある場合をいい、通常は契約約款等に基づいた事前の包括同意のみしかない場合を含まないとしている。そして、総務省は、その理由として、①契約約款は当事者の同意が推定可能な事項を定める性質のものであり、「通信の秘密」の利益を放棄させる内容は、通常その性質になじまないこと、②事前の包括同意は将来の事実に対する予測に基づいて行われることからその対象、範囲が不明確となることの２点を挙げている。

他方で、総務省は、同頁において、契約約款等による事前の包括同意のみしかな

---

93 以上について、総務省・前掲注 88）12 - 13 頁。

94 総務省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「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」＜https://www.soumu.go.jp/main_content/000575399.pdf＞（2018 年）12 頁。

いときであっても「有効な同意」となり得る場合として、❶利用者が、ISP において「通信の秘密」を侵すことについて通常承諾すると想定し得るため、契約約款等による同意になじまないとはいえない場合で、かつ、❷利用者に将来不測の不利益が生じるおそれがない場合を挙げている。

そして、総務省は、❷の将来不測の不利益が生じるおそれがないといえるか否かを判断するに当たっては、ⅰ）侵される通信の秘密の対象・範囲が明確であるか、ⅱ）利用者が、いったん契約約款等に基づいて同意した後も、随時、容易に同意内容を変更（設定変更）できるか、ⅲ）当該契約約款等の内容及び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か、ⅳ）契約約款等に基づく措置の内容、同意内容の変更の方法等について、利用者に相応の周知が図られているか、といった点を考慮する必要があるとしている[95]。

そのうえで、総務省は、前記注意喚起に関する当事者の「有効な同意」に関して、契約約款等による事前の包括同意で足りるとする余地がないか、以下のように判断している[96]。

ア　前記要件❶について

まず、総務省は、マルウェアに感染している可能性が高い端末の利用者に対する注意喚起を ISP が行うことや前記照合によって契約者を特定することは、一般的・類型的にみて、利用者における安全なインターネット利用環境の確保に向けられた行為であるとしている。そのうえで、総務省は、通常の利用者であれば、自らが利用している端末についてマルウェアに感染している可能性が高い場合には、注意喚起に必要最小限の範囲で、ISP が「通信の秘密」を利用することを承諾することが想定し得ることから、契約約款等に定めを置くことがその性質になじまないとはいえないとしている。

---

[95] なお、総務省は、ISP が、ネットワーク上でユーザーのアクセス先をチェックし、ユーザーによる海賊版サイトへのアクセスを検知した場合に警告画面を表示させる等の仕組み（アクセス警告方式）を用いる前提条件となる「有効な同意」についても、同様の規範を定立したうえで契約約款等による事前の包括同意がこれに当たるか検討している（もっとも、前記要件❶が満たされないと判断している）（総務省インターネット上の海賊版サイトへのアクセス抑止方策に関する検討会「インターネット上の海賊版サイトへのアクセス抑止方策に関する検討会報告書」＜https://www.soumu.go.jp/main_content/000638089.pdf＞（2019 年）11 頁）。

[96] なお、前提として、このような注意喚起を行うに当たっては、ISP として取得、管理している通信履歴等を用いて当該事業者の取扱中に係る通信の通信当事者を識別することとなることから、利用者の有効な同意又は違法性阻却事由がない限り、「通信の秘密」の窃用等に該当し、「通信の秘密」の侵害となると判断している（総務省・前掲注 94）12 頁）。

イ　前記要件❷について

また、総務省は、注意喚起に関して利用される「通信の秘密」の対象、範囲は、明確であり、利用者に不測の不利益が生じる可能性は高くないとしている。そのうえで、総務省は、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、b）利用者が、一旦契約約款等に同意した後も、随時、同意内容を変更できる（設定変更できる）ようにする、 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契約内容とする、d）本件対策の内容とともに、注意喚起を望まない利用者は随時同意内容を変更できる（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、といった条件が満たされている場合には、契約約款等による包括同意を行った当時において予測し得なかった事情が生じた場合についても、随時、利用者が同意内容を変更することができることから、将来、利用者が不測の不利益を被る危険を回避できるといえるとしている。そして、結論として、上記 a）乃至 d）の条件を満たせば、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」に当たると判断している。

第２節　「同意取得の在り方に関する参照文書」の公表

１．経緯

第１節でみてきたとおり、総務省は、「有効な同意」を得るためには、原則として「個別具体的かつ明確な同意」であることが必要であるとしてきた。もっとも、総務省は、この点に関する資料として、2021 年２月に「同意取得の在り方に関する参照文書」（以下「参照文書」という。）を公表し、従前の見解とは異なる考えを示した。

なお、参照文書は、総務省が「プラットフォームサービスに関する研究会最終報告書」において[97]、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とから、「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旨の報告をしたことから、策定・公表されたものである[98]。また、参照文書が公表された後、立案担

[97] 総務省プラットフォームサービスに関する研究会「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＞（2020 年）11 頁参照。

[98] 丸山和子ほか「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』」情報通信政策研究５巻１号Ⅳ-57 頁。なお、総務省プラットフォームサービスに関する研究会「改正電気通信事業法の施行に向けた準備」＜https://www.soumu.go.jp/main_content/000720817.pdf＞（2020 年）では、電気通信事業者に対する通信の秘密の規律の適用に関する予見可能性や

当者による同文書の解説（以下「参照文書解説」といい、参照文書と総称して「参照文書等」という。）も公表されている。

２．「個別具体的かつ明確な同意」に関する説明

まず、総務省は、参照文書において、「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。」と説明している[99]。この点に関して、参照文書解説では、「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」と解説されている[100]。なお、「有効な同意」であるか否かの評価と「同意取得の在り方」が適正であるか否かの評価の関係については、参照文書等において明言されていないものの、参照文書解説Ⅳ-63 頁において、「『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……」（下線は筆者による）と言及されていることからすると、これらの評価は表裏一体の関係にあると思われる。

また、総務省は、参照文書において、「個別具体的かつ明確な同意」について、同意が「個別具体的」であること及び「明確」であることが「有効な同意」における必要十分条件でないと説明している[101]。

以上をまとめると、総務省は、基本的には、「個別具体的かつ明確な同意」を取得したならば、適正な「同意取得の在り方」によって「有効な同意」が得られたと評価できると解しているものの、「個別具体的かつ明確な同意」を取得したときであっても「有効な同意」と評価されない場合もあれば[102]、「個別具体的かつ明確な同意」でない同意を取得したときであっても「有効な同意」と評価される場合もある[103]と解していることとなる。

３．「有効な同意」に関する総務省見解

透明性を高める観点から、利用者からの「同意取得の在り方」に関する考え方を明らかにし、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の参照文書として公表するとされている。

[99] 総務省・前掲注 47）11 頁。

[100] 丸山ほか・前掲注 98）Ⅳ-63 頁。

[101] 総務省・前掲注 47）11 頁。

[102] 総務省・前掲注 47）11 頁では、「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」としている。

[103] 例えば、第１節２で挙げた事例における同意取得方法が考えられる。

以上に加え、総務省は、参照文書において、「『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」り、「個別事例における『リスク』に比例して変わり得る」としている[104]。また、総務省は、「『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……一定の『リスク評価』の結果に応じた手続とすることがあり得る」としている[105]。

したがって、同じ同意手続であっても、「有効な同意」の有無や「同意取得の在り方」の適正性に関する評価は、「リスク」の大小によって変わり得ることとなる。この点、総務省は、これまで「有効な同意」に関する「リスク評価」について、詳細な説明を示してきたわけではない。そこで、次節では、「リスク評価」に関するいくつかの事項について考察することとする。

第３節　「リスク評価」に関する考察

１.「リスク」及び「リスク評価」とは

参照文書によると、「リスク」とは、行為の性質、結果の重大性及び結果発生の蓋然性等であるとされている[106]。

また、参照文書によると、「リスク評価」とは、リスクベースアプローチ[107]の一環で行われるプライバシー影響評価（PIA：Privacy Impact Assessment）[108]の考え方を「通信の秘密」に対して応用するものであり、当該行為の性質、当該行為から発生する結

---

104 総務省・前掲注 47）11 頁。

105 以上について、総務省・前掲注 47）８頁及び 11 頁参照。

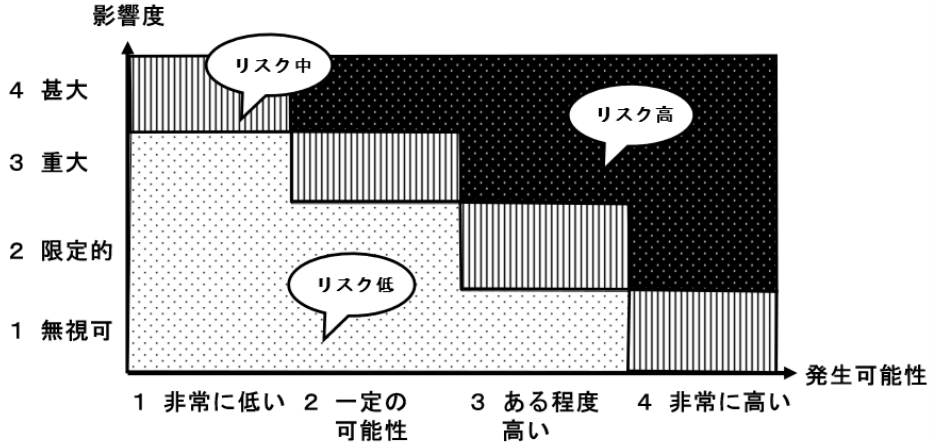
106 総務省・前掲注 47）８頁。なお、総務省・経済産業省「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」＜https://www.meti.go.jp/press/2020/08/20200821002/20200821002-3.pdf＞（2020 年）49 頁では、「リスク」を「目的に対する不確かさの影響。事象の結果とその起こりやすさ(発生確率)との組み合わせ」としている。

107 一律の要求事項を定めるのではなく、顕在化しうるリスクの内容に応じた対応方法の選択を実施する手法のこと（総務省・経済産業省・前掲注 106）49 頁)。総務省は、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が多様化していることから、政府・事業者においてもそれらの予測・把握が困難になっていると考えており、このような状況を踏まえ、リスクベースアプローチが新たに発生するリスクにも対応できる枠組みとして推奨されるとしている（総務省・前掲注 47）６頁)。

108 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あらかじめ把握し、適切な対応方法を設計するために行われるものである。PIA は、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されている。以上について、総務省・前掲注 47）６頁参照。

果の重大性及び結果発生の蓋然性等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とされている[109]。

「リスク」の評価方法について、参照文書等には具体的な手順等の詳細な説明はなされていないものの、一般的なPIAの手法について説明す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-」（以下「個情委資料」という。）において、「特定されたリスクについて、『影響度』及び『発生可能性』の観点で評価する」とされていることを踏まえると[110]、同様に、「リスク」を「影響度」と「発生可能性」の二軸で評価することができると解する。



＜図＞リスクマップのイメージ

＜図＞は、一例であるが、事業者は、「影響度」と「発生可能性」の組み合わせに応じて、「リスク」を高・中・低と評価することができると考える。

一般に、「影響度」が大きく「発生可能性」が高い場合、「リスク」が高いことから、

[109] 総務省は、「通信の秘密」に関する情報が一般に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るところ、「リスク評価」によって「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になるとする。また、「リスク評価」の際には、「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とし、「リスク評価」によって「通信の秘密」に係る情報の取得・利用等によるユーザー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及び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とする（以上について、総務省・前掲注47）7頁参照）。

[110] 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＞（2021年）13頁。

当該「通信の秘密」に係る情報の取得・利用等を中止することも含め、前提条件の変更を検討する必要が生じることとなる。また、「影響度」は小さいものの「発生可能性」が高い場合（あるいは、「発生可能性」は低いものの「影響度」が大きい場合）には、適切な対策を実施することで「リスク」を低減させることが求められることとなる。他方で、「影響度」が小さく「発生可能性」も低い場合には、「リスク」が低いことから、必ずしもリスク低減措置を講じなくてもよいといえる。

２．評価基準及び対応方針の設定とその影響

（１）評価基準及び対応方針の設定

参照文書等では明示的に説明されていないが、「リスク評価」が PIA の考え方を応用するものであることを踏まえると、事業者が実際に個別事例において「リスク」の評価を行うに当たっては、以下の２つの事項を検討する必要があると考える。

１つ目の検討事項は、「リスク」の評価基準の具体的内容である。この点、一例として示した＜図＞では、縦軸の「影響度」を、個情委資料に倣って、「無視可」、「限定的」、「重大」、「甚大」としているが、実際に運用するためには、これに加えて、それぞれの基準の具体的内容を定めることが必要となる。例えば、個情委資料では、「甚大」の基準を、「利用者に回復不可能な多大な不利益が生じ、これに伴い、企業の信用失墜や経済的損失が生じる」と定めている[111]。

２つ目の検討事項は、リスク回避又はリスク低減措置の要否に関する方針である。いかなる「影響度」及び「発生可能性」の組み合わせの場合に措置を要するのか、当該措置はリスク低減措置で足りるのか、リスク回避措置まで要するのか等の対応方針を定める必要があると考える[112]。

以上の設定をすることで、事業者は、リスクマップ上に個々の「リスク」を正確に示すことが可能となり、また、一貫性のある「リスク」対応をとることが可能となると考える。

（２）評価基準や対応方針の不合理な設定による影響

ところで、仮に、事業者が「通信の秘密」に係る情報の取得・利用等の必要性が高い等の理由から、「リスク」が低く見えるよう評価基準を設定したり、評価され

---

[111] 個人情報保護委員会・前掲注 110）13 頁。その他、「重大」を「利用者に一定の不利益が生じるものの、回復可能であり、企業の信用等への影響はそれほど大きくない」、「限定的」を「一部の利用者に不安感を与え、企業の信頼等に影響が及ぶ可能性があるが、その範囲は限定的」、「無視可」を「利用者への不利益の程度は極めて小さく、企業への影響は無視できるレベル」と、それぞれ設定している。

[112] 「リスク回避」とは、事業計画の中止も含め、事業の前提条件の変更をすることをいい、「リスク低減」とは、適切な対策を実施することでリスクを低減することをいう（個人情報保護委員会・前掲注 110）16 頁）。

た「リスク」に対する方針を著しく緩やかなものにしたりした場合、「有効な同意」の有無や「同意取得の在り方」に関する評価にいかなる影響が生じるか[113]。

まず、「有効な同意」の有無については、以上のような不適切な設定がされたことに起因して本来存在しないはずの「有効な同意」が「ある」と評価されることはないと解する。なぜならば、「有効な同意」の評価を左右するのは、あくまでも客観的な事実に基づく「リスク」それ自体であり、当該「リスク」を事業者がどのように評価したか（すなわち、「リスク評価」の結果内容）は、「有効な同意」の有無の評価を左右するわけではないからである。

他方、不適切な設定をしたうえで同意を取得したという事実は、不適正な「同意取得の在り方」であるとの評価に繋がり得ると解する。特に、不合理な「リスク評価」によって約款等による同意プロセスを恒常的に採用している等の場合には、「通信の秘密の確保に支障がある」（電気通信事業法第 29 条第１項第１号）として、改善命令の対象となるおそれがあると考える[114]。

以上を踏まえると、事業者は、「リスク評価」を実施するに当たり、「リスク」の評価基準及び「リスク」の対応方針を適切に設定することが肝要であるといえる。

３．「リスク評価」と利用者等の便益の関係

（１）問題の所在

総務省は、「リスク評価」には、①「評価対象となるサービス」プロセス、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」プロセス、③「リスクの特定・評価」プロセス、④「対策の決定・リスクの管理」プロセス等を考えることができ、各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としている[115]。そして、参照文書には、それぞれのプロセスにおける検討事項が列挙されている[116]。

---

[113] これらの設定は、あくまでも事業者による自主的な事前審査の際に用いられるものに過ぎないのであるから、唯一の正解があるわけではなく、合理的な範囲内で設定されている限り、同じ「リスク」に対する評価が事業者によって異なることもあり得るものと考える。

[114] 総務省プラットフォームサービスに関する研究会「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」＜https://www.soumu.go.jp/main_content/000734953.pdf＞（2021 年）９頁参照。

[115] 総務省・前掲注 47）10 頁。

[116] ①「評価対象となるサービス」プロセスでは、「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」が検討事項となっている。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」プロセスでは、「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

前述のとおり、「リスク評価」が PIA の考え方を応用するものであることを踏まえると、基本的にはこれらのプロセスや検討事項は、PIA の実施手順[117]に準拠するものであると考える。しかし、総務省は、参照文書内において、各プロセスにおける検討事項が「リスク評価」においてどのように用いられるか具体的な説明をしていない。特に、①「評価対象となるサービス」のプロセスで掲げられている「得られる利用者又は社会の便益」については、個情委資料では言及されておらず、それ自体が「リスク」の高低に関する評価を左右したり、「リスク」が高い場合であってもこれが「リスク」に優越することによって「有効な同意」と評価されたりするかのようにも受け取られかねないため[118]、その用い方を明らかにする必要があると考える。

（2）検討

ア　結論

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」が検討事項となっている。③「リスクの特定・評価」プロセスでは、「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」が検討事項となっている。そして、④「対策の決定・リスクの管理」プロセスでは、「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」が検討事項となっている（以上について、総務省・前掲注 47）10 - 11 頁)。

[117] 個人情報保護委員会・前掲注 110）８頁によると、PIA の一般的なプロセスは、❶「準備」プロセス、❷「リスクの特定・評価」プロセス及び❸「リスクの低減」プロセスに大別することができるとしている。まず、❶「準備」プロセスでは、PIA を実施するかどうかが検討され、その後、PIA を実施するための体制の整備や、個人情報等を取り扱う事業における当該個人情報等のフローを確認する等の多角的かつ幅広い情報収集・整理が行われるものとされている。つぎに、❷「リスクの特定・評価」プロセスは、❶「準備」プロセスをもとに、評価者が個人情報等の取扱いに係る「リスク」を具体的に特定・評価し、重大な「リスク」の所在や、「リスク」を低減するための対応を要する事項を洗い出すものであるとされている。そして、❸「リスク低減」プロセスでは、❷「リスクの特定・評価」プロセスで評価者が特定・評価した「リスク」を低減するための具体的な対策・計画を、設計者等が策定し実行するものとされている。

[118] 筆者は、利用者又は社会が得られる便益は、基本的にはプライバシー等への「影響度」や「発生可能性」を左右するものではないので、「リスク」の高低に関する評価に直接影響を与えるものではないと考える。また、利用者又は社会が得られる便益が大きいのであれば、「リスク」が高くても、緩やかな手続で取得した同意が「有効な同意」となるといった利益衡量は、総務省が「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」が必要としてきたことと必ずしも適合しないため、不適当であると考える。

筆者は、「得られる利用者又は社会の便益」は、一定の同意手続がとられるのであれば許容できる「リスク」であることを前提に、④「対策の決定・リスクの管理」プロセスにおいて、いかなる同意手続が適正な「同意取得の在り方」であるか、言い換えるならば、事前の包括同意等の緩やかな同意手続を許容できるか否かの判断要素として用いられるものと解する。

イ　理由

上記結論は、参照文書における「リスク評価」のプロセスと「第三次取りまとめ」における事前の包括同意が許容される要件の関係を整理することによって導くことができると考える。

まず、参照文書において、「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、……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」という記述があることを踏まえると[119]、総務省は、利用者又は社会（以下「利用者等」という。）が得られる便益の検討と、③「リスクの特定・評価」プロセスで行われる「リスク」の評価（以下「狭義のリスク評価」という。）を分けて捉えていることがうかがえる。

また、上記記述の注釈で挙げられている「第三次とりまとめ」をみると、事前の包括同意を許容するための要件として、❶利用者が、ISP において通信の秘密を侵すことについて通常承諾すると想定し得るため、契約約款等による同意になじまないとはいえないこと、❷利用者に将来不測の不利益が生じるおそれがないことが挙げられていることが確認できる。なお、前記注釈では、前記要件❷の考慮要素が引用されている。

以上を踏まえると、「リスク評価」のプロセスと「第三次取りまとめ」における事前の包括同意が許容される要件の関係は、必ずしも断絶されたものではなく、「第三次取りまとめ」は、「狭義のリスク評価」に相当する内容を前記要件❷として掲げ、いかなる同意取得方法が適切であるかの判断に資するものとして前記要件❶を挙げたと解することができる。したがって、「第三次取りまとめ」では、将来不測の不利益が生じない「リスク」であることを前提として、当該「リスク」に関して通常の利用者が承諾することを想定できるのであれば、事前の包括同意が適正な「同意取得の在り方」として認められると解していると再整理できると考える。

そして、利用者等が得られる便益の内容・程度は、「通常承諾する」か否かの判断に大きく影響するものであることを踏まえると、「得られる利用者又は社会の便益」は、「狭義のリスク評価」ではなく、いかなる同意取得方法が適切であるかの判断（すなわち、④「対策の決定・リスクの管理」プロセス）において用いる

[119] 総務省・前掲注 47）８頁。

べきであるといえる[120]。

第４節　個別事例の検討

１．総説

本節では、本稿の目的の１つである「通信の秘密」不可侵規制に関する諸論点の再考の一環として、総務省が過去に「通信の秘密」に係る「有効な同意」に関する判断を示した事例等に対して「リスク評価」を試行する。

具体的には、主に通信内容が問題となる事例として、「迷惑メール等のフィルタリング（デフォルトオン）」、「CGM サイト運営者によるミニメールの内容確認（デフォルトオン）」及び「電子メール解析を通じた広告配信」を検討する。また、通信外形的事項が問題となる事例として、「発信者情報通知サービス」、「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」及び「ゼロレーティングサービスの提供」を検討する[121]。

２．主に通信内容が問題となる事例

（１）迷惑メール等のフィルタリング（デフォルトオン）

ア　評価対象となるサービス

迷惑メール等のフィルタリングは、電子メールサービスに付随するものであり、これを行う目的は、ユーザーの同意を得ず一方的に送信される迷惑メール等を他のメールと同様に受信しないようにすることにある。これにより、ユーザーは、執拗なセールスの電子メールを受信したり、本来の目的に沿った電子メールがこれに紛れて受信に支障をきたしたりすることを防ぐことができる[122]。また、迷惑メール等の減少は、ネットワークに対する負荷の軽減にも繋がるといえる。したがって、迷惑メール等のフィルタリングは、ユーザー及び社会に対し、それぞれ便益を与えるものであると考える。

なお、前述のとおり、本稿で検討の対象としている迷惑メール等のフィルタリ

---

[120] ただし、得られる便益が国家や社会に対するものでしかない場合、必ずしも利用者が通常承諾することが想定できるとはいえないため、当該事例における他の事情を踏まえ、これが認められるか慎重に検討していく必要があると考える。

[121] なお、本来「リスク評価」は、個別事例における具体的事実に則して行われるものであるところ、本試行では必ずしもこれができないことから実際の「リスク評価」よりも簡略化して行われている。

[122] 髙嶋・前掲注 23）800 頁参照。また、ユーザーの契約内容次第では、着信によって生じるパケット料金が着信者側に課金されることもあるので、迷惑の度合いが増加すると指摘している。

ングは、電気通信事業者が管理するウェブサーバー等において行うものであり、事前に設定したキーワードが受信した電子メールの本文中に含まれているか否かを検索し、キーワードが含まれている電子メールをブロック等する方法によって実施することを想定している。

イ　「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

まず、受信した電子メールの本文中に事前に設定したキーワードが含まれているか否かを確認することは、当該メールが迷惑メールであるか否かを判定するうえで必要不可欠なものであるといえる。したがって、「通信の秘密」に係る情報の取得・利用等の必要性は認められる。

他方、受信した電子メールの本文の取得・利用等に比例性が認められるか否かの判断は、個別の事例における具体的事実によるところが大きい。例えば、受信者が受信指定したメールアドレスから送られてくる電子メールの本文は取得・利用等しないようにする等、迷惑メール等による支障を回避するのに必要な限度で「通信の秘密」に係る情報を取得・利用等すべきであると解する。

ウ　「リスク」の特定・評価

迷惑メール等のフィルタリングを行うに当たっては「通信の秘密」の中核である通信内容に係る情報を取得・利用等することとなる。しかし、その手法は、前述のとおり、迷惑メール等による被害防止に資するキーワードが受信した電子メールの本文中に含まれているか否かを機械的に検索するものに過ぎない。したがって、ユーザーのプライバシー等に対する影響は、一般的には小さいと考える[123]。

また、一般に、迷惑メール等のフィルタリングサービスは、随時、任意に同意内容を変更することができ、同意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が多いことを踏まえると、迷惑メール等のフィルタリングのために取得した電子メールの内容が他の目的で利用されたり、これに対する安全

[123] なお、事前に設定したキーワードを機械的に検索するのではなく、AIによる判定がなされる場合であっても、迷惑メール等を機械によってフィルタリングする点で変わりないことから、基本的には同様の評価がなされるものと解する。また、迷惑メールでないメールが迷惑メールとして扱われた結果、当該メールを見逃すことによって業務等に支障が生じることが考えられるが、（サービスとして成立している以上、）誤ったフィルタリングが看過できないほどに頻繁に起きるわけではないことや、多くのサービスにおいて、迷惑メールとして分類されたメールは、直ちに削除されるわけではなく、迷惑メール用の受信箱を確認することで当該メールを閲覧できる余地があることを踏まえると、フィルタリングの誤りが生じ得ることは、通常、「リスク」の評価においては無視できるものであると考える。

管理措置が適切に講じられていなかったりする等の特段の事情がない限り、ユーザーに対して将来不測の不利益を与えるおそれは小さいと解する。

したがって、迷惑メール等のフィルタリングサービスに係る「リスク」は低いというべきである。

エ　対策の決定・リスクの管理

前述のユーザーが得られる便益の内容や「通信の秘密」に係る情報の取得・利用等の必要性を踏まえると、受信した電子メールに係る通信内容を、事業者が迷惑メール等に対して一定の措置を講じるうえで必要最小限の範囲で機械的に取得・利用等することについて、通常のユーザーであれば承諾することが想定できるといえる。

したがって、「リスク」が低いと評価されることを前提にしたとき、事前の包括同意が「有効な同意」と評価される余地があると解する。

オ　総務省判断との比較

前述のとおり、総務省は、迷惑メール等のフィルタリングサービスをデフォルトオンで提供するために５要件を設けているところ（第１節２（１）参照)、要件①、要件②、要件③及び要件⑤については、「狭義のリスク評価」で同様の内容が求められており、また、要件④については、いかなる同意取得方法が適切であるかの判断に当たって検討されているといえる。

したがって、総務省判断と本試行における判断過程及び結論は、それぞれ類似しているものと解する。

（２）CGM サイト運営者によるミニメールの内容確認（デフォルトオン）

ア　評価対象となるサービス

CGM サイト運営者によるミニメールの内容確認措置は、CGM サイトに会員登録したユーザー間でメッセージを交換するサービス（ミニメールサービス）に付随するものである。あらかじめ設定された一定のキーワードを含む内容を機械的に検知して発信を防止し、発信後は目視を含めた内容確認に基づき規約違反メッセージの削除等を行うというのが一般的であるとされる[124]。

ミニメールの内容確認措置の目的は、青少年ユーザーの保護である。ミニメールを通じた児童被害については、青少年ユーザーの未熟な判断力に起因するものが多いとされており、事前・事後の内容確認により被害防止につながることが期待されている。したがって、ミニメールの内容確認措置は、青少年ユーザー及び社会に対して便益を与えるものであるといえる。

[124] 総務省・前掲注 88）９頁。

イ　「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

まず、事前に設定したキーワードがミニメール中に含まれているか否かを確認することは、当該ミニメールが青少年ユーザーに有害であるか否かを判定するうえで必要不可欠であるといえる。また、発信後の目視による内容確認も、キーワード検索のみでは対処できない有害なミニメールを検知するために必要不可欠であるといえる。したがって、「通信の秘密」に係る情報の取得・利用等の必要性は認められる。

他方、ミニメールの内容確認措置に比例性が認められるか否かの判断は、個別の事例における具体的事実によるところが大きい。例えば、成年者であることが確認できているユーザー同士のミニメールの内容確認は行わない等、青少年ユーザーの保護に必要な限度で「通信の秘密」に係る情報を取得・利用等すべきであると解する。

ウ　「リスク」の特定・評価

まず、ミニメールの内容確認措置を講じるに当たっては、「通信の秘密」の中核である通信内容に係る情報を取得・利用等することとなる。

しかし、事前に設定した青少年ユーザーの保護に資するキーワードが受信したミニメールに含まれているか否かを機械的に検索する行為がユーザーのプライバシー等に対して与える影響は、一般的には小さいと考える。他方、発信後に通信内容を目視で確認する行為は、青少年ユーザー保護に関係するものであるか否かにかかわらず通信の意味内容を他人に知られてしまうという点で、機械的にキーワード検索を行う場合よりもプライバシー等に対して大きな影響を与えると考える。したがって、全体としてみたとき、ミニメールの内容確認措置は、ユーザーのプライバシー等に対して一定程度の影響を与えるというべきである。

もっとも、一般に、ミニメールの内容確認措置に対する同意の内容は、随時、任意に変更できるものであることを踏まえると[125]、当該フィルタリングのために取得したミニメールの内容が他の目的で利用されたり、これに対する安全管理措置が適切に講じられていなかったりする等の特段の事情がない限り、ユーザーに対して将来不測の不利益を与えるおそれは必ずしも大きくないと考える。

[125] 不同意とした場合に事実上ミニメールの利用が不可能となる点については、CGM 運営者に役務提供義務がないこと、青少年ユーザーを保護するための行為であり、不当な差別的取扱いではないことから、許容されるとする（総務省・前掲注 88）13 頁参照）。

したがって、機械的な検索を行うのみのフィルタリングと比較して小さいとまではいえないものの、ミニメールの内容確認措置に係る「リスク」は低いと評価される余地があると考える。

エ　対策の決定・リスクの管理

もっとも、前述のとおり、ミニメールの内容確認措置は、青少年ユーザー保護を目的とするものであり、青少年ユーザーや社会にとって便益は認められるものの、成人ユーザーにとって直接的な便益が認められない。そのため、CGM サイト運営者がミニメールの内容確認措置を講じることについて、ユーザーが通常承諾することが想定できるとまで直ちに認められないと解する。

よって、ミニメールの内容確認等の措置については、原則として「個別具体的かつ明確な同意」を取得することが求められるというべきである。

オ　総務省判断との比較

前述のとおり、総務省は、ミニメールの内容確認等の措置をデフォルトオンで実施するに当たって、５要件を設けているが、要件④については、「利用者の包括同意は推定されにくい」として、直ちにこれが認められるとは判断していない（第１節２（２）参照)。この点について、筆者は、前記エにおいて同様の指摘をしていることを踏まえると、総務省判断と本試行における判断過程及び結論は、それぞれ矛盾するものではないと考える。

（３）電子メール解析を通じた広告配信

ア　評価対象となるサービス

電子メール解析を通じた広告配信は、ユーザーの興味関心に合致する効果的な広告配信を目的とした電子メールサービスに付随するものである。電子メールサービスを提供する事業者がユーザーの閲覧したメール（件名及び本文）を、当該事業者のウェブサーバーにおいて機械的に解析し、その結果をもとに当該ユーザーの関心と関連性の高い広告を配信する等の方法がある。

イ　「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

まず、電子メールの件名及び本文を取得したうえでこれを解析することは、ユーザーの興味関心に合致する効果的な広告配信に資するものであると思われる。もっとも、ユーザーの興味関心を把握する方法は、必ずしもメールの本文等の解析によらないと不可能というわけではないから、「通信の秘密」に係る情報の取得・利用等が必要不可欠であるとまではいえない。

また、広告配信のための電子メールの解析に比例性が認められるか否かの判断

には、個別の事例における具体的事実によるところが大きいが、利用者の興味関心に合致する広告を配信するのに必要な限度を超える情報が取得・利用等されるおそれがあるので留意する必要があると解する。

ウ　「リスク」の特定・評価

電子メール解析を通じた広告配信を行うに当たっては、「通信の秘密」の中核である通信内容に係る情報を取得・利用等することとなる。そして、一般に、電子メールでやり取りされる内容には機微性の高い情報が含まれる可能性があることから、ユーザーのプライバシー等に影響を与えることが考えられる。

この点、電子メールの解析が機械的に行われる場合、迷惑メール等のフィルタリングと同様に、ユーザーに与えるプライバシー等への影響は小さいようにも思える。しかし、迷惑メール等のフィルタリングは、迷惑メールであると推認させるキーワードが存在するか否か検索するだけであるのに対し、本件における電子メールの解析は、広告配信に資する様々な情報を収集するものであり、しかも、得られた情報からユーザーの興味関心という私事性の高い情報を獲得しようとするものであり、利用の対象となる情報の量や質が大きく異なる。さらに、多くの場合、電子メールの件名や本文がどのようなロジックで、いかなる広告枠において、いかなる広告主の広告配信に用いられ得るのか等について、ユーザーに対する事前の十分な説明がなされないことが考えられる。

以上を総合すると、電子メールの解析を通じた広告配信がユーザーのプライバシー等に与える影響は大きいというべきである。なお、当該電子メールサービスのもとで送受信されるすべての電子メールが「通信の秘密」に係る情報の取得・利用等の対象となることが想定されるから、ユーザーのプライバシー等に対して影響を与える事象の「発生可能性」は高いといえる。

したがって、電子メール解析を通じた広告配信は、ユーザーに対して将来不測の損害を与えるおそれが大きく、「リスク」は高いというべきである。

エ　対策の決定・リスクの管理

電子メール解析を通じた広告配信は、前述のとおり「リスク」が高いため、事前の包括同意の内容に当該「リスク」によって生じ得るユーザーに対するすべての影響に関する承諾が真意に基づいて存在しているとは評価し難い。したがって、事前の包括同意によって取得した同意は、「有効な同意」であるといえないと考える[126]。

[126] なお、本件のような広告配信が付随する電子メールサービスが一般的に無料であることに鑑みれば、広告配信を受けることについて、ユーザーが通常承諾することが想定できる余地がないわけではない。もっとも、それは、電子メールの件名や本文の解析についてま

よって、電子メール解析を通じた広告配信を行うに当たっては、「通信の秘密」に係る情報を取得・利用等することについて、「個別具体的かつ明確な同意」が必要であると解する。

オ　総務省判断との比較

総務省は、電子メール解析を通じた広告配信に関して４つの事項を挙げているが[127]、これは「個別具体的かつ明確な同意」の存在が認められる場合を示したものであると解する。したがって、本試行の結果は、総務省の判断と矛盾するものではないと考える。

３．通信の構成要素が問題となる事例

（１）発信者情報通知サービス

ア　評価対象となるサービス

電話サービスに付随する発信者情報通知サービスは、商業目的の電話セールスや意図的な嫌がらせ電話の対策として、1994 年８月に NTT が提供開始した「迷惑電話おことわりサービス」をさらに一歩進めたものであり、1997 年 10 月に NTT が一部地域で提供開始したものである。同サービスは、発信者が発信電話番号を通知する設定で発信した場合に、電気通信事業者が発信電話番号を取得し、着信者の端末にこれを送出するものである。

これにより、着信者は、発信者が誰であるかを知り、これに応答するか拒否するかの選択ができるようになった[128]。これを発信者側からみると、着信者に迷惑電話等と勘違いされずに応答してもらえる便益があるといえる。

イ　「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

まず、発信電話番号を受信者に伝達するために電気通信事業者が発信電話番号を取得・利用等することは、必要不可欠なものであるといえる。

また、発信電話番号の取得・利用等は、あくまでも着信者に発信電話番号を伝える限度で行っているものに過ぎないため、比例性が認められるものと解する。

ウ　「リスク」の特定・評価

発信電話番号の通知を行うに当たっては、通信内容の取得・利用等は行われず、機械的に取得した発信電話番号を通信の相手方当事者に通知するのみであ

で承諾していることを意味するわけではない。

[127] 総務省「ヤフー株式会社における新広告サービスについて」＜https://www.soumu.go.jp/menu_kyotsuu/important/kinkyu02_000122.html＞（2012 年）。

[128] 以上について、髙嶋・前掲注 23）787 頁。

る。また、発信電話番号の通知を望まない者は、随時、任意にこれを行われないよう設定することができ、通知の設定の有無によって他の提供条件が変わるわけではない。以上より、発信者情報通知サービスが発信者のプライバシー等に与える影響は小さいと考える。

以上を前提にすると、受信者に発信電話番号を通知するために取得した発信電話番号が他の目的で利用されたり、安全管理措置が適切に講じられていなかったりする等の特段の事情がない限り、発信者に対して将来不測の不利益を与えるおそれは小さく、発信者情報通知サービスにおける「リスク」は低いと解する。

エ　対策の決定・リスクの管理

前述の発信者が得られる便益を踏まえると、発信者情報通知サービス提供のために事業者が発信電話番号を機械的に取得・利用等するについて、発信者が通常承諾することを想定できるといえる。

したがって、発信電話番号通知サービスについては、事前の包括同意による同意取得であっても「有効な同意」と評価されると解する。

オ　総務省判断との比較

前述のとおり、総務省は、「発信者が発信者情報の通知を阻止しない場合には、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から、通信の秘密侵害には当たらないこととなる」とするにとどまり[129]、「有効な同意」の問題と位置付けているかについては、必ずしも明らかにされていない。

もっとも、本試行では、発信者情報通知サービスによる発信電話番号の通知が適法であると解しているため、少なくとも結論において総務省判断と矛盾していないものと解する。

（2）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

ア　評価対象となるサービス

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は、サイバー攻撃に対処することを目的としている。具体的な方法としては、ISP がマルウェアに感染している可能性が高い端末を認識した場合、送信元 IP アドレス、ポート番号及びタイムスタンプと当該 IP アドレス及びポート番号の割当て状況を確認して当該端末のユーザーを割り出し、電子メールの送付等の方法で個別に注意喚起を行うことが考えられる。これにより、C&C サーバー等との通信によっ

[129] 総務省・前掲注 48）112 頁。

て生じるユーザーの被害を未然に防止するとともに、ISP の電気通信役務の提供に関する支障を未然に防止することが期待できるとされている[130]。

したがって、当該注意喚起は、ユーザー及び社会に対して便益を与えるものであるといえる。

イ　「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

まず、送信元 IP アドレス、ポート番号及びタイムスタンプを取得・利用等することは、対象となる端末のユーザーを割り出す方法が他に想定し難いことから、前記注意喚起のために必要不可欠なものであるといえる。

また、送信元 IP アドレス、ポート番号及びタイムスタンプを取得したうえで、当該 IP アドレス及びポート番号の割当て状況を確認して当該端末のユーザーを割り出す行為に比例性が認められるか否かの判断は、個別の事例における具体的事実によるところが大きいところ、前記注意喚起に必要な限度で「通信の秘密」に係る情報を取得・利用等すべきであると解する。

ウ　「リスク」の特定・評価

前述の注意喚起を行うに当たっては、通信内容の取得・利用等は行われるわけではなく、あくまでも送信元 IP アドレス、ポート番号及びタイムスタンプの取得・利用等が機械的になされるのみである。また、当該注意喚起を望まない者は、自ら予めこれを行われないよう設定することができ、設定の有無にかかわらず、インターネットによる通信をすることができるのであれば、当該注意喚起によるユーザーのプライバシー等に対する影響は小さいと考える。

以上を前提にすると、マルウェアに感染した可能性が高い端末のユーザーに注意喚起するために取得した送信元 IP アドレス、ポート番号及びタイムスタンプを他の目的で利用したり、安全管理措置が適切に講じられていなかったりする等の特段の事情がない限り、ユーザーに対して将来不測の不利益を与えるおそれは小さく、当該注意喚起の「リスク」は低いといえる。

エ　対策の決定・リスクの管理

前述のユーザーが得られる便益を踏まえると、事業者が送信元 IP アドレス、ポート番号及びタイムスタンプを、マルウェアに感染した可能性が高い端末のユーザーに注意喚起するうえで必要最小限の範囲で機械的に取得・利用等することについて、通常のユーザーであれば承諾することが想定できるといえる。

したがって、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は、「リスク」が低いと評価されることを前提に、事前の包括同

[130] 総務省・前掲注 94）４頁参照。

意による同意取得であっても適正な「同意取得の在り方」による「有効な同意」と評価できると解する[131]。

オ　総務省判断との比較

前述のとおり、総務省は、当該注意喚起を事前の包括同意を得ることで実施できるための２要件を設けているところ（第１節２（３）参照)、要件②については、「狭義のリスク評価」で同様の内容が求められ、また、要件①については、いかなる同意取得方法が適切であるかの判断の際に検討されているといえる。したがって、本試行は、判断過程・結論ともに総務省判断と類似していると考える（なお、第３節３参照)。

（３）ゼロレーティングサービスの提供

ア　評価対象となるサービス

ゼロレーティングサービスとは、従量料金制又は上限データ通信量を定めた定額料金制の下で、特定のコンテンツ・アプリケーション・プラットフォーム（以下「コンテンツ等」という。）を利用した場合に限り、料金請求に係る使用データ通信量にカウントしない（または割り引いてカウントする）データ通信サービスである[132]。

イ　「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

まず、電気通信事業者が消費者に対してゼロレーティングサービスを提供するに当たっては、ゼロレーティング対象コンテンツ等に係るデータ通信かどうかを識別すること等が必要である[133]。そのため、通信の外形的事項であるアクセス先URL情報を取得・利用等しなければならないので、「通信の秘密」に係る情報の取得・利用等の必要性は認められる。

また、その比例性の判断に関しては、個別の事例における具体的事実によるところが大きいが、前記識別のために必要な範囲（量・質・期間）で「通信の秘密」に係る情報の取得・利用等が行われることが求められるものと解する。

---

[131] ISPが「通信の秘密」を取得・利用等してユーザーに対して注意喚起するという点ではアクセス警告方式も類似する手法ではあるものの、2019年に実施されたアンケート調査結果を踏まえると、少なくとも当時において、一般的・類型的に見て、通常のユーザーであればISPが「通信の秘密」を侵すことについて承諾すると想定し得えないため、契約約款等による事前の包括同意では「有効な同意」に当たるとはいえないこととなる（総務省・前掲注95）12頁)。

[132] 総務省「ゼロレーティングサービスの提供に係る電気通信事業法の適用に関するガイドライン」＜https://www.soumu.go.jp/main_content/000678277.pdf＞（2020年）５頁。

[133] 総務省・前掲注132）15頁。

ウ　「リスク」の特定・評価

ゼロレーティングサービスの提供を行うに当たっては、通信内容の取得・利用等は行われるわけではなく、あくまでもアクセス先URL情報の取得・利用等が機械的になされるのみである。それゆえ、ユーザーのプライバシー等に対する影響は大きいものではないとも思える。しかし、アクセス先URL情報がわかれば、通信内容（閲覧情報）を推測することは容易であること、閲覧情報には機微性の高いものが含まれる可能性があること、一部のゼロレーティング対象コンテンツ等に係るデータ通信か否かを識別するためにすべての通信におけるアクセス先URL情報が取得・利用等する必要があること等を踏まえると、ユーザーのプライバシー等に対する影響は大きいというべきである。

また、ユーザーが当該情報の取得・利用等がなされることを回避したいときに、単なる設定の切り替えでこれを実現することができず、他の料金プランへの変更を要するのであれば、必ずしも「通信の秘密」に係る情報の取得・利用等に対する同意を随時任意に変更できるとはいえない。

以上より、ゼロレーティングサービスの提供は、将来不測の不利益が生じるおそれが大きく、「リスク」は高いというべきである。

エ　対策の決定・リスクの管理

ゼロレーティングサービスの提供は、前述のとおり「リスク」が高いため、事前の包括同意の存在をもって当該「リスク」により生じ得るユーザーに対するすべての影響について、真意に基づく同意があるとは評価し難い。したがって、事前の包括同意によって取得した同意は、「有効な同意」であるといえないと考える。

よって、ゼロレーティングサービスの提供を行うに当たっては、「通信の秘密」に係る情報を取得・利用等することについて、「個別具体的かつ明確な同意」が必要であると解する。

オ　総務省判断との比較

総務省は、ゼロレーティングサービス利用者について、対象コンテンツ等に係るデータ通信を使用データ通信量にカウントしないために、「通信の秘密」に当たる情報を利用することについて、「個別具体的かつ明確な同意」を要すると判断している。

したがって、総務省判断と本試行における結論に矛盾はないものと考える。

第５節　Cookie 事例における「有効な同意」

１．総説

最後に第２部のまとめとして、Cookie の利活用事例について検討する。第１部では、Cookie が「通信の秘密」に該当し、これを利活用する行為が「通信の秘密」の侵害に当たり得ると解しているところ、本節では、Cookie の利活用を適法化するためにはいかなる方法によって同意を取得すれば、「有効な同意」となるか、２つの事例について検討する[134]。

２．サービス提供等に必須の Cookie 利活用

（１）評価対象となるサービス

サービス提供等に必須の Cookie（以下「必須 Cookie」という。）の利活用の例としては、会員制のウェブサイトにおいてログイン状態を維持したり、オンラインショッピングサイトにおいて買い物かごに商品を保持したりすること等が挙げられる。

必須 Cookie の利活用は、ユーザーが期待するウェブページの表示等（前述の例でいうと、ログイン状態を前提にした画面表示をしたり、買い物かごに選択した商品が入った状態で別のページに変遷したりすること）を目的としており、コンテンツ事業者サーバーがファーストパーティ Cookie（必須 Cookie）を発行すること等でこれを実現させる。当該目的を達成できないことは、利活用の対象となるウェブページを正常に閲覧等することができないことを意味するから、必須 Cookie の利活用によりユーザーが得られる便益は大きいといえる。

（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

まず、HTTP がステートレスな通信を行う性質を有することに鑑みれば、この性質から生じる不都合を解消するために行う「通信の秘密」に係る情報の取得・利用等の必要性は認められる。

また、必須 Cookie の利活用による「通信の秘密」に係る情報の取得・利用等に比例性が認められるか否かの判断は、個別の事例における具体的事実によるところが大きいが、前記目的の達成に必要な限度であることが求められると解する。

---

[134] なお、第４節と同様、本来「リスク評価」は、個別事例における具体的事実に則して行われるものであるところ、本試行では必ずしもこれができないことから実際の「リスク評価」よりも簡略化して行われている。また、各事業者において用いられている Cookie の名称それ自体は、「リスク評価」や「有効な同意」の判断を直接左右するものではなく、その目的や利用方法等を具体的に分析していく必要があると解する。

（3）「リスク」の特定・評価

ログイン状態を前提にした画面表示をしたり、買い物かごに選択した商品が入った状態で別のページに変遷したりする等、ユーザーが期待するウェブページを表示するうえで「通信の秘密」に係る情報を機械的に取得・利用等することは、ユーザーの表現を萎縮させたり、著しくプライバシーを害したり、通信に対する信頼を損ねたりするものではない。したがって、ユーザーに対する「影響度」は小さいといえる。ゆえに、安全管理措置が適切に講じられていない等の特段の事情がない限り、ユーザーに対して将来不測の不利益を与えるおそれは小さく[135]、「リスク」は低いと評価できると解する。

（4）対策の決定・リスクの管理

前述のとおり、必須 Cookie の利活用がなければ、利活用の対象となるウェブページを正常に閲覧等することができないことを意味するから、その限度で必須 Cookie を利活用することについて、通常のユーザーであれば承諾することが想定できるといえる。

よって、必須 Cookie の利活用については、事前の包括同意による同意取得であったとしても、「有効な同意」であると評価できると解する。

3．広告配信のための Cookie 利活用

（1）評価対象となるサービス

広告配信のための Cookie（以下「ターゲティング Cookie」という。）の利活用の例としては、以前ウェブサイトにアクセスしたことのあるユーザーを追跡して広告を配信したり、ユーザーのウェブ閲覧履歴をもとに分析した当該ユーザーの興味・関心に合致する広告を配信したりすること等が挙げられる。ターゲティング Cookie 利活用の目的は効果的な広告を配信することにあり、広告配信事業者サーバーがサードパーティ Cookie（ターゲティング Cookie）を発行する等してこれを行うことが考えられる。

（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

まず、効果的な広告配信のために「通信の秘密」に係る情報を取得・利用等することについては、ユーザーの興味関心を把握するために一定程度の必要性は認

[135] なお、必須 Cookie の利活用に係る同意の内容を事後に撤回することは、対象のウェブページを適切に表示できなくすることを意味する。しかし、必須 Cookie の利活用が当該ウェブページを適切に表示させることと技術的に表裏一体の関係にある以上、このような結果となることはやむを得ないことであり、将来の不測の不利益には当たらないものと解する。

められる。もっとも、ユーザーの興味関心を把握することは、必ずしもターゲティング Cookie の利活用によらないと不可能というわけではないから、「通信の秘密」に係る情報の取得・利用等が必要不可欠であるとまではいえない。

また、ターゲティング Cookie の利活用による「通信の秘密」に係る情報の取得・利用等に比例性が認められるか否かの判断は、個別の事例における具体的事実によるところが大きいが、利用者の興味関心に合致する広告を配信するのに必要な範囲（量・質・期間）を超える情報が取得・利用等されるおそれがあり、留意する必要があるものと解する。

（3）「リスク」の特定・評価

効果的な広告配信のためにユーザーのインターネット上の行動履歴に関する情報を取得・利用等することは、ユーザーに関する機微な情報を把握し得るものであり、また、取得・利用等される情報量は膨大なものになることが推測される。したがって、ユーザーのプライバシー等に対して与える影響は大きいと考える。

また、広告配信事業者サーバーが配信するサードパーティ Cookie は、複数のウェブサイトを横断して利用されることが想定でき、その活用方法次第で広告配信事業者は、複数のドメインに対するユーザーのアクセス情報を取得できることとなる。そのため、ユーザーが自らアクセスしたことのないウェブサーバーに、ユーザーの行動履歴に関する情報が広く収集されるおそれがあるといえる。

したがって、ターゲティング Cookie の利活用は、ユーザーに対して将来不測の不利益を与えるおそれが大きく、「リスク」が高いというべきである。

（4）対策の決定・リスクの管理

ターゲティング Cookie の利活用は、前述のとおり「リスク」が高いため、事前の包括同意の存在をもって当該「リスク」により生じ得るユーザーに対するすべての影響について、真意に基づく同意があるとは評価し難い。したがって、事前の包括同意によって取得した同意は、「有効な同意」であるといえないと考える。

よって、ターゲティング Cookie の利活用に当たっては、「個別具体的かつ明確な同意」を取得する必要があるものと解する[136]。

---

[136] 同一のターゲティング Cookie を複数のウェブサイト（例：ウェブサイト A、ウェブサイト B）利活用する場合、通常、ユーザーは、どのウェブサイトで当該ターゲティング Cookie が利活用されているか認識していないため、ウェッブサイト A を閲覧する際に取得した「有効な同意」は、ウェブサイト B の閲覧に係る「通信の秘密」侵害を対象にしていないと解するべきである。したがって、同意取得は、通常、それぞれのウェブサイト（前記事例においては、ウェブサイト A 及びウェブサイト B）で個別に取得する必要があると考える。

おわりに

１．本稿のまとめ

本稿では、「はじめに」で示した①Cookie の利活用と「通信の秘密」の関係を明らかにしつつ、②「通信の秘密」不可侵規制に関する諸論点について検討した。

（１）Cookie と「通信の秘密」の侵害（第１部）

ア　「通信の秘密」該当性

（ア）「通信の秘密」の範囲

まず、Cookie が電気通信事業法の「通信の秘密」に当たるか否か判断する前提として、「通信の秘密」の範囲について検討した。

筆者は、「通信の秘密」不可侵規制の趣旨を、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であると解したうえで、「通信の秘密」の範囲には、通信内容のみならず、通信の外形的事項が含まれると解した。また、「通信の秘密」不可侵規制の趣旨が上記３点にあると解することによって、法人に「通信の秘密」が認められることや、実務上「通信の秘密」該当性判断に当たって、逐一「表現」該当性等を検討されていないことを整合的に説明できることを確認した。

（イ）「通信の秘密」に該当するために求められる個々の通信との関係

つぎに、通信内容又は通信の外形的事項に該当するために求められる個々の通信との関係について検討した。

筆者は、「個々の通信に密接に関係する」と評価できる情報であればこれに該当するとしたうえで、「密接に関係する」か否かの判断は、「通信の秘密」不可侵規制の趣旨に照らして行うべきとした。

そして、Cookie が Cookie 送信通信及び記録対象通信いずれに対しても「密接に関係する」といえることを確認し、「通信の秘密」に該当し得るとした。

（ウ）「秘密」性を個別評価することの可否

また、「通信の秘密」に該当し得る情報に関して、個別事例における取得・利用等の目的や取得主体等の事情に応じて、「秘密」性の有無の評価が左右され得るか検討した。

この点、筆者は、「通信の秘密」に該当し得る情報であれば、取得・利用等の目的や取得主体にかかわらず、原則として「相当の利益」があるといえ、「秘密」性が認められるものと解した。もっとも、公然性を有する通信において伝送される通信内容等に係る情報は、「相当の利益」が認められないことから、例外的

に「秘密」性は否定されると解した。

（エ）Cookie の「通信の秘密」該当性

以上の検討を通じて、筆者は、Cookie が「通信の秘密」に該当すると判断した。

イ　「通信の秘密」に対する侵害の有無

（ア）自動的処理による侵害可能性/通信の相手方当事者による侵害可能性

まず、Cookie の利活用の場合のように、「通信の秘密」に係る情報の取得・利用等が自動的処理によって行われる場合があるところ、このような場合でも「通信の秘密」の侵害となり得るか検討した。

この点、筆者は、「通信の秘密」の共有範囲の外にいる者がこれを知り得る状態になるのであれば、自動的処理であっても「通信の秘密」の侵害は生じ得ると解した。

また、ファーストパーティ Cookie の利活用の場合のように、通信の相手方当事者が「通信の秘密」に係る情報を取得・利用等する場合があるところ、このような場合でも「通信の秘密」侵害となり得るか検討した。

この点、筆者は、通信の一方当事者のみにとどまる「通信の秘密」については、相手方当事者による知得が起こり得ると解した。また、「通信の秘密」不可侵規制の趣旨に鑑みて、相手方当事者による窃用及び漏えいも起こり得ると解した。

（イ）Cookie の利活用による「通信の秘密」侵害の有無

以上の検討を前提に、筆者は、Cookie の利活用は「通信の秘密」の侵害となり得ると判断した。

（２）「有効な同意」に関する「同意取得の在り方」（第２部）

ア　「有効な同意」の意義

「有効な同意」に関する「同意取得の在り方」を検討するに先立って、筆者は、「有効な同意」が「通信の秘密」の侵害に係る違法性を阻却するものであると解した。

イ　「有効な同意」に関する従前の整理及びこれに対する説明

まず、「有効な同意」に関して、総務省は、従前、原則として「個別具体的かつ明確な同意」であることが必要であるとし、そのうえで、一部の事例については、契約約款への合意等による事前の包括同意が例外的に「有効な同意」として認められ得るとしてきたことを確認した。

そのうえで、近年、総務省が「個別具体的」な同意か、「明確」な同意か、とい

う２つの要素が「有効な同意」の必要十分条件ではなく、「有効な同意」の有無は個別事例における「リスク」に比例して変わり得る等の見解を明らかにしたことを確認した。

ウ　「リスク評価」について

まず、筆者は、個情委資料を参照しつつ、「リスク評価」における「リスク」は、「影響度」と「発生可能性」の組み合わせとして評価できるとした。また、筆者は、「リスク評価」の実施に当たって、事業者において評価基準等の設定を適切に行う必要があることを指摘した。さらに、「通信の秘密」に係る情報の取得・利用等によって「得られる利用者又は社会の便益」は、「リスク」が一定の範囲内であることを前提に、いかなる同意取得方法が適切であるか検討する際に考慮すべき事項であるとした。

そして、総務省が「有効な同意」に関する判断を示した事例等に「リスク評価」を試行し、「有効な同意」を得るための適正な「同意取得の在り方」を検討した。

エ　Cookie 事例における「有効な同意」

最後に、Cookie 事例について、「通信の秘密」不可侵規制との関係で適法となる「有効な同意」を得るための「同意取得の在り方」を、「リスク評価」を用いて検討した。

この点、筆者は、必須 Cookie の利活用については、ユーザーの事前の包括同意が適正な「同意取得の在り方」となり得、それによって得られた同意は「有効な同意」となるとした。他方で、筆者は、ターゲティング Cookie の利活用については、「個別具体的かつ明確な同意」を要すると判断した。

２．残された課題等

本稿では、「リスク評価」を経て導かれる適正な「同意取得の在り方」のうち、事前の包括同意に焦点を当てて検討を行った。もっとも、「同意取得の在り方」は、これに限られるものではなく、本来であれば、いかなる場合に黙示の同意が適正な「同意取得の在り方」となるかについても明らかにできることが望ましいと考える。しかし、2022 年１月現在において、総務省が黙示の同意を「通信の秘密」に関する適正な「同意取得の在り方」として明示的に認めた事例がないことや、この点に関する議論が特段見当たらないことから、本稿ではこれを論じることはせず、残された課題とした。

また、本稿は、Cookie の利活用と「通信の秘密」不可侵規制との関係について論じたものであり、他の規制等は検討の対象外となっている。したがって、Cookie の利活用に当たっては、個人情報保護法による規制、プライバシー保護、レピュテーションリスク等について、別途検討する必要があると考える。

さらに、本稿は、Cookie 事例を対象に論じたものであり、広告識別子等の他のデータ利活用と「通信の秘密」不可侵規制との関係について、本稿の検討結果がそのまま妥当するかについては、別途検討する必要があると考える。