別紙２

ICT サービスの利用を巡る諸問題に対する利用環境整備に関する報告書

令和７年９月 10 日

ICT サービスの利用環境の整備に関する研究会

不適正利用対策に関するワーキンググループ
通信ログ保存の在り方に関するワーキンググループ
利用者情報に関するワーキンググループ

ICT サービスの利用を巡る諸問題に対する利用環境整備に関する報告書

はじめに

ICT サービスの拡大とともに、サービス利用に関する諸課題も多様化していることを背景に、令和６年２月６日に設置された ICT サービスの利用環境の整備に関する研究会は、利用者情報の不適切な取扱い、不適正利用への対処、各種違法・有害情報への対策等の様々な課題を検討してきました。

ICT サービスを巡る利用環境は、日々刻々と変わっており、不適正利用への対策、利用者情報の取扱いについて、様々な価値のバランスを適切に図りながら、利用者視点で更なる検討が必要となっていることを、改めて痛感しております。

一つ目に、電気通信の不適正利用へのより一層の対策が求められています。令和６年における財産犯の被害額は 4,000 億円を超えており、その大部分は詐欺による被害となっています。こうした被害への対策として、「国民を詐欺から守るための総合対策 2.0」（令和７年４月 22 日犯罪対策閣僚会議決定）が策定され、通信関連施策として、国際電話を悪用した詐欺電話への対策や通信履歴の保存の在り方の検討等が求められています。電気通信の不適正利用対策は、公共インフラとしての通信サービスへの信頼を高めるものである一方で、個々の利用者の権利保護等とのバランスを確保する必要があるため、課題ごとに適時適切に解決を図っていく必要があります。そのため、本検討会において、その時々の状況を具体的に把握し、個別に丁寧な検討を重ねることは、非常に有用なことだと思っています。

二つ目に、利用者情報の取扱いについて、プライバシーやセキュリティの一層の確保が求められています。スマートフォンにおいて利用される特定ソフトウェアに係る競争の促進に関する法律の施行を令和７年 12 月に控える中で、スマートフォンアプリにおける競争の促進への期待が高まっています。そのような中でも、関係事業者において、スマートフォン上のプライバシー、セキュリティ、そして青少年の保護についても、引き続きしっかりと確保されることが強く求められています。今回、令和６年 11 月に公表された「スマートフォン　プライバシー　セキュリティ　イニシアティブ（SPSI）」が改定され、新たに青少年保護を対象に加えるとともに、関係事業者のわかりやすさの観点から、対応が求められる度合いに応じて整理されたことは、誠に時機を得たものだと考えております。

今回の報告書の検討過程では、不適正利用対策、通信ログ保存の在り方、利用者情報の在り方に関して、様々な関係事業者から意見を聴きつつ、３つのワーキンググループで集中的に議論を行いました。本報告書は、ICT サービスを巡る利用環境を踏まえて、それぞれの課題についてどのような方向に進めていくべきか、それぞれの論点について本検討会としての一定の考え方を示すとともに、今後の方向性や在り方などについて幅広く提言を行うものであり、官民の関係者における今後のさらなる取組の一助となることを期待しております。

令和７年７月

ICT サービスの利用環境の整備に関する研究会

座長　東京大学大学院法学政治学研究科教授　宍戸常寿

不適正利用対策に関するワーキンググループ

第１部　検討の背景

第１章　不適正利用対策をめぐる環境変化

１　これまでの検討

ICT サービスの利用環境が変化する中、電気通信の不適正利用対策について、新たな対策が求められている。

不適正利用対策に関するワーキンググループは、令和６年２月６日、ICT サービスの利用環境の整備に関する研究会の下に設置された。本ワーキンググループは、親会の中で不適正利用への対処に関する検討を実施し、令和６年２月から６月で、計６回、SMS による不適正利用対策、携帯電話不正利用防止法[1]に基づく本人確認方法等の見直しについて議論した[2]。その後、これまでのワーキンググループでの議論の結果を、令和６年 11 月 29 日、親会にて、不適正利用対策に関するワーキンググループ報告書をとりまとめている[3]。

２　環境変化

（１）いわゆる「闇バイト」犯罪

昨年のワーキンググループ報告書公表後の新たな不適正利用対策を巡る環境変化の一つとして、いわゆる「闇バイト」に係る犯罪の増加がある。「闇バイト」とは、SNS やインターネット掲示板などで、短時間で高収入が得られるなど甘い言葉で募集し、応募してしまうと、詐欺の受け子や出し子、強盗の実行犯など、犯罪組織の手先として利用され犯罪者となってしまうような犯罪実行者募集を指す[4]。令和６年８月以降に発生した一連の強

---

[1] 携帯音声通信事業者による契約者等の本人確認等及び携帯音声通信役務の不正な利用の防止に関する法律（平成 17 年法律第 31 号）

[2] 総務省, ICT サービスの利用環境の整備に関する研究会, 令和 7 年 6 月 11 日アクセス, https://www.soumu.go.jp/main_sosiki/kenkyu/ICT_services/index.html

[3] 総務省, 利用者情報に関するワーキンググループ報告書（案）及び 不適正利用対策に関するワーキンググループ報告書（案）についての意見募集の結果の公表, https://www.soumu.go.jp/menu_news/s-news/01kiban18_01000240.html

[4] 警視庁, ＃BAN　闇バイト, https://www.keishicho.metro.tokyo.lg.jp/kurashi/drug/yami_arbeit/ban_yamiarbeit.html

盗等事件についても、こうしたいわゆる「闇バイト」の募集に応じた者が実行犯として使われていたことが確認されている[5]。この闇バイトの一環で電気通信が悪用されることがあり、携帯電話の不正 SIM 転売や SNS の闇バイトの募集などがある。

こうした事件を受けて、政府は、同年 12 月、「いわゆる「闇バイト」による強盗事件等から国民の生命・財産を守るための緊急対策」（令和６年 12 月 17 日犯罪対策閣僚会議決定）を策定し、対策を進めている[6]。警察庁によれば、令和７年５月 16 日時点においては、上述の一連の強盗事件と同様の事件は現状では確認されていない状況である。

（２）特殊詐欺

加えて、その他の新たな不適正利用対策を巡る環境変化として、特殊詐欺の被害の増加もある。令和６年の特殊詐欺の認知件数・被害額は、ともに過去最悪となり、認知件数は 2 万 987 件、被害額は 721.5 億円となった。また、令和７年に入っても、前年の同時期と比較すると、認知件数は 1.5 倍以上、被害額は３倍以上と、極めて深刻な状況である[7]。

---

[5] 総務省，不適正利用対策に関するワーキンググループ(資料８－２)「特殊詐欺の被害状況と通信技術の悪用実態」（警察庁），
https://www.soumu.go.jp/main_content/001008464.pdf

[6] 首相官邸，いわゆる「闇バイト」による強盗事件等から国民の生命・財産を守るための緊急対策，https://www.kantei.go.jp/jp/singi/hanzai/kettei/241217/kinkyu_taisaku.pdf

[7] 総務省，不適正利用対策に関するワーキンググループ(資料８－２)「特殊詐欺の被害状況と通信技術の悪用実態」（警察庁），
https://www.soumu.go.jp/main_content/001008464.pdf

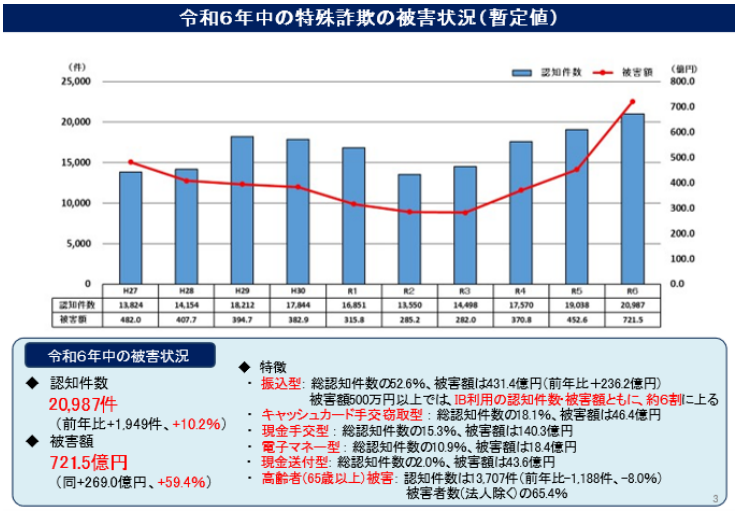
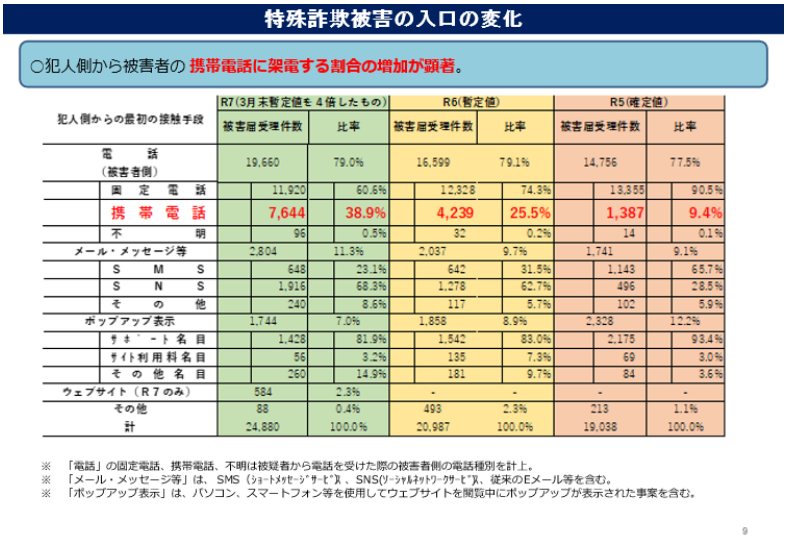


図１　令和６年中の特殊詐欺の被害状況（暫定値）[8]

このような特殊詐欺において、犯行グループからの被害者への接触手段は、電話が約８割、メール・メッセージ等、ポップアップ表示もそれぞれ１割程度となっている[9]。このうち、８割を占める電話の中の、７割強が固定電話であり、３割弱が携帯電話であることが判明している。

[8] 総務省，不適正利用対策に関するワーキンググループ(資料８－２)「特殊詐欺の被害状況と通信技術の悪用実態」（警察庁），
https://www.soumu.go.jp/main_content/001008464.pdf

[9] 総務省，不適正利用対策に関するワーキンググループ(資料８－２)「特殊詐欺の被害状況と通信技術の悪用実態」（警察庁），
https://www.soumu.go.jp/main_content/001008464.pdf



特殊詐欺被害の入口の変化

○犯人側から被害者の携帯電話に架電する割合の増加が顕著。

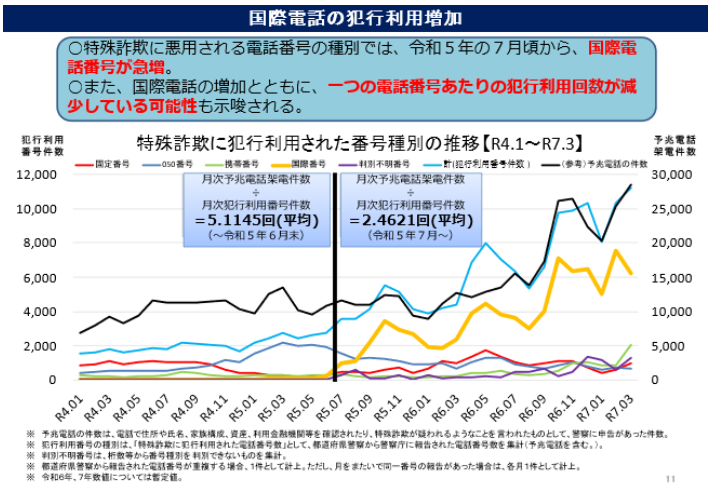
犯人側からの最初の接触手段		R7(3月末暫定値も４倍したもの) 被害届受理件数	R7(3月末暫定値も４倍したもの) 比率	R6(暫定値) 被害届受理件数	R6(暫定値) 比率	R5(確定値) 被害届受理件数	R5(確定値) 比率
電話（被害者側）		19,660	79.0%	16,599	79.1%	14,756	77.5%
	固定電話	11,920	60.6%	12,328	74.3%	13,355	90.5%
	携帯電話	7,644	38.9%	4,239	25.5%	1,387	9.4%
	不明	96	0.5%	32	0.2%	14	0.1%
メール・メッセージ等		2,804	11.3%	2,037	9.7%	1,741	9.1%
	SMS	648	23.1%	642	31.5%	1,143	65.7%
	SNS	1,916	68.3%	1,278	62.7%	496	28.5%
	その他	240	8.6%	117	5.7%	102	5.9%
ポップアップ表示		1,744	7.0%	1,858	8.9%	2,328	12.2%
	サイト名目	1,428	81.9%	1,542	83.0%	2,175	93.4%
	サイト利用料名目	56	3.2%	135	7.3%	69	3.0%
	その他名目	260	14.9%	181	9.7%	84	3.6%
ウェブサイト（R７のみ）		584	2.3%	-	-	-	-
その他		88	0.4%	493	2.3%	213	1.1%
計		24,880	100.0%	20,987	100.0%	19,038	100.0%

※ 「電話」の固定電話、携帯電話、不明は被疑者から電話を受けた際の被害者側の電話種別を計上。
※ 「メール・メッセージ等」は、SMS（ｼｮｰﾄﾒｯｾｰｼﾞｻｰﾋﾞｽ）、SNS(ｿｰｼｬﾙﾈｯﾄﾜｰｸｻｰﾋﾞｽ)、従来のEメール等を含む。
※ 「ポップアップ表示」は、パソコン、スマートフォン等を使用してウェブサイトを閲覧中にポップアップが表示された事案を含む。

9

図２　特殊詐欺被害の入口（犯人側からの最初の接触手段）[10]

この中で最も多い接触手段である電話において、特殊詐欺に利用された番号の種別については、令和５年７月以前は 050 番号が目立っていたものの、現在は、国際電話が急増している。



[10] 総務省，不適正利用対策に関するワーキンググループ(資料８－２)「特殊詐欺の被害状況と通信技術の悪用実態」（警察庁），
https://www.soumu.go.jp/main_content/001008464.pdf

図３　国際電話の犯行利用増加[11]

こうした被害状況も受けて、政府は、「国民を詐欺から守るための総合対策 2.0」（令和７年４月 22 日犯罪対策閣僚会議決定）を策定した[12]。同対策では、政府一丸となった取組を実施することとなっている[13]。

（３）犯罪行為の巧妙化、高度化

更に、新たな不適正利用対策を巡る環境変化として、犯罪行為の巧妙化、高度化がある。令和７年２月下旬、３名の中高生が不正に入手した大量の ID とパスワードの組み合わせ（計３３億件）を元に、楽天モバイル社に対して、生成AI を悪用して自作したプログラムを用いて不正アクセスを行い、多数の回線契約を不正に行ったことが発覚し、検挙されるという、大型の不正契約事案が発生した。その後、同様の手口による不正契約や、当該不正契約した通信回線を用いた新たな犯罪も判明。少年達は、楽天モバイル社の契約の上限数が多く、追加契約に本人確認が必要ないことに乗じたと供述している。このように、生成 AI などの技術が高度化する中で、それが犯罪行為にも悪用されるというケースが判明してきている。

---

[11] 総務省，不適正利用対策に関するワーキンググループ(資料８－２)「特殊詐欺の被害状況と通信技術の悪用実態」（警察庁），
https://www.soumu.go.jp/main_content/001008464.pdf

[12] 首相官邸，国民を詐欺から守るための総合対策 2.0，
https://www.kantei.go.jp/jp/singi/hanzai/kettei/250422/honbun-1.pdf

[13] 通信関連施策としては、例えば以下のような施策が策定されている。
・携帯電話不正利用防止法上、契約時における本人確認が義務付けられていないデータ通信専用 SIM について、悪用実態を踏まえ、電気通信事業者に対して契約時における実効性のある本人確認の実施を働き掛けるとともに、契約時の本人確認の義務付けを含め検討。
・契約変更等の機会も活用しながら、国際電話サービスを利用しない設定があることを一層強く国民に周知。また、将来的には、国際電話サービスを利用しない者に対する優遇措置等、国際電話を必要としない人への利用休止を促すような効果的な対策の導入を検討。
・通信履歴の保存の在り方について、電気通信事業における個人情報等保護に関するガイドライン改正や保存義務付けを含め検討。

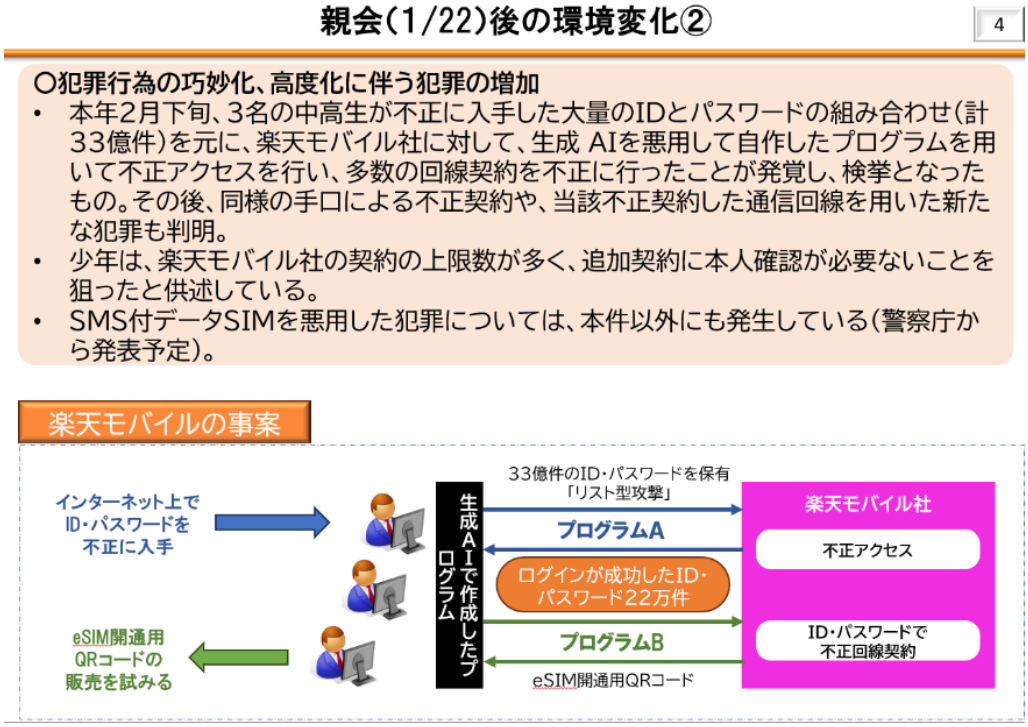


図４　犯罪行為の巧妙化、高度化に伴う犯罪[14]

本ワーキンググループでは、上述の新たな不適正利用対策を巡る環境変化を踏まえて、令和７年４月から６月で、計４回の議論を経て、対策に関して検討を行った。検討に当たっては、（１）携帯電話の契約時等の本人確認のルール関係と、（２）その他の特殊詐欺の電話・メール等対策について、２部に分けて議論を行ったところ、以下、２部構成で記載をしている。

第２部　携帯電話の本人確認のルール

第１章　携帯電話の本人確認に関する現在の対策

携帯電話不正利用防止法[15]においては、携帯音声通信事業者に対して、携帯電話の新規契約時、譲渡時及び貸与時の本人確認等を義務づけている。

同法では、契約者の管理体制の整備の促進及び携帯音声通信サービスの

[14] 総務省，不適正利用対策に関するワーキンググループ(資料７－１)「ICT サービスの利用環境を巡る諸問題について(案)」（総務省），
https://www.soumu.go.jp/main_content/001006426.pdf

[15] 携帯音声通信事業者による契約者等の本人確認等及び携帯音声通信役務の不正な利用の防止に関する法律（平成 17 年法律第 31 号）

不正利用の防止のため、以下を措置している。

１　契約締結時・譲渡時の本人確認義務等

２　貸与業者の貸与時の本人確認義務等

３　警察署長からの契約者確認の求め

４　携帯電話の無断譲渡・譲受けの禁止

５　事業者による役務提供の拒否

このほか、総務大臣による携帯音声通信事業者の監督事項や、法に違反した場合の罰則事項が設けられている。

近年、目視による真贋判定が困難なほど、券面が精巧に偽変造された本人確認書類を用いた携帯電話の不正契約や、偽造した本人確認書類で SIM カードの再発行を受けることにより、実在する人物の携帯電話番号を詐取するような事案が発生していること等を受けて、令和５年６月に閣議決定された「デジタル社会の実現に向けた重点計画」において[16]、携帯電話不正利用防止法における本人確認の厳格化が決定された。

これを受けて、本ワーキンググループにおいては、前述のとおり、令和６年２月から６月、計６回議論を行い、以下の携帯電話不正利用防止法の施行規則[17]改正の方向性を示したところである。[18]

① 偽変造されやすい本人確認方式（eKYC、住民票の写しのコピー）の廃止

---

[16] 「デジタル社会の実現に向けた重点計画」（令和６年６月閣議決定）においても、「犯罪による収益の移転防止に関する法律、携帯音声通信事業者による契約者等の本人確認等及び携帯音声通信役務の不正な利用の防止に関する法律（携帯電話不正利用防止法）に基づく非対面の本人確認手法は、マイナンバーカードの公的個人認証に原則として一本化し、運転免許証等を送信する方法や、顔写真のない本人確認書類等は廃止する。対面でもマイナンバーカード等の IC チップ情報の読み取りを犯収法及び携帯電話不正利用防止法の本人確認において義務付ける。また、そのために必要な IC チップ読み取りアプリ等の開発を検討する。加えて、公的個人認証による本人確認を進めるなどし、本人確認書類のコピーは取らないこととする。」と示されている。

[17] 携帯音声通信事業者による契約者等の本人確認等及び携帯音声通信役務の不正な利用の防止に関する法律施行規則（平成 17 年総務省令第 167 号）

[18] 総務省，不適正利用対策に関するワーキンググループ報告書(令和６年 11 月 29 日)，https://www.soumu.go.jp/main_content/000979524.pdf

② 偽造・改ざん対策が施された本人確認方式（住民票の写し等）の存置
③ IC チップの読み取りを原則義務化
④ IC チップのない本人確認方式（住民票の写し等）を一定条件のもと存置

上述の改正の方向性を受けて、令和７年４月１日に非対面方式の本人確認に関して携帯電話不正利用防止法の施行規則を改正したところであり、令和８年４月１日から施行予定である[19]。対面方式の本人確認についても、追って改正予定であり、「デジタル社会の実現に向けた重点計画」の工程表（令和７年６月 13 日閣議決定）[20]では、令和９年４月の施行が掲げられている。

また、事業者においても、こうした法令上の本人確認に加えて、業界として携帯電話の不適正利用を防止するため、自主的な取組としてデータ SIM の本人確認[21][22]や上限契約台数[23]等について、業界ルールを策定してきたところである。

第２章　携帯電話の本人確認に関する課題と検討

こうした携帯電話の契約時等の本人確認の厳格化の制度整備を進めているところだが、第一章の検討の背景で述べたような不適正対策を巡る環境変化も踏まえて、本ワーキンググループでは、以下６点の検討を行った。

---

19 総務省，携帯音声通信事業者による契約者等の本人確認等及び携帯音声通信役務の不正な利用の防止に関する法律施行規則の一部を改正する省令案に対する意見募集の結果の公表, https://www.soumu.go.jp/menu_news/s-news/01kiban18_01000247.html

20 デジタル庁，デジタル社会の実現に向けた重点計画，
https://www.digital.go.jp/policies/priority-policy-program#document

21 一般社団法人電気通信事業者協会，契約時の本人確認について，
https://www.tca.or.jp/mobile/confirmation.html

22 一般社団法人テレコムサービス協会，データ通信契約申込み受付時おける本人確認手続きに関する申合せ書, https://www.telesa.or.jp/vc-files/information/mvno-moushiawase-20210129.pdf

23 一般社団法人電気通信事業者協会，振り込め詐欺の被害防止対策の取り組みについて，
https://www.tca.or.jp/press_release/2009/0115_289.html

１　SIM の不正転売

令和６年末頃、いわゆる「闇バイト」の一つとして、青少年などに対して、携帯電話や SIM を高額で買い取るという触れ込みで、犯罪者自身の代わりに携帯電話などを契約させるアルバイトが横行した。現行法令上、契約者が携帯音声通信事業者に無断で SIM を譲渡等する場合、携帯電話不正利用防止法に抵触する（また、業として有償で譲渡した場合には、罰則も適用される[24]）。バイト応募者は、購入先の各携帯ショップで割賦契約を行うため、他人に譲渡や転売した後に一時的な報酬を得たとしても、多額の契約の分割金を払い続ける必要があり、負債が残る。また、バイト応募者が犯罪者に端末を譲渡または転売した場合、期せずして詐欺に加担することになる可能性が高いこともある。

事業者の不適正利用対策の取組としては、店頭での掲示による注意喚起や契約時の重要事項説明による確認を実施している。一方、事業者としては、見た目上は、正当な申込みとなるので、店頭で発見して抑止することが難しいことも課題となっている。

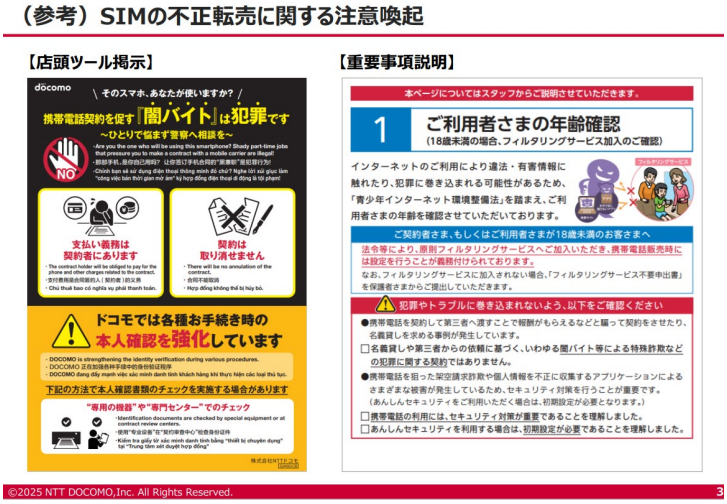


図５　事業者で実施している SIM 不正転売に関する注意喚起の例[25]

SIM の不正転売が増加し、詐欺への転用等の可能性が指摘されている中、転売の防止に向けてどのような効果的な対策が考えられるかについて議論

[24] 携帯法不正利用防止法第 20 条第 1 項

[25] 総務省，不適正利用対策に関するワーキンググループ資料７－３，https://www.soumu.go.jp/main_content/001006424.pdf

を行ったところ、構成員から以下のような指摘があった。

＜構成員の主な意見＞

- SIM の不正譲渡が携帯電話不正利用防止法に反する行為であることの周知を改めて徹底することが必要。
- 利用者への周知啓発の強化だけではなく、関与した本人も不利益を被る可能性があるなどのストーリーや、闇バイトに応募してしまった場合の相談先なども一緒に示すことが必要ではないか。
- 現状事業者の店頭掲示については、犯罪行為の警告や相談を勧告する内容だが、詐欺行為への加担者として民事の損害賠償責任を負う可能性についても警告してもよいのではないか。
- 関与した本人が捜査対象になる可能性があることをストレートに伝えていく方が良いのではないか。
- 利用者の本人確認を、公的個人認証サービスを活用するなどして、定期的に行い、転売を防ぐ仕組みが必要ではないか。

これらを踏まえ、今後は、事業者による不正検知が困難である中、犯罪抑止の観点から当面取りうる対策として、不正転売の違法性について政府及び事業者が利用者に対してわかりやすい周知啓発を一層強化していくことに加え、事業者による取組の推進なども必要である。例えば、わかりやすい周知啓発については、関与した本人も不利益を被る可能性や、関与した本人が捜査対象になる可能性があるなどのストーリーを示すことや、闇バイトに応募してしまった場合の相談先なども一緒に示すことなども考えられる。事業者における取組の推進については、不正転売を難しくするような携帯電話契約・端末割賦契約時の与信時の審査強化などの仕組みの導入や事業者による定期的な本人確認なども考えられる。

２　法人の代理権（在籍確認）

現行法令上、法人が新規契約をする場合は、法人の登記事項証明の提示に加えて、来店する担当者の本人確認が義務づけられている。一方で、来店する担当者と法人の関係性を担保する要件、例えば代理権があるかの確認

については、現行法令上求められていない[26]。事業者においては自主的な確認を実施しており、例えば委任状や名刺の提出や各種の書類を求めるような形になっているが、利用者目線からは、分かりづらいとの課題がある。

法人の担当者が契約を行う場合における在籍確認の手法について、法令上の規定がなく、事業者によって異なる取扱いとなっている中、利用者目線に立ってどのような方策が考えられるかについて議論を行ったところ、構成員から以下のような指摘があった。

＜構成員の主な意見＞

- 民法上の法律行為の代理権の確保というよりは、法人の名を騙る不正契約を防ぐ目的にあると考えており、民法的な意味での委任状よりも、来店者が当該法人に在籍をしている事実を示す書類であるかが重要であると考える。
- 中小企業や零細企業は、現実的な在籍確認は難しいので、デジタル庁の G-BIZ ID という取組の活用など、電子的な手法の導入も考えられないか。

これらを踏まえ、今後の方向性としては、法人契約については、現行の事業者の取組も踏まえつつ、利用者目線に立って予見可能性を高める観点から、来店する担当者と法人の関係性を明らかにするために最低限必要な書類の提出を求めるなど、所要の規定見直し（携帯電話不正利用防止法施行規則第 4 条）が必要である。最低限必要な書類については、電子的な書類も排除されないと考えられる。

３　他社の本人確認結果への依拠

本人確認結果への依拠については、昨年のワーキンググループにおいても議論を行い、その報告書[27]では、「過去の本人確認結果に依拠する方法については、事業者のニーズや本人確認の保証レベルとのバランスを鑑みつ

---

[26] 犯罪収益移転防止法においては同施行規則（犯罪による収益の移転防止に関する法律施行規則（平成二十年内閣府・総務省・法務省・財務省・厚生労働省・農林水産省・経済産業省・国土交通省令第一号）において、代表者の要件を定めることで、来店者とその法人の関係性を担保している（犯罪収益移転防止法施行規則第 12 条）。

[27] 総務省, 不適正利用対策に関する ワーキンググループ報告書, https://www.soumu.go.jp/main_content/000979524.pdf

つ総合的に検討することが適当である」としていた[28]。

今回のワーキンググループにおいては、公的個人認証サービスの活用以外の新しい依拠の形として、事業者から２つの具体的な提案があった。１つ目の提案は、金融機関への依拠スキームであり、以下の提案である。

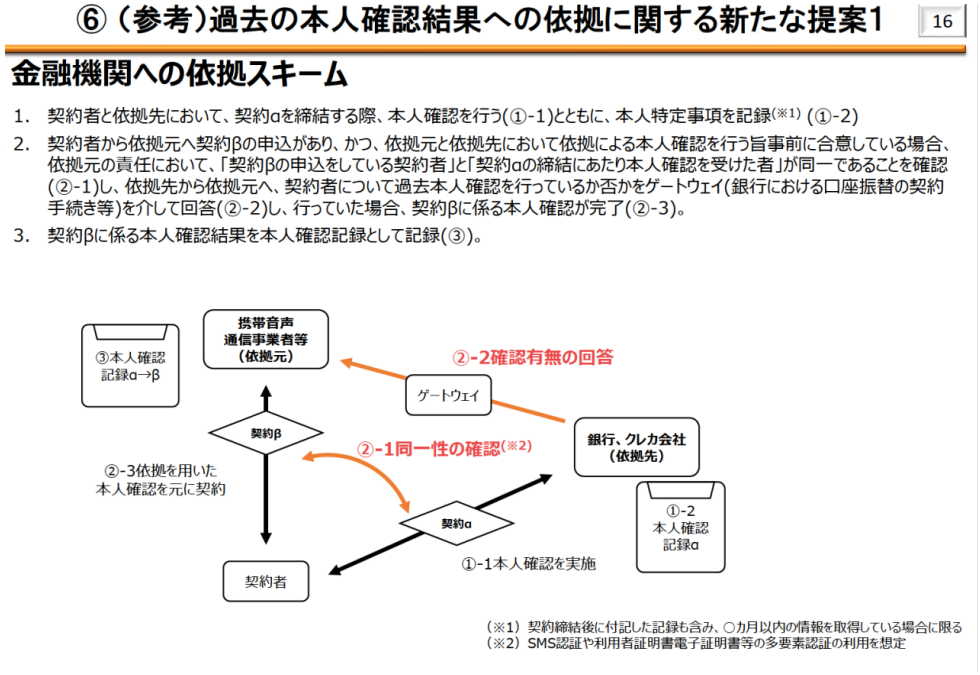


図６　金融機関への依拠スキーム[29]

２つ目の提案は、携帯音声通信事業者同士の依拠のスキームであり、以下の提案である。特に携帯音声通信事業者への依拠については、事業者からも具体的なニーズが認められている。

---

[28] ワーキンググループ報告書では、「本人確認における保証レベルが高く、一定の手続きのもと継続的に最新の本人特定事項を取得可能な本人確認を実施することが望ましい。こうした本人確認方法は、例えば、公的個人認証による方法が考えられ、過去の本人確認結果の依拠方法としては、公的個人認証を用いて本人確認を行った結果に依拠するとともに、依拠先において多要素認証等の当人認証を実施する方法が考えられる。なお、過去の本人確認結果に依拠する方法については、事業者のニーズや本人確認の保証レベルとのバランス等を鑑みつつ、今後、総合的に検討することが適当である。」としていた。

[29] 総務省, ICT サービスの利用環境の整備に関する研究会（第５回）資料５－１, https://www.soumu.go.jp/main_content/000988136.pdf

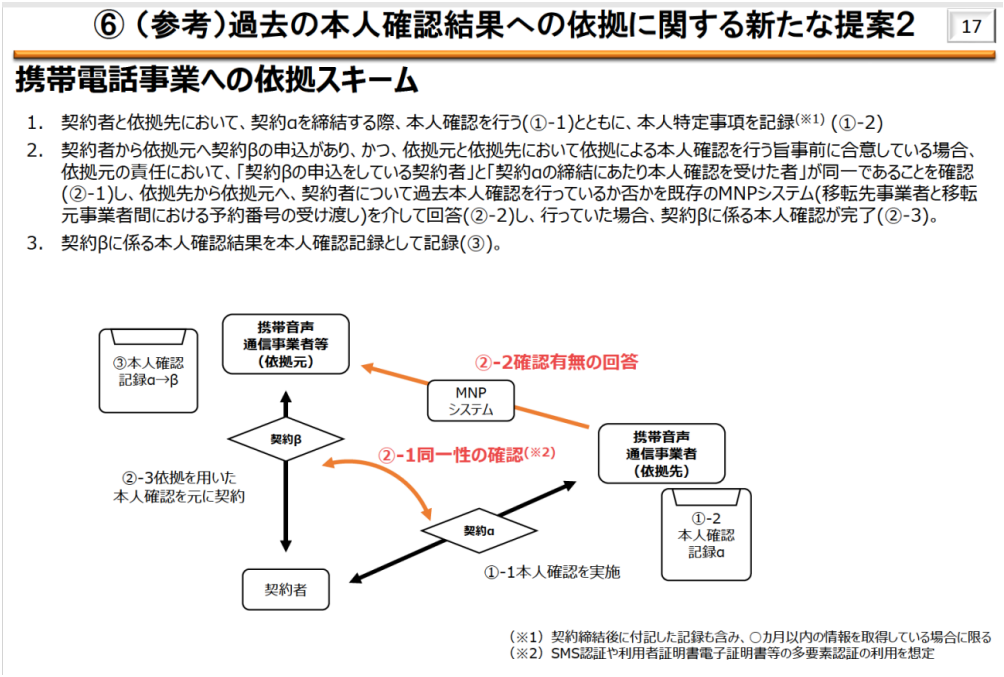


図７　携帯音声通信事業者への依拠スキーム[30]

一方で、他社への本人確認結果に依拠することは、ID/PASS による簡易な方法での本人確認を許容する契約形態を突いた不正契約が行われていること、金融機関への依拠については業界横断的な取組が必要であること、また、携帯音声通信事業者への依拠については、本人確認の保証レベルを上げる取組が未だ途上の段階であることに留意が必要である。

携帯電話の契約時における他社の本人確認結果への依拠について、上述の点を踏まえ、利便性と不正対策のバランスの観点から、どのように考えるべきかについて議論を行ったところ、構成員から以下のような指摘があった。

＜構成員の主な意見＞

- 検討の順番としては、不正への対応について十分に議論した上で、余裕がある限りに検討するという位置づけが良いのではないか。
- 依拠先と依拠元の情報提供に関して、個人情報のやり取りの観点から、ユーザーへの説明が十分になされるべきである。
- 依拠先としては JPKI をベースに本人確認を行っている事業者に限定するのが検討

[30] 総務省, ICT サービスの利用環境の整備に関する研究会（第 5 回）資料 5 － 1 , https://www.soumu.go.jp/main_content/000988136.pdf

の前提になると考える。

これらを踏まえ、他社の本人確認結果への依拠については、一部事業者からのニーズが認められるものの、昨今の犯罪手口の巧妙化、高度化も踏まえると、ID/PASS の不正入手への対策や他の見直し事項の議論の進展を見極める必要がある。今後の方向性としては、依拠先の本人確認の保証レベルが高く最新の本人特定事項となっていることや、依拠元の当人確認が適切に行われることなど、依拠が適切にできる要件を整理した上でルール整備を行うことも視野に、改めて本ワーキンググループにおいて検討を深めていくことも考えられる。

４　追加回線の本人確認

現行法令上、携帯音声通信に関して２回線目以降の追加契約をする場合は、本人確認書類を提示する方式に加えて、ID/PASS による簡易な本人確認方式[31]が認められている。

事業者の取組として、本人確認書類の提示を２回線目以降の音声契約でも自主的に求めている事業者もいるが、昨今の犯罪行為の高度化に伴い、この ID/PASS 方式で本人確認をしたものについて、不正契約が行われる事例が報告されている。警察庁からは、大手モバイルキャリアでの不正 SIM 発行事案において、少年被疑者のパソコンからは約 2,700 件の eSIM が発行できる QR コードが発見されており、この捜査では、約 100 件について立件をしていること、また、この立件した 100 件のうちの 17 件は音声 SIM であり、２回線目以降で本人確認がなされずに不正発行されたものであったことが判明しているとのことであった。

2 回線目以降の回線契約時の本人確認について、法令上の要件が１回線目とは異なっている中、昨今の犯罪手口の巧妙化、高度化に対し、どのような効果的な対策が考えられるかについて議論を行ったところ、構成員から以下のような指摘があった。

---

[31] 相手方から役務提供契約の締結の際に示された本人特定事項を、当該相手方の既に締結した役務提供契約に係る本人確認記録等及び料金の請求その他携帯音声通信役務の提供に必要な事項に係る文書の送付先と照合する方法（携帯電話不正利用防止法施行規則第３条第４項）

＜構成員の主な意見＞

- ２回線目以降の契約が簡易なことがどれだけ犯罪に寄与しているのか、また、追加回線の本人確認に簡易な本人確認手法を残すことが、利用者の利便性の確保がどれだけ切実なのかについての検証が必要。
- ユーザーとしては、なりすまし防止のために、本人確認を厳密にしてもらった方が、安心感があるのではないか。
- ID・パスワードのみの確認では不安なので、当人認証がデジタル庁ガイドラインの少なくともレベル２に当たるような本人確認を実施してほしい。同じ番号でデバイス追加の場合は、犯罪悪用可能性が低そうなことから、レベル 1 でも良いと思うが、悪用事案が出てくれば、今後再検討が必要。
- １回線目とは別機会の契約であり、悪用されるリスクが定型的に見いだされるため、本来、本人確認をしっかりする必要があって、基本的には現状許容されている簡便な確認方法では足りない状況が生じてきている。AppleWatch などのデバイス追加の際に有意な悪用リスクがないという評価ができるかが問われている。
- キャリアが発行している ID とパスワードが一つの軸になると思われるところ、JPKI を活用するなど本人確認とリンクさせた ID・パスワードの管理をガイドライン等で業界横断的にルール化していくことも考えられるのではないか。

これらを踏まえ、今後の方向性としては、簡易な本人確認手法には一定の利便性が認められる一方、現にそのような手法が犯罪の起点となっている点を踏まえれば、当人認証性を向上させるべく、デジタル庁の本人確認の手法に関するガイドラインも参考に、厳格化に向けた規定の見直し（携帯電話不正利用防止法施行規則第３条第３・４項、同規則第 19 条第５項等）が必要である。その際、犯罪実態を踏まえ、すべての回線契約（音声 SIM、音声 SIM 付 AppleWatch）に等しくルールを適用するかどうかについても検討すべきである。

５　上限契約台数

現行法令上、上限契約に対する台数制限はない。一方で一部の事業者で設定している自主ルールでは、音声 SIM については５台、データ SIM ないし AppleWatch については特段上限契約台数がないとされている。上述のとおり、台数上限がないことを奇貨として一度不正契約がなされた場合に、犯罪被害が広がった事例があると報告されている。

契約台数の上限がなければ、本人確認が適切になされない場合に、大量不正契約に繋がる可能性があるが、利用者のニーズと不正対策のバランスの観点から、どのように考えるべきかについて議論を行ったところ、構成

員から以下のような指摘があった。

＜構成員の主な意見＞

- 過少規制も過剰規制もよくないので、規制をかけることによって生じる利便性の阻害の程度や現在の状態が犯罪の増加に寄与している程度等の、基礎的な現状認識をしっかりさせる必要がある。
- 上限契約台数についてのニーズや利用実態を確認する必要がある。[32]
- 契約時の本人確認の強化や定期的な本人確認を行うことができれば、回線数の制限は不要ではないか。
- それぞれの契約が慎重にされるならば問題ないと思う一方で、当人認証の強化によって本当に十分な効果が生じるのかも丁寧に検証が必要。
- 一定のルールは必要であるが、新たなサービス提供の妨げとならないよう、例外措置の検討が必要。例えば、子供用の見守り GPS 端末や IoT などのデータ通信サービスは不正利用リスクが少ないと考えられる。
- 多数台契約をすること自体に怪しさはないか、また、それが現実化して不正利用されれば、被害規模が大きくなるのではないかという点について、複数台契約のニーズは様々に想定され、定型的な悪用リスクを想定できない。常識的な範囲内での台数制限を予防的に設けるという現在の自主的な取組を事業者に継続してもらいながら、状況を注視していくべきではないか。
- 複数回線で問題になるケースというのは、無断で譲渡するとか名義貸しだと理解した上で、上限というよりは目安を決めて、それを超える台数を契約したい人に、使用用途を聞くことも考えられる。もしも申告内容と異なる利用が発覚した場合には、規約違反として既存の通信契約を全部解除することもありうる。こうした方法がとれるのであれば、法律ではなくて自主規制でも良いのではないか。

契約台数の上限については、一部利用者からの複数台契約のニーズもあるものの、不自然に多数の契約が行われるケースもありうる。原則５台の制限を超えての例外的な契約について、使用用途の事前の確認をする一部の事業者がいることを踏まえ、事業者における自主的な取組を一層強化す

---

[32] 上限契約台数についてのニーズや利用実態について、事業者からは、一人で６回線以上契約されることは、市場全体での一定のボリュームはあると考えられることや、家族での多回線契約のニーズとして、金銭管理がしやすい、ポイントが貯めやすい、管理のしやすさといった理由が考えられるとのことであった。

るべきである。その上で、今後、少なくともそうした事業者の自主的な取組のルールの適用状況について検証を行い、更にその取組を促進するとともに、必要に応じて、犯罪との因果関係を踏まえながら、何らかのルール化について検討すべきである。

６　データ SIM の本人確認

現行の携帯電話不正利用防止法において、データ SIM は、対象となっていないが、一部の事業者においては、自主的な取組として、音声 SIM と同等の方式で本人確認がなされている。

警察庁の調査によれば、データ SIM を悪用した犯罪事例などが複数報告されている。特に SNS 型投資・ロマンス詐欺においては、当初の接触ツールや被害時の連絡ツールとして SNS が使用される場合が多く、SMS 付データ SIM については、その SNS などのアカウントをつくるための２段階認証に使用されているケースがある。令和６年４月から９月までの間に都道府県警察から警察庁になされた報告によれば、SNS 型投資・ロマンス詐欺に係る被疑事件で使用された SIM について、SIM 種別の特定に至ったものは 244 件あり、そのうちの 185 件は SMS 付データ SIM であり、残りの 59 件は音声 SIM という結果であった[33]。一方で、SMS 無しデータ SIM については、犯罪事例はあるが、現時点での定量的な犯罪実態を示すことは難しいとのことであった。

データ SIM の本人確認について、法令上の扱いが音声 SIM と異なっている中、犯罪実態を踏まえて、昨今の犯罪手口の巧妙化、高度化に対し、どのような効果的な対策が考えられるかについて議論を行ったところ、構成員から以下のような指摘があった。

＜構成員の主な意見＞

【総論】

- データ SIM について、アクセス元が何かあった時に犯罪の観点から特定できる仕組みを残すべきではないか。
- データ SIM については、警察庁の資料によれば、悪用の実態が相当程度確認される以上、悪用リスクはあると言うべきであって、筋論としては、本人確認の義務づけの対象となるのが原則ではないか。問題は、一定の観点から例外を設けるべきでは

[33] 総務省，不適正利用対策に関するワーキンググループ資料９－２，
https://www.soumu.go.jp/main_content/001009476.pdf

ないかということであり、SMS 機能がついていないものや IoT 機器等に利用されるものを除外するべきかどうか。これは悪用リスクの評価の問題であり、悪用リスクが低かったり、技術的にコントロール可能であったりということであれば除外してもよいと思う。

- SaaS や金融サービスの利用において、携帯電話番号が本人確認をするためのトラストアンカーになっていることから、本人確認の導入が議論されていると考えられるところ、SIM の通話機能・SMS 機能の有無によって、SIM が果たすトラストアンカーとしての役割というのが変わってくると考えられる。

【対象 SIM】

- SMS 付/無しデータ SIM について、定量的な犯罪実態の確認が必要。
- SMS 付データ SIM については、厳格な本人確認が必要ということで合意の方向だと考えるが、それを前提として、例外を精緻に議論する段階に入っているかと思う。どういうものを例外とすべきか、それらのリスクが低いと考えられる理由と併せ、精緻な議論が必要なのではないか。
- SMS 無しデータ SIM について、どの程度の悪用実態が現時点であるのかも併せて考えて、どのくらい厳格化していく必要があるのか考えていく必要がある。ネット経由で訪日前に購入されるというケースも多いと思われるところ、義務化は相当大がかりな変更が必要になるので、慎重な検討が必要。
- SMS 無しデータ SIM については、インターネット上で様々なサービスが利用できるが、Wifi や海外から持ち込まれた SIM へのローミングについても同じことが言えるのではないか。トラストアンカーについての役割を考えた際に、仮にデータ通信についても本人確認をすると、利便性の多大なる低下も予想される中、犯罪を抑制する効果を期待しているのか、捜査の精度を高めていく効果を期待しているのか疑問。

【利用用途（IoT)】

- IoT 用の SIM について、他の用途に利用できないかを確認をする必要がある。

【利用用途（訪日外国人向けプリペイド)】

- SMS 付訪日外国人向けのプリペイド SIM で、詐欺事件に利用されていたりするものはあるのか要検証。
- 自販機での販売は、厳格化した場合は事業継続が難しい事業者もいるとのことだが、日本人でも簡単に買うことができ、抜け穴にもなり得るのではないか。
- 訪日外国人については、ガイドライン等で短期間の利用に留めるなどのルールを設けて事業者の間でレベル感を合わせていくという取組が必要ではないか。

- プリペイドSIMを除外するべきかについては、利用可能期間の限定などによる、悪用リスクの評価・コントロールの問題があるが、より大きいのは、想定される利用者との関係での本人確認の現実的困難性の問題。訪日外国人に対しても原則どおりの厳格な本人確認を要求することは、訪日外国人にデータSIMを使うなと言うに近くなる。サービス自体が立ち行かなくなるという問題については、筋論としては、本人確認自体は必要であり、検討すべきはその方法の緩和である。貸与時の本人確認の規律を参考にするという案も含めて、引き続き検討が必要ではないか。

【本人確認の実効性】

- 例えば、ホテル宿泊の際に必ずパスポートの提示を求めている。パスポートが偽造かどうかにかかわらず、記録自体を残すことは、偽造パスポートの出所の調査へも繋がるなど、捜査に資するのではないか。

今後の方向性としては、データ SIM については、悪用の実態が確認されたことを踏まえ、一部の事業者で既に自主的に行われている本人確認の取組を確実に行う観点から、義務化について検討すべきである。ただし、義務化を検討するにあたっては、貸与時の本人確認の規律も参考に、対象 SIM や利用用途（訪日外国人や IoT 機器）等に関して、不正利用を防止しようとするあまり、過剰規制に陥ることのないよう、利便性へのバランスの観点から利用実態や実効性に配慮した規定とするべきである。

第３部　その他の特殊詐欺の電話・メール等の対策

第１章　その他の特殊詐欺の電話・メール等に関する現在の対策

総務省においては、特殊詐欺の電話・メール等対策に関しては、携帯電話不正利用防止法や犯罪収益移転防止法[34]に基づく本人確認、電気通信事業者による特殊詐欺に利用された固定電話番号等の利用停止等スキーム[35]、特定電子メール法[36]の執行等により、制度的な対策を実施してきている。またメールに関する対策については、送信側と受信側が協調し、総合的に送信ドメイン認証を行うなりすましを判定する技術（DMARC 等）について、

---

[34] 犯罪による収益の移転防止に関する法律（平成 19 年法律第 22 号）

[35] 総務省，電気通信事業者による特殊詐欺に利用された固定電話番号等の利用停止等スキームの改定，https://www.soumu.go.jp/menu_news/s-news/01kiban18_01000198.html

[36] 特定電子メールの送信の適正化等に関する法律（平成 14 年法律第 26 号）

その普及促進や受信拒否を要求するポリシーでの運用の働き掛けを実施してきたところである[37]。

また、事業者においても、固定・携帯電話、メール・SMS に関して、各種の詐欺対策サービスを提供しているところ、総務省としては、各種サービスの提供に当たって法解釈の相談に応じることや通信事業者への要請を実施すること等で、事業者の対策を促進する環境を作ってきたところである。

第２章　その他の特殊詐欺の電話・メール等に関する課題

総務省や通信事業者において従前より、特殊詐欺の被害防止に向けて、迷惑電話、迷惑 SMS、迷惑メール対策の各種サービスや機能の提供に加え、利用者への注意喚起等の各種対策を推進してきたところではあるが、第一章の検討の背景で述べたような不適正対策を巡る環境変化のとおり、特殊詐欺の認知件数・被害額は、ともに過去最悪となっていること、固定宛ての国際電話を悪用した詐欺電話が多いこと等を踏まえて、本ワーキンググループでは、以下３点から検討を行った。

１　固定・携帯電話、SMS・メール対策

（１）固定電話

詐欺電話被害の防止対策の１つとして、国際電話の利用を望まない利用

---

[37] いわゆる「なりすましメール」への技術的対策の一つである送信ドメイン認証技術（SPF、DKIM、DMARC 等）の普及に向け、同技術の導入と受信拒否を要求するポリシーでの運用を検討するよう、所管省庁を通じた金融機関、ＥＣ事業者、物流事業者、行政機関等への要請やインターネットサービスプロバイダー等のメール受信側事業者への要請を実施しているほか、「政府機関等の対策基準策定のためのガイドライン（令和５年度版）」（2023 年７月４日）へ DMARC の取扱い強化等技術的動向を踏まえた対策を記載している。また、迷惑メール相談センターにおいて受信者向けに迷惑メール対策の周知・広報を積極的に実施。さらに、電気通信事業者、送信事業者、ISP 事業者、セキュリティベンダー、消費者団体、学識経験者、関係省庁などが幅広く集まる迷惑メール対策推進協議会において、官民連携の技術実証も踏まえた「送信ドメイン認証技術 DMARC 導入ガイドライン」を周知するほか、「送信ドメイン認証技術導入マニュアル第 3.1 版」（2023 年２月改訂）の配布、DMARC におけるポリシーの変更を推進するためのガイドブックの作成等を行っている。

者に対しては着信制限による対策が効果的であることが考えられることから、民間の事業者で運営している国際電話不取扱受付センターでの固定電話宛ての国際電話の発着信の休止サービスの更なる周知や、運営の改善が有効である。

現在、国際電話不取扱受付センターについては、国際電話を休止したいという要望が増加しているため、申し込みが増加し、積滞している。そのため、不取扱センターの対策強化やキャパシティー向上を見据えた運用改善を検討することが課題である。それに加えて、利用休止を未検討の人に対し、契約変更の機会を捉えて利用休止の説明や、真に必要としない人に対して利用休止を促すような効果的な措置を検討することも課題である。

こうした中、令和７年６月 10 日、総務省として、電話の不適正利用対策を推進する観点から、電話の不適正利用対策に係る相談窓口（迷惑電話対策相談センター）を設置した。迷惑電話対策を含む電話の不適正利用対策に係る相談を幅広く受け付けるもので、具体的には、特殊詐欺の契機となる不審な電話への適切な対応に関する相談などの受付を開始している。

引き続き、国際電話番号からの特殊詐欺が増加しているところ、固定電話向けの電話について、どのような対策が取りうるのかについて議論を行ったところ、構成員から以下のような指摘があった。

＜構成員の主な意見＞

- 国際電話不取扱受付センターについて、このワーキンググループで初めて知ったので、一層の周知広報の余地があると考えられる。
- 国際電話不取扱受付センターの HP に設置目的や運営者名を明記し、なりすましと間違えられないようにするなど、利用者から使いやすいものとなるよう HP の改修をしてほしい。
- 総務省の相談窓口が開設されることを踏まえて、官民連携を進めるべき。

これらを踏まえ、今後の方向性としては、国際電話不取扱受付センターについて、積滞解消を行った上で、今後申請件数も増えることも踏まえて、総務省の迷惑電話対策相談センターとも官民連携を行い、適切に国際電話の不適正対策を推進することが期待される。

（２）携帯電話、SMS・メール対策

携帯電話、SMS・メール対策への詐欺電話被害の防止策としては、事業者各社が提供している、迷惑電話、SMS・メール対策サービスの活用が効果的だと考えられる。一方で、こうした迷惑電話、SMS・メール対策サービスに

ついては、サービスが十分に周知されていなかったり、初期設定がなく利用者側で改めて設定をする必要があったり、その結果、利用者に十分に浸透していないケースがある。また、事業者の対策サービスが、有料であることもあり、その点、利用者が利用しづらいという側面もあると考えられる。

引き続き、携帯電話利用者における詐欺被害の増加があるところ、迷惑SMS、迷惑メール等に伴う被害防止に向けて、どのような対策が取りうるのかについて議論を行ったところ、構成員から以下のような指摘があった。

＜構成員の主な意見＞

- 利用者としては、費用がかかることがネックとなって、せっかくの各社の詐欺対策サービスの利用を控えるということにならないよう、基本的な対策部分は、できるだけ低廉化していただきたい。できれば無料かつデフォルト設定にするのが望ましい。

これらを踏まえ、事業者の各種詐欺対策については、本年６月にサービスの低廉化の推進や注意喚起の周知等[38][39][40][41][42]を実施しているところ、今後の方向性としては、その取組に事業者間でばらつきがあったことから、利用者にとって詐欺対策がしやすくなるよう、一層の対策の低廉化を含めた効果的な取組の推進が期待される。

２　スプーフィング

携帯電話や固定電話のディスプレイに表示する電話番号を、実在する組織や団体の番号に偽装するようなケースが報告されている。電話を受ける側から見れば、表示される番号が実在する番号であるため、同番号にかけ

---

[38] NTT 東日本, 特殊詐欺犯罪の防止に向けた国際電話の利用休止の一元受付などの取り組みについて, https://www.ntt-east.co.jp/release/detail/20250610_01.html

[39] NTT 西日本, 特殊詐欺犯罪の防止に向けた国際電話の利用休止の一元受付などの取り組みについて, https://www.ntt-west.co.jp/news/2506/250610a.html

[40] KDDI, 迷惑電話対策サービスを 6 カ月無料提供、特殊詐欺被害の防止に貢献, https://newsroom.kddi.com/news/detail/kddi_nr-614_3948.html

[41] 楽天, 楽天モバイル、65 歳以上のお客様の生活を応援する 「敬老」キャンペーンを実施, https://corp.mobile.rakuten.co.jp/news/media/2025/0617_01/

[42] ソフトバンク, 国際電話を悪用した特殊詐欺に関するご注意, https://www.softbank.jp/mobile/info/personal/news/support/20250610a/

直してみると電話に繋がることが報告されている。これまで、一定程度の対策を実施しているところであるが、着信画面に任意の番号を表示させるアプリや、海外の通信会社の回線を使用している場合も報告されているところである。

本件については、通信事業者と連携して効果的な対策を検討し、できるところから実施しているところである。今後も国民に対して電話番号を偽装する手口に関しての更なる注意喚起を推進していくとともに、電話番号を偽装する手口について、引き続き検討を行っていくことが必要である。

３　海外電話番号による詐欺電話

例えば日本にいながら簡単に海外電話番号を取得可能なアプリが報告されており、それを使い捨て可能な電話番号として SMS 認証や特殊詐欺の電話番号として使われ得るというような状況である。

本件については、国民に対して国際電話発の詐欺電話に関する注意喚起を推進していくとともに、引き続き実態把握を行っていく必要がある。

参考資料

参考資料１

「不適正利用対策に関するワーキンググループ」構成員

（敬称略・五十音順）

【構成員】

（主査）大谷 和子 株式会社日本総合研究所 執行役員 法務部長
沢田 登志子 一般財団法人 EC ネットワーク 理事
鎮目 征樹 学習院大学 法学部 教授
辻 秀典 デジタルアイデンティティ推進コンソーシアム 代表理事
仲上 竜太 日本スマートフォンセキュリティ協会 技術部会 部会長
中原 太郎 東京大学大学院 法学政治学研究科 教授
星 周一郎 東京都立大学 法学部 教授
山根 祐輔 片岡総合法律事務所 弁護士

【オブザーバー】

警察庁 刑事局 捜査支援分析管理官
警察庁 サイバー警察局 サイバー企画課

参考資料２

不適正利用対策に関するワーキンググループ　検討過程

会合	開催日	主な議題
第７回	令和７年 ４月 21 日	○　事務局説明 ○　警察庁報告（データ通信 SIM の悪用実態） ○　ヒアリング ・ 株式会社 NTT ドコモ ・ KDDI 株式会社 ・ ソフトバンク株式会社 ・ 楽天モバイル株式会社 ・ テレコムサービス協会 MVNO 委員会
第８回	令和７年 ５月９日	○　事務局説明 ○　警察庁報告（特殊詐欺の被害状況と通信技術の悪用実態） ○　ヒアリング ・ 東日本電信電話株式会社・西日本電信電話株式会社 ・ 株式会社 NTT ドコモ ・ KDDI 株式会社 ・ ソフトバンク株式会社 ・ 楽天モバイル株式会社
第９回	令和７年 ５月 16 日	○　事務局説明 ○　前回発表の補足発表 ・ 警察庁 ・ 株式会社 NTT ドコモ ○　ヒアリング ・ 株式会社 U-NEXT
第　10 回	令和７年 ６月６日	○　中間的な論点整理に向けた意見交換

通信ログ保存の在り方に関するワーキンググループ

１　現状の課題及び検討の経緯

⑴　通信履歴[43]は、通信の構成要素であり、憲法の規定を受けた電気通信事業法第４条第１項の通信の秘密として保護されることから、電気通信事業者が通信履歴を記録・保存することは通信の秘密の侵害に該当し得る。そのため、電気通信事業者が通信履歴を記録・保存するためには、当該通信履歴に係る通信当事者の有効な同意を取得するか、正当業務行為等として違法性が阻却されることが必要となる。

⑵　電気通信事業における個人情報等の保護に関するガイドライン（同ガイドラインの解説を含め、以下「本ガイドライン」という。）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」とし、「いったん記録した通信履歴は、記録目的の達成に必要最小限の範囲内で保存期間を設定し、保存期間が経過したときは速やかに通信履歴を消去しなければなら」ず、保存期間の例示として、通信履歴のうち、インターネット接続サービスにおける接続認証ログ（ＩＰアドレスを割り当てた記録）の保存について、一般に６か月程度の保存は認められ、適正なネットワークの運営確保の観点から年間を通じての状況把握が必要な場合など、より長期の保存をする業務上の必要性がある場合には、１年程度保存することも許容されるとしている。[44]

⑶　電気通信事業者は、本ガイドラインを前提にその業務を運用しており、課金、料金請求、苦情対応、不正利用の防止その他業務の遂行上必要な場

---

[43] 本報告書における通信履歴とは、利用者が電気通信を利用した日時、当該電気通信の相手方その他の利用者の電気通信に係る情報であって当該電気通信の内容以外のものをいう（電気通信事業における個人情報等の保護に関するガイドライン（令和４年個人情報保護委員会・総務省告示第４号（最終改正令和６年個人情報保護委員会・総務省告示第４号））第３８条第１項の記載のもの）。

[44] 本ガイドラインは、課金、料金請求等が例示されるとともに、保存期間の例示として接続認証ログが挙げられていることから、インターネット接続サービスを提供する事業者であるいわゆるアクセスプロバイダ（以下「ＡＰ」という。）を主に念頭においた記載となっており、ＳＮＳやインターネット上の掲示板等を提供する事業者であるいわゆるコンテンツプロバイダ（以下「ＣＰ」という。）における通信履歴の保存の在り方については必ずしも明確になっていない。この意味においても、本ガイドラインにおける通信履歴の保存の在り方を整理すべき状況にあるといえる。

合に、必要最小限度の通信履歴を記録し、各電気通信事業者の業務内容等に応じて、記録目的に必要な範囲で保存期間を設定し、保存期間が経過したときは速やかに消去している。

⑷　近年の社会環境の変化として、ＳＮＳやインターネット上の掲示板等における誹謗中傷をはじめとする違法・有害情報の流通の高止まりを背景とし、特定電気通信による情報の流通によって発生する権利侵害等への対処に関する法律（平成１３年法律第１３７号。通称「情報流通プラットフォーム対処法」。）が相次いで改正され、同法に基づく発信者情報開示請求の件数も増加傾向にある。また、ＳＮＳやインターネット上の掲示板等で著しく高額な報酬の支払いを示唆するなどして、犯罪の実行者を募集する投稿（いわゆる「闇バイト」の募集投稿）等が掲載されるなど、違法情報の流通が社会問題となっている。

⑸　これらを背景として、①発信者情報開示請求をする者等から、誹謗中傷等の被害者救済の観点で、発信者情報の開示前に通信履歴が消去されているとして、通信履歴の保存期間が短い旨の指摘があり、②警察庁等から、犯罪捜査の観点で、サイバー空間における事後追跡上の障害の一つとして、通信履歴の保存期間が短い旨の指摘がある。

⑹　上記社会環境の変化や各指摘等を踏まえ、総務省では、通信履歴の保存の在り方について検討を開始し、具体的な検討は、通信履歴が通信の秘密として保護されるものであることを踏まえ、法学専門家を構成員とする「通信ログ保存の在り方に関するワーキンググループ」（以下「本ＷＧ」という。）において行うこととした。これまで、本ＷＧでは、ＣＰ及びＡＰ、警察庁、発信者情報開示請求事件を担当する弁護士のヒアリングを実施するなど、様々な観点から検討を進めてきた。これらを踏まえ、本ＷＧでは、通信履歴の保存の在り方の検討結果として、本ガイドラインの改正を行うこととし、以下のとおり、同改正案を提案する。

２　改正案

本ガイドラインの改正案（以下「本改正案」という。）は、別添のとおりであり、以下補足する。

⑴　概要

本改正案については、ＣＰ及びＡＰは、各サービス内容に応じた業務の

遂行上必要な通信履歴を対象として、少なくとも３～６か月程度保存しておくことが、誹謗中傷等の違法・有害情報への対策のための社会的な期待に応える望ましい対応であり、同対応のために通信履歴を同期間保存することは、電気通信事業法上の通信の秘密との関係で許容されるとの考え方を示すものである。

⑵　改正案の趣旨

本改正案は、社会環境の変化を踏まえ、ＣＰ及びＡＰに対し、社会的な期待に応える望ましい対応を示したものである。本ＷＧにおけるヒアリングでは、特に、前記１⑸の指摘の①について、通信履歴の保存期間の経過により、発信者情報の開示が受けられない事例が相当数認められるなど、被害者救済の観点で具体的な課題が顕在化した。同課題への対策としては、発信者情報開示手続の更なる迅速化など、必ずしも通信履歴の保存に限るものではないものの、少なくとも３～６か月程度の通信履歴の保存がなければ、被害者救済が困難であることを踏まえると、誹謗中傷等の違法・有害情報への対策のために通信履歴を保存することの必要性が認められる。一方で、通信の秘密やプライバシーの保護など、利用者利益とのバランスも考える必要がある。本改正案は、これらを踏まえ、ＣＰ及びＡＰは、誹謗中傷等の違法・有害情報への対策のために必要不可欠な通信履歴を少なくとも３～６か月程度保存することが望ましいとするもの[45]である。

⑶　保存期間

現時点の本ガイドラインは、接続認証ログを対象として、保存することが許容される期間として６か月程度（より長期の保存をする業務上の必要性がある場合に１年程度）を示すものであるが、本改正案では、保存することが望ましい期間（少なくとも３～６か月程度）を新たに示すものであり、望ましい期間を超えた保存を行うことも、業務の遂行上の必要性がある場合には、これまでどおり許容される。なお、本改正案に違反したことをもって直ちに法的責任が生じるものではない。

---

[45] 本改正に伴い、ＣＰ及びＡＰにおいて、対象となる通信履歴について、少なくとも３～６か月程度保存することが期待されるところ、当該通信履歴を保存するに当たり、安全管理のための必要かつ適切な措置を講じなければならないことは、本ガイドライン第12条、「９（別添）講ずべき安全管理措置の内容」等の記載のとおりである。

⑷　適用開始時期

本ガイドラインの改正に伴い、ＣＰ及びＡＰにおいて、通信履歴の保存に係る設備や人的体制の増強等が必要になる場合が考えられるところ、本改正案の具体的な適用開始時期については、これまでのＣＰ及びＡＰのヒアリングに加え、パブリックコメント等を踏まえ検討を行う。

⑸　今後の検討課題

本改正案の適用開始後に、通信履歴の保存の在り方等に関する事業者ヒアリングを実施するなど、本改正案の効果検証を行うこととする。仮に本ガイドラインの改正によっては前記課題の解決につながらないことが明らかになった場合には、通信履歴の保存について、利用者利益の保護を図ることを前提として、何らかの法的担保を含め本ガイドラインの改正以外の方法で検討することが必要になると考えられる。ＣＰ及びＡＰが本改正案に従った対応をとることが、社会的な期待に応える望ましい対応である。

電気通信事業における個人情報等の保護に関するガイドラインの解説
（下線部が改正箇所）
第 38 条（第1項）

1　電気通信事業者は、通信履歴（利用者が電気通信を利用した日時、当該電気通信の相手方その他の利用者の電気通信に係る情報であって当該電気通信の内容以外のものをいう。以下同じ。）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。

通信履歴は、通信の構成要素であり、通信の秘密として保護され、これを記録することも通信の秘密の侵害に該当し得る。しかし、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。

利用明細（第39条第1項参照）の作成に必要な限度で通信履歴を記録・保存することは、利用料金を正しく算定し、加入者に対して料金請求の根拠を示し得るようにするという点で、債権者たる電気通信事業者の当然の権利であるから、電気通信事業者は、加入者の同意がなくとも、正当業務行為として、利用明細作成に必要な限度の通信履歴を記録・保存することができる。

なお、発信者を探知するための通信履歴の解析は、目的外利用であるばかりでなく通信の秘密の侵害となることから、裁判官の発付した令状に従う場合、正当業務行為に該当する場合その他の違法性阻却事由がある場合でなければ行うことはできない。

【正当業務行為として違法性が阻却される事例】
事例）インターネットのホームページ等の公然性を有する通信において、違法・有害情報が掲載され、その発信者に警告を行わないと自己のサービス提供に支障を生じる場合（自己のサービスドメインからの通信がアクセス制限される場合等）に、発信者を特定して警告等を行う目的で、自己が保有する通信履歴などから発信者を探知すること。

いったん記録した通信履歴は、記録目的の達成に必要最小限の範囲内で保存期間を設定し、保存期間が経過したときは速やかに通信履歴を消去（通信の秘密に該当する情報を消去することに加え、該当しない部分について個人情報の本人が識別できなくすることを含む。）しなければならない。また、保存期間を設定していない場合であっても、記録目的を達成後は速やかに消去しなければならない。

保存期間については、提供するサービスの種類、課金方法等により電気通信事

業者ごとに（※１）、また通信履歴の種類ごと（※２）に異なり得るが、業務の遂行上の必要性、保存を行った場合の影響、社会環境の変化（※３）等も勘案し、その趣旨を没却しないように限定的に設定すべきである。

ただし、刑事訴訟法第197条第3項及び第4項に基づく通信履歴の電磁的記録の保全要請等法令の規定による場合その他特別の理由がある場合には、当該理由に基づく保存期間が経過する前の間、保存し続けることが可能である。また、自己又は第三者の権利を保護するため緊急行為として保存する必要がある場合は、その必要性が解消されるまでの間、保存することが可能である。

（※１）SNSやインターネット上の掲示板等のサービスを提供する事業者（いわゆる「コンテンツプロバイダ」。以下「CP」という。）とインターネット接続サービス提供事業者（いわゆる「アクセスプロバイダ」。以下「AP」という。）では、提供するサービスの内容等に違いがあることから、各サービスの内容に応じた業務の遂行上必要な範囲で、通信履歴の保存期間を設定することが考えられる。

（※２）例えば、通信履歴のうち、APが保有するインターネット接続サービスにおける接続認証ログ（利用者を認証し、インターネット接続に必要となるIPアドレスを割り当てた記録）の保存については、利用者からの契約、利用状況等に関する問合せへの対応やセキュリティ対策への利用など業務上の必要性が高いと考えられる一方、利用者の表現行為やプライバシーへの関わりは比較的小さいと考えられることから、電気通信事業者がこれらの業務の遂行に必要とする場合、一般に6か月程度の保存は認められ、適正なネットワークの運営確保の観点から年間を通じての状況把握が必要な場合など、より長期の保存をする業務上の必要性がある場合には、１年程度保存することも許容される。

（※３）社会環境の変化として、CPが提供するSNSやインターネット上の掲示板等における誹謗中傷をはじめとする違法・有害情報の流通の高止まりを背景として、特定電気通信による情報の流通によって発生する権利侵害等への対処に関する法律（平成13年法律第137号）が相次いで改正されている。また、SNSやインターネット上の掲示板等で著しく高額な報酬の支払いを示唆するなどして犯罪の実行者を募集する投稿等が掲載され、そのような投稿等に接して実際に犯行に及んだ者もいるなど、違法情報の流通が社会問題となっている。

CPについては、上記社会環境の変化を勘案すれば、CPにおける違法・有害情報への対策の必要性が高まるとともに、社会的にも期待されているといえるから、自社サービス内で生じた誹謗中傷をはじめとする違法・有害情報への対策のために不可欠な情報である通信履歴を保存することは、発信者情報開示請求等に対して実効

的な対応をする上でも、必要である。これを踏まえると、CPが、誹謗中傷等の違法・有害情報に係る投稿への対応を行うという目的で、各CPのサービス内容に応じた業務の遂行上必要な通信履歴、例えば、アカウント情報、ログイン情報、投稿情報等について、必要な範囲内で保存することが考えられ、その保存期間は、少なくとも3～6か月程度とすることが社会的な期待に応える望ましい対応と考えられる。

また、APについても、その業務の過程でインターネット上の投稿等に関する発信者情報を保有しているところ、例えば、誹謗中傷をはじめとする違法・有害情報への対応には、通常、CPだけではなく、APが保有する通信履歴が必要不可欠であるなど、APも違法・有害情報への対応に重要な役割を果たしており、そのために不可欠な情報である通信履歴の保存をすることも社会的に期待されている。そのため、APにおいても、CP同様に、必要な範囲内で、接続認証ログの通信履歴を保存することが考えられ、その保存期間は、少なくとも3～6か月程度とすることが社会的な期待に応える望ましい対応と考えられる。

上記については、一般に電気通信事業法における通信の秘密との関係において許容されると考えられる。上記期間は、近年の社会環境の変化を踏まえたCP及びAPにおける通信履歴の保存期間として望ましい期間の目安であり、より長期の保存をする業務上の必要性があるとき（※2参照）には、これを超えた期間を設定することも許容されると考えられる。

参考資料

参考資料１

「通信ログ保存の在り方に関するワーキンググループ」構成員

（敬称略・五十音順）

【構成員】

（主査）鎮目 征樹 学習院大学法学部 教授
梅本 大祐 英知法律事務所 弁護士
小林 央典 ＴＭＩ総合法律事務所 弁護士
宍戸 常寿 東京大学大学院法学政治学研究科 教授
曽我部 真裕 京都大学大学院法学研究科 教授
巽 智彦 東京大学大学院法学政治学研究科 准教授
森 亮二 英知法律事務所 弁護士

【オブザーバー】

警察庁 刑事局 捜査支援分析管理官
警察庁 サイバー警察局 サイバー企画

参考資料２

通信ログ保存の在り方に関するワーキンググループ　検討過程

会合	開催日	主な議題
第１回	令和７年 ３月 26 日	○　ヒアリング ・ ソフトバンク株式会社 ・ 楽天モバイル株式会社 ・ 株式会社 IIJ
第２回	令和７年 ３月 27 日	○　ヒアリング ・ 株式会社 NTT ドコモ ・ KDDI 株式会社 ・ NTT ドコモビジネス株式会社
第３回 （※１）	令和７年 ４月 11 日	○　ヒアリング ・ Meta
第４回 （※２）	令和７年 ４月 14 日	○　ヒアリング ・ TikTok ・ X
第５回 （※３）	令和７年 ４月 18 日	○　ヒアリング ・ Google ・ LINE ヤフー
第６回	令和７年 ６月６日	○　ヒアリング(発信者情報開示の観点) ・ 高橋参考人 ・ 長瀬参考人 ○　ヒアリング(捜査の観点) ・ 警察庁
第７回	令和７年 ６月 27 日	○　通信ログ保存の在り方に関する意見交換

※1　デジタル空間における情報流通の諸課題への対処に関する検討会（第 4 回）・デジタル空間における情報流通に係る制度ワーキンググループ（第 5 回）・ICT サービスの利用環境の整備に関する研究会 通信ログ保存の在り方に関するワーキンググループ（第 3 回）合同会合

※2　デジタル空間における情報流通の諸課題への対処に関する検討会（第 5 回）・デジタル空間における情報流通に係る制度ワーキンググループ（第 6 回）・ICT サービスの利用環境の整備に関する研究会 通信ログ保存の在り方に関するワーキンググループ（第 4 回）合同会合

※3　デジタル空間における情報流通の諸課題への対処に関する検討会（第 6 回）・デジタル空間における情報流通に係る制度ワーキンググループ（第 7 回）・ICT サービスの利用環境の整備に関する研究会 通信ログ保存の在り方に関するワーキンググループ（第 5 回）合同会合

利用者情報に関するワーキンググループ

第１章　検討の背景

１　これまでの検討

「スマートフォン プライバシー イニシアティブ（SPI）」は、スマートフォンの普及に伴い、スマートフォンアプリ等により取得・蓄積された利用者情報（アドレス帳、位置情報等）が、本人の意図しない形で外部送信されている事案が発覚、社会問題化したことを踏まえ、アプリ提供者等の関係事業者が利用者情報を適正に取り扱う上で実施することが望ましい事項について、総務省において平成 24 年に取りまとめられ、平成 25 年及び平成 29 年に改定された。

その後、国内制度の改正や諸外国及び民間事業者の動向に変化が生じていること等を踏まえ、令和６年３月から、「ICT サービスの利用環境の整備に関する研究会」（座長：宍戸　常寿　東京大学大学院　法学政治学研究科教授）（以下「研究会」という。）の下で開催される「利用者情報に関するワーキンググループ」（主査：山本　龍彦　慶應義塾大学大学院　法務研究科教授）（以下「本ワーキンググループ」という。）において、約７年ぶりに SPI の見直しについて議論を行い、同年 11 月、ダークパターンの回避やセキュリティの確保等について新たに規定した「スマートフォン プライバシー セキュリティ イニシアティブ（SPSI）」が取りまとめられた[46]。

２　「今後検討を深めていくべき事項」

令和６年 11 月開催の第４回研究会で SPSI の取りまとめが行われた際、以下のとおり、「今後検討を深めていくべき事項」として、（１）SPSI の対象スコープ、（２）青少年保護、（３）位置づけが示され、本ワーキンググループにおいて速やかに議論を進めることとされた。

---

[46] 総務省，利用者情報に関するワーキンググループ報告書（案）及び 不適正利用対策に関するワーキンググループ報告書（案）についての意見募集の結果の公表，別紙２，P28～62　https://www.soumu.go.jp/main_content/000979523.pdf

資料18－1　**SPSIについて今後検討を深めていくべき事項**

令和6年11月29日開催の第4回親会において、スマートフォン・プライバシー・セキュリティ・イニシアティブ（SPSI）について、今後の課題（WG報告書第３章）とされた、SPSIの対象スコープに関する課題のほか、パブリックコメントにおいて寄せられた意見を踏まえ、今後、以下の事項について検討を深めることとされた。

（１）SPSIの対象スコープ

①デバイス

スマートフォンとそれ以外のデバイスにおける利用者情報の取扱いについて、どのような点が共通し、又は異なるか等について調査等を行った上で対象スコープを議論すべきではないか。

②ウェブサイト

アプリケーションとウェブサイトとで取得する利用者情報の取扱いに差異があるか等について調査等を行い、関係事業者やウェブサイト運営者に対する説明やヒアリング等の必要な対応を行った上で、ウェブサイトを対象とするべきか検討すべきではないか。

（２）青少年保護

スマートフォンの低年齢からの利用が進んでおり、こどもの発達段階に対応した配慮を要することから、青少年保護の観点から取り組むべき事項、望ましい事項について検討すべきではないか。

（３）位置づけ

SPSIは、法令から一歩進んだベストプラクティスとして、関係事業者等の望ましい対応を記載しているところ、その望ましいとされる度合いについて整理して構造的に示すことを検討すべきではないか。

図１　SPSI について今後検討を深めていくべき事項[47]

上記（１）～（３）の事項について検討を深めるため、本ワーキンググループに新たに構成員・オブザーバを追加[48]した上で、昨年 12 月から SPSI の見直しに関する議論を行った。

[47] 総務省，利用者情報に関するワーキンググループ（資料 18－1）（総務省）より抜粋 https://www.soumu.go.jp/main_content/000983132.pdf

[48] 構成員として、LM 虎ノ門南法律事務所 上沼紫野弁護士、オブザーバとして、森・濱田松本法律事務所 蔦大輔弁護士、日本スマートフォンセキュリティ協会 仲上竜太技術部会長、早稲田大阪高等学校 米田謙三教諭の 3 名を本ワーキンググループに追加した。

第２章　スマートフォン プライバシー セキュリティ イニシアティブの改定

１　青少年保護

近年、青少年（18 歳未満）によるスマートフォン等の利用によるインターネット利用率が９割以上となるなど、スマートフォンの青少年への普及が進み、利用の長時間化や低年齢化も顕著である。また、SNS 等でプライバシーに係る情報の流出等を契機として青少年が被害に遭う事例も多く見られる。

このため、青少年のスマートフォンの安全・安心な利用に関して、SPSI における青少年保護の検討の必要性があると考えられるところ、SPSI に青少年保護を含めることについて、構成員や経済団体から以下のような意見があった。

（構成員等からの意見）

・ SPI の目的がスマートフォンアプリの安心安全であることを前提とすれば、利用者情報だけではなくセキュリティや青少年保護が入ってくるのは、普通の話ではないか。構成員等を拡大した WG の場で検討し、ベストプラクティスとして SPSI を出すことは、特に一覧性という観点から意味があるのではないか。【森構成員(第 20 回)】

・ 利用者情報の保護や取扱いの適正化に関する指針の中で、青少年保護に係る事項を盛り込むことは、SPSI の本来の目的や趣旨から離れてしまうため、違和感がある。【新経済連盟(第 20 回)】

・ 青少年のスマホ利用について、有害コンテンツ、犯罪に巻き込まれるリスク、中毒性、適正な利用時間管理、過大な課金など様々なリスクがあるが、全体を俯瞰しつつ SPSI で何をどこまで行うのか構造的に考えていく必要がある。【寺田構成員（第 21 回)】

・ 現実の必要性から見て、青少年保護を SPSI に含めることは賛成だが、他方で、SPSI の守備範囲との関係で、どこまで広げられるかは慎重に議論すべきでないか。無限定に広げるのではなく、これまでの SPSI の趣旨や目的とのつながりを重視すべきではないか。【山本主査（第 21 回)】

上記の議論を踏まえ、SPSI において青少年のスマートフォン利用に関する様々なリスクに網羅的に対応するのではなく、青少年の利用者情報やプライバシーの保護を通じて、青少年によるスマートフォンアプリ及び関連

サービスの安全・安心な利用を図るため、それに資する機能や仕組みの適切な提供を含む環境整備に関し、各事業者が取り組むことが望ましい事項を検討することとした。

上記の考え方に基づき、アプリ提供者、アプリストア運営事業者、OS 提供事業者のそれぞれが、青少年の利用者情報やプライバシーの保護の観点から実施することが望ましい事項について検討した結果、概要以下の内容を SPSI に追記することとした。

（アプリ提供者）

- 自ら提供する、青少年と他の利用者の交流などが発生するアプリにおいて、青少年保護の観点から不適切と考えられるコンテンツを報告する機能を備えるなど迅速に対応できる体制、ユーザーが不適切な言動を行うユーザーをブロックする機能などを備えること
- 自ら提供するアプリにおいて、青少年保護の観点から利用者情報の提供や課金の実施などのうち重要な判断が必要になる場合に、保護者の関与に関する仕組みや機能を備えること

（アプリストア運営事業者）

- 運営するアプリストアに掲載する個別のアプリに関して審査を行うこと。当該審査を行う場合には、年齢制限設定（レーティング）に関する基準を設定し、適切な年齢制限設定が行われるよう確認すること
- アプリストアへのアプリの登録審査について、その基準を作成し、あらかじめ公表するとともに、アプリの掲載を拒否する場合には、その理由について、アプリ提供者に対して迅速かつ適切なフィードバックを行うこと
- 運営するアプリストア内に青少年向けアプリを集めた専用の分類を設けること

（OS 提供事業者）

- アプリストア運営事業者において上記の事項が実施されているか必要な確認を行うとともに、適切な措置を講ずること
- 上記の措置に関して、アプリストア運営事業者に適切な説明及び情報提供を迅速に行うこと
- 個別のアプリに関して審査を行う場合には、その基準を設定し、あらかじめ公表するとともに、アプリの掲載を拒否する場合には、その理由について、アプリ提供者に対して迅速かつ適切なフィードバックを行うこと
- アプリストアにおける個別のアプリのダウンロード及び起動の可否、アプリス

トアの利用制限並びに、アプリストア及び外部ウェブサイトにおける利用者情報の提供及び課金に対する制限等を行うペアレンタルコントロール機能を実施するために必要な役務を提供すること

なお、複数の構成員から、利用者が青少年であるかどうか判別するためにはスマートフォン上で年齢確認が必要と考えられるところ、関係事業者が実施する取組として SPSI に記載するのかどうかについて明確にすべきとの意見が提示された。

（構成員からの意見）

・ 年齢確認についてどう考えるのか。責任を持って行う主体はどこか。【上沼構成員、生貝構成員、太田構成員ほか（第 21 回）】

上記の意見を踏まえ、アプリストア運営事業者による年齢制限設定に関する記載への注釈の中で、年齢制限の設定が適切に機能するためには、年齢等の発達段階が適切に把握されることが重要である旨指摘し、今後の技術的手段の発達や市場の状況を踏まえ、検討を行う旨記載している。

２　位置づけ

SPSI は、スマートフォンアプリの利用者情報の適正な取扱いに関し、法令から一歩進んだベストプラクティスとして、関係事業者が取り組むことが望ましい事項を定めたものであり、それ自体に法的拘束力はないと位置付けられている。他方、SPSI において関係事業者が対応することが望ましいとされている事項について、すべて「～～することが望ましい」と記載されており、令和６年 11 月の報告書において、望ましいとされる度合いについて整理して構造的に示すことが検討課題とされてきた。

まず、本ワーキンググループにおいて、「先進的事項」（利用者情報等の保護を高いレベルで確保する先進的な取組）、「望ましい事項」（利用者情報等の保護のため、より多くの関係事業者が取り組むことが望ましい事項）、「義務的事項」（国内法令上義務とされている事項又は利用者情報の保護に関する基本的な事項）の３分類に分けるイメージについて議論を行ったところ、構成員から以下の意見があった。

（構成員等からの意見）

・ 「義務的事項」について義務と義務的に分かれてしまう部分があるので、明確に書き分けたほうがよい。【寺田構成員（第 18 回）】

・ 公法的規制があれば義務的であり、プライバシー侵害は判断なので、必ず法令

の要求だとは言えないが、プライバシー侵害は「望ましい事項」で、あとはOS事業者によって達成されているものも「望ましい事項」と整理し、「先進的事項」「望ましい事項」「義務的事項」の区別をするのがいいのではないか。【森構成員（第18回）】

- ３段階の分類については、理論的には４段階もあり得るのではないか。「望ましい事項」をプリファードとストロングリープリファードに分け、後者について我々がどれぐらい強く望んでいるのかという主観的期待を込めた量的な概念を盛り込むことは、事業者に対して過度なプレッシャーにならないのではないか。【江藤構成員（第18回）】
- ストロングリープリファードはあり得るのではないか。特にこどもの利用者情報やダークパターンは、欧州はもとより、米国と比較しても、我が国に法規制がないのが不思議な状況。そこを特に望ましい事項として打ち出していく必要があるのではないか。【生貝構成員（第18回）】
- サイバーセキュリティ対策を行う上で、これだけは絶対やっておくべきといった基本的なものはある程度挙げることができるが、それ以外は、いろいろな脅威に対するいろいろな対策があり、リスクベース・アプローチにならざるを得ないという側面がある。【蔦オブザーバ（第18回）】

上記の議論を踏まえ、国内法令で義務付けられている事項と国内法令に準じた形での取扱いが強く求められる事項を区分する観点から、以下のとおり、「ベンチマーク事項」、「望ましい事項」、「基本的事項」、「法令事項」の４つに分類することとした。また、関係事業者が参照しやすいように、今回新たに追記された青少年保護の記載を含め、SPSI全体で同一の４つの分類を採用することとし、SPSIの本文における各事項に分類名を表示するとともに、分類ごとに文末の表現を使い分けることとした。

分類名	内容	文末の表現
ベンチマーク事項	利用者情報の適正な取扱い、セキュリティ確保及び青少年保護のための先導的取組として参照される事項	「～することが期待される」
望ましい事項	国内法令上の義務は必ずしもないが、利用者情報の適正な取扱い、セキュリティの確保及び青少年の保護のために望ましい（強く期待される）事項	「～することが望ましい」
基本的事項	国内法令に準じた形での取扱いが強く求められる事項	「～することが強く求められる」
法令事項	国内法令（個人情報保護法、電気通信	「～しなければな

	事業法等）上の義務とされている事項	らない」「～してはならない」

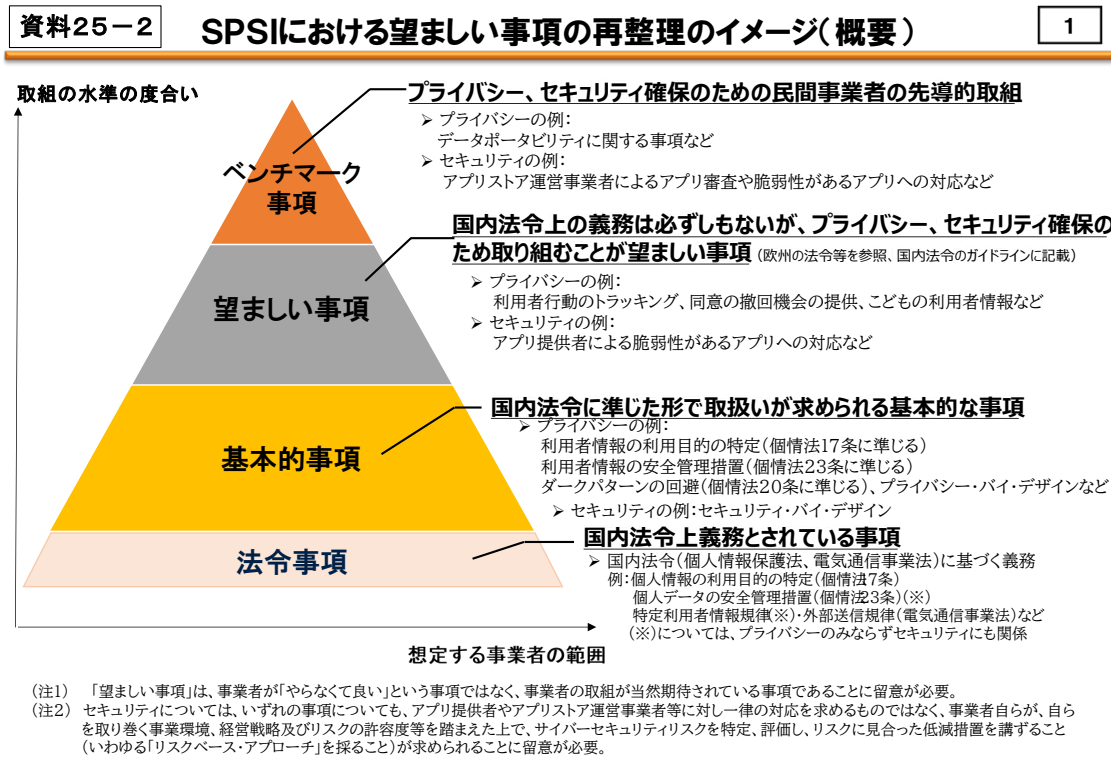


図２　SPSI における望ましい事項の再整理のイメージ（概要）[49]

一方で、セキュリティの確保に係る取組については、上記の議論を踏まえ、アプリ提供者やアプリストア運営事業者等に対して一律の対応を求めるものではなく、事業者自らが、自らを取り巻く事業環境、経営戦略及びリスクの許容度等を踏まえた上で、サイバーセキュリティリスクを特定・評価し、リスクに見合った低減措置を講ずること（いわゆる「リスクベース・アプローチ」を採ること）が求められる旨、明記することとした。

なお、４つの分類のうち、「法令事項」や「基本的事項」は国内法令との関係から整理したものである一方、「望ましい事項」は国内法令上の義務は必ずしもないものであるが、「望ましい事項」は諸外国の制度及び民間事業者の取組を踏まえて策定された、取り組まれることが強く期待されている事項であることについて、関係事業者は留意することが必要である。

[49] 総務省，利用者情報に関するワーキンググループ（資料 25－２）（総務省）より抜粋 https://www.soumu.go.jp/main_content/001011308.pdf

また、今回の見直しにおいてベンチマーク事項に整理された事項の数は多くないが、今後の技術動向や関係事業者における自主的な取組等を踏まえ、今後の見直しにおいてベンチマーク事項を追加することにより、関係事業者の利用者情報の保護、セキュリティの確保及び青少年保護に対する意識を更に醸成していくことが重要である。

上記のような本ワーキンググループにおける議論を踏まえ、別添のとおり、新たに青少年保護に関する取組を追加し、関係事業者の取組について望ましい度合いに応じて整理したSPSI改定案を取りまとめた。

第３章　今後の検討課題

１　ウェブサイトに係る調査・検討

現行のSPSIは、スマートフォンアプリの利用者情報の適正な取扱いに関して記載しており、利用者がスマートフォンやPCからブラウザを通じて閲覧するウェブサイトにおける利用者情報の取扱いについては対象に含んでいない。令和６年11月の報告書では、「アプリケーションとウェブサイトとで取得する利用者情報の取扱いに差異があるか等について調査等を行い、関係事業者やウェブサイト運営者に対する説明やヒアリング等の必要な対応を行った上で、次回以降の改定において、ウェブサイトを対象とするべきか、改めて検討することが適当である」とされており、アプリとウェブサイトにおける利用者情報の取扱いに係る差異について調査を行った上で、SPSIにおけるウェブサイトの取扱いについて検討を行った。

資料18－2　**ウェブサイトに関する検討の進め方（案）**

ウェブサイトへの対象拡大に関する検討については、WG報告書において「アプリケーションとウェブサイトとで取得する利用者情報の取扱いに差異があるか等について調査等を行い、関係事業者やウェブサイト運営者に対する説明やヒアリング等の必要な対応を行った上で、次回以降の改定において、ウェブサイトを対象とするべきか、改めて検討することが適当である。」とされている。

考え方

- SPSIは、スマホアプリの利用者情報の適正な取扱いに関して記載しており、スマホやPCからブラウザを通じたウェブサイト閲覧の際の利用者情報の取扱いについては対象に含んでいない。
- ウェブサイトへの対象拡大に関する検討の準備として、まずは、例えば以下のような事項について調査し、ヒアリング等も踏まえた上で、一定の整理を行っていくこととしてはどうか。

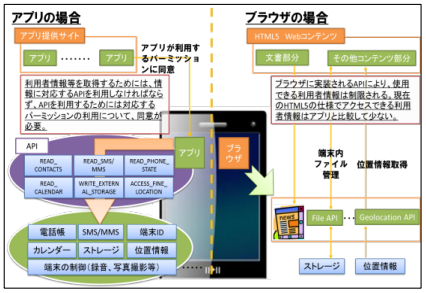
調査する事項（例）

アプリケーションとブラウザの間で、

- **利用者情報を取得する主体**にどのような差異があるか。
- **取得する利用者情報の種類**にどのような差異があるか。
- **取得する利用者情報の利用目的**や**取扱い方法**にどのような差異があるか。

→ウェブサイトを対象とするとした場合、SPSIと同じ内容が関係事業者に適用される場合とそうでない場合があるのではないか。

（参考）SPI策定当時（2012年）

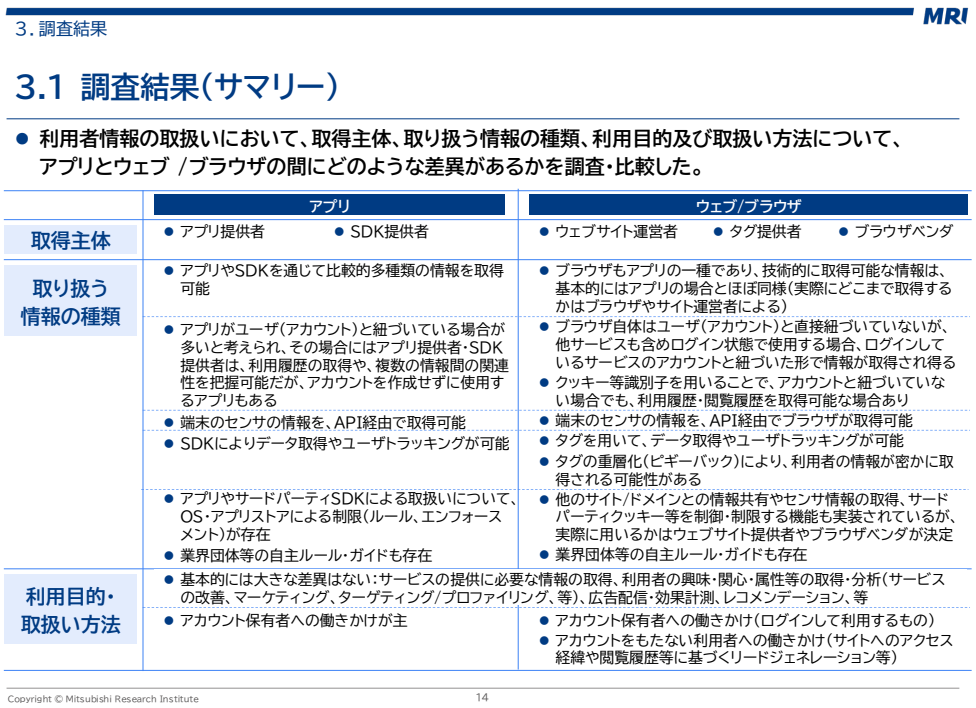


「スマートフォン プライバシー イニシアティブ」（平成24年８月）P74
図表5-3 アプリケーション及びブラウザがアクセス可能な情報等の違い

図３　ウェブサイトに関する検討の進め方[50]

アプリとウェブサイトにおける利用者情報の取扱いに係る差異について、（株）三菱総合研究所が行った調査によれば、ブラウザもアプリも技術的に取得可能な情報については基本的にほぼ同様（実際にどこまで取得するかはブラウザやウェブサイト運営者による）であるとともに、利用目的については、サービスの提供に必要な情報の取得、利用者の興味・関心・属性の取得・分析、広告配信・効果測定等であり、大きな差異がないことが確認された。

[50] 総務省，利用者情報に関するワーキンググループ（資料 18－２）（総務省）
https://www.soumu.go.jp/main_content/000983133.pdf



3. 調査結果

MRI

3.1 調査結果(サマリー)

- 利用者情報の取扱いにおいて、取得主体、取り扱う情報の種類、利用目的及び取扱い方法について、アプリとウェブ /ブラウザの間にどのような差異があるかを調査・比較した。

	アプリ	ウェブ/ブラウザ
取得主体	● アプリ提供者　● SDK提供者	● ウェブサイト運営者　● タグ提供者　● ブラウザベンダ
取り扱う情報の種類	● アプリやSDKを通じて比較的多種類の情報を取得可能	● ブラウザもアプリの一種であり、技術的に取得可能な情報は、基本的にはアプリの場合とほぼ同様(実際にどこまで取得するかはブラウザやサイト運営者による)
	● アプリがユーザ(アカウント)と紐づいている場合が多いと考えられ、その場合にはアプリ提供者・SDK提供者は、利用履歴の取得や、複数の情報間の関連性を把握可能だが、アカウントを作成せずに使用するアプリもある	● ブラウザ自体はユーザ(アカウント)と直接紐づいていないが、他サービスも含めログイン状態で使用する場合、ログインしているサービスのアカウントと紐づいた形で情報が取得され得る ● クッキー等識別子を用いることで、アカウントと紐づいていない場合でも、利用履歴・閲覧履歴を取得可能な場合あり
	● 端末のセンサの情報を、API経由で取得可能	● 端末のセンサの情報を、API経由でブラウザが取得可能
	● SDKによりデータ取得やユーザトラッキングが可能	● タグを用いて、データ取得やユーザトラッキングが可能 ● タグの重層化(ピギーバック)により、利用者の情報が密かに取得される可能性がある
	● アプリやサードパーティSDKによる取扱いについて、OS・アプリストアによる制限(ルール、エンフォースメント)が存在 ● 業界団体等の自主ルール・ガイドも存在	● 他のサイト/ドメインとの情報共有やセンサ情報の取得、サードパーティクッキー等を制御・制限する機能も実装されているが、実際に用いるかはウェブサイト提供者やブラウザベンダが決定 ● 業界団体等の自主ルール・ガイドも存在
利用目的・取扱い方法	● 基本的には大きな差異はない:サービスの提供に必要な情報の取得、利用者の興味・関心・属性等の取得・分析(サービスの改善、マーケティング、ターゲティング/プロファイリング、等)、広告配信・効果計測、レコメンデーション、等	
	● アカウント保有者への働きかけが主	● アカウント保有者への働きかけ(ログインして利用するもの) ● アカウントをもたない利用者への働きかけ(サイトへのアクセス経緯や閲覧履歴等に基づくリードジェネレーション等)

図４　アプリとウェブサイトにおける利用者情報の取扱いに係る差異に関する調査結果[51]

[51] 総務省，利用者情報に関するワーキンググループ（参考資料 27－1）（(株）三菱総合研究所）より抜粋 https://www.soumu.go.jp/main_content/001016782.pdf

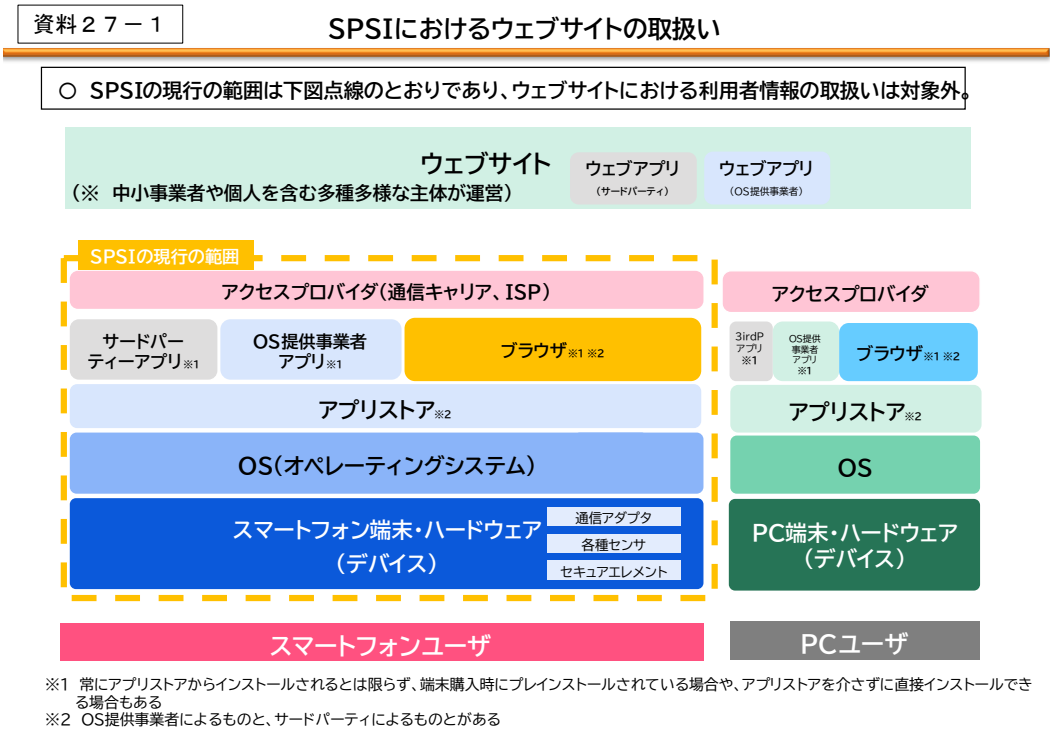


図５　SPSI におけるウェブサイトの取扱い [52]

当該調査結果や有識者等からのヒアリングを踏まえ、SPSI におけるウェブサイトの取扱いについて議論を行ったところ、構成員等から以下のとおり意見があった。

（構成員等からの意見）

- ブラウザもアプリの一種なので、アプリとブラウザで取得できる利用者情報にほぼ差はない。アプリと同様、ブラウザを通じたウェブサイトの閲覧でも利用者情報が第三者に外部送信されている。【太田構成員（第 26 回）】
- スマホ利用者はブラウザとアプリをそれほど意識的に区別して使っていないのではないか。【上沼構成員（第 26 回）】
- アプリとウェブの違いとは何か。ブラウザの中で閲覧できるコンテンツをウェブサイトとすると、ウェブアプリはどちらなのか。Webex もアプリ版とウェブ版があるが、ウェブ版はどちらなのか。【蔦オブザーバ（第 26 回）】
- SPSI の目的がスマホ利用者情報の安全安心であるならば、ウェブサイトの外部送信を除外するのは不合理。アプリによる第三者への外部送信とウェブサイトのタグによる第三者への外部送信は同じく扱われるべき。【森構成員（第 26

[52] 総務省，利用者情報に関するワーキンググループ（資料 27－1）（総務省）より抜粋 https://www.soumu.go.jp/main_content/001016664.pdf

回)】

- ウェブサイトとアプリにおける利用者情報の外部送信と利用者への影響についてほぼ差異はないと考える。もっとも、単に幅広く規制すれば良いということでもなく、関係者間での対話が重要ではないか。【呂構成員（第 26 回)】
- ウェブサイトは SPSI 以前から存在しており、種類や開設者も多種多様。SPSI のウェブサイトへの対象範囲の拡大について、どのような課題に対処するために何について誰を対象としたどのようなものかを議論すべきで、ウェブサイトに関する課題の解決手段が SPSI とは限らない。SPSI の内容が膨大になり関係事業者が参照しづらいものになることに懸念。【新経済連盟（第 26 回)】

２　今後の検討の方向性

従来、SPSI はスマートフォンのアプリを通じて収集される利用者情報に焦点を当てており、ウェブサイトの外部送信に関してウェブサイト運営者が取り組むことが望ましい事項の記載はない。なお、電気通信事業法における外部送信規律は、スマートフォンのアプリに係る外部送信のみならず、ウェブサイトに係る外部送信も規律の対象としている。

他方、ウェブサイトは、OS 事業者やアプリストア提供者による審査がない等、アプリとは構造が異なる上、中小企業や個人によるものも含め、日本におけるウェブサイトの数も相当数あると考えられ、法律に明確に規定されている事項を超えて、現在の SPSI の広範な事項をそのままウェブサイト運営者に求めることには実効性の観点を含め様々な課題があると考えられる。外部送信を含むウェブサイトの課題について、ウェブサイト運営者に対してどのような形でベストプラクティスを確保していくか、今後の課題として、SPSI との関係も含めて、速やかに検討を行うことが適当である。

３　その他の検討課題

このほか、令和６年 11 月の研究会報告書では、SPSI の対象スコープにスマートフォン以外のデバイス（例：タブレットやスマートウォッチ等）を含めることについて、「スマートフォンとそれ以外のデバイスにおける利用者情報の取扱いについて、どのような点が共通し、又は異なるか等について調査等を行った上で、次回以降の改定の際に議論することが適当である」とされているところ、引き続き検討を行うことが適当である。

参考資料

参考資料１

「利用者情報に関するワーキンググループ」構成員

（敬称略・五十音順）

【構成員】

	生貝　直人	一橋大学大学院　法学研究科　教授
	上沼　紫野	LM 虎ノ門南法律事務所　弁護士
	江藤　祥平	一橋大学大学院　法学研究科　教授
	太田　祐一	株式会社 DataSign　代表取締役社長
	木村　たま代	主婦連合会　常任幹事
	寺田　眞治	一般財団法人日本情報経済社会推進協会 客員研究員
	森　亮二	英知法律事務所　弁護士
（主査）	山本　龍彦	慶應義塾大学大学院　法務研究科　教授
	呂　佳叡	森･濱田松本法律事務所　弁護士

【オブザーバー】

個人情報保護委員会事務局

経済産業省

一般社団法人日本インタラクティブ広告協会

	蔦　大輔	森・濱田松本法律事務所　弁護士
	仲上　竜太	日本スマートフォンセキュリティ協会 技術部会部会長
	米田　謙三	早稲田摂陵高等学校　教諭

参考資料２

「利用者情報に関するワーキンググループ」開催状況

第１８回 （令和６年 12 月 20 日）	○SPSI の見直しについて ・事務局説明（ウェブサイト、望ましい事項の再整理、青少年保護等）
第１９回【非公開】 （令和７年２月 25 日）	○SPSI の見直しに関する事業者ヒアリング① ・事業者ヒアリング（Apple）
第２０回【非公開】 （令和７年２月 26 日）	○SPSI の見直しに関する事業者ヒアリング② ・事業者ヒアリング（モバイル・コンテンツ・フォーラム(MCF)、新経済連盟）
第２１回 （令和７年３月 10 日）	○SPSI の見直しについて ・事務局説明（望ましい事項の再整理、青少年保護） ・書面提出（Google LLC）
第２２回 （令和７年４月７日）	○SPSI の見直しについて ・事務局説明（望ましい事項の再整理、青少年保護）
第２３回 （令和７年４月 24 日）	○SPSI の見直しについて ・事務局説明（望ましい事項の再整理、青少年保護）
第２４回 （令和７年５月 19 日）	○利用者情報の取扱いに関するモニタリングについて ・事務局説明（モニタリングの観点）
第２５回 （令和７年５月 27 日）	○SPSI の見直しについて ・事務局説明（望ましい事項の再整理、青少年保護）
第２６回 （令和７年６月５日）	○SPSI の見直しに関する有識者・事業者ヒアリング③ ・有識者発表： 三菱総合研究所（アプリ・ウェブブラウザの比較）、 森構成員（SPSI とウェブサイトの外部送信） ・事業者ヒアリング（新経済連盟）
第２７回 （令和７年６月 24 日）	○SPSI の見直しについて（とりまとめ） ・事務局説明（SPSI 改定案、ウェブサイトの取扱い）

別添

スマートフォン プライバシー セキュリティ イニシアティブ

利用者情報に関するワーキンググループ

令和７年９月 10 日

1. スマートフォン利用者情報・セキュリティ取扱指針

（前文）

情報通信インフラとしてスマートフォンが急速に普及した中で、スマートフォン利用者のリテラシーのレベルの多様化が進んでいる。利用者に一定の自己責任が求められるとしても、利用者の不安を解消し、利用者が安全にスマートフォンを利用できるようにするためには、スマートフォンアプリケーションに係る関係事業者等が責任を持って、利用者情報の適正な取扱いに努める必要がある。具体的には、当該関係事業者等が個人情報保護やプライバシー保護の観点から利用者情報を適正に取り扱うとともに、利用者に分かりやすい説明を行い、利用者の理解及びそれを踏まえた選択を促すことが求められる。

また、スマートフォンにおける利用者情報の保護のためには、脆弱性があるアプリケーションや、不正なアプリケーションにおける利用者情報の取扱いに対する取組など、関係事業者等がスマートフォンアプリケーションにおけるセキュリティの確保に向けて適切な対応を取ることが求められる。

更に、近年、スマートフォンの青少年への普及が進み、利用の長時間化や低年齢化も顕著である。SNS 等でプライバシーに係る情報の流出等を契機として青少年が被害に遭う事例も多く見られることから、青少年のスマートフォンの安全・安心な利用に向けて、青少年が利用者情報の取扱いに関する情報を十分に得て適切に判断し行動することができるように、関係事業者等が青少年の発達段階に対応した支援を行うことが求められる[1]。

本指針は、法令上義務付けられてはいないものの、スマートフォンにおける利用者情報の適正な取扱い、セキュリティの確保及び青少年の保護のために実施することが求められる事項について、国内の関係法令[2]や諸外国の制度の動向、民間事業者における取組等を参考に取りまとめたものである。スマートフォンを巡っては、新たな技術・サービスが次々と出現し、利用者情報の適正な取扱いの観点から、今後新たな課題が生じることも考えられることから、本指針は随時見直しを行うこととする。

また、スマートフォンのサービス構造において、多様な関係事業者等がサービス提供や利用者情報の取扱い、セキュリティの確保及び青少年の保護に関わっており、本指針の目的を達成する上で、スマートフォンのアプリケーション提供者のみでは対応できる範囲が限られる場合があるため、アプリストア運営者・OS 提供事業者等の関係事業者等も連携し対応していくことが重要である。

---

[1] 本指針における青少年に関する記載は、青少年の利用者情報やプライバシーの保護を通じて、青少年によるスマートフォンアプリケーション及び関連サービスの安全・安心な利用を図ることを目的としている。

[2] 直近では、個人情報の保護に関する法律等の一部を改正する法律（令和２年法律第 44 号）により不適正利用の禁止や外国第三者提供時の情報提供の充実化等が規定されたほか、電気通信事業法の一部を改正する法律（令和４年法律第 70 号）により、特定利用者情報規律及び外部送信規律が導入されている。

1.1. 総則

1.1.1. 目的

- 本指針は、スマートフォンアプリケーションの利用者情報の適正な取扱い、セキュリティの確保及び青少年の保護に関し、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。）、プライバシーに関する判決、電気通信事業法（昭和 59 年法律第 86 号）、青少年が安全に安心してインターネットを利用できる環境の整備等に関する法律（平成 20 年法律第 79 号）、その他の関係法令等の趣旨を取り入れつつ、諸外国における制度の動向や、民間事業者におけるプライバシー保護に係る取組等も踏まえながら、スマートフォンアプリケーションに係る関係事業者等が取り組むことが求められる事項を定めたものである[3]。
- 本指針自体が法的拘束力を持つものではない（ただし、個別の法令によって義務付けられる事項（法令事項）を紹介した部分はあることに留意）が、関係事業者等がこれらの事項に取り組むことにより、次に掲げる事項を達成し、もって、スマートフォンにおけるイノベーションの継続的な創出や市場の中長期的な成長を促進し、利用者がスマートフォンやそれを通じて提供される利便性の高いサービスを安全・安心に利用できる環境を整備することを目的とする。
    ① 関係事業者等による関係法令等の遵守に資すること
    ② 利用者が自らの利用者情報の取扱いに関する情報を十分に得て、アプリケーションの利用に関し適切に判断し、行動することを支援すること

1.1.2. 4 つの分類について

- 本指針 1.2～1.5 で掲げる取組は、スマートフォンアプリケーションの利用者情報の適正な取扱い、セキュリティの確保及び青少年の保護について、関係事業者等の参考に資する観点から、取り組むことが求められる度合いに応じて、次の4つの分類により整理されている[4]。なお、各取組がどの分類に該当するかは、文末の【】に分類名を表示するとともに、以下のとおり分類ごとに文末の表現を使い分けている。

分類名	内容	文末の表現
ベンチマーク事項	利用者情報の適正な取扱い、セキュリティ確保及び青少年保護のための先導的取組として	「～することが期待される」

[3] 本指針は、スマートフォン上のアプリケーションについて関係事業者が取り組むことが求められる事項を定めたものであるが、ウェブサイトにおいて同様の利用者情報の取扱いが生じる場合があり、その関係事業者は本指針に定める事項を参考に対応を図ることが考えられる。

[4] ここにいう「ベンチマーク事項」、「望ましい事項」及び「基本的事項」は法的拘束力を有するものではないが、個人情報保護法及び電気通信事業法等の法令が適用される場合には、当該法令に従い対応する必要がある。

	参照される事項	
望ましい事項	国内法令上の義務は必ずしもないが、利用者情報の適正な取扱い、セキュリティの確保及び青少年の保護のために望ましい（強く期待される）事項	「～することが望ましい」
基本的事項	国内法令に準じた形で取扱いが強く求められる事項	「～することが強く求められる」
法令事項	国内法令（個人情報保護法、電気通信事業法等）上の義務とされている事項	「～しなければならない」、「～してはならない」

- なお、セキュリティについては、上記の「ベンチマーク事項」、「望ましい事項」及び「基本的事項」のいずれにおいても、アプリケーション提供者やアプリストア運営事業者等に対し一律の対応を求めるものではなく、事業者自らが、自らを取り巻く事業環境、経営戦略及びリスクの許容度等を踏まえた上で、サイバーセキュリティリスクを特定・評価し、リスクに見合った低減措置を講ずること（いわゆる「リスクベース・アプローチ」を採ること）が求められることに留意が必要である。

1.1.3. 定義

① 利用者情報

- 利用者の識別に係る情報、利用者の通信サービス上の行動履歴に関する情報、利用者の状態に関する情報等、スマートフォンにおいてスマートフォンの利用者の情報と結びついた形で生成、利用又は蓄積されている情報（電話帳等の第三者に関する情報を含む。）の総称。個人情報保護法における個人情報や、電気通信事業法における特定利用者情報を含む[5]。

（参考）

No.	情報の種類	具体例	適用される規律
(1)	通信の秘密に該当する情報で、個人情報でないもの	・電気通信役務の利用者である個人の通信の内容（特定の個人を識別することができるものを除く。） ・電気通信役務の利用者である法人の通信履歴	電気通信事業法
(2)	通信の秘密に該当する情報で、個人情報であるもの	・電気通信役務の利用者である個人の通信履歴（特定の個人を識別することができるものに限る。）	電気通信事業法 ＋個人情報保護法
(3)	電気通信事業法第27条の5第2号の情報で、個人情報でないもの	・電気通信役務の登録者を識別できるIDで、個別の通信に紐付かないもの（特定の個人を識別することができるものを除く。） ・電気通信役務の契約者データベースにある法人契約者名	電気通信事業法 【←令和4年改正法により追加】
(4)	電気通信事業法第27条の5第2号の情報で、個人情報であるもの	・電気通信役務の契約者データベースに含まれる契約者の登録情報（特定の個人を識別することができるものに限る。）	電気通信事業法 【←令和4年改正法により追加】 ＋個人情報保護法
(5)	電気通信事業法第27条の5第2号の情報でもなく、通信の秘密に該当する情報でもない、個人情報	・店頭で電気通信役務の利用者に対して行ったアンケートに記入された情報（氏名・住所等により分類整理されていないもの。特定の個人を識別することができるものに限る。）	個人情報保護法

なお、「具体例」欄に示している内容は、あくまでも一例であって、網羅的なものではありません。

② OS

- コンピュータシステム全体を管理するソフトウェアで、基本的な機能を提供するもの。

③ アプリケーション

- 通話やEメール等のコミュニケーションツール、ブラウザ、写真、ゲーム等の様々な機能をスマートフォンで実行するための利用者向けソフトウェア（OS を除く）。

④ アプリケーション提供者

- アプリケーションを提供する事業者又は個人。

⑤ アプリストア

- アプリケーションを提供するストアのことで、利用者はこのストアからアプリケーションをダウンロードする。

⑥ 情報収集モジュール[6]

- アプリケーションに組み込んで利用される一連のプログラムであって、利用者情報を取得するための機能を持つものをいう。

⑦ 情報収集モジュール提供者

- アプリケーション提供者に対し、情報収集モジュールを提供する事業者（当該事業者がアプリケーション提供者に当たる場合を除く。）。

⑧ アプリケーション提供者等

- アプリケーション提供者及び情報収集モジュール提供者の総称。

⑨ 関係事業者等

- スマートフォンをめぐるサービス提供に関係している事業者等。具体的には、アプリケーション提供者、情報収集モジュール提供者、アプリストア運営事業者、OS 提供事業者、移動体通信事業者、端末製造事業者、その他関係しうる事業者等（アプリケーション紹介サイト運営者、広告関係事業者等）のこと。

⑩ プライバシーポリシー

- 関係事業者等が個人情報保護又はプライバシー保護を推進する上での考え方や方針を明らかにする文書[7]。本指針においては、スマートフォンにおいて提供されるアプリケーションや情報収集モジュールについて、具体的な取得情報の項目、利用目的等を記載したものを想定している[8]。

⑪ 通知又は公表

- 「通知」は、書面（郵送等）、電子メール、口頭（電話等）等のいずれかの方法で個別に伝えること。「公表」は、官報・公報・新聞紙等への掲載、インターネット上での公表、パンフレットの配布、窓口等への書面の掲示・備付等のいずれかの方法により公にしておくこと（スマートフォンの場合、通知は書面、電子メールやアプリによるポップアップ等、公表はアプリケーション上又はウェブサイト等へのリンクを張ること等により行うことが想定される。）。

---

6 これには、分析ツール、広告ネットワークを含む。
7 「プライバシーポリシー」の名称でなくても、利用者情報の取扱いに関する方針を含む。
8 プライバシーポリシーについては、事業者単位で作成されるもの及びアプリケーション単位で作成されるものがあるところ、本指針においては、基本的にはアプリケーション単位で作成されるものを想定しているが、事業者単位で作成されるものも含まれる。

⑫ 個別の情報に関する同意取得[9]

- アプリケーション（組み込まれた情報収集モジュールを含む。以下同じ。）により取得される個別の情報（電話帳、位置情報等）について、取得や取扱いについて独立した形で同意を取得すること。[10]

⑬ ダークパターン

- サービスの利用者を欺いたり操作したりするような方法又は利用者が情報を得た上で自由に決定を行う能力を実質的に歪めたり損なったりする方法で、ユーザインタフェースを設計・構成・運営すること。

⑭ セキュリティ

- 「情報」と「機能」の両面において守るべき資産を脅威から保護すること。本指針においては、利用者情報へのアクセス管理等の対策によって利用者情報が利用者による同意の範囲内で適切に保護されている状態が達成されることや、スマートフォンの機能が利用者の操作やあらかじめの同意なく勝手に利用されてしまうことを防ぐこと。

【補足】

１．利用者情報の取得の有無による区別について

本指針の適用対象たるアプリケーション提供者及び情報収集モジュール提供者には、スマートフォンから利用者情報を自ら取得しない者も含まれる。これは、例えば、アプリケーション提供者がプライバシーポリシーを掲示等していない場合、アプリケーション提供者が利用者情報を取得していないためプライバシーポリシーを掲示等していないのか、利用者情報を取得しているにもかかわらずプライバシーポリシーを掲示等していないのかが不明であること、及び、アプリケーション提供者が利用者情報を取得しない場合であっても、情報収集モジュールにより利用者情報がスマートフォン外部に送信され情報収集モジュール提供者による取得となる場合があることなどに鑑み、利用者が自らの利用者情報の取扱いに関する情報を十分に得て、アプリケーションの利用に関し適切に判断し、行動することを支援するという本指針の趣旨に鑑みたためである。ただし、スマートフォンから利用者情報を自ら取得しない場合には、本指針の取得を前提とした箇所は、適用されない。

---

[9] 同意取得の方法について、個人情報保護法においては、「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によらなくてはならない」とされており（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）（平成 28 年 11 月策定。令和７年６月一部改正　個人情報保護委員会。以下「ガイドライン通則編」という。）2-16 参照。）、事案に応じて適切な同意取得の方法を検討する必要がある。プライバシー上の懸念が生じうる情報に係る同意取得においても、同様に、情報の性質等に鑑み事案に応じた検討が必要となる。

[10] アプリケーションに係るプライバシーポリシー等に基づき、アプリケーションの利用者情報の取得や取扱いについて一括して同意を取得するアプリケーションに関する同意取得とは異なることに留意が必要である。

２．「取得」について
　この指針の適用については、アプリケーション上において利用者本人が自ら利用者情報を提供するか、利用者情報が自動的にアプリケーションの外部に送信されるかにかかわらず、スマートフォン外部へのアプリケーション提供者等に対する利用者情報の送信があれば、通常、当該アプリケーション提供者等による取得があったといえる。

３．広告関係事業者について
　広告関係事業者は、その事業形態にもよるが、アプリケーション提供者又は情報収集モジュール提供者に当たる場合が多いと考えられる。

４．アプリケーション内のブラウザを通じて取得される利用者情報について
　スマートフォンの利用者情報については、アプリケーションの利用に伴い取得されるほか、当該アプリケーション内のブラウザでウェブサイトを利用する際に、当該アプリケーションの提供者により取得される場合があるため、本指針はアプリケーション内のブラウザを通じて利用者情報を取得する場合にも適用される。アプリケーション内のブラウザが表示するウェブサイトに Javascript タグ等を追加的に組み込むことで、利用者情報を取得する場合には、当該 Javascript タグ等についても、本指針における情報収集モジュールと同等に取扱うこととする。

1.1.4. 本指針の対象者

- 本指針は、アプリケーション提供者等を中心として、スマートフォン上の利用者情報の取扱い、セキュリティの確保及び青少年の保護に係るあらゆる関係事業者等において、それぞれの役割に応じた形で適用されることを想定している。なお、アプリストア運営事業者、OS 提供事業者、移動体通信事業者、端末製造事業者、その他関係しうる事業者等がアプリケーション又は情報収集モジュールを提供し、利用者情報を直接取得する場合、当該事業者等は、アプリケーション提供者又は情報収集モジュール提供者に該当し、それぞれの取組を行うものとする。

1.1.5. 基本原則

- スマートフォンにおける利用者情報の取扱い等について、アプリケーション提供者等は、次に掲げる基本原則に従うことが求められる。

① 透明性の確保

- 利用者情報の取得・保存・利活用・第三者提供・消去及び利用者関与の手段の詳細に

ついて利用者に通知し、又は容易に知りうる状態に置く。利用者に通知又は公表あるいは利用者の同意を取得する場合、その方法は、利用者がアプリケーションを利用する際の方法等を考慮して利用者が容易に認識かつ理解できるものとする。

② 利用者関与の機会の確保

- その事業の特性に応じ、その取得する情報や利用目的、第三者提供の範囲等必要な事項につき、利用者に対し通知又は公表あるいは必要な場合には同意取得を行う。また、利用者情報の取得停止や利用停止等の利用者関与の手段を提供することととする。これらの利用者関与の機会の確保に当たっては、利用者が容易に理解できる方法で情報提供を行うこととする。

③ 適正な手段による取得の確保[11]・不適正利用の禁止[12]

- 利用者情報を適正な手段により取得することとする。また、取得した利用者情報について、違法又は不当な行為を助長し、又は誘発するおそれがある方法で取り扱わないこととする。

④ 適切な安全管理の確保[13]

- 取り扱う利用者情報の漏えい、滅失又はき損の防止その他の利用者情報の安全管理のために必要・適切な措置を講じることとする。

⑤ 苦情相談への対応体制の確保

- 利用者情報の取扱いに関する苦情相談に対し適切かつ迅速に対応することとする。

⑥ プライバシー・バイ・デザイン／セキュリティ・バイ・デザイン

- 開発時から、利用者の個人情報やプライバシーが尊重され保護されるようにあらかじめ設計することとする。利用者の個人情報やプライバシーに関する権利や期待を十分認識し、利用者の視点から、利用者が理解しやすいアプリケーションやサービス等の設計・開発を行うこととする。
- 開発時から、セキュリティが適切に確保されるよう、アプリケーションの企画及び設計の段

---

11 個人情報取扱事業者は、偽りその他不正の手段により個人情報を取得してはならない【法令事項】（個人情報保護法第 20 条第 1 項）ことに留意が必要である。この点、「不正の手段」には、「偽り」のほかにも、不適法な又は適正性を欠く方法や手続も含まれ、具体的な判断については、事案ごとに同法その他の法令の趣旨や社会通念に委ねられると解されている（園部逸夫ほか『個人情報保護法の解説 第三次改訂版』（令和 4 年、ぎょうせい）161 頁）。

12 個人情報取扱事業者は、違法又は不当な行為を助長し、又は誘発するおそれがある方法により個人情報を利用してはならない【法令事項】（個人情報保護法第 19 条）ことに留意が必要である。

13 個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又はき損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない【法令事項】（個人情報保護法第 23 条）ことに留意が必要である。

階から、セキュリティの確保について検討し、適切な仕組みをアプリケーションに組み込むこと。

⑦ 特定の情報及び利用者の属性に応じた配慮

- 利用者本人に対する不当な差別、偏見その他の不利益が生じないよう特定の情報について適切な配慮を行うとともに、青少年の利用者情報については発達段階に応じた適切な対応を行う等、利用者の属性に応じ必要な対応を行い情報を適正に取り扱うこととする。

【補足】

個人情報保護法における個人情報への該当性等について

個人情報保護法において「個人情報」とは、「生存する個人に関する情報（※）であって」、「当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）」（法第２条第１項第１号）、又は「個人識別符号が含まれるもの」（同項第２号）をいう。

※本欄では生存する利用者に関する情報を想定する。

【単体で特定の個人の識別性がある場合】

スマートフォンからアプリケーション提供者等が取得する利用者情報に特定の個人の識別性がある場合、個人情報となる。例えば、電話帳においては、一般的に氏名と組み合わせた電話番号及びメールアドレス等、特定の個人の識別が可能な情報が登録される場合が多く、一般的に電話帳を取得すると個人情報を含む内容を取得することになると考えられる。契約者情報も、一般的に、氏名と組み合わせた住所等を含み特定の個人の識別が可能であるため契約者情報を取得すると個人情報として取り扱う必要があると考えられる。

【他の情報と容易に照合でき、それによって特定の個人の識別性を獲得する場合】

また、スマートフォンからアプリケーション提供者等が取得する利用者情報単体でみた場合に特定の個人の識別性がない場合であっても、取得した者が有している情報等、他の情報と容易に照合し特定の個人の識別性を獲得する場合には個人情報となる。例えば、電話番号、メールアドレス、契約者・端末固有 ID、ログイン ID 等が情報単体では特定の個人の識別性がない場合でも、契約者の氏名等個人情報と容易に照合することができる場合には特定の個人の識別性を獲得する。

また、ログインのための識別情報は、通常、単なる数字や記号等、それ単体では特定の個人の識別性を有しない。

上記の各 ID のいずれについても、それ自体にアルファベットの氏名を含む場合等、特定の個人の識別性を有することがある。

【行動履歴や利用履歴に関する情報】

行動履歴や利用履歴に関する情報としては、GPS や基地局・Wi-Fi アクセスポイント情報に基づく位置情報、通信履歴（通話内容・履歴、メール内容・送受信内容等）、ウェブサイト上の行動履歴等が蓄積される場合がある。また、アプリケーションの利用により蓄積される情報やアプリケーションの利用ログ、システムの利用に関するログ等が蓄積されることもある。これらは、それ自体で一般には特定の個人の識別性を有しないことが多いと考えられるが、長期間網羅的に蓄積した場合等において、態様によって特定の個人を識別可能となる結果、個人情報に該当する場合もある。移動履歴は、短期間のものでも、自宅、職場等の情報と等価になる場合がある。また、大量かつ多様なこれらの履歴の集積については、個人の人格と密接に関係する可能性が指摘される。

【図表 1：スマートフォンにおける利用者情報の性質と種類】

区分	情報の種類	情報の種類	利用者による 変更可能性	特定の個人の識別性等
第三者に関する情報	電 話 帳 で管理されるデータ	氏名、電話番号、メールアドレス等	×～△	電話帳には一般に氏名、電話番号等が登録されることが多く、特定の個人の識別性を有している場合が多い。
利用者の識別に係る情報	氏名、住所等の契約者情報	氏名、生年月日、住所、年齢、性別、電話番号等の情報や、クレジットカード番号等の個人信用情報等	×～△	契約者情報には一般に氏名、住所等が含まれており、特定の個人の識別性を有している場合が多い。
	ログインに必要な識別情報	各種サービスをネット上で提供するサイトにおいて、利用者を特定するためにログインさせる際に利用される識別情報	△～○ 利用者が必要に応じて変更・修正を行うことが可能	・ログインのための識別情報は変更可能な場合も有り。 ・ログインのための識別情報は、それ自体で氏名等、特定の個人の識別性を有する場合もある。単なる数字や記号等で単体では特定の個人の識別性を有さない場合もあるが、アプリケーション提供事業者等において他情報と容易に照合できる場合、特定の個人の識別性を有する。
	クッキー技術を用いて生成された識別情報	ウェブサイト訪問時、ブラウザを通じ一時的に PC に書込み記録されたデータ等	○ 利用者が必要に応じて消去することが可能	・利用者がブラウザ上で消去やオプトアウトを行うことが可能。 ・単体では特定の個人の識別性を有しないが、発行元等において他情報と照合し特定の個人の識別性を有する場合がある。
	契約者・端末固有 ID	OS が生成する ID（Android ID)、独自	×	・スマートフォンの OS やシステムプログラム、SIM

		端末識別番号（UDID）、加入者識別 ID（IMSI）、IC カード識別番号（ICCID）、端末識別 ID（IMEI）、MAC アドレス、Bluetooth Device Address 等	端末交換や契約変更をしない限り変更が困難	カード、端末そのもの等に割り振られ管理される。利用者は端末交換や契約変更をしない限り変更困難。 ・単体では特定の個人の識別性を有しないが、他の情報と容易に照合できる場合、特定の個人の識別性を獲得する可能性がある。 ・同一 ID に紐付けて行動履歴や位置情報を集積する場合、プライバシー上の懸念が指摘される。
	広告 ID	IDFA（Identifier For Advertisers）、AdID（Advertising ID）	○ 利用者が必要に応じて、許可・変更・修正を行うことが可能	・単体では特定の個人の識別性を有しない。他の情報と容易に照合できる場合、特定の個人の識別性を獲得する可能性がある。 ・利用者が OS 機能やその設定によって、各アプリケーションでのアクセスを個別にオプトイン又はオプトアウトすることが可能。
	ベンダーID	IDFV（Identifier for Vendor）、AppSetId	× オプトアウトの手段が提供されていないケースがある	・同じデバイス上で動作する同じベンダー（アプリケーション提供者）のアプリでは同じ値となる識別子。 ・単体では特定の個人の識別性を有しない。他の情報と容易に照合できる場合、特定の個人の識別性を獲得する可能性がある。
通信サービス上の行動履歴や利用者の状態に関する情報	通信履歴	通話内容・履歴、メール内容・送受信履歴	×～△ 端末や電気通信事業者のサーバーにおいて管理	・通信相手、記録の性質等により特定の個人の識別性を有する場合がある。 ・電気通信事業者の取扱い中のものは通信の秘密の保護の対象。 ・通信履歴はプライバシー上の懸念が指摘される。

	ウェブサイト上の行動履歴	利用者のウェブサイト上における閲覧履歴、購買履歴、検索履歴等の行動履歴	×～△ 端末やウェブサイト管理者、アプリケーション提供者等のサーバーにおいて管理	・利用者の行動履歴や状態に関する情報については、内容・利用目的等によりプライバシー上の懸念が指摘される。 ・蓄積された場合等、態様によって個人が推定可能になる可能性がある。
	アプリケーションの利用履歴等	アプリケーションの利用履歴・記録されたデータ等、システムの利用履歴等		
	位置情報	GPS 機器によって計測される位置情報、基地局に送信される位置登録情報、Wi-Fi ルータによって計測される位置情報、Bluetooth ビーコンによって計測される位置情報 [14]		
	写真・動画等	スマートフォン等で撮影された写真、動画等		・内容、利用目的等によりプライバシー上の懸念がある。 ・個人が判別できる写真・動画等は、個人情報に該当する。

14 「位置情報プライバシーレポート」https://www.soumu.go.jp/main_content/000434727.pdf

外国事業者について　近年は外国事業者によるアプリケーションや情報収集モジュールの提供が多く行われている。この点について、個人情報保護法第 171 条においては、個人情報取扱事業者、仮名加工情報取扱事業者、匿名加工情報取扱事業者又は個人関連情報取扱事業者が、国内にある者に対する物品又は役務の提供に関連して、国内にある者を本人とする個人情報、当該個人情報として取得されることとなる個人関連情報又は当該個人情報を用いて作成された仮名加工情報若しくは匿名加工情報を、外国において取り扱う場合についても、適用することとされている。

また、利用規約等において、専属的合意管轄裁判所を外国裁判所とし、準拠法を外国法としている場合においても、消費者である利用者からの訴訟提起の際や、不法行為に基づく請求の際には、日本の裁判所に国際裁判管轄が認められ、準拠法を日本国法とされる可能性がある。

したがって、外国事業者であっても、我が国においてサービスを提供する場合には、本指針を参照すべきである。

1.2. アプリケーション提供者等における取組

（アプリケーション提供者及び情報収集モジュール提供者）

1.2.1. アプリケーション提供者の取組

≪期待される役割≫

- アプリケーション提供者は、利用者情報を取得する場合、自身の利用者情報の取扱いに責任を負うことが強く求められる【基本的事項】。
- アプリケーション提供者は、アプリケーションを提供する場合において、当該アプリケーションによる情報の取得等について明確かつ適切に定めたプライバシーポリシーを公表することが強く求められる【基本的事項】。
- アプリケーションに組み込む情報収集モジュールに関しても、自己の意思で組み込み、情報収集モジュールから利益を得ている場合もあることから、情報収集モジュールの組み込みにあたって上記の点に十分に配慮するとともに、情報収集モジュールの透明性の確保や利用者関与の機会を確保することができるよう、情報収集モジュール提供者と協力することが強く求められる【基本的事項】。
- 利用者情報を取得しないアプリケーション提供者においても、利用者に対し、利用者情報を取得していない旨等を、あらかじめ通知又は公表することが望ましく【望ましい事項】、また、そのアプリケーションに組み込まれた情報収集モジュールにより利用者情報の取得が行われる場合は、その旨をあらかじめ通知又は公表し、オプトアウトの機会を提供することが強く求められる【基本的事項】。

≪具体的な取組内容≫

1.2.1.1. プライバシーポリシーの作成[15]

- アプリケーション提供者は、個別のアプリケーションについて、以下の①から⑩までの事項について明示するプライバシーポリシーをアプリケーションごとに日本語であらかじめ作成し[16]、利用者が容易に参照できる場所に掲示又はリンクを張ることが強く求められる[17]【基本的事項】。

---

15 メッセージ媒介サービス、SNS、検索サービス、ホームページの運営等の対象となる電気通信役務を営んでいる電気通信事業者は、外部送信規律を遵守しなければならない【法令事項】（電気通信事業法第27条の12）ことに留意が必要である。詳細については、1.2.1.7.を参照すること。

16 一のプライバシーポリシーに、複数のアプリケーションについてまとめて記載する場合であって、アプリケーションごとに取得・利用する情報が異なる場合には、取得・利用する情報の内容や利用目的等について、アプリケーションごとに分けて記載することが求められる。

17 個人情報取扱事業者は、保有個人データに関し、以下の①～⑤について本人の知り得る状態に置かなければならない（本人の求めに応じて遅滞なく回答する場合を含む。）【法令事項】（個人情報保護法第32条）ことに留意が必要である。

① 当該個人情報取扱事業者の氏名又は名称及び住所並びに法人にあっては、その代表者の氏名

① アプリケーション提供者の氏名又は名称及び連絡先等

- アプリケーション提供者の氏名又は名称及び連絡先等を記載することが強く求められる【基本的事項】。

② アプリケーション提供者が取得する利用者情報の項目等

- アプリケーション提供者が利用者情報を取得する場合に、スマートフォン外部への送信等により取得する旨を記載するとともに、その取得する利用者情報の項目・内容を列挙することが強く求められる [18][19]【基本的事項】。また、アプリケーション提供者が利用者情報を取得しない場合は、その旨を記載することが望ましい【望ましい事項】。
- アプリケーション提供者は、アプリケーションの主要な機能に関係する情報にのみアクセスする、アプリケーションの実行に必要な情報に限って収集及び使用する等、利用者情報の取扱いは、その利用目的との関係において適切で関連性があり、かつ、必要最小限の範囲とすることが強く求められる【基本的事項】。

③ アプリケーション提供者による取得方法

- アプリケーション提供者が利用者情報を取得する場合に、利用者の入力によるものか、アプリケーションがスマートフォン内部の情報を自動取得するものなのか等取得方法を明確に示すことが望ましい【望ましい事項】。

④ 利用目的の特定・明示

- アプリケーション提供者が利用者情報を取得する場合に、利用者情報を、アプリケーション自体の利用者に対するサービス提供（提供するサービス概要を簡単に記載する等）のために用いるのか、広告配信・表示やマーケティング目的のために取得するのか、それら以外の目的のために用いるのかを明確に記載することが強く求められる【基本的事項】。
  - アプリケーション自体が利用者に提供するサービス以外の目的のために利用する場合については、利用者が利用目的や利用方法を容易に想定できないことから、利用目的と取得する利用者情報の項目の関係について丁寧な説明を行うことが望ましい【望ましい事項】。

---

② 全ての保有個人データの利用目的
③ 保有個人データの利用目的の通知の求め又は開示等の請求に応じる手続及び保有個人データの利用目的の通知の求め又は開示の請求に係る手数料の額
④ 保有個人データの安全管理のために講じた措置
⑤ 保有個人データの取扱いに関する苦情の申出先

[18] その際、利用者への影響が大きいと考えられるものから順に記載するなど、利用者が理解しやすい方法で記載することが求められる。

[19] 例えば、プロファイリングにより利用者を分類する場合において、利用者が本人の分類の状況を確認できるようにすることは、利用者情報の取扱いの予測・想定に資すると考えられる。

- 広告配信・表示やマーケティング目的のために利用者情報の取得を行う場合には、適切にその目的を明示することが強く求められる【基本的事項】。利用者に対してターゲティング広告等の配信を行う場合にはその旨記載することが強く求められる【基本的事項】。
- 利用者に関する行動・関心等の情報を分析するいわゆるプロファイリング[20]を行う場合には、どのような取扱いが行われているかを利用者が予測・想定できる程度に利用目的を特定するとともに、かかる分析処理を行うことを含めて利用目的を特定することが強く求められる[21]【基本的事項】。
- 現段階では利用目的が明確ではなく、将来的な活用を見込んで利用目的の範囲を定めず様々な利用者情報を取得することは、必ずしも利用目的が特定されているとはいえないため、想定される利用目的の範囲をできるだけ特定し利用者に通知又は公表あるいは同意取得をした上で、その範囲で情報を取得し取り扱うことが強く求められる【基本的事項】。

⑤ 第三者提供、外国の第三者に対する提供、共同利用及び情報収集モジュールに関する記載事項

［第三者提供に関する記載事項］[22]

- アプリケーション提供者が取得した利用者情報を第三者提供する場合（第三者が当該情報にアクセスする権限を付与する場合を含む。）、第三者への提供を利用目的とすること及び第三者に提供される利用者情報の項目等を明確にプライバシーポリシーに記載することが強く求められる【基本的事項】。

[20] GDPR では「自然人と関連する一定の個人的側面を評価するための、特に、当該自然人の業務遂行能力、経済状態、健康、個人的嗜好、興味関心、信頼性、行動、位置及び移動に関する側面を分析又は予測するため、個人データの利用によって構成されるあらゆる形式の個人データの自動的な取扱いを意味する。」（第４条）と定義されている。

[21] プロファイリング結果に基づき、利用者にとって重要な決定が自動的に行われることがある場合には、その旨や当該決定に至る際に依拠する基準等を明示することが求められる。

[22] アプリケーション提供者が取得した利用者情報を第三者提供する場合、あらかじめ本人の同意を取得することが適切である。ただし、本指針では具体的に取り扱わないが、オプトアウトによる第三者提供を否定するものではない。なお、個人データの第三者提供に該当する場合には、個人情報保護法に基づき、原則としてあらかじめ本人の同意を取得しなければならない【法令事項】（同法第 27 条第１項）ことに留意が必要である。

［外国の第三者等に提供する場合の記載事項］[23][24]

- 外国にある第三者や委託先、共同利用相手へ利用者情報を提供する場合には、外国にある第三者等への提供を利用目的とすること、提供される利用者情報の項目及び提供先の第三者等の所在国の名称等をプライバシーポリシーに記載することが強く求められる【基本的事項】。

［共同利用する場合の記載事項］

- アプリケーション提供者が、特定の者と利用者情報を共同利用する場合には、①共同利用をする旨、②共同利用される利用者情報の項目、③共同して利用する者の範囲[25]、④利用する者の利用目的[26]、及び⑤当該利用者情報の管理について責任を有する者の氏名又は名称[27]及び連絡先[28]を明確にプライバシーポリシーに記載することが強く求められる[29]【基本的事項】。

［情報収集モジュール等に関する記載事項］

- 情報収集モジュール提供者の提供する情報収集モジュール（以下単に「情報収集モジュール」という。）が組み込まれていない場合は、アプリケーション提供者以外の第三者が情報収集モジュールを用いて利用者情報を取得しない旨をプライバシーポリシーに記載することが望ましい【望ましい事項】。

---

23 個人情報取扱事業者は、個人データに該当する利用者情報を外国（個人情報の保護に関する法律施行規則（平成 28 年個人情報保護委員会規則第 3 号。以下「個人情報保護委員会規則」という。）で定める外国を除く。）にある第三者（同規則第 16 条で定める基準に適合する体制を整備している者を除く。）に提供する場合、個人情報保護法により、原則として、提供先の第三者の所在国における個人情報の保護に関する制度、当該第三者が講ずる個人情報の保護のための措置その他当該本人に参考となるべき情報提供を行った上で、外国にある第三者への提供を認める旨の本人の同意をあらかじめ取得しなければならない【法令事項】（同法第 28 条）ことに留意が必要である。なお、個人情報保護委員会規則で定める国とは、平成 31 年個人情報保護委員会告示第 1 号に定める国を指す。

24 総務省告示により指定された電気通信事業者は、特定利用者情報を外国に保存する場合や外国の第三者に委託する場合には、情報取扱方針に必要な事項を記載しなければならない【法令事項】（電気通信事業法第 27 条の 8）ことに留意が必要である。

25 共同利用する者の範囲には、必ずしも共同利用者の名称等を個別に全て列挙する必要はないが、本人がどの事業者まで将来利用されるか判断できる程度に明確にする必要がある。

26 利用目的は、全て記載する必要がある。利用者情報の項目によって利用目的が異なる場合は、項目ごとに利用目的を区別して記載することが求められる。

27 全共同利用者の中で、第一次的に苦情の受付・処理、開示・訂正等を行う権限を有する者の氏名又は名称を記載する。

28 ⑤について、個人データを共同利用する場合には、当該個人データの管理について責任を有する者の氏名又は名称及び住所並びに法人にあっては、その代表者の氏名を、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置かなければならない【法令事項】（個人情報保護法第 27 条第 5 項第 3 号）ことに留意が必要である。なお、個人データの共同利用については注釈 29 も参照。

29 個人情報保護法上、特定の者との間で共同して利用される個人データを当該特定の者に提供する場合であって、個人情報保護法第 27 条第 5 項第 3 号に規定されている情報を、提供に当たりあらかじめ本人に通知し、又は本人が容易に知り得る状態に置いているときには、当該提供先は、本人から見て、当該個人データを当初提供した事業者と一体のものとして取り扱われることに合理性があると考えられることから、第三者に該当しないこととされているところ、必要な事項を本人に通知し、又は本人が容易に知り得る状態に置いていない場合には、これに当たらないことに留意が必要である。

- アプリケーション提供者が情報収集モジュールを組み込む場合、アプリケーションを通じた情報収集の実態について明らかにする上で、アプリケーション提供者は、自らが組み込んでいる情報収集モジュールを用いたサービスの名称、提供者等の基本的な情報について、利用者に対して説明することが強く求められる【基本的事項】。
  - 具体的には、アプリケーション提供者は、アプリケーションに情報収集モジュールを組み込んでいる場合、アプリケーションのプライバシーポリシーにおいても、①組み込んでいる情報収集モジュールの名称、②情報収集モジュール提供者の名称（外国にある第三者の場合はその国名）、③取得される利用者情報の項目、④利用目的、⑤情報収集モジュール提供者による情報利用の有無（ある場合はその目的）、⑥第三者提供・外国の第三者への提供・共同利用の有無等[30]について情報収集モジュールごとに記載するとともに、各情報収集モジュール提供者のプライバシーポリシーにリンクを張る等して容易に参照できるようにすることが強く求められる（情報収集モジュール提供者のプライバシーポリシーが日本語でない場合、アプリケーションのプライバシーポリシーにおいてその概要を明示する）【上記①～⑤はいずれも基本的事項。ただし、②の「外国にある第三者の場合はその国名」のみ望ましい事項、⑥は望ましい事項】。なお、その際、情報収集モジュールによりスマートフォン外部に利用者情報が送信される旨が分かるようにプライバシーポリシーに記載し、利用者の求めに応じて情報送信又は利用の停止（オプトアウト）の機会を提供することが強く求められる【基本的事項】。

⑥ 同意取得の方法及び利用者関与の方法

- 同意取得の方法：同意取得の対象となる利用者情報の範囲・取扱方法等についてプライバシーポリシーに記載することが強く求められる【基本的事項】。また、同意取得の方法がダークパターンとならないよう留意することが強く求められる【基本的事項】。
  - 利用者情報の取扱いについて同意しなければ利用することができない機能と、同意をせずとも利用することができる機能がある場合には、同意を取得する前に明示するとともに、あらかじめ同意をしない選択肢も提示することが望ましい【望ましい事項】。
- 利用者関与の方法：利用者情報の取得・利用を中止する方法等をプライバシーポリシーに記載することが強く求められる【基本的事項】。
  - アプリケーション提供者による利用者情報の取得・利用を中止してほしい場合に、アプリケーションそのものをアンインストールする以外に方法がないときは、その旨プライバシーポリシーに記載することが望ましい【望ましい事項】。

30 情報収集モジュールにより③取得される情報の項目、④利用目的、⑤第三者提供・共同利用の有無等について、情報収集モジュールのプライバシーポリシーやウェブサイト等に明示されている場合、そのリンクを張る等により代えることも可能であるが、その場合には、リンク先の記載の概要を併記することが求められる。

- アプリケーションを使用しながら、アプリケーション提供者による利用者情報の取得が中止される方法がある場合、又は利用者情報の取得は継続されるがその利用が中止される方法がある場合には、そのいずれであるかが分かるようにしてプライバシーポリシーに記載することが望ましい【望ましい事項】。
- 利用者情報の取得・利用を中止することにより利用することができなくなる機能がある場合には、利用できなくなる範囲について明示することが望ましい【望ましい事項】。
- プロファイリングを含むアプリケーション提供者による利用者情報の取扱いに異議がある場合に、その旨アプリケーション提供者へ申し立てる方法についてプライバシーポリシーに記載することが望ましい【望ましい事項】。

⑦ 問合せ窓口

- アプリケーション提供者が利用者情報を取得する場合に、利用者情報の取扱いに関する問合せ窓口の連絡先等（電話番号、メールアドレス、問い合わせフォーム等）をプライバシーポリシーに記載することが強く求められる【基本的事項】。

⑧ プライバシーポリシーの変更を行う場合の手続

- プライバシーポリシーの変更を行った場合の通知方法等を記載することが望ましい【望ましい事項】。

⑨ 利用者の選択の機会の内容、データポータビリティに係る事項

- 利用者情報の取得・利用の停止を利用者が求めることができるか否かをプライバシーポリシーに記載するとともに、停止を求める方法について記載することが強く求められる【基本的事項】。また、停止後にアプリケーションを継続して利用することが可能であるかについて記載することが望ましい【望ましい事項】。
- データポータビリティを確保している場合には、利用者情報の移転を行う方法や、移転先の条件についてプライバシーポリシーに記載することが期待される【ベンチマーク事項】。

⑩ 委託に関する事項

- 利用者情報の委託を行う場合には、委託を行う情報の内容や委託先、委託の目的をプライバシーポリシーに記載することが望ましい【望ましい事項】。

【補足】

プライバシーポリシーは、基本原則に定められた「透明性の確保」や「利用者関与の機会の確保」等を実現するための中核となる手段である。そのため、アプリケーション提

供者の取組として、まずプライバシーポリシーの具体的な作成項目を示している。

様々な利用者情報が大規模に蓄積されるスマートフォンにおいては、アプリケーションのプライバシーポリシーについては原則として企業全体のプライバシーポリシーやアプリケーションの利用規約と別に策定されることが求められる。また、アプリケーションのプライバシーポリシーを策定する際には、企業全体のプライバシーポリシーや当該アプリケーションの利用規約との整合性について確認し、必要に応じて調整を行うことが求められる。

なお、利用者から観た際に、利用者情報の取得がされないためプライバシーポリシーを作成・公表していないのか、取得がされているにもかかわらず作成・公表していないのか不明確であると利用者が不安になる可能性があるため、利用者が自らの利用者情報の取扱いに関する情報を十分に得て、アプリケーションの利用に関し適切に判断し、行動することを支援するという本指針の趣旨に鑑み、利用者情報をアプリケーション提供者が取得していない場合においてもプライバシーポリシーを通知又は公表することが求められる。具体的には、アプリケーション提供者が利用者情報を取得していない場合には、①、②、⑦及び⑧を記載したプライバシーポリシーへのリンクを張る、又はアプリストアのアプリケーション紹介文において記載する等して公表することが考えられる。

1.2.1.2. プライバシーポリシー等の運用

（１） 通知・公表又は同意取得の方法

[一般的な取扱い]

- アプリケーション提供者は、プライバシーポリシーを定め公表するとともに、アプリケーションをダウンロード又は利用開始しようとする者が容易に参照できる場所に掲示又はリンクを張ることが強く求められる[31]【基本的事項】。
- アプリケーションをダウンロード又は利用開始しようとする者がスマートフォンの画面上で容易に理解できるように、プライバシーポリシーの分かりやすい概要を作成して利用者が容易に参照できる場所に掲示又はリンクを張る等、利用者にとって分かりやすい方法[32][33]で示されることが望ましい（概要から詳細なプライバシーポリシーへリンクを張る方法等も有用である）【望ましい事項】。

---

[31] アプリケーションをダウンロード又は利用開始した後に利用者がプライバシーポリシーを確認した場合、既に利用者情報が取得されている可能性があるため、利用者がアプリケーションをダウンロード又は利用開始する前に通知又は公表することが求められる。なお、原則としてアプリストアのアプリケーション紹介ページにプライバシーポリシーへのリンクを張ることが求められる。ただし、アプリケーションの利用開始後に利用者がプライバシーポリシーを容易に確認することを可能とするため、アプリケーション内にもプライバシーポリシーが掲示されていることが求められる。

[32] 例えば、1.2.1.1.に示したプライバシーポリシーに記載する事項について、アプリケーションごとにその概要を作成し、アイコン等を用いてアプリストアの個別ページに掲示する方法が考えられる。

[33] 利用者の属性（こども、高齢者等）に配慮して適切な情報提供が行われることが求められる。

- プライバシーポリシーによる通知又は公表あるいは同意取得は、原則として利用者がアプリケーションをダウンロード又はインストールあるいは利用開始しようとする前に行うことが望ましく、それらの時点で行うことが難しい場合には、初回起動時に処理が実行される前に行うことが望ましい【望ましい事項】。
- 特に同意取得を要する利用者情報[34]については、アプリケーションをダウンロード又はインストールあるいは利用開始する前、初回起動時に処理が実行される前等、当該情報を取得するための処理が実行されうる前に同意取得が行われるように設計することが強く求められる【基本的事項】。
- アプリケーションに関する OS によるパーミッションは一般にアプリケーションがどのような情報にアクセスするかを示しているが、利用目的やスマートフォン外部への送信・第三者提供・共同利用の有無等の項目の記載がない場合には、OS によるパーミッションのみでは本項に示す通知又は公表あるいは同意取得として十分ではないことに留意することが強く求められる[35]【基本的事項】。
- OS によるパーミッションが表示される際に別途[36]アプリケーション提供者が作成したプライバシーポリシーのリンク先を示すなどの方法により通知又は公表を行うか、必要に応じて個別の情報に関する同意取得等を行うことが期待される【ベンチマーク事項】。

[同意取得等を要する利用者情報の取扱い]

- アプリケーション提供者による、プライバシー性が高いと考えられる利用者情報の取得又は利用のうち、現状の利用実態を踏まえ代表的なものの取扱いについて、以下のとおり個別に対応することが求められる。

① 個人情報を含む電話帳情報　アプリケーションが提供するサービスの目的に応じ必要とされる範囲（フィールド）を限定するとともに、プライバシー侵害を回避する観点から、個別の情報に関する同意取得を行うことが望ましい[37]【望ましい事項】。

② センシティブ情報[38]　不当な差別や偏見その他の不利益が生じないようにその

---

[34] 個人情報取扱事業者が、病歴、健康診断の結果等の要配慮個人情報に該当する利用者情報を取得する場合、個人情報保護法により原則としてあらかじめ本人の同意を取得しなければならない【法令事項】（同法第 20 条第２項）ことに留意が必要である。

[35] OS のパーミッション等において、実際に取得される情報の項目及び利用目的等が具体的に記載されるような形式がとられた場合等には、当該パーミッションにより通知・同意を行う可能性もある。

[36] OS のパーミッションを表示する際に合わせて表示される自由記入欄にプライバシーポリシーを表示することも一案と考えられる。

[37] その場合であってもこれらの情報は第三者に関する個人情報を含むにもかかわらず、一方当事者である利用者の同意のみしか得られていないため、利用者の一定の責任を免れない場合もあると考えられる。

[38] 人種・信条・病歴等のほか、本人に対する不当な差別、偏見その他の不利益が生じないようにその取扱いに特に配慮を要する利用者情報をいう。

取扱いに特に配慮を要する情報を収集する場合については、取得する情報の項目を明示した上で、個別の情報に関する同意取得を行うことが強く求められる[39]【基本的事項】。また、プロファイリングによりセンシティブ情報を予測・生成する行為は、センシティブ情報の取得につながるおそれも否定できないと考えられることから、原則として実施しないこととし、実施する場合には、利用者本人に対して個別の同意取得を行うことが望ましい【望ましい事項】。

③ こどもの利用者情報[40]　こどもが利用する可能性があるサービスを企画・開発する際には、こどものプライバシーを高い水準で確保するための適切な措置を講じることが望ましい[41]【望ましい事項】。例えば、プライバシーポリシーを簡潔で目立つように、利用者の年齢に適した明確な表現で記載したりすることが考えられる[42]【望ましい事項】。また、特に低年齢のこどもに関する利用者情報の取扱いに当たっては、事前に法定代理人等から個別の情報に関する同意取得を行うことが強く求められる[43]【基本的事項】。さらに、こどもの利用者情報のプロファイリングに基づくターゲティング広告の表示は実施しないことが望ましい【望ましい事項】。

④ 利用者行動のトラッキング　利用者は、端末やアプリケーション等によって提供される広告 ID 等の識別子に関連付けられることがあり、これらの識別子を他の情報と組み合わせることで、特定の個人の識別性を獲得する可能性があると考えられること、また、特定の個人の識別性は獲得しないものの利用者に対するプロファイリングが可能となることから、プライバシー侵害を回避する観点又は利用者利益の保護の観点から、事業者横断的なトラッキングを実施するために利用者情報を取得する際には、個別の情報に関する同意取得を行うこと

[39] 個人情報取扱事業者が、個人情報保護法上の要配慮個人情報を取得する場合には、原則としてあらかじめ本人の同意を得なければならない【法令事項】（同法第 20 条第 2 項）ことに留意が必要である。
[40] 対象とする年齢範囲については、例えば米国の児童オンラインプライバシー保護法（COPPA）は 13 歳未満を対象としているほか、GDPR におけるこどもの同意については、16 歳未満（加盟国ごとに 13 歳を下回らない範囲で設定が可能）の場合は親権者による同意が必要とされており、これらを参考とすることが考えられる。
[41] 英国 Children's Code（Age Appropriate Design Code ）が示す行動規範も参照しながら、プライバシーポリシーの作成・運用、アプリの開発等を行うことも考えられる。
[42] こども向けのプライバシーポリシーを別途用意することも有用である。
[43] 個人情報保護法上、本人同意の取得が必要であり、当該本人が未成年である場合については、「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すが、一般的には 12 歳から 15 歳までの年齢以下のこどもについて、法定代理人等から同意を得る必要があると考えられ」るとされていることにも留意が必要である（個人情報保護委員会「『個人情報の保護に関する法律についてのガイドライン』に関する Q&A」QA1-62）。

が望ましい[44]【望ましい事項】。

⑤ 契約者・端末固有 ID 等、契約や端末に対して一義的に指定・作成され、利用者側で変更が困難であるが、幅広い主体により利用される可能性があるものが ID 等の情報を取得するアプリケーション提供者等において特定の個人の識別性を有する情報と結びつきうる形で利用される場合、同一 ID の上に様々な情報が時系列的に蓄積し得ること、当該アプリケーション提供者等又は第三者において特定の個人の識別性を有する可能性があることから、個人情報保護法への抵触やプライバシー侵害の可能性を考慮し、個人情報に準じた形で取り扱うことが強く求められる【基本的事項】。具体的には、取得される項目及び利用目的を明確に記載し、その目的の範囲内で適正に扱うこととすることが強く求められる[45]【基本的事項】。

⑥ GPS 等による位置情報[46]は、アプリケーションが提供するサービスの提供又は機能に直接関連する場合にのみ取得することが強く求められる【基本的事項】。また、アプリケーション提供者は、プライバシー侵害を回避する観点から、個別の情報に関する同意取得を行うことが強く求められる【基本的事項】。また、アプリケーション提供者は、取得する位置情報の粒度や、取得する条件について利用者が設定可能とする等、取扱いに留意することが望ましい【望ましい事項】。

⑦ 通信内容・履歴、メール内容・送受信履歴等の通信履歴の取得　通信相手等の特定の個人の識別性を有する場合があること、及び通信の内容を含むプライバシー侵害を回避する観点から、個別の情報に関する同意取得を行うことが強く求められる[47]【基本的事項】。

---

[44] 電気通信事業法における外部送信規律は、同意の取得を義務とするものではなく、通知又は容易に知り得る状態に置くことを義務付けているところ、同意の取得についてはここでは取り組むことが望ましい事項として記載している。

[45] これらの情報は個人情報や個人関連情報に該当し得るため、個人情報保護法の規定を遵守する必要があることにも留意が必要である。例えば、個人情報に該当する場合、個人情報取扱事業者は、その取扱いに当たっては、利用目的をできる限り特定しなければならない【法令事項】（個人情報保護法第 17 条第 1 項）。また、あらかじめ本人の同意を得ないで、特定された利用目的の達成に必要な範囲を超えて、個人情報を取り扱ってはならない【法令事項】（同法 18 条第 1 項）。

[46] 位置情報の同意取得については、例えば、総務省の「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～」（平成 26 年 7 月）も参考となり得る。また、電気通信事業者においては、電気通信事業における個人情報等の保護に関するガイドライン第 41 条も合わせて参照されたい。

[47] 通信の相手方や内容に含まれる第三者の同意を得ない場合に、アプリケーション提供者等や利用者が一定の責任を免れないこともあると考えられる。

⑧ スマートフォンのアプリケーションの利用履歴[48]やスマートフォンに保存された写真・動画　アプリケーションによるサービス提供のために必要な範囲で用いられる場合を除き、プライバシー侵害を回避する観点から、個別の情報に関する同意取得を行うことが望ましい【望ましい事項】。また、アクセス範囲の限定等の設定を可能にする等、取扱いに留意することが望ましい【望ましい事項】。

【補足】

1.　プライバシーポリシー等の運用

プライバシーポリシーにより、利用者に対し、利用者情報の取得等に関して説明することは、アプリケーション提供者が社会の信頼を確保するために重要である。

個人情報の保護に関する基本方針では、プライバシーポリシー等を策定・公表することにより、「個人情報を目的外に利用しないことや苦情処理に適切に取り組む等を宣言するとともに、事業者が関係法令等を遵守し、利用目的の通知・公表、開示等の個人情報の取扱いに関する諸手続について、あらかじめ、対外的に分かりやすく説明することが、事業活動に対する社会の信頼を確保するために重要である」ことが示されている。

さらに、電気通信事業における個人情報等の保護に関するガイドラインにおいては、「電気通信事業者は、アプリケーションソフトウェア（以下「アプリケーション」という。）を提供する場合において、当該アプリケーションによる情報の取得等について明確かつ適切に定めたプライバシーポリシーを公表することが適切である」ことが定められており、事業者単位でのプライバシーポリシーではなく、アプリケーション単位でプライバシーポリシーを定め、公表することが示されている。

こうした観点により、1.2.1.1.プライバシーポリシーの作成において、具体的なプライバシーポリシーの項目を示しているが、プライバシーポリシーは、あくまでも手段であり、適切に運用されて初めて、利用者の信頼を得ることができるとともに、アプリケーション提供者の関係法令等の遵守に資するものである。そこで本節では、プライバシーポリシー等の運用に関わる具体的な取組を示した。

2.　プライバシーポリシーの掲示場所等

プライバシーポリシー等を適切に運用し、透明性を高めるためには、利用者が容易にプライバシーポリシーを確認できることが重要である。そのような観点から、容易に参照できる場所に掲示又はリンクを張ることを求めている。

[48] アプリケーションの品質向上等のために当該アプリケーションの利用履歴等を活用することは、アプリケーションにより提供されるサービス提供の一環と考えられるため、プライバシーポリシー等に明示しアプリケーションに関する通知又は公表あるいは同意取得を行うことで可能である。一方、他アプリケーションの利用履歴等については、分析、広告配信・表示やマーケティングを目的として取得することは望ましくない。アプリケーションのサービス提供に関連する場合であっても、個別の情報に関する同意取得を行うことが求められる。

3. 通知・公表又は同意取得のタイミング

まず、アプリケーションをダウンロード又は利用開始した後にプライバシーポリシーを確認した場合、既に利用者情報が取得されている可能性があるため、利用者がアプリケーションをダウンロード又は利用開始する前に通知又は公表することが求められる。なお、原則としてアプリストアのアプリケーション紹介ページにプライバシーポリシーへのリンクを張ることが考えられるが、一方で、アプリケーションの利用開始後に利用者がプライバシーポリシーを容易に確認することを可能とするため、アプリケーション内にもプライバシーポリシーを掲示することが求められる。

4. 同意取得等を要する利用者情報の取扱い

「プライバシー情報の収集について、本人の同意がある場合や、収集方法等に照らして定型的に推定的同意があると認められる場合には、人格的自律ないし私生活上の平穏を害する態様で収集されたということはできない」（東京地判平成 22 年 10 月 28 日客室乗務員 DB 事件）といった裁判例など、プライバシー性の高い情報を取得・利用・提供する場合、本人の同意があればプライバシー権侵害に当たらない場合がある。そのような観点から、アプリケーション提供者等がプライバシー性の高い利用者情報を取得する場合又はプライバシー性の高い態様で利用者情報を利用する場合には、個別の取得・利用に関する同意を取得することによりプライバシー侵害を回避しうる。

有効な同意と認められるかは、事案に応じて検討が必要である。例えば、アプリケーションに関する OS によるパーミッションにより「アプリケーションが当該情報にアクセスする権限」に対する許諾を得たとしても、「利用目的」、「利用者情報の外部送信」及び「第三者提供」について説明がない場合には、単体では第三者提供に係る同意取得の条件を満たしているとはいえないとの指摘がある。

（２） 利用者関与の方法

- 利用者情報が、プライバシーポリシーに反して、取得され又は取り扱われていることが明確である場合等については、利用者からの申出を受け利用の停止又は消去を行うことが強く求められる【基本的事項】。また、その手段についてプライバシーポリシーへ記載する等、利用者にとって参照しやすい方法で情報提供されることが強く求められる【基本的事項】[49]。

[49] 個人情報保護法上、保有個人データが特定された利用目的の達成に必要な範囲を超えて取り扱われている場合など一定の場合については、本人は当該保有個人データの利用の停止又は消去を請求することができ（同法第 35 条第 1 項）、また、保有個人データが第三者提供等に関する規制に違反して第三者に提供されている場合には、本人は当該保有個人データの第三者への提供の停止を請求することができる（同条第 3 項）とともに、保有個人データを当該個人情報取扱事業者が利用する必要がなくなった場合などにおいては、本人は当該保有個人データの利用停止等又は第三者への提供の停止を請求することが

- 利用者が利用者情報の範囲・取扱方法について同意した場合であっても、その同意の後に、簡単にアクセスでき、かつ、分かりやすい方法で当該同意の撤回等ができる機会を提供し、また、同意の撤回方法をプライバシーポリシーに記載することが望ましい【望ましい事項】。
  - ダークパターンを回避するため、同意を取得する場合と同程度の操作により同意の撤回画面へアクセスできるようにすることが望ましい【望ましい事項】。

（3） アプリケーションの更新等によるプライバシーポリシーの変更

- アプリケーションの更新等によりプライバシーポリシーを変更する場合は、利用者に対し、通知することが強く求められる[50]【基本的事項】。
- アプリケーションの更新等によりプライバシーポリシーに定めた利用目的から関連性を有すると合理的に認められる範囲を超えて利用目的が変更となる場合には、利用者から同意を取得することが強く求められる[51]【基本的事項】。
- なお、アプリケーションの更新等により、当初の同意取得の対象であった利用者情報の範囲・取扱方法が変更される場合には、元の利用者情報の範囲・取扱方法について、利用者との間での合意が成立しているため、利用者から同意を取得することが強く求められる【基本的事項】。

1.2.1.3. 苦情相談への対応体制の確保

- 利用者情報を取得するアプリケーション提供者は、利用者情報の取扱いに関する苦情や相談の適切かつ迅速な処理に努める。具体的には、苦情相談の窓口・連絡先を設置する等必要な体制の整備に努めることが強く求められる【基本的事項】。

［情報収集モジュールを組み込む場合の取扱い］

- アプリケーション提供者は、利用者から、情報収集モジュール提供者による利用者情報の取扱いに関する苦情相談があった場合であって、自らその苦情相談を処理することができないときは、情報収集モジュール提供者の相談窓口・連絡先に利用者を誘導することが望ましい【望ましい事項】。

できる（同条第 5 項）。また、これらの請求に応じる手続は、本人の知り得る状態（本人の求めに応じて遅滞なく回答する場合を含む。）に置かなければならない【法令事項】（同法第 32 条第 1 項第 3 号）こととされている。

[50] 個人情報取扱事業者は、個人情報の利用目的を変更した場合は、変更された利用目的について、本人に通知し、又は公表しなければならない【法令事項】（個人情報保護法第 21 条第 3 項）ことに留意が必要である。

[51] 個人情報取扱事業者は、利用目的の達成に必要な範囲を超えて個人情報を取り扱う場合には、原則としてあらかじめ本人の同意を取得しなければならない【法令事項】（個人情報保護法第 18 条第 1 項）ことに留意が必要である。

1.2.1.4. 適切な安全管理措置

- 取り扱う利用者情報が漏えい、滅失又はき損の危険にさらされることがないように、利用者情報の安全管理のために必要かつ適切な措置を講じることが強く求められる【基本的事項】[52]。
- 利用目的に必要な期間に限り保存し、目的達成等により不要となった際には、適切に消去することが強く求められる【基本的事項】。
- 利用者がアプリケーションをアンインストール等したこと又は一定期間利用していないことが判明した後のデータの保存期間、その後の処理等についてあらかじめ定めておくことが望ましい【望ましい事項】。
- 利用者情報を取得するアプリケーション提供者が、利用目的の達成に必要な範囲において、利用者情報の取扱いの全部又は一部を外部委託する場合は、委託先における利用者情報の取扱いの安全管理についても監督することが強く求められる【基本的事項】[53]。

1.2.1.5. アプリケーションの開発時における留意事項

- アプリケーション提供者は、利用者の個人情報やプライバシーが尊重され保護されるように、アプリケーションの企画及び設計の段階から、当該アプリケーションにおける利用者情報の取り扱われ方について検討し、適切な仕組みをアプリケーションに組み込むことが強く求められる【基本的事項】。アプリケーション提供者がアプリケーションの開発を委託する場合、委託先とともに利用者情報の取扱いに関する要求事項を整理し、当該要求事項がアプリケーションに組み込まれるよう指示し、監督することが強く求められる【基本的事項】。加えて、アプリケーション提供者は、あらかじめプライバシーポリシーを作成するとともに、委託先からのアプリケーションの納品を受ける際に、プライバシーポリシーの記載事項とアプリケーションの挙動が一致するかを検証することが強く求められる【基本的事項】。

1.2.1.6. ダークパターン回避の対応

- 利用者利益の保護を図るため、サービスの利用者を欺いたり操作したりするような方法又は利用者が情報を得た上で自由に決定を行う能力を実質的に歪めたり損

---

[52] 個人情報取扱事業者は、その取り扱う個人データの漏えい等の防止その他の個人データの安全管理のため、必要かつ適切な措置を講じなければならない【法令事項】（個人情報保護法第 23 条）ことに留意が必要である。なお、講じなければならない措置には、個人情報取扱事業者が取得し、又は取得しようとしている個人情報であって、当該個人情報取扱事業者が個人データとして取り扱うことを予定しているものの漏えい等を防止するために必要かつ適切な措置も含まれる（ガイドライン通則編 3 - 4 - 2）。

[53] 個人データについては、委託した個人データの安全管理が図られるよう、当該委託先に対する必要かつ適切な監督を行わなければならない【法令事項】（個人情報保護法第 25 条）ことに留意が必要である。

なったりする方法で利用者情報の取扱いを行わないことが強く求められる[54]【基本的事項】。

【補足】

ダークパターンの具体的な事例は、例えば以下の場合が考えられる[55]。

- アプリケーションの利用開始後に利用者情報の取得・利用をオプトアウトすることが可能であるにもかかわらず、利用開始時には同意を拒否する選択肢が提示されず、デフォルトで同意をすることとなっている場合。
- 同意を取得する場合の操作に比べ、同意を撤回する場合の操作が煩雑になっている場合、又は同意を撤回する方法に容易に到達することができない場合。
- 同意の取得画面において、同意ボタンが目立つように表示されており、拒否するボタンが表示されていない又は目立たない形で表示されている場合。
- 利用者が一度拒否したにもかかわらず、同意が得られるまで繰り返し同意取得画面を掲出する場合。
- 同意の取得画面又はその直前の画面において、利用者情報の取得・利用に同意することによるメリット又は同意しないことによるデメリットのみを強調し、同意へ誘導している場合。
- 同意取得時に、利用者に対して金銭等のインセンティブを提示することにより、同意へ誘導している場合。
- 同意取得時に、後で同意を撤回する方法が用意されている旨説明していたにもかかわらず、実際には同意を撤回する方法が用意されていない場合。情報の取得範囲を利用者が設定できるようにしている場合において、より多くの情報を取得する選択肢がデフォルトで選択されている場合。

1.2.1.7. 電気通信事業法への対応

- 通信の秘密[56]に該当する利用者情報の取扱いについては、電気通信事業法第4条において、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【法令事項】こととされている点に留意が必要である。
- 総務省告示により指定された電気通信事業者においては、特定利用者情報の取扱いについて、情報取扱規程の策定・届出、情報取扱方針の策定・公表等の対応を行わな

[54] 本指針においては、あくまで基本的事項として記載しているが、関係する他法令においてこのような取扱いが禁止されている場合には、当該法令に従い対応する必要がある。

[55] パターンの具体的な事例については、欧州データ保護会議（EDPB）による”Guidelines 03/2022 on Deceptive design patterns in social media platform interfaces: how to recognise and avoid them”（https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032022-deceptive-design-patterns-social-media_en）や、OECD による”Dark Commercial Patterns”（https://www.oecd-ilibrary.org/science-and-technology/dark-commercial-patterns_44f5e846-en）を参考に記載している。

[56] 通信内容にとどまらず、通信当事者の住所・氏名、発受信場所、通信年月日等通信の構成要素及び通信回数等通信の存在の事実の有無を含む。

ければならない【法令事項】。詳細については、電気通信事業における個人情報等の保護に関するガイドラインを参照すること。

- メッセージ媒介サービス、SNS、検索サービス、ホームページの運営等の対象となる電気通信役務を営んでいる電気通信事業者は、利用者に関する情報を利用者の端末の外部に送信させる場合[57]には、送信される情報の内容や送信先、利用目的等について通知、公表、本人同意の取得又はオプトアウト措置を行わなければならない【法令事項】。詳細については、電気通信事業における個人情報等の保護に関するガイドラインを参照すること。
  - 本人同意の取得及びオプトアウト措置については、必ずしも法令上の義務が課されるものではないが、利用者関与の機会の確保の観点からは、本指針を参考に対応することが望ましい【望ましい事項】。

1.2.2. 情報収集モジュール提供者の取組

≪期待される役割≫

- 情報収集モジュール提供者は、利用者情報を取得する場合、自身の利用者情報の取扱いに責任を負うことが強く求められる【基本的事項】。
- 加えて、情報収集モジュール提供者は、情報収集モジュールの挙動や取得した情報の利用に一義的に関与していることから、情報収集モジュールの利用者情報の取扱いに関する透明性等が確保されるようアプリケーション提供者を支援することが望ましい【望ましい事項】。

≪具体的な取組内容≫

1.2.2.1. プライバシーポリシーの作成

- スマートフォンから利用者情報を収集する情報収集モジュール提供者は、1.2.1.1 を踏まえ、プライバシーポリシーを作成することが望ましい。その際、1.2.1.1 の適用に当たっては、適宜、「アプリケーション提供者」を「情報収集モジュール提供者」と、「アプリケーション」を「情報収集モジュール」と読み替えるものとする。

1.2.2.2. プライバシーポリシーの運用等

- 1.2.1.2 を踏まえて、プライバシーポリシーの運用等を実施することが望ましい。その際、1.2.1.2 の適用に当たっては、適宜、「アプリケーション提供者」を「情報収集モジュール提供者」と読み替えるものとする。
- ただし、アプリケーションの利用者に対する通知又は公表あるいは同意取得に関しては情報収集モジュール提供者自身が実施することは困難だと考えられ、アプリケーション提供者を介して行われることが想定されるため、情報収集モジュール提供者は、関連す

[57] 委託先に対する送信についても例外ではないことに留意が必要である。

る内容を含むプライバシーポリシーを公表し、アプリケーション提供者へ通知することが強く求められる【基本的事項】。

- アプリケーションの利用者から、情報収集モジュール提供者に対し、取得した利用者情報に関する問合せ又は取得した利用者情報の消去等の申出があった場合、必要に応じてアプリケーション提供者と協力し、これに応じることが強く求められる【基本的事項】[58][59]。
- プライバシーポリシーの内容について変更があった場合は、プライバシーポリシーを更新するものとし、プライバシーポリシーの内容について重要な変更があった場合には、プライバシーポリシーを更新し、公表するとともに、アプリケーション提供者へ通知することが強く求められる[60]【基本的事項】。

1.2.2.3. 苦情相談への対応体制の確保、適切な安全管理措置及びダークパターン回避の対応

- 苦情相談への対応体制の確保及び安全管理措置については、1.2.1.3、1.2.1.4 及び 1.2.1.6 を踏まえて取り組むことが強く求められる【基本的事項】。

1.3. 他の関係事業者等における取組

- 適切な取扱いや利用者における安全・安心の向上のために、アプリケーション提供者等以外の関係事業者等についても、基本原則等を考慮しつつ、以下のような取組をそれぞれの立場で、また相互に協力しつつ進めることが求められる。

1.3.1. アプリストア運営事業者[61]、OS 提供事業者

- アプリストア運営事業者は、アプリケーション提供者等において、「1.2 アプリケーション提供者等における取組」における事項が実施されているか確認することが望ましい【望ましい事項】。
- アプリストアへのアプリケーションの登録審査時に本指針を踏まえた基準等を作成し、あらかじめ公表することが望ましい【望ましい事項】。

---

[58] 個人情報取扱事業者は、本人から個人情報保護法第 35 条第 1 項の規定に基づく保有個人データの利用停止又は消去の請求を受けた場合であって、その請求に理由があることが判明したときは、原則として、違反を是正するために必要な限度で、遅滞なく、当該保有個人データの利用停止等を行わなければならない【法令事項】（同法第 35 条第 2 項）ことに留意が必要である。

[59] 本人確認が不可能な場合など適切かつ合理的な方法により当該申出に応じることが出来ない場合は、利用者に対し、その理由とともに応じることが出来ない旨を説明する。

[60] 個人情報取扱事業者は、利用目的を変更した場合は、変更された利用目的について、本人に通知し、又は公表しなければならない【法令事項】（個人情報保護法第 21 条第 3 項）ことに留意が必要である。

[61] アプリストアの運営に当たっては、例えば、英国の “Code of practice for app store operators and app developers” (https://www.gov.uk/government/publications/code-of-practice-for-app-store-operators-and-app-developers/code-of-practice-for-app-store-operators-and-app-developers-new-updated-version)（以下、「英国コード・オブ・プラクティス」という。）が示す行動規範を参照することが考えられる。

- アプリケーションの掲載を拒否する場合には、その理由について、アプリケーション提供者に対して適切なフィードバックを行うことが強く求められる[62][63]【基本的事項】。
- アプリストアの個別のアプリケーションページ上にプライバシーポリシーや取得される情報の概要等の表示場所を提供する、表示すべき事項や標準的なアイコンを示す等、アプリケーション提供者等に対し、適切な対応を行うように支援することが望ましい【望ましい事項】。
- 説明や情報取得の方法が適切ではないアプリケーションが判明した場合の対応(アプリストアから削除する等)を実施するとともに、連絡通報窓口を設置することが望ましい【望ましい事項】。
- OS によるパーミッションがある場合、利用者に分かりやすい説明を行う努力を継続することが望ましい【望ましい事項】。目的に応じ注意すべきパーミッション等がある場合、利用者が安全に利用できるための方策を検討することが望ましい【望ましい事項】。
- 必要に応じ関係事業者や業界団体等とも協力しつつ、アプリケーション提供者等に対し啓発活動を進めることが望ましい【望ましい事項】。

【補足】

アプリストアにおいて、仮にプライバシー侵害を行うアプリケーションが多数販売されているような場合、アプリストア運営事業者は、ユーザーに対して注意喚起その他の義務を負うと解される可能性があることから、アプリケーション提供者等に対する、各種取組を行うことが求められる。

なお、アプリストアや OS の利用規約等において専属的合意管轄裁判所を国外の裁判所とし、準拠法を外国法としている場合においても、消費者である利用者からの訴訟提起の際や、不法行為に基づく請求の際には、日本の裁判所に国際裁判管轄が認められ、準拠法を日本国法とされる可能性があることは既に述べたとおりである。

1.3.2. 移動体通信事業者・端末製造事業者

- スマートフォン販売時等に、既存チャンネルを通じて利用者に必要事項を周知することが望ましい(例えば、従来の携帯電話との違い[64]、情報セキュリティやプライバシー上留意すべき点等の周知等)【望ましい事項】。

---

62 特定デジタルプラットフォームの透明性及び公正性の向上に関する法律(令和２年法律第 38 号、以下「デジタルプラットフォーム取引透明化法」という。)に基づき、特定デジタルプラットフォーム提供者の指定を受けた事業者は、特定デジタルプラットフォームの提供の拒絶を行うときには、当該拒絶の内容及び理由を開示しなければならない【法令事項】(デジタルプラットフォーム取引透明化法第５条第３項第２号) ことに留意が必要である。

63 アプリケーション提供者へのフィードバックの方法については、英国コード・オブ・プラクティスにおける開発者に対する明確なフィードバックに関する規範を参照することが考えられる。

64 水平分業モデルで PC と類似した自由度があるが、マルチステークホルダーで自己責任リスクがあるスマートフォンの違いを十分周知する必要がある。

- 移動体通信事業者のアプリストアにおいて、アプリケーション提供者等に対し、適切なプライバシーポリシー等の作成・公表等の対応を促すことが望ましい【望ましい事項】。プライバシーポリシー等の表示場所を提供する等、アプリケーション提供者等に対し、適切な対応を行うように支援するとともに、必要に応じ関係事業者や団体等とも協力しつつ、アプリケーション提供者等に対し啓発活動を進めることが望ましい【望ましい事項】。
- 移動体通信事業者のアプリストアにおいて、説明や情報取得の方法が適切ではないアプリケーションが判明した場合の対応（アプリストアから削除する等）を実施するとともに、連絡通報窓口を設置することが望ましい【望ましい事項】。
- 今後「利用者」として増加する可能性があるのは、現在スマートフォンを使いこなしている層に加えて、ICT リテラシーに乏しい消費者、高齢者等と考えられることから、移動体通信事業者はリテラシーに応じたスマートフォンの機器やサービス設計、周知啓発活動を端末製造事業者との協力も考慮しつつ検討することが望ましい【望ましい事項】。

【補足】

電気通信事業における個人情報等の保護に関するガイドラインでは、「電気通信事業者は、アプリケーションを提供するサイトを運営する場合において、当該サイトにおいてアプリケーションを提供する者に対して、当該アプリケーションによる情報の取得等について明確かつ適切に定めたプライバシーポリシーを公表するよう促すことが適切である」と定められており、各関係者の取組の促進に資することが期待される。

1.3.3. その他関係しうる事業者等

- 独自の基準に基づきアプリケーションの推薦等をしているアプリケーション紹介サイトやアプリケーションに関する広告は、利用者がアプリケーションを認知し、選択する際に影響力を有する情報源となる場合がある。
- アプリケーション紹介サイト運営者、アプリケーションを通じて取得された利用者情報を用いて広告に関する事業を行う者等関係する事業者は、可能な限りプライバシーポリシー概要の掲載等を検討したり、説明や利用者情報取得、第三者提供等の方法が適切でないアプリケーションが判明した場合の対応を検討する等、基本原則や指針等を考慮しつつ、取組を協力して進めることが望ましい【望ましい事項】。

1.4. セキュリティの確保に係る取組[65]

1.4.1. アプリケーション提供者等

1.4.1.1. アプリケーション提供者[66]

［セキュリティ・バイ・デザインを確保するための取組］

- アプリケーション提供者は、アプリケーションの開発時には、セキュリティが適切に確保されるよう、アプリケーションの企画及び設計の段階から、当該アプリケーションにおけるセキュリティの確保について検討し、適切な仕組みをアプリケーションに組み込むことが強く求められる(例:業界標準の暗号化技術の使用[67]、最小権限、セキュアコーディング等)【基本的事項】。
- アプリケーション提供者は、提供するアプリケーションにおいて使用する情報収集モジュールについて、セキュリティの確保の観点から内容を確認することが強く求められる【基本的事項】。

［脆弱性があるアプリケーションへの対応等］

- アプリケーション提供者は、アプリケーションに係る脆弱性情報を継続して収集するとともに、アプリケーション内に発見された脆弱性について適切かつ迅速に報告を受けられるよう、脆弱性情報の窓口・連絡先を設置する等必要な体制を整備することが強く求められる【基本的事項】。
- アプリケーション提供者は、アプリケーションを提供する際にはセキュリティの確保に影響を与え得る脆弱性が含まれないようにあらかじめ確認するとともに[68]、セキュリティの確保に影響を与え得る脆弱性が発見された場合には、アプリケーションのアップデートを適切かつ迅速に提供する等、必要な対応を取ることが強く求められる【基本的事項】。

---

65 個人情報取扱事業者は、その取り扱う個人データの漏えい等の防止その他の個人データの安全管理のため、必要かつ適切な措置を講じなければならない【法令事項】(個人情報保護法第 23 条) ことに留意が必要である。なお、講じなければならない措置には、個人情報取扱事業者が取得し、又は取得しようとしている個人情報であって、当該個人情報取扱事業者が個人データとして取り扱うことを予定しているものの漏えい等を防止するために必要かつ適切な措置も含まれる (ガイドライン通則編 3-4-2)。

66 情報システム等の供給者は、利用者が情報システム等の安全性及び信頼性の確保のために講ずる措置に配慮した設計・開発、適正な維持管理に必要な情報の継続的な提供など、利用者がサイバーセキュリティの確保のために講ずる措置を支援する取組を行うよう努めなければならない【法令事項】(サイバーセキュリティ基本法第７条第２項)。

67 例えば、CRYPTREC (Cryptography Research and Evaluation Committees) の電子政府推奨暗号リストに掲載されている暗号技術を参照すること等が考えられる。

68 アプリケーション提供者による脆弱性の確認手段として、例えば以下のような取組が参考になる。
・第三者による脆弱性評価の実施 (脆弱性診断サービスなどの客観的かつ専門的視点をもつ診断事業者による脆弱性評価の取組)
・ウェブサービスに対するペネトレーションテストの実施 (スマホアプリと連携して動作するウェブサービス・API サービスに対するセキュリティ態勢の脅威ベースでの評価の実施の取組)
・事業基盤 (サービス環境) に対するペネトレーションテストの実施 (サービスを提供する事業者や組織の事業基盤に対する、セキュリティ態勢の脅威ベースでの評価の実施の取組)
・ツールによる脆弱性診断の実施 (オープンソースツールなどを利用した脆弱性診断ツールによる脆弱性の評価の取組)

- アプリケーション提供者は、提供するアプリケーションにおいて個人情報漏えい等のセキュリティインシデントが発覚した場合には、関係者に対して適切かつ迅速に周知することが強く求められる【基本的事項】[69]。

1.4.1.2. 情報収集モジュール提供者

- 情報収集モジュール提供者は、1.4.1.1を踏まえ、セキュリティの確保に取り組むものとする。その際、1.4.1.1 の適用に当たっては、適宜、「アプリケーション提供者」を「情報収集モジュール提供者」と、「アプリケーション」を「情報収集モジュール」と読み替えるものとする。

1.4.2. アプリストア運営事業者、OS 提供事業者

- セキュリティの確保の観点から、アプリストア運営事業者は、次に掲げる取組を進めることが望ましい。

［アプリストアとしての基本的対応］

① アプリストア内で提供されるアプリが満たすべきセキュリティ要件を示し、当該要件を満たしているかを審査する（例：業界標準の暗号化技術の使用、最小権限、セキュアコーディング　等）ことが期待される【ベンチマーク事項】。

② アプリストア内で提供されるアプリケーションについて、利用者情報が保存・処理される法域、利用者情報へのアクセスが許可される者の範囲、利用者情報へアクセスする目的、アップデートの最終更新日等の情報を公開し、利用者が購入及びダウンロードする前に確認可能な場を設けることが望ましい【望ましい事項】。

［脆弱性があるアプリケーションへの対応］

③ アプリストア内で提供されるアプリケーションが、脆弱性報告のための窓口を有し、かつ、アプリケーション提供者が適切なタイミングで脆弱性を開示するための手続を有していることを確認することが期待される[70]【ベンチマーク事項】。

④ アプリケーション提供者からアップデートが提出された場合には、利用者に対してアプリケーションが最新版にアップデートされるよう促す等、必要な対応を取ることが望ましい【望ましい事項】。

⑤ アプリケーションが長期間アップデートされない場合には、アプリケーション提供者にアプリのサポート状況を確認することが望ましい[71]【望ましい事項】。

---

69 個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失、き損等の事態であって個人の権利利益を害するおそれが大きいものとして個人情報保護委員会規則で定めるものが生じたときは、当該事態が生じた旨を個人情報保護委員会に報告しなければならず、原則として、本人に対し当該事態が生じた旨を通知しなければならない【法令事項】（個人情報保護法第 26 条）ことに留意が必要である。

70 関連する取組として、アプリケーション提供者は、適切な手段により脆弱性開示の取組を実施することが求められる。

71 関連する取組として、アプリケーション提供者は、サポート終了時にアプリストア運営事業者に連絡することが求められる。

［不正なアプリケーションへの対応］

⑥ アプリストアにおいて、利用者等が不正なアプリケーションを報告できるよう報告窓口を設置することが望ましい【望ましい事項】。

⑦ 不正なアプリを発見した場合には、速やかに当該アプリを削除するとともに、当該アプリケーションを作成したアプリケーション提供者が開発した他のアプリケーションについても調査を行うことが望ましい【望ましい事項】。

［アプリケーション削除・掲載拒否時の対応］

⑧ アプリケーションの掲載を拒否する場合には、その理由について、アプリケーション提供者に対して適切なフィードバックを行うことが強く求められる【基本的事項】[72][73]

- OS提供事業者は、利用者のためにセキュリティやプライバシーを保護するため、アプリストアが上記の取組を実施することを奨励するとともに、必要な措置を講じることが望ましい【望ましい事項】。

[72] デジタルプラットフォーム取引透明化法に基づき、特定デジタルプラットフォーム提供者の指定を受けた事業者は、特定デジタルプラットフォームの提供の拒絶を行うときには、当該拒絶の内容及び理由を開示しなければならない【法令事項】（デジタルプラットフォーム取引透明化法第５条第３項第２号）ことに留意が必要である。

[73] アプリケーション提供者へのフィードバックの方法については、英国コード・オブ・プラクティスにおける開発者に対する明確なフィードバックに関する規範を参照することが考えられる。

1.5. 青少年の保護に係る取組

1.5.1. アプリケーション提供者

- アプリケーション提供者は、自ら提供するソーシャルネットワーキングサービスやユーザー生成コンテンツなど青少年[74]と他の利用者の交流などが発生するアプリケーションにおいて、例えば、青少年による利用者情報の発信に係る注意喚起の仕組みや機能、青少年のプライバシーを含む情報など青少年保護の観点から不適切と考えられるコンテンツを報告する機能を備えるなど迅速に対応できる体制、ユーザーが不適切な言動を行うユーザーをブロックする機能などを備えることが望ましい【望ましい事項】。
- アプリケーション提供者は、提供するアプリケーションにおいて、青少年保護の観点から利用者情報の提供や課金の実施などのうち重要な判断が必要になる場合に、保護者の関与に関する仕組みや機能を備えることが強く求められる【基本的事項】。

1.5.2. アプリストア運営事業者

- アプリストア運営事業者は、運営するアプリストアに掲載する個別のアプリケーションに関して審査を行うことが望ましい[75]【望ましい事項】。当該審査を行う場合には、年齢制限設定(レーティング)に関する基準[76][77]を設定し、適切な年齢制限設定が行われるよう確認することが望ましい【望ましい事項】。
- アプリストア運営事業者は、アプリストアへのアプリケーションの登録審査について、その基準を作成し、あらかじめ公表するとともに、アプリケーションの掲載を拒否する場合には、その理由について、アプリケーション提供者に対して迅速かつ適切なフィードバックを行うことが強く求められる【基本的事項】[78]。
- アプリストア運営事業者は、運営するアプリストア内に青少年向けアプリケーションを集めた専用の分類を設けることが望ましい【望ましい事項】。

1.5.3. OS 提供事業者

- OS 提供事業者は、アプリストア運営事業者において、前節において取り組むことが望ま

---

74 青少年は 18 歳未満とされているが、利用者情報の取扱いに当たっては発達段階に対応した配慮を行うことが求められる。

75 OS 提供事業者が個別のアプリケーションに関して審査を行う場合を含む。

76 各国で広く一般に使用されている基準や国際的なレーティング基準（IARC（国際年齢評価連合）を含む）を採用することなどが考えられる。アプリストアの利用に関する年齢制限を設けている場合は、年齢制限設定（レーティング）を行うことを要しない場合がある。

77 年齢制限の設定が適切に機能するためには、関係事業者等により年齢等の発達段階が適切に把握されることが重要である。今後の技術的手段の発達や市場の状況を踏まえ、検討を行う。なお、年齢等の発達段階の把握の目的のために収集した情報は他の目的に使用しないことに留意が必要である。

78 デジタルプラットフォーム取引透明化法に基づき、特定デジタルプラットフォーム提供者の指定を受けた事業者は、特定デジタルプラットフォームの提供の拒絶を行うときには、当該拒絶の内容及び理由を開示しなければならない【法令事項】（デジタルプラットフォーム取引透明化法第５条第３項第２号）ことに留意が必要である。

しいとされている事項が実施されているか必要な確認を行うとともに、適切な措置を講ずることが望ましい【望ましい事項】。

- OS 提供事業者は、上記の措置に関して、アプリストア運営事業者に対して適切な説明及び情報提供を迅速に行うことが望ましい【望ましい事項】。
- OS 提供事業者は、個別のアプリケーションに関して審査を行う場合には、その基準を設定し、あらかじめ公表するとともに、アプリケーションの掲載を拒否する場合には、その理由について、アプリケーション提供者に対して迅速かつ適切なフィードバックを行うことが望ましい【望ましい事項】。
- OS 提供事業者は、アプリストアにおける個別のアプリケーションのダウンロード及び起動の可否、アプリストアの利用制限並びに、アプリストア及び外部ウェブサイトにおける利用者情報の提供及び課金に対する制限等を行うペアレンタルコントロール機能[79]を実施するために必要な役務を提供することが望ましい【望ましい事項】[80]。

79 ペアレンタルコントロール機能とは、保護者が青少年のアプリケーションの利用を適切に管理するための技術的手段をいう。

80 なお、関係事業者等は、アプリストアから提供される個別のアプリケーションに対してペアレンタルコントロール機能が作動し、利用される環境の実現に向けて、互いに協力や意見交換を行うことが求められる。

2. 今後の技術・サービスの進展に対する柔軟な対応

- 本指針は、新技術・サービスの進展、利用者情報の利用形態の変化等を踏まえ、必要に応じ、見直しが図られることが望ましい。

【補足】

今後、IoT 等の新技術・サービスが急速に進展することが予想される。本指針は、関係事業者等に対する、スマートフォンにおける利用者情報の取扱いに関わる取組を定めたものであるが、IoT 等の新技術・サービス等にも準用可能なものも存在すると考えられる。ただし、本指針は、必ずしも IoT 等の新技術・サービスを想定したものではなく、IoT 等の新技術・サービスに本指針を準用する場合には、十分な検討が行われることが望ましい。

また、多くの情報収集モジュールがアプリケーションに組み込まれていること、関係事業者等の利用者情報の取得、送信、利用等への関わり方が複雑化していること等、実際の情報利用の仕組みが極めて複雑化しており、利用者が自身の情報の取り扱われ方について、理解し、判断するということが今後困難となることが予想される。そのような中で、今後、利用者に対する、利用者が自ら判断するための十分な情報提供が難しい場合について、利用者情報の取扱いの在り方を検討する必要が生じることも想定される。

（以下略）