資料７－２

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（案）

令和７年９月

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 3
不適正利用対策に関するワーキンググループ 5
第１部　検討の背景 5
　第１章　不適正利用対策をめぐる環境変化 5
　　１　これまでの検討 5
　　２　環境変化 5
　　（１）いわゆる「闇バイト」犯罪 5
　　（２）特殊詐欺 6
　　（３）犯罪行為の巧妙化、高度化 9
第２部　携帯電話の本人確認のルール 10
　第１章　　携帯電話の本人確認に関する現在の対策 10
　第２章　　携帯電話の本人確認に関する課題と検討 12
　　１　SIM の不正転売 13
　　２　法人の代理権（在籍確認） 14
　　３　他社の本人確認結果への依拠 15
　　４　追加回線の本人確認 18
　　５　上限契約台数 19
　　６　データ SIM の本人確認 21
第３部　その他の特殊詐欺の電話・メール等の対策 23
　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 23
　第２章　　その他の特殊詐欺の電話・メール等に関する課題 24
　　１　固定・携帯電話、SMS・メール対策 24
　　（１）固定電話 24
　　（２）携帯電話、SMS・メール対策 25
　　２　スプーフィング 26
　　３　海外電話番号による詐欺電話 27
参考資料 28
通信ログ保存の在り方に関するワーキンググループ 30
１　現状の課題及び検討の経緯 30
２　改正案 31
参考資料 37
利用者情報に関するワーキンググループ 39
　第１章　検討の背景 39

１　これまでの検討 39
２　「今後検討を深めていくべき事項」 39
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 41
１　青少年保護 41
２　位置づけ 43
第３章　今後の検討課題 46
１　ウェブサイトに係る調査・検討 46
２　今後の検討の方向性 50
３　その他の検討課題 50
参考資料 51

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

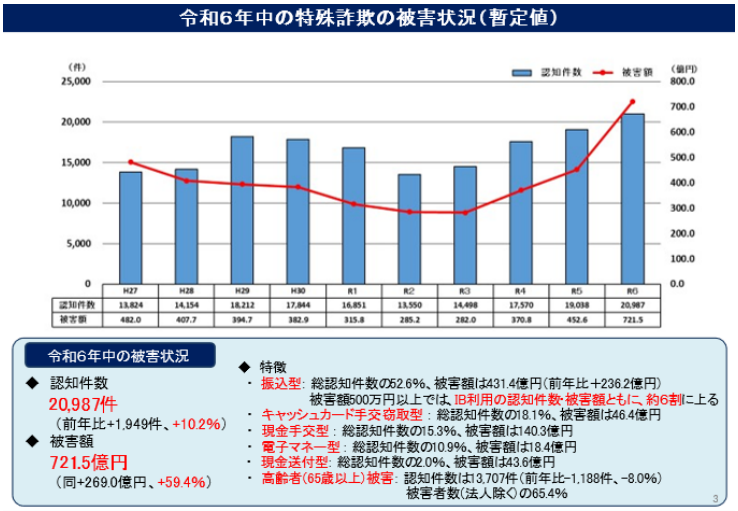
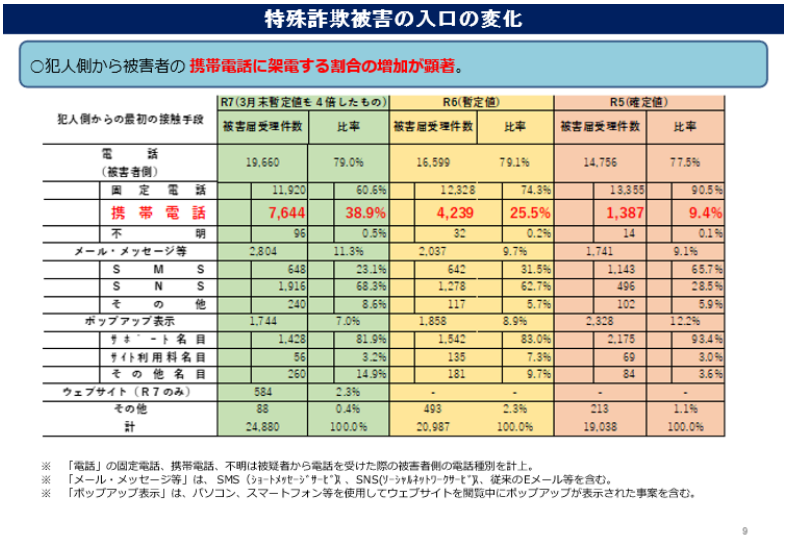


図１　令和６年中の特殊詐欺の被害状況（暫定値）[8]

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。

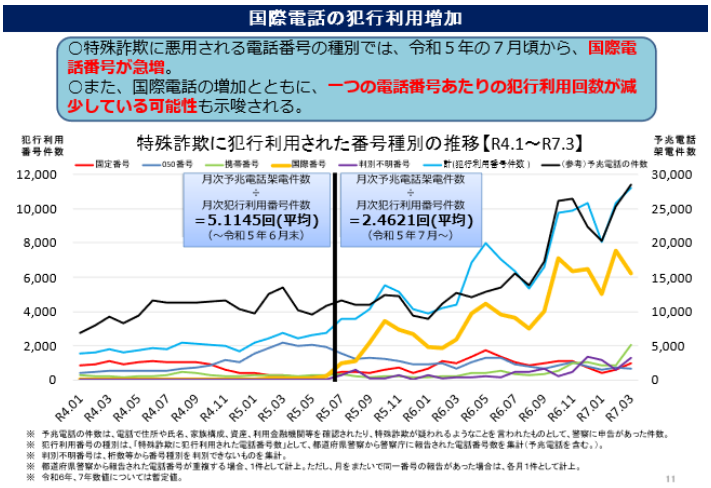
犯人側からの最初の接触手段		R7(3月末暫定値も４倍したもの) 被害届受理件数	R7(3月末暫定値も４倍したもの) 比率	R6(暫定値) 被害届受理件数	R6(暫定値) 比率	R5(確定値) 被害届受理件数	R5(確定値) 比率
電話（被害者側）		19,660	79.0%	16,599	79.1%	14,756	77.5%
	固定電話	11,920	60.6%	12,328	74.3%	13,355	90.5%
	携帯電話	7,644	38.9%	4,239	25.5%	1,387	9.4%
	不明	96	0.5%	32	0.2%	14	0.1%
メール・メッセージ等		2,804	11.3%	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。

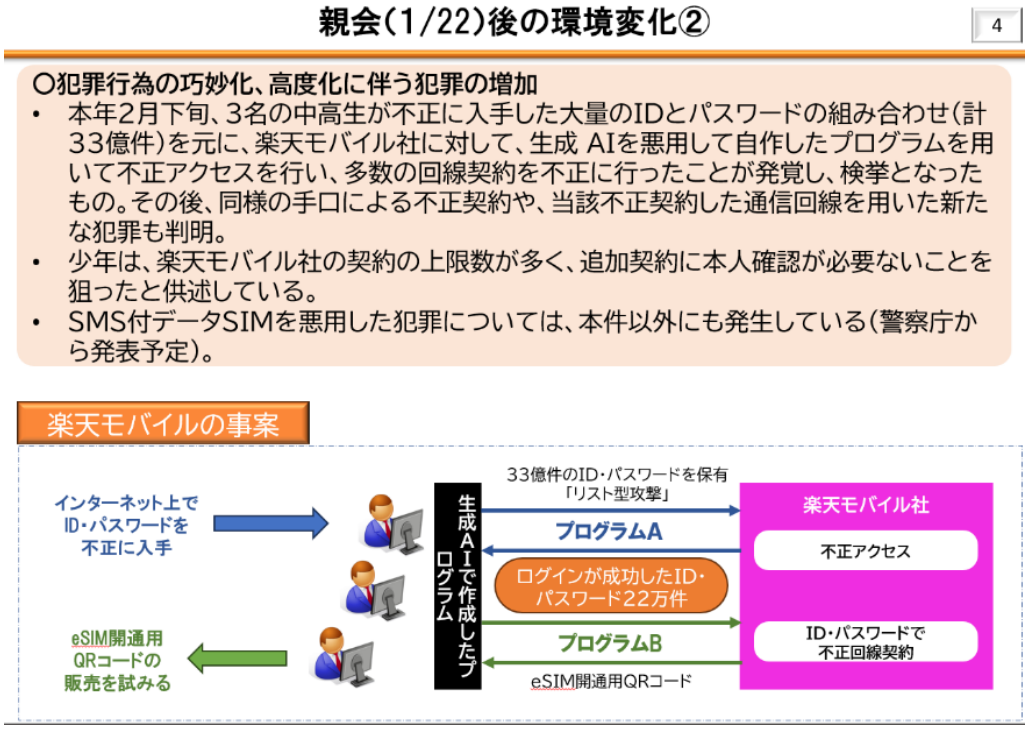


図４　犯罪行為の巧妙化、高度化に伴う犯罪[14]

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。

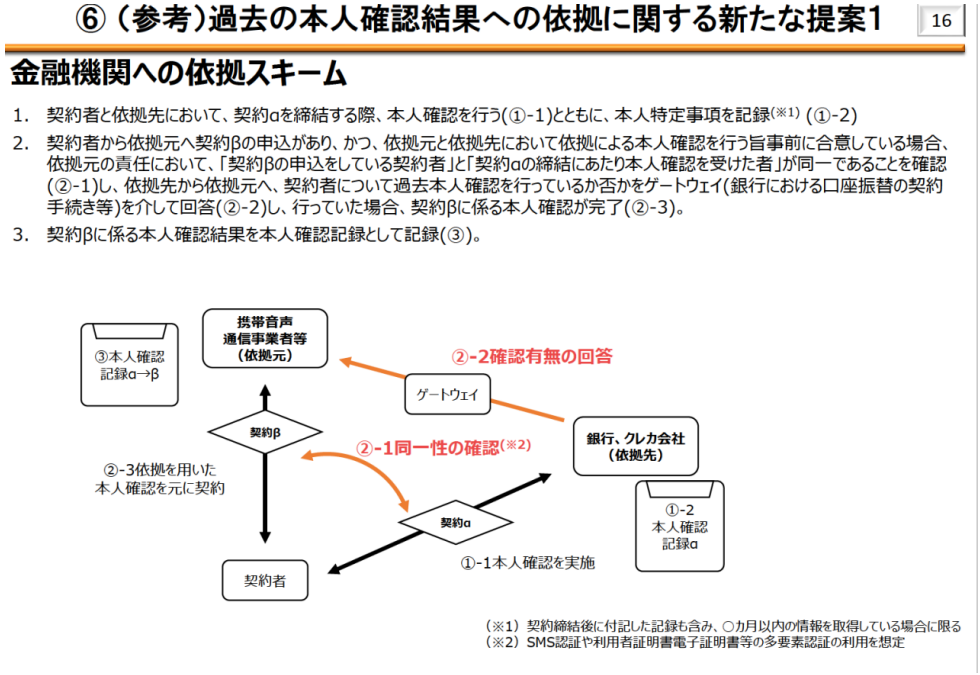


図６　金融機関への依拠スキーム[29]

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

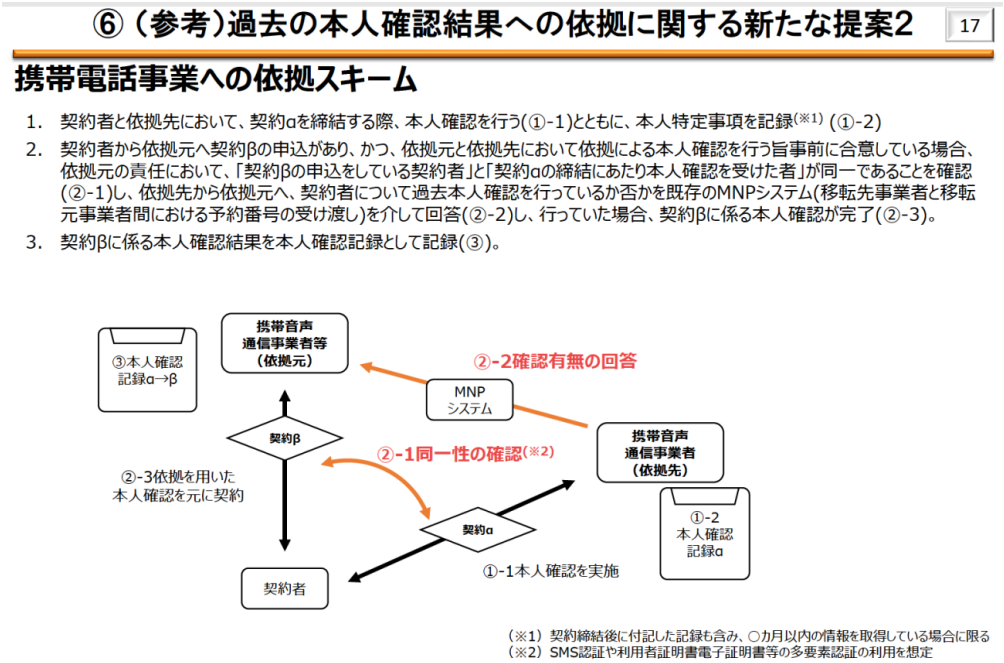


図７　携帯音声通信事業者への依拠スキーム[30]

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、その普

---

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）

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。

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。

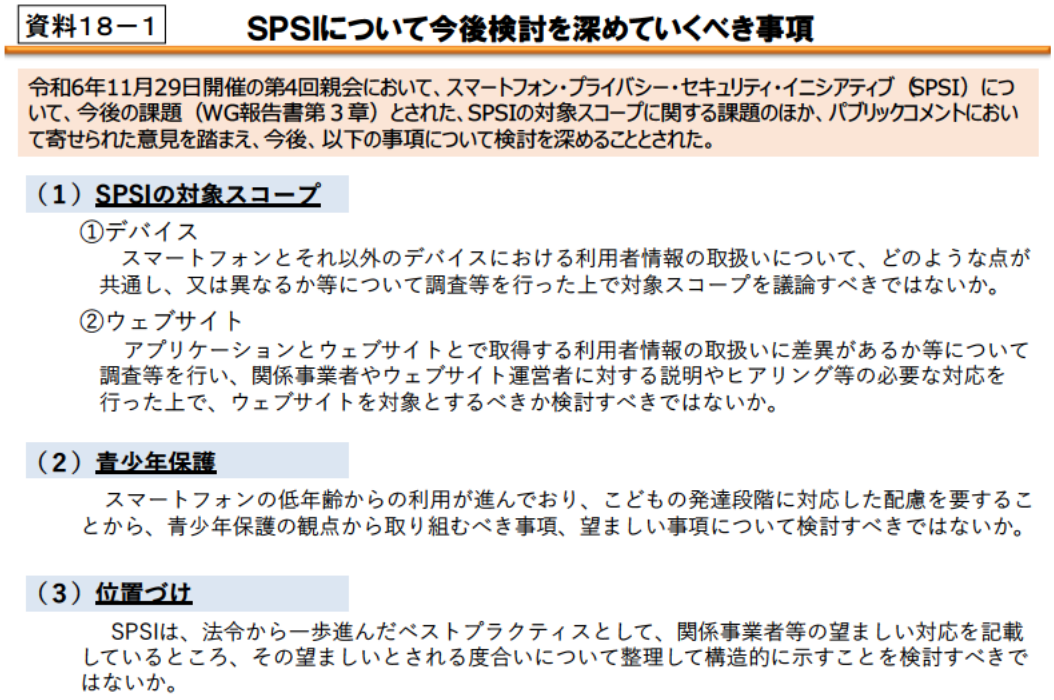
その後、国内制度の改正や諸外国及び民間事業者の動向に変化が生じていること等を踏まえ、令和６年３月から、「ICT サービスの利用環境の整備に関する研究会」（座長：宍戸　常寿　東京大学大学院　法学政治学研究科教授）（以下「研究会」という。）の下で開催される「利用者情報に関するワーキンググループ」（主査：山本　龍彦　慶應義塾大学大学院　法務研究科教授）（以下「本ワーキンググループ」という。）において、約７年ぶりに SPI の見直しについて議論を行い、同年 11 月、ダークパターンの回避やセキュリティの確保等について新たに規定した「スマートフォン プライバシー セキュリティ イニシアティブ（SPSI）」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

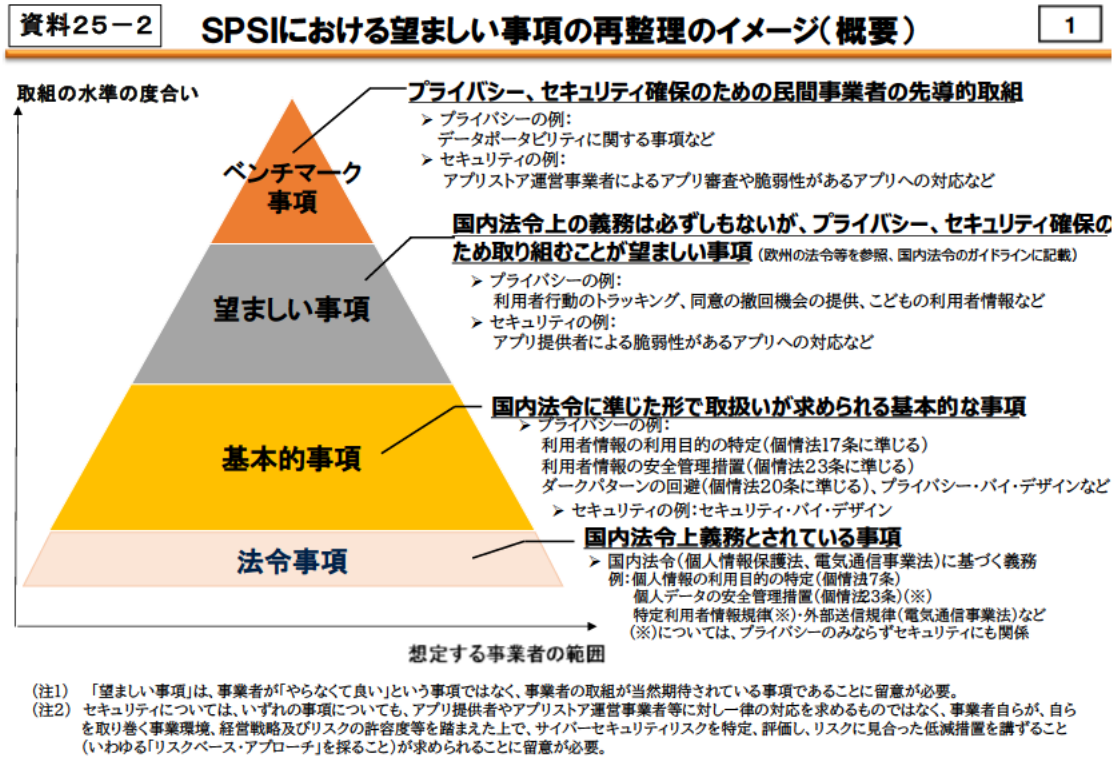


図２　SPSI における望ましい事項の再整理のイメージ（概要）[49]

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。

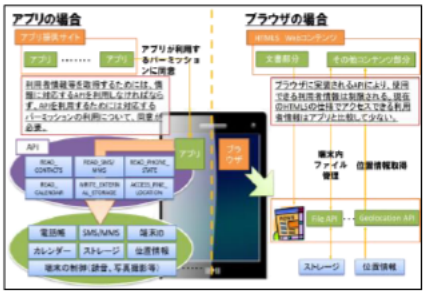
調査する事項（例）

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）

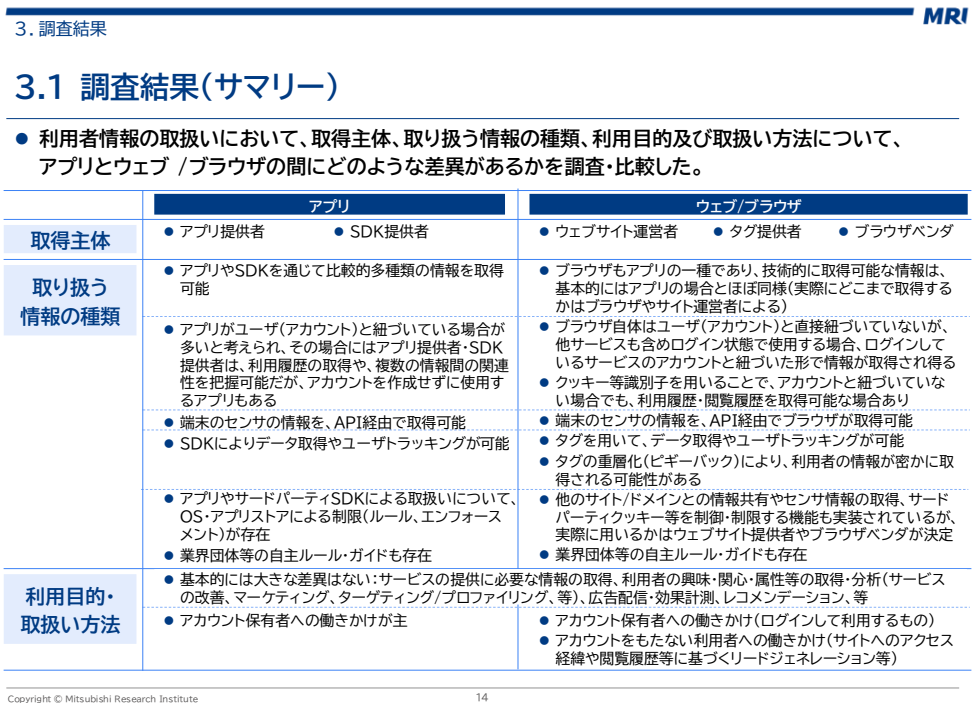


「スマートフォン プライバシー イニシアティブ」（平成24年８月）P74
図表5-3 アプリケーション及びブラウザがアクセス可能な情報等の違い

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

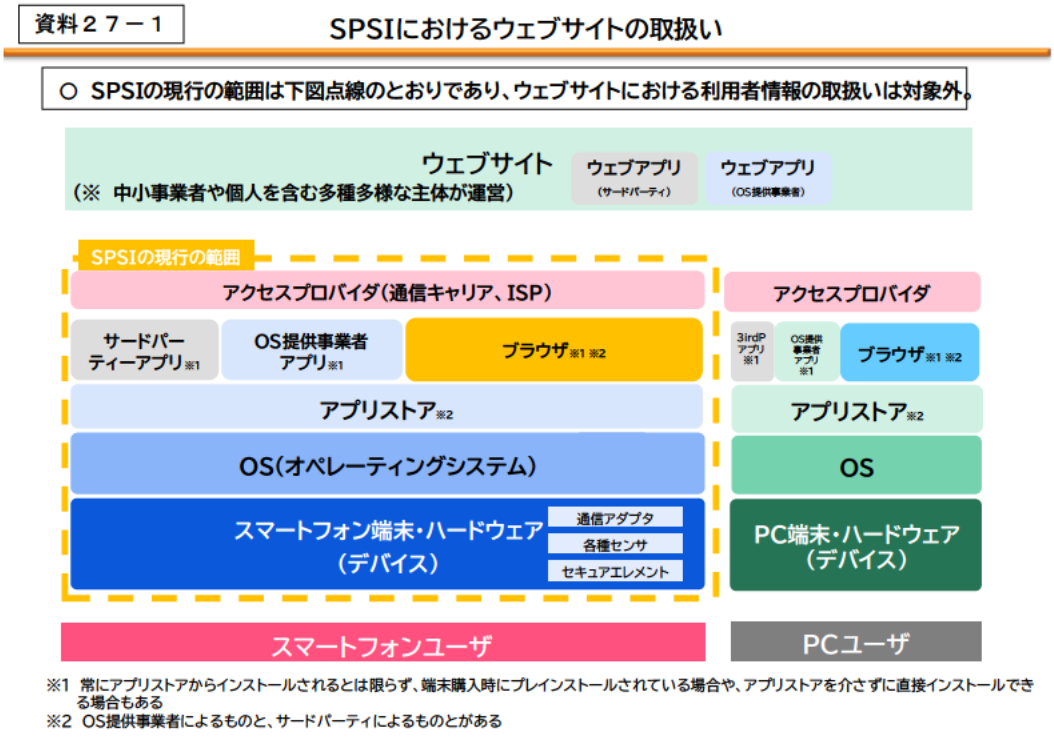


図５　SPSI におけるウェブサイトの取扱い[52]

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）