

総務省の「ICTサービスの利用環境の整備に関する研究会」にてまとめられた報告書案2点について行った意見募集について、NACSでは以下の通り意見を提出いたしました。」

利用者情報に関するワーキンググループ報告書（案）の要約

「SPI（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）では、ダークパターンや欺瞞的な行為の禁止が求められている。ダークパターンの具体例や、利用者が簡単に同意を撤回できる手段の提供も重要とされる。また、日本の商慣習に合った判断基準の設定が望ましい。スマホ以外のデバイスを含む情報収集の実態調査が急務であり、特に子どものプライバシー保護については強い規定が必要とされる。」

不適正利用対策に関するワーキンググループ報告書（案）の要約

「マルウェア感染端末への注意喚起やSMSフィルタリングによる感染検出、利用者への個別対応が重要である。また、不正SMS送信防止のための業界ルール整備や、ICチップを用いた認証による偽造防止も求められている。非対面契約の増加に伴い、本人確認の電子化にはプライバシー保護とデジタルディバイドへの配慮が必要である。確認記録の保存方法や情報開示も慎重に行うべきである。」

意見書

意見提出者

所属（会社名・団体名等）（※1）	公益社団法人 日本消費生活アドバイザー・コンサルタント・相談員協会
氏名（※2）	名称：公益社団法人 日本消費生活アドバイザー・コンサルタント・相談員協会 代表者の氏名：副会長 樋口 容子、副会長 丹羽 典明
住所（※2）	主たる事務所の所在地：東京都千代田区富士見2-4-6 宝5号館2F
連絡先	連絡担当者氏名：ICT委員会委員長 和知雅樹（わち まさき）

※1 個人の場合は「個人」と御記入ください。

※2 法人又は団体の場合は、名称、代表者の氏名及び主たる事務所の所在地を御記入ください。

意見提出フォーマット

<利用者情報に関するワーキンググループ報告書（案）>

頁	行目	章	項目	該当箇所	ご意見
12	210	2	2.	SPIにおいて、ダークパターンまたは欺瞞的な行為の禁止を明確に示す必要があるのではないか。その上で、ダークパターンの判断の線引きは難しい面もあるが、具体的に例示が必要ではないか。	ダークパターンについて、「判断の線引きは難しい面もあるが、具体的に例示が必要ではないか。」と寺田構成員の指摘に賛同します。 ただし、マーケティングや心理学等の観点から諸外国等で分類されているダークパターンには、ダークパターンに当たらないのではないかと思慮するものもあり、日本国内の商慣習や国民性などを鑑みて判断されることを望みます。
13	245	2	2.	これを踏まえ、EDPBによるガイドライン等も参照の上、原則として欺瞞的な方法による利用者情報の取扱いが行われないことが望ましい旨記載することとした。	<u>意見1</u> 記載にはダークパターンの具体的な例も示していただくことを要望します。 <u>意見2</u> 日本では違法とはされておらず、既存の規制の枠組みでも対処できるものであっても、諸外国の取組などを参考にして、禁止も視野にいれた法制度整備を希望します。 (理由) 例えばダークパターンは、消費者に「経済的損失」「プライバシーに関する被害」「心理的な被害」「時間の損失」など、様々な影響を及ぼす可能性があるためです。 <u>意見3</u> 賛成します。 (理由) 定期購入やレスキュー商法など、まさに欺瞞的なダークパターンにより、消費者をだます表示が横行しています。消費生活相談の現場には、それらの相談が多数寄せられています。 EUのDSAにおいてダークパターンが明示的に禁止さ

					れている (P10) ことを踏まえ、SPI では、同意の取り方や、ダークパターン等の禁止を記載すべきと考えます。
18	382	2	2.	簡単にアクセスでき、かつ分かりやすい方法で同意の撤回ができる機会を提供し、またその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旨、記載することとした。	対応を評価します。その上で、将来的には、記載を義務付けることと、撤回の申し出があった場合は必ず撤回手続きを行うことを記載すべきと考えます。 (理由) 本来、「同意」は事業者等から提示された内容をよく確認し、納得した上ですべきものですが、一般の消費者は時間の制約や提示内容が多いことなどから、よく確認せずに「同意」をしている場合がよく見られます。ダークパターンでも、このような習性を利用したものがあります。このような実情から、同意の撤回ができることとその方法についてプライバシーポリシー等に記載することは重要です。
21	423	2	2.	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場合には同意取得を行うことや、位置情報や写真データ等にアクセスする場合には、同意取得を行うとともにアクセス範囲の限定等の設定を可能とすることが望ましい旨記載することとした。	記載することに賛同します。 併せて「同意」することの重さを各自が感じることができるとの啓発が大切と考えます。 (理由) 消費生活相談の現場では、安易に同意をしてトラブルを招いている実態があるからです。
23	470	2	2.	KDDI 株式会社から、令和 5 年度「通信アプリに含まれる不正機能の検証に関する実証」について説明があった。	WG の同社配布資料には、スマホは常時ネットワークに接続された状態で利用者が携帯することから、利用者の行動履歴や通信履歴等の情報を多数収集・蓄積することが可能とあります。セキュリティと自身の情報を安易に流さないためにも、利用者の意図しない利用者情報の取扱いの実態について、更に周知すべきと考えます。

25	517	3	—	<p>・タブレットやスマートウォッチ、スマート家電、コネクテッドカー等、スマホ以外のデバイスを対象にする必要はないか。そのまま SPI を対応させることは難しいかもしれないが、例えばスマホと違いがあるのか、どのような点が共通しているか、調査検討する必要があるのではないか。（第1回寺田構成員）</p> <p>（対応の方向性） まずは、対象範囲はスマートフォンとしつつ、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。</p>	<p>現状でも様々な切り口で、極めて多くの情報を取得できるデバイスが存在することから、次回の改定を待たずに議論を始めることが急務と考えると考えます。</p> <p>（理由） スマートウォッチやスマートリングは利用者の身体情報を常時取得することが可能です。見守りカメラは被監視者の生活状況を常時取得することが可能です。また、スマートスピーカーや電子ペットは生活状況に加え、端末への声掛けの状況なども取得できます。</p>
35	5	1.1.4	①	<p>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。</p>	<p>「P22、449 行目のアイコン等を用いてアプリストアの個別ページに掲載する方法が考えられる旨記載することとした」とあるように、この項にも「アイコン等を用いる方法が望ましいとの追記を希望します。</p> <p>（理由） 小さなスマホ画面では視認性の問題がよく言われます。長文のプライバシーポリシーを読むのが苦痛で安易に同意する利用者が一定数いるため、重要事項は、標準化の考え方で、わかりやすい表示を推奨してください。</p>
46	32	1.2.1.2	⑧	<p>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。</p>	<p>変更を行ったとき、及び変更により利用者情報の変更が行われる場合には、利用停止をできるか、また、利用停止後にアプリケーションの利用が可能か</p>

					<p>についても記載することが望ましいと追記を希望します。</p> <p>(理由)</p> <p>P53(3)の3番目の項に同意取得の必要性の記載がありますが、プライバシーポリシーにも記載を望みます。アプリを長期間利用していた場合は、ロックイン状態になっているため、変更内容に納得がいらず利用を停止したいと思ってもできなくなっている可能性があるためです。</p>
49	17	1. 2. 1. 2	③	<p>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。</p>	<p>こどもの利用者情報の項では、「望ましい」ではなく、「強く望まれる」「必要である」等の表現に変更してください。</p> <p>(理由)</p> <p>こどもは、契約など様々な場で保護されています。他の項目より、強い表現が必要と思われます。</p>

<不適正利用対策に関するワーキンググループ報告書(案)>

頁	部	章	項目	該当箇所	ご意見
11	1	2	1	<p>マルウェア感染した端末及び回線を特定の上、同端末及び回線利用者への注意喚起を行うことが必要である。</p>	<p>注意喚起を行うことに賛同します。</p> <p>(理由)</p> <p>消費生活相談の現場において、マルウェアに感染し、意図せずSMSを不特定多数に送付したという相談が寄せられています。高齢者はandroidスマホの所有率が高いため、通信の秘密の窃用等の問題を法的にクリアし、同社スマホの利用者への注意喚起が行えるようにしてもらいたいと思います。</p>
13	1	2	1	<p>通信キャリアが提供するSMSフィルタリングサービスでブロックしたSMSの通信通内容等を用いて注意喚起すべきマルウェア感染端末を検知し、通信に係るログ情報を利</p>	<p>左記によって、マルウェア感染による不正なSMS発信以外の、利用者が意図して行った利用履歴までもが拾い上げられることのないよう、取得方式の検討を望みます。また、取得した利用履歴が目的外利用</p>

				用し、マルウェア感染端末を使用している利用者を特定の上、個別に注意喚起を行う取組については、上述の条件を満たす場合には、契約約款等による包括同意であっても本件対策を行うための通信の秘密に属する事項の利用等について有効な同意であるということができ、有効な同意に基づいて実施するのであれば、通信の秘密の侵害に当たらないと整理することができる。	されることのないよう、データの慎重な管理を望みます。
14	1	2	3	SMS 発信元の明確化・透明化に係る取組やSMS 認証代行業者等の悪質事業者への対策などを盛り込んだ業界 ルールを策定し、正規メッセージがしっかり正規のものと分かる形で配信されるよう、効果的な対策を実行する必要がある。	左記の対策実行に賛同します。 (理由) キャリア等が既にスミッシングを防ぐ取り組みを行っているので、業界ルールをさらに整備し、不正なSMS 発信を根絶することを希望します。
19	2	1	3	対面契約の場合でも目視による真贋判定だけに頼るのではリスクが高くなっているのではないかと指摘されている状況を踏まえ、マイナンバーカードに搭載されているICチップを活用した公的個人認証による確認方法や、運転免許証等の本人確認書類に搭載されたICチップの情報を読み取る方法など、デジタル技術を活用した本人確認方法を導入すべきではないかとの意見があった。	この意見に賛同します。 P22⑧の問題をクリアして早期の導入に期待します。 (理由) 身分証明書等の偽造精度が向上し、キャリアショップの販売員レベルでは偽造を見破るのが難しくなっていると想像されます。不適正契約を防ぐため、購入者のプライバシーに配慮しつつ、埋め込まれたICチップを利用した本人確認する方法(手順)の確立が必要と考えるためです。
20	2	1	3	スマートフォンに搭載された情報の活用によって本人確認を行うことが可能となるため、携帯電話契約時の本人確認にも適用されるよう、携帯電話不正利用防止法施行規	左記の提案に賛同します。 (理由) 既に各キャリアショップでは、マイナンバーカードや運転免許証の偽装チェックを体系的に行っていると聞いています。スマホに搭載したカード代替

				則を整備するべきではないかと提案があった。	電磁的記録で本人確認が行えるよう、施行規則の整備を希望します。
24	2	1	3	デジタル技術の活用が難しい高齢者等の利用者への対応や災害時（通信障害時）の対応への考慮が必要である。	左記の対応への考慮することに賛同します。 （理由） 超高齢化社会の進展に伴い、消費生活相談の現場ではデジタルディバイド関連の相談が増えています。サポートの中に、保管方法を含め、悪用されないための啓発も含めて必要と思います。
24	2	1	3	また、プライバシーの保護や新たな不正利用のリスクへの対策という観点から、本人確認書類の写しや券面の画像情報なども確認記録に保存しないようにするといった、電子的確認方法における確認記録への保存の在り方の見直しを行うべきではないかといった意見があった。	見直しと同時に、電磁的方法における確認記録の保存方法（どの国、どの企業のサーバーにどのくらいの期間保存されるか等）の見直しを行うだけでなく、利用者にもその情報を開示することを希望します。 （理由） 価格的に有利なオンライン料金プランの普及により、今より今後非対面での契約が増えていくと思われます。非対面契約時の電子的確認方法が一般的になることには賛成します。しかし、昨今、大量の個人情報流出するインシデントが起きていることを勘案すると、身分証明書を電磁的に提出することに躊躇する人も多いのではないのでしょうか。不正利用が発覚した場合に警察からの照会に対応するためにも一定期間保存も必要と思われるので、利用者にも開示することが必要と考えます。