別紙１

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）についての意見募集で寄せられた意見

○　意見募集期間：2025 年７月５日～2025 年８月４日

○　意見提出数：57 件

※意見提出数は、意見提出者数としています。

※いただいた御意見につきましては、記載の明確化のため、体裁の修正や実質的な内容の変更をもたらさない形式的な修正を行っております。

受付順	意見提出者	受付順	意見提出者
1	JCOM 株式会社	9	UUUM 株式会社
2	一般社団法人日本音楽事業者協会	10	一般社団法人モバイル・コンテンツ・フォーラム
3	株式会社ラック	11	楽天モバイル株式会社
4	株式会社 NTT ドコモ	12	一般社団法人安心ネットづくり促進協議会
5	一般社団法人日本スマートフォンセキュリティ協会	13	ソフトバンク株式会社
6	一般社団法人クリエイターエコノミー協会	14	一般社団法人日本インタラクティブ広告協会
7	一般社団法人テレコムサービス協会	15	KDDI 株式会社
8	スカイワゴン株式会社		個人（42 件）

不適正利用対策に関するワーキンググループ

提出された御意見	御意見に対する考え方（案）	御意見を踏まえた案の修正の有無
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		
［意見］ 本人確認を的確に行われるために、 携帯音声通信事業者について、 人材サービス業者から、 キックバックをもらい受けないよう、 ご指導と、税務調査等での監視をお願い致します。 ［理由］ 携帯電話の新規契約時、譲渡時及び貸与時の本人確認につきまして、 実際は、店頭（ショップ）で、 携帯音声通信事業者ではなく、人材派遣スタッフが行っている事例が多いです。 なぜなら、求人情報で、携帯電話の販売スタッフの募集がございます。 募集を行っているのは、主に、携帯音声通信事業者ではなく、 人材サービス業者が求人を行っております。 よって、人材サービス業者が、 不正に携帯電話を入手しようとする組織と結びついていれば、 本人確認について、まともに行われないリスクがございます。 なお、人材派遣契約を受けるときに、 発注者が、受注者の人材サービス業者から、 キックバック（金品）をもらい受けることが常態化しております。	今回お寄せいただいた御意見も参考にしつつ、検討を進めて参ります。	無

こうなると、お金をもらい受ける携帯音声通信事業者は、 お金を払う人材サービス業者の言いなりになることがございます。 キックバックのお金は、出所が不明でございます。 不正に携帯電話を入手しようとする組織からの金品である懸念がございます。 私は、キックバック（金品）をもらい受けない人が、報われる社会を望んでおります。 以上、お手数をおかけしますが、制度が正しく運用できるよう、管理のほどをお願い申し上げます。敬具 【個人】		
第２部　携帯電話の本人確認のルール 第２章　携帯電話の本人確認に関する課題と検討		
１ SIM の不正転売		
・定期的な本人確認の必要性が海外を含む業界で議論されて始めていることは認識しております。 ・一方で、定期的な本人確認を継続的に実施する場合、お客様は利用継続のために都度本人確認書類を準備し定期的な本人確認に対応する必要がある等、お客様・事業者双方の負担が増加することが懸念されます。 ・そのため定期的な本人確認は、お客様負担影響とその軽減方法、及び不正契約抑止効果を踏まえて慎重な検討を要望いたします。なお、カード代替電磁的記録による本人確認や JPKI 等の利便性の高い本人確認手法がより一層普及することで、お客様負担の軽減に繋がる可能性も考えられます。 【株式会社 NTT ドコモ】	今回お寄せいただいた御意見も参考にしつつ、本人確認方法の在り方等について、検討を進めて参ります。	無
闇バイト等による SIM の不正転売は、偽造された本人確認書類等による不正契約ではなく、騙された消費者から真正の本人確認書類により正しく契約が行われることが多いため、事業者における取組の推進にて例示されて	今回お寄せいただいた御意見も参考にしつつ、検討を進めて参ります。	無

いる「定期的な本人確認」については、闇バイト等による SIM の不正転売の抑止に繋がりづらいものと考えております。 闇バイト等による SIM の不正転売が犯罪行為であることを、事例を踏まえて官民連携のうえ広く周知啓発・注意喚起を行っていくことが非常に重要であると考えます。 【一般社団法人テレコムサービス協会】		
SIM の不正転売の防止に向けて、犯罪抑止の観点から政府に加え「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」が必要（P14）とされているところ、当社では、店頭にて回線契約または製品を購入されるお客様に対し、不正転売の違法性に対する理解促進、それによる不正行為抑止の観点から、周知啓発に係る以下の取組を実施しております。 ・重要事項説明書により不正転売等を含む禁止行為を説明 ➢ 店頭契約に際し、スタッフとお客様とで上記を含む重要事項説明書の内容等を読み合わせ、お客様による個別確認及び署名を依頼 ・SIM 送付時の外装に啓発シールを貼付し、禁止行為（受領後に第三者へ転送、転売する行為等）について注意喚起 また、「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」（P14）とされているところ、本来役務提供をすべきではない申込を排除する精度が高まり、不正転売等の犯罪抑止に繋がると考えられることから、今後も与信時の審査強化等に適切に取り組んでまいる所存です。 なお、定期的な本人確認については、利用者及び事業者への負担が大きい一方で不正転売を行う者は、契約後短期間のうちに転売すると考えられることから、不正転売等の犯罪抑止の効果は限定的と思われるため、慎重に検討すべきと考えます。ただし、不正利用等が疑われる契約者に対し、事業者の判断により本人確認を求め、これに応じない場合に利用停止等できるようにすることは望ましい措置であると考えます。 【楽天モバイル株式会社】	今回お寄せいただいた御意見も参考にしつつ、本人確認方法の在り方等について、検討を進めて参ります。	無

SIMの無断譲渡は明確な違法行為であり、政府主導でその違法性の周知徹底を行うことで、一定の抑止効果が期待でき、業界全体としての適正な利用環境の構築につながるものと考えます。 不正転売を未然に防ぐことを目的とした「定期的な本人確認」の導入については、顧客利便性を損なう可能性があることに加え、事業者にとっても運用コストが生じる一方で、転売行為そのものを未然に防ぐ効果は限定的であるため、導入は不要と考えます。現在、携帯電話業界では公的個人認証（JPKI）による本人確認の導入及びその拡大が見込まれており、より簡易かつ正確な本人情報の取得が出来るようになると想定されるため、こうした認証手段の高度化の状況を見極めた上で検討すべきと考えます。 【ソフトバンク株式会社】	今回お寄せいただいた御意見も参考にしつつ、本人確認方法の在り方等について、検討を進めて参ります。	無
また、14ページに記載されている「構成員からの指摘」の中に、「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」というものがありました。この2点の指摘について同意します。そのような事例に関与すること自体が自身にとって危険なことであるという意識を、利用者それぞれが持つべきだと思うので、啓発として有用であると考えます。「気軽に」「知らないうちに」ネットワークや通信を用いた犯罪行為に加担することを防ぐためには、わかりやすく警告をすることが必要だと思います。 【個人】	本文の記載への賛同の御意見として承ります。	無
不正利用をしていない大多数のお客様に対して定期的な本人確認を求めることは、お客さまにとって負担が大きいと考えます。 既存のお客さま全てが定期的な本人確認に対応いただくことは現実的に困難であり、定期的な本人確認に応じていただけないことをもって、通信停止や解約を行うのか等、役務提供上の課題が生じると考えられるため、慎重に検討いただくことを要望いたします。 【KDDI株式会社】	今回お寄せいただいた御意見も参考にしつつ、本人確認方法の在り方等について、検討を進めて参ります。	無

２ 法人の代理権（在籍確認）		
・当社では、委任状により来店者が法人代理権を有することの確認、又は名刺若しくは社員証等により来店者の在籍確認を実施しております。 ・法制度化をする場合、必要な在籍確認書類の選択肢を統一することは考えられますが、例えば営業担当者が法人事務所を訪問し契約手続きを行う場合等、当該法人と法人担当者の関係性が明らかな場合は在籍確認書類の提出を省略可能とする等、慎重な検討を要望いたします。 【株式会社 NTT ドコモ】	今回お寄せいただいた御意見も参考にしつつ、本人確認方法の在り方等について、検討を進めて参ります。	無
法人の担当者が契約を行う場合、当社では在籍確認のため以下の書類を提出頂いているところ、事前に確認頂けるよう、当社 Web サイト等で明示しております。 ・　法人の登記事項証明書又は印鑑証明書等 ・　担当者の本人確認書類 ・　担当者の名刺、社員証、健康保険証又は在籍証明書のいずれか また、「利用者目線に立って予見可能性を高める観点から（略）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」（P15）とされているところ、「最低限必要な書類」の規定方法によっては、事業者による本人確認方法の裁量が制限されるとともに、事業者の判断により不正が疑われる申込者に法令で規定されていない書類を要求することとなった際、当該申込者との意思疎通が困難になる事態も想定されることから、書類の種類等につき規定で詳細に定めることは不要と考えます。 【楽天モバイル株式会社】	今回お寄せいただいた御意見も参考にしつつ、本人確認方法の在り方等について、検討を進めて参ります。	無
法人の代理権（在籍確認）については、与信に関する各社の考え方によるところであり、法令で一律に統一することは、各社の柔軟な与信判断を妨げる可能性があることから、法令等での統一化まで図る必要はないと考えます。仮に見直しを行う場合においても、現行の事業者の取組みを踏まえ、各事業者への負荷を生じさせないことを前提とした見直しの検討が必要と考えます。	今回お寄せいただいた御意見も参考にしつつ、本人確認方法の在り方等について、検討を進めて参ります。	無

利用者目線に立った予見可能性を高めていくことは必要ですが、法令等での定めを遍く利用者が認識することは困難であり、利用者と事業者とのコミュニケーションの中で適切な案内がされることが肝要と考えます。弊社においては会社ホームページで必要書類を掲示する等利用者利便に配慮した取り組みを実施しています。 また、利用者は、携帯電話契約に限らず、銀行口座開設や取引先との契約など、様々なビジネスシーンで法人関連の書類を準備・提出する機会があり、多くの場合、企業内で一元的に管理していることが想定されるところ、書類が事業者間で統一されていることが利用者の利便性に与える影響は限定的と考えます。 【ソフトバンク株式会社】		
今後、規定見直しが行われる場合は、お客さまへの周知等含め、一定の準備期間をいただけるよう要望します。 また、最低限必要な書類については、偽造が比較的容易である書類（例えば名刺等）を除くことは考えられると思いますが、偽造が容易でない書類については、複数の選択肢の中から選択できるようにすることや、担当者と法人の関係性を確認する趣旨であれば、訪問による確認の他、電話・Eメールによる確認等の手段も考えられるなど、複数の書類や手段による選択肢の中から選択できるようにすることを要望します。 なお、訪問して法人契約を受付する等、相手方担当者が明らかに当該法人に在籍していると考えられるような場合は、当該担当者と法人の関係性を明らかにする書類の要否も含め、来店して法人契約を受付する場合とは、区別して規定するべきと考えます。 【KDDI 株式会社】	本見直しに係る携帯電話不正利用防止法施行規則の施行に当たっては、いただいた御意見を参考にしつつ、検討を進めるとともに、適切な準備期間が確保されるよう努めて参ります。	無
３ 他社の本人確認結果への依拠		
・他社の本人確認結果への依拠については、依拠先の本人確認（身元確認の保証レベル）、契約者の同一性確認（当人認証の保証レベル）が適切に	今回お寄せいただいた御意見も参考にしつつ、本人確認方法の在り方等について、検討を進めて参ります。	無

行われない場合、なりすまし等不正申込の発生がリスクとして想定されるため、慎重な検討が必要と考えます。 ・ そのため、依拠先における適切な本人確認や本人確認記録の最新化の担保や依拠元における適切な本人同一性確認について、適切な方法が実現可能か十分な検討が必要と考えます。 【株式会社 NTT ドコモ】		
依拠先の他社の本人確認結果が法令に基づくものであれば、広く普及しているサービス間等で安全に当該本人確認結果を活用することにより多くの利用者が利便性を享受でき、当人認証レベルの確保も同時に実現可能であると考えます。 なお、「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」（P18）とされているところ、社会インフラである携帯電話においても、デジタル 3 原則に基づく本人確認手続きの必要性は高いことから、本人確認の保証レベルを上げる取組と並行して、既に実施されている取組をベースとしつつ、本件のルール整備を早期に推進頂きますようお願い致します。 【楽天モバイル株式会社】	今回お寄せいただいた御意見も参考にしつつ、本人確認方法の在り方等について、検討を進めて参ります。	無
本報告書案で示されたとおり、本人確認に用いられる認証手段に関しては、保証レベルの高さと情報が最新であることが重要です。その観点から、本人確認の依拠先としては、公的個人認証を行っている事業者に限定すべきと考えます。 【ソフトバンク株式会社】	今回お寄せいただいた御意見も参考にしつつ、本人確認方法の在り方等について、検討を進めて参ります。	無
記載の考え方に賛同いたします。 まずは店頭やオンライン契約における本人確認強化の取組をしっかり進めていき、本人確認の精度をより高めることが先決であると考えます。 【KDDI 株式会社】	本文の記載への賛同の御意見として承ります。	無
４ 追加回線の本人確認		

・当社は現状、2回線目以降の契約について、基本的には音声・データ通信契約に関わらず、1回線目と同様に本人確認書類の提示による本人確認を実施しております。 ・ワンナンバーサービス・副回線サービスについては、すでに音声通信契約をご契約済みのお客様が付加的に利用可能なサービスであるため、例外としてwebサイトにおける申込み時にID/PASS等による本人確認を実施しております。 ・ID/PASS等による本人確認はなりすましの可能性が高いと認識しておりますが、音声SIMとのペアリングを前提とするウェアラブルデバイス利用においては、規定の見直しによりお客様利便性が下がる懸念があるため、JPKI等の利便性の高い本人確認手法の普及状況等も踏まえ慎重な検討を要望いたします。 【株式会社NTTドコモ】	今回お寄せいただいた御意見も参考にしつつ、本人確認方法の在り方等について、検討を進めて参ります。	無
簡易な本人確認手法の厳格化に向けた規定の見直しの検討にあたっては、消費者の利便性を維持する観点からも、必要最低限の見直しとなるようご議論いただくことを要望いたします。 簡易な本人確認手法については、現行法令に基づく対応に加えて「多要素認証等の追加実施」により当人認証レベルを高めることで、犯罪の起点となることを抑止することができるものと考えます。 【一般社団法人テレコムサービス協会】	今回お寄せいただいた御意見も参考にしつつ、本人確認方法の在り方等について、検討を進めて参ります。	無
2回線目以降の回線契約時の本人確認に関し、「当人認証性を向上させるべく、（略）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」（P19）とされているところ、追加回線の本人確認においては、現行法令に基づく対応に加え、多要素認証等を追加実施等することにより当人認証レベルを高めることができ、結果、不正契約の抑止に繋がると考えます。 当社では、既契約者の本人確認情報に変更がない場合の追加回線の申込において、法令ではいずれかで良いとされているID/PASS方式及び本人確認情報を提示する方式を併用しての本人確認に加え、本年4月より既契約番号へのSMS通知及びワンタイムパスワード認証の追加実施を開始し、その不正防止効果を確認しているところです。	今回お寄せいただいた御意見も参考にしつつ、本人確認方法の在り方等について、検討を進めて参ります。	無

【楽天モバイル株式会社】		
2回線目以降の契約に際して、1回線目と異なる法令上の要件が設定されている点については一定の合理性があると考えます。 一方で、IDやパスワードの詐取を通じた不正契約の防止を徹底するためには、既存回線を利用したログインの必須化や、ワンタイムパスワード等による認証の導入など、当人認証性のさらなる強化が必要です。 その上で、こうした当人認証性の強化が図られることを前提とすれば、主たる回線契約時に実施された本人確認結果を活用して、以後の契約における本人確認手続を一定程度簡素化することは、利用者の利便性向上に資する合理的な措置であると考えます。とりわけ、オプションのようなかたちで提供される付随的な回線契約については、不正利用のリスクが相対的に低いと想定されるため、本人確認手続の簡素化を認める等、利用実態やリスクの度合いも踏まえた検討が必要と考えます。 【ソフトバンク株式会社】	今回お寄せいただいた御意見も参考にしつつ、本人確認方法の在り方等について、検討を進めて参ります。	無
AppleWatchや副回線（au回線の通信がつながりにくい時でも、切り替えてご利用いただけるもの）のように、本人確認を行った主契約に紐づくサービス等については、引き続き簡易な本人確認手法を実施できることを要望いたします。 【KDDI株式会社】	今回お寄せいただいた御意見も参考にしつつ、本人確認方法の在り方等について、検討を進めて参ります。	無
５ 上限契約台数		
本案に賛同いたします。 今後のモバイル通信サービスは、IoT等による利用シーンの拡大により多様化することが想定されるため、契約台数の上限規制はそのようなイノベーションを阻害することが強く懸念されます。 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る必要が生じた場合は、そのような観点も踏まえつつ、ご議論いただくことを要望いたします。 【一般社団法人テレコムサービス協会】	本文の記載への賛同の御意見として承ります。	無

契約台数の上限について、「（略）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るべきである」（P.20-21）とされているところ、当社としては、多要素認証等による当人認証の強化は不正契約自体の抑止に繋がると考えており、引き続き適切な対応を進めてまいる所存です。 なお、「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、（略）何らかのルール化について検討すべきである」（P21）とされているところ、当該検証を行うにあたっては、事業者に過度な負担を課すものとはならないよう留意頂きたく存じます。 【楽天モバイル株式会社】	今回お寄せいただいた御意見も参考にしつつ、本人確認方法の在り方等について、検討を進めて参ります。	無
不正への対策としては、まずは本人確認の徹底、SIM の無断譲渡が違法であることの周知徹底、2 回線目以降の本人確認における当人認証性の強化（ワンタイムパスワードによる認証等）等が必要と考えます。 一方で、契約可能な回線数の上限に関する制度設計については、利用者の多様なニーズや用途を踏まえた柔軟な対応が必要であり、過度な一律制限は適切でないと考えます。現在、各事業者においては、業界自主ルールに加え、与信判断に基づく独自の制限措置を既に講じており、こうした対応により一定の管理は行われている状況にあります。 したがって、新たな法令や規則による一律の規制強化を行うのではなく、各事業者の与信管理や自主ルールの徹底を通じて、業界全体としての対策水準の引き上げを図ることが望ましいと考えます。 【ソフトバンク株式会社】	今回お寄せいただいた御意見も参考にしつつ、本人確認方法の在り方等について、検討を進めて参ります。	無
６ データ SIM の本人確認		
・23 ページ目 訪日外国人に対して本人確認は義務化すべきと考える。 SIM 利用でパスポートの提示を渋るということは、提示できない何らかの理由を抱えている可能性が高いため。	音声 SIM については本人確認が義務化されておりますので、データ SIM の本人確認について、今回お寄せいただいた御意見も参考にしつつ、検討を進めて参ります。	無

資料にも記載があるが不正を未然に防ぐ点で有効だと考える。 【個人】		
データ SIM の本人確認義務化を検討するに当たっては、契約の相手方についても検討されるべきと考えます。 不適正利用対策に関するワーキンググループ（第 7 回）資料 7-2 P.6 において「（略）一自然人に対し大量にデータ通信 SIM を発行する事業者が、悪意者によって狙われている」旨が指摘されており、悪用されるデータ SIM の多くは自然人に向けたプランと推定されます。自然人との契約においては本人確認を義務付けることにより、一定の犯罪抑止が期待できると考えます。 その一方で、現時点では法人等との契約における悪用実態の把握は十分になされていないと認識しております。本人確認の義務付けを行うことにより、ユーザーおよび事業者に過度な負担を強いることや過剰規制に陥ることを避けるべく、まずは、悪用実態の把握を十分に行うべきと考えます。 悪用実態の把握の結果、法人との契約に本人確認を義務付けることとする場合、以下の３点について懸念があります。 ①　　事業者においてはシステム整備が必要になりますが、データ SIM は用途が多様であり BtoB や BtoG 領域での活用拡大が見込まれることから、一口に法人等といっても、多様な契約の相手方や提供形態毎の対応が求められ、その整備に当たっては相当の期間・費用が必要となります。 ②　　本人確認の実務においても、その煩雑化や本人確認書類の真正性判断の負担増、不備等の対応の負担増が考えられ、サービス提供遅延につながる恐れがあります。 ③　　その結果、ユーザー側の利便性が損なわれる可能性が高まります。 特に上記①に関連して、これまで、データ SIM の本人確認義務化に際しては、SMS 機能有無や対象機器等の機能面に着目した議論がなされてきていますが、データ SIM の多様な利用用途に応じ、例えば携帯電話不正利用防止法施行規則第 6 条に規定する相手方（人格のない社団又は財団 等）のように、多様な契約の相手方も想定されることから、契約の相手方につい	今回お寄せいただいた御意見も参考にしつつ、本人確認方法の在り方等について、検討を進めて参ります。	無

ても着目した議論をしていただくなど、今後詳細な検討が必要であると考えます。 【JCOM 株式会社】		
・データ SIM のうち、SMS を受信できる SIM は不正アクセスに利用されているものと認識しており、本人確認の義務化を検討することにに賛成いたします。 ・データ SIM については、固定 IP 電話の転送役務を用いた詐欺電話やメール・SMS 送信等によるフィッシング詐欺への悪用は考え得るところであり、規律の強化は一定の効果が見込まれるところですが、SIM 利用の利便性と犯罪等の悪用可能性とのバランスを考慮した検討が必要と考えます。 ・例えば IoT 機器利用や見守りサービス等、通信接続先や利用機器が制限されるサービスは、特殊詐欺等の悪用リスクが低いと考えられることから、本人確認の義務化の対象外とすることを要望いたします。 ・また本人確認の義務化を行う場合は、MVNO 等の関係事業者意見も踏まえた検討及びシステム対応等を想定した十分な移行期間の設定を要望いたします。 【株式会社 NTT ドコモ】	本見直しに係る携帯電話不正利用防止法施行規則の施行に当たっては、いただいた御意見を参考にしつつ、事業者や利用者への過度な負担とならないよう、検討を進めるとともに、適切な準備期間が確保されるよう努めて参ります。	無
「SMS 無データ SIM（いわゆるデータ通信専用 SIM）」は、IoT 機器や訪日外国人向けのプリペイド SIM 等にも利用されておりますため、本人確認を義務付けることとなると、利便性を大きく損なったり、利用者の排除（例えば訪日外国人の日本国内でのスマートフォン利用を排除してしまうこと等）に繋がることが強く懸念されます。 また、MNO と比べて MVNO は事業規模が小さく、事業者側の対応コスト増によりサービス提供価格の維持が困難となったり、サービス提供終了や MVNO 事業からの撤退の判断をせざるを得なくなるということが発生することが想定されます。 データ通信専用 SIM は公衆無線 LAN サービス等のインターネット接続サービスと同様（インターネットに接続するだけ）であるところ、義務化の検討にあたりましては、過剰規制に陥ることがないよう、「悪用の実態」と「利用実態や実効性」に加えて、「対応コストや準備期間等を踏まえた事	本見直しに係る携帯電話不正利用防止法施行規則の施行に当たっては、いただいた御意見を参考にしつつ、事業者や利用者への過度な負担とならないよう、検討を進めるとともに、適切な準備期間が確保されるよう努めて参ります。	無

業者側への影響」についても十分にご配慮いただき、利用形態ごとに極めて慎重かつ丁寧にご議論いただくことを強く要望いたします。 制度見直しの際は、約2,000あるMVNOの多くが準備等による対応が必要となることが想定されますため、施行時期については十分な準備期間を確保いただくことを強く要望いたします。 【一般社団法人テレコムサービス協会】		
データSIMの本人確認について、「悪用の実態が確認されたことを踏まえ、（略）義務化について検討すべきである。義務化を検討するにあたっては、（略）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」（P23）とされているところ、データSIMはIoT機器での活用等を通じビジネスを支えていたりすることから、当該検討を行うにあたっては、こうした実態に留意の上、健全な経済活動等を阻害する方向性を含む議論となることのないようお願い致します。 【楽天モバイル株式会社】	今回お寄せいただいた御意見も参考にしつつ、本人確認方法の在り方等について、検討を進めて参ります。	無
弊社では、業界の自主ルールに則り、音声SIMと同等の本人確認をデータSIMについても実施しており、今後もこの取組みを継続していく方針です。不正利用防止の観点からも、一定の本人確認は重要であると認識しております。 しかしながら、データSIMに係る本人確認手続のルール化、特に義務化を前提とした制度設計については、義務化ありきで進めるのではなく、慎重な検討が必要と考えます。 例えば、訪日外国人向けに短期利用を前提としたプリペイド型データSIMや、通信先・接続デバイスが限定される用途特化型のデータSIM等については、そもそも不正利用のリスクが低く、本人確認義務を一律に適用することは、かえって過度な手続負担を生じさせることになります。そのため、こうした不正リスクの低いと考えられるものについては、本人確認	今回お寄せいただいた御意見も参考にしつつ、本人確認方法の在り方等について、検討を進めて参ります。	無

義務の対象外とする等、利用者利便を損なわないようにすることが重要と考えます。 【ソフトバンク株式会社】		
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、という考え方に賛同いたします。 SMS は日常のコミュニケーションの中で利用されており、その日常に溶け込ませる形で、スミッシング等、直接的な詐欺のツールとして使われていると考えられることから、義務化の検討は必要と考えます。 一方で、構成員の発言にもある通り、SMS 無データ SIM については、本人確認義務の対象外としていただいたうえで、別途悪用実態の状況等を踏まえて慎重に検討いただくことを要望いたします。 ＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊ ＜構成員発言＞ ・ 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。 ＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊ 観光目的等で入国する訪日外国人については、滞在期間が短く、住居等が確認出来る本人確認書類の準備が困難であることから、早急に通信手段を確保したいニーズに対応するためにも、本人確認義務の対象外としていただくことを要望いたします。	本文の記載への賛同の御意見として承ります。 今回お寄せいただいた御意見も参考にしつつ、本人確認方法の在り方等について、検討を進めて参ります。	無

IoT 等で使われるような「通信先やデバイスが限定されているサービス」は、特殊詐欺に悪用されるリスクが低いと想定されるため、本人確認義務の対象外としていただくことを要望いたします。 仮にそういったサービスを利用する際に本人確認が必要になると、人間と人間の対話・コミュニケーションではないサービスや、その通信先がごく一部に限定されており、不特定多数と通信出来ないサービスに対しても本人確認義務がかかることになり、円滑な提供が出来なくなる懸念や、販売現場での混乱を招く可能性があると考えます。 【KDDI 株式会社】		
第３部　その他の特殊詐欺の電話・メール等の対策 第２章　その他の特殊詐欺の電話・メール等に関する課題		
フィッシング目的の迷惑メールまでは執行猶予も含めた刑罰で良いと思うが、不正アクセス以上は全て禁固刑とし、終身刑も含めた刑罰を検討すべきだと思う。 【個人】	いただいた御意見は今後の参考とさせていただきます。	無
１ 固定・携帯電話、SMS・メール対策		
・24 ページ目「国際電話の利用を望まない利用」 現在利用者側が制限を申し込まなければ国際電話につながる仕組みになっているのであれば、国際電話に繋ががらないことを初期設定とし、国際電話を利用したければ申請する方法に変更するのがいいのではないか。 国際電話を休止したいという要望が増加しているということは、国際電話は無用の長物と感じている利用者が多いということではないか。 【個人】	今回お寄せいただいた御意見も参考にしつつ、検討を進めて参ります。	無
携帯電話利用者における詐欺被害の防止に関し、「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」(P26) とされているところ、当社では、「迷惑電話、SMS 対策アプリの利用」及び「携帯電話やアプリの操作方法」に関するサポートを店頭で受けられるサービス等を 6 ヶ月間実質無償でご利用頂けるプロ	今回お寄せいただいた御意見も参考にしつつ、検討を進めて参ります。	無

グラムを 65 歳以上のお客様を対象に提供しており、特にこの年齢層のお客様向けに、高機能の「迷惑電話、SMS 対策サービス」をご利用頂きやすい環境の整備に努めております。 加えて、「特定の電話番号からの着信や番号非通知電話の着信の拒否」機能を具備する他社の無償アプリの周知や、OS 標準アプリにおける「特定の電話番号からの着信や SMS 受信の拒否」機能及び「番号非通知電話の着信拒否や消音着信」機能の店頭での情報提供等を行っております。 各種の詐欺防止策を広く浸透させる観点から、引き続きこうした活動に積極的に取り組んでまいる所存です。 【楽天モバイル株式会社】		
２ スプーフィング		
スプーフィングについて、他人の電話番号をその他人の同意なく表示させる行為及び使用されていない電話番号を表示させる行為を刑事罰の対象とすべき。 【個人】	今回お寄せいただいた御意見も参考にしつつ、検討を進めて参ります。	無
スプーフィングについては各携帯会社が個々人の契約時や更新時に危険性を伝えるべきです。 そういった情報を知らないでネット検索するケースが多いですし、その情報が信用できるかは保証できません。携帯会社関係の会社からの電話番号の可能性がある場合には携帯ショップに行って問い合わせれば実際にかけたか分かる事も周知すべきです。 海外または不透明な番号についても各携帯会社から、この番号には注意すべきと通達すべきです。 【個人】	今回お寄せいただいた御意見も参考にしつつ、検討を進めて参ります。	無

通信ログ保存の在り方に関するワーキンググループ

提出された御意見	御意見に対する考え方（案）	御意見を踏まえた案の修正の有無
本改正案は、通信ログの望ましい保存期間について、少なくとも３～６か月程度としている。また、通信ログの保存期間を限定すべき理由として、通信の秘密やプライバシーの保護を掲げている。 本改正案については、従前よりは保存期間を延長するものであり、そのこと自体は妥当であるものの、以下の理由から、未だ保存期間としては必要十分とは言い難く、さらなる保存期間の延長をするべきである。 そもそもインターネット通信は、現代社会における日常生活や、表現活動、経済活動等に欠かすことのできない社会インフラであり、通信ログはその社会インフラを構成する一要素である。そして、不特定多数の者が閲覧可能なインターネットにおいて公然と行われる誹謗中傷について通信ログが適切に保存されていなければ、誹謗中傷等の被害者にとっては、被害救済の道が物理的に閉ざされることとなる。 そのため、通信ログの保存については、社会インフラとしての保存を基本理念とした上で、通信の秘密やプライバシーの保護については、権利侵害の明白性や正当な理由など発信者情報開示請求における要件の判断において考慮されるべきものであり、これらを通信ログの存在自体の早期削除を正当化する理由として用いることは相当ではない。 以上を前提に、通信ログの望ましい保存期間について検討する。 アーティストやタレント等の著名人を対象としたインターネットを通じた誹謗中傷被害においては、いわゆる炎上事案も相まって、誹謗中傷の投	お寄せいただいた御意見も参考にしつつ、検討を進めて参ります。 なお、本ガイドラインで対象にする通信ログは、誹謗中傷等を含む違法・有害情報に関する通信ログに限るものではないため、保存される通信ログの全てについて、御指摘の「発信者情報開示請求における要件の判断」が行われるものではありません。また、御指摘の警察庁における実態調査（通信ログ保存の在り方に関するワーキンググループ「資料 6-1」）については、未検挙である事件に限定して集計し、そのうちの「通信履歴（ログ）の不存在による障害」があったと回答された 74 件を全数として「事件発生から照会等までの期間」の割合を示すものです。（同「資料 6-1」p. 2、同「資料 6-4」p. 2 及び p. 5）	無

稿が膨大な数に及ぶことが多い。そのため、誹謗中傷の震源を特定したり、被害の実情を解明するためには相当の時間を要することがある。また、著作権やパブリシティ権などの知的財産権の侵害事案については、投稿が社会的注目を集めない場合が多々あることから、インターネット上で公然と行われた投稿であっても、被害の発見自体に相当の時間を要する場合がある。このように、権利侵害の投稿がされてから発見に至るまでの期間や弁護士や警察等に相談するまでの期間については、相当程度のタイムラグが生じざるを得ないのが実情である。そのため、実際に被害者が発信者情報開示を申し立てた際には、保存期間経過により加害者の特定に至らない事案が未だに見受けられる。 　このことについては、警察庁の実態調査（WG 第 6 回資料 6-1）においても、事件発生から照会等までの期間について、６か月以上とされるものが全体の４割近く（37.9%）を占めており、このうち６か月以上１年未満のものは３割近く（28.4%）にも及んでいることからも窺われる。すなわち、これらのデータは、誹謗中傷等の被害を受けた被害者が実際に警察に相談するまでにタイムラグがあることを示唆するものである。これらを前提に、警察庁では、１年６か月保存されていれば、ログの不存在を原因とした捜査上の障害を概ね解消できるとされている。 　また、他の法制との均衡という観点からは、民法上の不法行為の消滅時効が３年間とされていることと比較しても、現在の通信ログの保存期間の制限は、あまりに均衡を失しており、被害者に過度の負担を強いるものである。 　以上によれば、通信ログの保存期間については、誹謗中傷等の被害救済の機会を確保するために必要十分な期間とするべきである。具体的には、		

警察庁の実態調査を踏まえれば、通信ログの望ましい保存期間は、通信ログの不存在を理由とした被害回復の断念という事態を根絶させるという観点から、少なくとも１年６か月程度とするべきである。 【一般社団法人日本音楽事業者協会】		
本ガイドライン改正案において、通信履歴の保存期間について、必要最小限度の範囲内で設定するとしていたものを、SNS や掲示板等での誹謗中傷等の対策のための社会的な期待に応えるため、大きく転換し、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ヶ月程度保存することが望ましいとされた点については、賛成する。ただし、誹謗中傷等の違法・有害情報に対処していくためには、CP 及び AP によって、本ガイドラインが遵守されていくことが必要であるため、「今後の検討課題」に記載されているとおり、本ガイドライン改正案が施行された後に、CP 及び AP が本ガイドラインを遵守しているかについて調査し、その結果、遵守が不十分であった場合には、しかるべき対応を検討されたい。 特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律の一部を改正する法律（令和三年法律第二十七号）により導入された新たな裁判手続により、CP 及び AP に対する消去禁止命令が導入されたこととあいまって、多くの CP における誹謗中傷事案では、３～６ヶ月の通信履歴があれば、被害者救済が図られることが見込まれることから、本ガイドラインの改正案に賛成する。他方で、AP の情報提供等に長期間をかけたり、提供命令に応じなかったり、特定の類型では速やかに通信履歴を削除したりする CP も存在しており、３～６ヶ月の通信履歴が保存されるようになったとしても、被害救済がなされない事案は残る。かかる事案に	お寄せいただいた御意見も参考にしつつ、検討を進めて参ります。	無

おける被害者救済のためにも、そうしたCPに対して適切な対応を促す、もしくは、そうしたCPの存在を前提としても、発信者情報開示請求をした際に、通信履歴が消去されているという事態が生じないような期間の保存を推奨するなどの対応も検討されたい。 【一般社団法人クリエイターエコノミー協会】		
本ガイドラインの改正案において、SNS や掲示板等での誹謗中傷等が社会問題となっていることを受け、通信履歴の保存期間を必要最小限度の範囲内で設定する従前の通信履歴の保存の在り方から大きく転換され、社会的な期待に応える望ましい保存期間として少なくとも３～６か月程度とすることが示された点については、賛成する。しかしながら、誹謗中傷が行われる主要な大規模プラットフォームの多くは国外CPであり、そのなかには裁判所の提供命令に従わない方針をとっているところもあるようで、ガイドラインのような拘束力のない枠組みでは通信ログ保存の実効性に限界がある。また、通信事業者ごとにログの保存期間が不統一なため、同じ被害であっても通信事業者がどの CP であるかによって救済の可否が左右されるような不公平な状況も存在しているので、一定の事業者（アクティブユーザー数・収益規模などの基準で範囲を定める）へのログ保存の義務付けを含めて検討されたい。 誹謗中傷対策の実務において、CP 又は AP におけるログ保存期間の経過により、発信者の特定が不可能になるケースが多いことが挙げられる。手続きに要する時間については、被害者が投稿に気付いて弁護士に相談するまでに数週間～1 か月程度を要し、さらに弁護士に相談後、弁護士との面談・契約・書類準備等にさらに 1 か月前後を要することが一般的であり、また CP のログの調査に２か月以上かかるケースがあることや、CP が権利	お寄せいただいた御意見も参考にしつつ、検討を進めて参ります。	無

侵害性を争う場合、裁判期日は１か月単位で設定・進行されることも考慮すると、CP からの発信者情報の開示までに投稿から６か月以上かかる事例も少なくなく、３～６か月程度のログの保存期間では救済されない事案が残ると思われる。よって、通信ログの保存期間については少なくとも 6 か月以上（可能であれば 12 か月）の保存が検討されることを期待する。早期の開示を期待して導入された提供命令と消去禁止命令については、強制力が弱いため、国内 CP であれば一般的に提供命令の遵守が期待できるものの、提供命令に従わない方針をとっている国外 CP もあるようで、その場合、提供命令と消去禁止命令がほとんど機能していないという現実がある。また、国外 CP の一部には、アカウントや投稿の削除後、1 か月程度で通信ログが消去される運用を行っているケースも確認されており、その場合、悪意ある発信者の「逃げ得」になってしまうため、通信ログの保存期間については、アカウントや投稿の削除後も例外なく保存対象となる制度設計をされたい。 【UUUM 株式会社】		
「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」(P33)とされているところ、当該ヒアリングを行うにあたっては、事業者に過度な負担を課すものとはならないよう留意頂きたく存じます。 また、「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、（略）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」（P33）とされているところ、当該検討にあたっては、通信の秘密やプライバシーの保護と、誹謗中傷違法・有害情報への対策とのバランスに留意頂	お寄せいただいた御意見も参考にしつつ、検討を進めて参ります。	無

きたく存じます。 【楽天モバイル株式会社】		
通信ログの保存期間の延長に関しては、その保存に要する社内インフラの整備や、データ管理体制の増強、人的リソース確保等に、多大な費用や期間を要します。今後、本報告書案に示された期間を上回るような保存を求められることのないよう要望します。 本改正案の適用開始時期については、通信履歴の保存に係る設備や人的体制の増強等を実施するための十分な準備期間を確保する必要があると考えます。 したがって、具体的な対応可能時期に関しては各事業者へのヒアリング等を行ったうえで調整を実施いただくことを要望します。 【ソフトバンク株式会社】	お寄せいただいた御意見も参考にしつつ、検討を進めて参ります。 なお、ログ保存の在り方については、今後も、社会環境の変化を踏まえた検討が必要であると考えており、仮に本改正によって課題の解決につながらないことが明らかになった場合は、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改正以外の方法で検討することが必要になると考えております。	無
１.「通信ログ保存の在り方に関するワーキンググループ」２（２）（同３２頁）において、「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」との記載があります（以下「本記載」といいます）。 この点について、 （１）「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」との点について、どのように調査・把握をしたのでしょうか（本記載は、第 6 回ワーキンググループにおける発信者情報開示の観点からのヒアリングに基づいた記載という理解でよろしいでしょうか）。 （２）本記載における課題を解消するために、現行の非訟手続が創設され	1⑴について 御指摘の箇所については、ワーキンググループにおける事業者や弁護士等のヒアリングを踏まえ、有識者との意見交換に基づき記載したものです。 1⑵について 現行の法制度下において課題があることを踏まえ、本ガイドラインの解説の改正を行うものです。 2 について 仮処分手続における「保全の必要性」については、裁判所において、個別具体的な事案ごとに適切に	無

たものと理解しておりますが(「発信者情報開示の在り方に関する研究会最終とりまとめ」(令和2年12月)参照)、本記載は、現行の非訟手続の効果や課題の検証を踏まえたものなのでしょうか(現行の非訟手続では、保存期間の経過の問題の解消としては不十分であることが前提とされているのでしょうか)。 ２.「通信ログ保存の在り方に関するワーキンググループ」２(３)(同３２頁)及び同別添(同３４頁以下)の記載は、通信ログの保存期間の長期化を推奨ないし許容するものと理解しております(「望ましい」という表現への改正や、同別添(同３５頁)の「(※３)」の記載等)。 この点について、通信ログの保存期間の長期化は確かに発信者情報開示の実現の増加につながると思われる一方で、保存期間の長期化に伴い現行の仮開示の仮処分手続における「保全の必要性」の要件が認められにくくなる可能性があると思われます。この点について、どのように整理しているのでしょうか。 【個人(弁護士)】	判断されるものと承知しておりますが、本ガイドラインの解説の改正は、保存することが望ましい期間を明示するものであって、事業者にログの保存を法的に義務付けるものではないことから、一般論として、本改正が「保全の必要性」の判断に影響を与え得るものとは考えておりません。	

利用者情報に関するワーキンググループ

提出された御意見	御意見に対する考え方（案）	御意見を踏まえた案の修正の有無
全般		
## 【意見の要旨】 本報告書案は、不適正利用対策の強化、通信ログ保存の在り方の検討、利用者情報保護の強化を目的としており、その方向性については賛同いたします。しかしながら、利用者情報保護の観点から、現在スマートフォンアプリに限定されている対象範囲を拡大し、ウェブサービスにおけるスクレイピング対策を含めることを提案いたします。 ## 【具体的な意見】 ### 1. 現行案の課題について 本報告書案における利用者情報保護の取組は、主にスマートフォンアプリを対象としており、ウェブサービス上の利用者情報保護については「今後の検討課題」として先送りされています。しかし、現在多くの利用者が日常的に使用するX（旧Twitter）、Googleドライブ等の主要ウェブサービスにおいて、利用者データがサーバーに保存され、利用規約においてスクレイピングを含むデータ利用への同意が求められている実態があります。 これらのサービスでは、データ利用に同意しない場合、サービス利用が実質的に不可能になる構造となっており、利用者の真の自由な選択が確保されているとは言い難い状況です。 ### 2. スクレイピングによる被害の深刻性	いただいた御意見については、報告書(案)第３章における今後の課題の検討を進めていく上での参考とさせていただきます。	無

ウェブサービスからスクレイピングされた利用者情報は、以下のような用途で悪用されるリスクがあります： - フェイク画像・動画の素材としての利用 - ポルノ画像の素材としての悪用 - 広告配信のためのリスト作成 - なりすまし・詐欺行為の素材としての悪用 - 国際的には著作権侵害とみなされる可能性のある生成 AI 企業によるスクレイピング行為 特に生成AI企業によるスクレイピングについては、欧米諸国において著作権侵害や個人情報保護法違反として法的問題となっているケースが増加しており、日本においても同様のリスクが懸念されます。これらの問題は、スマートフォンアプリにおける利用者情報の不適切な取扱いと本質的に同じ性質を持っており、同等の保護措置が必要と考えます。 ### 3. 提案する対策 以下の対策を報告書に盛り込むことを提案いたします： #### （1）対象範囲の拡大 利用者情報保護の取組について、スマートフォンアプリとウェブサービスを区別することなく、統一的な保護基準を設定すること。 #### （2）スクレイピングに関する規制の明文化 - スクレイピングに関する明確で理解しやすい同意取得プロセスの義務化 - データ利用目的の具体的かつ詳細な明示（生成AI学習用途を含む） - 実質的なオプトアウト（拒否）選択肢の確保 - 同意撤回後のデータ削除義務の明文化		

- 著作権を有するコンテンツについては、著作権法との整合性を確保した取扱いルールの策定 #### （3）事業者への要求事項の強化 - 利用規約における透明性の確保 - データ利用実態の定期的な報告義務 - 第三者提供先・利用目的の変更時における再同意取得の義務化 - 生成 AI 企業等への大規模データ提供については、利用者への事前通知と個別同意の取得 ### 4. 法的根拠と整合性 この提案は、個人情報保護法の趣旨、電気通信事業法の外部送信規律との連続性、著作権法との整合性、および国際的なプライバシー保護基準（GDPR 等）との調和を図るものです。技術的にも、既存の同意管理技術や API アクセス制限技術の活用により実現可能です。 特に生成 AI 分野においては、国際的な規制動向を踏まえ、日本が後れを取ることのないよう、先進的かつ実効性のある対策を講じることが重要です。 ### 5. 期待される効果 上記対策の実施により、以下の効果が期待されます： - プライバシー侵害リスクの軽減 - 利用者の自己決定権の実質的な確保 - デジタル社会における基本的人権の保護強化 - 透明性の高いサービス運営の促進 - 知的財産権保護と技術革新のバランスを図った健全な AI 産業の発展 - 国際競争力のある日本のデジタル政策の確立		

## 【結論】 利用者情報保護を実効性のあるものとするためには、技術的手段や提供形態にかかわらず、利用者情報を取り扱うすべてのサービスを対象とした包括的なアプローチが不可欠です。特に近年急速に発展している生成 AI 分野においては、国際的な法的リスクや倫理的課題への対応が急務となっています。本報告書案において、ウェブサービスにおけるスクレイピング対策を含む利用者情報保護の強化について、具体的な検討と対策の明記を強く要望いたします。 【個人】		
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**		
・アプリ提供は、契約締結含め web 画面等専ら非対面で行われるため、正確な保護者確認の担保が困難と想定されます。 ・そのため、「保護者関与の仕組みや機能を備えること」について、有効かつ幅広いアプリ提供者が取り扱うことが可能な方法の事例を、SPSI や総務省ホームページ等でご紹介いただくことを強く要望いたします。 【株式会社 NTT ドコモ】	当該記載は、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となる場合に、保護者が関与できる仕組みや機能を備えることを求めるものであり、御指摘の「正確な保護者確認の担保」のための仕組みや機能を必ずしも厳格に求めるものではありません。保護者が関与できる仕組みや機能の具体例としては、課金の際に、保護者が事前に設定したパスワードの入力を求めるといったことが考えられます。	無
グローバルサービスでも一般的な自己申告で年齢確認を行っているので、日本もそれに倣い、利用者側の責任で自己申告にすることが望ましいと考えます。 【日本スマートフォンセキュリティ協会（JSSEC）】	スマートフォン上での年齢確認については、年齢制限の設定が適切に機能することが前提となります。 このため、関係事業者等において年齢等の発達段階が適切に把握されることが重要であり、今後の技術的手段の発達や市場の状況を踏まえ、総務省において検討を行うことが適当と考えます。	無
１．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に関する意見 ①青少年保護	本案に対する賛同の御意見として承ります。 また、関係省庁と連携した青少年保護の取組を引き続き進めて参ります。	無

スマートフォンの利用者が低年齢化し、さまざまな問題が表出するなか青少年保護は喫緊の課題であり、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（以下 SPSI）へ含めることに賛同いたします。また、青少年保護の課題は多岐に渡るものであるところ、すべてを SPSI で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が検討されたことについても、本来の SPSI の趣旨に沿うものとして評価いたします。つきましては、今後も他省庁などとの連携がより緊密に行われて青少年保護対策がさらに進むこと、ならびに二重の規制的なものとならないように配慮されることを期待いたします。 【一般社団法人モバイル・コンテンツ・フォーラム】		
インターネット上のサービスや情報は、年齢にかかわらず誰もがアクセスできることから、青少年保護に関する検討は当然に必要であり、今回、SPSIに青少年保護の観点を盛り込むことにつき、強く賛成する。 なお、青少年に対する検討は高齢者に対する配慮としても参考になると考えている。 【一般社団法人 安心ネットづくり促進協議会】	本案に対する賛同の御意見として承ります。	無
SPSI の起源から考え、青少年の利用者情報やプライバシーの保護の観点からの項目の追加になることはやむを得ないとはいえ、現在、青少年の送信に関わるリスクについての法制度・対策が極めて手薄となっていることに鑑み、かかる観点からの検討も是非行っていただきたい。 【一般社団法人 安心ネットづくり促進協議会】	青少年の発信に係るリスクへの対策等については、関係省庁と連携して引き続き検討して参ります。	無
スマートフォン利用の低年齢化に伴い、利用者を「青少年」と一律に括ることなく、発達段階を踏まえた機能（機能制限や保護機能を含む）を提供することが必要である。その観点から、利用者年齢の確認について検討を行うことについて強く賛成する。 【一般社団法人 安心ネットづくり促進協議会】	本案に対する賛同の御意見として承ります。	無

青少年保護に関しては、SPSI 以外にも、例えば、個人情報保護委員会における「個人情報保護法　いわゆる３年ごと見直し」にて、「こどもの個人情報等に関する規律の在り方」等の検討が進められています。 今後、SPSI に青少年保護に係る内容を追記する場合には、こうした検討状況との整合性を図っていただくことを要望します。 【KDDI 株式会社】	青少年保護に係る取組については、引き続き、個人情報保護委員会のほか関係省庁と連携し、整合性を図りながら取り組んで参ります。	無
（P.41） 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 ・生成 AI に関して、先述の個人情報ももちろん、例えばいわゆる「ジブリ風」に変換する個人が写る画像（写真）がどのように使われるか、という（保護者等も含めた）教育の不足により、生成 AI モデルに「質問」をすることによりその写真へアクセス出来てしまう可能性を生んでしまっています。 ・一方で利用ルールの遵守がされていない例として、利用規約に「13 歳未満の利用」が禁止されているにもかかわらず、夏休みなどに「生成 AI 利用講座」の対象に小学生を含んでいる場合が見受けられます。（SNS の多くも 13 歳未満が利用禁止となっているはずですが、保護者がそれを認識・関連付けて考えられているかにもよります） （最後に） ・生成 AI に関する不正は、例を挙げただけでもごく一部だと考えています。 ・生成 AI（と一般に呼ばれるものは）汎用性が高く、またそのデータが正当な手段で、権利の保護・法令の遵守がされた上で収集されたかも疑問が残るものが多く、その利用や、そもそもの学習についての制限はなされるべきだと考えます。 ・汎用性が高いということは、生成 AI も含め規制がなければ犯罪にも使われるということを前提に、サービスのルールに関する監視・指導は徹底すべきだと考えています。	いただいた御意見については、参考として承ります。	無

【個人】		
２　位置づけ		
②位置づけ 各事項の位置づけについて、これまですべて「～～することが望ましい」と記載さ れ、各事項の重要性の度合いが不明であったところ、4 つの分類とすること、およびそれぞれの位置づけの考え方が示されたことを評価すると同時に、それぞれの分類の趣旨について賛同いたします。つきましては、今後関連する他省庁等の法改正や新法の施行が予定されているところ、より一層の青少年保護がはかられるよう適宜の見直しが進められることを強く求めます。 【一般社団法人モバイル・コンテンツ・フォーラム】	SPSI 本文の記載への賛同の御意見として承ります。	無
第３章　今後の検討課題 **１　ウェブサイトに係る調査・検討**		
報告書でのご指摘の通りスマホアプリとブラウザにおいて利用可能な機能に差異はほぼなくなりつつあります。スマホアプリは、常時起動が可能であることや通信サービス機能が可能なこと、デバイス内の情報へのアクセスなど、スマートフォン機器とより密接な動作が行える点においては依然として多少の差異はあるものと考えます。 SPSI がこれまで情報取得機能が充実したスマホアプリを中心に据え事業者の対応を整理してきたところから、あらためて一般的なウェブサイトを SPSI の対象にすることについては、ウェブサイト運営事業者のすべてが対象になることになり、報告書にある通り、様々な課題が出てくるものと思料します。例えば、スマホアプリ内に表示されるウェブサイトに限定する等の配慮が有効ではないかと考えます。 【日本スマートフォンセキュリティ協会（JSSEC）】	いただいた御意見については、報告書(案)第３章における今後の課題の検討を進めていく上での参考とさせていただきます。	無
②第 3 章 今後の検討課題に関する意見 1.ウェブサイトに関わる調査・検討 Web ブラウザーは、アプリ内、ブラウザー単体(PC、ダブレット、スマートフォン)、デバイス組込み型(ゲーム機他、IT デバイス、自動車)に加え	いただいた御意見については、報告書(案)第３章における今後の課題の検討を進めていく上での参考とさせていただきます。	無

て、今後あらゆる機器に組み込まれてくる可能性がありますので、今後別途の対応が必要で、速やかにご検討いただけること大変感謝いたします。 特に、PC・タブレット・スマートフォンでのブラウザー単体と、アプリに組み込まれたブラウザーを同一扱いして、ルールを決めていくことは、セキュリティ上のリスクが非常に高く、コンテンツへの一定の規制かけることが出来るアプリストア(3rd Party アプリストア含む)へは積極的に取り組んでいくべきと考えます。 【スカイワゴン株式会社】		
２．第 3 章　今後の検討課題に関する意見 ①ウェブサイトに係る調査・検討 ウェブサイトに関して調査、検討が行われたことを評価いたします。ウェブサイトはスマートフォンに限らず、さまざまなデバイスで利用されるものであること等から、 SPSI の範囲を単純に拡大するのではなく、今後の課題として別途の対応が必要と考えられ、今後速やかに検討を行うことが適当であるとされたことに賛同いたします。 【一般社団法人モバイル・コンテンツ・フォーラム】	報告書本文の記載への賛同の御意見として承ります。	無
２　今後の検討の方向性		
利用者の視点からすれば、スマートフォンを安心して利用できることが重要であるから、ウェブサイトについても当然に含めるべきと考える 【一般社団法人 安心ネットづくり促進協議会】	いただいた御意見については、報告書(案)第３章における今後の課題の検討を進めていく上での参考とさせていただきます。	無
ウェブサイトにおける利用者情報の取扱いについて議論する際は、多様なウェブサイト運営者に対する十分な説明を行うとともに、OS やブラウザに実装されている機能や利用実態、デフォルト設定や利用者が利用可能な選択肢等について調査し、それらを踏まえた上で具体的に検討すべきであると考えます。 【一般社団法人日本インタラクティブ広告協会】	いただいた御意見については、報告書(案)第３章における今後の課題の検討を進めていく上での参考とさせていただきます。	無
「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、すでにウェブサイトも含む個人情報等の取扱いが示されています。今後、SPSI にウェブサイトにおける利用者情報の取扱いを記載する場合には、当	いただいた御意見については、報告書(案)第３章における今後の課題の検討を進めていく上での参考とさせていただきます。	無

該ガイドラインとの関係性を明確にするとともに、内容の整合性を図っていただくことを要望します。 【KDDI 株式会社】		
３　その他の検討課題		
②その他の検討課題 　スマートフォン以外のデバイスについても調査と検討を行うことが適当とされたことを評価いたします。GIGA スクールなどでは、大規模な導入に伴う形での青少年保護が求められるなど、さまざまな状況の違いがあることにも鑑み、政府の取組みに資する形で安心・安全な ICT サービスの実現が進むよう、さらなる検討が進められることに期待します。 【一般社団法人モバイル・コンテンツ・フォーラム】	報告書本文の記載への賛同の御意見として承ります。	無
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（改定案）		
全般		
①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(改訂案)に関する意見 　特に非常に早い速度で、進化が進んでいる AI の利用は、今後誰もが意識せずにスマートフォンだけでなくあらゆる デバイス・環境で利用しているという状況が普通になってくると考えられます。別途成立している AI 法も特定のデバイスをターゲットとしたものではありませんので、より一般的な記述で適切であると考えております。 【スカイワゴン株式会社】	いただいた御意見については、報告書(案)第３章における今後の課題の検討を進めていく上での参考とさせていただきます。	無
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（改定案）について、昨今の状況を考えると、望ましい事項や基本的事項などではなく、法令で定めて安全性を高めるべきだと思います。 　大手 SNS(X や Instagram)はアップロードした画像や情報を生成 AI に学習させているが、特にこれは個人情報流出の危険性が高く犯罪に巻き込まれてしまう可能性も高いです。これらの対策には膨大なコストがかかることが予想されるため、法令がなければ危険性が高いままとなるでしょう。	いただいた御意見は、総務省における今後の政策検討の際の参考とさせていただきます。	無

守るべきは必要な措置を怠るアプリケーション提供者ではなく日本の青少年の未来です。 現状の事例をよくみて厳しく対応していくべきです。 【個人】		
15 ページのアプリケーション提供者等における取組から、いくつか必須の事項としてほしいものが望ましい事項となっていたため、基本的事項に引き上げてほしいです。 ・16 ページの 3.4 ・18 ページの［情報収集モジュール等に関する記載事項］ ・19 ページの 6 ・20 ページの 8 ・22 ページ 2 ・23 ページ ・24 ページ 6 ・30 ページ などは、必須の事項としてほしいです。 個人情報を取り扱うことにおいての主体は、個人情報の元となる本人であるという前提は絶対的なものとして崩してはならないと考えますし、新しい技術や体制を理由にそこが蔑ろにされるとまではいかずとも、後回しにされるようなことがあってはなりません。 個人の権限の主体性が失われる事態であるならば、最優先で保護すれことを考えるべきであると考えます。それは今後いかなる技術的発展の理由や、産業的利益が見込める状況であってもです。 個人が守られる形で、正しく情報が取り扱われるようになることを望みます。 【個人】	SPSI における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ているもので、「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ことから、原案のとおりとさせていただきます。なお、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として位置づけられています。	無
３．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（改定案）に関する意見 MCF では、これまで改定が進められてきたスマートフォン プライバシー イニシアティブに準じて各種ガイドラインを策定し、業界が守るべき規範として普及・啓発を進めてまいりました。今般の改定において、MCF におい	SPSI 本文の記載への賛同の御意見として承ります。	無

て規範としてきたものの大半が基本的事項として分類されたことは、この普及・啓発を進めるうえで極めて重要かつ力強い支援となるものであると評価いたします。 AI をはじめとするさらなる技術の発展、これまでになかったサービスやビジネスモデルの登場等、ICT を取り巻く環境は日々常に進化し続けており、関連する新たな立法や法改正も間断なく行われています。これらとの整合性を取るとともに、今後も関連事業者にとっての規範、ベストプラクティスとなるよう適宜の検討が行われることを期待いたします。 【一般社団法人モバイル・コンテンツ・フォーラム】		
「法令事項」に分類されている「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」（P.44-45）について、「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」（別添 P30）と明記されていることはこれを遵守する上で非常に有用であるところ、国内法令の改正等により「法令事項」が追加等された場合にも、参照すべき運用指針等を同様にスマートフォン プライバシー セキュリティ イニシアティブ（以下「SPSI」）に追記等頂きたく存じます。 また、「基本的事項」に分類されている「国内法令に準じた形での取扱いが強く求められる事項」（P44）についても、利用者情報を扱うスマートフォンアプリの関係事業者が参照すべき具体的な運用指針等や、これに違反した場合のリスク等についても、同じく SPSI に記載頂きたく存じます。 【楽天モバイル株式会社】	いただいた御意見については、今後の検討を進めていく上での参考とさせていただきます。	無
1.1.5. 基本原則		
端末固有 ID 含む識別子や利用者情報の性質について検討する際は、法令上の位置付けや規制、取得や利用に係る技術的条件、関連規約による制約、業界ごとの自主規制による規律、サービスの実装様態や利用実態、デフォルト設定や利用者が利用可能な選択肢等について具体的に検討すべきであると考えます。 一例として、広告 ID（IDFA、AAID）については、ブラウザからは取得できないことに加え、注釈 45 にある通り個人関連情報としての規律が課せら	いただいた御意見については、今後の検討を進めていく上での参考とさせていただきます。	無

れている。また、他の識別子や個人を特定し得る情報との突合は広告 ID を提供する OS 事業者の規約においてデフォルトで禁止されており、それらの処理を行う際は利用者の明示的な同意が必要となっている等の制約がある。 【一般社団法人日本インタラクティブ広告協会】		
1.2.1.2. プライバシーポリシー等の運用		
利用者情報のトラッキングについて検討する際は、トラッキングに用いられる識別子や利用者情報の性質や取扱いの実態について、法令上の位置付けや規制、取得や利用に係る技術的条件、関連規約による制約、業界ごとの自主規制による規律、サービスの実装様態や利用実態、デフォルト設定や利用者が利用可能な選択肢等について、具体的に検証すべきであると考えます。 【一般社団法人日本インタラクティブ広告協会】	いただいた御意見については、今後の検討を進めていく上での参考とさせていただきます。	無
1.5. 青少年の保護に係る取組		
アプリ提供者についても、自らが提供するアプリの対象年齢を想定し、その利用に適した設計をすべきであることから以下を追加するよう求める。 「・自ら提供するアプリが青少年の利用を想定している場合、『青少年保護バイデザイン』を実施し、その推奨年齢を想定すると共に、その利用に適した機能を提供する。」 【一般社団法人 安心ネットづくり促進協議会】	個別のアプリケーションについては、年齢制限設定（レーティング）を含めて審査を行うことが、アプリストア運営事業者における望ましい取組として記載されていることから、原案通りとさせていただきます。アプリ提供者においては、アプリ運営事業者が適切な審査を行うことができるよう、必要な情報を提供することが期待されます。	無
年齢制限設定（レーティング）はペアレンタルコントロールを行う際の重要な指針であるため、アプリストアは基準策定に関する指針を公表するなど、社会的な合意を得られるよう務める必要があると考える。 したがって、文案を「基準を設定し、社会情勢や利用者の実情に合わせた適切な年齢制限設定が行われるよう確認すること」とすべきである 【一般社団法人 安心ネットづくり促進協議会】	年齢制限設定（レーティング）に関する基準については、脚注 76 において、国際的なレーティング基準や、各国で広く一般に使用されている基準を採用することなどが考えられる旨を記載しており、御指摘の趣旨は含まれていると考えられることから、原案通りとさせていただきます。	無
保護者が適切なペアレンタルコントロールを行うためには、必要な情報を入手する必要がある。このため、OS 提供事業者においては機能の適切な利用方法や必要性など関連する情報についても提供していただきたい。	本記載は、青少年保護の観点から OS 提供事業者において実施することが望ましい事項を記載したものであるため、原案のとおりとします。	無

したがって、該当文案を「ペアレンタルコントロールを実施するための機能および関連する情報を提供すること」とすべき 【一般社団法人 安心ネットづくり促進協議会】	一方、保護者が適切にペアレンタルコントロールを行うためには、正確な情報・状況の理解が必要となることから、総務省において青少年の保護者に対する啓発活動を継続することが適当と考えます。	
その他		
個人情報の漏洩リスクが高いままに突き進んではいけない。 情報漏洩全般を甘く見ることは、国家の機密を内外に漏洩することに繋がる。企業も保たなくなる。中長期的に情報管理のリテラシーを高めること。 【個人】	SPSI は、スマートフォンアプリにおける、個人情報を含む利用者情報の適正な取扱い等に関し、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す。	無
データはアプリケーションでオフしても（オプトアウト）、バージョンアップするとオプトイン状態になるものや、クラウドにアップしたものをスクレイピングされて利用されたりするので法令で取り締まることのできるものを作らないと対策にならないかと思います。 悪用を罰するより AI 事業者に罰則ありでガイドライン適用させた方が EU の AI 法にも触れず発展するのではないでしょうか。 【個人】	いただいた御意見については、今後の検討を進めていく上での参考とさせていただきます。	無

共通

提出された御意見	御意見に対する考え方（案）	御意見を踏まえた案の修正の有無
弊社としては、安心安全な ICT サービスの開発・利用に向けて各種のサイバーセキュリティ事業に取り組むとともに、情報リテラシーの向上に取り組んでおります。こうした中、ICT サービスが社会経済活動に深く浸透している現状を踏まえ、ICT サービスの利用に関して、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、利用者視点で検討いただいていることについて、弊社としては大変時宜を得たものであり、賛同いたします。 【株式会社ラック】	本文の記載への賛同の御意見として承ります。	無
日本スマートフォンセキュリティ協会は、スマートフォン・IoT 機器が安心・安全に利活用できるよう利用面、技術面、リテラシー面から様々な取り組みを行っている団体です。 ICT サービスが社会経済活動に深く浸透している中、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、利用者視点で検討いただいていることについて、当協会としては大変時宜を得たものであり、賛同いたします。 【一般社団法人日本スマートフォンセキュリティ協会】	本文の記載への賛同の御意見として承ります。	無
その一：貴庁におかれましては、日々、国家のために尽力されておりますこと、心より敬意を表します。このたび公表されました報告書を拝見し、内容がたいへん充実していることに、深く感銘を受けた次第でございます。一人の市民として、こうした細やかな検討がなされていることは誠にありがたく存じます。 しかしながら、僭越ながら、いくつかの点につきましては正直なところ戸惑いを感じております。そこで、このパブリックコメントの機会をお借りして、拙筆ながらも所感を述べさせていただこうと考えた次第です。ところが、本報告書の重要な部分にかかわる「不適正利用対策に関するワーキンググループ」（令和７年５月９日、５月 16 日、６月６日開催）および	本報告書（案）についての意見募集を改めて行うことは予定しておりません。 いただいた御意見は今後の意見募集実施にあたっての参考とさせていただきます。	無

「利用者情報に関するワーキンググループ」（同年 5 月 19 日、5 月 27 日、6 月 5 日、6 月 24 日開催）について、8 月 4 日の意見募集締め切りの時点においてもなお議事概要が公表されておりませんでしたことは非常に残念に存じます。 　一方、「通信ログ保存の在り方に関するワーキンググループ」につきましては、6 月 27 日開催分までの議事概要が公開されており、私も拝読させていただき、大変参考になりました。専門的な議論の積み重ねが理解の助けとなり、報告書の内容把握に欠くべからざるものであると実感いたしました。 　意見を申し述べるにあたっては、報告書作成に携わられた有識者の方々の議論をしっかりと理解することが肝要であると考えております。ゆえに、十分に情報が揃わないまま軽率に意見を述べることは控えるべきと判断し、今回は意見の提出を見送らせていただいた次第でございます。恐らく、私と同様に、必要な情報の欠如により意見表明を控えられた方々も多いことと拝察いたします。 　貴庁のご担当者様におかれましては、日々多忙な業務に励まれていること、痛み入るばかりでございます。しかしながら、議事録の公開は国民との信頼関係の基礎であると考えます。つきましては、すべての議事概要が公開されてから改めて意見募集の機会を設けていただきたく、謹んでお願い申し上げます。 その二：議事概要を熟読した後、「通信ログ保存の在り方に関するワーキンググループ」につきまして愚見を記すべく意見提出様式を拝見いたしましたところ、「項目／部」の選択肢に「ログ（第２部）」「利用者（第３部）」と記載されておりました。 　しかしながら、報告書を改めて拝読いたしましたところ、「通信ログ保存の在り方に関するワーキンググループ」および「利用者情報に関するワーキンググループ」には、明確に「第〇部」といった部別の構成は見当たらず、どの記載が何を指しているのか判断がつかず、戸惑いを覚えた次第でございます。貴庁にてご用意くださった意見提出様式を、一市民の立場である私が勝手に書き換えるわけにもまいりませんが、どのように記入すべ		

きであったか、今なおわからずにおります。差し支えなければ、今後このような際における記載方法について、ご教示賜れますと幸甚に存じます。 その三：このたび意見提出を試みるにあたり、e-Gov における意見募集ページのプライバシーポリシーを拝読いたしましたところ、利用者情報が「当サイトが提供するサービスの利便性を向上させるため、利用者によるサービスの利用傾向を分析する際の参考として利用します」との旨が明記されておりました。また、これに同意しなければ意見を送信することができない仕様となっておりました。 　しかしながら、国民からの意見募集という趣旨は、本来、行政施策に対する多様な声を受け止めるものであり、情報提供の目的が「サービスの利便性を向上させるため」とされているとはいえ、それに協力しない者には意見提出の機会すら認めない、という運用は、制度の理念と齟齬を来しているのではないかと懸念いたします。 　殊に、プライバシーに対する感度が高まる現代においては、利用者の意見提出という公的行為と、自身の情報の利活用とを切り分けて考える余地が保障されるべきではないかと存じます。 　つきましては、このような利用者情報の取扱いと意見提出の条件付けの是非について、ぜひとも専門的かつ建設的な議論を、関係有識者による会議体にて集中してお取り扱いいただきたく、謹んでお願い申し上げます。 その四：募集要領ならびに e-Gov 上の案内を熟読いたしましたところ、提出様式と提出手段に関して、制度上の整合性に欠ける記載が見受けられ、戸惑いを禁じ得ませんでした。 　募集要領には e-Gov のサイトでは「添付ファイルは利用できません。添付ファイルを送付する場合は、（２）により提出してください」との記載がございますが、e-Gov の入力画面では添付ファイルが使用可能とされており、Excel ファイルも利用可能な形式として明示されております。一方、電子メールによる提出においては、「添付ファイルを送付する場合、ファイル形式は、テキストファイル、マイクロソフト社 Word ファイル、ジャストシステム社一太郎ファイルにより提出してください（他のファイル形式とす		

る場合は、担当までお問合せください。)」とあり、Excel ファイルが添付可能な形式に含まれておらず、提出希望者には「お問い合わせください」とのみ案内されている状態でした。 　しかも、今回の意見提出様式としては、貴庁より Excel 形式のファイルが指定・配布されており、その使用が前提と理解されます。にもかかわらず、提出方法に関する説明に不整合があることにより、私のような一市民にとっては、どの方法で、どのファイル形式を用いて提出すべきかが分からず、思い悩んだ末に、ついに提出を断念せざるを得ませんでした。 　率直に申し上げまして、制度として国民の声を受け止めようとされている姿勢に敬意を抱いていたからこそ、考え抜いた意見を届けることができなかったことは、まことに口惜しく、無念の思いでおります。意見を伝える機会を前にしながら、その門前で躊躇し、引き返さざるを得なかった心境は、私に限らず他にも同様の思いをされた方がいらっしゃるのではないかと拝察いたします。 　つきましては、今後におかれましては、提出様式・受付手段・システム案内等の間に齟齬が生じぬよう制度運用の整合性をご検討いただき、せっかく声を届けようとする国民が、その手前で立ち止まることのないよう、ご配慮を賜りますとともに、諸条件を整えられた上での改めての意見募集を行っていただきますよう、謹んでお願い申し上げます。 【個人】		
闇バイト、特殊詐欺、不正アクセス、飛ばしの携帯、ダークパターンなど、日本の法規制が緩く、また刑罰などが軽いことを良いことに、ICT を取り巻くさまざまな犯罪が日々なされている。 　日本人の個人情報、データ、財産などが狙われた場合であっても、執行猶予が付くなど、刑罰が軽すぎると思う。 【個人】	いただいた御意見については、今後の検討を進めていく上での参考とさせていただきます。	無
グローバルに知りたい情報を得られる現代ですが、その弊害の一つが昨今の闇バイト、SNS 等を悪用した犯罪であるのは明白です。 　今回の報告書を読み、青少年の保護を目的とした個人情報に関する法律、各媒体に求める情報の管理について、一刻も早い法規制が望ましいと考えます。	本報告書は青少年保護の観点から法律に基づく規制を導入することを検討したものではございませんが、いただいたご意見については、今後の検討を進めていく上での参考とさせていただきます。	無

今の日本は、各個人が使うパソコンや携帯端末からの情報の吸い上げ、取得に関する法律や防衛が甘く、やりたい放題の状態にあると思います。 なので今回報告書にまとめられた方向で規制をかけていくことに賛成です。 また、これは日本だけの問題ではないと考えますが、グーグルやヤフーといった検索エンジンがインターネット上にある情報へのアクセスや搾取が混乱を招いている状態にもあると思います。 色んな情報媒体等で注意が促されていますが、生成 AI は誤った、或いは偏った情報を拡散する可能性が高く、その一つがグーグルの「AI による概要」、ChatGPT です。 技術の進化自体は喜ばしく、生活水準の向上が望めますが、現状ではデメリットが強く作用し、情報ツールを使った犯罪やデマといった問題として今表面化していると思います。 ただしい情報の管理、運用の基礎を築く法改正を望みます。 その為にも、携帯といった情報端末、SIM といった媒体の管理、入手の仕方の規制を早く進めることが望ましいと考えます。 現代は子ども以外にもお年寄りも気軽にネットを使う時代です。いわゆる情報弱者が騙されない、安全にネットを使える環境が整うことを望みます。 【個人】		

その他

提出された御意見	御意見に対する考え方（案）	御意見を踏まえた案の修正の有無
2. その他の検討課題 GIGA スクール等の大規模プロジェクトで今後ますます学校への IT デバイスの導入が進むことが考えられますので、 そこに特化した取り組みへの言及していただき、学生の保護も最大限に考えて、さらなる検討が進められることと 大変期待しております。 【スカイワゴン株式会社】	いただいた御意見は今後の参考とさせていただきます。	無
現在、画像や音または動画を生成する AI 機能によるディープフェイクポルノや詐欺が急増している。 これらのネット犯罪を抑制する為に AI の使用用途や開発技術を規制する法律を施行して貰いたい。 【個人】	本報告書（案）は生成 AI の利用等ルールに関して検討を行ったものではございません。	無
生成 AI を利用した犯罪は目に見えず、表沙汰になっていない所で事例が上がっています。 開発段階で AI を利用したところで個人情報の保護はどうなるのでしょうか？漏洩した場合の危険性は？ 過去何度もインターネットトラブルによる情報漏洩が発生しています。生成 AI もまたその事例の一つとなり兼ねないと懸念しています。 また、多くのデータ（アート、音楽、文章）を無断機械学習を禁止する法規制を定めていただきたいと願っています。 【個人】	本報告書（案）は生成 AI の利用等ルールに関して検討を行ったものではございません。	無
●生成 AI について 生成 AI を用いた犯罪が急速に拡大しており、早急な対応が不可欠だと考える。	本報告書（案）は生成 AI の利用等ルールに関して検討を行ったものではございません。	無

ディープフェイクを用いることにより実在の人物の声を合成した詐欺やデマの流布がすでに行われている。有名人の動画を合成し投資詐欺に使うなど手口はいくらでも考えうる。さらに海外では両親の声を生成し誘拐に使われる危険性もあると警告がされている。 実在の人物に対するフェイクポルノによる被害も深刻である。ネット上に上げた個人の写真や卒業アルバムから、フェイクポルノが作成される事が問題になっている。さらに、そのフェイクポルノを利用した恐喝も、今後国内で起こると予想される。 生成AIを利用した詐欺メール・詐欺広告もすでに広がっている。従来よりも、簡単に、短時間に、そして大量にこれらの詐欺に用いる素材が生成AIによって作り出し易い環境になっている。日本を標的にした海外からの詐欺には、生成AIによる翻訳がより強力に用いられいてる。 こういった問題が起こる背景には、生成AIの学習データセットに『無許可の個人情報』や『児童虐待記録物』が用いられている。有名人のディープフェイクや、実在する未成年の猥褻な動画や画像を合成できるのはそのためだ。 詐欺などの被害を防ぐためにも、生成AIで生成された動画や画像、文章などには、『生成AIを用いたとラベル付する』事を義務化すべきである。 さらには、無許可の個人情報や、児童虐待記録物など法的倫理的に問題のある学習データセットを用いた生成 AI は使用禁止も議論されることを望む。 【個人】		
罰則をつけて法整備を早急に進めて欲しいです。 【個人】	いただいた御意見は今後の参考とさせていただきます。	無
生成AIがあらゆる犯罪（ディープフェイク、ポルノ、なりすまし等々）に悪用されている現状から、「罰則付き」で生成AIで作成された画像、音声、	本報告書（案）は生成AIの利用等ルールに関して検討を行ったものではございません。	無

動画、文書には「生成 AI 製」であることの表示義務付けが必須であると考える。 現状生成 AI は詐欺に最も貢献しているツールだと認識を国民が共有しなければならない。 【個人】		
P9「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。」 分かっているのなら早く規制してください。状況はどんどん悪化しています。生成 AI を含む AI を活用したいのならば、罰則付きのルールをつくって悪用させないようにしてください。 ディープフェイクと著作権侵害ばかりで日本はまったく発展していません。 【個人】	本報告書（案）は生成 AI の利用等ルールに関して検討を行ったものではございません。	無
資料にもある楽天モバイルでの事案だけに留まらず、生成 AI による犯罪は今後さらに増加すると考えています。本来、生成 AI は未成年に対しては年齢による制限があるはずですが、楽天モバイルの件にて犯行に及んでいるのは中高生であり、単なる制限では防ぎきれておりません。 生成 AI 使用者の登録及び管理の義務付け、出力結果に対する生成 AI ラベリングの義務付け、それらを違反した場合や悪用が認められた場合に刑事罰による重い罰則など、生成 AI 独自の法律が必要と考えています。年齢や知識を問わず、短時間に多くの犯罪ができてしまう生成 AI からあらゆる情報を守るべきです。 【個人】	本報告書（案）は生成 AI の利用等ルールに関して検討を行ったものではございません。	無
犯罪の高度化は SNS の高性能化や気軽さに由来する部分が多いと思われるため一定年齢以下に対する利用の制限をより呼びかけるべきと思われる。 特に Twitter や Instagram は今や利用=情報流出に同意したとも思えるサービスや規約を提供していると考えても過言ではない。 しかしながら一定年齢以上であってもこれらの危険性を理解していないと思われる人間が多いことも現状事実であると考える。	本報告書（案）は生成 AI の利用等ルールに関して検討を行ったものではございません。	無

特に生成 AI を通じて利用者に提供「させた」データ、もしくは生成 AI を介して侵入・取得されたデータがまた別の利用者(犯罪者)に提供されることは考えるに易く実際そうなのだろうと思われる。 特にリテラシーの不十分な利用者は遊び半分にディープフェイク等の画像や映像を作り、身近な人間に対する被害者にもなり得ると考えられる。 SNS 全体はむずかしいとしても生成 AI に対する注意喚起は、被害者と加害者の双方を増やさないためにもより行っていくべきと考える。 とかく、電話やチラシ(ダイレクトメール)といった現物に対しても、SNS や Web サービスといった目に見えないものに対しても、正しい知識や認識を持つための啓蒙をより行っていくべきであると思う。 【個人】		
まず、国内外のクリエイターの著作物を無断で二次利用している現状の生成 AI は使用せず、盗品であることを周知してください。 データセットには著作物だけでなく、犯罪や戦争被害者や CSAM も含まれています。 政府が推進すべきは「著作物等の無断使用は違法である」という原則を広く周知した上で、著作権者と事業者との間での公正な取引を推進する政策です。よろしくお願いします。 個人情報や著作物や肖像を取り込まれる点からも、LLM による情報漏洩や合成による悪用は危険視される内容です。 犯罪に利用できないように罰則付き規制を求めます。MAGA の資金力だと少額の罰金は取るに足らないもので、抑止力にすらなりませんので厳しい規制をしてください。 【個人】	本報告書（案）は生成 AI の利用等ルールに関して検討を行ったものではございません。	無
生成 AI による犯罪の増加・巧妙化は本当に深刻だと思います。 犯罪の敷居が極端に下がり、本人が犯罪を犯している実感、罪悪感なども感じづらく軽視してしまうケースもあるのではと危機感を覚えます。	本報告書（案）は生成 AI の利用等ルールに関して検討を行ったものではございません。	無

「文章・画像・映像・音声等一切のメディア媒体に限らず生成 AI による出力物は「生成 AI での出力である」情報をかならず表示させるように義務づける」ようにする事で、偽情報である事が区別できるようになると思います。 ただし現状の SNS の流れを見る限り、違反に対する罰則をきちんと設けないと効力は全然期待出来ません。 しっかりとした明言・罰則が必要であると考えます。 【個人】		
４２２ AI 生成物のラベル付与に関する対応の在り方 プラットフォーム事業者に対しては、電子透かしや来歴管理とラベル付与との技術的差異やそれぞれの効果や実現性の比較をしつつ、４ １ １ ３で述べた「自主規制型行動規範」を活用するか、引き続き、検討をしていくことが適当である。 自主的に規制を求めるのではなく、義務付けなければならない事案であります。 災害やテロ等の大きな事件が発生した際、ラベル付けされていない映像等の精巧な虚偽情報は社会的混乱をもたらすのには十分過ぎる程の物です。 既に検討の域を脱する領域の悪質な虚偽情報の流布が起きており、流布した人物、並びにラベル付けをしない企業等に対して監査や法的罰則を与える抑止力は必要不可欠な状態です。 各国の生成 AI に対する情勢を鑑みてもラベル付けは、最低限の条件として見ていいと考えており、日本だけラベル付けされていない状態のまま検討を続けるのは国際的な信用、交易に置いても不利を被るのは明白です。	本報告書（案）は生成 AI の利用等ルールに関して検討を行ったものではございません。	無

更に述べるなら、本国の災害発生頻度の高さからしてもラベル付けされていない生成 AI による、虚偽情報は避難や人命救助等の非常事態に対して致命的な遅れをもたらすのは想像に難くありません。 【個人】		
生成 AI による高度な犯罪が横行しているなかで、出力された画像や動画にはその旨を表記することを義務化して欲しいです。一般人ではとてもそれが出力されたものなのか否かを判断することは難しく、ディープフェイクによる誤報に騙されることも多いと思います。誰が見ても分かるように生成 AI で出力した画像または動画であると表記をして欲しいと感じます。 【個人】	本報告書（案）は生成 AI の利用等ルールに関して検討を行ったものではございません。	無
生成 AI の悪用による犯罪の巧妙化、高度化を指摘されております。このことが起こるのは、日本では生成 AI に対する法規制がないためと考えております。今年 5 月に成立した「AI 新法」では、AI 技術の発展の萎縮を懸念して罰則を一切設けることはありませんでしたが、善良な企業ならまだしも「悪用」に対してまで萎縮を懸念する必要はありません。生成 AI および AI の適切な規制は、悪用を抑制し日本の AI の健全な発展に必要不可欠になると考えます。また、実犯罪によってじわじわの広まってきた市民の AI 全般に対する不安を挽回することもできるのではないでしょうか。 3 年前に AI が起こしうる問題として予想されていたことが、今現実で犯罪として、特にインターネットを利用した犯罪として実現してしまっています。AI は応用の幅が広く、資料で挙げられた例以外のケースも増大するのは想像に容易です。実際に AI を利用した犯罪がこれ以上に恒常化・悪化する前に、法規制などを実効性のある施策によって先手を打つことをお願いいたします。 【個人】	本報告書（案）は生成 AI の利用等ルールに関して検討を行ったものではございません。	無
我が国はこれまで日本語を母語として営んでおり、言語障壁はグローバル化の課題である一方で強固なセキュリティとして機能してきました。しかしここ数年の生成 AI の登場により正確性はともかく、大まかな翻訳が可能になり、文字通りボーダーレスとなってしまった現状、外国からのサイバー攻撃や詐欺が劇的に増え、今や犯罪者の金鉱脈といっても過言ではない状況です。	本報告書（案）は生成 AI の利用等ルールに関して検討を行ったものではございません。	無

現行犯が我が国にいない場合自国のみでの対応はほぼ不可能であるため、各国規範と連携と協調が取れるように一層厳格な法整備が必要かと存じます。同様に国内の過失においても責任の所在が曖昧となっており、そういった面での対策も必要と存じます。 欧州では先日発表された AI 法のほか英国などは年齢確認の厳格化を施工し、その他の国でも同様に未成年保護の対応に乗り出しております。 デンマークは現行法では生成 AI から人々を守ることができないとシュミット文化大臣が発言し、超党派の合意を得て 6 月 26 日に誰もが自分の声や身体特徴に対する権利を持てるように著作権法を改正いたしました。これらは国民を第一に考えたディープフェイク対策として実施されるものです。 米国でもトランプ大統領が One Big Beautiful Bill にて盛り込もうとした著作権などの人権を 10 年間規制させないという条項は与野党ともに多数の反対をもって却下されました。一方で 7 月下旬には共和党の Josh Hawley 上院議員は民主党の Richard Blumenthal 上院議員とともにテック企業に対しデータの著作権侵害について法に基づき訴えられるよう AI 保護法案を提出しました。 こうした流れの中我が国が国外からのサイバー犯罪に対し国際的な連帯を得るためには協調が必要かと存じます。 青少年育成に対しては我が国はマイナンバーを国民に付したのですから、これらを持ってインターネット上の年齢確認などの連携をとり、未成年の自由意志等の成長を阻害しない範囲でのコンテンツ制限をかけるべきかと存じます。特に生成 AI を使ったディープフェイクポルノを制限する事は昨今ニュースでも取り上げられている卒業アルバムなど同級生の顔を取り込ませたディープフェイク対策にもなると考えます。 偽広告におけるロゴや著作物の無断利用に関しても Cloudflare が実装したクレデンシャル機能（あるいはそれに類するもの）を利用することにより追跡が可能となりますので官民一帯で奨励することを進言いたします。		

あるいは緩めの免許制にすることで使途の明文化が為され、追跡が容易となるのではないでしょうか。 兎にも角にも我が国は非常に狙われやすい国であるため、早急に対策を要するものと考えます。その中で何が必要であるかを改めて議論を重ね取捨選択すべきと存じます。 【個人】		
生成 AI による出力物を「生成 AI による出力結果」だと簡単に判別できるラベル付けの義務化を求めます。そもそも誰もが簡単に生成 AI を利用できる現状に問題があるので、現状の生成 AI は利用禁止にするのが妥当だと思います。誰もが使える ChatGPT など LLM による情報漏洩のリスクが付いて回ること、生成 AI を利用する為に無駄な電力と冷却水用の水を大量消費し続けていく必要があること、どれも紛れもない事実です。こんなものの活用を無理矢理推し進めても詐欺が横行し犯罪のハードルが下がり環境破壊が進むだけでろくな利点がありません。可能ならば現状の生成 AI 利用を禁止にするべきです。 利用禁止が叶わないのであれば、生成 AI による出力結果へのラベル付け義務化を早急に実現してください。国民の安全な生活を犠牲にし無駄な電力を大量消費し続けてまで、生成 AI を活用する価値が本当にあるのでしょうか。 【個人】	本報告書（案）は生成 AI の利用等ルールに関して検討を行ったものではございません。	無
現在、IT に関わる犯罪が多く発生している事は身近に感じて（実際に海外からの迷惑電話、インターネット WEB サイトへの多くのスクレイピング、SNS で開放している DM 等への詐欺勧誘等）います。 数年前に生成 AI が現れてから、さらに迷惑行為は増加しています。（これらに関しては、生成 AI でのディープフェイク、災害時への偽アナウンスでの迷惑行為、そして、実際に受けた被害としては、i2i と呼ばれるイラストを生成 AI に取り込ませて、新たにその取り込んだイラストをベースとしてディープフェイク画像を合成生成する行為、それらの被害を発言する事による誹謗中傷等で心身共に被害を受けています）	本報告書（案）は生成 AI の利用等ルールに関して検討を行ったものではございません。	無

生成 AI は知識が必要なく、時間も圧倒的に短縮出来てしまうので犯罪へのハードルが劇的に下がり、犯罪行為がしやすくなったのが大きいと思います。 早急に生成 AI に対する規制や禁止を対策する必要があります。 【個人】		
報告書案９から１０頁に楽天への不正アクセスの事件について例示されているように、昨今は生成ＡＩを悪用、時には法を犯している自覚もない使い方をして、逮捕される事案が相次ぎ、ニュースによる犯罪の警鐘も増えています しかし、本年に可決されたＡＩ推進報ではＡＩを推進することを優先とし、業者に対しては指導・悪質な場合は公表までであり、なんら罰則のない、抜け道がいくらでも作れるような内容となっております。 （日経新聞『ＡＩ技術の開発・活用を推進、悪用事業者は国に調査権　初の法整備』より参考） 昨今の情報流出や詐欺、ディープフェイクの制作を容易にするこれらをＡＩ業者に規制するのではなく、使用者の問題、使用者側の責任としたままでは、ユーザーは業者に対して不審が募り、生成ＡＩ技術は忌避され、技術の発達どころか利益を上げられなくなります。 罰則、あるいは罰則にあたる強い規制が必要だと思います。 【個人】	本報告書（案）は生成 AI の利用等ルールに関して検討を行ったものではございません。	無
「個人情報には個人が特定可能な画像や動画も含まれる」とされていますが、そうなればより一層 LLM による情報漏洩などは危険視されるべきだと思います。 また、犯罪利用できないように罰則付きの規制の制定が必須です。 【個人】	本報告書（案）は生成 AI の利用等ルールに関して検討を行ったものではございません。	無
こちらは要望ですが、構成員の意見についてどの構成員がどの意見を発しているのか、より多く同意見がなのかを明確にして欲しい。 【個人】	いただいた御意見は今後の参考とさせていただきます。	無

本文 10 ページ、『（３）犯罪行為の巧妙化、高度化』にて『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。』とありますが、その通りだと存じます。 生成 AI の悪用により、詐欺、脅迫、ディープフェイクポルノ（セクストーション含む）被害は増える一方です。 生成 AI は CG 作成技術に乏しい素人でも精巧なディープフェイクを簡単かつ大量に生成できる技術です。 その物量は現行法では対応しきれない問題かと存じます。 生成 AI を簡単に悪用できないよう、罰則付きの法規制が必要です。 また、生成 AI の開発には、数十億にも上る利用許諾のない個人情報や著作物データが大量に使われている（無断機械学習）ことも問題です。 現に海外では、OpenAI をはじめとした開発企業が、報道機関やクリエイターの方々から著作権侵害の裁判を多数起こされています。 無断機械学習されたデータは、いつ何時情報流出するかわかりません。 データセットを掘り起こせば、個人を特定することも容易です。 個人情報保護やプライバシーの保護、強いては個人の安全（情報流出によって、犯罪に遭うリスクは増すため）を確保するためにも、開発企業に対し『個人情報や著作物は無断利用してはいけない』という明確かつ罰則付きの規制が必要です。 【個人】	本報告書は、生成 AI に対する規制を導入することを検討したものではございませんが、いただいた御意見については、今後の検討を進めていく上での参考とさせていただきます。	無
生成 AI を利用した犯罪の事例がありましたが、個人情報保護やプライバシーの観点からも、LLM による情報漏洩などは危険視されるべき内容かと思います この資料では個人情報には個人が特定可能な画像や動画も含まれるとされています 犯罪利用できないように罰則付きの規制の制定が必要だとおもいます。 【個人】	本報告書は、生成 AI に対する規制を導入することを検討したものではございませんが、いただいた御意見については、今後の検討を進めていく上での参考とさせていただきます。	無
（前提） 生成 AI モデル：	本報告書は、生成 AI に対する規制を導入するこ	無

・ChatGPT などの、生成 AI のデータベース。データは以下のような形で（本人の意図とは関係無く）収集される。 ・「学習拒否設定」（オプトアウト）をしないまま、当該サービスへ入力される ・インターネット上のアクセス可能なサイト（SNS 等）から無差別にデータを収集する ・同様に成立した他の生成 AI(モデル)にアクセスしてデータを収集する 不適正利用対策に関するワーキンググループ (P.9) 1-1-2 (3)犯罪行為の巧妙化、高度化 ・生成 AI で良く言及されるものは「汎用生成 AI」とも言われ、大量アクセスや権利保護されているデータの不正利用により成立しているものです ・当該部分では、プログラムソース（これらは公開し、限定的な利用に関して許容されているものも多い）を利用したものですが、例えば「個人情報の窃取を目的とした処理」を大量に埋め込み、生成 AI モデル（生成 AI のデータベース）へと学習させ、サービスとして共有されることにより、「生成 AI を用いたプログラムの作者が意図しない形で、不正行為の当事者となってしまう」という脅威が発生し得ます ・また、生成 AI の自由度が高いために「業務やプログラム制作の効率化」を目的に、生成 AI モデルに学習されない設定（オプトアウト）をオフにしないまま個人情報を入力させてしまうケース自体は、多くあると考えています。(「Web サービス側が個人情報は保存しないだろう」という思い込みによるもの) 【個人】	とを検討したものではございませんが、いただいた御意見については、今後の検討を進めていく上での参考とさせていただきます。	
本文 10 ページ、『（３）犯罪行為の巧妙化、高度化』にて『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。』とありますが、その通りだと存じます。 生成 AI の悪用により、詐欺、脅迫、ディープフェイクポルノ（セクストーション含む）被害は増える一方です。	本報告書（案）は生成 AI の利用等ルールに関して検討を行ったものではございません。	無

生成 AI は CG 作成技術に乏しい素人でも精巧なディープフェイクを簡単かつ大量に生成できる技術です。 その物量は現行法では対応しきれない問題かと存じます。 生成 AI を簡単に悪用できないよう、罰則付きの法規制が必要です。 また、生成 AI の開発には、数十億にも上る利用許諾のない個人情報や著作物データが大量に使われている（無断機械学習）ことも問題です。 現に海外では、OpenAI をはじめとした開発企業が、報道機関やクリエイターの方々から著作権侵害の裁判を多数起こされています。 無断機械学習されたデータは、いつ何時情報流出するかわかりません。 データセットを掘り起こせば、個人を特定することも容易です。 個人情報保護やプライバシーの保護、強いては個人の安全（情報流出によって、犯罪に遭うリスクは増すため）を確保するためにも、開発企業に対し『個人情報や著作物は無断利用してはいけない』という明確かつ罰則付きの規制が必要です。 【個人】		
「不適正利用対策に関するワーキンググループ」の「（３）犯罪行為の巧妙化、高度化」において挙げられている事例への対策として、生成 AI の悪質な利用方法への規制、罰則の必要性は明らかであるにも関わらず、「生成 AI のイノベーションを阻害する」という理由で法整備を意図的に滞らせている。 発生することが明らかである犯罪行為に対する規制、罰則の整備が急務である。 【個人】	本報告書（案）は生成 AI の利用等ルールに関して検討を行ったものではございません。	無
生成 AI は「自然人になりすます」ことが可能です。 携帯電話不正利用防止法然り、他の既存法でも相手が自然人であって、当然警察や事業者も自然人であることが前提として成り立っているはずです。 昨今の詐欺は、相手が実は生成 AI で作られた偽物警官だったという案件が増えてきています。ビデオ通話等でも判別できないほどです。	本報告書（案）は生成 AI の利用等ルールに関して検討を行ったものではございません。	無

真贋判定が難しいほどの精巧さで偽造された本人確認書類も、生成 AI がその作成を容易にしている事実があります。 参考記事 生成 AI の進化で身元確認書類の偽造が容易に、KYC の終焉 https://rocket-boys.co.jp/security-measures-lab/ai-id-spoofing-end-of-kyc-era/ 「YouTube」に著名投資家の音声合成した偽広告 詐欺の新手口か https://www3.nhk.or.jp/news/html/20250620/k10014839541000.html せめて、ディープフェイクは禁止する罰則規定を作っておかなければ、携帯電話不正利用防止法そのものが成り立たなくなることも可能性として考えられます。生成 AI により本人確認書類の信頼性が担保できなくなってからでは遅いです。 【個人】		
報告書(案)9 ページ(3)「犯罪行為の巧妙化、高度化」内に、「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」という記述がありますが、これについては現状大変深刻な問題であると考えます。 資料内にも記載がありましたが、生成 AI などの技術を用いることで未成年者でさえ気軽に犯罪行為を行うことができてしまうという現状の背景には、そもそも「生成 AI を用いた悪質な行為」に対する適切な罰則が設けられていないこと・法整備が十分でないことが原因として挙げられると思います。罰則が設けられていないことが、犯罪行為へのハードルをグッと下げているように思えてなりません。 インターネットや通信の不適正な利用への対策をより進めるためにも、生成 AI などの新しい技術には一刻も早く適切な規制を設けるべきだと考えます。 【個人】	本報告書（案）は生成 AI の利用等ルールに関して検討を行ったものではございません。	無
現在、生成 AI によるディープフェイク等の人権侵害や詐欺犯罪、誤情報や差別的回答の拡散、著作権侵害等の事案が多発していますが、被害を防止	本報告書（案）は生成 AI の利用等ルールに関し	無

するための法規制等の対策が講じられておらず、野放しとなっている状態です。 ・性的ディープフェイクによる人権侵害の事案 ・生成 AI を使用した巨額の投資詐欺事件 ・生成 AI も使用した巨額の証券口座への不正アクセス事件 ・生成 AI 音声を使用した「オレオレ詐欺」事件 ・生成 AI チャットボットを利用していた未成年者が痛ましい事件が起きてしまい、保護者が AI 企業を提訴した事件 米のセキュリティ企業の調査では、今年の 1 月から 5 月での全世界の新種メール攻撃のうち 84%が日本を標的としているという調査結果があり、その原因として生成 AI の使用が挙げられています。 本報告書でも言及されているように、携帯電話等の ICT サービスにおける問題において、特殊詐欺やフィッシング詐欺や人権侵害等は重大な問題であり、 すでにスマートフォンや PC に生成 AI を組み込んで販売している事業者が増加していることからも、携帯電話や PC に組み込まれた生成 AI やアプリストアの AI アプリ等を用いて、特殊詐欺やフィッシング詐欺、不正アクセス、ディープフェイク等の犯罪行為のハードルがさらに下がる可能性が高い状況です。 このような状況は新たな段階での深刻な社会問題と言えますので、被害を防止するための法規制を含めた対策が急務です。 【個人】	て検討を行ったものではございません。	
犯罪利用できないようにするためには罰則が必要です。特に生成 AI 絡みのものに関しては、それ自体を「ガイドラインで規制できる」という方針で	本報告書（案）は生成 AI の利用等ルールに関し	無

進める限り、被害は広がるばかりでしょう。「悪用される件もある」のではなく「悪用しかされていない」のであり、その使用がさらなるデータの不正利用、ひいては不正アクセスに繋がることを思えば、犯罪の温床としてのみ機能していると言えるでしょう。「それっぽいものを出力する」ことに関しては非常に優れたものを作り出してしまうという性質のせいでよけいに、ということです。 こういった闇バイトの契約や携帯電話の複数回線契約に関して、騙された被害者側や仲介させられた事業者側に責任を問うのではなく、騙した側、ひいてはそのシステムをのさばらせている企業、国の責任を重く受け止め、重い罰則規定を設けることが必要不可欠と考えます。 【個人】	て検討を行ったものではございません。	
P.9　3 犯罪行為の巧妙化、高度化 について触れられている通り、生成 AI が犯罪のハードルを著しく下げている事を顧みて、犯罪に利用されない法律の整備と規制が必要であると考えています。 (あとに続く本人確認のルールを厳しくというのも勿論大切なのですが)対策という視点から見ても、簡単に不正や詐欺に悪用可能なツールをまず規制したほうが良いのではないでしょうか。 【個人】	本報告書（案）は生成 AI の利用等ルールに関して検討を行ったものではございません。	無
不適正利用対策に関するワーキンググループ 第１章 不適正利用対策をめぐる環境変化 につきまして、 犯罪行為において昨今の生成 AI と呼ばれる剽窃ツールにより個々人の画像を卑猥なものや虚構に改造され使われています。 個人情報の特定の際の画像、動画等がそれらに悪用されないための罰則つきの規制が必要です。 大手の OpenAI のサム・アルトマン本人でさえ（（始めた本人が今頃あたりまえのことに気付いたのかという話ではありますが）今になってやっと個人的な情報、機密情報等は AI に入力すべきではない旨を理解し発信する時代になっています。	本報告書（案）は生成 AI の利用等ルールに関して検討を行ったものではございません。	無

【個人】		
不適正利用対策に関するワーキンググループ を通しての意見 第１部１章の２、（３）にも記載されているような生成 AI の悪用による不正契約や、本人確認書類の偽造も生成 AI により容易になります。 詐欺被害の爆増の背景には生成 AI による影響も多いかと思われます。 携帯電話などの契約時の本人確認などおける具体的な対策に、詐欺へ使用されることの観点から生成 AI の適切な規制を求めることも含めていただきたいです。 【個人】	本報告書（案）は生成 AI の利用等ルールに関して検討を行ったものではございません。	無
本件において生成 AI を利用した不正アクセスの危惧は当然ですし、闇バイトのような集団による犯罪行為も危惧すべきなのは同意です。 しかし携帯電話における本人確認には限界があり、偽のマイナンバーカードなどですり抜けてしまう恐れがあります。 また生成 AI を利用した加害行為については携帯電話、スマートフォン、パソコンのアプリやプログラムに組み込まれた生成 AI を用いた生成情報から他者の個人情報（パスワードや個人の配送先住所等）を盗み取られる事や、生成した画像や音声データや文章を悪用したいじめであったりディープフェイクや詐欺行為、生成したコンピューターウィルスのコードや個人情報を用いて不正アクセスが可能になるなど、一個人の犯罪行為がしやすくなっております。 このような犯罪行為を安易に起こさせない為にも、個々人が簡単に加害行為で生成 AI が使えないように個人情報に関わるデータ（著作権の有無だけでなく画像や文章関係なく）収集ができないよう国内外の事業者へ法規制をすべきです。 【個人】	本報告書（案）は生成 AI の利用等ルールに関して検討を行ったものではございません。	無
（前提） 生成 AI モデル： ・ChatGPT などの、生成 AI のデータベース。データは以下のような形で（本人の意図とは関係無く）収集される。 ・「学習拒否設定」（オプトアウト）をしないまま、当該サービスへ入力される	本報告書（案）は生成 AI の利用等ルールに関して検討を行ったものではございません。	無

・インターネット上のアクセス可能なサイト（SNS 等）から無差別にデータを収集する ・同様に成立した他の生成 AI(モデル)にアクセスしてデータを収集する 不適正利用対策に関するワーキンググループ (P.9) 1-1-2 (3)犯罪行為の巧妙化、高度化 ・生成 AI で良く言及されるものは「汎用生成 AI」とも言われ、大量アクセスや権利保護されているデータの不正利用により成立しているものです ・当該部分では、プログラムソース（これらは公開し、限定的な利用に関して許容されているものも多い）を利用したものですが、例えば「個人情報の窃取を目的とした処理」を大量に埋め込み、生成 AI モデル（生成 AI のデータベース）へと学習させ、サービスとして共有されることにより、「生成 AI を用いたプログラムの作者が意図しない形で、不正行為の当事者となってしまう」という脅威が発生し得ます ・また、生成 AI の自由度が高いために「業務やプログラム制作の効率化」を目的に、生成 AI モデルに学習されない設定（オプトアウト）をオフにしないまま個人情報を入力させてしまうケース自体は、多くあると考えています。(「Web サービス側が個人情報は保存しないだろう」という思い込みによるもの) 【個人】		
(P.25？) 第２章 その他の特殊詐欺の電話・メール等に関する課題 ・生成 AI は、映像、音声や読み上げさせる文章のそれぞれのモデルを連携させれば、自動で電話をかけ、著名人の音声や自動応答により、虚偽の投資を持ちかけるなどが可能と考えます。(AI 語り部などの有用な技術が、音声・映像等のデータを悪用する例。一般にディープフェイクと区別されますが、根幹の技術は共通です) ・あずかり知らぬ所で学習されたことにより、不正行為への加担をしたとしてえん罪が発生することへの危機感を持っています。	本報告書（案）は生成 AI の利用等ルールに関して検討を行ったものではございません。	無

・生成に関して有用な部分があるのは承知の上ですが、まずは「生成 AI モデルへの学習をされない権利」という面が確立されることを望みます。【個人】		