資料８－１

総務省

ICTサービスの利用環境を巡る諸問題について

～不適正利用対策をめぐる環境変化と新たな対策について・第11～12回の不適正利用対策に関するワーキンググループの報告（案）～

令和７年12月８日

総合通信基盤局

これまでの検討経緯

	ICTサービスの利用環境の整備に関する研究会（親会）	不適正利用対策に関するワーキンググループ
本年 4～9月	7月3日（第7回） 報告書とりまとめ案 7月5日～8月4日 意見募集 9月8日（第8回） 意見募集の結果報告 9月10日　報告書とりまとめ	4月～6月（第7回～第10回） 検討 （1）携帯電話本人確認のルール （2）特殊詐欺、闇バイト等対策
10～12月	12月5～8日（第8回） メール審議	11月4日（第11回） ➢ ①上限契約台数 （事業者団体ヒアリング　有） 11月21日（第12回） ➢ ①上限契約台数に関する論点整理 ➢ ②フィッシングメール対策 （事業者ヒアリング　有）

9月報告書までの検討状況 （第7回～第10回　不適正利用対策WG）

背景

いわゆる「闇バイト」犯罪の増加

- ✓ 携帯電話の不正SIMの転売が報告される

特殊詐欺被害の深刻化

- ✓ 特殊詐欺の8割が電話経由（国際電話が急増）

犯罪行為の巧妙化、高度化

- ✓ 青少年が生成AIを悪用した自作プログラムで携帯電話を不正契約

検討項目

(1)携帯電話本人確認のルール

1. SIMの不正転売
2. 法人の代理権(在籍確認)
3. 他社の本人確認結果への依拠
4. 追加回線
5. 上限契約台数
6. データSIM

(2)特殊詐欺、闇バイト等対策

1. 固定電話の対策
携帯電話・SMS・メールの対策
2. 既存番号のスプーフィング(なりすまし)
3. 海外電話番号による詐欺電話

令和7年4月から6月まで、計4回の議論を経て、上記項目について検討を行い、
9月に報告書をとりまとめ

9月報告書の概要 （不適正利用対策WG箇所抜粋）

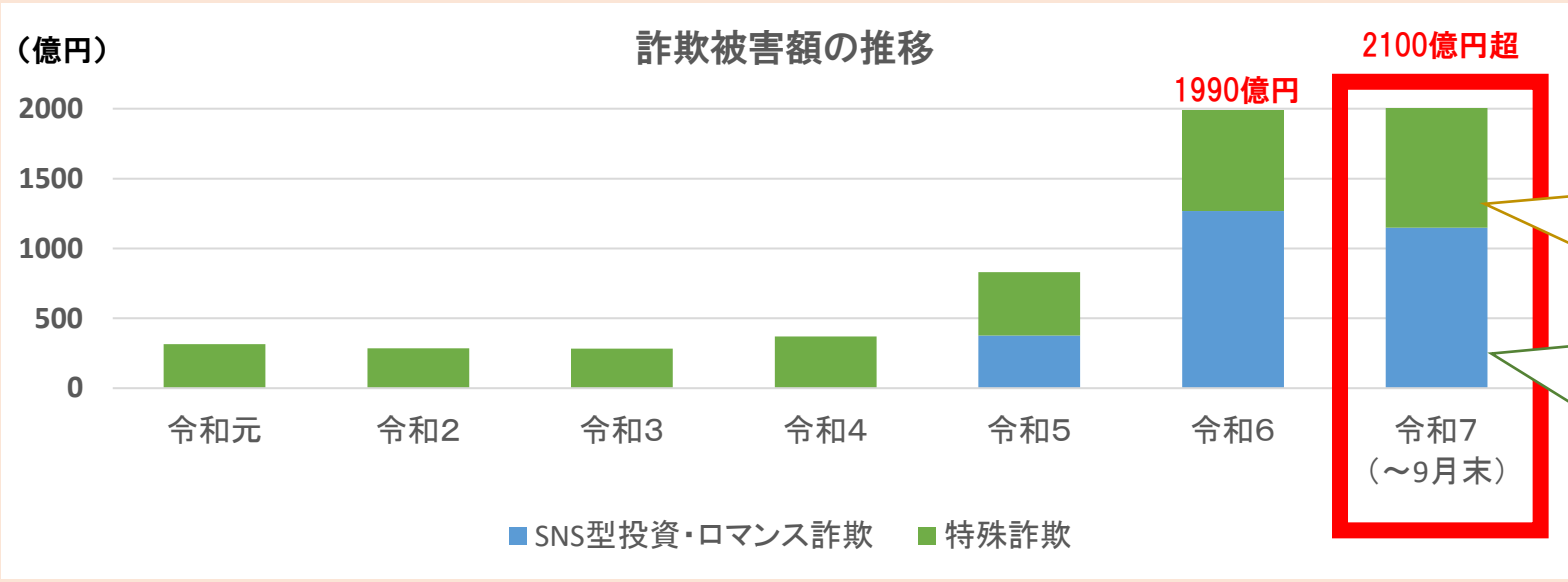
- ICTサービスの利用環境の整備に関する研究会において、令和7年９月、報告書をとりまとめ。
- 携帯電話の本人確認ルールの厳格化を含む課題について、今後の取組の方向性を整理。

●令和７年９月の報告書の概要 [注１]

1 SIMの不正転売	SIMの不正転売の違法性について**周知啓発の推進**や事業者の**取組の強化**（与信強化等）
2 法人の代理権	法人契約担当者が当該法人に在籍しているかの**確認を強化** ⇒法制化を検討 [注2]
3 他社の本人確認結果への依拠	自社の他サービス/他社サービスの本人確認結果への依拠については、まずは、本人確認の厳格化の**取組の進展を見極めた**上で、本人確認の保証レベルの確保等、**依拠が適切にできる要件を整理**
4 追加回線	追加回線の契約時には、IDパスワードによる本人確認が認められていたところ、**多要素認証**（生体認証、ワンタイムパスワード等）**を求めるべく厳格化** ⇒省令改正を検討
5 上限契約台数	現在実施されている一定数以上の契約を拒否するという業界ルールの進展について**検証**を行い、必要に応じて、何らかの**ルール化について検討** ⇒ワーキンググループ（第11～12回不適正利用対策WG）にて、検討
6 データSIM	**義務化を検討**。ただし、対象SIMや利用用途等に関して、利便性と不正利用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 ⇒法制化を検討

[注１] このほか、特殊詐欺、闇バイト等対策関連についてもとりまとめている。
[注２] 報告書においては、省令見直しが必要である旨記載しているが、それを行うための環境整備として法改正も必要となる見込み。

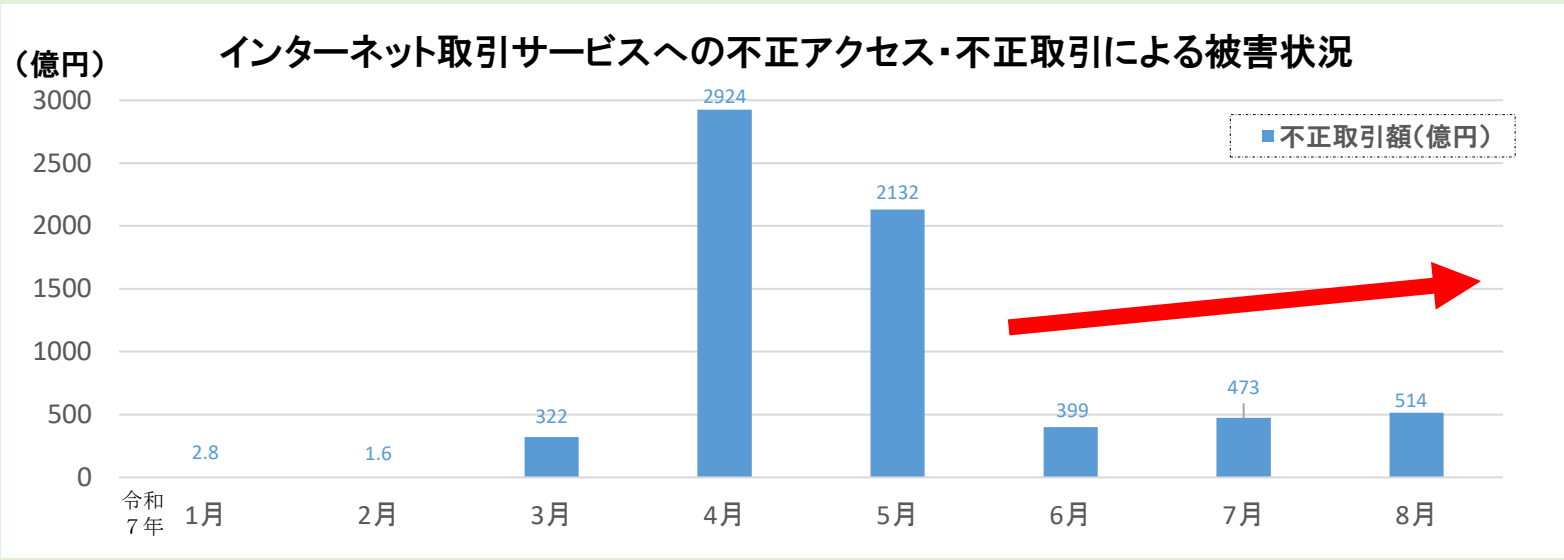
不適正利用の現状



特殊詐欺
965.3億円
✓ 電話での接触が全体の約8割

SNS型投資・ロマンス詐欺
1149.1億円
✓ SNSで募集し、LINEへ移行

出典：警察庁「特殊詐欺及びSNS型投資ロマンス詐欺の認知・検挙状況等（令和7年上半期・暫定値）について」（令和7年7月31日）



令和7年1月～8月の不正取引額
（不正売却金額・不正買付金額）

6,768億円

出典：金融庁「インターネット取引サービスでの不正アクセス・不正取引（第三者による取引）の被害状況」

9月以降の検討事項（第11～12回不適正利用対策WG）

9月報告書でとりまとめた内容		今回の検討事項
(1)携帯電話本人確認のルール	1 SIMの不正転売 2 法人の代理権(在籍確認) 3 他社の本人確認結果への依拠 4 追加回線 5 上限契約台数 6 データSIM	①上限契約台数についての中間検証・検討
(2)闇バイト、特殊詐欺等対策	1(1) 固定電話の対策 1(2) 携帯電話・SMS・メールの対策 2 既存番号へのスプーフィング（なりすまし） 3 海外電話番号による詐欺電話	②要請等を踏まえた、詐欺メール対策の対策

法制化に当たり検証が必要とされていた事項

報告書の記載:
・・・今後、少なくとも業界ルールの適用状況について検証を行い、更なる自主的な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はないか。

要請等のフォローアップが必要な事項

報告書の記載:
・・・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。

⇒フィッシングメールの被害急増を踏まえて、総務省より要請(9/1)・意見交換(9/22)を実施

通信事業者団体からのご発表

●（業界ルール）

- 自主基準については、現状、MNO4社の中では申合せもしており、今、自主基準に参加していないMNOはない。仮にお客様から5台を超える利用の要望があった場合、利用用途や事情等を個別に確認し、状況によっては例外的な運用も実施。（TCA）
- データSIMについては、現状、MNO4社、各社で定める契約台数を制限しており、自主的取組の在り方については、現在、TCAでも検討を行っている状況。（TCA）
- MVNO各社の上限回線数については、業界ルールはなく、家族構成の都合で6回線以上を希望する声を受けて、5台以上の上限契約台数を設定する事業者もある。（MVNO委員会）

構成員からのご質問

●対MVNO委員会

- 契約回線上限を5回線としている事業者は、柔軟な対応をして、6回線以上の契約を取っていることはあるのか。また、複数回線を契約する場合、契約者以外が使用する回線に対して、本人確認を実施しているか。（→例えば、6回線以上を上限としている事業者2社では、利用者登録は行っているが、利用者の本人確認は必ずしもできていない）
- MVNOが現在の上限台数の設定をするに当たって、システム上などの技術的な制約があるのか。（→15社中11社は、システムや卸元仕様が制約となり、個別対応不可。残り4社は、利用用途を確認するなどで個別対応可だが、実績はほぼない）
- 音声SIMとデータSIMで上限回線数の設定に差があるのはどのような理由か。（→データSIMは幅広い利用実態や利用シーンが多様であることが想定されるため）

構成員からのご意見

●(業界ルール他)

- 原則として5台の上限を設けつつ、お客様の事情を個別確認した上で例外的な契約を認めるという運用を実施している業界ルールは、バランスの取れた対応になっているのではないか。他方で、業界の自主基準が浸透し切っているかというと、必ずしもそうではないので、そこを後押ししていく必要はある。(第11回山根構成員)

- 「5」という数字の妥当性が明確に示せないのであれば、例えば「10」というような数字で、再度、その上限数設定を検討してはどうか。また、スミッシング等の攻撃があるので、SMSがありか、なしかで分けるというのは妥当であり、SMSなしデータを法人で使う場合においては、制限台数も設けないほうがいいのではないか。(第11回辻構成員)

- SMS付きSIMは、音声SIMと同様に、特殊詐欺などに使われるリスクがある一方、現状ではSMSなしデータSIMに関しては、そういったリスクがあるということは指摘されていない。当面、業界の事業者の自主ルールに任せるとしても、SMSなしデータSIMのルール化は、慎重なほうがいいのではないか。(第11回鎮目構成員)

- 業界のルールが進展しているということであれば、法律で一律に規律するよりも機動性が保てるという観点において、業界ルールで進めていただく形がよいと思う。また、数については、契約者管理などで利用者の本人確認をすることも考えられる。(第12回辻構成員)

構成員からのご意見

●(役務提供拒否について)

- 多数台契約について、事情があれば契約締結を拒むことができることを定めるという手法は考えられる。一方で、危険性は認められない多数台契約が排除されないようにする観点から、その規定の仕方については要検討。(第11回中原構成員)
- 役務提供拒否との関係を明確化するというところは一つあり得るアプローチである。(第11回山根構成員)
- 正当な理由があるのであれば原則以上の台数を認めるという形にしつつ、実際、代理店で判断できないものについては本社で対応するという形などが望ましいのではないか。(第11回星構成員)
- 法律上の規制事項とした上で、省令等により具体的に定めるという手法も十分に考えられるところであり、電気通信事業法121条等の解釈指針として示すよりも、文脈適合的で安定的な規律が望めるというメリットがあろうかと思う。(第12回中原構成員)
- 考え方案に賛同。今後、ある一定台数の基準を示すことになったときに、基準の数よりも台数の上限を低めに設定する事業者も見込まれるところ、電気通信事業法の121条1項の役務の提供義務との関係についても併せて整理していく必要がある。(第12回山根構成員)
- 利用形態は様々なケースがあり得ると思うので、上限台数を一律に決めるのではなくて、あくまで利用目的とかSIMの種別などの個別事情に応じて、事業者が提供可否を判断できるようにルールを明確化するという形で後押しするという考え方案に賛成したい。(第12回沢田構成員)

構成員からのご意見

●(運用上の対応その他の方策)

- 多数回線の契約のハードルを少し上げる手段として、利用者にやってほしくないことを規約に明記して注意喚起することや誓約書へのサインも選択肢ではないか。(第11回沢田構成員)
- 契約者の本人確認のみを行い、その方の名義で複数台契約をした場合に、上限が場合によっては適用されていない領域があるとすると、そこに潜む危険に対して十分に対応ができていなかったのではないか。今後、十分に整理しながら、実態を踏まえて検討していく必要がある。(第11回大谷主査)
- 契約時の対応の強化について、利用者が安易に犯罪に手を貸さないようにするという意味で、事業者にまだもう少し御協力いただけることがあるのではないのかと思っており、考え方案に賛成。(第12回沢田構成員)

今後の方向性(案)

⇒　上限契約台数の制限については、業界ルールの進展が一定程度図られたことが認められるものの、今後、多くの事業者への更なる浸透を図るとともに、利用者視点から一定の予見可能性の確保が望ましいこと等を考えると、総務省として制度面から事業者の自主的な取組を後押しする環境を整備する必要があるのではないか。

例えば、一定台数を超える契約を利用者が求めた場合に、利用目的やSIMの種別を踏まえ、事業者として提供拒否ができることについて、法令上の措置を含め、明確化の観点からルール化すること等、所要の環境整備を迅速に進めていくことが適当ではないか。

⇒　総務省において、上記ルール化等を通じて事業者の更なる自主的な取組を促進するとともに、事業者において、不正契約を防止するための契約時の対応強化に一層取り組むべきではないか。また、取組状況を受けて必要になる場合には、犯罪との因果関係を踏まえながら、名義人が契約したSIMの実際の使用者を把握する方法を含めた検討や、一層のルール化を含む対策の強化(例:一律の上限契約台数制限)についても検討すべきではないか。

【今回の検討事項②フィッシングメール対策】第12回不適正利用対策WGにおける報告（1）

○　フィッシングメール被害の急増を踏まえて、総務省から4通信事業者団体に対して、生成AIを用い、自然な日本語を大量に生成できるようになり、これまで以上に精巧なフィッシングメールの送付が容易となっている中、こうしたフィッシングメールへの更なる対策が求められるところ、総務省より事業者へ要請（9/1）、意見交換（9/22）を実施。

9/1要請の内容

（1）フィルタリングの判定技術の向上や迷惑メール判定における AI の活用等、メールのフィルタリングの精度の一層の向上を積極的に図ること。また、迷惑メールのフィルタリング強度を適切に設定するなどして、高度化するフィッシングメールに対応可能なメールフィルタリングを目指すこと。

（2）なりすましメール対策として有効な DMARCの導入やDMARC ポリシーの設定（隔離、拒否）を行うこと。送信側だけでなく受信側についても、適切なDMARC ポリシーに基づく処理やレポート送信を設定すること。また、ドメインレピュテーション、BIMI、踏み台送信対策等の更なる対策の導入を積極的に検討していくこと。

（3）提供しているフィッシングメール対策サービスについて、様々な利用者層に向けた一層の周知・啓発を行うこと。

プルーフポイントからのご発表

●2024年末から大規模なDDoS攻撃が国内企業・団体に集中（金融、航空、通信など）。

●全世界の新種のメール脅威も急激に増加。全世界のメール攻撃のうち80%が日本をターゲットにしている（※プルーフポイント調べ）。フィッシング攻撃には日本を標的にした高度なフィッシングキットが使用される。

- 2023年 4.3% → 2024年 21.0% → 2025年 83.3%

●メール詐欺には、ユーザーになりすましてメール送信するものと、実際にユーザーのアカウントでなり代わってメール送信する2種類がある。このうち、前者に関しては、DMARC及びBIMIで対応が可能。一方、日経225企業でも、DMARCの隔離・拒否まで行っているのは20%と課題。

携帯通信事業者からのご発表

●要請（1）

4社共通で、フィルタリング精度のさらなる向上を現在検討中。

●要請（2）

4社の主要メールサービスではDMARCを導入済み。BIMIに関しては、一部未導入な事業者も。

●要請（3）

4社共通で、HP等にてフィッシング詐欺に関する注意喚起を実施。また、フィルタリングサービス未設定の利用者への注意喚起や適切なフィルタリング強度設定を推奨する事業者もあり。

【今回の検討事項②フィッシングメール対策】第12回不適正利用対策WGにおける報告（3）

構成員からのご意見

●各キャリアにおいてフィッシングメール対策の強化を着実に行っているということで、大変心強い限り。現在、事業者の皆様においてやっている対策の強化が、件数を実際に押し下げる方向に働くのかどうかということを今後注視していく必要がある。いたちごっことなるので、着実に手を打ちつつ、さらに先回りした対応を引き続き考えていく必要がある。（第12回鎮目構成員）

●日本スマートフォンセキュリティ協会としても、フィッシングメールの増加と攻撃傾向の変化については注視している。DMARCやDKIM、BIMIといったメール送信者・メールサービス提供者・受信者が一体となった取り組みによりメールの信頼性確保への取り組みが行われることが望ましく、キャリア各社の努力についてもご発表いただき感謝している。フィッシングメール・スパムメール排除については、真に受信者に届くべきメールを遮断してしまう「誤遮断」の課題が常に存在するが、メールの健全性確保のため不正メール排除の取り組みについての周知も重要と考える。（第12回事後 仲上構成員）

今後の方向性（案）

以上を踏まえ、事業者において、フィルタリング精度の精緻化やDMARCのポリシーの強化等の取組を進めていただく予定。