消費者委員会本会議（第466回）
議事録

内閣府消費者委員会事務局

消費者委員会本会議（第466回） 議事次第

1. 日時 令和7年7月15日（火） 10時00分～11時40分
2. 場所 消費者委員会会議室及びテレビ会議
3. 出席者

（委員）

【会議室】 鹿野委員長、黒木委員長代理

【テレビ会議】 今村委員、大澤委員、小野委員、柿沼委員、山本委員、

（説明者）

内閣官房副長官補付 榊野内閣参事官

警察庁刑事局組織犯罪対策部組織犯罪対策第二課 塩谷課長補佐

警察庁サイバー警察局サイバー企画課サイバー事案防止対策室

岡嶋課長補佐

経済産業省商務情報政策局情報経済課デジタル取引環境整備室

渡辺室長補佐

経済産業省商務・サービスグループ商取引・消費経済政策課 堀川課長補佐

経済産業省商務・サービスグループ文化創造産業課 中村課長補佐

金融庁総合政策局リスク分析総括課金融犯罪対策室 神谷課長補佐

総務省総合通信基盤局電気通信事業部利用環境課 田中課長補佐

総務省情報流通行政局情報流通振興課情報流通適正化推進室

武田課長補佐

総務省情報流通行政局参事官室 田熊参事官補佐

法務省大臣官房秘書課 満田課付

法務省刑事局公安課 長谷川局付

法務省刑事局総務課 佐藤局付

（事務局）

小林事務局長、吉田審議官、友行参事官

4. 議事

(1)開 会

(2)「国民を詐欺から守るための総合対策2.0」等について

(3)閉 会

《1. 開会》

○鹿野委員長 皆様、おはようございます。本日は、お忙しいところ、お集まりいただき、ありがとうございます。

ただいまから、第466回「消費者委員会本会議」を開催いたします。

本日は、黒木委員長代理と、私、鹿野が会議室にて出席しており、今村委員、大澤委員、小野委員、柿沼委員、山本委員がテレビ会議システムにて御出席です。

なお、中田委員、原田委員、星野委員は、本日所用のため、御欠席と伺っております。

それでは、本日の会議の進め方等について、事務局より御説明をお願いします。

○友行参事官 本日もテレビ会議システムを活用して進行いたします。

配付資料は、議事次第に記載のとおりでございます。もしお手元の資料に不足等がございましたら、事務局までお申し出いただきますようお願いいたします。

以上です。

○鹿野委員長 ありがとうございます。

《2. 「国民を詐欺から守るための総合対策2.0」等について》

○鹿野委員長 本日最初の議題は『「国民を詐欺から守るための総合対策2.0」等について』でございます。

SNSやマッチングアプリを通じたやり取りで相手方を信用させ、投資等の名目で金銭をだまし取るSNS型投資詐欺、ロマンス詐欺が急増していることを受けて、令和6年6月に政府において「国民を詐欺から守るための総合対策」が策定されました。

当委員会では、この総合対策について本会議でヒアリングを行った上で、令和6年9月に取りまとめた「次期消費者基本計画策定に向けた消費者委員会意見」において、この総合対策の施策に着実に取り組むべきであると指摘してきたところでございます。

しかし、総合対策に基づく官民の対策が進められる一方で、犯人側は手口を巧妙に変化させており、令和6年中のSNS型投資詐欺、ロマンス詐欺の被害額は、前年の約3倍に増加しております。

こうした状況を踏まえて、政府においては、詐欺対策を抜本的に強化するため、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を統合するという形で、本年4月に、従来の総合対策を「国民を詐欺から守るための総合対策2.0」へと改定されたと伺っているところです。

そこで、本日は内閣官房より、令和6年に策定された総合対策の取組状況及び今般改定された総合対策2.0の内容を御説明いただくとともに、詐欺等に対する行政機関の対応など

について、関係省庁との意見交換を行いたいと思います。

改めて、本日の御出席者について紹介させていただきます。

本日は、内閣官房副長官補付の梶野内閣参事官に会議室にて御出席いただいております。

また、質疑対応として、警察庁刑事局組織犯罪対策部組織犯罪対策第二課の塩谷課長補佐、警察庁サイバー警察局サイバー企画課サイバー事案防止対策室の岡嶋課長補佐、経済産業省商務情報政策局情報経済課デジタル取引環境整備室の渡辺室長補佐、経済産業省商務・サービスグループ商取引・消費経済政策課の堀川課長補佐、そして、経済産業省商務・サービスグループ文化創造産業課の中村課長補佐に会議室にて御出席いただいております。

また、金融庁総合政策局リスク分析総括課金融犯罪対策室の神谷課長補佐、総務省総合通信基盤局電気通信事業部利用環境課の田中課長補佐、総務省情報流通行政局情報流通振興課情報流通適正化推進室の武田課長補佐、総務省情報流通行政局参事官室の田熊参事官補佐、法務省大臣官房秘書課の満田課付、法務省刑事局公安課の長谷川局付、法務省刑事局総務課の佐藤局付にオンラインにて御出席いただいております。多くの皆様に御出席いただきまして、ありがとうございます。

それでは、今から内閣官房副長官補付、梶野内閣参事官に約20分程度で御説明をお願いいたします。よろしく申し上げます。

○内閣官房副長官補付梶野内閣参事官 ただいま御紹介に預かりました、内閣官房副長官補室で参事官をしております、梶野と申します。本日はよろしく願います。着座にて失礼いたします。

それでは、資料が画面に共有されているかと思えますけれども、資料に沿って御説明させていただきますと思います。

先ほど委員長から既に御説明していただきましたけれども、政府といたしましては、近年、特にSNSやキャッシュレス決済の普及が進む、インターネットの進展も含めてですけれども、そういった中で、特に財産犯の中での詐欺の被害が加速度的に拡大する状況を憂慮してございまして、それで昨年、こちらでも御説明させていただいたと承知しておりますけれども、令和6年の6月に、「国民を詐欺から守るための総合対策」、無印といいますか、それを策定したところでございました。

政府といたしましては、その総合対策に基づいて対策を講じてきたところではありますけれども、今、御覧いただいている資料の棒グラフが左側にありますが、財産犯の被害額の推移を御覧いただきたいのですけれども、オレンジが窃盗で、青が詐欺、財産犯、国民のお金が奪われる犯罪ですけれども、これが、ただでさえ令和5年の段階で増えてきて、対策を取りまとめたところですが、令和6年が異常なぐらいに伸びてしまっているという状況にありまして、これは平成元年以来最も高かった平成14年当時の被害を上回る額になっておりますけれども、特にその中の構成です。

平成14年のときはオレンジが多かったので、いわゆる窃盗が多くを占めていた状況下にありましたが、同じ額でも令和6年の青が非常に伸びている。すなわち、詐欺の額が伸びて

いるということで、財産犯の構造そのものに変化があったという認識でございます。

では、その詐欺の中でどういったものが問題かというのが、特に右側の棒グラフのほうにいていただきたいのですけれども、令和5年から令和6年の間に特に伸びているのは、やはりSNS型の投資・ロマンス詐欺ですとか、特殊詐欺、特にSNS型投資・ロマンス詐欺が激増しているということでございます。

皆様におかれましては、御案内かもしれませんが、典型的な例として、SNS型の投資詐欺というのは、SNSで、例えば、まずは詐欺を匂わせるわけではなくて、友人関係とか、知り合いとかになった中で、仲よくなって、こういう投資があるよと言ってお金を引っ張って、そのままどろんするという犯罪が典型的でございますし、ロマンス詐欺というのもそうです。初めにお金のお話をするわけではなくて、恋愛感情を匂わせて仲よくなって、大体私のイメージですと、海外とか遠距離に在住しているという設定で、あなたのところに会いに行くには、お金が必要だとか、あなたと結婚するためには、自分の借金を返さなくてはいけない、親が病気だからお金が必要だと、恋愛感情につけ込んで多額の金銭を振り込ませるなりして、どろんするという詐欺が典型だと承知しております。

そういった犯罪が激増している中で、なかなか恐縮ではございますけれども、総合対策1.0といいますか、昨年御説明させていただきました総合対策だけでは足りないのではないかとというのが、政府側の認識でございます。この間、各政党から提言とかもいただいた中で、政府として令和7年の4月22日の犯罪対策閣僚会議におきまして「国民を詐欺から守るための総合対策2.0」というものを取りまとめさせていただいたということでございます。

今申し上げたように、この投資・ロマンス詐欺の激増に対応しているということではございますけれども、1枚目の資料の下の「総合対策の改定」という字の箱がでございます。

その2番目の○なのですけれども、詐欺に限らず、実は覚えていらっしゃるかわかりませんが、昨年未だ、いわゆる闇バイト強盗という事件が頻発しておりました。これは、SNSで犯罪者の上層グループが実行犯という実際に強盗に入る人を募集して、お金を持っている一戸建ての老人の宅に入らせて、監禁したりとかをして現金を奪うということで、結果的に殺害事件まで発展するような事件があって、社会的に大きな反響を呼んだので、当時12月に、これも犯罪対策閣僚会議でございましたけれども、闇バイトによる強盗事件から国民の生命・財産を守るための緊急対策というものを、緊急ではございましたが取りまとめていっておりました。

ですので、この闇バイトに対する対策と今回の投資・ロマンス詐欺の対策を併せて「国民を詐欺から守るための総合対策2.0」に盛り込んで、全てを統合して今回の4月に取りまとめということなので、大きくその2つの内容が入っているということになってございます。

経緯としては、以上でありますけれども、次の2.0の内容について御説明したいと思っております。

オンラインの方ですと、見づらくて恐縮ではございますけれども、今、御覧いただいているのは「『国民を詐欺から守るための総合対策2.0』における主な施策」ということでございますが、先ほど申し上げたように今回の2.0は、1.0からのアップデートに加えまして、全体の構成を見直しているということではあるのですけれども、今、御覧いただいているパワーポイントに書いてあるものは、およそ1.0には書かれていないもの、2.0において新規の施策ということで書かれているものがほとんどです。

本日は、それに沿って御説明をさせていただきたいと思っておりますけれども、それも大部にわたりますので、その中で主立ったものを私のほうから御説明差し上げたいと思っております。

まず、根本的にSNS型の投資・ロマンス詐欺に対応するという意味で大事になってくるのは、やはり金融と通信の2本の柱でございます。もちろんお金の話なので、金融関係の施策は必要だし、大体SNSと名がつくように、SNSを使っている以上は、通信にも何らかの規制というわけではないのですけれども、対策が必要だということなので、大きく通信と金融、この2本と、あとは捜査の中で何ができるのかという話を、今回の2.0に盛り込んでいるというのが、全体を貫く哲学でございます。

その上で、まず、SNS型投資・ロマンス詐欺対策として、1の大きな箱の中に(1)から(5)までございますけれども、細かいものもございまして、まず、こういった対策を今回打っていくかということですが、(1)の1つ目の○です。

携帯電話を使う、スマートフォンを使って犯罪をするというのは当たり前なのですが、携帯電話不正利用防止法上ですが、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、携帯電話事業者、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かけるとともに、契約時の本人確認の義務付けを含めて検討するということです。

これは、今まで音声通話ができる携帯電話というのは、当然、契約における本人確認が義務付けられているものですので、もし、それが転売されてしまえば、なかなか難しいのですけれども、そこをたどっていくことは一応可能ではあったのです。ただ、データ通信専用SIMというのは、やっていただいている業者さんもいたのですけれども、必ずしも義務付けられているというわけではなかった。それは音声通話がないからという考えもあったのですけれども、今、アプリだけでも全然通話とかができてしまうので、それに差異があまりないのではないかという中で、こういったものが悪用されている実態が、なきにしもあらずではないかということで、こういった対策を考えているということでございます。

続きまして(2)にまいります。すみません、順番が前後しますけれども、今回の構成を見直したのは、犯行の段階のフェーズごとに対策を並べておりまして、まず、準備段階、着手段階、そして、実行段階、それで被害が起こった後という並びになっていますが、犯罪の時系列に沿って対策が並んでいると理解をしていただければ結構かと思っております。

「(2) 着手段階への対策」でございますけれども、このうちの2つ目の○でございます。いわゆる国際電話サービスに関してですが、皆様もお使いになっいらっしゃる方はいら

っしゃるかもしれませんが、国内の高齢者向けの犯罪の電話と申しますか、連絡というのは、国際電話を使用するケースが結構あるという警察当局からの話がございます、それをどうにかできないかという話ですけれども、必ずしも高齢者の方が国際電話を日常的に使わないケースもあるのではないかという前提に立ちまして、国際電話は、一応、電話会社さんに連絡すれば利用しない設定にすることができます。オフにできるのですね。そういった設定があることを必ずしも周知されていないのではないかという問題意識の中で、一層強く国民に周知するというのを対策としてやっていくことに加えまして、将来的に国際電話サービスを利用しない方に対して何らかのインセンティブ、優遇措置みたいなのができないか、電話を必要としない人の利用休止を促すような効果的な対策がどういふものがあるのかということを考えていこうということでございます。

次の○ですけれども、迷惑電話、迷惑SMS、皆さんも携帯電話をお持ちであれば、たまに何か謎のメールが来たりするケースがあるかもしれませんが、そういったものを受信した際に、それをフィルタリングと申しますか、ブロックするような措置ですとか、受信した際に何らかの、これは危ないですよという警告をしたりというサービスが、各携帯電話会社さんでやっていたところがございます。

それは、サービスによっては有料だったりするものですから、そういった事業者の方に対して、こういった詐欺が蔓延している状況の中で、その無償化を含めた効果的な措置というのが何かできないかということをお相談させていただくとともに、被害防止機能向上のために、より効果的な方策があれば、そういったものを検討していくべきではないかということをお願いしていただいております。

続きまして(3)を飛ばしまして(4)、こちらは金融関係です。金銭、実際にだまされてしまった人がお金を犯人側に渡す段階のお話ですけれども、1つ目の○、インターネットバンキングの初期利用限度額の適切な設定や、申込みがあった際、利用限度額引上げ時の確認。

SNS型投資・ロマンス詐欺の被害が、これだけ伸びた1つの原因としては、インターネットバンキングを利用した振込というのは、必ずしも限度額が、一般の普通の生のATMと比べると、少し高い金額が場合によっては設定できてしまう、1回の振込みで1,000万とかがいけてしまうという状況がある。それは、もちろん、法人さんとしては必要な可能性もあるのですけれども、個人として必ずしも必要かどうか分からない以上、そういった適切な限度額の設定というのができますよということを、できる限り広報啓発しながら、仮に残念ながら被害に遭うことがあったとしても、それを最小限に食い止めるには、こういう設定が必要なのではないかということの取組を推進していこうということでございます。

金融関係が続きますけれども、3つ目の○ですが、預金取扱金融機関において不正利用口座に係る情報を共有しつつ、速やかに口座凍結を行うことが可能となる枠組みについて検討ということでございますけれども、これは、いわゆる銀行のことですが、各金融機関さん、銀行さんは、現在でも非常に取組を進めていただいているのですけれども、それぞれ

特定のA銀行の中で疑わしい口座とか、疑わしい取引があれば、そのA銀行の全国のネットワークの中で、これは怪しいという共有は既にやっていたところがございます。

ただ、それがA銀行の中で完結している現状の中で、B銀行、C銀行との共有が必ずしもできていなかった。そうすると、犯人側が口座をA銀行からB銀行、B銀行からC銀行に移すのに、それぞれの銀行に、また警察から照会が行くとタイムラグが発生するので、A、B、C全ての預金取扱金融機関、銀行の中でのネットワークを一元的に構築できないか、そうすれば、スピーディーに疑わしい情報が共有されることによって、各銀行の怪しい人の名義の口座について凍結なりがスピーディーにできるのではないかという問題意識でございます。

こちらも全銀協さんも含めて、取組を進めていただいているところと承知してございますけれども、今回の2.0に盛り込んでおりますので、その対策を進めていきたいと考えてございます。

続きまして、4つ目の○、これは、捜査手法の関係でございますけれども、捜査機関を管理する架空名義口座を利用した新たな捜査手法や法令の改正を検討するというので、報道でも取り上げていただきましたけれども、必ず、基本的には、詐欺を使うという犯罪のときには口座を使います。

それは、どういう口座を使うかということ、他人名義の口座ですとか、例えば、誰かに口座をつくってもらって、それを買い取って、要するに犯人グループは、自分の名義だと自分の身柄が割れてしまいますので、ほかの人の口座を使って、それを幾つか経由して、最終的に自分のところにローンダリングしてたどり着かせるというのが一般的ではありませんけれども、その中で、警察が架空口座みたいなものをつくって、そういったアンダーグラウンドのマーケットか何かに流し込んでしまえば、もし、その口座に引っかければ、その警察の口座、もちろん警察の口座とは言わないわけですが、その口座から流れている金の流れがリアルタイムで分かるので、犯人グループに近づけるというメリットもございまして、ある意味、インセンティブというか、抑止的な効果として、警察の口座が口座のマーケットみたいなところにあり得るのではないかとということになると、犯人側グループも、おいそれと、なかなか口座を簡単に買い取って使うというのが困難になる可能性もあるのではないかとということで、こういった取組を進めていこうということでございますけれども、これについては、関係法令の改正が必要となり得るということですので、今回の2.0に盛り込んでおりますけれども、捜査当局、金融当局の中で検討が進められて、実現に向けて検討を進めていただきたいと考えてございます。

続きまして(5)、これは犯行が行われてしまった後に、犯人をどうやって捕まえていくかという話でありますけれども、こちらは通信のほうに戻りますが、やはり使われている通信系のアプリは、匿名性が高い通信アプリということでございまして、外国で使われているような履歴が残らないというアプリが多いやに承知してございます。

そういった犯罪に悪用されるアプリについて、どういった通信内容を捜査当局が得られるのか、さらには登録者情報を、もし、会社が持っているのであれば、それを捜査に役立てられるのかということについて、まだまだ日本としては取組が不十分な部分があるのではないかと思いますので、諸外国における取組をちゃんと参考にしながら、どういった技術的アプローチ、いわゆる警察から、ハッキングではないですけども、アプローチができるのかということですか、そのためには、どういった法制度が必要なのかということの可能性も含めて検討していただくということでございます。

2つ目の○は、秘匿性が高いアプリに限らず、普通の携帯電話のメールでも構わないのですけれども、犯人が犯行を行った場合には、本来は、必ず記録が残ります。でも、それが一定期間を経過すると、やはり携帯電話会社さんも含めて、メールとか通信の履歴というのは、順次消されていくのが一般的ではございます。

でも、やはり警察からすると、半年前、1年前の犯行ですと被害届を出されても、記録が残っていないと何の話でしたかという話にもなりますし、捜査がなかなか困難を極めるということですので、その通信履歴と、いわゆるログの保存と呼ばれておりますけれども、その在り方について、捜査に必要な範囲内で、このガイドライン改正、保存の義務付けを含め検討というのは、いわゆる今の保存期間をなるべく延ばせないか、どこまで延ばせないかという話を進めていきたいということでございます。

次の○は、投資・ロマンスと書いてありますけれども、これは闇バイトの対策でやったものなのですけれども、仮想身分捜査というのは、報道で出ましたけれども、令和7年の1月に制定した実施要領に基づいて、犯人の検挙を推進ということで、これは、報道で既に仮装身分捜査を実施して、犯人の検挙に至ったということもあると承知してございますけれども、いわゆる、警察官が警察官であることを隠して、犯人が、こんな高額報酬、闇バイトを募集しているよということに応募して、そこから、その現場に行って一網打尽にするというのが理想的なケースでございますけれども、そういうようなことを仮装身分捜査と言っております。つまり、警察官が自分の身分を秘匿する、警察官ではないですよと言って、犯人側に接触するということですが、これは、基本的に特段の法改正は不要という判断で、刑法上の正当行為として違法性が阻却されるだろうということで、実施要領のレベルで行けるだろうということでやって、実際、今は進んでいるということでございます。

大きく言うと、次の3番のID・パスワードとかの不正利用対策というのは、(1)にありますけれども、これは1.0でもございましたけれども、フィッシングサイトとかを判定するために、生成AIを活用した取組というのは、全世界的に進んでおりますので、それは、引き続きやっていただきたいと、政府としても考えておりますので、そういった対策を推進するということでございます。

あと、時間もあれですので、4番の治安基盤の強化というところにまいります。

以上のような対策をやっていく中で、1つ目の○ですけれども、かなりアナログではあり

ますが、やはりそういった対策を打つ中でも、警察の体制を強化していかなくてはいけないというのは、引き続き必要だと考えておりますので、首謀者検挙、警察・検察におけるサイバー人材の更なる育成ですとか、体制の強化というのは、地道でございますけれども、継続的にやっていかなければいけないということでございますので、更なる増強を図るよう警察をお願いしているところでございます。

少し毛色が変わりますけれども、4つ目の○でございますが、特殊詐欺にも生かせると思っておりますが、この地方創生の交付金を活用した防犯カメラの設置等、防犯力の強化に資する取組の支援を行うということですが、やはり全世界的に見ても、日本でもそうですけれども、防犯カメラの犯罪捜査の果たす役割というのは、非常に大きいものになってございます。

という中で、必ずしも全てのエリアにまだあるわけではないですけれども、その防犯カメラがなかったことによって、闇バイトの犯人がなかなか捕まらないようなこともあったので、地域のこういった交付金で防犯カメラを使っていいよということで、政府的に後押しすることによって、可能な限り犯罪の抑止に資するような防犯カメラの設置を全国的に進めていただければいいなと思っております。特に振り込め詐欺とかの場合には、実際、今、そういったアナログのものがあるかどうか、私は分かりませんが、受け取りに来るような場合には、防犯カメラがあれば、そこから犯人を追跡することも可能だと考えております。

雑駁ではございますけれども、以上のような対策を2.0に盛り込んでおまして、この4月の22日に犯罪対策閣僚会議で決定したものですから、今、まさに各種検討が進められているものもあれば、既に実行しているものもありますけれども、引き続き、政府としては対策に取り組んでまいりまして、少なくとも高止まりしている詐欺の状況が、1年、2年の範疇の中で改善していくように、引き続き取り組んでいきたいと考えております。

資料としては、フォローアップといいますか、1.0の取組もありますけれども、そういったものも着実に進めているということでございますので、もし御質問があれば、いただければと思います。

私としては以上でございます。ありがとうございました。

○鹿野委員長 御説明ありがとうございました。

それでは、これより、質疑応答と意見交換を行いたいと思います。時間は60分程度を予定しております。いかがでしょうか。

柿沼委員、お願いします。

○柿沼委員 柿沼です。よろしくお願いいたします。何点か質問とコメントをさせていただきます。

まず、フィッシング詐欺についてなのですが、近年、企業、公的機関を装ったフィッシング詐欺が増加しております。2024年の月間報告件数が18万件を超えるなど、消費者被害が深刻化しています。

特に、なりすましメールによる個人情報への窃取や金銭的被害が多発しており、消費者からの相談が消費生活センターにも多く寄せられているという状況です。

対策として、DMARCが挙げられるかと思うのですが、日本のJPドメイン全体での導入率が30%にとどまっているという状況、また、特に中小企業や地方自治体では導入が遅れている状況ということですが、外国は導入率が70%から100%ということで、なぜ日本がこれだけ遅れているのか、また、DMARCの導入促進について対策を講じているということがあれば、具体的に教えていただきたいと思います。

それから、2点目です。SNSの投資被害です。投資のレクチャー費用がかかるが、すぐに元が取れるからと言って、クレジットのキャッシングや消費者金融から借りさせる手口が横行しています。消費者契約ですと、カードのキャッシングの借入額は、貸金業法の総量規制で決められていますが、データベースの反映が1日ぐらい遅れるということで、総量規制を超えた額を借りられてしまうという被害が寄せられており、結局債務整理を余儀なくされるという状況に陥っています。金銭的な喪失にとどまらず、家族関係にも深刻な影響が及んでいるという状況があります。家庭の崩壊に至っている状況ということもあります。このデータベースの反映が遅れるということの対策を講じることは難しいのでしょうか、こちらについて、結局は、お金が詐欺的な人たちに渡ってしまっているということですから、なるべく借入額を少なくするための対策を講じることは難しいのか、今、データベースの反映については、リアルタイムで行うことが可能なのではないかと私は思っておりますので、その辺りについても何か、今、手だてをなさっているということであれば、お伺いしたいと思います。

それから、3点目です。ネット通販の詐欺です。今回は、どちらかというところ、SNSの投資被害やロマンス詐欺などの金額が高額なものについての詐欺の対策ということですが、例えば、SNSや動画共有サイトの広告を見て注文したところ、表示とは全く違うもの、それから表示の性能が劣るもの、こういうものの相談が、今、大変多く消費生活センターに寄せられているところだと思います。

それで、返品したいけれども連絡が取れないとか、あとは、最近多いのが代引きで届くことが多く、代引きを代行する会社に電話をしても全然つながらないという状況です。こちらについてですが、詐欺的な商法で海外にお金が行っているという状況です。広告を表示するプラットフォーム事業者や、あとは宅配会社、こちらにも責任があると感じておりますが、こちらについて何らかの対応をされていますでしょうか。さらにPIO-NETのデータを見ていただくと、この手の相談が多く寄せられているのは、もう明白です。金額が少ないため諦めてしまう消費者もいますが、金額が少ない詐欺事案についても、当然国民を詐欺から守るという対策の中に入っているかと思っておりますので、このような詐欺事案についても目を向けていただきたいのと、何か対応を取られているということであれば、教えていただきたいと思います。

特に、広告を掲載しているデジタルプラットフォーム事業者と宅配会社について、何ら

かの対応をされているのか、そちらについてお聞きしたいと思います。

それから、4点目です。迷惑電話相談センターが開設されました。相談をした場合、どのような対応が受けられるのでしょうか、対処方法の案内だけなのか、必要に応じて関係機関との連携などの支援をしていただけるのか、こちらについてもお伺いしたいところでございます。

また、詐欺のアジトが海外にあるということで、電話をかけるのも国際電話を通じてということで、国際電話不取扱受付センターにて電話を止めるのも一法であると、消費生活センターから御案内をします。ただ、不取扱受付窓口では、国際電話からの電話全てを一括でブロックするとお伺いしていますので、海外に家族がいるとなると止められないという方もいらっしゃいます。例えば、アメリカだけは電話を通じるようにするとか、そういう手だてを取ることができないのかということをお伺いしたいと思います。

すみません、長くなりますが、次の点についてです。消費者金融からお金を借りる方法を遠隔操作で教えると言われて、リモート操作をしたことをきっかけに、不正利用されたという相談が寄せられています。金融機関のサイトは、遠隔操作した人からは、見えないようにするなどの工夫を講じることはできないのでしょうか、こちらについてもお伺いしたいと思います。

最後なのですが、要望ですが、投資被害とか、ロマンス詐欺に家族が陥っているということを、家族が、そのような問題に気づき、本人にやめるように言っても、なかなか止めさせることができず、対応に苦慮しているというケースが多く見受けられます。

このような場合、どうすればよいかと、切実な相談が消費生活センターに寄せられています。家族の話も聞き入れられないような、そういう人に対して、専門的な支援が受けられるような、そういう窓口の設置を強く望みます。私が知らないだけなのかもしれませんが、もしもあれば、そういう設置する窓口についても、広く国民に対して、こういう相談窓口がありますよという御案内をしていただきたいのと、もしもない場合には、そういう窓口の設置を強く望むところです。

すみません、質問とコメントがありますけれども、お答えいただければと思います。よろしく願いいたします。

○鹿野委員長 質問と御意見をいただきましたが、これは、梶野参事官からですか。

○内閣官房副長官補付梶野内閣参事官 いいえ、担当省庁から全て。

○鹿野委員長 そうですか、それでは、まず、フィッシング詐欺については、岡嶋課長補佐からお願いします。

○警察庁サイバー警察局サイバー企画課サイバー事案防止対策室岡嶋課長補佐 サイバー企画課の岡嶋と申します。御質問ありがとうございます。

委員御指摘のとおり、フィッシングメールにつきまして、昨年約172万件ということで、右肩上がりの数字が続いております。

その他、クレジットカードの不正利用につながるような個人情報の窃取や、インターネ

ットバンキングの不正送金事案についても非常に高止まりというのが現状でございます。

また、委員から言及をしていただきましたようにDMARC、こちらの促進というのは警察庁も取り組んでいるところでございますが、中小企業等が非常に多いという日本の特性もございまして、なかなかその普及率というのが上がっていないというのも御指摘のとおりでございます。

ただ、やはりDMARCの普及というのが、このフィッシングメールを防ぐためには、まず第一と考えております。警察庁といたしましては、都道府県警察ともしっかり連携をして、より中小企業にも届くように、DMARCの促進を引き続き徹底していきたいと思っております。

また、DMARCを導入していただいた際、不正なメールへの対応方法を定める3つ設定がございまして、いわゆるnoneという何もしないというものと、quarantineという、フィッシングメールが来たら迷惑メールフォルダに送るというものと、rejectということで完全に不正なメールを拒否してしまうという3つの設定がございまして。

事業者においてDMARC技術を導入しても、その設定がnoneのままでは結局フィッシングメールが届いてしまうということもございまして、引き続きnoneではなく、quarantineであったり、rejectという形で、フィッシングメールが顧客のお手元に届かないように設定をしていただくように、事業者の方へのフォローアップというの、引き続きやっていきたいと思っております。

以上でございます。

○鹿野委員長 それでは、2番目の御質問について、消費者金融でデータベースへの反映が遅れることによって、総量規制の、言わばくぐり抜けが見られるのではないかとこの点だったかと思いますが、それは、どなたにお答えいただいたらよろしいですか。

金融庁様からお答えいただけますか。

本日、金融庁から神谷課長補佐にオンラインで御参加いただいていると思っておりますが、神谷様、お答え可能でしょうか。

○金融庁総合政策局リスク分析総括課金融犯罪対策室神谷課長補佐 金融庁です。貸付けの総量規制をシステム上の問題で超過できてしまっているという点については、我々も認識しておりまして、関係者ともどういった対応ができるのかということについても、相談をしていきたいと思っております。

○鹿野委員長 それでは、後でまた柿沼委員から補足で質問があれば言っていただくということにして、3点目がネット通販詐欺についてだったと思っております。これについての対応、特に通販業者だけではなくて、このネット通販詐欺に至るまでに関わるような事業者も含めて、何らかの対策が講じられているのかという御質問だったように伺いましたが、これは、どなたにお答えをいただきますか。

それでは、岡嶋課長補佐、お願いします。

○警察庁サイバー警察局サイバー企画課サイバー事案防止対策室岡嶋課長補佐 サイバー

企画課の岡嶋でございます。

委員から御質問をいただきました、詐欺サイトによる詐欺等についても、やはりこの入り口としてフィッシングメールが、非常に多いという現状です。

先ほどのDMARCの導入促進については、昨年の12月、各事業者、例えばプラットフォームであったり、宅配業者等も含めたところに対しまして導入を要請しております。今後も申し上げたような対策を着実に推進していきたいと思っています。

また、都道府県警察で、そうした詐欺サイトを認知しますと、警察庁に対して報告が行われております。報告を受けた詐欺サイトのURLを警察庁で精査した後に、フィルタリングをする事業者等に提供し、詐欺サイトへのアクセスを防ぐ取組も行っています。

さらに、テイクダウンという詐欺サイトを閉鎖する活動も行っております。詐欺サイトを発見した際に、事業者が、Abuse通報をすることで、ドメイン事業者等に詐欺サイトの閉鎖の依頼をしています。

県警察でも、民間の方や大学生等を中心としたサイバー防犯ボランティアの方の協力を得て、サイバーパトロールを行っています。そうした方々と一緒に、詐欺サイトやフィッシングサイト等を見つけた際には、サイト管理者などへ通報もしてくれているところでございます。

以上でございます。

○鹿野委員長 ありがとうございます。

今まで3点について、まずはお答えいただきましたけれども、柿沼委員、それでよろしいですか。

○柿沼委員 ありがとうございます。

技術的な対応にとどまらず、制度、それから連携を各方面から対策を講じるようお願いするところと、あと、最後の偽の通販サイトなのですけれども、恐らくテイクダウンしている間に、詐欺サイト自体が、もうサイトを閉じてしまうことが多いです。

消費者から広告とは全く違うものが届いたけれども、サイトとは連絡が取れないという相談が多くございまして、こちらから宅配会社に電話をかけても、宅配を引き受けた代行会社に連絡するようと言われるだけで、今の温度感では何の対応もしていただけないという現状です。

ただ、そういうところから受け取っている荷物で、こういうトラブルが起きているということをご存じなわけですから、宅配会社についても、もう少し真摯に考えていただきたいということで、国のほうからも、そのような働きかけを求めているところでございます。

ですので、恐らく国土交通省ですかね、そのようなところにも働きかけをお願いしたいと思います。よろしく願いいたします。

○鹿野委員長 ありがとうございます。

それから、4点目と5点目についてですが、4点目は相談対応。

○総務省総合通信基盤局電気通信事業部利用環境課田中課長補佐 総務省利用環境課の田中でございます。御質問いただきまして、どうもありがとうございます。

御説明にもありましたとおり、特殊詐欺の入り口としての電話というのが、今、8割に上っているということを受けまして、総務省におきまして、6月10日に、電話の不適正利用対策に係る相談窓口を設置いたしました。こちらは、通称「でんわんセンター」と呼んでおります。

こちらのセンターでは、いわゆる詐欺電話にかかわらず、迷惑電話一般のことについて、相談窓口となっております。何でも迷惑電話に関する困りごとであれば受けるという形となっております。一般の方、法人の方、自治体の方、また、警察を含む行政の方から幅広く相談を受け付けております。利用料は無料ですので、ぜひ御活用いただければと思っております。

こちらの連携ということで御指摘もいただきましたけれども、国際電話発の固定向けの詐欺電話が非常に増加しているということを受けておりまして、国際電話の利用を望まない利用者に対しては、着信制限の対策が効果的だろうと思っております。着信制限のための民間の事業者で運営しております国際電話不取扱センターというのがございまして、固定電話宛ての国際電話の発着信休止ができるという形になっておりますので、こちらのセンターと連携をしながら、適切に国際電話の不適正対策を推進していくことを考えております。

以上です。

○鹿野委員長 ありがとうございます。

柿沼委員、最後のほうでおっしゃった、消費者金融からリモートでお金を借りさせるというところについては、これは、御質問と捉えていいですか。

○柿沼委員 そうですね、何かの対策を講じられないのかということをお伺いしたいのと、今、総務省様のほうから電話相談センターについて御案内がありまして、そちらについては理解できたのですが、国際電話不取扱センターについての御質問の中で、これは、連絡をすると国際電話からの電話が全てがかかかってこない、それから、電話をかけることもできないようになっているかと思うのですが、そうではなく、一部だけ、例えばアメリカとかカナダだけは、電話が通じるようにしたいとか、そういうことはできないのかというところを、先ほどお尋ねしたのですが、御回答がなかったようなのですが、そちらについては、いかがなのでしょう。教えていただければと思います。

○総務省総合通信基盤局電気通信事業部利用環境課田中課長補佐 ありがとうございます。

御指摘いただきまして、国際電話不取扱センターで行っている休止業務というのは、国際電話番号を全て着信できなくするというものでございます。こちらは、国際電話であるかを判別し、システム上対応することは可能だということなのですが、そこをどこの国からという形で対応するというのは、今、難しいところがございます。

ですが、一部民間のサービスなどで、この国からはブロックですとか、この番号からは

ブロックと指定する迷惑電話サービスを実施、提供している事業者はございますので、こちらのほうを御活用いただければと思います。

○鹿野委員長 ありがとうございます。

それで、最後の点、先ほど確認させていただいたのですが、どちらに伺いましょうか。

柿沼委員。

○柿沼委員 すみません、鹿野委員長、2つございまして、遠隔操作についての手だてをされているのかということと、それから相談窓口、もう信じ切ってしまうと、なかなか家族のことも聞き入れられないような方に、専門的な支援が必要かと思うのですけれども、そのような窓口の設置があるのか、なければ設置を強く望みたいと思います。

○鹿野委員長 それでは、まず、遠隔操作について、どこにお答えいただけますか。本日、かなり多くの省庁の方々にお越しいただいているのですが、どこにお答えをいただくのが一番適切か。

○内閣官房副長官補付榊野内閣参事官 振込みの関係であったらば、金融庁です。

○鹿野委員長 先ほどの例としては、リモート操作を用いて、振込み等をさせ、あるいはお金を借りさせて振り込ませるということでしたので、金融庁に伺ってみますか、金融庁様、いかがでしょうか。

○金融庁総合政策局リスク分析総括課金融犯罪対策室神谷課長補佐 金融機関のサイトの、例えば遮断ということについて、恐らく御質問されていたかと思うのですけれども、それが、一金融機関において対応できるものなのかという技術的なところについてあまり承知しておらず、そういった手口もあるということについて問題意識も持ちながら、様々な対策を進めてまいりたいと思います。

○鹿野委員長 今後、また、進めていただくということをお願いします。それでは、相談についてですが、詐欺の加害者のほうの言うことを信じ切ってしまうと、家族のアドバイスとかも聞き入れないという人たちについての相談について、どういう対策が考えられるかということで、それでは、榊野様。

○内閣官房副長官補付榊野内閣参事官 すみません、委員から御指摘のあったような、家族が手を尽くしたのにという、その専門の窓口があるかどうかというのは、関係省庁に、すみません、必ずしもそれがあのかどうか、私も網羅的に承知しているわけではございませんけれども、御指摘いただいたようなケースの場合、家族の一員が、恐らく投資詐欺ですとか、そういった詐欺にはまっているにもかかわらず、家族の忠告に耳を傾けないという場合には、シンプルではございますけれども、最寄りの警察署に御相談いただくのが一番よいかと思います。

それが、犯罪が疑われるようなことがあれば、警察は即捜査に入りますので、さすがに警察の手が入っても耳を貸さないということであれば、それは、詐欺でなければ、ある程度はあれかもしれませんが、詐欺の場合は、警察は何らかの手段を講じて止めさせてくれると、私は信じてございますので、最寄りの警察署に御相談いただくのが一番スピーディ

一、かつ実効的かと理解してございます。

以上です。

○鹿野委員長 柿沼委員、よろしいですか。

○柿沼委員 はい、分かりました。詳細にわたり、御説明いただきましてありがとうございました。

○鹿野委員長 ありがとうございます。

それでは、大澤委員からお手が挙がっていますので、お願いします。

○大澤委員 御説明いただき、ありがとうございました。

どなたに伺っていいのか分からないのですが、いろいろ資料を拝見していて気になったことなのですけれども、恐らく詐欺といってもいろいろな手口があるのではないかと思います。例えばオレオレ詐欺だったり、いわゆるSNS型でもロマンス型とか、投資型とか、いろいろあると思うのですが、ざっくりとした質問なのですけれども、この被害者の年齢の傾向というのが、恐らく詐欺の手口によって違うのかなと思っているのですが、資料を拝見していますと、例えばオレオレ詐欺に関して、これは実際の対策が功を奏しているところがあると、オレオレ詐欺なのか、要は銀行で振込みについて、声かけをして少し減らしましたということも資料には書かれておりましたけれども、例えば、そういった振込みを使わせてということになると、確かに高齢者の場合が多いのかなという印象を持ちましたが、一方で、SNS型に関しては、結構幅広い年代でと拝見をしております。

他方で、闇バイトというのは、むしろ、お金目当てで、要はアルバイト感覚で加害者になる場面だと思うのですが、こちらに関しては、私も大学で仕事をしていますので、若者が安易に、若者はお金ないですから、やはりお金を短期間で得られるということで手を出しているのかなと、いろいろ資料等を見ていると理解をしています。

年齢に関しては、恐らく、それぞれの対策にも多少の差異が出てくるのではないかと思います。例えば、先ほどの銀行やATM等々での声かけ等で功を奏したと、減少をしたというのも、すみません、資料のどこかに記載されていたと思うのですが、要は、それぞれの年代に応じて、例えば高齢者の場合ですと、先ほど来出ている、例えば国際電話を使えないような設定にするよう促すとか、あるいは何か窓口、あるいはATMで何か動きが、少し様子を見て、少しおかしいなと思ったら声かけをすとか、そういったことで対策ができるのかもしれませんが、もちろんいろいろな対策はあると思いますが、私の近所を見ても、確かに銀行の前に市の職員なのか、市のボランティアの方が、銀行の前に立って、その振込みは大丈夫ですかというプレートを持って立っているのを見たことがありますので、そういう対策は現に行われていると理解しています。

他方で、問題は若者の、特に闇バイト等々に手を出してしまうというのを、一体どうやって防げばいいのだろうかというのが、私はやはり大学で勤めていて非常に考えるところが大きいのですが、恐らく若者がどういう経緯でそれを知ることというのは、SNSとか、いろいろなものがあるのだろうと思うのですけれども、やはり年代によっても加害者になる

場合、被害者になる場合も両方を含めて、それぞれの年齢に応じた対策というのはあり得るのではないかと考えていますが、年齢について、全体的に詐欺から守るところなのですが、消費者教育等々にも関わってくると思うのですけれども、何かその傾向等がありましたら、あるいはそれぞれの年代に応じた対応等がありましたら、教えていただきたいと思います。

すみません、すごく一般的な質問で、どなたに伺えばよろしいのか、分からないのですが、よろしくをお願いします。

○鹿野委員長 どうぞ。

○警察庁刑事局組織犯罪対策部組織犯罪対策第二課塩谷課長補佐 警察庁でございます。御質問いただきありがとうございます。

まさに委員御指摘のとおり、例えば、特殊詐欺の世界であれば、65歳以上の高齢者の方の被害が65%となっております。他方で、SNS型投資・ロマンス詐欺については、投資詐欺であれば、40代から70代を中心にと幅広い年齢層で被害が発生しております。また、ロマンス詐欺については、40代から60代が多く、手口によって年齢層が変わっているという傾向はあろうかと思えます。

そういった意味でも、まさに犯罪の情勢、手口をいかに分析して対策につなげていくかということが大事かと思っております。

先ほど「闇バイト」の話がございましたが、特殊詐欺事件において、いわゆる「闇バイト」に応募して検挙された者については、10代、20代の者が約7割を占めております。そういった意味では、やはり、10代、20代に、学校現場を含め、いかに注意喚起をしていくか、いかに闇バイトが危ないかという危険性について周知していくかということが大事かと思っております。

そういった意味で、今回の総合対策2.0におきましても、先ほどの資料の、例えば1の(3)の欺罔段階への対策として、変化する欺罔の手口について、広報、啓発をしていくということになってはいますが、やり方として、10代、20代に対してどうすれば響くかという部分については、例えば、警察庁のホームページに広報資料を載せましたといったような方法では、なかなか見てくれないというのが現実かと思えます。

そういった意味では、やはりSNSの活用や若者に対して訴求力のある芸能人の方に御協力いただくとか、そういった形で、手口の変化に合う形で対策を講じていくことが大事かと思っております。

以上です。

○内閣官房副長官補付榊野内閣参事官 補足で、内閣官房でございますけれども、先生から特に闇バイトの学校現場での対策と周知徹底はどうなっているのだという話は、今日は、多分文科省はいらっしやらないので、すみません、私が代わりに御説明いたしますけれども、その問題意識は政府としてもありますので、必ずしも全てではないかもしれませんが、学校に警察官を派遣して防犯教室を開いたりということもやってございますし、

文科省と連携して、大学現場とかでも、そういった注意喚起、闇バイトの募集というのは、やはり駄目ですよということは推進していきたいと思っております、その取組は進めている最中でございます。

さらに、少しキャッチーなところで申し上げますと、先ほどもありましたけれども、若者は、なかなか警察庁のホームページなどは見るわけではないですけれども、テレビもなかなか見ないという中で、アドトラックを御存じですかね、繁華街をトラックが走り回っていて、高額報酬だとか、ホストの顔で宣伝しているみたいな、繁華街を走っているトラックがありますけれども、この闇バイト対策の一環として、若者が繁華街に多数いる可能性があるということで、ああいうトラックに闇バイトは犯罪ですよというのをぱっと書いて繁華街を走り回らせました。

ある程度、若者も、ああいうのがありましたねという声も聞かれているという話も聞いてございますので、政府としても、それだけにとどまらず、大学現場だけではなくて、そういった訴求力のあるような広報啓発には、引き続き努めていきたいと考えております。

以上です。

○鹿野委員長 大澤委員、よろしいですか。

○大澤委員 ありがとうございます。

私は前から気になっていたことなのですが、闇バイトかどうかをどうやって見抜けるのだろうかというのを、何か私も新聞等で読んだことがあるのですが、いきなり闇バイトっぽく人材募集をしているのではなくて、非常に報酬としては、もちろん、いきなり1回で100万もらいますという、これは何か変だなと思うと思うのですが、結構巧妙な人材募集を、SNS等でしていることがあるというのを伺ったことがあって、記事等でも見たことがあるので、もちろん学生に、私も大学にいる人間として、そんな簡単に、お金などは稼げないですよという話は、よく消費者法や民法の授業の中でもやってはいるのですが、若者に注意喚起するというのは、もちろん、今、十分なさっているのも分かっておりますし、そこは一定の評価をしています。

それで、とても大事なのですが、他方で、これは、今回の資料1にも載っておりますけれども、例えば違法情報の削除要請を行うインターネットホットラインセンターのガイドラインを改定して、犯罪実行者募集情報を位置付けて削除しましたとか、やはりそういう消費者教育だったり、注意喚起というのもとても大事ですし、私も微力ながらやっていきたいのですが、やはりハード面で、SNSを含め、何か違法情報がある、あるいは現に、実は、前はそうでしたというのを削除していくとか、そういうのは、もちろんプラットフォーム事業者の協力等々も必要になってくると思うのですが、そういうハードの対策というのもないと、なかなか若者は、闇バイトは駄目なのだというのは、さすがに分かっていると思うのですが、それが闇バイトだと認識できるかどうかというところが、なかなか難しいのかなという印象を持っていますので、ぜひハードな対策も頑張ってくださいというのが、個人的な意見になります。

以上です。

○内閣官房副長官補付榊野内閣参事官 内閣官房でございます。

闇バイトに関しては、すみません、説明では割愛してしまったのですが、先生がおっしゃるように、どれが闇バイトか若者が分からないではないかというお話だったと思っておりますけれども、確かにそういう状況はございました。どういうものが闇バイトなのか分からないだろうという指摘があったので、去年の12月の段階で、職安法に基づきまして、求人というのがある、それは、どれがまともなもので、まともではないのかというのは、確かに分からなかったのですが、職安法の解釈を明確化することによりまして、求人者の氏名、名称、住所、連絡先、業務内容、就業場所、そして賃金の表示、これら全てそろっていないものは違法だということを確定的にしましたので、例えば、即日100万稼げるから、ここに連絡しろというのは全部違法になりました。それが、確かに全て削除できているかどうかというのは、警察のマンパワーにもよるのですが、もし、先生のお立場で、学生さんとかに対して、例えば、どういうものが闇バイトなのだと聞かれた場合には、今の全ての要件がそろっていないものは、およそ闇バイトだとおっしゃっていただいて結構かと思っております。そのぐらいの感じで政府としては取り組んでおりますので、さすがに求人者の氏名、名称、住所、連絡先と業務内容と賃金が全部明記されているものであれば、確認が取れるはずですので、どういう企業か、どういった職場なのかというのを確認が取れば、それは闇か闇ではないかという判断は、従前よりは可能になったのではないかと、政府としては考えております。

以上です。

○大澤委員 どうもありがとうございました。私の無知をおわび申し上げます。非常によろしい対策ではないかと思っておりますが、あと、問題は、やはりそういう情報が違法情報だということが、もうこれではっきりしていますので、あとは、そういうのを削除するとか、そういったことのフェーズに、今はもう来ているのではないかと思っております。

以上です。どうもありがとうございます。

○鹿野委員長 それでは、小野委員、お願いします。

○小野委員 小野でございます。

内閣官房の榊野参事官をはじめ、御説明をいただきまして、ありがとうございました。今、私自身も闇バイトの定義を控えまして、大学の授業などでも活用してまいりたいと思いました。

今回の総合対策の改定に当たりまして、私からはコメントと質問と、それから1つ提案をさせていただきたいと思っております。今回の対策はSNS型等詐欺と、特殊詐欺対策を併せたものであることを理解できました。

消費者教育を専門にしている立場からですと、対象と目的について2つの構図が見えてきたかと思っております。

1つ目が対策の対象者ですね、大きく分けて判断が不十分な状況にある人、必ずしも高齢

者ではないと思っていたのですが、先ほどの年代についてお聞きしますと、高齢者と捉えるのも、1つ分かりやすいかなと思いました。

もう一つは、だます側、こちらも必ずしも若年層とは言えないのですが、それでも今回の情報では、若い人が多いと思いました。こうした2つの対象への対策が求められると思います。

それから、2つ目の目的になりますが、消費者教育は、被害に遭わない、未然防止、これは大きいのですが、被害者にしないという、だまされないための啓発と、改めて犯行に加担させない、加害者にならないための啓発、教育というものが大切であり、今回御説明をいただきました主な施策でも、その辺りを踏まえて整理されていきましたので、分かりやすいものになっていると思います。

以上を受けまして、消費者教育についてなのですが、本日は消費者庁、それから文科省の方はいらっしゃるのですが、その2つの省庁を中心としながらも、やはり関係省庁の連携が必要だということで、警察庁、経産省、金融庁、それから総務省、法務省の御担当の方には、改めて御協力をお願いしたいと思いました。

今日、御説明をいただいただけでも、警察庁ではサイバーパトロールの取組があるとか、総務省様では国際電話不取扱の受付センターがある、それから学校へ警察官を派遣していたり、あるいはアドトラックを活用しているということで、いろいろな情報が集まっているのですが、これからは質問なのですが、こうした連携の充実をするために、国民向けの取組状況について情報がまとまったポータルサイトのようなものがあるのかないのか、私が調べた限りでは見つけられなかったのですが、ありましたらお知らせをいただきたい。そして、そういったポータルサイトのようなものがありますと、家庭科教員だけではなく、こういったものを扱う教員にとっても大変役に立つものになるかと思っておりますので、お伺いをする次第です。

長くなりましたが、以上です。お願いいたします。

○鹿野委員長 ありがとうございます。

これは、梶野参事官から、お答えいただけますか。

○内閣官房副長官補付梶野内閣参事官 内閣官房でございます。

各担当ごとに広報啓発を、新しいものを含めて取り組ませていただいているところでございますけれども、先生御指摘のような全てを一括したポータルサイトの存在については、私の知る限りでは、確かにございません。

今、先生からそういったお話をいただきまして、一応ポータルには届かないかもしれませんが、総合対策とか、そういったもののフォローアップがどうなっているのかというのは、一応内閣官房のサイトでは見られるようになっているのですが、多分、先生のお考えとしては、それだけでは多分不十分で、国民向けの発信がポータルとしてできるべきではないかというお話ですが、そこは将来的に必要性も含めて、関係省庁間で考えていかなければいけないのかなと思いますけれども、中長期的な課題として承り

たいと考えております。

以上です。

○鹿野委員長 ありがとうございます。

ほかは、いかがでしょうか。

黒木委員長代理、お願いします。

○黒木委員長代理 ありがとうございます。

総合対策1.0は、各省庁の対策を寄せ集めたようでパッチワーク的でしたが、2.0では非常に体系的に整理され、特に法律家の視点から見ると、詐欺行為を着手行為である欺罔行為、被害者の錯誤、被害者からの財の交付、犯罪者への財の帰属という4つの段階に分けて対策が整理されており、大変見やすくなりました。今後もこの方向で進めていただけることを期待しています。

それを前提として、4点質問させていただきます。

まず、1点目の質問として欺罔行為である広告についてお尋ねします。

8～9ページの広告関連で、総務省と経産省にお尋ねします。総務省でモニタリングを実施し、DPF取引透明化法に基づく大臣評価も行われたとのことですが、これらによって広告DPF事業者は、昨年大問題となった著名人の詐欺広告にどのような対応をしてくれているのでしょうか。

次に2点目の質問として被害者の錯誤についてお尋ねします。

令和6年における特殊詐欺及びSNS型投資・ロマンス詐欺の認知・検挙状況等について等、多くの資料で、被害時の連絡ツールとして9割程度がグループLINEに誘導されているとされていますが、そうした特定事業者への捜査協力度合いが昨年からどの程度変わっているのか、警察庁に教えていただけますでしょうか。

次に3点目の質問として財の交付についてお尋ねします。

交付のところにつきましては、これは、多くの場合が銀行口座への振り込み送金が利用されているとのこと。先ほども少し説明をいただきましたけれども、金融機関相互の連携ということは、お話いただきました。ただ、同時に、刑事上行為者を特定するというだけではなく、被害者からすると、民事上の被害の回復を行うことで、行為者に利得を帰属させないという点では、我々弁護士としては、民事上の責任をこういう犯罪者に対して、どう追及できるかという点も非常に大きな問題であります。

その点で御質問なのですが、振り込め詐欺被害救済法の口座凍結という方法は、弁護士にとっては非常に大きな救済方法となっております。総合対策の12ページ以下で御指摘のある金融機関間における情報共有の枠組みの創出というところは、非常にレベルの高い議論だと思っております。振り込め詐欺被害救済法によって凍結された口座は、もうほとんど抜け殻になってしまっていて、別の口座に送金されていることが殆どです。そこで、早急に被害者側のほうに、どこの口座に送金されたかという情報を開示する方法について御検討されていないかということです。

最後に4点目として犯人への財の取得についてお尋ねします。

暗号資産について、世取山茂さんという方の警察政策の27巻の論文によると、I-GRIP（インターポール国際資金移転迅速措置制度：Interpol Global Rapid Intervention of Payments）が機能しており、警視庁がNCB（国家中央事務局）に指定されているとのことです。I-GRIPを活用した暗号資産等の凍結について、現在どの程度まで議論が進んでいるのでしょうか。

以上4点についてお聞かせください。

○鹿野委員長 1点目は、総務省様ですかね。

○黒木委員長代理 総務省と、それから経産省です。

○鹿野委員長 それでは、まず、総務省様から、お答えいただけますか。

○総務省情報流通行政局参事官室田熊参事官補佐 総務省情報流通行政局でございます。

黒木委員から御質問いただきました、広告の関係でございます。少し経緯から御説明させていただきますと、昨年6月の「国民を詐欺から守るための総合対策」を踏まえまして、まず昨年の6月に、プラットフォーム事業者に対しまして、SNSにおける、なりすまし型の偽広告への対応について、要請を実施したものでございます。

それを踏まえまして、きちんと対応されているかどうかを確認するために、昨年の10月にプラットフォーム事業者にヒアリングを実施したところでございます。そのヒアリングの結果ということで、ヒアリング総括という名前で、11月に公表したものでございます。

それを踏まえまして、今後、モニタリングをしていくということでございまして、モニタリング指針というものを、今年7月に意見募集を凶っているところですけれども、当該モニタリング指針に基づきまして、プラットフォーム事業者に対して、モニタリングを実施してまいりたいと考えております。

以上でございます。

○鹿野委員長 それでは、経産省様、お願いします。

○経済産業省商務情報政策局情報経済課デジタル取引環境整備室渡辺室長補佐 経済産業省デジタル取引環境整備室の渡辺でございます。

黒木委員から御質問がございました点のうち、経済産業省としてアプローチしております、正当な広告主を偽りました悪質な広告への対応について、御説明をさせていただきます。

まず、経済産業省が所管しております、プラットフォーム取引透明化法については、正当な広告主が、なりすまし被害に遭いまして、広告掲載取引上の不利益を受けることを防止する観点から取り組んでおります。

「国民を詐欺から守るための総合対策」のフォローアップのところに記載させていただいておりますけれども、大規模プラットフォーム事業者に対しまして、広告の出稿者、事前審査、または事後的な削除に関する要請や、その対応状況に関するヒアリングにつきまして、昨年の5月から6月にかけて、プラットフォーム取引透明化法の規律の対象とし

ております3社に対しまして、緊急的に聞き取りを行いまして評価を公表いたしました。

そのうち、いろいろ各社によって対応は異なりますけれども、例えば、例を挙げさせていただきますと、広告主の本人確認を行う対象が限定的であること、人の目による広告審査を機械による判別が困難な場合に限定していること等を確認されましたため、先ほど黒木委員からも御指摘ございましたとおり、今年の2月に公表させていただきました大臣評価におきまして、プロセスの改善を求めています。

引き続き、今後とも対応してまいりたいと考えております。

○鹿野委員長 ありがとうございます。

それでは、2点目について、警察庁様、お願いします。

○警察庁刑事局組織犯罪対策部組織犯罪対策第二課塩谷課長補佐 2点目、特定の事業者への捜査協力ということで、御質問をいただきました。

結論を申し上げますと、前回、1年前からどういったやり取りがあったかについては、詳細には承知しておりませんが、大幅に捜査に御協力をいただけるようになっていると考えております。

そもそもアカウントを登録するときに、いわゆるSMS認証という形で本人確認をしっかりといただくということも始まっておりますし、また、例えば登録者情報について、差押えによらずとも、通信の秘密に当たらないものについては、捜査関係事項照会書により回答をいただくという形にも対応していただいております。

登録者情報の回答が得られる日数も、かなり短くなっており事業者にはかなり御協力をいただいているものと考えております。

あと、捜査の話ではありませんが、当該事業者との間においては、犯罪に使われたアカウントにつき、警察から事業者に情報提供を行い、事業者において適宜当該アカウントを削除するというスキームも運用を開始しておりまして、そういった観点でも御協力をいただけているものと考えております。

○鹿野委員長 3点目は。

○黒木委員長代理 振り込め詐欺被害防止法に基づく情報開示の問題について、金融庁か内閣官房にお尋ねします。要するに金融機関相互の連携というところの話なのですけれども、そこについてです。我々弁護士は弁護士法23条照会等を金融機関に対して行っています。しかし、それに基づいて対象口座の残高を開示してもらったとしても、もうもぬけの殻です。彼らは、あつという間に移します。

そこで、資金移動先についても、開示してもらってもいいのではないかというのが、被害救済をやっている弁護士側からすると強い要望です。先ほど、A行、B行、C行で情報共有しようという話がありました。それを被害者の被害回復のために、移転先の口座情報等を開示してもらえる制度というのは考えられないかということなのです。その辺りのところについて、何か御関心というか、こういう方法があるかもしれないというのがありましたら、教えていただきたいと思えます。

では、金融庁のほうで。

○金融庁総合政策局リスク分析総括課金融犯罪対策室神谷課長補佐 金融庁です。

御指摘いただいた、今、全銀協さんのほうで検討いただいている不正利用口座に係る情報共有というものが実現して進むようになりますと、被害金の受け皿口座として使われた口座を凍結した場合に、その情報が共有されることになると思っております、そうなる、その被害金の移転先などについても凍結などの対応ができるようになってくるかと思えますけれども、その被害回復に資するものと考えております。

ただ、この仕組みの構築に当たっても、様々法令上の問題というものがございまして、検討が進められているものと承知しておりますので、この点、いただいた問題意識についても、また、似たような法令上の問題というのが出てくるかと思えます。

あと、暗号資産の凍結に関し、I-GRIPについて、当庁では把握をできておらず、もし警察庁さんのほうで把握されていられれば御回答いただければと思えますけれども、被害金が暗号資産に流れていくという実態があるとも伺っておりますので、暗号資産周りの話についても、当庁所管の暗号資産交換業者に関しては適切に対応できるようにしてまいりたいと思えます。

○黒木委員長代理 I-GRIPは如何でしょうか。

○警察庁刑事局組織犯罪対策部組織犯罪対策第二課塩谷課長補佐 警察庁でございます。

I-GRIPの枠組みについては承知しておりますが、責任を持ってお答えするための手持ちの資料がございませんのでお答えを差し控えさせていただきます。申し訳ございません。ただし、問題意識として暗号資産が海外に流れているという点については非常に重要だと考えております。

○黒木委員長代理 分かりました。ぜひ、シンガポールとかでは、I-GRIPを利用して、暗号資産を押さえた実績があるといったことが、先ほどの論考でも紹介されています。やはり、最終的に暗号資産に変えてしまえば、犯罪による収益の移転防止に関する法律の規制に関わりなく罪の移転が可能となることができそうです。最後は、悪い人たちは制度がぬるいところに来るのですね。彼らは徹底的にそれを研究していますので、その点も含めて金融庁さんと、それから警察庁さんのほうでも、ぜひこの暗号資産に基づく、犯罪者が財を取得できない方法を検討していただきたいと思っております。

これは、本当にお願いです。よろしくお願いたしたいと思えます。

○警察庁サイバー警察局サイバー企画課サイバー事案防止対策室岡嶋課長補佐 暗号資産の関係で、先生の御質問と直接関連してるかは明確ではありませんが、御指摘のとおり、銀行口座が転々と移し替えられた結果、口座には被害金が空になり、銀行口座から暗号資産口座に被害金が流れているケースが見受けられます。実際、インターネットバンキングを利用した不正送金が昨年、一昨年にかけて大幅に増えており、被害の状況からは、口座名義人と異なる振込依頼人名で送金されている事実が確認されています。そういった被害状況を受け、警察庁は異名義送金対策として、暗号資産の取引所に送られる前に、異名義

の送金をやめていただくように、金融庁様と連携して要請文を関係事業者に出させてもらっております。

そうした取組も引き続きフォローアップしていきたいと思っております。

○黒木委員長代理 最後は意見になります。結局のところ犯罪者というのは外国にいて、国富がこれだけの規模で国外に流出している、しかもそれが消費者というか、普通の国民が、個人では全くそれをブロックすることができない。それで国富がこれだけ犯罪者に渡っている。これを何とかしていただきたいと思っておりますので、ぜひよろしくお願ひしたいと思っております。

○鹿野委員長 ほかは、いかがでしょうか。

よろしいでしょうか。それでは、予定した時間もまいりましたので、ここで質疑応答、意見交換を終わらせていただきたいと思います。関係者の皆様には、御説明、御回答をいただき、ありがとうございました。

ここで、今まで出された御意見等に、私の意見等も若干加えて簡単にまとめさせていただきます。

まず、全体としてですが、政府を挙げた対策が進められてきたにもかかわらず、令和6年中のSNS型投資詐欺、ロマンス詐欺の被害額が前年の約3倍となるなど、現状は極めて深刻な状況にあると認識しております。これは、冒頭にも発言させていただいたところです。

本日は、総合対策の2.0では、金融と通信を2本の柱として対策の強化が図られたということをお説明いただいたところでございます。

今後もSNSとか、あるいはキャッシュレス決済の普及が一層進むと見込まれる中で、従来の総合対策で位置付けられていた施策に加え、今回の総合対策の見直しで追加された施策についても、ぜひ、迅速な対応を進めていただきたいと思います。

それから、個別のところについてですが、本人確認の強化ということについては、一定、進められてきたということをお伺ったところでございます。これについても、ぜひ、より厳格な本人確認を実施するよう、しかも、聞くところによると、やはり関係事業者によっても、対応が違っているようなお話もお伺ったところでございますので、広く関係する事業者に対して、より厳格な本人確認を実施するよう働きかけていただきたいと思いますところがございます。

犯罪に悪用されるアプリもあり、特に海外の秘匿性が高いアプリについては、本日、海外の対策等を参考にしながら、日本でも対策を進めていくのだという方向性については伺ったところでございまして、これについても、ぜひ進めていただきたいと思います。

それから、ネットバンキングについて、総合対策では金融機関と連携した被害の未然防止の取組が推進されてきたこと等を承知しているところでございますが、近時の状況を見るとインターネットバンキングの利用が、被害の高額化の1つの要因となっているのではないかと、そういうことが伺われるところでございます。

これについて、既に対策を講じられてきたとは思いますが、初期利用額、限度額の適切

な設定とか、あるいはインターネットバンキングの申込み時あるいは利用限度額の引上げ時など、適切な時期において利用者に十分な確認や注意喚起を行う等の取組を進めるよう、対策として推進していただきたいと思います。

それから、照会対応の迅速化等についてでございます。

総合対策によって一定の事業者について、照会対応の迅速化等の措置が講じられてきたのだと認識しているところでございます。

ただ、先ほども言いましたが、犯行に利用されるSNSは、時に応じて変化しているということもございますので、より広く関係事業者に対して照会への対応の迅速、円滑化に関する要請を実施していただき、関係省庁において照会に対する協力を得るための実効性のある方策について、更に御検討いただきたいと思います。

それから、捜査協力的な側面では、こういう照会に対する対応というのは進んできたのではないかと考えるのですが、一方で、特に黒木委員長代理がおっしゃったように、民事的な被害回復というところも非常に重要だと認識しているところです。私は、もともと民法を専門としている者でございまして、やはり民事的な点に関する方策ということも重要なのではないかと考えているところでございます。

もちろん予防も必要なのですが、被害が全くゼロになるというのは、現実的には想定できないので、被害が発生したときの回復につなげられるような対策も講じていただきたいと思います。

特に、不正に利用された口座とか、あるいは不正に取得した資金について、これが暗号資産に流れているのではないかと御指摘もいただいたところでして、そのような不正な資金を早期にブロックするというところがなければ、被害回復ということにはつながらないということにもなりそうです。

また、先ほどの照会対応ということについても、民事的な観点から被害回復を進めようとするときに、SNS等の事業者がなかなか答えてくれないということも伺っているところでございまして、その辺も含め、被害回復につなげるための仕組みということを、ぜひ、検討していただいて、対策を進めていただきたいと思っています。

また、被害救済については、通信履歴の保存の義務化というところも重要な政策であると考えておりまして、この点の進展に期待したいと思っています。

そのほか、全部は繰り返しません、本日は、いろいろな委員から御質問、御意見が出され、意見交換をさせていただきました。

特に、柿沼委員からはフィッシング詐欺について、あるいはネット通販詐欺に対する対策について、あるいは相談窓口の充実、それから詐欺的な国際電話への対策ということについても御指摘があったところでございます。

それから、大澤委員からは、闇バイト対策について御指摘があり、その御回答の中で、教育面でも進めているけれども、それ以外に所定の情報が記載していないと違法となるということを確認したという御回答もいただいたところで、これは、非常に有益なのでは

ないかと思うのですが、その点まで含めて、特にこういう闇バイトに引っかかってしまうおそれのある若者などを中心にして、周知するということが重要であると思います。

さらに、小野委員からも関連する御指摘として、いろいろな対策が講じられていることについて、国民に届けるための、更なる分かりやすい発信が必要なのではないかという御指摘もいただいたところでございます。

そのほか、いろいろと御指摘もあったところでございますけれども、時間の関係もありますので省略させていただきます。

関係省庁におかれましては、詐欺等の被害の未然防止、拡大防止のため、政府一丸となって「国民を詐欺から守るための総合対策2.0」を着実に取り組んでいただくとともに、金融業界や通信業界等の事業者とも連携しながら、あるいはプラットフォーム事業者にも御協力いただけたところはあるのではないかと思います。そのような関係事業者とも連携しながら、社会全体で対策を推進していただきたいと考えております。

御出席いただいた皆様におかれましては、お忙しいところ御対応いただき、誠にありがとうございました。

○黒木委員長代理 ありがとうございます。

《3. 閉会》

○鹿野委員長 本日の本会議の議題は以上になります。

最後に、事務局より今後の予定について御説明をお願いします。

○友行参事官 次回の本会議の日程と議題につきましては、決まり次第、委員会ホームページを通してお知らせいたします。

以上です。

○鹿野委員長 それでは、本日は、これにて閉会とさせていただきます。お忙しいところ、お集まりいただきまして、ありがとうございました。