

消費者委員会本会議（第330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330回）

議事次第

1. 日時 令和2年11月5日（木） 10時00分～11時45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】 山本委員長

【テレビ会議】 受田委員、大石委員、片山委員長代理、柄澤委員、
木村委員、清水委員、新川委員、丸山委員

（説明者）

警察庁生活安全局情報技術犯罪対策課加門官民連携推進官

総務省総合通信基盤局小川消費者行政第二課長

消費者庁内藤消費者政策課長

フィッシング対策協議会 事務局（一般社団法人JPCERT/CC） 平塚 伸世様

一般社団法人JPCERTコーディネーションセンター 佐々木 勇人様

フィッシング対策協議会 事務局（一般社団法人JPCERT/CC） 吉岡 道明様

（事務局）

加納事務局長、渡部審議官、太田参事官

4. 議事

（1）開 会

（2）消費者基本計画の検証・評価・監視（フィッシング対策）

（3）消費者委員会ワーキング・グループ設置・運営規程改正

（4）その他

（5）閉 会

《 1. 開会 》

○山本委員長 皆様、本日はお忙しいところをお集まりいただきまして、ありがとうございます。

ただいまから、消費者委員会第330回本会議を開催いたします。

本日は、受田委員、大石委員、片山委員長代理、柄澤委員、木村委員、清水委員、新川委員、丸山委員がテレビ会議システムにて御出席です。

生駒委員が御欠席です。

まず、会議に先立ちまして、本日は新型コロナウイルス感染症拡大防止のため、3密を回避しながら、消費者委員会会議室及びテレビ会議システムにより会議を進行いたします。

また、感染拡大防止の観点から、引き続き一般傍聴者は入れず、報道関係者のみ傍聴していただき、開催いたします。

議事録につきましては、後日、消費者委員会のホームページに掲載いたしますが、議事録が掲載されるまでは、本日の会議の様子を、明日11月6日金曜日15時より、ホームページで動画配信いたします。

それでは、会議の進め方及び配付資料の確認につきまして、事務局よりお願いいたします。

○太田参事官 本日もどうぞよろしくお願いいたします。

本日、山本委員長以外はテレビ会議での御参加となります。

資料についてでございますが、議事次第の下に配付資料として記載しておりますとおりでございます。もしお手元の資料に不足などがございましたら、事務局までお申し出くださいますよう、お願いいたします。

以上でございます。

《 2. 消費者基本計画の検証・評価・監視（フィッシング対策） 》

○山本委員長 本日の議題は、フィッシング対策の取組についてです。

昨今、フィッシングの報告件数が急激に増加しております。具体的事案としては、フィッシングのメールやSMSを受信した消費者が偽サイトにアクセスし、IDやパスワード等の情報を入力してしまうことで、当該情報を不正利用される等の被害が生じているものと認識しております。

委員会といたしましては、今般の状況を踏まえ、消費者基本計画の検証・評価・監視の一環として、フィッシング対策について関係行政機関等からヒアリングを行うことといたしました。

本日のヒアリング内容につきましては、フィッシング対策協議会から、フィッシングの報告件数や事例の傾向、対策等について、警察庁からは、サイバー犯罪の情勢、インターネットバンキングに係る不正送金事案の発生状況や手口、被害防止策等について、そして総務省からは、フィッシング対策にも有効な技術的対策の一つである送信ドメイン認証技術の概要及び普及状況や消費者へ

の注意喚起等について御説明をいただきます。

本日は、御説明者として、フィッシング対策協議会の平塚様、JPCERTコーディネーションセンター佐々木様、警察庁生活安全局情報技術犯罪対策課の加門官民連携推進官、総務省総合通信基盤局消費者行政第二課の小川課長に、また質疑対応として、消費庁消費者政策課の内藤課長にお越しいただいております。

なお、フィッシング対策協議会の吉岡様には、オンラインにて御参加をいただいております。

皆様におかれましては、お忙しいところを御出席いただきまして、誠にありがとうございます。

それでは、それぞれ10分程度で説明をお願いいたします。

○フィッシング対策協議会平塚様 まず、フィッシング対策協議会から御説明させていただきます。

フィッシング対策協議会は、セキュリティベンダーやオンラインサービス事業者、金融・クレジットカード関連の企業からなる、フィッシング対策を行いたい企業が集まる団体です。

次の資料に行かせていただきます。協議会の活動としては、主に一般の方や企業の方からフィッシング報告を受け付けまして、その内容を確認し、フィッシングサイトが稼働中の場合には、JPCERTコーディネーションセンターへ連絡して、サイト閉鎖の調整、いわゆるテイクダウンの調整や、フィッシングURLをセキュリティベンダーに共有して、自社の製品に組み込んでいただき、被害の抑制に役立てていただいております。

ページ数を言っていなかったのですが、次に5ページ目まで行かせていただきます。早速ですが、フィッシング報告件数やURLの数の推移について説明させていただきます。

こちらの表を見ていただくとお分かりのように、2020年から非常に急激に報告数が伸びております。報告数増加の要因や特徴としては、フィッシングメールの大量配信の頻度が増加しているということがございます。1日に20通、30通同じメールを受信されて、それを全て報告されてくる方もいらっしゃいます。

また、本物と同じドメインを使ったなりすまし送信の増加が目立っております。新たなユーザー層をターゲットとしたフィッシング攻撃も発生しております。いわゆる国内ECサイトやフリーマーケットサービス、行政サービス等です。

6ページ目に移らせていただきます。フィッシング報告数の年別のグラフです。こちらを見ていただきますと、2014年に数が増えています。この時期は不正送金目的やオンラインゲームの認証情報の詐取のフィッシングが非常に増えまして、こちらは事業者側の対応努力により、その後、数が減っています。

昨年からまたフィッシング報告が急激に増え始めたのですが、今年2020年度はそれをはるかに上回る数の報告が来ています。現状、フィッシングの目的としては、クレジットカード情報を盗むことを目的としたフィッシングがメインとなっています。

7ページ目を説明させていただきます。フィッシング報告の対応内容なのですが、報告者はほとんどが一般の方です。不審なメールを受け取ったりフィッシングサイトを発見したという報告をいただいております。そのフィッシングメールの内容を確認し、実際にサイトにアクセスしてみても、フィッシングサイトである場合にはJPCERTコーディネーションセンターを通じてテイクダウ

ンの調整を行っております。

8 ページ目に行かせていただきます。事例紹介なのですが、これは先日発生したフィッシングで、特別定額給付金に関する通知を装うフィッシングです。こちらはなりすましメールで送られていて、対象が広く一般の方になっているので、今までのフィッシングと少し違う感じになっています。報告数については、こちらを御覧いただければ分かるのですが、非常に数が多くなっております。

9 ページ目を説明させていただきます。フィッシング対応における問題点なのですが、いろいろ課題がございます。ただ、現状フィッシングのほとんどはメールによる誘導が行われております。また、フィッシングメールの発信元やフィッシングサイトも海外で稼働しているケースが多いです。

これらのフィッシングはメールで来ているので、フィッシングメールを送信させない、受信させないという行為によって、大量配信されているメールだけでも93%に及ぶので、こちらを減らせるかと思われます。

10 ページ目を説明させていただきます。その他にもいろいろ問題がございます。現状ではフィッシングサイトが稼働している場合にはテイクダウンの調整を行っているのですが、海外に連絡をするので、時差の関係などもありまして、なかなかすぐにテイクダウンに至らない状況になっています。また、現状は報告数が増える一方でして、全てのフィッシングについて、今後も関係機関の連絡を全て行うことは非常に難しい状況となりつつあります。

テイクダウンに時間がかかっているということです。フィッシングの通常の生存時間は12時間から長くても48時間程度です。この時間に全然追い付かないという状況になっております。

あとは不審なメールに関する報告や対応の窓口が分散していて、そういうメールを受け取ったときに、消費者の方がどこに相談したらよいのかが分からない。取りあえずここに送ってみようという形で送ってくださる方もいらっしゃいます。どこかで一括で報告を集めて、案件に応じて専門の窓口が対応できればよろしいのですが、今は警察、迷惑メール相談センター、消費生活センター、フィッシング対策協議会、その他いろいろな対応窓口がある状況です。

11 ページに行かせていただきます。やはりフィッシングのテイクダウンが間に合わないときに、どのように被害を抑制するかということで、URLフィルタリングを使ったブロッキングが有効かと思われます。今も、フィッシングサイトにアクセスすると赤い警告画面が出て、それでアクセスせずに済みましたという報告もいただくのですが、いかに早くURLフィルタリングに登録するかが重要な課題になっております。

ただ、こちらは安定的に登録を行うためには、専門の対応窓口に集中してやる必要があるかと思っています。現状では、フィッシング対策協議会ではそのような対応を行っておりません。その分、セキュリティベンダーにはURLを共有しているので、そちらにお任せしている状態になっております。

このようなサービスは、国内ブランドのフィッシングサイトが登録されづらいというケースもございます。海外の担当者の方が見て、これは日本のブランドかどうか分からない、正規サイトが

どこか分からないという状況があって、登録されないというケースがあるようです。

緊急対応窓口が不明。こちらはフィッシング被害に遭う、いわゆる情報を入力してしまった場合に、その情報を使って不正利用されて、二次被害が起きないためにはどこに連絡をすればよいのが被害者の方に非常に分かりづらい状況になっているかと思われます。こういうフィッシングメールが出ていますよという情報は掲載されているのですけれども、それに引っかかった場合にはどうすれば良いかという対応方法が明確でない場合がございます。

最近ではスマートフォンユーザーが非常に増えています。以前はPCユーザーが多くて、現状のフィッシング対策はまだPCユーザーが中心に考えられている状況でございます。ただ、今ではスマートフォンユーザーがPCユーザーよりもはるかに多く、スマートフォンしか使っていないユーザーもすごく多いです。ですので、今までPCで可能だったメールセキュリティ対策ができない状況でございます。この辺りについては各方面で知恵を出し合って、効果的な方法を模索する必要があるかと思われます。

12ページ目に行かせていただきます。今までのような問題点を軽く図にしたものなのですが、右側の真ん中のメールの大量配信というところから説明させていただきます。いわゆるフィッシングメールが大量配信されて、通信事業者によるフィルタリングやDMARC対応によるなりすましメール検出が対策として考えられます。

課題としては、まずは利用者の同意を取ること。あと、例えばISPなどのところで対応すると思うのですが、そういうところに対応を依頼する、設備更新に係る費用等をどこが負担するのかという問題があるかと思います。

下に行きますけれども、メールの大量配信を受けた一般ユーザー、利用者側では、迷惑メールフィルタを利用して、そういうメールを識別する。

課題については、サービス利用時にフィルタリングに関する同意をする必要があるのですが、それがないと自動的にフィルタリングはされないで、そういう同意を行わなければいけないという問題があります。ただ、利用者側はこういうメールは受け取りたくないという方が非常に多いので、御案内すれば比較的容易に包括同意は取れるかと思われます。

また、実際にフィッシングサイトに情報を入れてしまった場合に、二次被害を防ぐために、サービス側の案内が、もっといろいろなきちんとした対応方法を載せる必要があるかと思われます。

実際にフィッシングサイトにアクセスした場合、今度は上の不正コンテンツへの誘導に行くのですが、ブラウザやセキュリティソフトによるフィルタリングという対策で被害の抑制が望めます。課題としては、いかに早くURL情報を共有できるかにございます。

一番上の攻撃インフラに関しては、不正サイトのテイクダウンについては、攻撃のスピードに追いついていないので、現状ではこの対策はあまり現実的ではないという状況です。

また、不正サーバやアカウントの不正利用に関して、契約段階で認知できないかという問題に関しては、各事業者の集まりの情報交換などで方法を模索している状況かと思われます。

最後の13ページの取組なのですが、軽く整理をしたのですが、事業者側での対策としては、まず全体としてDMARC推進、普及、いわゆるなりすましフィッシングメールの対策が望まれます。

SPFとDKIMというのも送信ドメイン認証にはございますが、それを単体で使う場合とDMARCで使う場合では、なりすましで判定するメールアドレスとか、そこのドメイン部分が少し違います。現状でフィッシングメールというのは、SPF、DKIMはパスして送ってくるなりすましメールが非常に多いです。ですので、DMARCでなければ効果が発揮できないので、ここはDMARCを推進したいと考えております。

URLフィルタサービスへの迅速な情報共有。これはフィッシングサイトを発見した事業者がいち早くURLフィルタに登録することが望まれます。

また、メールサービスを提供する事業者側としては、DMARC検証結果によるなりすましメールの判定をユーザーに分かる形でメールに付加する。あとは、迷惑メールフィルタなど、各種メールセキュリティ対策の実装を行って、ユーザーが利用できるようにすること。

オンラインサービス提供事業者側においては、本物のサイトに常にアクセスさせるための取組、技術や手法の導入が望まれます。いわゆるスマートフォンアプリを使うと必ず正規サイトにアクセスできるので、それを用意する。また、ブラウザのセキュリティ機能による警告で、正規サイトに誘導するなどです。

利用者がフィッシングメールやサイトを判別するための情報を確認しやすくする。これは、ログインした際に、例えばアカウントサービスなどで、サービス側が利用者に送ったメールを確認できるような仕組みを取り入れるサービスもございます。そのようなものがありますと、このメールは本物かなと受け取った方が考えたときに確認する手段があるということが重要かと思われれます。

消費者側での対策としては、迷惑メールフィルタの利用により、不審なメールを判別することができます。あとは正規アプリ、正規サイトからの利用を行う。こちらは啓発活動で、ログインを促すようなメッセージを受け取った場合にも、メールのリンクではなくて必ずアプリや正規サイトからアクセスしてくださいという御案内を当協議会で行っております。

その他、攻撃しづらくさせる取組が一番重要かと思われれます。フィッシング対策協議会やJPCERTでテイクダウンなどの対応を行っているのですが、こちらは効果的ではなくて、全体として対応する方法を考える時に来ているかと思われれます。メール配信に用いられる国内インフラの不正利用への対処とか、URLフィルタサービスへの迅速な情報共有とか、フィッシングにより認証情報が詐取されても二次被害に拡大させない取組などが考えられます。

14ページ目は参考情報として幾つかリンクを掲載させていただきました。なりすまし対策ポータル「ナリタイ」に関しては、そういう電子メールがなぜなりすまし送信ができるのかとか、DMARCの有効性であるとか、DMARCを使うためのいろいろな法整備の状況について、法解釈についての具体例が載っております。

また、フィッシング対策協議会のホームページでは、緊急情報・事例公開のページで、今まであったフィッシングに関して、フィッシングメール文面とフィッシングサイトの画像を載せて確認できるようにしております。その他月次レポートでは、その月のフィッシングのトレンドを掲載したり、事業者がどのようにフィッシング対策を行ったら良いかというガイドラインも出しております。以上です。

○山本委員長 次は、警察庁からお願いします。

○警察庁加門官民連携推進官 警察庁より、サイバー犯罪の情勢と警察の取組につきまして、フィッシング対策を中心として御説明させていただきます。

ページをつけておりませんが、次のスライドをお願いいたします。

サイバー犯罪の情勢につきまして、御説明をします。右に囲った部分にサイバー犯罪とはとしておりますが、これに含まれる犯罪としましては、不正アクセス禁止法違反などの情報技術を利用する犯罪を言います。いわゆるフィッシングに関しましては、不正アクセス禁止法では、他人のID・パスワードを不正に要求するフィッシングサイトを開設するような行為が禁止の対象とされております。

左側、御覧のグラフがサイバー犯罪の検挙件数の推移でございます。増加の傾向が続いておりまして、令和元年中の件数は9,519件と過去最高となっております。

右側に本年上半期と前年同期の数字を出しておりますが、本年の上半期が4,361件で、前年同期とほぼ同じ水準か若干の増加となっております。サイバー空間における脅威は引き続き深刻な情勢が続いているものと認識しております。

次のスライドをお願いします。次に、インターネットバンキングに係る不正送金事犯について御説明をいたします。この不正送金事犯は、サイバー犯罪対策における昨今の最も大きな課題の一つであります。左側のグラフが不正送金事犯の発生状況です。青色の令和元年における発生件数が1,872件、オレンジ色の被害額は約25億2100万円となっております。発生件数としては過去2番目に多く、被害額から見ても過去3番目の規模となっております。平成26年、27年をピークとしまして減少の傾向が続いていたところですが、ここ1年で状況が一変したということになります。

また、このグラフの右側の3本が半年ごとの数値ですけれども、令和2年上半期における状況は、発生件数が885件、被害額が約5億1200万円となっており、直前の半年と比べますと比較的大きく減少してはおりますけれども、昨年同期、令和元年上半期と比べますと、極めて大幅な増加という状況となっております。

この不正送金被害急増の背景にある手口についてですが、ショートメッセージや電子メールを用いて、金融機関を装ったフィッシングサイトへ誘導する手口によるものが多数を占めると考えております。以降のスライドで御説明いたしますけれども、フィッシングを手口とする不正送金事犯は、多数の役割で分担される組織的な犯罪でございます。右側のグラフがそれら関連犯罪の検挙状況の推移でございまして、令和元年は46名を検挙しておりまして、一番右側、今年令和2年は上半期だけでも60名を検挙している状況にございます。

次のスライドをお願いします。こちらはフィッシングを手口とします不正送金の全体像のイメージとなります。全体のスキームの中で、犯罪者はまずフィッシングサイトを準備いたしまして、同時に不正送金先となる預貯金口座も準備します。そして、金融機関を装うなどしてショートメッセージなどを送信、正規の口座名義人を誤信させて提供させたIDパスワード、ワンタイムパスワードなども使いまして、金融機関のインターネットバンキングシステムに不正ログインをし、準備していた口座に不正な送金を実施、出し子を使ってATMから現金を引き出すという全体像になります。

この犯罪者の中には、フィッシングサイトを準備する者、預貯金口座を準備する者、ショートメッセージや電子メールを送る者、IDやパスワードを盗み取る者、不正アクセス、不正送金をする者、ATMから現金を引き出す者など多くの役割から構成されており、複数の犯罪者が関与する組織的な犯罪となっております。

次のページをお願いします。罪種という観点から見ますと、個別の事案につきましては具体の検討が必要ですが、ここでは一般論として御説明いたしますと、これらの犯罪行為に関連して、成立し得る代表的な犯罪といたしましては、フィッシングサイトの準備などに関する不正アクセス禁止法違反、預貯金口座に関する犯罪収益移転防止法違反や詐欺、不正送金に関する電子計算機使用詐欺、ATMからの出金に関する窃盗などが考えられます。警察におきましては、これら犯罪に係る捜査を徹底しておりまして、検挙状況につきましては先ほどのスライドで御説明したとおりでございます。

次のスライドをお願いします。続きまして、フィッシングの手口に対する被害防止対策について御説明をいたします。

まず右側、一般の皆様には不審点に気づいていただくというポイントがございます。フィッシングの手口にだまされない回避の行動を取っていただくという役割でございます。その他の対策を取りましても100%の対策を施すことは不可能ですので、この部分はとても重要な部分となります。

また、先ほど御紹介もありましたが、フィッシングサイトについてですが、有害なサイトで分かっているものについて、ユーザーがそれらのサイトにアクセスしようとする際、ユーザーの手元の画面に警告の表示が行われるようにするなど、被害に遭いそうなユーザーに対して、直接注意を促すことができる仕組みなどを活用することが考えられます。

これらに関連する警察の取組につきまして、以下で御説明します。

次のスライドをお願いします。警察におきましては、様々な注意喚起、広報啓発の取組を行っております。例えば警察庁におきましては、不正送金事犯が急増した際には、全国銀行協会等と連携しつつ注意喚起を行い、サイバー犯罪の情勢を定期的に取りまとめまして、ウェブサイトを提供するなどをしております。

また、インターネット上だけではなく、スライドにありますように、フィッシングも含む各種犯罪の手口に関するパンフレット等の資料を作成するなどしております。

右側、都道府県警察におきましても、名称といたしましては「サイバーセキュリティカレッジ」など名前はいろいろですが、各種のイベントを行い、更には一般の方々に御活躍いただいているサイバー防犯ボランティアと連携した取組などにも力を入れているところであります。

次のスライドをお願いします。こちらのスライドが警察において、フィッシング被害を防止するための対応として一般の皆さんに適宜お願いしている内容の例示となります。具体的な内容としつつ、国民一人一人がサイバーセキュリティの確保に必要な注意を払う状況が実現されるよう取り組んでいるところであります。

次のスライドをお願いします。また、気づきにつなげるという観点からは、できるだけ具体的に最新の情報を提供するというところもポイントになるかと思います。このような情報の提供につ

きましては、こちらのスライドで御説明します日本サイバー犯罪対策センター、略称JC3における取組がございます。このJC3ですが、産学官の連携した取組でございまして、我々警察が参画しているとともに、分野横断的に産業界の御参画をいただき、それぞれの情報、知見を持ち寄りまして、議論、分析を通して、以後の事案発生の防止に資するための活動をしておりますが、これらの活動で生成する情報のうち、広く一般で活用していただきたいものにつきましては随時ホームページに掲載するなどをしております。

スライドの右に掲載しておりますのが、JC3において注意喚起がなされた最近の不正送金に係るフィッシングの手口の一つです。フィッシングのショートメッセージの内容としましては、左上にありますように、荷物を自宅に届けたいけれども不在のために持ち帰った、リンク先で確認してくださいというようなものを送りまして、最後には、これと論理的な関係がないのですが、金融機関のフィッシングサイトに誘導するという手口でございます。荷物の話をしてにおいてリンク先では口座の情報を要求するというものでございまして、こういう手口があるということを知っておいていただければ、これを知らないことと比べかなり被害の発生を抑えることができるのではないかと思います。

この手口の流れがJC3のホームページでは、下側にありますように動画でも用意されております。文章や図での説明以上に分かりやすく理解しやすくなっているのではないかと思います。これらの取組によりまして、一般の皆様の気づきにつながり、被害が発生することのないように努めているところであります。

次のスライドをお願いします。

続きまして、我々警察で把握しているフィッシングサイトなどに一般の皆様がアクセスしてしまった際、利用されているブラウザなどの画面に警告が表示されるといったことを実現するための取組でございます。

対象としましては、フィッシングという観点ではなくて、左上、偽サイト等としておりますけれども、この偽サイト等と言いますのは、実在する企業のウェブサイトを装ったものやネットショッピングを利用した詐欺などを言いまして、結果としてフィッシングサイトの一部も含まれるものでございます。

警察におきましては、偽サイト等の被害に遭ったインターネットの利用者等から相談や被害の届けを受理いたしますが、これらに係るURL等の情報をJC3などからの情報も含めまして、警察庁で集約しております。

一方、ウイルス対策ソフトや各種ブラウザソフトには、開発企業が有害と判断するサイトにユーザーがアクセスした際、警告の表示を行うなどしてユーザーに対して注意を促す機能がございますので、これらの警告表示等に反映していただくことを目的として、我々が集約した偽サイトの情報をウイルス対策事業者等に提供する取組を実施しております。

表示される警告の例といたしましては、スライド中央下のような真っ赤な警告表示が出るなどいたします。このような取組により、警察で把握する偽サイト等における以後の被害発生の防止を図っているところでございます。

以上、警察の取組について御紹介いたしました。我々といたしましては、引き続きサイバー犯罪の捜査を徹底するほか、捜査活動等により得られる知見に基づき、サイバー犯罪による被害の防止に向け、積極的な活動を続けてまいりたいと思っております。

以上でございます。

○山本委員長 それでは、総務省からお願いします。

○総務省小川消費者行政第二課長 続きまして、総務省から、迷惑メール対策につきまして、またその一環としての送信ドメイン認証技術の導入推進に向けた取組、また、消費者の方々への注意喚起についての取組について御紹介をさせていただきます。

まず、スライドの1ページ目でございますけれども、我が国における迷惑メールの現状でございますが、我が国の電気通信事業者が受信した電子メールの中で、迷惑メールが占める割合は現在、5割前後でございます。以前は7割でございましたので、少し減っておりますが、今日も非常に多くの迷惑メールが送られてきているということでございます。また、PC向けの迷惑メールのうち9割以上、携帯向けの迷惑メールのうちの6割前後が外国発となっております。迷惑メールのうち、出会い系サイトや物販の広告宣伝を内容とするものが8割近くを占めているという現状になっております。

次のスライドを御覧ください。我が国への迷惑メールの送信元でございますけれども、我が国発のものを除きますと、月によって変動はございますが、米国や中国発のものも継続的に多く見られる現状でございます。

スライドの3ページ目を御覧ください。特定電子メールの送信の適正化等に関する法律ということで、迷惑メールの対策に取り組んでおります。この法律につきましては、総務省と消費者庁が共管ということで取り組んでおりまして、具体的には、広告宣伝メールについてはオプトイン規制が導入されておりまして、同意のない方への送信は原則として禁止されているということでございます。また、送信を行うことについての同意を記録する保存義務、表示義務、送信者の情報を偽装してはいけないという義務、架空の電子メールアドレス宛での送信も禁止されております。

この法律に基づきまして、総務省としては電気通信事業者や登録送信適正化機関とも協力しながら取組を行っておりまして、警告などの取組も行っております。

また、罰則として、送信者情報を偽った送信を行った場合には、1年以下の懲役または100万円以下の罰金というものも設けられております。

次のページを御覧ください。特電法に基づきます執行体制でございますけれども、迷惑メール相談センターというところでモニター受信機を設置しておりまして、迷惑メールを受信して分析しております。1年で70万件以上のメールをモニター受信機で受信しております。

また、迷惑メールを受信しました国民の皆様方から情報提供をいただいております。令和元年度ですと1750万件以上の情報を提供いただいております。また、電話相談もいただいております。2,600件以上の相談を令和元年度はいただいております。

これらの多くの情報を分析いたしまして、その結果につきまして、例えばアソシエーション参加事業者、これは迷惑メール対策ソフトベンダーなどがございますけれども、こちらに第三者への転

送に同意された一般の方からの迷惑メールを転送して、分析などをいただいております。これが令和元年度では約29万件行われております。

また、総務省、消費者庁が民間事業者による自主的なメール対策を促すために実施している迷惑メール追放支援プロジェクトに基づく対応依頼をISP事業者に6,000件以上行っております。これは具体的には迷惑メールの送信者を割り出しまして、この送信者は迷惑メールの送信者ですよとISP事業者にお知らせして、解約、利用停止などを行っていただくというものでございます。

それから、違反状況の報告は、警告などを作成いたしまして、6,000件以上、迷惑メール送信者に対して行っております。

また、海外執行機関とも協力をしておりまして、違反メールの情報提供を令和元年度は約10万件以上行っているということで、迷惑メールの防止に向けて幅広く活動を推進しているということです。

次に5ページを御覧ください。迷惑メールの撲滅を目指しまして、2008年以降、産官学の迷惑メール対策の関係者間で効果的な迷惑メール対策の推進を図ることを目的としまして、迷惑メール対策推進協議会を設置しまして、活動を推進しております。こちらにつきましては、構成員として電気通信事業者、広告事業者、セキュリティベンダー、学識経験者と共に、関係省庁として総務省、消費者庁、警察庁などが参加してきております。この中の技術ワーキングにおきまして、送信ドメイン認証技術も含めまして様々な最新技術の動向を検討した上で、普及に向けた活動などに取り組んでおります。

こちらのスライドにもございますように、毎年迷惑メール白書を出すとともに、送信ドメイン認証技術導入マニュアルを出しておりまして、また右側のブルーの冊子「電子メールのなりすまし対策～送信ドメイン認証でなりすましを防ぐ～」ということで、最新の情報について発信してきております。

スライドの6ページを御覧ください。こちらが送信ドメイン認証技術による技術的対応でございまして、迷惑メール送信者は受信者にメールを開いてもらうために、有名なサイトに見せかけたり、送信者を特定しづらくするためにドメインを詐称して送信することが多いということで、受信側でこの詐称を検出できるようにするために、送信ドメイン認証技術、先ほども御紹介がありましたSPFやDKIM、DMARCなどがございます。

こちらの送信ドメイン認証技術の導入をすることによりまして、認証結果を踏まえて詐称と判断されたメールは受信しないなどの対策を取ることが可能となっております。

こちらの図にありますのは、送信ドメイン認証技術のうちのSPFの概要でございます。例えば総務省のメールにつきまして、111.111.111.1というところから送りますということにつきまして、DNSサーバというところでSPFレコードを宣言しておきますと、今度迷惑メール送信事業者が総務省だと偽装して222.222.222.2という別のところからメールを送った場合には、受信側のメールサーバがDNSサーバに問合せをすることによって、これは総務省からのメールではありませんということで、送信者情報が詐称されているということを判断して受信者にお知らせすることが可能といった内容になっております。

7 ページを御覧ください。こちらが先ほど御紹介いたしました送信ドメイン認証技術のうち、SPFに対応しているメールがどの程度送信されているかということでございますが、85%以上のメールが現在、SPFに対応しているというデータでございます。

8 ページを御覧ください。2つ目の技術であるDKIMに対応しているメールの割合でございますが、こちらについては60%以上ということで、以前に比べて大分普及が進んできているということでございます。

9 ページ目から、迷惑メール対策に係る利用者の方々への周知啓発への取組でございます。こちらにございますように「撃退！迷惑メール」ということで分かりやすい冊子、詐欺メール対策のリーフレット「そのメール、詐欺カモ！？」といったものも発行しております、冊子としてお配りするとともに、ホームページにおいて全文を掲載しております。

10ページ目は「撃退！迷惑メール」からの抜粋でございます。警察庁などにも御協力をいただいております、令和時代の迷惑メール最新トレンドということで、トレンド1に、正に先ほどもデータがございましたけれども、フィッシングメールによる被害が拡大していますよということで、気づきをいただくように情報提供しております。

11ページ目からは具体例でございます、1つ目の例として偽のSMSで被害急増ということで、大手企業ブランドになりすましてやる手口がありますということを御紹介しております。

12ページ目でございますが、先ほども事例として御紹介がございましたが、大手宅配会社の不在通知を装ったSMSということで、漫画仕立てで絵も示して、注意を呼びかけて、相談窓口として消費者ホットラインやIPAの連絡先、各携帯電話事業者の連絡先なども掲載しております。

13ページ目が銀行になりすました詐欺（フィッシング）メールということで、あなたの預金が狙われていますよということで、こちらにも漫画で分かりやすく手口をお示しした上で、メールの特徴、対処法、相談窓口について分かりやすくお示しして、利用者の方々に気づきをいただくような形で周知をしております。

このように、総務省といたしましても、消費者庁、警察庁なども含めた関係省庁と連携をしながら、迷惑メール対策に一層取り組んで、送信ドメイン認証技術の導入率も高めていくとともに、消費者の方々への注意喚起を引き続き進めてまいりたいと思っております。

以上でございます。

○山本委員長 ありがとうございます。

それでは、御質問、御意見のある委員から御発言をお願いいたしますけれども、まず私から御質問をさせていただきます。

先ほど、フィッシング対策協議会から11ページで、スマートフォンについていろいろ対策が難しいというお話があったのですが、現時点で、スマートフォンを利用する場合に消費者としてどのような点に特に気をつければよいかという点と、今後どういった対策をスマートフォンについて推進していく必要があるかという点についてお伺いしたいです。

それから、総務省にお伺いしたいのですが、フィッシング対策協議会からDMARCの普及が重要であるというお話があったのですが、DMARCの普及状況に関しては現在どうなっているのです

ようか。

その点をそれぞれお伺いしたいと思います。

○フィッシング対策協議会佐々木様 まず、スマートフォンで、一般の利用者の対策という点でございますけれども、メールです。今日も各省庁の皆様から対策という部分で、いわゆる一般利用者の方々が送信元の詐称箇所を目視等で御覧いただいて気づくという対策を書かれておりましたけれども、スマートフォンの場合ですと、メールのメッセージとして表示される送信者名やメールアドレスといった情報が、いわゆるパソコンで表示する場合と異なっているケースが多くありますので、そういった際に目視での気づきという部分がなかなか難しい点がまず1点目としてございます。そういった中で、ほかにもあるのですが、簡単に言いますと気づきという部分で一般利用者の方が回避することは非常に難しいという点が取り上げられたと思います。

一方、対策の部分ですけれども、スマートフォンの場合ですと、近年では様々な銀行のアプリや金融アプリ、その他様々なオンラインサービスをアプリで使われるという方が多いと思います。そういった際に、例えば従前ですとなりすましメールが来て、メールに書かれているリンクをクリックしてしまって、不正サイトに誘導されるということが多いと思いますけれども、例えばアプリですと、そういったメールによる誤ったURLの誘導等が行われずに、ちゃんとオンラインサービス事業者側が提供するアクセス経路を通じて、正規のサービスにアクセスできるという点がありますので、正規アプリの利用を推進するという点で、スマートフォンにおけるフィッシングサイトへの誘導数をかなり減らすことができるのではないかと考えております。

一方で、まだ依然としてアプリの利用が進んでおらず、いわゆるメールで誘導されてくるリンクをクリックして、サービスに向かっていく、あるいは偽サイトに誘導されるというケースも多くございますので、その辺りは各オンラインサービス事業者様側のアプリの普及等の取組に期待したいところだと考えております。

○総務省小川消費者行政第二課長 総務省です。御質問ありがとうございます。

DMARCの普及状況については、現在、数%程度ということで、まだあまり高くないというのが現状でございます。しかしながら、DMARCにつきましては、導入の前提としてSPF・DKIMを導入した上でDMARCのポリシーを設定していくということになっておりますので、SPF、DKIMの普及率が高まってくることが大前提でございますので、そちらについて高めるとともに、DMARCについて導入が更に推進されるように、普及啓発などにつきまして、関係の機関とも協力しながら、一層取り組んでまいりたいと思っております。

以上です。

○山本委員長 ありがとうございました。

それでは、オンラインで参加をされている木村委員、丸山委員から御発言があるということで、まず木村委員からお願いします。

○木村委員 木村です。

デジタル化が進む中で、消費者が安全・安心に通信を利用できるようにこういった対策は本当に大切だと思いますし、何をどう気をつけるのかということを考えながら話を聞いていたのですけれ

ども、消費者に対する周知がまだ不足しているのではないかと考えております。

例えばオレオレ詐欺にしましても、これだけいろいろ周知されていますけれども、それでもまだまだ被害があるというところですので、今後どうしたら情報が消費者に届くのかというところをポイントに、是非周知をしていかなければいけないのではないかと考えています。

質問なのですけれども、フィッシング対策協議会の資料の11ページで、一番最初の段落なのですが、迅速にURLをレポートすることが重要というところの次なのですが、URLのフィルタリングサービスが海外サービスであるためというところで、もしかしたら説明されたかもしれないのですが聞き取れなくてすみません。国内サービスは今のところはないのかというところと、もう一点、黄色のところ、国内ブランドのフィッシングは登録されづらいというところなのですけれども、そこはなぜ難しいのかというところをもう少し詳しく教えていただきたいなと思います。

以上です。

○山本委員長 それでは、丸山委員、お願いします。

○丸山委員 丸山でございます。

1つは、フィッシング対策協議会もしくは総務省にお伺いしたいと思うのですけれども、恐らく私自身は、使っているメールサービス事業者は、個人的にも大学的にもあまり迷惑メールは届かないという状態になっております。お伺いしたい点としましては、利用を開始するときの迷惑メールなどのフィルタリングの強度のデフォルトを様々な業者に高めに設定していただくことは可能なのかどうかという点でございます。

恐らく利便性は下がるというか、普通のメールもプロモーションなどに分類されたりすることは起こってしまうのですけれども、感触としましては、迷惑メールが来ないほうが私としては良いという印象もございますので、そういったフィルタリングの強度のデフォルトを開始時に高めに設定するというのを日本としてやっていくということは、難しいことなのかどうなのかということをお伺いしたいと思いました。これが第1点です。

第2点としましては、警察庁にお伺いしたいのですけれども、被害に遭ってしまった消費者は非常にパニックに陥ったりすると思うのですが、現状におきまして、警察にまずは相談をするということで、現在は適切な行動を教えていただける状況になっているのかという点を教えていただければと思いました。警察に駆け込んだときにこうしたら良いよという初期の行動についてまでレクチャーいただけるような現況なのかという点を教えていただければと思います。

以上です。

○山本委員長 ありがとうございます。

それでは、お答えをいただけますでしょうか。

○フィッシング対策協議会佐々木様 まず、木村委員の御質問のフィルタリングサービスのところなのですけれども、資料の11ページ目の点になります。言葉足らずで失礼しました。

フィルタリングサービスなのですけれども、皆様が主に使われている部分につきましては、ウェブブラウザ、インターネットでウェブサイトを御覧になる際のブラウザに標準装備されている場合がございまして、アクセスしようとする警告表示が出て、ブロックされるといったものになってお

ります。

こちらは、御認識のとおりこういったブラウザのソフトウェアのほとんど海外メーカー様が製造されて、展開されているものですので、必然と海外側でのブラウザをつくっているメーカーなりプロバイダー側での対応ということになりますので、どうしても海外側で収集している情報を基にブロックをしていくということが量的に多くなっているという状況になっております。

フィルタリングサービスにつきましては、アンチウイルスソフトでブロックされたりするのですが、このほかにも、こういったフィルタリングに必要なブラックリスト的な情報を収集して、それぞれのソフトウェア等に提供するようなサービスもございます。こういったサービスの大半が、国内もあるのですが、量的には海外のセキュリティメーカー等が取り組まれていることが多いということで、必然的に、海外のフィッシングサイトがそういった情報を集めやすいということで、相対的に見ると日本固有のブランドをかたるフィッシングサイトは日本語が判らないと判別が難しいためブラックリスト入りしづらく、海外のフィッシングサイトがフィルタリングのブラックリスト入りしやすいという状況となっております。

当然、我々でもそういった海外側の様々なブラックリスト的なフィルタリングURLを集める活動との連携も取っているのですが、どうしてもブラックリストを実装する側、サービスとして提供する側は海外事業者が多いということで、記載したような状況となっております。

2点目の丸山委員からの御質問については、我々からではなく総務省からの御回答がよろしいかなと考えておりますが、よろしいでしょうか。

○山本委員長 それでは、総務省にお答えいただいて、それから警察庁にお答えいただくということにしましょうか。お願いします。

○総務省小川消費者行政第二課長 丸山委員から御質問いただきましたフィルタリングの話でございますけれども、提供主体が様々ございまして、通信事業者が提供している場合もございますし、セキュリティソフトの設定の場合もございますし、また、大学であったり、企業であったり、官庁であったり、所属されている団体におけるポリシーであったり、いろいろな場合があるかと思っております。必要なメールは届きながら、不要なメールが届かない、危険なメールが届かないというのが非常に重要な機能でございまして、様々な形で改善をされてきているものかと思っております。

このフィルタリングの強度については、基本的に選べるような形になるのが望ましいところとは思っております。そういう意味で、できるだけ迷惑メールが届かないような設定、強度の高いものが導入されていくことは望ましいと思っております。

○山本委員長 お願いします。

○警察庁加門官民連携推進官 警察庁でございます。

丸山委員から、警察における対応体制について御質問がございました。

サイバー犯罪につきましては、警察におきましても非常に重要な分野の一つということで取り組んでいるところでございます。現状、全国の都道府県警察におきまして、それぞれサイバー犯罪対策を担当するところが準備されております。また、都道府県警察には、サイバー犯罪専門の相談窓

口も設置しております。

警察への相談の窓口といたしましては、例えば警察署又は警察相談電話「＃9110」という窓口がございまして、専門部署と連携をいたしまして、対応しているところでございます。

以上でございます。

○山本委員長 ありがとうございます。

それでは、大石委員、柄澤委員、片山委員長代理、新川委員にもいただいておりますけれども、まず2人ずつにします。大石委員と柄澤委員、お願いします。

大石委員からお願いします。

○大石委員 大石です。質問させていただきます。

まず、資料1の9ページ、.の4番目には日本が遅れていると書いてありました。先ほどの木村委員の御質問にも関係するかと思うのですが、大手4社というのが一体どこなのかというのがもし分かれば教えていただきたいというのが1つです。

あと、経験的にAndroidとAppleではかなりフィルタリングの能力が違うということは、いろいろな情報で見聞きするわけですが、これは、個人が設定できるものなのかどうかというところでは、先ほどの総務省のお答えの中にもありましたが、私たちが携帯電話を契約するときに、その辺りの説明については十分ではないという面もあると思います。消費者が一体どこまで自分で予防というか防衛できるのかというところが分かりづらいと思うのですが、その辺りの事情を協会に消費者にお伝えいただいているということでしたら、是非御紹介いただきたいというのが1点です。

あと、警察庁で、サイバー犯罪について予防策はいろいろと書いていただいているのですが、サイバー防犯ボランティアという名称は今回初めて聞きました。8ページ、9ページ辺りの内容については、消費者に届いていないのではないかという疑問を持ちました。今後は、更にこのような取組や情報の必要性は増すと思います。なるべく多くの消費者、特にアクティブシニアと呼ばれる60代、70代、また80代の方たちにも届くような努力をお願いできればと思います。

以上です。

○山本委員長 それでは、柄澤委員、お願いします。

○柄澤委員 ありがとうございます。柄澤です。

御説明、ありがとうございました。

私からは、むしろ感想的なお話になると思いますが、非常にフィッシングの問題というのは、私どもは注視すべき課題であるということを十分認識できる御説明だったと思います。ありがとうございました。

まず、フィッシングの場合ですけれども、実在する事業者をかたって、利用者に本物のサイトと誤認させて、ID、パスワード等を入力させるフィッシングということにおきましては、事業者側ができることに一定限界があるなど。私どもも実はこの被害に遭っているわけですが、まず利用者本人がフィッシングに遭わないように注意いただく必要がある。このための継続的な注意喚起が極めて重要だと思います。

しかし、これが簡単なことではない。というのは、例えば私どもの会社におきましては、全社員

に継続的に標的型メール訓練を実施いたしまして、不審なメールに掲載されたURLをクリックしないよう指導するとともに、訓練用メールも送付しております。徐々に効果を上げてきておりますが、残念ながら一定の割合、2%ぐらいの割合でだまされて、クリックしてしまう状況が続いております。しかも上級者ほどクリックする比率が高いというのが憂慮すべき状況だと思っております。

また、フィッシングではなく、利用者が知らない間に被害に遭うケースにおきましては、事業者側の対策として、事業者が厳格に本人確認することによる「なりすまし」防止など、可能な被害防止策を講じる必要があると強く認識いたします。

万一、被害が発生した場合には、早急なお客様への連絡とか、被害拡大の防止とか、関係機関との密接な連携などを実施していくことになるのだろうなと思っております。

また、保険の観点でお話しいたしますと、事業者側にこのような利用者被害を補償する規約があれば、その規約に則って利用者への補償が行われ、また、その裏支えとしての保険も存在いたします。加えて、事業者が法律上の責任があれば、その賠償リスクを補償する保険も存在いたします。このような保険に加入いただくにあたっては、事業者側に不正使用検知システムの導入や保険料のリザルト・レーティングの実施等々によって、事業者側の注意喚起を高めていくインセンティブを図っているところでございます。

以上です。ありがとうございました。

○山本委員長 ありがとうございました。

それでは、それぞれお答えいただけますでしょうか。柄澤委員からは質問ではなくコメントということだったのですけれども、もし何か御発言がございましたら、併せてお願いしたいと思います。

それでは、協議会からお願いします。

○フィッシング対策協議会佐々木様 まず、大石委員の御質問の点でございますけれども、資料の9ページ目になりますが、我々の書きぶりが分かりづらくて大変失礼しました。

資料の3.目の部分にあります上位4ブランドという部分ですけれども、4社と申しますのは、なりすまされてしまっている大手カードブランド様ですとか、大手オンラインショッピングサービス様等のことを指しております。一方で、4.目の送信ドメイン認証等の導入が進んでいない側の事業者というのは、なりすまされる側ではなくて、メールの配信等を行っているプロバイダー様等になります。

導入が遅れているという部分なのですけれども、我々からも主観的な意味合いで書いてしまいましたが、全く後れを取っているというよりは、導入が正にこれから検討されているという部分かと存じ上げております。既にこういったプロバイダー様等、メールサービスを提供している事業者様でも、総務省と連携をして導入等の対策が進められてきているところだと思っております。

それが、海外に比べて相対的に少し遅れているのではないかと書かせていただきましたけれども、これにつきましては逆に言いますと、海外側のそういったメールサービスにつきましては、かなり強力な規約等の縛りによって、利用者の方が気づかないうちにと申しますか、最初の利用段階であまり意識せずに使っていると、実は裏側ではしっかりとフィルタリングブロックをしているという状態になっています。

例えばですけれども、千差万別あるとは思いますが、場合によっては、本来は届くべきメール等も誤ってブロックされるという事象も比較的多く発生している可能性もあると思いますので、そういった点では、先ほど総務省から御回答がありましたけれども、利用者の方が誤ってブロックされてしまう可能性等も含めて、そういった強力なフィルタリングサービスや認証サービスの利用を御理解いただいて、選択できるような仕組みについては、今後そういったプロバイダー等の皆様方の御議論とか、かなり念入りな準備等が必要だと思っておりますので、そういった点を我々としてもサポートさせていただきたいと考えております。

柄澤委員から御意見をいただきました部分ですけれども、簡単に弊センターからも感想になってしまいますが、御指摘のとおり、利用者被害が発生した場合の対応でございまして、フィッシング対策協議会にも、いわゆるなりすましをされてしまって、当該事業者のお客様が被害に遭ってしまうという部分について、大きな関心を寄せているといった動機で参加されている金融機関様やカード会社様等がたくさんいらっしゃいます。そういったときに、我々からも求めていますけれども、やはり一般利用者の方がフィッシングサイトを通じて情報を取られてしまうという部分の防御は、本日御説明させていただきましたとおり、非常に技術的には難しいところが多々ありますので、そういった場合ですと、現時点においては、残念ながら一次被害として情報が取られてしまった後の二次被害、不正送金やその他の金銭的な被害を速やかに防止する、場合によっては軽減策を講じるという部分についても、現時点においては各事業者様と共に取り組んでいきたいと考えておりますが、これについては我々や他の専門機関というよりは、なりすまし被害に遭ってしまった金融機関様やカード会社など様々なオンラインサービス事業者様で講じていただくべき点でございまして、そういった点については、社会全体のニーズとして推進を進めていただきたいと考えております。

○山本委員長 それでは、警察庁からお願いします。

○警察庁加門官民連携推進官 警察庁でございます。

大石委員から、サイバーの防犯に係る活動が消費者に十分に届いていないのではないか、また、サイバー防犯ボランティアを初めて聞いたという御指摘をいただきました。まず、サイバー防犯ボランティアについて御紹介いたしますと、サイバー防犯ボランティアの団体数の推移につきまして、平成24年4月には67団体であったものが、令和元年末には274団体になっております。活動している構成員の人数も、この間、3,440名から9,625名に増えているところでございます。活動の幅はこのように広がっているところでございます。

御指摘のとおり、現下、全ての方に届いていないということが事実であると思いますが、地道に取組を継続するとともに、様々な層に届くよう活動の拡大を図っていききたいと考えております。

以上でございます。

○山本委員長 それでは、総務省からお願いします。

○総務省小川消費者行政第二課長 柄澤委員からも、消費者が注意する必要があるという御指摘がございました。総務省といたしましても、もちろん迷惑メール対策を事業者、関係省庁としっかりと取り組むとともに、消費者に対する周知啓発に一層取り組んでまいりたいと思います。

○山本委員長 ありがとうございます。

それでは、片山委員長代理、お願いします。

○片山委員長代理 御説明ありがとうございました。

私からは2つ、1つ質問と1つお願いがあります。

まず質問ですけれども、こういうフィッシング被害に遭っている被害者の特性といったものの分析はなされていますでしょうか。1つ考えられるのは、スマートフォン等を利用しているけれども十分にその仕組みやリスクを理解できていない層、例えば高齢者の人たちが、特に気づきが遅れて被害に遭っている傾向が高いとか、そういうことがもし何らかのデータで分かれば教えていただきたいと思います。

それから、皆さんも指摘されているように、消費者が気づけるように効果的な警告、気づきを促すという啓発が一番大切だと思います。先ほど御紹介のありましたJC3の動画サイトだとか、ホームページでのいろいろな啓発がなされているようですが、そこに対するアクセス件数、利用状況が分かりますでしょうか。

JC3に限らずですが、いろいろなところで、ある意味ばらばらにそれぞれが啓発に努力をしておられるのだと思いますが、消費者が被害に遭ったときには大変なパニックになっていると思いますので、まず何をしたらいいか、どこにアクセスしたら良いかというふうに分かりやすく案内していくということも大切だと思います。

その辺で、今後の啓発の在り方として今、検討されているところがあれば、どなたからでも結構ですので御説明いただければと思います。よろしくお願いします。

○山本委員長 ありがとうございます。

それでは、新川委員、お願いします。

○新川委員 新川でございます。よろしくお願いいたします。

今日はありがとうございました。

1つお伺いしたかったのは、今回3者ともに、フィッシングもサイバー犯罪も、また迷惑メールも、いずれも海外事業者の関わりがあって、この辺りは国際的な枠組みというか、海外の規制機関あるいは関係機関との協調や連携など、それぞれ事業者への対応ということもあると思いますけれども、この辺りは何か共通の枠組みや考え方はあるのか、そしてそこでの取組の中で、今後対策が進んでいく可能性があるのかというのが1点お伺いしたかった点でございました。

2つ目は、国内での対策で、先ほど片山委員長代理からもございましたけれども、今日のお話のフィッシングにせよ、サイバー犯罪あるいは迷惑メールにしても重なっているところが相当ございます。この辺りは消費者向けの啓発だけではなくて、防止や具体的な事業者規制といったところ、3者間での連携、あるいはひょっとすると消費者庁も深く関わらざるを得ないのかもしれないのですが、この辺りの連携体制のようなものはどうなっているのか、あるいはどのような今後の考え方を持っておられるのか、お伺いしたかった。

以上2点でございます。よろしくお願いいたします。

○山本委員長 ありがとうございます。

それでは、それぞれお伺いします。先ほどJC3の話もありましたので、警察庁からまずお願いできますでしょうか。

○警察庁加門官民連携推進官 片山委員から、フィッシングの被害者の分析について御質問であります。被害者の分析は統計がございません。ただ、警察といたしましては、手口と被害の実態を把握しながら、被害防止対策、注意喚起等にしっかりとつなげていきたいと考えているところでございます。

以上でございます。

○山本委員長 それでは、協議会からお願いします。

○フィッシング対策協議会佐々木様 こういった被害者の方々ですけれども、実際に入力してしまった、あるいはおかしい送金等があったというような被害が出てしまった場合につきましては、各都道府県警様の窓口等に御相談に行かれることが多いかと思います。フィッシング対策協議会の窓口には寄せられる情報の大半が一般の利用者、いわゆる被害者の方々からだと申し上げましたが、この統計については正確に取ったものはないのですが、いわゆる最近量的に多いものとしましては、うちの窓口担当はアクティブシニア層と申し上げていますけれども、スマートフォンをそれなりに使いこなされている御高齢の方等を含めて、広い年代層の方から情報の提供をいただいております。こういった方々は被害に遭う一歩手前で御連絡いただいている方々ですので、いわゆる従前の我々を含めた警察庁、総務省等の普及啓発活動をどこかでお目にかかるなどして、そういった意識を高めていただいていたところ、そういったメールに気づいて、早急に情報提供に協力いただけたという方々だと思っております。

繰り返しですけれども、高齢者層の方々も多く含まれておりまして、その点についてはある程度の普及啓発を行うことで、年齢層関係なく、一定の気づき等につなげることは十分にできるのではないかと考えております。

あとは、新川委員の御指摘の国際枠組みの部分につきましても、警察庁からも資料がありましたが、我々からとしましても、従前から不審サイトのテイクダウン、実際の海外サーバ事業者等に調整等を行って、不正なサイトを止めるという作業につきましても、JPCERTコーディネーションセンターの従前からのサイバー攻撃対処の国際連携枠組みを活用しております。

これに加えまして、専門機関以外にも様々なサービス事業者も含まれておりますけれども、各海外当局、専門機関等が集まった国際的なフィッシング対策の枠組みに参加しまして、会合等も参加するのですけれども、従前からの情報連携等も行いまして、対策を進めているところでございます。

いずれにしても、状況は各国とも同じだと思っております。大量のメール配信をどうしていくかという部分、あるいは攻撃者が非常に素早くフィッシングサイトを設置して、もう数十時間で撤収するといった量的、スピード的な課題に対処するかという部分でお互いに各国間で頭を悩ませているところでございます。

○山本委員長 ありがとうございます。

それでは、総務省からお願いします。

○総務省小川消費者行政第二課長 総務省でございます。

まず1つ、啓発が非常に重要だということで、こちらについては警察庁、フィッシング対策協議会も含めて連携をして、今後も周知啓発をしていきたいと思っております。

また、迷惑メール対策推進協議会も総務省、消費者庁、警察庁も含んでおりまして、官だけでなく産官学連携しながら周知啓発をしていくことが重要だと思いますので、こういう枠組みを活用しながら、ネット、スマホ、様々な場面を含めて、情報を今後も周知啓発していきたいと思っております。

また、海外の当局との協力でございますが、迷惑メール対策というとやはり海外から送信されるものが多くございますので、海外執行機関との連携、協力というのは非常に重要でございます、こちらについては覚書を結ぶ等して取り組んできております。違反メールの情報提供についても、先ほども御紹介しましたが、令和元年度も10万件以上ということで、こちらについては海外の執行機関とも国際的な枠組み、それから2国間でも連携をしているところでございまして、こういう取組を今後も進めてまいりたいと思っております。

以上でございます。

○山本委員長 ありがとうございます。

それでは、よろしいでしょうか。

本日は、御説明、そして御回答をいただきまして、どうもありがとうございました。コロナ禍等の社会情勢やパソコン・スマートフォンに触れる機会が増えつつある中、このようなフィッシングに係る被害が更に拡大しないように、改めて関係行政機関の対応や取組を促進し、また消費者への注意喚起や対策等の周知を強化する必要があると考えております。

対策として、いろいろな局面における対策があるということが、本日のそれぞれの御説明からよく理解できましたし、現状及びこれからの課題という点についても、それぞれいろいろな御指摘をいただきました。

消費者委員会といたしましては、本日のヒアリング結果も含めまして、引き続き関係行政機関の対応や取組状況を精査し、必要に応じて何らかの意見表明を行うということも含めて、調査審議を行ってまいりたいと思います。

それでは、本日はフィッシング対策協議会、警察庁、総務省、消費者庁におかれましては、お忙しいところ審議に御協力いただき、ありがとうございました。

それでは、ここで5分間の休憩といたします。再開は11時25分といたします。

(警察庁、総務省、消費者庁、フィッシング対策協議会 退室)

(休 憩)

《3. 消費者委員会ワーキング・グループ設置・運営規程改正》

○山本委員長 そろそろ11時25分ですので、再開をいたします。

次の議題ですが、消費者委員会ワーキング・グループ設置・運営規程の改正についてです。

第5次消費者委員会では、消費者法分野におけるルール形成の在り方等検討ワーキング・グループを設置し、同ワーキング・グループにおいて、取引分野に係る消費者法のルール形成の在り方や実効性確保のための方策などについて検討し、ルール及び担い手のベストミックス等の観点を示した報告書をまとめました。

その後、第6次消費者委員会において、委員の間で議論した結果、同ワーキング・グループの報告書で示された観点の重要性に鑑み、更に深掘りをして検討することが必要ではないかという結論に至りました。

そこで、第6次消費者委員会において、同ワーキング・グループの活動を再開し、具体的な検討を行いたいと思います。これに伴い、消費者委員会ワーキング・グループ設置・運営規程を改正する必要がありますので、同規程の改正案の内容について、事務局より5分程度で御説明をお願いいたします。

○太田参事官 事務局参事官の太田でございます。

資料4-1が消費者委員会ワーキング・グループ設置・運営規程の改正案でございますが、その内容につきまして御説明させていただきます。

具体的には、もう一つ資料4-2という形で新旧対照表をおつけしております。分かりやすさのために、そちらで御説明させていただきたいと思います。

資料4-2の左側が現行の規程、右側が改正案となっております。

改正のポイントは主に2つございまして、まず1つ目は、会議に出席することができるオブザーバー、参考人に関する規定を少し変更するというところでございます。

もう一つは、第6次消費者委員会といたしまして、このルール形成ワーキング・グループを再開することに伴う更新ということでございます。

まず、オブザーバー、参考人に関する規定の整備でございますが、資料4-2の1ページ目、第5条第4項がオブザーバーに関する規定、第5条の第5項が参考人に関する規定でございます。変更点は2つございまして、1つ目は、それぞれについて対象を拡大するというところでございます。専門的な知見を幅広く調査審議の場に取り入れるという観点から、いずれも臨時委員、専門委員、行政機関職員、当該会議における調査審議事項に関して識見を有する者を広く対象とできるように改めたということでございます。

2つ目は、オブザーバーと参考人とがあるわけでございますけれども、それぞれの役割について明確化を図ったということでございます。オブザーバーにつきましては、継続的に参画いただく場合も含むといった形にしまして、その際、単に説明していただくということだけではなくて、意見を述べていただくことができるということも含めてございます。

他方、参考人につきましては、座長が会議の各回の調査審議事項等に関する説明を得る必要があると認めたときに、求められた事項について説明をしていただくということで、その点で両者が異なるということでございます。

次に、第6次での再開に伴う更新ということでございますが、資料4-2の3ページ目の別紙を

御覧いただければと思います。名称につきましては変更ございませんが、目的のところは若干表現ぶりを変更してございます。

大きく変わっているのが構成員のところでございますけれども、第5次と第6次で委員が替わっているということでございまして、山本委員長は前期に引き続きの御参加でございますが、第6次になったことに伴いまして、片山委員、新川委員、丸山委員を構成員として追加しているということでございます。

座長と座長代理につきましては、委員長の御指名によりまして、座長を丸山委員、座長代理を新川委員をお願いしているところでございます。

御説明は以上でございます。

○山本委員長 ありがとうございます。

それでは、御質問、御意見のある方はお願いいたします。いかがでしょうか。

特によろしいでしょうか。

それでは、本ワーキング・グループの再開と設置規程の改正につきまして、このようにさせていただければと思いますがよろしいでしょうか。いかがでしょうか。

結構ですというメッセージがございました。

それでは、皆様の御了解をいただいたということで、規程について原案どおり改正をし、本ワーキング・グループを再開したいと思います。

それでは、事務局におかれましては、本ワーキング・グループの開催に向けて手続を進めていただきたいと思います。

なお、既に大石委員及び柄澤委員より、本ワーキング・グループが正式に開催されることとなった場合には、オブザーバーとして御参画をいただけるとの御意向を伺っております。お二方におかれましても、よろしくお願いいたします。

続きまして、その他といたしまして、新開発食品調査部会から報告事項があります。受田部会長からお願いいたします。

○受田委員 よろしくをお願いいたします。

それでは、特定保健用食品の表示許可に係る答申について、私から御報告をさせていただきます。

令和2年7月9日に開催した第53回新開発食品調査部会及び同年8月31日に開催した第54回新開発食品調査部会の議決について、新開発食品調査部会設置・運営規程第7条に基づき、委員長の同意を得て委員会の議決とし、10月8日付け及び10月29日付けで内閣総理大臣へ答申を行いました。

参考資料1及び2の答申書を御覧ください。記載の品目について内閣総理大臣より諮問を受け、それぞれ第53回及び第54回新開発食品調査部会において安全性及び効果について審議を行った結果、指摘事項を確認の上了承することが部会長に一任され、申請者からの解答書を確認し、特定保健用食品として認めることといたしました。

私からの報告は以上でございます。

○山本委員長 ありがとうございます。

それでは次に、消費者委員会に寄せられた意見等の概況につきまして、事務局より報告をいた

きたいと思います。

○太田参事官 参考資料3をおつけしておりますけれども、四半期に1回ごとに行っております消費者委員会に寄せられた要望書、意見書等の一覧でございまして、今回御報告いたしますのは、今年7月から9月分ということでございます。

この間寄せられた意見書等につきましては19件でございます。それぞれ分野ごとにまとめてございますけれども、最初、取引・契約関係といたしましては8件でございまして、上から6つぐらいが、当委員会でも意見をまとめていただきましたネットにおける定期購入契約に係るトラブルへの対応についての御意見でございます。消費者団体、弁護士会などから複数御意見が寄せられているということでございまして、被害への迅速な対応や必要な法改正、消費者への啓発といったことを行ってほしいという御意見でございます。

1 ページ目の一番下から次のページにかけまして、当委員会でもヒアリングを行いました消費者庁の特商法と預託法の検討委員会の件でございますけれども、そちらについても御意見を2つほどいただいております。必要な法改正等を速やかに行ってほしいといった趣旨の御意見でございます。

2 ページ目に参りまして、安全関係で1件いただいております、新型コロナの関係で、アビガンの関係でございます。

その下、地方消費者行政の関係で5件いただいております、いずれも地方消費者行政専門調査会におきまして報告書の骨子をまとめていただきましたけれども、それに対する御意見でございまして、更に審議を深めてほしいといった趣旨の内容となっております。

これらいただいた御意見を踏まえまして、専門調査会でも更に御議論いただきまして、報告書を取りまとめていただいたということかと理解しております。

3 ページ目に参りまして、公益通報関係で1件いただいております、こちらは公益通報者保護法が改正されまして、いろいろ関係法令の整備などを進めているところでございますけれども、実効性のあるような制度整備を行ってほしいといった内容でございます。

次に、料金・物価関係ということで2件ございまして、いずれも電力改革の関係でございます。容量市場の見直しや賠償負担金・廃炉円滑化負担金の託送料金の参入に関する御意見でございます。

更にその下、集团的消費者被害救済制度についても1件いただいております、いわゆる施行3年後の見直しということで、それぞれ必要な見直しを行ってほしいといった御意見でございます。

その他として、国民生活基礎調査の継続といったところについても御意見をいただいているところでございます。

御説明は以上でございます。

○山本委員長 ありがとうございます。

それでは、ただいまの説明につきまして、御意見等がある方は発言をお願いします。

清水委員から発言があるとのことですので、お願いします。

○清水委員 ありがとうございます。

今の意見なのですが、地方消費者行政の部分で骨子への意見が出ています。また、8月には報告書が公表されまして、地方の消費者行政の現場では、この報告書に動揺を受けています。消費者委

員会としては、コロナ禍ですけれども、もう少し現場と対話する必要があると思いました。特に、以前の建議ではPIO-NET、全国消費生活情報ネットワークシステムの入力に係る費用負担については国が一定の費用を持つべきとの建議が出ているのに、今回の報告書には、例えば整合性がないという意見をいただいております。

消費者庁は各地方に部局を持っていません。このまま地方消費者行政が衰退すれば、国の消費者行政が衰退します。そういう意味からすると、この報告書を生かすためにも、誤解のないようにきちんと説明をする場を設けるべきだと思いました。

以上です。

○山本委員長 ありがとうございます。

その他にいかがでしょうか。よろしいでしょうか。

○太田参事官 先ほどの清水委員の御指摘へのコメントをさせていただきます。

8月に報告書を取りまとめていただきまして、意見ということで消費者庁に対して発出しておりますけれども、事務局といたしましても、それを出しっ放しということではなくて、地方の現場の皆様積極的に御説明をしていきたいと考えております。その取組の一環といたしまして、秋から冬にかけて、消費者庁におきまして各地方ブロックにおいて地方消費者行政のブロック会議を開催しております。そちらに私ども事務局としましても参加をさせていただいて、この報告書の内容につきまして御説明をさせていただき、各地方の現場の皆様と意見交換をさせていただきたいと考えております。

また、その後も必要に応じてフォローアップなどを行っていくという形で、この報告書の趣旨の浸透を図っていきたいと考えているところでございます。

以上でございます。

○山本委員長 ありがとうございます。

ただいま御説明がございましたように、委員会としてもこれから関係団体、関係機関とよく連携を取り、また、そこコミュニケーションを取って進めていきたいと考えております。

とりわけ、この地方消費者行政の問題に関しましては、その場でも私自身も申しましたけれども、これを使って議論をしていただきたいという趣旨でございます。2040年を見据えてという趣旨の報告書でして、中長期的な観点から報告書を作成しています。それから、地方それぞれの事情もございます。したがって、必ずこのようにするべきであると言っているわけではなく、このような可能性があるということを挙げた上で、関係団体あるいは関係機関でこれからよくそのことを意識していただいて、議論をしていただく必要があるという趣旨の報告書でございます。したがって、消費者委員会としても、これから報告書を基にして関係諸方面と議論していくことができればと考えております。

私もこれから今日の午後、その関係のことがあるのですけれども、そういう形でコミュニケーションを取っていただければと思っております。

新川委員から御発言があるとのことですので、お願いします。

○新川委員 新川でございます。ありがとうございます。

今の山本委員長のお話と同趣旨のことをお話ししないといけないかなと思っておりました。私自身もこの報告書を契機に、幾つかこの内容について別の機会にお話をさせていただく機会がありました。将来に向けてこれをどのように進めていくのかということについて、皆様方の御関心が高いということもよく分かりました。

是非、消費者委員会としても、この報告書の趣旨や内容、将来の展望やそれに向けての次の一手といったところについて皆様方と御議論をし、よりよい地方消費者行政、そして国全体としての消費者行政の進展に努めてまいりたいと思いますので、是非消費者委員会としても積極的に関わっていくということで、進めさせていただければと思っていた次第です。

以上です。

○山本委員長 大石委員から御発言があるとのことですので、お願いします。

○大石委員 ありがとうございます。

今のお話に関連してご紹介しますが、やはり私どもの団体でも、今回の地方消費者行政に関する取りまとめに対して、地方支部の会員をはじめ大変関心が高いということで、消費者委員会の事務局の方には御足労いただきますけれども、NACSで報告書の説明会を開いていただいて意見交換ができればと思っております。

新型コロナウイルスの影響でなかなか集まらない時期ではありますが、ウェブを使えばいろいろなところで意見交換もできると思います。まず今回どのような形になるか、まずはやってみようということで開催しますけれども、地方消費者行政の問題に限らず、その他の課題についても、ウェブを使って消費者の意見を聴くことはできると思います。消費者委員会としても、内側だけの話ではなく、是非積極的にウェブの会議などのシステムを利用して、いろいろ外からの声を聴くことが必要かなと思っています。

以上です。

○山本委員長 ありがとうございます。

ほかはよろしいでしょうか。

委員会に寄せられた意見書、要望書等につきましては、今後とも全委員で情報共有するとともに、定期的に委員間で意見交換を行う機会をつくっていきたいと思いますので、よろしく願いいたします。

《 4. 閉会 》

○山本委員長 本日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説明をお願いいたします。

○太田参事官 本日も長時間にわたりまして、熱心に御議論いただきまして、ありがとうございます。

次回の本会議につきましては、日程が決まり次第、委員会のホームページを通じてお知らせいたします。

以上でございます。

○山本委員長 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。