不適正利用対策に関するワーキンググループ（第２回）

令和６年３月14日

【小澤利用環境課課長補佐】　時間になりましたので、始めたいと思います。

改めまして、本日は皆様、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す。不適正利用対策に関するワーキンググループ第２回会合を開催いたします。事務局の小澤でございます。よろしくお願いいたします。

毎度の御案内でございますが、ウェブ会議の開催上の注意事項について御案内をさせていただきます。

本日、会合の傍聴者につきましては、ウェブ会議システムによる音声及び資料投影のみでの傍聴とさせていただいております。事務局において傍聴者の方は発言ができないように設定させていただいておりますので、設定を変更しないようにお願いいたします。また、本日の会合につきましては、記録のために録画をさせていただきます。

次、構成員の方におかれましては、ハウリングや雑音混入防止のため、発言時以外はマイクをミュートにしていただきまして、映像もオフにしていただきますようお願いいたします。御発言を希望される際は、事前にチャット欄に発言されたい旨を書き込んでいただき、それを見て座長から御指名の後、御発言をお願いしたいと思っております。発言の際にはマイクをオンにして、映像もできればオンにしていただいて、御発言をお願いします。発言が終わりましたら、いずれもオフに戻してください。また、接続に不具合が出ました場合については、速やかに再接続を試していただくようにお願いいたします。その他、随時チャット機能等で事務局宛てに連絡いただければ対応いたしますので、よろしくお願いいたします。

資料の確認について、本日、事前に配付いたしておりますとおり、議事次第と資料２－１から２－５までの５つになっております。

注意事項は以上になります。

それでは、早速、議事に入りたいと思います。これ以降、議事の進行につきましては、大谷先生にお願いしたいと思います。よろしくお願いします。

【大谷主査】　大谷でございます。それでは、今日の議事の最初に、SMS対策に関する関係者からのヒアリングを実施させていただきます。本日は、まずドコモ様、KDDI、ソフトバンクの３社と、それから警察庁から迷惑SMS対策の取組の状況について御説明いただ

きまして、その後に質疑応答の時間を設けたいと思います。その後で事務局からの御説明という段取りで進めさせていただきたいと思います。本日は質疑と意見交換の時間を十分にとりたいと思っておりますので、各自10分程度で御説明くださるようにお願いいたします。

それでは、まずはNTTドコモの大橋様、御説明をお願いいたします。

【株式会社NTTドコモ】　NTTドコモの大橋でございます。では、お手元、資料２－１に基づきまして、当社の発表をさせていただきます。１ページを御覧ください。本日はこちらの４点について御説明させていただきます。

２ページを御覧ください。フィッシングSMSに関するお客様からの申告の状況をお示ししております。件数については構成員限りということで御容赦いただければと思いますが、2020年頃より増加傾向が続いている状況となっておりまして、対策も打っておりますが、迷惑メッセージの多様化、巧妙化が激しく、申告者の増加が続いている状況でございます。

ここから対策についての御紹介でございます。まず機能面になりますが、危険SMS拒否設定を2022年、おととしから提供しております。こちらはURLや電話番号、発信者などの情報から総合的にフィッシングSMSと判定したものをブロックするものでありまして、こちらは包括同意という形で、申込み不要で提供をしているところでございます。拒否を希望しない方はオプトアウトで設定いただくことが可能となってございます。

５ページでございます。こちらはオプトアウト手順の画面を御紹介したものでございます。

６ページでございます。ブロックの件数でございます。左側に構成員限りで件数をお示ししておりますが、非常に多くの件数がこちらで検知され、ブロックをしているという状況でございますが、検索についてもなだらかに上昇傾向にあると考えております。

７ページでございます。こちらはプラスメッセージという携帯キャリア各社が共通で提供しているサービスにおいても、迷惑メールのフィルタリング、ブロックの機能を提供しているところでございます。

８ページでございます。企業でSMSを配信される場合に、迷惑SMSとして判定されないように、４キャリア共通の番号を付与するという、共通ショートコードを御用意しております。0005から始まる８桁から10桁の番号でございまして、こちらの付与に当たっては、一定の審査を経て送っていただいておりますので、共通ショートコードが付いたSMSは正規メッセージとして判別をすることを行っております。

続きまして、９ページ以降でお客様への注意喚起、周知啓発の取組について御紹介いたします。

まず10ページ、こちらは月並みになりますけれども、フィッシング詐欺に関する注意喚起ということで、ホームページなどを用いて事例の御紹介なども行っているところでございます。

11ページでございます。こちらは個別の注意喚起になりますけれども、例えばマルウェアに感染してしまったお客様、このマルウェアがお客様の端末を発射台にしてSMSを大量送信するようなケースがありますけれども、こういった状況が検知された場合には、該当のお客様に個別にSMSをお送りして注意喚起をすることを行っているところでございます。

12ページでございます。事業者、関係機関との連携の取組について御紹介をいたします。

13ページでございます。危険SMSに関する情報を、一定の匿名化加工を行った後に事業者間で情報共有をいたしまして、拒否する際の検知の精度向上に活用しているという取組でございます。

14ページでございます。こちらはスライド全体をマスクさせていただいており恐縮でございますが、関係機関との情報連携も行っているというところでございます。

15ページでございます。迷惑SMSを送信している方に対しては、申告情報などに基づきまして一定程度判断される場合には、利用停止や契約解除などの措置を講じているところでございます。

また、16ページからになりますが、被害に遭われた方への救済対応も行っております。

17ページでございます。先ほど御説明したとおり、マルウェア感染によりまして、お客様の端末自体が踏み台となってSMSの大量送信が行われた場合には、お客様に対してSMS通信料金が高額請求になる事例が散見されております。こういった場合については、送信自体は正規に行われているものになりますけれども、マルウェア感染等の状況をお伺いして総合的に判断した結果、お客様に対してSMSの通信料金を減算する、お返しするという対応を行っております。直近で始めたものとなりますので、まだ件数自体は多くありませんけれども、こういった被害救済の取組も始めているところでございます。

19ページ、まとめでございます。これまでの繰り返しになりますけれども、まず機能面においては、危険SMS拒否設定をはじめとする様々な対策機能を提供しております。また、お客様に対しては注意喚起などの取組を行っております。関係事業者間との連携によりまして、対策の精度向上などの取組を行っているところになっております。また、被害に遭

われたお客様に対する特別対応なども行っているところでございます。

フィッシングSMSにつきましては、常に巧妙化、多様化しておりまして、非常に変化をしているというところでありますので、通信事業者もそれに合わせて対策強化を続けていくところになりますけれども、お客様自身による対策の実施、セキュリティーソフトのインストールなども含めて、リテラシーの向上に向けた取組というのが不可欠ではないかと考えているところでございます。

当社からの発表は以上でございます。

【大谷主査】　ありがとうございました。

それでは続きまして、KDDI様から御説明をお願いいたします。

【KDDI株式会社】　KDDI、小頭と申します。資料の番号は２－２となりまして、KDDIより御説明させていただきます。よろしくお願いします。

本日の内容でございます。私からの御説明は、SMS単独の迷惑対策のみではなく、電話番号を使ったメッセージングサービス、こちら資料中では電番メッセージと表現させていただいておりますが、こちらの話をさせていただきます。流れとしては、まず迷惑対策に入る前に電番メッセージのサービスや市場、全体像がどうなっているのかというのを説明しまして、その後、各対策の全体像、現状と今後という御説明になります。

また１点補足させていただくと、先ほどNTTドコモ様から御説明いただいた内容、この後ソフトバンク様から御説明いただく内容を含めて、本日、携帯電話キャリア３社集まっておりますが、同じような内容を３回、構成員の皆様、事務局の皆さんに御説明すると内容重複がありもったいないと思いまして、事前に３社で意識合せみたいなことをさせていただいております。その上で、各個別の対策については、多少の濃淡ですとか凸凹はあろうとも、ほぼ３社とも違いなく機能を提供しておりまして、３社それぞれ違った観点で御説明させていただくことで、いろいろな角度、観点からの情報であったり、幅広い情報を共有できればと思って構成しております。

では、中身に移ります。３枚目、電番メッセージのB２C配信という内容でございます。先ほどNTTドコモ様から説明もあったように、２種類のサービスというか機能が、電話番号を使ったB２Cの配信というものでございまして、まずスマホを持つ原則全ての人に届くSMSというものと、画像やファイル送信などをリッチに送れるプラスメッセージ、ないしは技術的にはRCSと呼ばれているものがございます。こちらが企業様ですとか自治体様から生活者、消費者、エンドユーザーに向けて、電話番号を使って送れるというサービスで

ございます。

この電番メッセージの市場規模でございますけれども、世界的な市場規模は２～３兆円と言われております。どういった状況かといいますと、全てのスマホ宛てに送れるので、海外ではB２Cメッセージの主媒体として使われております。皆様も御利用いただいていると思いますが、例えばアプリケーションサービスの２段階認証、ワンタイムパスワードと呼ばれる数字を入れたり、あるいは最近ですと歯医者さんの予約ですとか、宅配便の連絡、クーポンの配信など、いろいろな用途で使われておりまして、日本の市場規模は、昨年度のものでございますけども、2022年度で約200億円と呼ばれています。

日本の市場規模は海外に比べてまだ、人口や経済規模から比較すると全然小さくて、さらなる成長の余地がありまして、ここ数年におきましても、2018年度からの比較で、約４年で５倍の市場規模に成長しているという状況でございます。実際にどのようなユースケース、業種で使われているかといいますと、先ほど申し上げたアプリやサービスの認証と重要なお知らせ、予約、督促などの業務連絡用途がメインで近年、増加しています。業種で言いますと、我々のような携帯電話事業者をはじめとした情報通信をはじめ、不動産、医療、金融、ないしは自治体様もはじめ、いろいろな幅広い用途が広がっているというところでございます。

この件に関して、要するにということで一度、まとめさせていただくと、SMSが非常に手軽で便利だから使われているところもあります。電話番号さえ分かれば送れる、配信の許諾は必要ですけれども送れるというところと、テキスト文章のみですのでよくも悪くもシンプルに送れるというところと、携帯電話ないしは携帯電話番号というのは、通信キャリアが回線をお渡しする際に本人確認を実施しておりますので、本人性が比較的高いというところから、市場においては便利でコスパもよいのでたくさん使われていて、先ほど申し上げたとおり市場成長が続いているというところですが、他方で送信元のなりすましであったり、電話番号だけで勝手に送れる、言い換えると便利で伸びているからこそ悪用も増えているという、市場全体の状況かと思います。

次に、ではそういった迷惑対策について何をしているのかというところで、こちらはもう皆様御存じのとおりなので一部省略しますが、基本的にお客様からの申告や同意をいただくことによって対策可能な状態になっておりまして、先ほどNTTドコモ様、この後ソフトバンク様から説明いただく内容も、基本的にはこの３つの種別に大別されるかと思います。業務的な対策、アプリでの対策、ネットワークでの対策でございます。

では、次にネットワークでの対策です。こちらはKDDIもドコモ様もソフトバンク様も同様の、ネットワーク側でのフィルターというものを導入しておりまして、通信キャリア側の設備で内容を分析して、迷惑と判定したSMSを事前にブロックする。全てのお客様にデフォルトを無償で提供しているという状況でございます。迷惑SMSの状態も日々変化、進化しておりますので、毎日のようにフィルターをチューニングしながら運用改善して、お客様を守りつつ、SMSという通信媒体の価値も守っているという状況でございます。

あくまでも事例になりますが、KDDIのお客様からいただく迷惑申告数としては、例えば2023年度のピークにおいては前年度比約３倍に増加しておりますが、フィルターのチューニングですとか効果の影響で３分の１程度まで戻っているという状況も、分析しております。

次に、アプリでの対策でございます。こちらはいろいろな各社対策を講じているんですが、こちらを大別すると無料汎用の対策と有料個別の対策というものがございます。先ほど申し上げたネットワーク側での対策では、いろいろ通信の秘密ですとかお客様の不利益回避の観点から、完全には防ぎ切れないという課題がありまして、ではお客様の手元の端末、ないしアプリケーション側で出し分け表示をしてお客様を保護するということに取り組んでおります。

この後も補足しますが、無料のものはアプリケーション側でホワイトな送信と身元が明らかなものを明示するというもので、有料個別のものは逆にブラックな送信元を独自の迷惑判定を使ってブロックしたり非表示にするというところで、出し分けを行ったという。あくまでも事例ですけれども、プラスメッセージというアプリを使ったお客様の見た目としては、ホワイトのものは例えば連絡先登録済み、ブラックであるものは迷惑メッセージというタブ分けですね、eメールですとフォルダー分けみたいになると思いますけれども、それのSMS版というところで御理解いただけるかと思います。なかなか判別できないものはグレーとして、不明な差出人というような見せ方をしております。

企業様、自治体様が使うＢ２Ｃにおいては、先ほどドコモ様から御説明のあったSMS共通番号というものを使っておりまして、事前に各社が審査をしておりますので、この番号から配信されたメッセージは安心ですよというところを表示させていただいております。

これからが、プラスメッセージというアプリ、ないしはサービスでの見え方でございます。先ほどの共通番号はSMSを対象としておりますが、プラスメッセージは公式アカウントというものを用意しておりまして、こちらも同様に事前に携帯３社が企業様、自治体様

を審査しまして、安心安全な送信元として証明している形になりまして、お客様が手元で使っているアプリケーションにおいて、ロゴですとかチェックマーク、認証マークを表示して、安心ですよということを表示しているという状況です。

このSMS共通番号とプラスメッセージの公式アカウント、我々のほうで生活者、消費者に対して定性調査を実施していまして、結論を言うとアイコン、画像とかチェックマークがある公式アカウントのほうが安心ですが、SMS共通番号だけだとこの番号自体が何か分からないところがありまして、公式アカウントのほうがよりよいであろうと考えております。

そういったこともありますことから、このアプリケーションにおいてSMS共通番号とプラスメッセージ、プラメの公式アカウントをひもづけるという機能を、我々のほうで入れておりまして、そうすることで実際のメッセージ媒体としたSMS共通番号で送られているけれども、我々のアプリケーションのほうで特別な処理をいたしまして、同一の共通番号で特定の企業様を指していると、示しているという状況であれば、共通番号の電話番号の羅列ではなくてロゴですとかチェックマークを表示して、より生活者、エンドユーザーにとって安心できるような環境を対策しております。

通信キャリア各社においてネットワーク側の対策ですとかアプリ側の対策、いろいろやっておりますが、それぞれにおいて濃淡ですとか長所短所がありますので、組合せでいろいろお客様、市場を保護する形で対策をさせていただいております。我々の思いとしては、電話番号というのが非常に貴重なID、便利なものになっておりますので、B側、ビジネス側もC側、コンシューマー側も安心安全につながる世界へというところで、いろいろ対策をさせていただいている次第です。

以上でございます。

【大谷主査】　KDDIの小頭様、どうもありがとうございました。

それでは続きまして、ソフトバンク様、御用意よろしいでしょうか。

【ソフトバンク株式会社】　ソフトバンク松崎から御説明させていただきます。資料２－３になります。

ソフトバンクからは、先ほどKDDI小頭様から御説明があったように、ソフトバンクからは迷惑SMSの動向について御説明させていただきます。ここは我々の対策なので、飛ばさせていただきます。まず、我々ソフトバンクとしてURLで、まずはブロックを開始しました。昨年、ブロックする要素を増やしまして、拡張して、SMSのブロックをしております。

判定要素を追加することで、効果を上げて、継続して今ブロックしている形になっております。

ここから、携帯事業者側で観測されているマルウェアについて御説明させていただきます。日本で見られているのがこの２つ、赤枠で囲っているマルウェアになっております。このマルウェアの特徴として、迷惑SMSを不特定多数に送信してしまうような形になっているマルウェアをダウンロードさせて誘導するものと、あとは端末によってフィッシングサイトへ誘導するものと、この２つが見られるのが特徴となっております。

先ほどのMoqHaoというものとKeepSpyというものは観測されていまして、このMoqHaoというのが主にお昼頃配信されていて、内容が宅配を騙っているものが中心になっております。KeepSpyというものは夕方配信されていて、ここがいろいろなものを騙っている、銀行だったり通信事業者を騙っているものが見られています。特徴として、本文とURLがプラスされているというのが特徴になっております。これが昨年の４月の段階で、こういう形になっておりました。

ここが、昨年10月になると、もともとSMS１通で送られていたものが、本文とURLを分けて２通で送っているような形で、SMS、スミッシングが送られていました。ここは、各事業者がいろいろ対策しているのを回避しているのではないかと思っております。ただ、これがまた２通で送ってしまうと、１日の送信数は限られていますのであまり送れないと気づいたのか、また１通に戻っております。現状は１通になっているのですが、本文の内容が多彩な内容になっていて、簡単に止められないような形が見られております。もう一つのKeepSpyというものが、もともと夕方しか配信されていなかったのが、朝方に配信されるのが時々見られます。その内容が、大体銀行系だったり金融系のもので、寝起きで焦ってリンクを踏んでしまうようなものを狙っているのか、朝方送られたり夕方送られたりというのが見られるようになっています。これはさらに分析をしていきます。

ここは、我々が受信しているSMSの総数の中で不正アプリがどれだけ含まれているかという、割合だけを出したものになっています。全体から見ると少し、割合としては少ないものですけれども、URLつきのSMSの中では半分以上を示すような形になっていました。これは昨年の４月の段階です。これが10月以降になると、今年の２月にも割合を見てみたのですけれども、イベントによるショップの期間とか、そういう正しいSMSが増えているということもありまして、不正アプリからの割合は少し減っているような形になっています。ただ、割合としては減って、送信数としてはあまり変化がありませんでした。今年の２月

に見たところは、送信数の割合は変化がないんですけれども、送信数としては少し増えているようなものが見られています。

ここは、不正アプリからの送信状況を確認しているところ、昨年の４月では大体4,000番台ぐらいからこの不正アプリというのが送られていて、少し送信数も多いものになっていました。これが10月の段階だとちょっと感染端末が増えている状況になっていて、１台の送信数というのは少し減っている。それで、ユーザーに気づきにくいような状態が続いているような形になっていました。

これが先ほどの10月。２月に１回計測したところ、少し送信の感染端末は減っているような形になっていました。減っていたのですけれども、送信数のほうが増えるような、50通を超えるようなのが10月からは増えているような形になっていますので、全体の送信数は変わらず。端末のほうは少し減ってはいるんですけれども、増加しているように見られています。

これが、先月ソフトバンクを騙るものがすごく多かったので、そこだけをピックアップしてみました。そうすると、ソフトバンク側でブロックをしたタイミングで本文がころころと変わるような観測がされていまして、ブロックされているというのを検知してなのか、パターンを変えて、この４パターンで送られてきて、止めた以降はソフトバンク騙りはなくなったんですけれども、こういう形で見られます。なので、推測ですけれども、ブロック、止められたというのを検知して、変えているというように見えています。

なので今後、感染端末に対してブロックを強化して、それを増加させないということをしっかりやっていきたいと考えています。あとは、ユーザーは気づきにくいので、感染端末への対策というのを考えていかないといけない。それから、企業を騙るフィッシングが多数増えてきていますので、ドコモさん、KDDIさんがおっしゃっているように、企業発の業界ルールのようなものをしっかり策定して、やっていきたいと考えております。

以上になります。

【大谷主査】　松崎様、どうもありがとうございました。

次は、警察庁からの御説明をいただきたいと思います。御準備よろしいでしょうか。よろしくお願いいたします。

【中嶋オブザーバー】　警察庁サイバー企画課の中嶋と申します。よろしくお願いいたします。

警察庁からは、SMS認証に関しての不正利用状況について、御説明したいと思います。

我々はSMS認証代行と呼んでおりまして、要は多要素認証の時に使われているSMS認証をかいくぐってポイントを不正取得したり、フリマサイトで不正出品等をしているような内容について、御説明をしたいと思います。

まず、SMS認証代行の内容でございます。SMS認証代行とは、いろいろなサービスにおいて２段階認証、多段階認証の一つとして利用されているSMS認証を他人になり代わって代行するような手口でございまして、いわゆる犯罪インフラの一つと考えられております。この図のとおり、まずSMS認証代行者とその認証代行を依頼する者に分かれます。

SMS認証の代行者は、まず準備行為として、携帯電話事業者とSMS付きのデータSIM等を契約しておきます。この際、この契約において本人確認がなされていない、もしくはなされているけれども実質的にしっかりと確認をしていないような状況がありますと、こういった認証代行というのができてしまうというような形になります。したがいまして、我々警察としては、このSMS付きのデータSIMサービスにおいては、本人確認をしっかりしていただきたいというのが、考えでございます。

SMS認証代行の説明に戻りますと、まず契約後、依頼者が２番で認証代行を依頼します。この認証代行の依頼につきましては、基本的には認証代行者がインターネット上で認証代行をして欲しい人を募集するといった形で行われていることを把握しております。認証代行の依頼を受けますと、認証代行者は依頼者に電話番号を伝達します。この際、あらかじめ取得しておいたSIMカードについては、特に依頼者には送付したりせずに、認証代行者の側で保有している状況がうかがわれます。

認証代行者から依頼者に電話番号を伝達しますと、依頼者側で自分が契約したいサービスのホームページ等でアカウントを作ろうとします。これが４番のアカウント取得要件になります。そうしますと、大抵IDやパスワードを設定した後で電話番号の入力が要求されます。依頼者は先程教えてもらった電話番号を入力し、これに呼応してサイトから認証コードをSIMの方にSMSで通知するような形になります。そして、認証代行者側でこの認証行動を依頼者に通知し、依頼者側で認証行動を入力します。そうすることによって、依頼者は目的のサービスのアカウントを不正取得することができるようになります。

こういった行為がインターネット上で行われている訳でございますが、業界団体におかれましては、こういった状況に関して我々警察庁、そして総務省から対策の検討依頼をさせていただいております。こうした検討依頼を受けまして、令和３年１月にテレコムサービス協会のMVNO委員会におきまして、データ通信契約申込み受付時における本人確認手続

に関しまして、申合せを締結していただいております。この申合せの内容につきましてはこちらに記載しているとおりでございますが、SMS機能付きデータ通信契約において、原則、携帯電話不正利用防止法と同一の本人確認方法による契約の受付をしていただくと。

また、SMS付きが付与されていないデータ通信契約、こちらも場合によってはいろいろな犯罪インフラとして悪用される可能性もございますが、こういったものについては引き続き検討するといった形で申合せを結んでいただいております。令和５年11月現在の数字でございますが、こうした申合せに基づきまして、23社におかれまして、SMS機能付きデータ通信契約において、契約を受け付ける際に携帯電話不正利用防止法と同一の本人確認方法による契約の受付を実施していただいていると承知しております。

また、警察における対策でございまして、これについては当然、検挙を推進しているということを御紹介させていただきたいと思います。当然ですが、SMSの利用につきましてはこういったSMS認証代行以外にも、例えば特殊詐欺におけるコミュニケーションツールとして使われるなどといった実態もございまして、今回御説明をさせていただくのはあくまでも一例、氷山の一角と認識していただければ幸いでございます。

それでは、若干簡単に説明をさせていただきますが、令和４年９月に京都府警察等におきましてSMS認証代行に関する取締りを実施しておりまして、これに基づきまして認証代行者及び依頼者６名をそれぞれ電磁的記録不正作出、同供用の容疑で検挙しております。端緒といたしましては、サイバーパトロールを行い、インターネット上でこの認証代行者がSMS認証代行しますよといった形で依頼者を募集しているところを把握し、捜査を始めたといった形になります。

先程も少しお話をしましたが、この認証代行者は認証代行以外にも特殊詐欺の実行犯に自信が契約したSIMの供与をしている実態も、捜査を進める中で把握しているところでございます。この認証代行者がどういった者に提供していたかというと、例えばフリーマーケットサイトのアプリのアカウントの不正作出、もしくはオークションサイトのアプリのアカウントの不正作出、そして出会い系アプリアカウントの不正作出等を行ったといった形で把握しております。

こういった事例は最近増えており、中にはSMS認証代行を1,000件以上実行していたという事例もございます。引き続き、警察といたしましては、こうした犯罪の捜査、被疑者の検挙等を進めてまいりますが、そうした中でも重要なのが事後追跡性の確保だと考えております。犯罪を実行した者を検挙するためには、誰が、どういった人がサービスを契約し

たかといった、本人確認をはじめとした事後追跡性が確保されていないと実行者にたどり着くことは当然できないわけでございまして、そうした観点からも、先程、業界団体の方で本人確認の強化等をしていただいておりますが、引き続きこういった形でSMS機能付きのデータSIMのサービス等における本人確認の強化を、是非ともお願いしたいと考えている次第でございます。

私からの説明は以上です。ありがとうございました。

【大谷主査】　中嶋様、どうもありがとうございました。認証代行者が電磁的記録の不正作出罪で検挙されたということで、依頼者だけではなくて認証代行者自身もということでよろしいですか。

【中嶋オブザーバー】　おっしゃるとおりでございます。認証代行者と依頼者が、ともに共犯として検挙されております。

【大谷主査】　共犯ですね。すみませんでした。確認させていただきまして、ありがとうございました。

【中嶋オブザーバー】　よろしくお願いいたします。

【大谷主査】　それでは、今、四方から御説明をいただきましたけれども、御質問がありましたらお受けつけしたいと思います。いかがでしょうか。

それでは、仲上構成員、よろしくお願いします。

【仲上構成員】　日本スマートフォンセキュリティー協会の仲上と申します。御三方、警察庁様も含め、御説明いただきありがとうございました。特に各社、３社からは、様々な対応をしていただいている旨について御説明いただき、大変理解が進んだ次第でございます。ソフトバンク様からの発表について御質問がございまして、SMSブロックにおいて非常にリアルタイムな手続で実施をいただいているところについて、非常に興味深くお話を伺いました。P18で、可能であれば時間軸がどのような時間軸でパターンの変化に追従されているのかというのが分かると、対応のスピード感みたいなものに見識が広がると思った次第でございます。

あと、ブロックを検知するということは、攻撃者がその仕組みを持っているということかと思いますので、そういった意味では、攻撃者側が自分たちで発信したメッセージが届く届かないというのを判定しながら送り出すメッセージを調整しているという実態があることについては、なかなか対応策が難しい問題なんだというのを改めて認識しました。以上でございます。

【大谷主査】　ソフトバンクの松崎様から御回答、お願いいたします。

【ソフトバンク株式会社】　時間軸は正確にはお答えできないんですけれども、なるべく早く登録をするような形で動いてはおります。

【仲上構成員】　承知いたしました。ありがとうございます。

【大谷主査】　ありがとうございます。　沢田構成員、お願いいたします。

【沢田構成員】　ありがとうございます。皆様、大変貴重なお話、御説明ありがとうございました。勉強になりました。NTTドコモ様に１点と、KDDI様に１点、お尋ねをしたいことがございます。

ドコモ様に関しましては、事業者間で情報共有するに当たって、匿名化をされているという御説明があったかと思います。不正検知に関しては、電気通信事業法上は包括同意のもとでやっていらっしゃるということで、もちろん適法で問題なくいろいろな情報を取っていらっしゃると思うのですが、その結果分かったことを他の事業者様と共有するに当たっては匿名化しないとまずいというのは、どの部分を匿名化しているのかももう少し伺えればと思ったのですが、電気通信事業法上の制約なのか、個人情報保護法などほかの法令との関係なのかというのが、質問でございます。

KDDI様への御質問も、続けてよろしいでしょうか。最初に市場規模の御説明をいただきましたが、それは何を意味するのか、ということです。この規模というのは通信料金、SMSの利用料の金額ということなのでしょうか。以上です。ありがとうございます。

【大谷主査】　ありがとうございます。

それでは、まずドコモ様のほうから、匿名化につきまして御回答いただければと思います。

【株式会社NTTドコモ】　NTTドコモの大橋でございます。沢田先生、御質問ありがとうございました。正確なところは、もし間違っていたら御容赦いただきたいですけれども、まず包括同意についてはお客様が受診されるSMSの通信の中身を当社で拝見して、危険と判断されるものについてはブロックするものでございまして、お客様、通信の秘密を侵害される当事者にとって便益が高いということで、包括同意という形をとっているものでございます。

一方で、今回受信したSMSの情報を事業者間で共有するというのは、すなわち第三者提供するということになるのかと思いますが、これは迷惑SMSを発信している人の通信の秘密というのもありながら、受信している側にとっても通信の秘密になりますので、ここの

部分については通信の秘密の配慮という観点から匿名化を図っているというところになります。匿名化している部分については、この資料13ページにも書かせていただいているとおり、受信日時、送信者・受診者の情報、あと本文中に具体的なURLや電話番号などが書いてある場合についても削除しているというものでございます。以上です。

【沢田構成員】　ありがとうございます。

【大谷主査】　それでは、KDDI様の資料の３ページのところの金額、こちらについてよろしいでしょうか。

【KDDI株式会社】　ありがとうございます。結論から申し上げるとＢ２Ｃの配信に係る市場規模でございます。資料中の１個前のページ２に構成図を書いているのですけれども、こちらの青の箱で書いてある企業や自治体様、要は配信をしたいという配信元から料金をいただくことで成り立っている市場のことを指しております。補足させていただくと、いわゆる個人間のメッセージ通信、Ｃ２Ｃと呼ばれているものについては、この数字の中には含まれておりません。以上です。

【沢田構成員】　ありがとうございます。よく分かりました。

【大谷主査】　ありがとうございました。それでは、中原構成員、お願いいたします。

【中原構成員】　中原です。大変分かりやすいプレゼンテーションをしていただきまして、誠にありがとうございました。携帯電話の利用者がスミッシングに利用されているということで、SMSを自分の携帯電話からたくさん送信されていることを知るという、そういう利用者に対する警告であるとか注意喚起というのが非常に重要だと思うんですけれども、それが具体的にどのようなものであって、どれだけ効果があるかということに関心があります。

具体的にはNTTドコモ様で、２点指摘してくださったと思いますが、11ページでSMSの送信状況に関する注意喚起の実施、それから17ページでSMS大量送信被害への特別対応を御紹介くださいましたけれども、まず11ページの送信状況に関する注意喚起については、どういう基準で注意喚起をするのか、単純に件数を見ているのかそれともその人のSMSの送信の増加量とかを見ているのかという、その基準の問題です。それから、注意喚起をされたうちのどれだけの人がどのような対応をとっているのかということについて、伺えればと思います。

大量送信被害への特別対応のほうで、これは直近に導入された仕組みだということで、なかなかデータとしてはないのかとも思いますけれども、どの程度件数としては発生して

いるのか、それからどの程度の被害額なのかということ、それから特別対応として通信料金の減算について、差し支えない範囲で、何を考慮してどの程度の減算をしていらっしゃるのかを伺えればと思います。以上です。

【大谷主査】　それでは、ドコモの大橋様、よろしくお願いいたします。

【株式会社NTTドコモ】　ドコモの大橋でございます。中原先生、御質問ありがとうございました。具体的な数字等については、この場で申し上げるのは控えさせていただければと思いますが、まず11ページの大量送信のところについては、文章で書かせていただいているとおり、多数のSMS送信が確認されたとなっておりますので、件数に基づいて注意喚起を行っているところでございます。

17ページについて、基本的にはお客様から申告をいただいた場合になっておりまして、全容がどのぐらいの件数、被害額が想定されるかはなかなか難しいところでありまして、SMSの送信自体は正常に行われていることになるので、お客様からの苦情相談、申告に基づかざるを得ないかと考えております。以上です。

【中原構成員】　どうもありがとうございました。

【大谷主査】　中原構成員の御質問の中にあった、警告などを受けた方がそれによって行動がどういうふうに変わったかというところについて、私も関心があったのですが、そういった情報については難しいでしょうか。

【株式会社NTTドコモ】　ドコモの大橋でございます。注意喚起を行った人がその後、どういうふうにしたかというところまでは、正直、現状は追えていないところでありますので、今後何ができるかは考えてまいりたいと思います。

【大谷主査】　ありがとうございました。すみません、私から御質問で、これだけキャリア様でいろいろ手を打っていただいてもなかなか減らないというか、逆に増えてきたりということも現象としては起きているのですけれども、何が足りないのかといったところをできれば各キャリア、簡潔に教えていただけるとありがたいと思っておりまして、ドコモ様、KDDI様、ソフトバンク様、それぞれから教えていただけますと幸いでございます。いかがでしょうか。

【株式会社NTTドコモ】　ドコモの大橋でございます。件数がなかなか減らない原因は、難しいところではあるのですけれども、被害に遭ってしまう方がそれなりに出ているということで、悪意を持った行為をする人にとって何かうまみがある状態が継続しているということなのかとは想定をしております。あまりはっきりした返事になっておらず、申し訳

ありません。以上です。

【大谷主査】　ありがとうございます。すみません。では、KDDIの小頭様、いかがでしょうか。

【KDDI株式会社】　ありがとうございます。KDDIの小頭です。少し五月雨になってしまいますが、回答をコメントさせていただきます。まず、現在の対策と発生件数で、いたちごっこの環境は否めないところでございます。他方で、先ほど市場規模が成長しているという点も申し上げましたが、年率で申し上げると20～30％の比率で毎年、例えば件数、通数、Ｂ２Ｃの配信件数が増えておりますので、迷惑申告の数ですとか迷惑したブロックの数ですとかを市場全体の比率で見ると、維持できているか多少減っているのではないかとは思っています。

ただ、相対的に比率が維持できているからといって必要十分だとは思っておりません。それに対する課題感でございますけれども、企業発とか別の事業者から配信されるＢ２Ｃのものは、比較的、携帯電話キャリアが事前に配信元の企業や間にいる代行事業者と会話できて、いろいろ審査やあるいは問題が発生した場合の即時停止ができている状況でございます。

なので、課題となっているのは個人間のルート、配信ルートで発生している、特にマルウェアからの自動配信が今最大の課題であろうかと思っていまして、個人のお客様ですので、配信する前とか配信した後にコミュニケーションするのがなかなか難しい状況でございますので、先ほどの中原先生の御質問ですとかNTTドコモ様からの回答にありましたとおり、それに対してどうやって告知して、エンドユーザー、お客様にどう事後対応してもらうのか、端的に言うとマルウェア削除になると思いますが、この一連の対応を今後詰めていかなきゃいけないと考えております。以上です。

【大谷主査】　ありがとうございました。それでは、ソフトバンクの松崎様からもよろしいでしょうか。

【ソフトバンク株式会社】　大体同じになってしまうのですけれども、対策として今できているのが受信側に対しての対策になっておりますので、送信している人に対してのアプローチというのが必要かと考えております。以上になります。

【大谷主査】　どうもありがとうございました。

御説明いただいた内容を踏まえて、これから対策などについて意見交換をしていくわけですけれども、まず事務局からSMSの不適正利用対策の方向性などについて、資料の御説

明をいただければと思います。よろしくお願いいたします。

【小澤利用環境課課長補佐】　大谷先生、ありがとうございます。前回と今回の皆様からのインプット、プレゼンテーションに基づきまして、対策の方向性の議論をお願いしたいと思っております。今、不適正利用対策の方向性（案）と書きましたが、何かここに案があるというよりは、これから皆さんに御意見をいただきたいという趣旨でございますので、御了承いただければと思います。

前回、SMS対策に関する論点（たたき台）ということで提示をさせていただきました。前回の最後のほうに説明させていただきました。前回のマクニカ様、あとトビラシステムズ様のプレゼンテーションの中で、どちらかというと、今回ソフトバンク様から御紹介いただきましたけれども、マルウェア感染端末からのSMS発信への対策が喫緊に必要ではないかという御提案をいただいたと認識していまして、赤字で補足をさせていただきました。

先ほど小頭様からもお話がございましたけれども、マルウェア感染端末回線の特定をまずして、利用者への警告、注意喚起をすると。こちらを進めていくのが重要なのではないかと前回伺いまして、書かせていただいております。また、前回のマクニカ様の資料の中でもございましたけれども、ニュージーランドの事例で、政府、公的機関でスミッシングメッセージの申告受付をして、対策をとりましたという話がございまして、アメリカとかほかの国の対策の状況も御説明いただきました。

スミッシングメッセージの申告も数が少ないという話もありまして、先ほど、キャリアさんごとに受けつけられていますという話、特にドコモ様のお話にもございましたけれども、こちらを円滑に、横連携で活用して対策をとれるような、仕組みを構築してはどうかということで、書かせていただいております。

発信番号、キャリア番号とかRCSについては各キャリアさんからの御説明に、認証代行、データSIMについては、警察庁の中嶋室長からの御説明にもございましたが、SMS配信者、受信者の不適正利用対策については、まず事業者様での対策、あとは利用者での対策で御提案いただきましたので、取り得る対策について、本日御意見いただければありがたいと思っております。

前回の事務局の御説明で追加させていただきたいことが２つございます。１点目がマルウェア感染端末の特定、ないしは注意喚起が、本日の議論にもありましたけれども、通信の秘密との関係でどう整理されるのかにつきまして、こちらは平成30年９月26日に公表しております、電気通信事業におけるサイバー攻撃の適正な対処の在り方に関する研究会の

第三次取りまとめで、特に当時IoTにマルウェアが感染する場合について指摘があったところですけれども、マルウェアに感染している可能性が高い端末の利用者への注意喚起について整理をしております。

ここに細かく記載されていますけれども、利用者が一旦契約約款に同意した後も随時、同意内容の設定変更ができるようにすること、要するにオプトアウトができること等を条件にして、そのほかにも幾つか条件はございますけれども、契約約款に基づく事前の包括同意であっても有効な同意と整理できるとされております。また、注意喚起前の検知についても、マルウェアに感染している可能性が高い場合に注意喚起を受けられるというサービスが提供されると、これとセットでオプトアウトもできる、希望しない者は対象にならないということを条件に、事前の包括同意であっても有効な同意と整理できるとされておりまして、こちらと同様の整備が今回のSMSについても可能ではないかと考えております。こちらに基づいて事業者様のほうで対策を進めていただけないかと考えております。

最後に、特にSMSの関連事業者、特にキャリアさんだけではなくて、さっきＢ２Ｃの話がありましたが、SMS配信事業者さんを含めて連携を、業界団体みたいなSMSに特化したものもございませんので、さらに推進すべきではないかと。特に先ほど業界でのルールを事業者様からも御提案いただきましたけれども、そちらに対応するべくお声がけさせていただきまして、SMS不適正利用対策事業者連絡会を立ち上げさせていただきました。

これは担当者レベル・実務者レベルで、随時集まって定期的に情報交換をするというのがまず一つ、さらに自主的な対策ですとか業界のルール、あとは利用者への周知広報も個社個社でやるのではなく連携してやるというところを念頭に、立ち上げさせていただいております。こちらの枠組みもぜひ活用させていただいて、課題に対応できるといいのかと考えております。

事務局からの説明は以上になります。

【大谷主査】　御説明どうもありがとうございました。

それでは、構成員の皆様からの意見交換の時間にしたいと思っております。質問やコメントをいただきたいと思います。

それでは、沢田構成員、よろしくお願いいたします。

【沢田構成員】　ありがとうございます。２度目になってしまって申し訳ありません。今御説明いただきました連絡会、大変良い取組だと思いますので、ぜひお進めいただきたいと思いました。もし可能であれば、もう既に動き出していらっしゃるのかもしれないの

ですが、１点追加で御提案差し上げたいことがあります。それは、今構成員として挙げていただいた事業者のほかに、SMSを利用する事業者の参加も御検討いただけないかということです。理由として、まず１点目が、先ほども御紹介いただいたように市場規模が伸びていて、特に２段階認証でSMSを利用する企業や公的機関がどんどん増えてきているように思います。本来はマイナンバーカードで認証してほしいとも思いますが、それはちょっと別の話なので置いておいたとして、スミッシングのようなことを意識したとしてもフィッシング対策の一環として考えていらっしゃる企業が多いのかもしれないと。今までのお話を伺っていると、eメールとは別の特殊性があるようにも思いましたので、SMSを通じたフィッシングにも意識を向けていただく必要があるのではないかというのが１点です。

理由の２点目は、ユーザーとしてもSMSを利用する事業者に少し要望したいことがあります。先ほど業界ルールというお話もあり、そういう方向でもいいかと思うんですが、まず一目で身元が分かるようにしてほしいと。発信者のところが番号だけだと受信した側は不安になります。共通番号という話があることも、今回、初めて知りました。利用者は表示名に企業名が入っていればちょっと安心できるわけですが、ごく僅かのケースでしか入っていません。何か制約があると伺ったことがある気もしますが、私のところに来るSMSでは、PayPalとかSlackとか、短い海外系のところぐらいしか社名が入っていないです。

プラスメッセージになるとそれが可能になるのかもしれないのですが、逆になりすましの不安がどの程度あるのかという辺り、ユーザーが知らないことも多いので、知識を共有できるといいという問題意識です。あと、正規のSMSの中にURLが貼ってあるケースも結構多いんですが、本当にリンクがないと送る目的が達成できないのかどうかを、もう一度、利用事業者さんに考えていただきたいと思います。

我々はサービスを申し込むときとか契約するときに携帯電話番号を聞かれることが多いです。聞かれれば答えますが、緊急連絡先として以外にいろいろなSMSを送るという使い方をするなら、事前に明示していただきたいと思います。お知らせはできるだけアプリで通知して欲しいと思うユーザーも結構いると思いますので、その辺りを御検討いただきたい。なりすまされる側に罪はないとはいえ、スミッシングと見分けがつかないような文面はやめて、何か工夫してもらえないものかと思います。

３点目はユーザーからの申告をスムーズにするためです。現状ではなりすまされた側の企業に連絡が行くケースも結構あると思います。全体像を把握するためには、企業に入ってくる申告内容も活用して、合体して分析すべきと思います。正規のSMSなのかスミッシ

ングなのかがキャリアさんの立場からでは分からないこともあるかと思いますので、正規の発信者との連携で対応しやすくならないかと。

先ほど、企業さんとの間はうまくコミュニケーションがとれているという御紹介もありましたので、筋違いかもしれないですが、そういった可能性を追求することで、現在のブロックの精度を上げられないかと思いました。すみません、長々、失礼しました。以上です。ありがとうございます。

【大谷主査】　貴重な御意見をどうもありがとうございました。私も、本当に一目で分かればいいと思いながら、機種によってはなかなかアプリが入らないとかそういう問題もあるようですので。それでは、今の点について事務局のほうで、SMSを利用する配信元の事業者さんを連絡会に巻き込んでいただくという御提案について、いかがなものでしょうか。

【小澤利用環境課課長補佐】　沢田先生、ありがとうございました。貴重な御意見だと思います。今回、連絡会を立ち上げましたけれども、先ほど確かに構成員を見ていただくと通信事業者ばかりだというのはおっしゃるとおりだと思います。今までは通信事業者側、特に配信事業者のＢ２Ｃをやられている事業者の横連携もなかったことがまず一つかと思いましたので、まずこれはこれで横連携したいと思います。

なりすまされる側との連携も、私も迷惑メール対策を別でやっていますけれども、迷惑メール協議会とフィッシング協議会の役割分担といいますか、これも連携しているのですけれども、迷惑メール協議会は通信、ISPとかメールベンダーさんが多く、フィッシング協議会はなりすまされる側も入っていて、情報交換しながらやってきたというのもありますので、一緒にやらないと決められないようなルールづくり、特に大手事業者さんがSMS認証を使うときこういうルールでやりましょうみたいな、御提案いただいたところは、通信業者側だけではできないルールもあると思いますので、うまく、特にフィッシング協議会とかほかの団体とも連携して、、なりすまされる側の方ともお話できれば、ぜひ、ありがたいと思いますので、よろしくお願いします。

表示送信元をちゃんと表示すべきとか、ユーザー間申告をしっかり活用すべきというのもおっしゃるとおりだと思いますので、取り組ませていただければいいなと思います。事務局は以上です。

【沢田構成員】　ありがとうございます。

【大谷主査】　ありがとうございます。せっかく横連携の枠組みがありますので、有効

活用していただければと考えます。

それでは、まず星構成員、その後に鎮目構成員から御発言いただきたいと思います。よろしくお願いします。

【星構成員】　すみません、お先に失礼いたします。どうもいろいろと御説明いただきまして、ここまでキャリアの方、警察庁さんの方も含めてありがとうございました。

今、SMS対策に関する論点（たたき台）という形で大きくマルウェア感染端末からのSMS発信対策というのと、不適正利用の対策というところを上げていただいていて、これはもちろんこの方向で、特に今回赤字で入っているところもぜひ進めていただきたいとは思うんですけれども、例えばマルウェア感染端末回線の特定とか利用者への警告注意喚起の実施ということを進めていくことによって、そういったものが減らせるだろうということは確かにそのとおりなんですけれども、要するにそういう警告を受けた人に対応していただけるという、言わば性善説に立っているというところがあるというところが気になりまして、もちろん大多数の方はそうしてくださるはずなんですが、実はこういうマルウェアに感染した端末を用意する側、犯罪者の側、あるいは犯罪者の側から小遣いをもらっているような人たちにとってみれば、警告を受けたところで対応はしていただけないという問題が生じ得ると。その場合に何ができるのか。

もちろんそういう場合にわざわざマルウェア感染端末を用意するという人は、数からいえば少数なのかもしれないんですけれども、蟻の一穴といいますか、特にネットではそういう端末が１個でも２個でもあるのであれば、そこから影響が非常に広がっていくということで、根本的な対策というところからするとかなり厳しい状況が生じ得るのではないかと。

実際、ネットの世界のボットネットについては、わざわざ感染端末を用意するような人たちがいて、ちっとも根絶できないという問題があるようにも伺ってはおります。ですから、今回のこの検討会でどこまで織り込むかというのはもちろんいろいろあろうかと思いますけれども、利用者側が性善説で対応してくれるんだと、たまたま気づいていないだけだからそれを気づかせてあげるんだ、それだけでも１個大きな進歩だと思いますけれども、恐らく問題はそこから先にもまだ残っているのではないかというところです。

そうしますと、結局誰が使っている端末なのかがウイークポイントとして残るのではないかというところです。そこは、質問というよりは単なるコメント、感想ですけれども、気になったところを申し上げさせていただきました。ありがとうございます。

【大谷主査】　貴重な御意見、どうもありがとうございました。

【小澤利用環境課課長補佐】　星先生、ありがとうございました。おっしゃるとおり、マルウェア感染端末を意図的に感染させたり、それで送らせているようなことはあるんだろうと思います。ただ、通信の中を見ているだけだとまだ見分けがつかないところなので、まずここをやってみないと、この先にどれぐらい悪意を持ってやっている人がいるのかというのが分からないんだろうと思います。まず特定して警告して動きを見て、警告して終わりじゃなく、その先の行動変容を見ないと意味がないという意味で、非常に重要な論点だと思いましたので、そこをちゃんとウォッチした上で、さらにそれが減らないようであればもう一歩、次の対策を検討したいと思います。ありがとうございます。

【星構成員】　ありがとうございます。大分先走って話をしているというのは私も自覚しておりますので、ありがとうございます。

【大谷主査】　ありがとうございました。それでは、鎮目構成員からお願いいたします。

【鎮目構成員】　ありがとうございます。本日は現状について詳細に御説明いただき、ありがとうございました。１点意見と、それに関連する質問がございます。これは星先生も言及されていましたが、最後に事務局にお示しいただいた対策案、マルウェア感染端末を特定し、利用者へ警告ないし注意喚起を行う。この点については通信の秘密との関係が当然、気になるところですが、先ほど御説明いただきましたように、総務省のサイバー研第三次取りまとめで、IoTとの関連で前例があるということですので、包括同意とするのが前例と伺いましたが、ぜひこれは同様の観点から積極的に整理を進めていただきたいと思います。

とはいえ、１点、気になるところが、警告や注意喚起の実効性でして、携帯電話のキャリアのユーザーというのは相当な数がいるということと、あとマルウェア感染端末の件数もかなりの数だと伺いましたので、利用者への警告や注意喚起の具体的な方法としてどのようなものを想定されているのかということを、現時点でのお考えで構いませんので、教えていただければと思います。SMSというのはまず考えられますが、気になるのはSMSでそういうものを送ったときに、それこそ迷惑メールと同様に見過ごされてしまうのではないかと。ただ、そもそも引っかかるような人なので、それを送れば反応があるのかという想定もあるかもしれません。

他方、電話で１点１点警告するとなると、これは大変なコストということになるので、そういったことが果たして可能なのか、事務局、それからもし可能であれば携帯キャリア

３社の皆様から、警告や注意喚起として具体的にはどのような方法が実効性あるものとして、あるいはコスト的に可能なのか、その辺りについて教えていただけると幸いです。以上です。

【大谷主査】　ありがとうございます。それでは、せっかくですので、まずキャリアの皆様、警告や注意喚起の具体的な方法について御発言いただければと思います。その上で、また事務局からの御意見をいただければと思いますが、ドコモの大橋様、いかがでしょうか。

【株式会社NTTドコモ】　ドコモの大橋でございます。現状行っている注意喚起については、今日、御説明差し上げたところでありますので、今後については、今回の議論をきっかけにさらに何ができるかを考えてまいりたいと思います。

【大谷主査】　ありがとうございました。具体的に文例も出していただいていましたので、イメージしやすいと思います。

それでは、KDDIの小頭様、いかがでしょうか。

【KDDI株式会社】　ありがとうございます。KDDIの小頭です。具体的な手法は、先ほどNTTドコモ様が申し上げられたSMSですとか、先ほどKDDIから御説明させていただいたプラスメッセージ、ないしはRCSという技術を用いてやるのが主流だろうとは思います。といいますのも、先ほど沢田先生からも御指摘があった見分けのつき方とのセットになると思っていて、消費者、エンドユーザーからの、なかなかこれがグレー、ブラックですというのをエンドユーザーに見分けていただくのはなかなか難しいと思いまして、先ほどの説明資料にもあったホワイトであることを我々が証明、啓蒙するという活動とセットで、KDDIからのお知らせという形でロゴと認証マークを表示した上で、ここから来たものは安心して御覧ください、その上でいろいろ御対応をお願いします、のような形態であれば、相乗効果が期待できるのではないかと思います。

もう一つ、まだ何も決定事項ではございませんが、先ほど話もあったアプリ、携帯電話各社がいろいろなアプリを持っておりますので、お客様にとって信頼のできるアプリからの通知というのも一つの手段になろうかと思います。以上です。

【大谷主査】　ありがとうございました。

では、ソフトバンクの松崎様、いかがでしょうか。

【ソフトバンク株式会社】　ソフトバンク松崎です。今、実際できている注意喚起としては、全体に向けてのホームページ告知だったりという形になります。あとは、感染とか

になると個人に対してのSMSになると思います。ただ、１日に送れる数だったり、夜中に届いてしまうとお客様の御迷惑になってしまうので、数、母数にもよるのかと考えております。以上になります。

【大谷主査】　ありがとうございました。鎮目先生に満足いただけるお答えだったのかよく分からないんですが、事務局、いかがでしょうか。

【小澤利用環境課課長補佐】　ありがとうございます。警告の実効性を保つためにどういう方法が望ましいのか、効果とコストのバランスを見ながらではありますけれども、非常に重要な論点と思います。そもそもSMSを勝手に送られてしまっている人に対して、SMSで通知して見てくれるのかとか、そういうやってみないと分からない課題はあると思っていまして、ただ、さっき幾つか事業者様から御提案いただきましたので、そういうところから始めてみて行動変容が見られるかどうかというのをウォッチして、一番いい方法を探していくということかと思いますので、ぜひ一番効果的な方法を探していければいいのかと思います。

【大谷主査】　鎮目構成員、いかがでしょうか。

【鎮目構成員】　ありがとうございました。確かに一気に全部解決するというのは難しいことかと思いますので、やれるところから御提案のような対策をとっていって、警告を受けた方の行動変容が実際どのように起こるのか、対応してくれるのか、その辺りをしっかり追跡していくということを取りあえずやってみようと、その辺りについては賛同できると考えております。ありがとうございます。

【大谷主査】　貴重な御意見をありがとうございました。私としても、ばらばらにそれぞれの事業者さんがやられるよりは、多分一斉にキャンペーン的にやられたほうが、印象が違ってくるのではないかと。例えばテレビ広告、ACみたいな広告などと一緒に連動して、気づきを促すような仕組みがとれたらいいのかと考えております。

山根構成員、よろしくお願いします。

【山根構成員】　感想めいたコメントですけれども、現状のマルウェア感染端末からの送信が非常に大きな課題になっているということに鑑みれば、これについて対策を進めるというのは非常に重要になってくるかと思います。スミッシングの受付申告が進んでいないという現状があるということで、これは申告受付が進むと分析の高度化にも使えると思いますし、KDDIさんの御説明ですと送信元への利用停止措置の一つのトリガーにもなり得るということだったかと思いますので、申告受付を進めていくというのは特に重要になっ

てくるかと思っております。

それを円滑に受けつけられる仕組みづくりと、利用者一般としてあまりスミッシング、怪しいメールが来たら申告しようというような意識がまだ十分にないんじゃないかという気もしますので、そういったところの啓発活動も重要になってくると思いました。また、連絡会の立ち上げも非常に重要だと思いまして、ぜひ進めていただきたいと思っております。

沢田構成員から既に御指摘があったとおり、私もなりすまされる側との連携も非常に重要になってくると思っておりまして、例えば金融機関等でもなりすましフィッシングなり、スミッシングなりの注意喚起をやっていたりするかと思うんですけれども、そういったなすまされる側との情報連携をするということで分析の高度化にもなりますし、利用者に対する注意喚起もより効果的になっていくのではないかと思っておりまして、その点についてもぜひ進めていただきたいと思います。以上です。

【大谷主査】　貴重なコメントありがとうございました。本当にどのぐらい受けつけられているのか、現在も多分、十分ではないと思いますので、件数を増やして分析・解析ができるようにというのは、本当に必要なことだと思います。

ほかに、コメント等ございますでしょうか。

【沢田構成員】　何度も申し訳ありません。ありがとうございます。平成30年の第三次取りまとめに関してコメントさせてください。これは存じ上げなかったですけれども、大変重要だと思いました。よく分かりました。ただ、正当業務行為として認められる範囲はすごく狭いという感想も持ちました。「当該ISPのサービス提供に支障が生ずる蓋然性が具体的にある場合」という限定もついていますし、「その支障を防ぐために必要な限度で」「その端末の利用者に対してのみ」というあたりがかなり限定的と思いました。先ほどの情報共有の話と関連し、感染端末に関する情報を通信事業者間で共有するということは、この限りにおいては想定されていないし、包括同意の対象としても想定されていないという理解でよいのかどうかというのが質問でございます。

意見としては、もう少し認められるようにしないと、今やりたいことができないのではないかということで、この取りまとめ自体は携帯電話を念頭に置いたものではないかもしれないですが、何か新たな整理がされるのかが、次の質問でございます。

もう１点、感染の可能性が高い端末を持っていて、知らずに悪用されている人の気持ちで考えると、自分の端末が感染していることを教えてもらえたらうれしいです。悪意でな

い場合は、友達に迷惑がかかるから対処しなきゃと思います。拒否する人はあまりないので、包括同意で全然オーケーで個別に同意を一々取る必要はないように思いますが、透明性という観点では、どの主体が自分に関してどんなデータを見ているのか、自分の通信について誰が何をどこまで知っていて誰と共有しているのかということは、法律上の要請とは別に、きちんと説明していただきたいと、ユーザーとしては思いました。以上でございます。ありがとうございます。

【大谷主査】　大変鋭い御質問、ありがとうございます。この整理の射程が今回のスミッシング対策にどの程度応用がきくのかという点で、貴重な御質問だったと思いますので、事務局のほうで御回答可能な点がありましたら、御回答お願いします。

【小澤利用環境課課長補佐】　事務局です。御質問、ありがとうございました。簡単な回答になりますけれども、（１）の※印の正当業務行為のところと思っています。こちらは、細かいですけれども包括同意のパターンの場合と、正当業務行為、違法性阻却事由が該当するので包括同意がなくても業務の範囲でやれますという話と、別のパターンで、包括同意があって有効な同意と整理する場合の負担と、それ以外でこういう場合は別に正当業務で許容されますという２パターンで、どちらかというと包括同意のほうが今回に合うのではないかと御説明したので、両方ないとできませんという意味じゃないと、私は理解しています。

個別の事案ごとの判断になりますので、正当業務行為は厳しく適用されますというのはおっしゃるとおりだと思っていますが、今回の警告、注意喚起の話は包括同意の話だと認識しています。

（２）は同意を取るに当たってしっかり説明するという点、ここには細かく書いていないですが、もちろん基本的に通信の秘密は個別かつ明確な同意を取得するというのが大原則であり、ここまでこういうふうに説明されてこういうサービスがあってこういう条件があれば事前の包括同意であっても有効な同意ですよと、そういう構成になっていまして、同意を取るときは説明されると思っております。

もう一つ、事業者間で横連携しないと有効ではないという御提案をいただきまして、まず通信事業者側で解析し、で、それをどのように横で連携して使えるのかは、まだ連絡会が立ち上がったばかりですので、それぞれが申告なり自社の解析で得たデータを横連携して有効な対策が新しく出てきたときに、もし法的な壁があるのであれば検討させていただきたいと思います。

【沢田構成員】　ありがとうございました。もう少し勉強します。

【大谷主査】　どうもありがとうございます。かなりポイントを絞って資料を御用意いただきましたので、次回はまた違ったテーマを取り扱うことにはなりますけれども、実際に利用者にどういった情報を提供した上で包括同意を受けるのかといった、少し細かい資料についても事務局のほうで御用意いただいて、共有していただけますと、今後の注意喚起に向けての議論の土台になるかと思いますので、お願いしたいと思います。

今日はせっかく警察庁からも新しい手口、レポートをいただいておりますので、それに対する御質問などでも結構だと思いますが、いかがでしょうか。

星構成員、よろしくお願いいたします。

【星構成員】　せっかくの機会なので。SMS認証代行についてもちょくちょく報道は伺っていたんですけれども、実情について御説明いただきまして、ありがとうございました。認証代行は基本的にはアカウントの不正作出に使うというものであって、それ以外に用途はないと思いますが、何か変な使い方をされる土台になることはあったりするんでしょうか。すみません、ざくっとした質問で申し訳ないですが、もし可能であれば教えていただければと思います。

【中嶋オブザーバー】　御質問ありがとうございます。警察庁の中嶋です。基本的には先程申し上げた形が多いことを把握しておりまして、要はポイントの不正取得とかフリマサイトにおける不正出品等に利用するためのサービスアカウントの不正取得が多く確認されております。一方で、認証代行者は、アカウントの不正取得を単純に言えば代行しているという形ですので、例えばSMS認証を伴うようなサービスを使うサービスについては、何れもなりすましが可能となってしまうと捉えていただくのがいいかと思います。

いずれにしましても、基本、今回御説明をさせていただいたような手口に悪用され、特殊詐欺におけるコミュニケーションツールの取得なども、２段階認証を求められるようなものが多くございますので、そういったものを使う際も悪用されていると御理解いただければと思います。よろしくお願いいたします。

【星構成員】　ありがとうございます。２段階認証は本人確認を強力に進めるためのツールとなっていますが、そこを破ると、もちろん電磁的記録不正作出等々でできれば困っていないのかもしれないですが、感覚としては不正アクセス行為に近い性質があって、最終的に取り締まればいいという考え方もあるかもしれませんけれども、もうちょっと重い感覚を持ってもらうのも大事かと思った次第です。すみません、余計なことを。ありがと

うございました。

【大谷主査】　ありがとうございました。私も、携帯電話不正利用防止法と同一の本人確認をしてもらうことで、相当解決に向けて前進しているとは思っていたのですけれども、引き続き課題が残っているようでしたら手当てを考えていく必要があると思います。

そろそろ議論は尽きないところですが、この辺りで討議を終了させていただければというような時刻になってまいりました。これまで多岐にわたる論点について活発な御議論、それから貴重な御意見をいただきまして、ありがとうございました。

それでは、次の会合につきまして、事務局から御案内をお願いしたいと思います。よろしくお願いします。

【小澤利用環境課課長補佐】　御議論いただきまして、ありがとうございました。また、今回いただいた御意見を踏まえて、取りまとめに反映していきたいと思っておりますので、よろしくお願いいたします。

次回会合につきましては、別途日程を調整して御連絡させていただきますので、どうぞよろしくお願いいたします。

事務局からは以上です。

【大谷主査】　それでは、以上で不適正利用対策に関するワーキンググループの第２回会合を終了させていただきます。本日は皆様、お忙しいところ御出席いただきまして、ありがとうございました。