不適正利用対策に関するワーキンググループ（第１回）

令和６年２月26日

【小澤利用環境課課長補佐】　少しお時間過ぎてしまいまして申し訳ありません。皆さんおそろいのようですので、始めたいと思います。

改めまして、本日は、皆様、お忙しい中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１回会合を開催いたしたいと思います。このたび本ワーキンググループの事務局を務めます総務省総合通信基盤局利用環境課課長補佐の小澤でございます。よろしくお願いいたします。

まず事務局より、定例ではございますが、ウェブ会議による開催上の注意事項について御案内いたします。

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設定とさせていただいておりますので、音声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、録画をさせていただきます。

続きまして、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、オフにしていただいて、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したい旨を書き込んでいただきまして、それを見て座長のほうから発言者を御指名いただくという方式で進めたいと思っております。御発言される際はマイクをオンにして、映像もできればオンにして発言をお願いします。発言が終わりましたらオフに戻してください。接続に不具合がある場合については、速やかに再接続を試していただくようお願いいたします。その他、チャット機能で随時、事務局や座長宛てに連絡をいただければ、対応させていただきたいと思います。

本日の資料につきましては、本体資料として議事次第と資料１－１から１－５を用意しております。

注意事項は以上になります。

議事に先立ちまして、初回ですので、本ワーキンググループの開催につきまして事務局より説明を申し上げたいと思います。

ワーキンググループの開催要綱につきまして、資料１－１でございます。事前に、親会

に当たります研究会の座長、ワーキンググループの構成員の皆様には御了承いただいております。

本ワーキンググループの主査につきましては、大谷先生にお願いをさせていただいております。この資料、このメンバーのとおりになっております。

要綱にございますけれども、本ワーキンググループの主査は、親会の座長により指名されることとなっておりまして、親会の座長たる宍戸先生から、親会とワーキンググループについては緊密に連携を図りながら、迅速かつ効果的に御議論いただく観点から、大谷先生にお願いしたい旨指名がございましたので申し添えます。

それでは、初回でございますので、構成員の皆様の自己紹介をお願いしたいと思っております。簡単に一言ずつお願いさせていただければと思っております。

それでは、一般財団法人ECネットワーク理事の沢田先生でございます。よろしくお願いします。

【沢田構成員】　一般社団法人ECネットワークの理事をしております沢田と申します。よろしくお願いいたします。Eコマースのトラブル相談を受けている組織でございます。今回の不適正ワーキングの検討内容は、消費者にとって重要なことであると同時に、SMS等に関しましては、成り済まされる側のEC企業や金融機関にとっても重要な課題だと感じております。どうぞよろしくお願いいたします。

【小澤利用環境課課長補佐】　ありがとうございます。

続きまして、学習院大学法学部教授の鎮目先生でございます。よろしくお願いします。

【鎮目構成員】　よろしくお願いいたします。学習院大学の鎮目と申します。私の専門は、いわゆる刑法でして、サイバー犯罪の処罰の在り方をはじめとする、情報通信ネットワークと刑法の関係について関心を持って勉強しております。本ワーキンググループは、我が国の社会が直面する喫緊の課題に関わる大変意義深いものと心得ておりまして、このワーキンググループに参加する機会を得たことは、私にとっても大変貴重な機会であると受け止めております。何とぞよろしくお願いいたします。

【小澤利用環境課課長補佐】　ありがとうございました。

続きまして、デジタルアイデンティティ推進コンソーシアム代表理事の辻先生でございます。よろしくお願いします。

【辻構成員】　はじめまして。私、DIPC代表の辻と申します。私は情報セキュリティ大学院大学というところで、情報セキュリティに関して20年近く取り組んでまいりましたが、

実は、政府が進めますJPKI、公的個人認証のスマートフォン搭載という形のディスカッションが始まったときに、当時の総務省の番号室のメンバーと共に有識者会議の立ち上げ等にも関わらせていただいて、今実現しておりますJPKI、公的個人認証のスマートフォンでの利用に関して、ずっと有識者として関わってきました。

現在、それに加えて、デジタル庁にそれは引き継がれたんですけれども、マイナンバーカードの機能、残りの機能を全てどうやってスマートフォンに移行するのか、これは免許証も含めていろいろ変わってくることになると思うので、そういったディスカッションにも関わっており、公的個人認証を中心とした本人確認、署名といったところと、不正利用といったところ、携帯電話、スマートフォンと密接な絡みがある世界でございますので、そことの絡みということで今回参加させていただきました。ぜひともよろしくお願いいたします。

【小澤利用環境課課長補佐】　ありがとうございました。

続きまして、日本スマートフォンセキュリティ協会技術部会部会長の仲上先生でございます。よろしくお願いします。

【仲上構成員】　よろしくお願いいたします。私、日本スマートフォンセキュリティ協会技術部会部会長の仲上と申します。日本スマートフォンセキュリティ協会は、今から約13年前に設立された団体でございまして、日本の携帯３大キャリア様、それから、当時Android端末を主に開発していたわけですけれども、そういったスマートフォン端末のメーカー様、あとサイバーセキュリティーの専門企業が集まってできたセキュリティの団体となっております。

近年では、日本でもスマートフォンの開発というものが大分規模が少なくなってきたんですけれども、アプリケーション開発の観点とかスマートフォン利用、それからIoTの利用といったところで、サイバーセキュリティーの観点から、様々な観点で利用者、それから開発者の方に情報を提供するという活動を行わせていただいております。

本日は、こういった会議に参加させていただき、発言の機会をいただき、どうもありがとうございます。よろしくお願いいたします。

【小澤利用環境課課長補佐】　ありがとうございました。

続きまして、東京大学大学院法学政治学研究科教授の中原先生でございます。よろしくお願いします。

【中原構成員】　東京大学大学院法学政治学研究科の中原と申します。民法を専門とし

ております。一連の研究会に参加していたわけではなくて、今回が初参加ということで、いろいろと至らないところもあると思いますが、民法の観点から、微力ながら協力させていただければと思っております。どうぞよろしくお願いいたします。

【小澤利用環境課課長補佐】　ありがとうございました。

続きまして、東京都立大学法学部教授の星先生でございます。よろしくお願いします。

【星構成員】　東京都立大学の星と申します。よろしくお願いいたします。私も鎮目先生と同じく刑事法を研究させていただいている者ですけれども、犯罪ツールの規制の在り方ということをちょっとかじったことがあるといったようなことで、今回このような御縁を持たせていただきました。ぜひともよろしくお願いいたします。

【小澤利用環境課課長補佐】　ありがとうございました。

続きまして、片岡総合法律事務所弁護士の山根先生でございます。よろしくお願いします。

【山根構成員】　よろしくお願いいたします。片岡総合法律事務所の弁護士の山根と申します。私は以前、総務省の旧消費者行政第二課に２年間出向しておりまして、現在は通信分野や金融分野における規制法対応を中心に取り組んでおります。主に金融事業者における犯収法対応などの文脈ではあるんですけれども、顧客の本人確認に関する御相談等についても多く扱っておりまして、そういった観点から、本ワーキンググループにおける議論にも微力ながら貢献できればと思っております。どうぞよろしくお願いいたします。

【小澤利用環境課課長補佐】　ありがとうございました。

そして、座長は、先ほど申し上げました大谷先生でございます。大谷先生には後ほど座長の進行のほうをお願いしたいと思います。

オブザーバーの御紹介を先にさせていただきますと、ワーキンググループでは、先ほど要綱のほうにもございましたけれども、警察庁刑事局捜査支援分析管理官の野村様と、サイバー警察局サイバー企画課の中嶋室長にお願いさせていただいておりますので、どうぞよろしくお願いいたします。

それでは、これ以降の議事進行を大谷主査にお願いしたいと思います。大谷主査、どうぞよろしくお願いいたします。

【大谷主査】　大谷でございます。このたび、このワーキンググループの主査を務めることになりました。どうぞよろしくお願いいたします。

では、このワーキンググループですけれども、不適正利用対策につきまして、最近の動

向などを踏まえて、専門的な観点から集中的に検討することを目的としたいと思いますので、構成員の皆様には、それぞれの専門領域をまた乗り越えて、闊達な御意見、御議論のほどいただければと思います。

それでは、時間も限られておりますので、早速議事に入りたいと思います。

本日、初回ということですので、まず事務局から、ICTサービスの不適正利用対策をめぐる諸課題について御説明をいただきます。そしてその次に、株式会社マクニカの角谷様からSMS・スミッシングについてお話しいただき、その後にはトビラシステムズ株式会社の柘植様からスミッシングモニターについて御説明いただきまして、その後に意見交換の時間をいただきたいと思います。

それでは、まず総務省、事務局からの御説明をお願いいたします。

【小澤利用環境課課長補佐】　ありがとうございます。改めまして、小澤でございます。資料に基づいて御説明させていただきます。少々お待ちください。

今回ワーキンググループの開催に当たりまして、ICTサービスの不適正利用対策をめぐる諸課題についてということでまとめさせていただきました。一部、親会であります研究会のほうでも御紹介した内容と重複するところもございますけれども、御了承いただければと思います。

皆様御承知のところかと思いますけれども、不適正利用の課題につきまして、特に特殊詐欺、被害者に電話をかけるなどして、対面することなく信頼させて現金をだまし取る犯罪のことを総称して特殊詐欺と言いますけれども、非常に厳しい状況になっております。前回親会以降、警察庁さんのほうで最新の数字が発表されまして、令和５年の１年間の被害総額、下のグラフがございますけれども、441.2億円ということで、昨年もかなり３割ぐらい伸びて厳しい状況だったのが、またさらに２割ほど増加して、厳しい状況にあると思っております。

また、フィッシング詐欺です。特にコロナ禍以降の巣ごもり需要ですとか、いろんなサービスがネットを経由して受けられるようになってきたところを背景に、こちらは日本クレジット協会さんの最新の数字がまだ発表されていなかったので、令和４年の数字でありますが、それでも411.7億円ということで、かなり厳しい状態にあります。これはクレジット番号盗用被害額ということで、全てフィッシングというわけではないですけれども、かなりの部分フィッシングに基づくものがあるのではないかと思って、かなり厳しい状況かなと。

いずれも共通するところとしましては、特殊詐欺は特に電話を入り口として、フィッシング詐欺はメールや、この後今日議論していただきますSMS、あとはウェブサイト上のポップアップ広告とか、ネット上からの入り口という意味でICTサービスの不適正利用による犯罪ということもあり、これについて総務省としても対策を検討してきましたが、さらに検討する必要があると思っております。

特殊詐欺の対策については、やはり足のつかない電話番号を使って電話をしてくる、その電話番号をもって高齢者の方に信用させるという手口が主でございまして、もともと携帯電話、飛ばし携帯みたいなことを言われますが、こちらのほうに基づく、これも最初はプリペイドだったものが、レンタル携帯とかいろいろなSIMカードで増えてきたということでこれらの対策を進めてきました。

スマートフォンとかPCから電話転送で、相手に03番号を表示させて、ちゃんとした会社からの電話だなということで信用させるといったような手口も非常に増加しておりました。さらに、昨年から特に、050IP電話を悪用する手口が増加してきた、特に、海外からアプリを使ってというものも増えてきたということがございます。

これらの対策として、まず契約時の本人確認を徹底してまいりました。携帯電話不正利用防止法につきましては、携帯電話契約時の本人確認を義務づけしております。先ほど050アプリの話もしましたけれども、こちらも今年の４月から、携帯電話不正利用防止法対象の役務に追加をする省令改正を行っております。また、電話転送につきましては、犯罪収益移転防止法に基づく本人確認を義務づけております。また、携帯電話とか固定電話で使われた電話番号を利用停止するということを業界団体さんと一緒になって取り組んできております。

それぞれスライドに基づいて説明しますと、携帯電話不正利用防止法につきましては平成17年から始まっておりまして、先ほど言いましたプリペイドがかなり盛り上がった頃です。レンタルが増えた頃、平成20年に改正法されております。契約時の本人確認義務が一番柱でありますけれども、それ以外にも、警察署長からの契約者確認の求めというのがございまして、本人確認取り直した後に役務提供を拒否するということができるようになっております。また、レンタル業者についても本人義務があったり、あと無断譲渡の禁止といったような条項もございます。

続きまして、犯罪収益移転防止法につきましては、金融機関と同じ法律、法令になっておりまして、電話転送や電話受付代行、電話秘書サービス、こういったようなものが対象

になっておりますが、金融機関と同等の本人確認等の義務が課せられております。取引時確認といいまして、法人については、個人だけじゃなく、最終的に自然人まで遡って本人確認されるような制度になっております。また、疑わしい取引の届出といった追加的な義務もございます。

利用停止スキームにつきましては、後半のほうでまた議論させていただきたいと思っておりますが、特殊詐欺に使われた電話番号、特に固定電話番号、こちらのほうを卸元の電気通信事業者さんと協力をいたしまして、警察からの要請に基づく利用停止を行うという取組を、令和元年から開始しております。これも順次拡大してきておりまして、050番号を追加したり、新たに、TCAさんだけではなくて、JUSAさん、日本ユニファイド通信事業者協会さんとも取組をスタートしました。去年６月には、悪質な電話転送サービス事業者の保有する固定電話番号、在庫番号の利用停止ということで、かなり広範に特殊詐欺に使われる電話番号を防ごうと取組を進めているところでございます。

昨年の３月、犯罪対策閣僚会議で、SNSで実行犯を募集する手口による強盗・特殊詐欺事案に関する緊急対策プランが策定されております。SNSで実行犯を募集する手口というのは、いわゆる闇バイトのことでありまして、闇バイトに基づく事案が発生したということで、いろんな施策を各省庁位置づけられておりますけども、特に黄色マーカーしたような、電話や通信に関する対策というのも数多く盛り込まれております。昨年６月のフォローアップでも、総務大臣から発表いたしましたけれども、順次取組を進めてきておりまして、周知広報の取組ですとか、ナンバーディスプレーの普及拡大、そういった取組をしてきています。６月時点では準備・検討を進めていると書いていましたが、050アプリ電話については省令改正を実施しておりますし、在庫番号の対策というのも進めております。

今回議論いただきたい内容として、携帯電話契約時の本人確認のマイナンバーカードの活用、また、券面の偽変造による不正契約というのが非常に厳しい状態ですので、その更なる対策を進めたいと思っております。ほか、今回まさに議論いただきたい話で、SMSの対策については現状分析を進めてきたところでございます。この後、SMSについてはマルウェアに基づくものが多いとか、データに基づいて詳しく御説明いただきたいと思いますので、これは割愛したいと思います。

まとめますと、特殊詐欺対策については、本人確認のマイナンバーカード活用、偽変造への対策などについて議論いただきたい。また、利用停止スキームについては効果を上げておりまして、これをさらに適用事業者を拡大していくために取り組むべき事項について

議論いただきたいと思っております。SMSについては、特にマルウェアに感染したスマートフォンなどへの対策、実効性のある対応策について検討いただきたいと思っております。

夏までの大まかなスケジュールでございますけれども、今日が初回で、初回と第２回にわたってSMSに関する議論、３回目、４回目にわたって本人確認に関する議論、５回目、６回目にわたって電話の不適正利用、利用停止スキームですとかナンバーディスプレーについての議論を予定しております。

私のほうからの説明は以上になります。

【大谷主査】　事務局からの御説明ありがとうございました。

次に、マクニカの角谷様からお話しいただきたいと思います。どうぞよろしくお願いします。

【株式会社マクニカ】

それでは、SMS・スミッシングについて、進めてまいりたいと思います。よろしくお願いいたします。

今日、時間的には少ししかないので、たくさん詰め込んでおりますけれども、皆様、見て、聞いていただければと思います。全体的には、まず自己紹介を少しだけさせていただいた後、SMSという全般的なお話をさせていただいて、それを活用してといいますか、悪用してといいますか、スミッシングというところが今増えてきているというところで、その御説明をさせていただきます。事例とか文面とかも含めて御紹介をさせていただいて、どのような状況になっているのかというのを見ていただきたいと思います。その中でもさらに、マルウェア感染というところがかなり深刻になっておりますので、その実態や手口を御説明させていただいて、現状、海外で見えている事例と国内で見えている事例というところに進めさせていただきたいと思っております。

我々、まず撲滅活動を、もうずっと長きにわたって活動してきています。技術、知見、経験を土台として、この社会課題を解決していこうと、撲滅していきたいという思いを持って活動しております。

現在４つのパターンで進めさせていただいているんですが、フィッシングの対策支援サービスとしては、通信事業者様向けであるとか、エンタープライズ企業様向けであるとかいうような取組を実施させていただいております。さらに、フィッシング対策協議会などにも参加いたしまして、上流でガイドラインを組んでいって、より皆様と一緒に御支援を深めていく中で、進めていきやすい方向性をみんなで考えようということで、各種ワーキ

ンググループに参加して活動を行っております。私自身、運営委員もさせていただいておりまして、ワークショップの企画であるとか運営であるとかというところに携わらせていただいております。

そのほか業界の連携の支援も実施しておりまして、いろんなところで登壇を行っていましたり、技術勉強会を開催したり、あとは公共メディアで解説等も行っておりまして、今日来ているマクニカのほかのメンバーもおるんですが、ユーチューブの動画でユーチューバーデビューしております。

そのほか専門的な知見も我々として持っているところがありますので、特に全体像を俯瞰して見るような、手口であるとかメカニズムであるとか、犯罪エコシステムであるとかというようなところを具現化してホワイトペーパーをリリースし、英語版もリリースしています。

このような活動の一番土台にあるところは、もともとセキュリティに関する企業であるというところもありまして、研究センターやセキュリティドメインのチームであったりとか、テレコムのセキュリティチームであるとかいうところで、もともとやっていた御支援の内容だったり技術調査だったりとかというところを土台にして、我々の支援が昇華されているとお考えいただければいいかなと思っております。

では、本題に入っていきますが、SMSです。ここはもうおさらいにはなってくるんですけれども、ショートメッセージサービスの略語になっています。こんな感じでiPhoneだったりとかAndroidで、マスキングされているんですけども、これは電話番号の表示になっていて、一部アルファベットで表記されるケースもあるんですが、このような形で、件名がなくて、70文字程度のメッセージというのがショートメッセージサービスになっています。これを略してSMSと呼んでいて、４つの大きな特徴があります。

まず１つ大きいのが、SMSは全ての携帯電話に含まれる機能で、これはもともとアプリなどの設定は不要で、もう買ったタイミングで利用ができるというところです。あとは、電話番号で送受信が可能になるので、電話番号からそのままメッセージを送ることができるということで、とても簡単です。あとはスマホの機能になるんですけれども、ポップアップで着信をお知らせしてくれると、そしてそれをタッチすると、そこに書いてある、例えばリンクだったりとか電話番号に触るだけで閲覧できたり、電話につながったりということで、タイムリーに受領されて、次のアクションがとても取りやすい状況になっているというのがSMSになっています。

SMSの利活用の状況も見ていただくと、これはミックITリポート最新版から取ってきた情報にはなるんですが、２つ大きな発信源があります。まずは携帯電話の端末、私たちが使っているような携帯電話の端末からの発信と、２つ目、SMSの配信事業者からの配信があります。今回、この２つ目、企業が発信するSMSの通数をこのグラフに落とし込んでいるんですけれども、2023年は27億通だったところが、2028年、もちろん見込みにはなりますが、95億通と、年成長率が26.4％ということで、かなり利用用途が広がってくると見込まれていることが分かります。

どのような形で利用されているかといいますと、皆さんも受け取ったことがあるので分かる方もいらっしゃるかもしれないですが、本人認証としてワンタイムパスワードでSMSから送られてくるケースだったりとか、お知らせを企業さんがユーザーの方々に配信していきたいというときに、一斉配信を行ったりとかするときのお知らせ配信に使う。あとは、やはり回答率、開封率、着目数が高いというところもあって、アンケートをSMSを使って配信するというような形を取っていたり、あと督促として、緊急の用事があってお伝えしたいというような場合に使われるケースが多く見られております。

ここから少しずつディテールに入っていくのですが、SMSの配信経路、これは実は大きく分けて３つあります。こちら１番が国内携帯電話の端末、私たちが普通に使っていて、キャリアさんに行って契約をするというような形で、番号が090から始まるもの、080から始まるもの、070から始まるものなどがあります。

SMSの配信ルート２つ目は、国内の配信事業者さんです。ここが国内の固定番号、03番とか0120番号、そして後で少し触れるんですけれども、キャリアの共通番号というものも、この配信事業者さんから0005を使って配信されるという形になります。

３つ目が海外通信事業者になります。海外から来る場合、例を出しているんですけれども、050のパターンで、海外から来る場合はここが、例えば、ここにアマゾンと英語で書かれているケースなどが海外から来るというような形で考えていただければと思います。

この配信経路で一番大きなポイントは、３つとも、集約されて一本にまとまって、携帯加入している通信事業者のSMS配信サーバーを通過してSMS受信者に届くというところが最大のポイントでございます。必ずこれは加入している通信事業者のSMSの配信サーバーを経由していきます。例えば、ここに写っているSMSの受信者の方が、例えばドコモさんの電話でお話をしている場合は、SMSが来る場合、どこから来るとしても、必ずドコモさんのSMSの通信サーバーを通るような形になっているというところが重要なポイントになり

ます。

では、じゃあスミッシングって何でだったっけというところもおさらいをさせていただきたいと思います。まずフィッシングという言葉です。多分皆様は十分御存じかと思いますが、フィッシングというのは、まずクレジットカード番号や口座番号など個人情報を釣り上げる、いわゆるお魚釣りのフィッシングが語源になっているフィッシングになっています。このフィッシング行為をSMSで行うSMSフィッシングというのが、略してスミッシングと呼ばれているという内容になっております。なので、先ほどもありましたけれども、メッセージの下に電話番号やURLがついてきていて、ここをクリックさせて別のサイトへ誘導するというような形を取っているところになります。

先ほどの小澤さんの資料の中にもあったので、ちょっと重複している部分ではあるんですが、フィッシング詐欺が深刻な社会課題となっていて、かなり注目を今集めていて、私たちがいつも指標としているデータ、見ているデータとしては、クレジットカード協会さんのもので、私のほうで新しく出ていたデータも追加はしていて、少し減ってはいるものの、やっぱり376億、2022年には411億、これ全てがもちろんスミッシングではないにしても、トリガーとなって発生している可能性が大いに考えられるという意味で、私たちはこの数値を見ています。さらには、警察庁さんからも出ていたインターネットバンキングに関わる不正送金の被害額も、今回令和５年でかなりぐっと上がって80億になっているというのが現状ですので、やはりかなり深刻な状況になっていて、これだけを切り取ってみても氷山の一角であるということで、レポートされていないものとかも考えると、やはりもっと大きな被害があるのではないかと考えられています。

最近のスミッシングの事例を具体的に見ていただければと思って、こちら用意をしております。まず、SMSに記載されたリンクから詐欺のページにアクセスをさせる、ここは重要なお知らせを、三菱UFJ銀行をかたっているという形にはなりますが、一時規制しているので本人確認してくださいねということで、このリンクをSMSと一緒に飛ばしてくると。受け取った方がここをクリックしていくと、まさに本物なのではないかというようなページが現れてくるのですが、これは銀行口座利用に必要な情報を、この用意しているサイトに入力をさせるための偽ページということになっています。なので、ここに本人確認が必要なんだなと思って、いろんなことの情報を入れてしまうと、それがそのまま釣られてしまうという状況になっております。

文面も多々ありまして、先ほどのように、口座が凍結しちゃうから確認してねとか、本

人確認が必要なので、不正利用の可能性あるから見てくださいねとか、あとはよくあるのが国税庁をかたった、未払いのものがあるので確認してくださいとか、宅配系で、御不在だったのでお荷物を持ち帰ったので確認してくださいというような形で、様々な確認依頼が届くんですけれども、これは全て共通して言えるところは、受け取った方のまず不安をあおる文面で確認を急がせる内容が総じて多いということになっております。

これは先ほどの経路の図とかぶっているところなんですが、最近はマルウェアの感染端末がすごく増えているというところが深刻さをさらに増しているというところです。一昔前は、海外からやってくるスミッシングの発信が多いとされていたんですが、現在はマルウェアに感染した端末が主な発信元となっていて、そこから発信されていくので、９割以上がマルウェア感染で送られてくるスミッシングだと考えられています。

なので、先ほどの配信経路３つありましたというところの、個人の携帯端末にマルウェアがインストールされてしまうという形で、そのままスミッシングが受領者のところに届いていると。ただ、最後に、今各キャリアさんのほうでブロックを行うなどの対策も行っていただいているので、国内の事例のところでお話ししていきますが、もちろん進んではいるものの、やはりなかなか難しくて、何がそんなに難しいのかというと、感染端末というのは皆さんずっと肌身離さず持ち歩いていたりするというところもあるので、対策を実施していくというところがかなり難しいのかなと。なので、感染端末の把握であるとか、感染数の把握であるとか、無害化をどうやってやっていくのかというところの検討が、小澤さんも言われていましたけれども、かなり急務であるというふうに我々も考えております。

では、マルウェア感染端末のスミッシング配信の仕組みですけれども、スマートフォンが、意図しない不正アプリ、マルウェアをダウンロード、スミッシングでクリックしてしまって、そうするとChromeをアップデートしてくださいみたいなのが出てきて、イエスと押してしまうと。そうすると感染してしまい、自分でイエスと押している本人は、まさか自分が不正アプリをダウンロードしているとは全く思っていなくて、ただ端末はしっかり感染してしまっているので、このように悪い人がC&Cサーバーというサーバーに命令を出すと、このサーバーから、じゃあ感染端末の人はスミッシングを送ってくださいという指令を送って、一斉に配信するという形になっております。なので、個別のスマホユーザーに詐欺SMSが届いていくという実態になっています。このC&Cサーバーの命令はいろんなパターンがあるらしく、電話帳に入っている人にスミッシングを送るというケースもあれ

ば、用意した一覧の人たちにこの端末から送らせるとか様々できると聞いております。

マルウェアの感染の原因と手口ですけれども、フィッシングと同じです。結局リンクをSMSで送ってきて、ウェブサイトに誘導し、アクセスさせることでマルウェアに感染となります。

手口として２つありまして、クリックして飛ばすときに、Androidの場合とiPhoneの場合で挙動が違うといいますか、ウェブサイト側で端末がどれなのかというのを認識して動いているという事実があります。AndroidでURLクリックすると、このようにChromeをバージョンアップしてくださいねと出てきて、オーケーを押すと、有害なファイルの可能性がありますと、これをこのままダウンロード続行してしまうと不正アプリがインストールされるという形になります。

iPhoneで受け取った場合、iPhoneの場合はリンクをクリックすると、iPhoneはアップルストアから買ってくださいとか、アプリをダウンロードしてくださいということで他のところからローディング、ダウンロードすることができないということで、感染しないとされています。なのでiPhoneの場合は、アップルアカウントは安全異常があるので再度ログインしてくださいというような形で、不正アプリをダウンロードさせる仕組みにはならず、アップルIDを取得するという方向に動くという形になっています。

マルウェア感染の対策例として幾つかあるんですけれども、今回はニュージーランドのケースを皆さんに御紹介します。こちらは2021年９月に始まったFluBotマルウェアで、最初の９日間で11万件の通報があって、ニュージーランド国内の通信事業者に大きな影響を与えていました。被害が欧州全体に広がってきて、最終的にはたくさんの方々がインボルブされて、法執行機関やいろんな国の方々と協力して、悪いことを行っているサーバーを止めるという手段に至っていますが、これは政府が介入して行われた事例になっています。

基本的には、攻撃手法は先ほどの内容と同じで、スミッシングをこういうスマートフォンに送信し、リンクにアクセスさせて、ダウンロードさせて、マルウェア感染させて、どんどんそれが拡散されていってという状態をぐるぐる回していって、被害が増えていくという状態になっていました。対策の内容として一番最初にポイントとして見ていただきたいのは、体制の確立と初動の対応と、最終的にサーバーを止めるという対応を行ったという、この３つのフェーズに注目していただければと思います。

対策に関しては、DIA、内務省さんが緊急対策グループというのを設立して、いろんな関係各所、通信事業者さんとか機関とかに入ってもらって、最初の通報から３時間以内で

立ち上げて、２つの対策、まず初動対策をしています。感染者向けに、あなたのお電話、端末が感染していますよということで所有者に連絡をして、マルウェアの削除手順を通知するというのを24時間400回の連絡をして、マルウェア感染している被疑の電話番号の端末も600件見つけて対処を行う。その一方で、SNS等でも、スミッシングでこういう怪しいものが飛んでいるという告知もやりながら、怪しいメッセージはしっかりとレポーティングして、この7726というスパムレポーティングサービスへの通知を促して最新情報を更新しながら対応を行っていたということになります。そして最終的には、ユーロポールなども含めて、しっかりと国際協力を行った上で、そのサーバーをしっかりと停止するというような形の活動がなされていたという報告があります。

そしてもう一つ、先ほど出ていたスパムのレポーティングメッセージですけども、こちらもスミッシングの共通窓口による対策の推進だったことになります。ニュージーランドは7726ということで、実はこれ、ニュージーランドだけではなく、アメリカやイギリスでも実施されている申告窓口になっています。ガラケーでぽちぽちやったことある方は分かるかもしれないですけど、「SPAM」だと、７をたたきますよね、７を４回。Pは７を１回で、Aが２が１回の、Mが６ということで、7726で「SPAM」だったということで、すごい納得感がある番号だったということでございます。

国内の事例、SMSを通るのは全て、キャリアさんのサーバーを介して通っていきますというお話がありましたけれども、こちらドコモさん、KDDIさん、ソフトバンクさんの３社はネットワーク側の対応も進めていただいておりまして、2022年３月から順次、ドコモさんが一番最初に危険SMS拒否設定をスタートされまして、その後、ソフトバンクさん、KDDIさんということで順次、迷惑SMS、危険SMSのブロックがスタートしています。さらには端末側の対応も行っているキャリアさんもいらっしゃるので、その辺りでしっかりと国内でも、不正なSMSをブロックする対策が進んできているという状況になります。

そして、新たな取組としてRCSと共通番号も出てきています。リッチコミュニケーションサービスという正式名称のRCS、頭文字を取っています。これは世界標準に基づいて、SMSと同じように携帯電話番号で送ることができるメッセージではあるんですが、SMSとはまたちょっと違っていて、違いとしては、SMSより多くの文字を送付できたり、公式マークというのを設定してメッセージ自身やり取りができたり、テキスト以外に画像だったりグループチャットが行える。あとは、呼び方が、ドコモさん、KDDIさん、ソフトバンクさんでは「＋メッセージ」と呼んでいて、楽天モバイルさんではRakuten Linkという名称で

サービスの提供が行われています。アップルに関してはRCSのユニバーサルプロファイルを2024年の後半にサポートする予定ということで表明されているので、広がってくるメッセージサービスというところになります。

あと、キャリアの共通番号です。最後に0005も御説明していきたいと思います。

通信事業者４社、ドコモさん、KDDIさん、ソフトバンクさん、楽天モバイルさんが管理する0005から始まる８から10桁の番号です。これは、ユーザーが契約している通信事業者が、どこのキャリアでも、１企業は同じ送信番号を使ってメッセージを送ることができますよということになっています。さらには通信事業者側でも審査があるので、番号が重複してないよねとかいった審査を通り抜けて、共通番号として使われる形になります。それを企業さんが事前にウェブサイトなどで、こういう共通番号を使ってSMSを送りますよというようなお話をお客様に事前にしていただくとすると、より安心して受け取っていただけるのではないかという取組になっています。

キャリアさんがそれぞれ配信をするというよりは、SMSの送信サービス、先ほどあった国内の事業者さん、配信事業者さんがありますというお話があったと思うんですけど、そことの連携になりますので、0005番号というのが、真ん中の配信系のところに組み込まれていた形になっています。

まとめとしては、戻りますが、SMSは全てのスマートフォンで利用可能で、買ったタイミングで使えます。高い到達率で開封率を誇る、とても便利なメッセージサービスになっております。ただ、その便利なところに便乗して、スミッシングが横行していて、大きな被害が出ていて社会問題になっています。さらにスミッシングがマルウェア感染を深刻化しているということもありますので、感染数の把握だったり、スミッシングの稼働状況だったり、そういったディテールを見ながら対策の検討というのが急務ではないかというところです。あと、マルウェアの感染は、ニュージーランドをはじめ、日本以外でも発生が確認されていて、実際に政府が協力して対策を講じている例も存在しているということなので、その辺りのやりようというのは、今後我々が対策を進めていく上でも参考になるのではないかというところになっております。

私からの説明は以上となります。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。ぴったり25分で、ありがとうございます。完璧でした。

【株式会社マクニカ】　ありがとうございます。

【大谷主査】　では、次はトビラシステムズの柘植さんにお願いしたいと思います。よろしくお願いいたします。

【トビラシステムズ株式会社】　トビラシステムズの柘植と申します。

では、トビラシステムズのほうから、Androidマルウェアによるスミッシングの状況をお話させていただきますが、スミッシングモニターというタイトルになっていたかと思います。我々のほうで先日２月１日に、スミッシングの状況がリアルタイムに分かるウェブサイトを公開しましたので、そのサイトについても最後にお話をしたいと思っております。

まず、トビラシステムズ、我々の会社概要の話になります。我々トビラシステムズは、特殊詐欺犯罪の被害をゼロにすることを目指しております。設立は2006年でして、創業は2004年と、もうすぐ20年になる会社で、本社は名古屋に構えてやっております。代表の明田の写真が載っておりますが、明田の祖父が、原野商法と言われる、ほとんど価値のない土地を、別荘地として値上がりするなどと偽って高額で売りつけるというような商法があるんですが、それに引っかかってしまいまして、何とかこういった方々を助けたいと、詐欺の被害を少なくしたいという思いで、我々の主力の製品であります迷惑電話フィルター及び、そこからその後、迷惑SMSのフィルタリングというのも始めまして、今では利用者数が1,500万人以上のサービスに成長しております。

先ほどの詐欺SMSとか詐欺電話とか、特殊詐欺及びフィッシング詐欺に対しては、我々のほうでも重要な社会課題であると認識しておりまして、これらの解決に向けたアプローチとして、我々のほうでは迷惑情報データベースというものをつくってサービス化しております。特殊詐欺やスミッシングといったものの被害を考えてみますと、危険な電話に出てしまうとか、あるいは受信したSMSに反応して危険なURLを触ってしまうといったことが被害に遭うきっかけとなるわけでございます。ですから、この電話番号ですとかSMS、URLというのを収集して迷惑情報データベースというものをつくりまして、これを活用してブラックリスト化するなどいたしまして、当社のサービスの利用者を危険から守ると、フィルタリングすることで、こういった電話とかSMSに反応しないようにというサービスを提供しているものでございます。

下半分に関しましては、この迷惑情報データベースの強みというところで挙げさせていただいております。左のところに３点挙げておりますのは、我々のデータベースには警察から、犯罪や攻撃に使われたと見られる電話番号ですとか、URLのデータ提供を受けておりまして、このデータが含まれているという点が１つ目の強み。それから２つ目、利用者

から電話番号やSMSのフィードバックを受けられる体制、そういったサービスになっているというところで、利用者様、今1,500万人以上みえますが、その方々の電話の発着信ログであるとか、SMSの受信ログ、こういったデータを基に、日々データベースの精度を高めているというところがございます。また、これらのデータを使いまして、当社の調査チームは日々調査分析を重ねて、最新のデータを反映しているという状況でございます。以上が我々の迷惑情報データベースの強みです。

次に行きまして、このデータベースを活用しまして、大きく３つの分野でサービスを展開しております。１つが左にありますモバイル向けと、真ん中が一般の御家庭で使っていただくような固定電話向けのもの、そしてビジネスフォン向けと、３種類に展開をしております。電話に関しての脅威に関しては全方位からカバーしていまして、重ねてになりますが、1,500万以上の方に使っていただいている状態です。

今回のスミッシングのお話でいいますと、一番左のモバイル向けです。上に３つアプリのアイコンが並んでおりますが、こちらはソフトバンクさんとドコモさん、あとauさんと、３キャリアのサービスを通じて我々のフィルタリングサービスを提供しているといった状況になります。モバイル向けですので、モバイルにかかってくるような電話とかSMSというのをブロックして、日々データベースの精度を高めてサービスしているといった状況です。

ごめんなさい、それと、ちょっと資料に載せていないんですけれども、冒頭でお話のあった犯罪に使われているような電話番号を停止するスキーム、JUSAのほうに我々も加盟しておりまして、総務省様と警察庁様、各県警と連携いたしまして、各通信事業者様に対して、この番号は犯罪で使われたものだから停止してくださいというような要請を行う取組に我々も参加しております。我々自身のサービスだけではなくて、そういった外部との連携も強めて、特殊詐欺なりに対策をしていこうという体制でやっております。

これまでが会社の概要の御説明になります。本題に入りまして、ここからはスミッシングの話になります。

１点目、国内のSMSフィルタリングはどこでやっているのかという２つのポイントの話と、２つ目はスミッシングと不正送金被害の状況です。３点目に、スミッシングはどこからやってくるのかといった送信元の話です。ここまでの話の中で、Androidマルウェアによるばらまきというのが多いというお話があったかと思いますが、その割合はどれぐらいなのか、一方でiOSはどうなのかという話に少し触れたいと思います。４点目が実際

Androidマルウェアについての詳細なお話です。現在２大Androidマルウェアというものがあると我々のほうでは考えておりまして、これらの御説明になります。最後５点目として、冒頭タイトルになっていましたスミッシングモニターです。公開の中ではスミッシング以外も、詐欺のSMSも含めて全般使うというものにいたしましたので、名称としては、すみません、詐欺SMSモニターとなっております。

それでは１点目、国内のSMSフィルタリングの２レイヤーということで、現状、国内のSMSフィルタリングは、ネットワーク型のところとクライアントアプリ型のところ、２つのレイヤーでの防御となっている状況でございます。左側に図示しておりますとおり、まず前段にネットワーク型のファイアーウオールがおります。ここでフィルタリングにかかればSMSは破棄されます。ここで擦り抜けてしまったものというのが２つ目、クライアントアプリ型のところです。スマートフォンまで到達して、このアプリでフィルタリングにかかれば、警告をするか、あるいはスパム、迷惑フォルダーに隔離するといった状況になります。

この特徴を右側の表に少しまとめておりますが、ネットワーク型というのは破棄されますので、端末に届かないわけで、非常に強力で、ユーザーはそのSMSに触りようがありませんので非常に安全といった特徴があると思いますが、一方で、フィルターされたSMSというのをユーザー様は確認できないので、誤検知の影響は大きいものとなってしまうという特徴もございます。一方、下の２つ目のクライアントアプリ型では、警告あるいは隔離するにとどまりますので、端末には届くというところから、フィルターされたSMSでもユーザーが確認できて、誤検知の影響は少ないという特徴があるかと思います。ですので、ネットワーク型のほうは、強力だが消極的にならざるを得ないところがあります。一方でクライアントアプリ型は、到達してしまうんですけれども、その代わり積極的なアプローチが取れるといった特徴があるかと思います。

本資料、ここからデータなんですけども、我々のほうで提供していますクライアントアプリ、こちらの利用者、現状ソフトバンク様、au様、ドコモ様と、３キャリア様を通じてやっておりますが、ここのSMSのログに基づくものとなっております。

２点目です。スミッシングと不正送金被害の状況ということで、我々のデータと、警察庁・金融庁様から出ているデータ、右側のところはこれまでも何度か出ておりましたので、よいかなと思っておりますが、左側のグラフは我々のデータになります。2022年11月ぐらいから、我々の見ているスミッシングというのが大幅に増加しているのがグラフ上でも見

てとれるかと思います。これに合わせて連動していると言い切っていいかはちょっと不明ですけれども、右側の2023年のインターネットバンキングに係る不正送金の被害というのが、令和５年、2023年は80億を超えるという状況になっておりまして、スミッシングも増えているし、ここの被害も増えているというような状況が見てとれるかと思います。

３点目になります。ここからスミッシングの送信元の話に入っていきますが、Androidマルウェアによるばらまきがほとんどであると、先ほどマクニカ様のお話にもありましたとおりで、我々の観測するスミッシングにおいても、９割以上はAndroidマルウェアによるばらまきのSMSであるというのが確認されております。ここに映っているのは、直近先月の最終日、１月31日のデータを少し持ってきたものでありますが、一番左のところ、Androidマルウェアの感染疑いのある携帯電話番号からのものというのが99.6％と、ほとんどを占めるという状況にあります。

その中でも文面を見てみますと、ブランドのところ、この日はですが、宅配事業者をかたるものが56.3％と半数以上を占め、その下のソフトバンク様を語るものが43.1％と、この２つがかなり多い状況であるというのが分かるかと思います。

続いて、iOSのマルウェアがあるのかというところです。iOSアプリを用いたスミッシングということでいいますと、現時点では流行はしていないのかなと考えております。App Store、アップルのアプリをダウンロードするアプリケーションのほうにアプリをアップロードする、公開するには、かなり審査が厳しいということも一つありますけれども、あとiOSの仕様上、ユーザーが操作しないSMSを送信するような機能、こういった機能が開発できないわけです。ですので、Androidのように、バックグラウンドでSMSを大量にばらまくといったようなアプリをそもそも開発できないという特徴がございます。ですから、スミッシングのSMSのばらまきの手段として、iOSはそもそも対象にされていないと現状では思われます。

ただ、最終的にアプリをインストールさせるものかは不明なんですけれども、ここにスクリーンショットを載せておりますが、構成プロファイルというファイルをダウンロードしてインストールすると、端末の中の設定を幾らか書き換えられる仕組みがありまして、そういったもののインストールを誘導して、端末に何らかの害を及ぼすおそれのある攻撃、こういったものは確認したことがあります。

続いて、ここからAndroidマルウェアの詳細に入っていきますが、２大Androidマルウェア、２つの大きなAndroidマルウェアが存在しているかと我々のほうでは考えております。

１つ目が、左側にありますMoqhaoあるいはXLOADERと呼ばれるようなものでして、これは主に宅配便の不在連絡、不在通知ですね、こういったSMSをばらまいて、iOSに関してはAppleをかたるフィッシングに誘導し、Androidに関しては同じMoqhaoのマルウェアをインストールするように誘導されます。

右側が２つ目です。こちらはKeepSpyなどと呼ばれているものでして、直近の手口で言えば、12月22日から今年の１月23日の期間においては、三菱UFJ銀行様をかたるフィッシング、これはiOSとAndroid、両方とも三菱UFJ銀行様をかたるフィッシングに誘導するものでした。１月26日から、24、25は空いているんですけど、この２日間はドコモ様のd払いをかたるものを確認しております。26日からはソフトバンク様をかたるSMSがばらまかれておりまして、iOSに関しては同じソフトバンク様がたりの架空請求サイト、Vプリカというプリペイドカード、このVプリカに書かれているコードを入力すると４万円分で使えるというものなんですけど、これを入力して４万円分奪うといった手口です。Androidに関しては、同じこのKeepSpyをインストールするように誘導されるといった手口になっています。

ちょっと直近のデータで、資料上はないんですけれども、21日からは、ソフトバンク様がたりからKDDI様がたりに変わっております。手口としては似たようなもので、Vプリカの請求、あるいはマルウェアのインストール誘導という形になっております。

インストールの流れを示しています。これはMoqhaoです。宅配便がたりのほうを一つ持ってきておりますが、インストールしてしまうと、Chromeのブラウザを装うマルウェアをインストールさせるといった手口になっています。

SMSのリンクをクリックすると、Chromeの最新バージョンにアップデートしていくという内容の画面に着地して、以降ダウンロードしていきたいという、この手口は、正規のAndroidアプリですとGooglePlayからダウンロードするというのが正規のルートなんですけれども、Chromeからダウンロードするということになるので、提供元不明なアプリと定義されますので、ここの提供元不明のアプリを許可するとしないとインストールができないということですので、既にオンに設定済みの場合はこのステップは要らないんですけれども、初めての場合にはここをオンにしないとインストールに進めないという状況です。

その後は、インストールをタップして開くというところまで行って、インストールが完了となります。

続いて、初回起動のときに、もろもろ権限を取得する動きがございます。その流れにな

ります。

SMSをばらまく点でいえば、一番最初のSMSの送信も許可するかというところで許可をすれば、ばらまくことになってしまうというところでございます。

そのほか、連絡先のアクセス、電話の発信・管理のアクセス、メディア・写真等のアクセス、あとバックグラウンドの実行の許可、それと最後、SMSのアプリとして設定するかというところで、Chromeと出ていますが、これはマルウェアのことですね、マルウェアを設定してしまうとSMSのデータについてアクセスができてしまうといったところでございます。

次、マルウェアのばらまきの時間の傾向を示しております。これは2023年、去年の12月の日ごとの時間別のスミッシングの件数のグラフになっております。

これを見ますと、赤枠で囲ったものが、宅配便をかたるMoqhaoがばらまいている時間帯。それと黄色のところ、ここがKeepSpy、通信キャリア様や官公庁様、金融機関をかたるものです。見ると、昼のMoqhao（宅配便）と、夜のKeepSpyとすみ分けがされているような印象を受けます。

最後、先ほどのスミッシングモニターについてです。詐欺SMSモニターですけれども、これは一般のユーザー様向けに、注意喚起あるいは啓発目的のウェブサイトとして我々が制作したものでございます。サイバーセキュリティー月間に合わせて、２月１日から３月18日まで、限定公開の予定で公開をしております。Androidのマルウェアをはじめとしたスミッシングの情報をいち早く確認できるようにつくったものでございます。

大きく４つのコンテンツがありまして、１つ目は詐欺SMSの件数のリアルタイムなグラフです。前のページでお見せしたような、ばらまきが発生しやすい時間、警戒すべき時間の傾向を可視化して、一般のユーザー様には日頃見えにくいところ、ばらまきの波があるといったところをお伝えできればと思って用意したものでございます。

２点目が、Androidのマルウェア感染端末台数です。ここは我々のサービスを通じて集まってくるSMSのログ、その傾向を基に、当社で観測する限りのマルウェア感染が疑われる台数というのを掲載しております。

３点目に関しては、「知っていますか」というタイトルになっておりますが、一般の方々はまだまだ、スミッシングの送信者というのは多くは被害者、つまりマルウェア感染者であることを知らないのかなと私のほうでは感じておりまして、こういったことを知っていただきたいなと思ってコンテンツ化したところでございます。あとは、マルウェアの

感染手口についてもコンテンツ化して掲載をしております。

４点目は、詐欺SMSのギャラリーとして、こんなSMSがばらまかれているよという文例を幾つか掲載をしております。

最後、ちょっと参考データに触れようかなと思いますが、これは生成AI活用ということですが、右側に見えているのは12月25日のクリスマス、MoqhaoのばらまきのSMSが47種類、この日は確認されておりまして、あした再配達を予定だというようなメッセージが来ますと。「クリスマスのプレゼントがあしたになってしまう」と慌ててURLにアクセスしてしまう人も、中にはいるのかなというところです。

ここなんですけれども、「ここ最近」と書いてあるのは10月26日以降ですが、１日当たり数十種類の文種がほぼ毎日、しかも重複なく送信されている傾向を確認しております。

これを人間が毎日つくり続けられるかというとちょっと疑問を感じるところでございまして、恐らく生成AIを活用しているのかなと考えているところでございます。

最後、これは日ごとのターゲットになっているブランドの割合です。2024年１月、先月のターゲットブランドの割合になっています。

注意点として、これはSMSの本文中のブランド名称を集計したデータでありまして、宅配便がたりというのは本文中にブランド名称を現在かたれませんので、ヤマトさんとか佐川さんとか有名なところの名前が入ってこないもの、こういったものは除いているという形になります。ですから主にKeepSpyと考えられます。KeepSpyプラス少量のものですね。

見てみると、先ほどちょっとお話ししたような１月23日までは三菱UFJ銀行様がたり、26以降はソフトバンク様がたりが多いといった傾向が見られます。

というところでございまして、我々、特殊詐欺、あるいは詐欺SMSを含めて、３キャリア様を通じて横断したデータを用いて、幾つかの統計とかは出せるので、このワーキンググループに関しても、例えばこんなデータが見たいとか、そういった統計的なデータをお出しするという点で、何かお力になれることがあればなというふうに考えております。

それから、やはり今回、Androidのマルウェア感染の端末の特定ですとか、それらの方々に対してどうアプローチするのかというところが主題になっているかと思いますので、先ほどの詐欺SMSモニターの②のところ、感染端末台数というのも我々は出しておりますので、これは推移とか、日ごとにどう移り変わっていくのかといったところなども、もしかしたら一つのベンチマークとして置かせていただくことができるのかなというふうに思っています。

以上となります。ありがとうございました。

【大谷主査】　どうもありがとうございました。貴重なデータを提供いただきましてありがとうございます。

それでは、事務局の説明に始まりまして、マクニカ様、トビラシステムズ様からの発表がございましたので、その内容について、御意見あるいは質問、コメントなどございましたら、右下のチャット欄を使いまして、送信先を全員としていただきまして、御発言の希望を御記入いただければと存じます。

特にテーマは絞らずに行きたいと思いますので、どこからでもお願いしたいと思います。私が見えていないところもありますので、事務局のほうでもし書き込みを見つけてくださいましたら、お知らせいただけるとありがたいです。

ありがとうございます。沢田構成員からの御質問、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。大変貴重なお話を両社からいただきましてありがとうございました。

マクニカさんとトビラシステムズさんに、可能であれば２点ずつ御質問させていただきたいです。まずマクニカさんのお話で、SMSについて実はあまり何も知らなかったことに気づきました。特にSMSの配信事業者という存在があることを知らなかったので、非常に基本的な質問で恐縮なのですが、我々エンドユーザーとしては、SMS配信事業者さんとはもちろん契約はしていないと思うのですが、なぜ配信事業者からのSMSが我々に届くのかということをお尋ねしたいです。恐らくは、通信キャリアさんと我々が契約するところで何らかの同意をしているのではないかと思うのですが、そういう理解でよいのかどうか。また配信事業者さんは、我々個人ユーザーの携帯電話番号のリストを持っているのか、それとも、キャリアさんの保有するリストを使って配信しているのかという、非常に基本的な仕組みの質問です。これが１点目です。

２点目が、ニュージーランドの例を御紹介いただいて大変興味深かったのですが、それと同じような、サーバーを停止したり、感染していると思われる端末をお持ちの方に警告を発したりということを日本でやろうとした場合に、法的に制約があるのかどうかということです。ニュージーランドでやっていることが日本でできるのかどうかをお尋ねしたいと思いました。

取りあえずそこまで。ありがとうございます。

【株式会社マクニカ】　ありがとうございます。まず、配信事業者さんと企業さんがそ

れぞれ契約をされていて、企業さんも、お知らせだったり、例えばサービスが終わった後のアンケートとかというのを、配信事業者さんにお願いをして出してもらうというような形を取っているというところです。なので、ビジネス利用の場合は、企業がお持ちのリストを使っていくというのが回答になるかと思っております。

あとは、電話を契約するときとかに、そういうお知らせを配信するのに、例えば事業者さんを使いますよみたいなところは、契約に含まれるというような流れになる理解でございます。

あと、ニュージーランドの件は、まさにこのWGで議論をしていけたらなというのが小澤さんの一番のお話だったかとは思うのですが、まずは通信の秘密という法律がありますので、例えばキャリアさんが持っているサーバーとかで端末に感染していそうだなというのは、恐らく、今日はキャリアの皆様もいらっしゃるので、あらかた分かるケースもあれば、トビラさんみたいにもう確実にそうだろうというのもあるはあるのですが、その情報を基にコンタクトを取っていくというところに関しては、小澤さんももしあれば御意見いただければと思うのですが、やはり通信の秘密で、本来であればそういう情報というのは見ないし分からない、みたいなところがそもそものベースなので、やはりそこを突き止めてコンタクトを取るということに対してどうなのかなというところを、法の解釈であったり、もちろん、それで多額に例えば請求が来ちゃうから困ります、みたいなところでオーケーが出るケースも人によってはあるかもしれないし、というところで、やっぱりその辺りがあるのかなというので、全く同じことを今すぐ右に倣えでやれるかというと、ちょっと今いまは難しいのかなというところが見解です。

【沢田構成員】　ありがとうございました。

【大谷主査】　ありがとうございます。そのまま続けてトビラさんにも御質問がおありですか。

【沢田構成員】　ではお言葉に甘えまして。トビラシステムズさんの話も大変興味深く伺いました。キャリアさんのサービスと思って利用していましたが、実はこのデータベースのお世話になっているというのを初めて知った次第です。ありがとうございます。

質問は、通信の話とはちょっとずれてしまいますが、クレジットカード情報の不正利用も別枠で大きなテーマになっていて、そちらでも、不正取引の情報を集めたデータベースをつくって共有する試みを少しずつ始めようとしています。通信の秘密というよりは個人情報の問題ですね、電話番号にしても何にしても個人にひもづくデータ――個人に関する

データだと思いますので、その点について、データベースを作るにあたり何か制約があったのか、特になかったらなかったということで結構ですし、あったけれどもこうやって乗り越えたという話があれば、御教示いただければというのが１点です。

２点目は、OSの違いによってセキュリティーの組み方が違うということで、iOSのほうはバックグラウンドで勝手に送信しないようにしているというのも大変よく分かったんですが、今後のことは置いておいて、現状は、Androidのほうは結構まずい状態だと思うのですが、それに関してGoogleさんは何とおっしゃっているかという、OS事業者さんとお話しされたことがあれば教えていただきたいなと思いました。

以上２点です。ありがとうございます。

【大谷主査】　では、トビラシステムズさんのほうから御回答をお願いいたします。

【トビラシステムズ株式会社】　１点目、まずクレカの不正利用の情報を共有することにつきまして、どうやって乗り越えたのか。これは個人情報に近しいものであるというところから、どう乗り越えたのかというところだったかと思います。

我々のほうでSMSなりから得られる詐欺のURLとか、この中にもやはり個人情報というのが含まれておりまして、これをどうやって横展開するかといったような趣旨なのかなと伺いましたけれども、我々の中では、そもそもアプリを通じて、ユーザー様から同意を得てデータをいただいておりますので、その範囲の中でしか扱えないというのはそのとおりでございまして、その範囲の中で使っているというのが回答になるかなと思っていますが、御趣旨に適っておりましたでしょうか。同意をいただいている範囲の中であるからやれているという形になります。

【沢田構成員】　分かりました。ありがとうございます。

【トビラシステムズ株式会社】　２点目、OSの違いについての話で、Googleが何と言っているかというところですけれども、ちょっとここは、私どもで直接Googleさんとお話ししたことはなくて、フィッシング対策協議会様などを通じて、Googleのほうでの取組というのは聞いているところの範囲の中ではありますけれども、やはりAndroidマルウェアが流行しているというのは認識はされているようでして、アプリケーションを特定するようなアプリケーションIDというものがありますが、これが不正なものがあれば報告するとしますと、同じようなアプリケーションIDはインストールできないというようなことを、GoogleのAndroid端末の中でやっていただくような、そういうセキュリティーの機能がありますので、それで対策をしているということは聞いております。

【沢田構成員】　ありがとうございました。

【大谷主査】　御回答ありがとうございました。

それでは続きまして、辻構成員から御質問があるそうです。よろしくお願いします。

【辻構成員】　今、発表になった２社さんに限らず広くということでしたので、ちょっと御質問をさせていただきたいのが、まずSMSの仕組みって、私、大変不勉強で理解していないところもあって、御説明いただいて大変理解できたところではあるんですけれども、そもそも最初の、不正利用で400億以上、令和５年度にありましたという中で、このマルウェアによって送られるものが原因なものがどれぐらいあって、マルウェア以外のものはどれぐらいあるのか。

マルウェアのものが多ければそのマルウェアに対応すればいいというのは分かるんですけど、マルウェア以外のものであれば、今度はSMSの仕組み自体にある程度手を入れていくことが必要かなと思って、そういったところの、逆に言うとSMSの仕様でいうと、これは多分国際標準とかそういったところも絡んでくると思うんですけれども、日本国内に限らず国際的な状況ってどうなっているんでしょうかというのがちょっと気になりました。

というのがそもそもとして知りたいポイントではあります。ただ、これはどなたに質問していいか、ちょっと分かりません。

それで、コメントなんですけど、先ほどあったOSについてなんですけど、世の中でよく感じる――すみません、セキュリティの専門家としてちょっと言わせていただくと、何か世の中的にiOSはすごく安全というふうに思われがちなんですけれども、決してそうじゃなくて、iOSはAppleがエコシステムというか、囲い込んでいるがゆえにマルウェアが入りづらい世界を実現できているんですけれども、逆に言うと、何かアクションを取ろうとしたときにiOSは非常にやりにくいということも御認識いただきたいなと思っておりまして、世界的なシェアでいうと、iOSとAndroidは、Androidが７割でiOSのほうがマイナーな３割で、日本国内に関してはこれが５対５ぐらいであるという特殊事情であると。

さらに、私、スマホ搭載をちょっとやった経緯でいいますと、Androidは逆に言うと話しやすく――つまりGoogleとですね、話しやすいし、新しいことを提案しやすく、組み込みやすい。ではありますけど、Appleに関してはそこは非常にやりづらい。

ですので、Appleが単純に安全だからといって、Androidがどうだからという議論は、ちょっと気をつけたほうがいいかなと思っております。これはコメントです。

以上、よろしくお願いします。

【大谷主査】　質問とコメントをありがとうございました。最初の質問は、被害総額におけるマルウェア感染している端末の割合ということなんですけれども、この400億というのは特殊詐欺全般ということなので、そもそも多分、相当違うと思うんですけれども、事務局のほうで御存じの情報などがありましたら、まず事務局のほうから御回答いただいてもよろしいでしょうか。

【小澤利用環境課課長補佐】　事務局でございます。今、大谷先生がおっしゃったとおりて、特殊詐欺の被害額400億というのがありましたし、クレジットカード盗用被害額も400億みいな話がありましたけれども、いずれにしても、フィッシングについて、これがSMS発なのか、メール発なのか、ポップアップ広告発なのかというのは、なかなかそこまでの統計がないと。さらに、SMS発のもののうちマルウェア発のものがどれぐらいなのかというのは、さらに見えていないところです。

先ほどの99%みたいな話は、キャリア側のフィルタリングないしトビラさんの、メールのメッセージを見て止めたものの中で９割以上という話があって、だから類推するしかないところであるんですけれども、被害額に基づいて、そこの出本がどれかというデータは、多分ないのかなとは思っております。

【株式会社マクニカ】　ありがとうございます。弊社マクニカの鈴木一実からぜひ追加で。

【株式会社マクニカ】　僭越ながら、マクニカの鈴木からコメントさせていただきます。集計のデータがないというのはそのとおりなのですが、しかし対策する上で、ないと言い切ってしまうとなかなか考えも進まないかと思いますので、コメントさせていただきます。

まず、フィッシングの発生の被害を大きく２ステップに分けて考えると分かりやすいかなと思っています。前工程というふうに考えていいと思うのですが、ステップ１が、フィッシングによって情報を抜き取るという行為です。この前工程に当たる部分は、今SMSを使って偽サイトに誘導して情報を抜き取るというのが主流になっています。

では後工程はというと、その抜き取った情報を、また別の誰かが不正利用していくというものです。先ほどあったクレジットカード利用の年間400億とか390億とかいう被害額は、その後工程によって発生していくものになります。

例えば、クレジットカード番号の不正利用に関していうと、あれは番号盗用被害といいまして、オンラインで盗まれてしまった情報を盗用されての被害になるんですけど、技術的には、その中身というのはフィッシングで盗まれるパターンとか、あとウェブスキミン

グなどの技術とか、あとはいわゆるデータベースの情報が漏えいしてしまってクレジットカード番号とかが全部漏れるというケースとか、いろいろごっちゃになっていると私のほうでは考えております。

フィッシングのお話でいえば、先ほどのお話のとおり、前工程でSMSが主流になってきたと。そこですね。

以上になります。

【辻構成員】　すみません、今のお話で、前工程でSMSが主流ということなのですが、SMSの発信元自体は、マルウェアに乗っ取られた端末によるものが多いということなんですか。

【株式会社マクニカ】　そうです。今、日本国内はそういうことになります。９割以上がマルウェア感染端末だと言われています。

【辻構成員】　承知しました。

【大谷主査】　鈴木さん、どうもありがとうございました。

それで、辻構成員からの御質問のもう１件、国際的な動向についてはどうなのかといったことについて、どなたか情報をお持ちの方はいらっしゃいますでしょうか。事務局のほうで何か集めていらっしゃる情報はありますでしょうか。

【小澤利用環境課課長補佐】　事務局でございます。国際的な状況については、なかなか我々も理解し切れていないところもあるんですけれども、先ほどちょっとあった、メールの世界では我々もこれまでいろいろやってきたところもあって、迷惑メールセンターに来たデータに基づいて、国際協力で通報、情報を提供したりとか、そういうのはあるんですけれども、このSMSの話では、すみません、ちょっと持ち合わせているものはないので、マクニカさんとか、もしなければ、すみません。

【大谷主査】　ありがとうございます。

マクニカさんかトビラシステムズさんのほうで、何か補足説明がございましたら。なければ大丈夫ですということです。

【株式会社マクニカ】　現状は、本当に今日お届けした内容が、私たちが今持っている情報という形にはなるのですが、そのほか、もしかしたら警察関連の皆様とかが分かる範囲とかがあればという気持ちも、ちょっとあります。

【大谷主査】　ありがとうございます。関心の高いところだと思いますので、今日、オブザーバーで参加してくださっているサイバー犯罪関係の御担当の方たち、もし情報があ

るようでしたら、今回というよりは次回以降に、何か提供できる範囲で情報を御提供いただいて、この議論のために活用させていただければと存じます。

それから、コメントもありがとうございました。辻構成員から、OSの違いについてということで頂戴しております。

では続きまして、鎮目構成員のほうからも御質問の御要請がありましたので、よろしくお願いします。

【鎮目構成員】　すみません、恐らく時間も押していると思いますので１点だけなのですが、私、iOSを普段使っているので、Androidについてはあまり知らなかったんですけれど、マルウェアをインストールさせる方法があれだけ見え見えで、しかも流行しているマルウェアが限られているということになると、いわゆるセキュリティソフト、アンチウイルスというものがパソコンなどではありますけれど、そういったものがある程度普及していれば、ユーザーレベルでそれなりに対策が取れるのかなという疑問もあるのですが、そもそもそういう対策を取ること自体が困難なのか、あるいは、取れるけれども、あまりセキュリティソフトを入れるということが現状では一般的でなくて普及していないのか、その辺りについて、もし情報をお持ちの方が両社の関係者の方でおられましたら、教えていただければと思います。

【大谷主査】　御質問ありがとうございます。その件はトビラシステムズさんが、まさにアンチウイルスソフトを提供されているので、お話しいただければと思います。お願いします。

【トビラシステムズ株式会社】　具体的な数字なりのデータを持っているわけではないですが、我々も昔から、特殊詐欺にせよ、セキュリティのソフトを皆さんに使っていただきたいと思ってやっておりますけれども、やはり皆さん、自分はだまされないと思っていることが一番の障害かなというふうに思っております。

結構有名な手口とかですと、皆さん知っているから大丈夫と思いがちかなと思っておりまして、ただ、特殊詐欺の一事例ではあるんですけれども、被害者の方にお話を聞いてみると、半分ぐらいは「手口を知っていた」というふうに回答されているんです。

ですから皆さん、知っていると思って自信を持ってしまっていて、でもやはり巧妙な手口によってだまされてしまうといったことがあります。なので過信して、皆さん、大丈夫だと思ってセキュリティソフトを入れないとか、そういった事情があるのかなと私は見ております。

以上です。

【大谷主査】　ありがとうございます。鎮目構成員、大丈夫でしょうか。

【鎮目構成員】　大丈夫です。ありがとうございます。

【大谷主査】　ちょっとその関係で教えていただきたいんですけど、アンチウイルスのシステムの導入率というのは大体どのくらいなのでしょうか。キャリアによって違うのでしょうか。端末の数に比べて何パーセントとかという数値はないものですか。

【トビラシステムズ株式会社】　すみません、私どものほうで、ユーザー様の総数に対してどれぐらいの方が使ってみえるかというのは、データは持っていないです。

【大谷主査】　そうですか。ありがとうございます。私、それに救われたことがあるので、声を大にして入れるべきだと言いたいです。

すみません、次の質問の御要請をいただいています。山根構成員、お願いいたします。

【山根構成員】　大変勉強になる御発表をありがとうございました。まず、マクニカ様に２点御質問がありまして、対策として国内の事例なども御紹介いただいたんですけれども、RCSの導入というか普及を一つ御紹介いただいたと思うんですけれども、これはどういう意味で対策になっているかというと、公式マークを設定することで、信頼できる送信者だということが分かるようになるという意味で対策になっているという理解でよいのか。何かほかの意味合いがあるのであれば御教示いただければと思っております。

また、国内における対策として、どれぐらい効果が上がっているのか。なかなか効果測定、定量的なものは難しいかなと思うんですけども、何かあれば御教示いただければと思っております。

あと、すみませんもう１点。トビラシステムズ様にも１点御質問がございまして、スミッシングのターゲットブランドの割合などを御紹介いただいたかと思うんですけれども、こういったターゲットブランド、なりすまされる側になりやすい企業とか、そういった傾向などがあったりするのか、もし分析の結果として分かっていることがあれば、教えていただければなと思います。

【大谷主査】　御質問ありがとうございました。

まず、それではマクニカ様のほうから御回答をお願いいたします。

【株式会社マクニカ】　送信元認証といいますか、やはり公式マークとして発行されるという意味で、SMSだとやはり電話番号だけで、タイトルもなくて、すごく簡易なメッセージで来るというところに比べると、RCSだと公式マークで認証を分かりやすくして、受

け取る人もどこから来ているのかというのが見やすいという意味で、そこがいいのかなと思っています。

【大谷主査】　あともう１件、取組の効果について御質問があったかと思いますが、定量的なものはなかったとしても。

【株式会社マクニカ】　そうですね。ただ、RCS自体が、そこまでの認知度がまだ、あんまり消費者的にはなかったりとか、それこそ今日お集まりいただいている皆さんは、SMSとRCSってこういう違いがあるよねとかというのも、ある程度もしかしたら御理解があるのかもしれないですが、一般の消費者的に見ると、結構ごちゃっとなっている可能性も非常に高いのかなというところで、そういう状況からすると、なかなか定量的に、そっちを使うから安心なのかなとかというところは、まだ分かりづらい部分はあるのかなと。今後、RCSだから安心で、じゃあSMSをシンプルにやめたらいいのかというと、そういう単純な話でもなくて、RCSはRCSでセキュリティ的な部分でいうと結構未熟だったり、危険な部分とかがあって、複雑な詐欺に使われたりするんじゃないかみたいな懸念とか、画像だったり動画だったりが一緒に送られるので、より焦らせる動機につながるんじゃないかとか、いろんな懸念もあるので、一概にRCSを使うことでSMSをなくして代わりにするみたいなのでいいのかと。それこそSMSはSMSで、すごく携帯の機能としても盛り込まれているので、本当に誰もが買ったタイミングで使えるという、アプリのインストールとかも要らなくてという便利さだったり、届けやすさという意味を持ちつつ、そこをすごく活用しながら使っていくのかというところが、議論の分かれるところなのかなという感じで。あんまり答えになっていなくて本当に申し訳ないです。

【大谷主査】　山根構成員、大丈夫でしょうか。

【山根構成員】　はい、ありがとうございます。

【大谷主査】　では、トビラシステムズさんのほうにも御質問いただいていまして、ターゲットブランドの件なのですが、お願いいたします。

【トビラシステムズ株式会社】　ターゲットになりやすい、成りすまされやすい側の傾向があればということだったかと思いますけれども、やはりユーザーをたくさん抱えているところで、クレジットカード情報ですとか、ID・パスワードを使ってログインする機構とか、そういったものを提供している事業者で、かつユーザーが多いところというのがやはりターゲットになりやすいというのはあるかなと思います。

加えて言うと、恐らく攻撃者側もシステムについてかなり研究しているかと思いますの

で、脆弱性が確認できているとか、ここは弱そうであるとか、そういった傾向を調査した上で狙うというのが、恐らくはオーソドックスかなと思っています。

ただ、やはり長く行動を続けていますと、試してみようとか、そういったところもあるかと思いますので、例えば、２年ほど前でしたでしょうか、銀行を狙うとすればやはりメガバンクさんとか大手を狙うというのがあるかと思うんですけども、中小の地方銀行が軒並み狙われていたというような時代もありましたので、そういったところというのは逆に、フィッシングのターゲットになったときにどう対応すればいいのかというような知見が少なかったりするわけです。ですから、逆にそこが脆弱性となって狙われるというようなこともあるかと思います。

あとは、やっぱり時流に乗ったというか、先ほど少し話に出ていたかなと思うのですが、コロナ禍で巣ごもり需要みたいなのがあれば、例えば自宅で動画をよく見る、ネットフリックスとかそういったものをよく見るとなれば、そこがかたられるとか、そういったこともあるかなとは思います。

以上になります。

【大谷主査】　山根構成員、大丈夫でしょうか、今のお答えで。

【山根構成員】　はい、ありがとうございます。

【大谷主査】　ありがとうございます。

それではもうひと方から。仲上構成員のほうから、マクニカ様への御質問があるそうです。どうぞお願いします。

【仲上構成員】　JSSEC、仲上でございます。本日は大変貴重な発表をありがとうございました。資料のほうも拝見させていただいて、非常に勉強させていただいている次第でございます。

お示しいただきました資料の中で、国際的な海外の取組というところを御紹介いただきまして、こちらも、やはりイギリス、アメリカ、ニュージーランドといったところでも対策、情報共有の取組が進んでいるというお話があったかと思うのですが、キャリア様の取組、特に海外のキャリアの取組というところが非常に気になっておりまして、そういったところでのSMSスミッシングに対する取組はどういったものが、具体的にはどう止めているのかというところでの取組というのはどうなのかなというのを、御存じでしたら教えていただければと思いました。

【大谷主査】　お願いします。

【株式会社マクニカ】　ありがとうございます。海外のキャリアさんですよね。これはなかなか、すみません、さくっとお答えするのが難しいといいますか、我々も情報がまだないところではありまして、一旦、弊社のメンバーで、テレコムに長く携わっているメンバーがおりますので、発言をお許しいただくことは可能でしょうか。

【株式会社マクニカ】　マクニカの塚田です。テレコムのほうをいろいろ見せていただいていますので、知っている範囲で御回答させていただきます。

例として、今、私たちで調べたのがアメリカのケースで、アメリカは通信事業者団体のCTIAというのがあるのですが、その中で幾つかの取組をしています。

取組の１番目が、今日も発表の中にありましたスミッシングの共通の受付窓口です。7726というところ、それは、そのオペレーター団体が運用しております。

あとは、そこの団体の中でプリンシプルガイドラインというのを出しておりまして、これは、メッセージの送信者に守ってほしいということをまとめております。例えば、送るときはちゃんと確認を取ってねとか、そういった本当に基本的な原則を幾つか書いておりまして、この原則自身は法的な規制力はないのですが、ユーザー側からアンケートを取ってみて、その結果、期待されていることをまとめている形になっております。

例えばベライゾンなどは、オペレーターによっては、そのプリンシプルに基づいて、メッセージを送る人に対して、このガイドラインを守ってくださいということを要望して、そこをまたブロックの根拠に使うという、そういう使い方もあります。

まとめといたしましては、アメリカの場合、団体のほうでガイドラインをつくっている、窓口をつくっている。そこに基づいて、各オペレーターは行動を取っているというところが、今調べている中で出てきております。一つの例として御報告させていただきます。

【仲上構成員】　ありがとうございます。大変参考になりました。

【大谷主査】　非常に貴重な情報をありがとうございました。後で結構ですので、少し詳しめの、何か出所というか、どこを見たらいいのかというようなところを教えていただけると大変助かります。よろしくお願いいたします。

【株式会社マクニカ】　分かりました。

【大谷主査】　ありがとうございます。

今のところ、御質問などは一通り終息した感じでして、マクニカ様、それからトビラシステムズ様、どちらも大変有意義なプレゼンテーションをいただきましてありがとうございました。

【株式会社マクニカ】　ありがとうございました。

【大谷主査】　ありがとうございます。では、時間の関係もございますので、このあたりで検討を一旦終了させていただきまして、本日の議論を踏まえた論点の確認などを、ちょっと事務局にお願いしたいと思います。

【小澤利用環境課課長補佐】　先生方、ありがとうございました。

それでは、資料１－５に基づいて、今回いろいろいただいた御質問、御意見などを踏まえて、また座長とも相談して修正をしたいと思いますが、御発表の中にもあったものですとか、これまで緊急プランとかの中でも触れられてきたような事項を、私のほうでたたき台ということでまとめております。

これについて御意見があれば、また別途いただければと思いますが、まず、マルウェア端末の修正、こちらについては今回主眼だったと思いますが、マルウェア感染端末の特定ですとか、利用者への警告・注意喚起、これを進めるべきではないかというような御提案があったと思っております。

これについては質疑の中でも議論がございましたが、通信の秘密の関係の整理が一定必要だと思っておりますので、これは次回また御説明の準備をしたいと思っております。

また、Google、Appleの話もありました。マルウェアをOSレベルでも検討できないかというところについても、幾らか課題が御提起されたと思っております。

また、海外の事例、スミッシングメッセージの情報提供、これは今、メールのほうでは迷惑メールセンターですとか、あとフィッシング協議会さんだったりも取り組まれております。こちらのほうのお話がございました。

マルウェア以外も含む論点であります。下のほうです。不適正利用対策のうち、SMS発信元については、特に共通番号0005番号の話の御紹介がございました。

あと、海外から来るようなものについても、どういうふうに届いてくるのかという御紹介がございました。

あと、私の事務局説明資料のほうにちょっと出てきたんですけども、SMS機能つきのデータSIM、先ほどマクニカさんの資料にもありました、携帯SIMから送られるようなパターンもSMSとして含まれておりますので、こちらの中でSMS機能付きデータ通信専用SIMカードの、特に契約時の本人確認については、携帯電話不正利用防止法の対象外ではありますけれども、事業者のほうで自主的にやっていただいている部分でありますので、この現状の把握ですとか、さらなる推進というようなところを入れさせていただいております。

今日の話題には出ませんでしたけれど、SMS認証代行事業者というような、SMS認証を他人にさせて、自分の番号以外のもので任意のアカウントをつくるといった事案もございます。こういったものへの対処というのも、これは緊急プランですとか、その文脈でよく言われていた話で入れております。

SMS事業者、配信事業者が、そもそもそういうものがいると知らなかったという話もありましたけれども、配信事業者ですとか通信キャリアといったものが、まず業界というか、サービスとしてまだまだ発展途上というところもあって、横の連携というのもまだ十分ではないかなというところもありましたので、情報連携、自主的対策と。

あと、RCS、＋メッセージ等の御紹介もございました。こちらのほうも論点に加えさせていただきます。

私のほうから、ざっくり説明させていただきました。以上です。

【大谷主査】　事務局のほうで幅広に論点を拾っていただきまして、冒頭でたしか事務局で御説明いただいた資料によりますと、次回もSMSスミッシング対策についての回ということで、さらにまた専門家のほうからお話をいただいたりして、論点をさらに深掘りできるのではないかなと思っております。

ただ、今日議論になったところで、角谷さん、それから柘植さんのほうからいろいろ教えていただいた点で、御質問であるとか、あるいは論点にこれも付け加えるべきではないかといった御意見があるようでしたら、少し皆様からお時間をいただきたいと思います。

15時まではお時間をいただいているので……中原構成員からコメントがあるようですが、よろしいでしょうか。お願いします。

【中原構成員】　すみません、先ほど発言しそびれてしまいました。質問ではなくコメントですけれども、このICTサービスの不適正利用というのは、民法とか消費者法的な枠組みで捉えると、消費者が悪質な者との間で自ら消費者契約を結ぶということが問題となっているんじゃなくて、消費者が直接に悪質な者による不正行為の被害者となる、あるいはマルウェア感染等によって知らず知らずのうちに不正行為に加担してしまうという、言ってみれば不法行為的な事案であるということに特徴があると思います。

ただ、不正行為をした者が責任を負うということ自体は当然ですけれども、それだけでは効果が乏しいので、そもそも不正行為による被害が生じるのを未然に防ぐために、詐欺行為者が通信事業者との間で締結する契約関係であるとか、あるいは消費者が通信事業者との間で締結する契約関係等に、公益的な観点から一定のコントロールを及ぼす、このレ

ベルで契約の問題が出てくるということではないかなと思います。

もっとも、これは、民法の観点から取り上げやすいところを取り上げただけであり、１側面に過ぎず、より広い視野から見ていくことも必要であると感じたところであります。

本日の事務局からの御説明、それから２社からのプレゼンテーションを伺って、改めて感じるのは、こういう詐欺行為というのは極めて巧妙でありまして、それを端緒の段階で根絶するということは難しいと。最終的な被害に至るプロセス、今回のスミッシングでいえば、詐欺グループによる当初のSMS等の発信、それが送られてきた携帯電話利用者による閲覧・操作とか、それから不正アプリのインストール等によるマルウェア感染、感染端末利用者による知らず知らずのSMSの発信、それが送られてきた携帯電話利用者による閲覧・操作で、それによる個人情報・クレジットカード情報等の詐取、最終的に当該情報が悪用されるといった各プロセスについて、できることを地道にやっていくほかないという点であります。

事務局から示された論点のたたき台というのも、そうした観点からのものでありまして、そこで示されていることに全く異論はありません。

３点だけ、より具体的に考える必要があるかなという点がありまして、１点は、携帯電話の利用者の端末が、マルウェア感染によって言わば乗っ取られているというような状況をいち早く把握して、当該利用者に対応を求めるという、その対処というのが被害の防止を拡大するという意味で重要だと思います。

現状、各携帯電話事業者等がどういうふうに対応しているのかというのは存じ上げませんけれども、それまでの当該利用者の利用状況から見て、急にSMSの発信件数が伸びているというような不審な状況を把握して、当該利用者に警告するというようなことが、事が通信に関わるだけに難しい面を含むんですけれども、重要であるように思いました。

知らず知らずのうちに大量のSMSを送信した端末の利用者が、高額の利用料を請求されるというトラブルもあるというふうに聞いていますので、こうした対応は、スミッシングの被害者のみならず、乗っ取られたほうの消費者の損害の拡大を防止するという点でも重要であると感じています。

それから、あと２点、非常に手短にですけれども、マクニカ様から御紹介があった、海外のスミッシング共通窓口のような情報収集の仕組みは、もろもろの対策の前提であって、まさにトビラシステムズ様が民間レベルで実践しているのだと思いましたけれども、海外の事例を見ると、より公的なレベルで、公的な機関も関わって対応しているように見える

わけでして、具体的にどんなものかは分かりませんけれども、日本でも情報収集の仕組みがより体系的に構築されるべきなのではないかということは、議論に値するように思います。

それからあともう１点、フルボットについてのニュージーランド政府の対応の例というのは、個別の感染者への対応・連絡というレベルで参考になるだけではなくて、大規模事象への対応というレベルでも、恐らく教訓が多く含まれているのではないかというふうに想像されるところであります。こういった事柄は初動対応が非常に重要でありまして、日本で同様の事象が起きた場合に、どういう体制でどういう対応が取られるのか、それが迅速かつ実効的なものなのかというのは、検証の必要があるように思いました。

長くなりましたが、以上です。

【大谷主査】　整理されたコメント、ありがとうございました。

星構成員からもお手が挙がっておりますので、よろしくお願いいたします。

【星構成員】　すみません、お時間のないところ申し訳ございません。

１点だけ、今、中原先生からもお話がありましたフルボットの対応、これはやっぱり、この問題を考える上で非常に重要なところがあるかなということで、日本と同様の現象ということでもありますし、あと国際協調ということも求められていく観点かなと思います。

資料１－５でお示しいただいたたたき台のどこかに織り込まれているということであればそれでいいのですけれども、もしそうでないということであれば、こういったところも視野に入れていただくのも一つの選択かなと思った次第です。

以上でございます。ありがとうございました。

【大谷主査】　ありがとうございます。大事な論点だと思いますので、論点の中に加えていただければと思います。

併せて、過去にNICTなどで、IoT関係で、ノーティスとかnicter警告、マルウェアに感染しているIoT機器について警告をしたりという取組があったと思いますので、その辺りの参考となるような情報を整理して、事務局のほうで御提供いただければ、多少参考になり得るかなとも思っております。

それでは、時間が参りましたので、今日も多岐にわたる論点について活発な御議論をいただきまして、貴重な御意見を多数いただきましてありがとうございました。

以上をもちまして、不適正利用対策に関するワーキンググループの第１回会合を終了させていただきます。本日は皆様、お忙しいところどうもありがとうございました。