不適正利用対策に関するワーキンググループ（第12回）

令和７年11月21日

【田中利用環境課課長補佐】　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。定刻となりましたので、不適正利用対策に関するワーキンググループ第12回会合を開催いたします。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田中でございます。

事務局からのウェブ会議による開催上の注意事項については、投影している通りでございます。

また、本日の資料は本体資料として議事次第と資料12－１から12－６を用意しております。

本日は中原構成員が欠席と御連絡いただいております。

注意事項は以上になります。

では、早速ですけれども議事に入りたいと思います。これ以降の議事進行は大谷先生にお願いします。大谷主査、よろしくお願いいたします。

【大谷主査】　大谷でございます。それでは、早速議事に入りたいと思います。本日は、まず上限契約台数について事務局から御説明をいただきまして、皆様との意見交換の時間を取らせていただきたいと思います。そして、その後ですけれども、フィッシングメールの対策につきまして、日本プルーフポイント、チーフエバンジェリスト増田様から御発表、そしてそれに続きまして質疑応答の時間を取りたいと思います。そして、次にNTTドコモ様、KDDI様、ソフトバンク様、楽天モバイル様の御順に発表と質疑応答の時間を取らせていただきたいと思います。

それでは事務局、よろしくお願いいたします。

【田中利用環境課課長補佐】　ありがとうございます。第12回の事務局説明を始めたいと思います。検討のスケジュールでございますけれども、前回の11月４日、上限契約台数に関する事業者団体ヒアリングを実施いたしまして、本日はそれを受けました論点整理をする予定でございます。また、２つ目の議題としまして、フィッシングメール対策について事業者ヒアリングを予定しております。今年の不適正ワーキンググループはこちらで終了とさせていただき、利用環境研究会に12月４日に報告をする見込みでございます。

早速内容ですけれども、上限契約台数のヒアリングについてサマライズしたものでございます。まず上半分ですけれども、事業者からの御発表内容について御紹介いたします。TCAの御発表の中で、業界ルールに関しまして現状存在しておりまして、MNO４社の中では申し合わせをしており、５台を超える利用の要望があった場合については例外的な運用も実施しているということでした。２ポツ目に移りまして、TCAからですけれども、一方でデータSIMに関してはMNO４社各社で定める契約台数制限がある中で、今業界ルールについての在り方については検討を行っている状況だと聞いております。３ポツ目に移りまして、MVNO委員会でございますけれども、こちらは業界ルールはなく、家族構成の都合で６回線以上希望する方については５台以上の台数設定をする事業者もあると聞いているところでございます。

事業者の御発表に対して、構成員から御質問を３点いただきました。下半分でございますけれども、１ポツ目、質問事項１ですけれども、上限回線数を５契約としている事業者が、それ以上の契約をしたいという申出があったとき柔軟な対応をしているかどうか。また、複数回線を契約する場合、契約者以外が使用する回線に対して本人確認を実施しているかどうかという点です。２点目については、２ポツ目ですけれども、上限台数の設定をするに当たって、システム上の技術的な制約があるのかどうかという点です。３点目につきましては、音声SIMとデータSIMで上限回線数の設定に差があるのはどのような理由かということです。こちらについては後ほど、事務局説明の後にMVNO委員会から補足をいただく予定です。

以上の発表を踏まえまして、構成員から御意見をいただいたものを簡単にサマライズしたものが次、２ページになります。業界ルールその他に関して御意見をいただいておりまして、１ポツ目、原則として５台の上限を設けつつ例外的な契約を認めるという運用をしている業界ルールは、バランスのとれた対応になっているのではないか。他方で業界の自主基準が浸透しきっていない部分もあるので、そこを後押ししていく必要があるというような御意見を山根構成員からいただいております。

２ポツ目につきましては、５という数字の妥当性が明確に示せないのであれば、よく検討してはどうか。また、SMSあるかなしかで分けるのは妥当であり、SMSなしデータSIMについて法人で使う場合については制限台数を設けないほうがよいのではないかという御意見を、辻構成員からいただいております。また、３ポツ目につきまして、SMSつきSIMについては特殊詐欺に使われるリスクがある一方で、SMSなしデータSIMについてはそういった

リスクは指摘されていないので、SMSなしデータSIMのルール化は慎重なほうがよいのではないかという御意見を、鎮目構成員からいただいております。

次のページに移りまして、役務提供拒否について事務局から御提案をした事項について、御意見をいただいたものになります。１ポツ目については、多数台契約について、事情があれば締結を拒むことができると定める手法については考えられる。一方で、危険性が認められない多数台契約もあるので、その規定の仕方については要検討すべきではないかという御意見を中原構成員からいただいております。２ポツ目につきまして、役務提供拒否との関係を明確化するということは一つあり得るアプローチであると、山根構成員から御意見をいただいております。３ポツ目につきましては、正当な理由があるのであれば原則以上の台数に認めるという形にしつつ、実際代理店で判断できないものについては本社で対応するという形が望ましいのではないかという御意見を、星構成からいただいております。

下半分に移りまして、運用上の対応、その他の方策です。１ポツ目ですけれども、多数回線の契約ハードルを少し上げる手段として、利用者にやってほしくないことを規約に明記して注意喚起することや、誓約書へのサインも選択肢ではないかという御意見を沢田構成員からいただいております。また２ポツ目、契約者の本人確認のみを行い、その方の名義で複数台契約をした場合、上限が場合によって適用されていない領域があるとすると、そこに潜む危険に対して十分に対応ができていなかったのではないかという懸念があるので、実態を踏まえて検討していく必要があるという御意見を大谷先生からいただいております。

以上の御意見を踏まえまして事務局側で提示させていただく考え方としては、こちらのスライドに投影しているものでございます。まず１パラから御説明いたします。上限契約台数の制限についての業界ルールの評価がございますけれども、進展が一定程度図られたことが認められると考えております。ただ、今後多くの事業者へのさらなる浸透が必要になってくると思うことから、そこを図るとともに、利用者視点から一定の予見可能性の確保が望ましいことなども考えると、制度面から事業者の自主的な取組を後押しする環境を整備する必要があるのではないかというような形で御提案させていただきました。

事業者の自主的な取組を後押しする具体的な内容としましてはその次のパラグラフにありまして、例えば一定台数を超える契約を利用者が求めた場合に、利用目的やSIMの種別を踏まえ事業者として提供拒否ができることについて、法令上の措置を含め、明確化の観

点からルール化することなど、所要の環境整備を迅速に進めていくことが適当ではないかとさせていただいております。

次の矢印に移りまして、総務省において上記ルール化を通じた事業者のさらなる自主的な取組を促進していくということも重要ですので、そちらを書かせていただいたのと、事業者においても一層の取組が必要だと思いますとあったので、不正契約を防止するための契約時の対応強化に一層取り組むべきではないかという形で記載しております。その後、また取組状況を受けて必要になる場合には、犯罪との因果関係を踏まえながら、名義人が契約したSIMの実際の使用者を把握する方法を含めた検討や、一層のルール化を含めた対策の強化についても検討するべきではないかというような形でまとめさせていただいております。以上が上限契約台数に関する論点提示ということでございます。

続きまして、資料の後半の、フィッシングメール対策の関係の背景について御説明させていただければと思います。こちらについては、今年に入りまして証券会社を語るフィッシングメールが急増していることを受けまして、被害もかなり出ているということを踏まえて、総務省から４通信事業者団体に対して９月１日に要請を行ったところでございます。

９月１日の要請の内容ですけれども、下枠にございますとおりで大きく３つございます。１つがフィルタリングの精度の一層の向上を積極的に図ること。２つ目につきましては、なりすましメール対策として有効な送信ドメイン認証技術、DMARCの導入、またその適切な設定、またその先にありますドメインレピュテーション、BIMI、踏み台送信対策などの対策を積極的に検討していくこと。また３つ目としまして、メールサービス事業者が提供している各種のメール対策サービスについて、利用者層に向けた一層の周知・啓発を行うこととしてございます。今回、MNO４事業者にお集まりいただきまして、各社が行っているフィッシングメール対策について御発表いただく予定でございます。こちらの事業者の取組を踏まえて、目指すべき方向性について御議論いただければと思っているところでございます。

以上で事務局からの説明となります。

【大谷主査】　御説明、ありがとうございました。

それでは続きまして、テレコムサービス協会のMVNO委員会様から、前回のワーキンググループで上限契約台数を超える契約についての詳細の御質問をいただいておりまして、御回答を用意していただきましたので、御説明いただければと思います。MVNO委員会様、よろしいでしょうか。

【MVNO委員会（井原）】　よろしくお願いします。MVNO委員会、井原です。前回のWGで御質問いただいておりまして、その場で回答できずに申し訳ございません。MVNO各社にヒアリングをさせていただいた結果を報告させていただきます。また、資料の画面共有ではなく口頭になりますことを御了承いただければと思います。

まず、音声で上限６回線以上を提供している２社からの回答でございます。御質問内容は音声SIMで６回線以上の上限設定に関して、利用者情報、利用者の確認や利用者の本人確認の実施有無等についてでございます。両社とも利用者登録は行っているんですけれども、利用者の本人確認は必須での確認ができていないという状況です。また、契約者や利用者以外が利用することを防ぐ方法についてでございます。契約時に無断の譲渡の禁止などについての注意喚起を行うことで抑止には努めているんですけれども、現状実質的に防ぐことは難しいという状況になってございます。

続きまして、上限回線数を超える回線契約要望への各社の対応及び制約があるかどうかということについてです。こちらは15社から回答を頂戴しました。15社中11社は、個別対応は不可となっております。理由はシステムや卸元仕様が制約となっているためとのことでございます。また、対応可能な４社は、利用用途を確認するなどで個別対応が可能となっているんですけれども、実績はほぼないということでございました。

最後に音声とデータで契約上限回線数が異なる理由についてです。まず、音声よりもデータSIMのほうが上限契約回線数が多いという傾向でした。回答いただいた事業者のコメントをまとめますと、データSIMは幅広い利用実態や想定される利用シーン、例えばスマートフォンだけではなくてタブレットとかIoT機器などなんですけれども、このような状況を踏まえましてデータの上限契約回線数を音声SIMよりも多く設定している傾向となっておりました。

以上でございます。

【大谷主査】　改めて詳細を御確認いただきまして、ありがとうございました。

それでは、次は自由討議に移らせていただきたいと思います。事務局から御説明いただいた資料で言いますと５ページまでの上限契約台数について、ここで議論をしたいと思います。本日御欠席となっている中原構成員から事前に御意見を頂戴しておりますので、私のほうで代読をさせていただければと思います。それでは、今から読み上げます。

前回、多数台契約の規制の在り方について、携帯電話不正利用防止法11条のリストに単純に加えるのは落ち着きが悪いかもしれないこと、法律ではなく解釈指針による規制も考

えられることを申し上げました。もっとも、前者については携帯電話不正利用防止法11条は「役務の提供を拒むことができる」場合を列挙する規定であり、必ずしも同法が正面から禁止する行為でなくても正当な理由なき役務提供の拒否を禁じる、電気通信事業法法121条の趣旨に反するとまでは言えないものと思います。むしろ、ある程度定量的な指標をもって判定し得る不正行為については、携帯電話不正利用防止法11条に挙げていくことにより、今後様々生じ得る事態に対処する基礎をつくることにも十分な意義があるものと思います。

また、後者については法律上の規制事項とした上で、省令等により具体的に定めるという手法も十分に考えられるところであり、電気通信事業法121条等の解釈指針として示すよりも、文脈適合的で安定的な規律が望めるというメリットがあろうかと思います。したがいまして、私としては前回申し上げた事柄に固執するわけではなく、法令上の措置を含めたルール化を進めていくことに異存はございません。もっとも、省令等による具体的な規制に当たっては、これまでも指摘されてきたとおり、悪用の実態に即して事業者、利用者の双方にとって無理のない形で規制の具体的な対応や対象を考えていくべきであると思います、との御意見を頂戴しております。

それでは委員の皆様、質問やコメントをお寄せいただければと思います。お手数ですが、チャット欄に書き込みをお願いいたします。

それでは、沢田構成員からお手が挙がっております。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。考え方をお示しいただいて、ありがとうございます。利用形態は様々なケースがあり得ると思いますので、上限台数を一律に決めるのではなくて、あくまで利用目的とかSIMの種別などの個別事情に応じて、事業者さんが提供の可否を判断できるようにルールを明確化するという、そういう形で後押しすると理解しました。なので、この記載に賛成したいと思います。

今のは２段落目の話ですが、もう１点、３段落目の話として、契約時の対応の強化にも触れていただきまして、こちらも感謝申し上げたいと思います。利用者が安易に犯罪に手を貸さないようにするという意味で、まだもう少し御協力いただけることがあるのではないのかと思っておりましたので、この記述にも賛成したいと思います。以上です。ありがとうございます。

【大谷主査】　賛同意見として承ります。

それでは、辻構成員、よろしくお願いいたします。

【辻構成員】　まず、５ページにつきまして、業界のルールが進展しているということであれば、法律で云々よりも機動性が保てるという観点においても、業界ルールで進めていただく形がよいようにも思います。

あと私、利用台数に関して前回も５台がということを言い、数はともかくとして利用台数の考え方、増やすのはいいんですけれどもそれぞれの利用がどういう状態、実態がどうなのかの確認をしたほうがいいのではないかという意見が前回も結構出ておりましたが、それもそのとおりかと思いまして、２台、３台、４台と契約していく中で、それは誰が使うんですかであったり、案として例えば誓約書を取るであるとか、もしくはその利用者の本人確認を取るとか、いろいろ方法は考えられると思うんですけれども、数は緩和するけれども確認は強化するということは、やはり必要なのではないかと私も思っております。以上です。

【大谷主査】　辻構成員からも御賛同の意見をいただいております。

他の方はいかがでいらっしゃいますか。私のほうで見えているチャット欄につきましてはさらなる御意見の申出、質疑、質問等はなさそうでございますが、大丈夫でしょうか。

それでは、山根構成員、よろしくお願いいたします。

【山根構成員】　ありがとうございます。私も基本的にはここで示していただいた考え方の案に賛成するところです。その上で今後のルール化を含めて検討していくに当たっての視点という意味でコメントさせていただこうかと思っておりまして、一定台数を超える契約のところで、もし一定の台数の具体的な基準を示すということになってくると、現状の業界ルールの５台というのが一つの基準になる数字になってくるのかとは思います。他方で前回の会合でも辻構成員から、５台という数字の明確な根拠を示せないのであれば10台でもいいのではないかというような御意見もありまして、この辺りをどういう数字にしていくかというところは今後、具体的に検討していくということかと思います。

現状の業界ルールよりも一定台数の基準の数を増やすということになったときに、基準の数よりも台数の上限を低めに設定する事業者も見込まれるのではないかと思っております。そういうことがあったときに、電気通信事業法121条１項の役務提供義務との関係で、基準の台数より低めの上限台数を設定することが直ちに問題になるものではないだろうと私は思っておりますけれども、そことの関係についても併せて整理していく必要があるのではないか、要するに一定の台数を示すということでそれ以下の上限台数を設定すること

ができないというような、逆向きのメッセージになってしまわないように、そこの打ち出し方は少し気をつける必要があるのかとは思った次第でございます。

あとは２つ目の矢印の部分で言いますと、複数台契約のときの利用者の本人確認まで、先ほどのMVNO委員会の御質問への回答の中でも、必ずしも本人確認まで実施していないというような状況があるというところで、それが実際に不正利用にどれぐらい寄与してしまっているのかといったところは、今後、状況をよく見つつ対策を検討していく必要があると思った次第です。以上です。

【大谷主査】　山根構成員からも丁寧なコメント、ありがとうございました。重要なポイントかと思います。どのような環境整備で後押しをするのか、法令上どこまで細かく基準を定めるのか、あとは正当な理由によって上限台数を超える場合の基準の明確化などをどのように図っていくのか、幾つも具体的な定め方については課題があると思いますけれども、今の意見を参考にさせていただくことが重要かと思います。

他の方、送信先は全員宛に設定して、御意見をお寄せいただければと思います。

今回、沢田構成員からも御指摘がありましたように、利用目的やSIMの種別を踏まえるといったところ、そこでもより明確化するポイントというのが示されているかと思いますし、また２つ目の矢印のところですけれども、運用上の工夫であるとか努力というのを一層事業者に求めていきたいということについては、恐らく皆様の賛同を得られているところではないかと思います。

それでは、また後で戻る可能性もあるということで、一旦は先に進めさせていただければと思います。

それでは、続きまして日本プルーフポイント、チーフエバンジェリスト増田様から、フィッシングメール対策についての御説明をお願いいたします。

【日本プルーフポイント（増田）】　皆さん、こんにちは。プルーフポイントというサイバーセキュリティの会社でエバンジェリストをさせていただいております、増える田んぼで増田と書きますが、これで「そうた」というふうに申します。警察大学校ではサイバーセキュリティの授業を持たせていただいております。私から見えている世界のメール脅威についてお伝えさせていただきたいと思います。

サイバー攻撃というのは地政学上の影響を多分に受けるものでございまして、例えば2022年、ロシアのウクライナ侵攻を期にぐんと攻撃量が上がっているというのがお分かりいただけるかと思います。以前はどうだったかというと多くてもこの程度、これが最近どう

なったのかというのを見ていただくと、このような形で一気に攻撃量がスパイクしているといったのがお分かりいただけると思います。弊社、プルーフポイントは世界のメールトラフィックのうち４分の１を見ている世界で最大のメールセキュリティ企業ですけれども、我々が見た全世界の新種のメール脅威がこのように昨年の12月から爆増しているといった形になります。

この爆増している脅威がどこに向かっていているかといったところなんですが、これが、実はほとんどが日本でございます。昨月10月の統計で言いますと80.7％が日本に向けた攻撃ということを確認しておりまして、主にCoGUIというフィッシングキットが使われております。このフィッシングキットなんですけれども、確実に日本の被害者だけをターゲットにするといった機能が盛り込まれておりまして、被害者の方が開いた携帯あるいは端末、パソコンのIPアドレス、これが日本であるかどうかを確認する。ブラウザの言語設定ですとかOSのプラットフォーム、こういったものが日本人であるかどうか、日本人がよく使うものであるかどうかというものを必ず確認する。

あるいは、リサーチャーとかはモニターをたくさん使っていたりするので、モニターが１個だけであるかとか、こういったものを確認して通常の一般の日本人であるなとなると、これが詐欺サイトに誘導していくと。そうでなければリダイレクトして正規のサイトに送り込むといった形になりますので、３月ぐらいまでのところ、なかなか他社さんのベンダーでは検知できなかったような攻撃になっています。どれぐらい日本が今まで狙われてきたかといいますと、2023年で言うと4.3％、昨年2024年は12月から攻撃が上がっておりますので21％、で今年、先月10月までの統計で言うと83.3％が、全世界の攻撃のうち日本への攻撃となっております。

どういったタイプの攻撃なのかですけれども、先ほどこちら色分けをしておりますが、一番下の肌色の部分が企業向けの認証情報を窃取するタイプのフィッシングメールです。ですので、Microsoft365のアカウントを狙うものがほとんどとなっております。こちらの濃いピンクのところが個人向けのサービスの認証情報窃取のフィッシングになりますので、証券会社、銀行、Amazon、PayPay、そういったようなコンシューマー向けのサービスの認証情報を狙うタイプのものです。こちらの中間のピンク色というのは、個人向けともエンタープライズ向けとも区分けがつかないようなものを狙ったようなものになっております。皆さん、今お使いの端末はほとんどWindows11になってきていると思います。かつてWindows７だった頃はメールにも添付ファイルとかがついていて、添付ファイルをクリックする

とコンピューターウイルスがダウンロードされて、それで感染をしていく、感染していくときにはOSの脆弱性を使って感染をしていくと、こういった形になるんですけれども、どうしても今Windows11になってくるとOSの脆弱性のパッチがかなり当たっている状態で、どんどんOSがアップグレードされていく。こういったところでシステムの脆弱性を突くのが難しいので、こういった形のフィッシングメール、認証情報を取るタイプのクレデンシャルフィッシングというものが増えております。今、攻撃者もデータが欲しいと思えば皆さんお使いのクラウドにデータがあるといった形になりますので、クラウドのデータを狙うために攻撃者もIDとパスワードを狙ってきているといった状況となります。

この攻撃がどこから来ているかといったところですけれども、先ほどの日本を狙っているCoGUIのフィッシングキットですが、これの攻撃だけを抽出しております。１月の頭から４月の末まで日付ベースで並べておりますが、ちょっと攻撃が減っているところがあります。これが春節の期間。こういったところから分かるのは、攻撃者が春節をお休みになる文化をお持ちである。あるいはフィッシングサイトの設定に楽天証券の「楽」と「証」の漢字のフォントが違ったりしますので、こういった中国語をお使いになる攻撃者である可能性がある。あるいは中国の攻撃と見せかけたい者、そういった可能性があるのではないかと私のほうでは考えております。

実は中国のアンダーグラウンドが今本当に日本向けのフィッシングの攻撃情報で溢れておりまして、例えばこちら、こういったような投稿があるんですけれども、内容を日本語に訳しますと、AIによる代筆で一字一句全部違ったフィッシングのおとりのメールをつくれると宣伝をしていたりします。日本を狙った中国のフィッシングビジネスが最近非常に盛んになってきております。

こういった半面があるので、中国産のフィッシングキットでビジネスが一気に拡大しています。ソーシャルエンジニアリングの中にはこういった警察を語ったようなものもあったり、あとはウェブ担当者に対して著作権侵害しているみたいな、こういったようなメールを送りつけるもので、中身にはzipファイルに格納されたコンピューターウイルス、マルウェアがあったりとか、あと企業向けにも日本語のリスクの高いメールというのがいろいろと着弾していて、最終的にはMicrosoft365のアカウントを狙ってくると、こういったような攻撃が非常に多く観測されております。

今日本が狙われている理由ですけれども、一つ挙げられるのは生成AIの影響によって非常にだましやすいきれいな日本語のナチュラルなメールがつくれるようなった。今までは

どうしても日本語が変なものが多いといったところで、非常に人の感覚で気づけるところが多かったものが人の感覚で気づけなくなったといったところ。今までどうしても言語の壁に守りを頼っていた部分、各国、他の国に比べて詐欺メール対策、特にDMARCとかその辺りが弱いといったところで丸裸の日本を狙う。企業の知的財産は価値が高く、個人の情報もアンダーグラウンドで高値で売れると、こういったような状況になっています。

あとは不気味なDDoS、犯行声明がないようなDDoSと同じようなタイミングで来ていたりしますので、DDoSが目くらましであって実際にはメールアカウントの乗っ取り、それによる企業の中への侵入、こういったところを企てているのかと思われるようなふしもございます。今までメールというのはただのやり取りのツールで、メールのアカウントが乗っ取られればメールのやり取りが盗られると思われがちですけれども、企業においてはシングル・サイン・オンでつながるIDとなっております。メールアカウントが乗っ取られれば、その方がアクセスできるシステム全てにアクセスできると、こういったようなことを考えなくてはいけないと、そういうふうに考えております。

メール詐欺にいかに対応するかといったことを簡単にお伝えしますと、大きく分けてメール詐欺は２パターンございます。一つが、勝手にその人になりすましているものです。もう一つはもう乗っ取ってなり代わるといったタイプのものになります。なりすますものにはドメインのなりすまし、そして表示名の詐称、あとは類似ドメインを使ってくる、こういったものがあります。一方で乗っ取りに関してはパスワードスプレー攻撃とかフィッシングメールとか、マルウェア、コンピューターウイルスを使うもの、こういったものがあるわけなんですけれども、これをよくこちらのなりすましのほうから見ていきますと、なりすましメールの手口、表示名の詐欺、山田太郎さんだけれどもメールアドレスが全然違うとか、これは教育トレーニングしましょうねとよく言うやつです。

あとは類似ドメインを使うもの。「Yamadashoji」の「o」がゼロになっていたりするもの、これは企業側でドメインのテイクダウンが必要になります。あとはドメインのなりすまし、スプーフィング、いつもやり取りしている正規のメールアドレスを攻撃者が勝手に使ってしまっているもの、これに関してはDMARCのRejectでブロックすることが可能になります。Rejectを行った後にBIMIまで使っていただくとこの全てに対して気づきを与えることができると、こういった形になりますので、この詐欺メール対策、ドメインスプーフィングに関してはDMARCで、そしてこのBIMI、DMARCをRejectにした後にロゴを入れるBIMIまで入れていただくと、しっかりと全てのなりすましに対して対応することができると。

結局はこのなり代わる、乗っ取るというものもなりすましのメールから始まりますので、なりすましメールを効果的に抑制することによって乗っ取りも防いでいくと、こういった形になります。そのため、総務省さんが出された９月のフィッシングメール対策の強化で、フィルタリングの強化、DMARCの隔離・拒否のポリシー、あとドメインレピュテーション、BIMIとかの対応、あとユーザーさんの教育、この辺りは非常に的を射ている政策ではないかと考えております。

このDMARCですけれども、なかなか導入が進んでおりません。私も政府に対してロビー活動を３年半かけて行いまして、政府統一基準の中にようやく入れていただきましたけれども、まだまだ日経225でも隔離・拒否まで行っているのがたったの20％にしかすぎません。ぜひこういったところをしっかりやっていただいてBIMIのロゴまで行ければ、全てのなりすましメールを気づきやすいような、こういったようなサジェスチョンをユーザー様に与えていただくことができると思っております。

御清聴いただきまして、ありがとうございます。

【大谷主査】　増田様、御説明ありがとうございました。

ただいまの説明につきまして、皆様から御質問などを受けつけたいと思います。またチャット欄を御利用ください。

それでは、沢田構成員、よろしくお願いします。

【沢田構成員】　ありがとうございます。御説明ありがとうございました。大変分かりやすく、恐ろしいお話だったと思います。１点感想と、１点質問をさせてください。感想は12ページの辺り、日本がそんなに狙われているというのは衝撃というか、恐ろしいなと思いまして、迷惑メール以外でもSNSにも入り込んできて認知戦を繰り広げているという話もありますし、様々な攻撃を仕掛けてきて、日本がどの程度防衛できているかテストしているのかなと、今のお話を伺って思いました。

きっと弱点も既に把握されているんだろうから、次来るのは何だろう、怖いなというふうな感想なんですけれども、それはもうどうしていいか分からないので判断停止をすることにしまして、もうちょっと身近なところで質問させていただきますと、18ページで御紹介いただいたBIMI、これは利用者にも分かりやすくて本当にいい方法だと思う一方で、残念ながら私の環境ではお目にかかれなくて、OSが古いとかバージョンの問題とかメールクライアントの問題とかいろいろあると思うのですが、夫の環境ではちゃんと見えるんですけれども、ただ彼は意味を知らなかったというのもあって、利用者に意味が分からなけれ

ば効果は薄いと思いますし、ロゴがついていないメールは開けないほうがいいよとまで言えるようになるにはまだかなり時間がかかるのかと思いまして、その辺りを利用者サイドに対してはどんな啓発をしていけばよいか、お考えがあれば、というか既にされていたらどんなことをされているのかを教えていただければと思いました。

【日本プルーフポイント（増田）】　これはメールプロバイダー依存になってくるので、例えばすごく残念なのはMicrosoftのOutlookで対応できていないというのがすごく痛いです。ただし、Microsoftさんは今意見招請を始めていますので、意見招請を始めたということはBIMIの搭載も考えていらっしゃるのかなといった、そういった兆しが見えます。ただ、携帯キャリアさん、ここにいらっしゃるところほとんどで言うと結構メーラーはもう搭載されているのではないかと思いますので、もうそういったところを搭載されているところであれば、ロゴがあるものに関してはそこから来ている正規のものですよということをお伝えしてもいいのではないかと。通常いつも受け取っているメールがロゴつきなのに今日はついてないとなると、それは怪しいメールだと簡単には判断できますよというのはお伝えできるのではないかと思います。

【沢田構成員】　分かりました。既にかなり浸透している分野で、分野というか領域もあるということですね。

【日本プルーフポイント（増田）】　そうですね。結局ドメインを持っているほうの対応と、先ほどお見せした導入率というのはドメイン保持者のほうの対応ですけれども、もう既にメールサービスを提供しているほうは、ほとんどが日本のコンシューマー向けサービスだともうBIMIの表示までできているのではないかというような印象を受けますので、あとは企業様の対応が徐々に上がってくるのを待つといったフェーズかと思います。

【沢田構成員】　分かりました。ありがとうございます。

【大谷主査】　ありがとうございました。ほかに御質問などございますでしょうか。

それでは、星構成員、お願いいたします。

【星構成員】　東京都立大学の星と申します。大変に勉強になるといいますか、本当に恐ろしいお話をいただいたなと実感しております。貴重な勉強をさせていただきまして、ありがとうございました。

私からは、聞き漏らしてしまったかもしれないんですけれども、２点ばかり御質問させていただければと思います。まず一つ、DMARCがこれだけのそれなりに守るための仕組みがありながらいまいち普及が進んでいないみたいなお話しをいただきましたけれども、そ

の辺りの原因といいますか、それは単に認知度の問題、あるいは危機意識がそこまで広がっていないから行かないのか、あるいはDMARCについて金銭的、あるいは手間といいますかね、そういったようなところも含めたコストがかかるということなのか、あるいはDMARCを入れたからといって全部が恐らく防げるわけではないと思うんですけれども、精度に対してコストパフォーマンスが得られていないというような認識が広がってしまっているのか、その辺りの率直なところをもし差支えのない範囲でお話しをいただければというのが１点。

あともう１点、守り一辺倒でやっていかざるを得ない今フェーズなのかなと言いつつ、先ほど春節の時期には攻撃が弱いとか、本当かどうか分かりませんけれども簡体字が入っているとか、もう既に攻撃元は分かっているわけで、守りから攻めのゲームチェンジみたいなことができないのか。技術的に可能かどうかというものと、あと差し支えなければ法制上、日本ではこういうことがあるからできないんだみたいなところ、もし率直なところのお話を聞かせていただければと思います。要するにどの辺りが隘路になっているのかというところを教えていただければということで、長々と恐縮ですけれどもよろしくお願いいたします。

【日本プルーフポイント（増田）】　まず、星様の１つ目の御質問のDMARCがなかなか日本において普及しない原因なんですけれども、DMARCというのは対応がメールを受信する側とドメインで送信する側というので２つ対応させます。受信側に関してはもう15分ですぐ設定ができるので、四の五の言わずにすぐオンにしてくださいという、それだけの話です。問題は送信のドメインのほうです。自分が持っているドメインで送信するメールに対して、Noneという一番最初に簡単にやることはもう15分でできる話なので、そこはもう15分でやってくださいという話です。

NoneからQuarantine、Reject、隔離・拒否というところの課題としては、そのドメインが使っている全ての正規の送信元のセンダー、送信元のサーバーというのを全て把握していかなければいけないです。把握した上でSPFかDKIMでそのサーバーにSPFかDKIMを入れていくこと、あともう一つはSPFで認証したドメイン、あるいはDKIMのDタグのドメインと、こちらにある差出人のヘッダー、fromという、ここのところを一致させなければいけないです。

これを一致させるに当たって何が問題になってくるかというと、まずITセキュリティ側で全ての自分のところのドメインを使って出すセンダーのシステムを把握していないとい

うことがあったりします。例えばマーケティング部門でMarketoを使っているとか、営業部門でSalesforceを使っていて、そこからもう自分のドメインとしてメールが出てしまうと。こういったところがあると、業務側の担当者によって、例えばSalesforceとかだと最初のSPFのデフォルトが違ったりするので、そこをちょっとずつ変えていかなければいけない。アライメントをとるというんですけれども、こういった全ての自分のところが認めているセンダーに対して、このSPF、DKIMを入れていく。このアライメント、ここの見てくれの差出人のところのドメインと一致をさせるという作業を全てにやっていかなければいけないです。

日本の企業だと、製造業さんだと大体200とか300ぐらいのセンダーが半年ぐらいで見つかります。そのほとんどが、半分以上が大体攻撃者が勝手に使ってしまっているやつです。なので、実際に正規で使っているのが100ぐらいになってくるので、それを１個１個見てSPF入れる、DKIM入れる、それを対処していく、１個１個レコードを変えるごとに毎回DNSの再起動が必要になってくるといったことになるので、なかなか日本の企業はDNSを触るのも嫌だったりするし、結局業務側がなんかいろいろ使っているサービスなので、業務側のほうがパワーが強くてなかなか言うことを聞いてくれない。業務側のパワーが強すぎるがゆえにセキュリティが普及できないというのが日本の大きな課題なんですけれども、そういった面があってなかなかRejectというところに一気にいけない。

Rejectに行くためには可視化して、例えばSalesforceであればこういうくせがあるからこっちでやろうとか、MarketoだとこういうくせがあるからこっちのDKIMで対応しようとか、そういったような知見を伴いながらやると、大体うちのお客さんだと平均で240日でNoneからRejectに行けたりします。なので、そういったツールとか知見を使っていただくと、そうすると１年以内にRejectには行ける感じになってきます。

あと２つ目の、守り一辺倒で、どういうふうに守りから攻めに転じるかといったところですけれども、例えば今回、能動的サイバー防御法というのが可決成立しましたけれども、この中で一番痛いのがそもそも警察、自衛隊というのが攻撃者のサーバーに対してテイクダウンしに行くという権限を与えられたわけですけれども、脅威インテリジェンスという攻撃者の情報を集める機関がないです。自衛隊にしても警察にしても、今私たち一般人と同じように、インターネットを見ているのと同じルールで戦わなければいけないという、非常にビハインドの条件で戦わざるを得ないと、ほとんど情報が取れないんです。

そういった中で海外はというと、アメリカはサイバーコマンドがいてNSAが支援してい

ると、イギリスだってサイバー部隊がいてそこに対して情報をバンバン入れる部隊が山ほどいると、オーストラリアに当たってはシギント、情報を見ている、分析するところの部隊の中にこのテイクダウンしに行く部隊がいると、こういったような状態になるので、日本はこの青色のテイクダウンしに行くところだけが今定義されていて、それを支えるインテリジェンス部門がない状態で今走り始めました。ここが、ゲームチェンジになるためにはこの緑色の部門がいなければいけない。こういったところで高市さんが国家情報局を設置しますよとおっしゃったのがすごく今後、他国と同じように足並みをそろえるための第一歩、第二歩目になるのかなというふうに、私の中では思っています。

【星構成員】　ありがとうございます。最後、大分大きな話になってしまったんですけれども、あと１点だけ、すみません。先ほど企業さんの「o」を「ゼロ」にしてしまうような類似のドメイン、あれはテイクダウンをしていく必要があるというふうに言っていたわけですが、それはテイクダウンをしてもらえる機関にお願いをしてそれでやってもらえているという。

【日本プルーフポイント（増田）】　そうですね。基本的にはICANさんにこれをテイクダウンしに行くんですけれども、大体３か月ぐらいかかってしまうんですよね。１か月かかっていると大体フィッシングのメールのキャンペーンは終わってしまうので、テイクダウンはしに行くもののそれが的を射ていないというところがあるので、バーチャルテイクダウンというようなものがあったりします。例えばプルーフポイントは世界の４分の１に幅を利かせられるので、そこのブロックリストに入れていく。うちのパートナーさんでCloudflareさんとかAmazon、AWSとか50社と提携しているので、うちでバーチャルテイクダウンでそれをブロックリストに入れてねというふうに他のパートナー企業にも言うと、大体うちの場合は24時間以内、他社さんも含めて３日ぐらいでバーチャル的にはそこには通じなくできるような、こういったものもあったりします。

【星構成員】　そういうことなんですね。それは自主的な取組といいますか、そういうバーチャルでということであるから強制権限みたいなものはなくてもできると、そういう形になるわけですね。

【日本プルーフポイント（増田）】　はい。

【星構成員】　分かりました。すみません、いろいろとありがとうございました。

【日本プルーフポイント（増田）】　BIMIまでやっていただいて類似ドメインであればマークが出なくなるので、やはりこのBIMIに持って行っていただくというのが。

【星構成員】　そうですね。そちらのほうで。

【日本プルーフポイント（増田）】　一番、このなりすましメール全体に対していいことかなと思います。

【星構成員】　承りました。ありがとうございました。すみません、いろいろと勉強になりました。ありがとうございます。

【日本プルーフポイント（増田）】　とんでもないです。

【大谷主査】　星構成員からの大変よい質問で、具体的な課題というのが明らかになったかと思います。守りの方法というので、これから十分に伸びしろがあるところですので、そこを頑張っていくということがとても期待されているかと思います。また、増田様には丁寧な御説明いただきまして、ありがとうございました。

それでは、時間の都合もございますので、事業者様からフィッシングメール対策の各社の取組についての御説明をお願いしたいと思います。質疑応答は４社まとめてとさせていただきますので、まずNTTドコモ様からお願いいたします。

【NTTドコモ（福山）】　NTTドコモの福山です。よろしくお願いいたします。それでは、資料の12－３に基づきまして、当社のフィッシングメール対策強化の取組について御説明させていただきたいと思います。

右下のページ番号１ページ目です。まずはフィッシングメールの発生状況についてです。先ほど増田様からの御発表にもありましたとおり、当社に寄せられている迷惑メールの申告件数につきましても増加傾向が見えております。左下のグラフを御参照ください。フィッシングメールの内容の傾向ですが、こちらは当社に寄せられているものと社会全般で見られる傾向は同じようなものと認識をしており、例えば企業を装うフィッシングメールのほか、直近では国勢調査の回答依頼やハロウィン宝くじ企画の御案内等々、季節のイベントと関連づけたフィッシングメールも確認されている状況となっております。

２スライド目です。こちらでは迷惑メール対策に関するこれまでの当社の取組について、御紹介をさせていただいております。当社はフィッシング詐欺からお客様を守るため、従来から電気通信事業者の責務として迷惑メール対策、利用者への周知・啓発を積極的に実施してまいりました。下の表に示しておりますのが当社の対策内容を示した表になっておりますが、迷惑メール対策サービスについては多くのサービスを無料で御利用いただけるようにしているところです。例えばこちらに記載しております１番から４番の対策内容につきましてはいずれもお申込みが不要で、かつ無料で御利用いただけるものとなっており

ます。また、２番から４番につきましてはデフォルトオンで機能を御利用いただけることとなっております。

３ページ目になります。こちらではフィッシングメール対策強化に関する当社の取組状況につきまして、９月１日の要請文書を踏まえて大きく３点、御説明をさせていただきたいと思います。まず、１点目です。フィルタリング精度の向上についてですが、弊社で収集しましたフィッシングメール情報をセキュリティベンダーに提供する等、セキュリティベンダーとの連携によるフィルタリング精度の向上につきまして取組を実施しております。また、お客様から当社に寄せられる迷惑メール申告の分析をする際に、機械学習による分析の効率化の取組も実施しております。さらに、フィッシングメール判定のシステム改良やAIの活用等、フィッシング精度のさらなる向上とつきまして現在、検討をしているところでございます。

続いて、先ほども御説明にあったDMARCの導入の状況について御説明をさせていただきます。送信ドメイン認証技術、DMARC等の導入につきましては、当社では従前より推進をしております。さらに、国民を詐欺から守るための総合対策、同2.0を踏まえまして、取組をさらに促進している状況にございます。具体的に申し上げますと、キャリアメールであるドコモメールでは既にDMARC、BIMI、双方導入済みの状況になっております。その他、当社で他のメールサービスも提供しておりますが、それらについてもおおむね2026年度の上期までにDMARC、BIMIの導入を完了することを予定しております。３点目、ドメインレピュテーション導入に向けたシステム仕様等の検討についても、現在実施しているところになります。

そして、最後に利用者に向けた周知・啓発についてです。当社のホームページに「フィッシング詐欺への対策」とのサイトがございまして、こちらで最新のフィッシング詐欺事例、事前対策、被害に遭った場合の対応方法などを紹介しており、フィッシング詐欺に関する注意喚起について継続的に実施している状況になっております。

その次のページからは参考になりますが簡単に御紹介しますと、４スライド目につきましては、2025年の２月からになりますが、これまでDMARCについて拒否ポリシーのみに準拠しておりましたが、２月から新たに隔離ポリシーにも対応するようになり、迷惑メールフォルダの機能を追加したとの御紹介になります。

５スライド目ですが、こちらは2024年の10月からとなりますが、ドコモメールのなりすましメールの警告表示機能を導入しましたとの御紹介です。

６スライド目ですが、こちらも同じく2024年10月からですが、ドコモメールにBIMIを導入しましたとの御紹介スライドとなっております。

そして７スライド目になりますが、こちらが先ほど御紹介させていただきました「フィッシング詐欺への対策」サイトになっておりまして、ドコモからのお知らせとして、こうしたフィッシングサイトに御注意くださいであるとか、被害に遭わないためにこうしてください、万が一被害に遭ったらこういうことをしてくださいといった内容を御紹介しているものとなっております。

簡単ですけれども、NTTドコモからは以上となります。ありがとうございました。

【大谷主査】　御説明、ありがとうございました。

続きまして、KDDI様から御説明、お願いいたします。

【KDDI（山本）】　KDDIの山本です。資料12－４で御説明させていただきます。まず、本日の御説明の内容でございますが、大きく２点でございます。一つが当社の迷惑メール対策、これまでに対応しているものでございます。それから２つ目が新たなフィッシングメール対策の検討状況でございます。

まず、スライド１でございます。こちらが当社のこれまでの迷惑メール対策の状況でございます。弊社の場合、2012年より当社のEメールサービスにおいて迷惑メールの疑いのあるメールを自動的に検知し、そして規制するフィルタリングサービス、名前としては迷惑メールおまかせ規制というものを提供しております。直近では2023年にDMARC及びBIMIなどの導入により、フィッシング対策を強化しております。

こちらの絵でございますが、時系列でお示ししておりますけれども、左下、2012年に提供を開始し、2013年にはEメール契約時に自動設定するという形にしております。そして、2019年には全てのお客様に一斉適用する。そして、直近の対応としては2023年に対策を強化しておりまして、DMARC、BIMIの導入、あるいはDMARCポリシーの設定、それから踏み台送信、ドメインレピュテーションなどなど対応しております。つまり、９月１日付の総務省様からの要請との関係で言いますと、（２）につきましては既に対応済みということでございます。

続きまして、次のスライドは新たなフィッシングメール対策の検討状況でございます。こちらは９月１日付の要請で言うところの（１）への対応という形になります。具体的にはフィルタリング精度の向上、強度の適正化を2025年度から段階的に実施することを検討中でございます。フィルタリング設定の促進、あるいはなりすましの疑いのあるメールに

対する注意喚起、これを2025年度中に実施できるよう検討中でございます。左下に書いてございますとおり、精度の向上と強度の適正化につきましては、判定に必要な情報の拡充によりまして精度を向上していくと。つまり、正規メールが本来届くべきものでございまして、迷惑メールはフィルタリングの精度を向上し、自動的に破棄する。あるいは隔離フォルダなどの設置なども検討しているところでございます。

続きまして、右側がお客様への周知・啓発でございます。フィルタリングサービス未設定のお客様に対して継続的に設定を促すと、フィルタリング設定はこちらという形で御案内する。それから、メール開封時になりすましメールの可能性、こちらはどうしても全て取り除くことができない場合、可能性があるものについては注意喚起をする。なりすましメールの可能性がありますので御注意くださいという形の御案内をしていく。こういった取組をしまして、９月１日付の要請にしっかりと対応してまいりたいと思います。

非常に短いプレゼンではございますが、弊社から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、続きましてソフトバンク様から御発表、お願いいたします。

【ソフトバンク（平田）】　ソフトバンクの平田でございます。では、発表させていただきます。資料12－５に基づいて御説明させていただきます。

まず、当社では下に記載しているような各種迷惑メールの対策サービスを現在、既に提供しているところでございます。こちらの各サービスについては弊社のEメールサービスの機能として無料で御利用いただけるものとなっております。ですので、本日はそれ以外の状況につきまして、９月１日にいただいた要請の内容に基づいて、状況を御説明させていただきます。

まず１個目、フィルタリングの精度の向上の件、検討事項という上の欄に書いているのは要請の文章に書かれてた文言そのものですので読み上げはいたしませんが、当社の状況としましてはまず迷惑メールデータの収集とか解析をより一層強化するということを今検討しておりまして、メールフィルタリングの精度向上に努めております。それから、迷惑メールのフィルタリングについて現在提供しているものについては、強度が「強」とか「標準」とあるんですけれども、「強」と設定するほうが効果的であるというような周知を弊社のウェブサイトで掲載をしているということ。あと、またそれに加えてメール迷惑メールフィルタリングの強度を「強」に設定することをより強く推奨していく内容を今後、当社のウェブサイトなどで掲載してやっていく予定をしております。こちらが参考までで

すが、現在の強度の設定に関する弊社のサイトの記載になります。

続きまして、なりすましメール対策です。下の当社の状況というところですけれども、なりすましメール拒否設定としてDMARCは既に導入し、お客様に提供しております。また、踏み台送信の対策として、アカウント不正利用対策及び送信元なりすまし防止の２点を実施しております。また、BIMIに関してですが、弊社のEメールサービスの中でEメール（i）というものについては導入済みでございます。その他のEメールサービスについても現在準備を進めているところです。

最後に周知・啓発ですけれども、本年の６月に国際電話の詐欺電話に関していろいろ要請をいただいたことを踏まえて当時、総務省さんででんわんセンターが開設されるのに併せて、特殊詐欺に関する注意喚起のお知らせというものをホームページ上で行いました。その中で詐欺電話の話だけではなく迷惑メール等の対策についても、有用である当社のサービスというような紹介等を行っておりました。また今般、詐欺電話に加えてフィッシングメールの危険性について契約者に注意喚起を行うウェブサイト、特設サイトみたいなものを現在作成中でございまして、12月中には完成する見込みでおります。こちらのサイト内で先ほど申し上げたメールのフィルタリングの強度に関するところの推奨も行う予定にしております。これが６月に出した注意喚起になりますので、参考に載せております。

弊社からの御説明は以上になります。

【大谷主査】　平田様、ありがとうございました。

12月中に完成するフィッシングメールの危険性について注意喚起を行うサイト、ぜひ私もチェックさせていただきたいと思います。見やすいものを期待しております。よろしくお願いいたします。

続きまして、楽天様からの御発表をお願いいたします。

【楽天モバイル（小田）】　楽天モバイル、小田でございます。では、資料12－６を使って御説明させていただきます。本日は御説明の機会をいただきまして、ありがとうございます。当社のメールサービスの概要、それからフィッシングメール対策、利用者の方々に向けた周知・啓発等について御説明させていただきます。

まず、初めに当社を提供するメールサービスについて御紹介させていただきます。当社は2022年７月より無料のオプションサービスとして楽メールというサービスを提供しております。この楽メールは楽天モバイルの契約者の方々が専用アプリ内で申し込みをすることで利用可能となるものでして、スマホで撮影した高解像度の写真ですとかちょっとした

動画も扱えるように、大容量の添付ファイルにも対応しているといった特徴がございます。

この楽メールにおけるフィルタリング及びなりすましメール対策について御説明させていただきます。このサービスにおきましては、従来より一般的な特定のアドレスですとかドメイン、それからメール事業者別の受信設定に加えまして、左側にありますようなフィッシングメール対策としても機能するメールフィルタ機能を具備しております。具体的には、DMARCを含めて対応したなりすましメール、それから大量送信者からのメール、ウイルスメールをそれぞれ検知しまして、迷惑メールとして別フォルダに隔離する機能がございます。これはデフォルトオンで設定して、提供してございます。また、URLリンクを含むメールを隔離する機能も任意で設定可能というものをやってございます。当社といたしましては、今後もAIや機械学習の活用等も視野に入れまして、フィルタリング精度の一層の向上等を行うことで、フィッシングメールからお客様お守りできるメールサービスを提供していくべく、引き続き取り組んで参る所存でございます。

続きまして、当社の利用者の方々に向けた周知・啓発について御説明させていただきます。当社のウェブサイトですとか周知メール等でフィッシングメールや偽SMS、それからなりすましメール等の様々な不正手口を紹介してございます。特にウェブサイトにおきましては各不正手口の狙いですとか、それらに直面した際の注意事項、スマートフォン上での具体的な対処方法等を情報提供することで、一過性の啓発にとどまらず万一の際に参照いただけるページとして御利用いただけるよう、作成している次第でございます。

最後に今年８月に開始しました最強保護というオプションサービスについて御紹介させてください。大きく３つの機能がございまして、左側の個人情報流出、それから中央の危険なウェブサイトやWi－Fiへのアクセスを検知といったような機能と、右側に御紹介しておりますトラブル解決サポートをセットで御提供するものとなっております。このトラブル解決サポートいうところではトラブル時に相談等ができる専用の電話窓口を設けておりまして、また経済的な損失に関する補償サービスも御提供しております。これらによりましてデジタルな不正に対する消費者の方々が抱える漠然とした不安、あるいは万一巻き込まれた際の事後対応をサポートするものでして、本日議題になっているフィッシングに限らず様々な不正に対応するものになってございます。

次のページは、先ほど日本プルーフポイントの増田様からバーチャルテイクダウンのお話がありましたが、まさにフィッシング対策観点の参考資料として、当社の最強保護で検出した危険なウェブサイトにアクセスがあった場合に警告表示を出すというもので、こう

した警告画面が出るという機能を提供していますので、御参考までに示させていただいております。

当社からの御説明は以上でございます。ありがとうございました。

【大谷主査】　御説明、ありがとうございました。

それでは、ただいまの御説明につきまして御質問がありましたら、お願いしたいと思います。また、４社から御説明いただきましたけれども、事業者の取組の御発表を踏まえまして、今後目指すべき方向性について御意見などを頂戴したいと思います。それでは、またチャットをお願いしたいと思います。

先ほど楽天様から御説明いただいたんですが、このときにDMARCの導入をされて隔離・拒否をされているということですけれども、総務省から９月１日付の要請事項の（２）のところに対して、DMARCポリシーに基づく処理は一定程度されているという理解でよろしいかと思いますが、ドメインレピュテーション、それからBIMIなどの対策の状況について十分に聞き取れなかったので、少し補足説明していただけるとありがたいんですが、小田さんいかがでしょうか。

【楽天モバイル（小田)】　楽天、小田です。資料中、あるいは私の御説明中で言及が漏れており、恐縮です。いただいた件に関しまして、ドメインレピュテーションですとか踏み台送信対策機能については対応が完了しているんですけれども、BIMIについてはまだ準備中の状況でして、今準備を進めているという状況でございます。以上です。

【大谷主査】　では、BIMIについても準備されているということですので、早期の実現を期待したいと思います。どうぞよろしくお願いいたします。

それでは、私のほうで見ているチャット欄で、鎮目構成員、よろしくお願いします。

【鎮目構成員】　本日は事業者の皆様から丁寧な御説明をいただきまして、ありがとうございました。各キャリアにおいてフィッシングメール対策の強化を着実に行ってくださっているとうかがい、大変心強い限りです。ただ、警察庁によって発表されているサイバー空間をめぐる脅威の情勢などの統計的な資料を参照すると、フィッシングの報告件数が右肩上がりで増えている状況が続いています。

現在、取り組んでいる事業対策の強化が、件数を実際に押し下げる方向に働くのかどうかということを今後注視していく必要があるでしょう。様々な対策を打てば新しいやり口をどうしても犯罪者は見つけてくるというところがありますので、結局はいたちごっこになるのかもしれませんが、着実に手を打ちつつ、さらに先回りしてどういった対応が考え

られるのかということを、引き続き考えていく必要があるのではないかと思った次第です。

私からは感想ですが、以上でございます。

【大谷主査】　貴重な御意見をいただきまして、ありがとうございます。

他の構成員の皆様、いかがでしょうか。

できましたら９月１日の総務省からの３点にわたる、２点目については中身が非常に濃い内容になっているかと思いますが、それぞれの取組などについて引き続き注視し、進捗度合が多くの方の目に触れるような形で整理され、公表されていくことが望まれるのではないかと、私のほうでは考えております。また、先ほど増田様から非常に衝撃的な、日本に対する攻撃について御説明いただいたところですので、引き続きこういった情報収集を行いまして、実際の攻撃に見合った対策がとられているかといったことについて常に注視していく、そして必要な対策をお願いしていくという共同体制がとれればよろしいのではないかと考えている次第です。

それでは、特にチャット欄への追加の書き込みがないようですので、この辺りで質疑応答を終了させていただければと思います。もし、どうしてもここを確認したいということがありましたら後ほど事務局宛にでも御連絡いただきまして、個々の事業者様からの御回答などをお願いできればと思います。どうぞよろしくお願いいたします。

本当に活発な御議論、それから貴重な御意見を賜りまして、ありがとうございました。このワーキンググループですけれども、本日で一区切りとさせていただきたいと思っております。本日の議論を踏まえまして、事務局、大内利用環境課長から御挨拶いただけるとのことでございますので、よろしくお願いいたします。

【大内利用環境課長】　ありがとうございます。構成員の皆様におかれましては、大変御多用の中、精力的に御議論を賜りまして、誠にありがとうございます。総務省利用環境課長の大内でございます。

今日は大きく２つの点で方向性を示しいただいたかと思ってございます。１点目の携帯電話の不正利用対策につきましては、多回線契約の在り方につきまして、犯罪等の抑止と利便性のバランスを取る形で、しっかりと方向性をまとめていただいたかと思ってございます。既にデータ専用SIMですとか法人契約の代替確認についてもまとめていただいていますので、今日の件を含めて大きなまとまりとしての一定の方向性をお示ししていただいたと思ってございまして、今後親会の議論を経る必要がございますけれども、行政、総務省としてもしっかりと受け止めさせていただきまして、必要に応じたルール化に向けた検

討を進めたいと考えているところでございます。

もう１点、フィッシングについてですけども、増田様からの御報告にもありますとおり、日本がある意味狙い撃ちとなっている状況でございまして、証券業界からも対策強化の期待が寄せられている中で、総務省として要請ですとか意見交換を行わせていただいてきたところでございます。本日、今後の方向性について御意見いただいておりまして参考にさせていただきますけれども、まずは携帯電話各社様からこれまでの対策に加えまして新たにフィルタリングの精緻化ですとか認証技術の高度化といった対策に向けて、歩みを進めるといった旨の具体的な表明をいただいたことを歓迎いたしまして、できるだけ早くこれらのサービスを実装していただくことによりまして、いわゆる詐欺誘因メールといったものが目に見えて減ったと言えるような環境の実現を大いに期待したいと考えているところでございます。

以上となりますけれども、引き続き、どうぞよろしくお願い申し上げます。よろしくお願いいたします。

【大谷主査】　ありがとうございます。

本日も構成員の皆様から様々な御意見、貴重な御意見をいただきました。これらの御意見を含めまして、親会であるICTサービス利用環境の整備に関する研究会への御報告を取りまとめていきたいと思います。これから後の作業としましては、事務局と主査との間で意見交換をしながら取りまとめをしてまいりたいと思いますが、その作業の内容については主査である私に御一任いただきたいと思いますが、いかがでございますでしょうか。

御異議がないようですので、ありがとうございます。それでは、取りまとめを行いまして、親会への御報告を進めていきたいと思います。

それでは、事務局から御連絡をお願いいたします。

【田中利用環境課課長補佐】　ありがとうございます。本ワーキンググループは本日で一区切りですけれども、親会であるICTサービス利用環境整備に関する研究会の開催については、別途事務局から御案内いたします。事務局からは以上でございます。

【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第12回会合を終了させていただきます。本日、それからこれまでのワーキンググループ、12回にわたって皆様、お忙しい中、御出席いただきまして、ありがとうございました。これにて閉会とさせていただきます。ありがとうございます。