

消費者委員会 消費者をエンパワーするデ
ジタル技術に関する専門調査会（第3回）
議事録

消費者委員会 消費者をエンパワーするデジタル技術に関する
専門調査会（第3回）
議事次第

1. 日時 令和6年6月14日（金）14:00～16:26
2. 場所 消費者委員会会議室及びテレビ会議
3. 出席者

（委員）

【会議室】

橋田座長、原田委員、山口委員

【テレビ会議】

森座長代理、荒井委員、田中委員、鳥海委員、松前委員

（オブザーバー）

【テレビ会議】

柿沼委員、黒木委員、山本委員

（参考人）

【会議室】

池谷秀史氏 BBソフトサービス株式会社プロダクト本部
PR企画部/サポート企画部副本部長(兼)ディレクタ

【テレビ会議】

坂倉翼氏 トビラシシステムズ株式会社
執行役員 営業企画部長 営業統括室長
藤井仰氏 トビラシシステムズ株式会社
営業企画部プロダクト企画課長
藤井智康氏 トビラシシステムズ株式会社執行役員 CTO
佐々木貴浩氏 トビラシシステムズ株式会社コアデータベースR課長
柘植悠孝氏 トビラシシステムズ株式会社
コアデータベースR課セキュリティリーサーチャー
太田祐一氏 株式会社DataSign代表取締役社長

（事務局）

小林事務局長、友行参事官、江口企画官

4. 議事

(1) 開会

(2) ①事業者ヒアリング（トビラシステムズ株式会社）

②事業者ヒアリング（BBソフトサービス株式会社）

③事業者ヒアリング（株式会社DataSign）

(3) 閉会

《1. 開会》

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

ただいまから、消費者委員会第3回「消費者をエンパワーするデジタル技術に関する専門調査会」を開催いたします。

本日は、原田委員、山口委員は会議室で、森座長代理、荒井委員、田中委員、鳥海委員、松前委員はテレビ会議システムにて御出席いただいております。森座長代理は少し遅れて参加されるとのことです。

本日は、所用により、相澤委員、坂下委員は御欠席との御連絡をいただいております。

消費者委員会からは、オブザーバーとして、柿沼委員、黒木委員、山本委員はテレビ会議システムにて御出席いただいております。柿沼委員は少し遅れて参加されるとのことです。

本日は、事業者ヒアリングとして、トビラシステムズ株式会社の坂倉様、BBソフトサービス株式会社の池谷様、株式会社DataSignの太田様に御発表をお願いしております。坂倉様、太田様はオンラインでの御参加となります。

ここで、これまで所用により御欠席されていた松前委員が御出席されておりますので、自己紹介をお願いいたします。また、本専門調査会において検討を予定している内容に関する問題意識や御関心分野などについても併せて一言お願いできればと思います。

では、松前委員、よろしくお願いします。

○松前委員 駒澤大学の松前と申します。

第1回、第2回は残念ながら都合のつかない日程での開催となってしまいまして、今回から参加させていただくことになりました。どうぞよろしくお願いいたします。

私は、プライバシー、個人情報保護法制の研究をしております。特にEU、米国との比較法制度研究や、新しい先端的な情報技術によって生じるプライバシー、個人情報保護の問題等についての研究を行っております。この検討会でも出てきておりました話との関係では、例えばダークパターンに関するアメリカカリフォルニア州の法規制ですとか、あとは脆弱性との関係では、子供の個人情報保護に関する研究なども行っております。

この検討会との関連での問題意識としましては、2つ申し述べさせていただきたいと思います。

1点目は、消費者の意思決定に関する問題です。私の理解している範囲では、この検討会の趣旨の一つに、現代社会における消費者の意思決定が必ずしも合理的にはなされていない中で技術的な仕組みを使って支援していく、エンパワーしていくというところがあると理解しておりますけれども、意思決定をめぐるのは、個人情報保護の世界でも同様の問題がございます。御案内の方も多いとは思いますが、個人情報保護法制においては、個人情報

報の処理を行う際に、その処理の内容を本人に通知して、それに対して本人が同意するというのが基本的なプロセスになりますけれども、この通知に当たるプライバシーポリシーを必ずしも皆さん読んでいないとか、十分に理解できないといった問題がありまして、私もこの問題についてここ数年、どういった対策が取り得るのかということを、法制度との関係ではありますけれども研究してきております。ですので、この辺りのお話はもしかするとこの検討会でも共有させていただけることがあるかもしれませんし、皆様からいろいろと御教授いただきながら、議論に参加させていただければと思っております。

それから、もう一点目ですけれども、この検討会の検討内容の一つに、個々の消費者にパーソナライズしたAIを検討するというものがあると理解しております。これはどういうシステムを作るかによろしいと思いますので、あくまで一般論にはなりますけれども、個々の消費者にパーソナライズするとなりますと個人情報収集していくことになりまして、特にこの検討会では脆弱性の高い人々、特に高齢者の方々といった方の個人情報も収集する可能性がある。そうなりますと、高齢者の見守りサービスなどでも既に生じている問題ですが、要配慮個人情報ですとか、あとはそれに該当しなくても極めてセンシティブ性の高い、プライバシー性の高い個人情報を収集していくという可能性も出てきます。こうした個人情報、プライバシー保護の問題をクリアしつつ、実効性のある技術的支援の仕組みをどう作っていけばよいのかというところには非常に興味を持っておりますので、この辺りも皆様にいろいろと教えていただきながら、意見交換させていただければと思っております。

以上になります。どうぞよろしくお願いいたします。

○橋田座長　ありがとうございます。どうぞよろしくお願いいたします。

では、本日の会議の進め方等について、事務局より説明をお願いいたします。

○江口企画官　議事に入る前に配付資料の確認をさせていただきます。

お手元の議事次第に配付資料を記載してございます。

もし不足等がございましたら、事務局までお知らせください。

本日は、報道関係者を除き、一般傍聴者はオンラインにて傍聴いただいております。

議事録については後日公開いたします。

以上でございます。

○橋田座長　では、前回に続きまして、デジタル技術の活用例、消費者の支援に活用するアイデア、社会実装するに当たっての課題と考えられる事項などにつきまして、関係者のヒアリングを行った上で、さらなる活用について意見交換をしたいと思います。全体を通じて、委員からの積極的な御発言をお願いいたします。

まずは迷惑電話フィルタ製品や迷惑電話番号データベースを用いたサービスなどを提供されているトビラシステムズ株式会社さんから御発表をお願いいたします。20分程度でお願いいたします。

では、トビラシステムズ株式会社の坂倉様、よろしくお願いいたします。

《2. ①事業者ヒアリング（トビラシステムズ株式会社）》

○坂倉氏 お世話になっております。トビラシステムズの坂倉と申します。

本日は、こういった場にお呼びいただきまして、誠にありがとうございます。

画面を映しながら説明に入らせていただきますので、少々お待ちいただければと思います。

では、説明させていただきます。

弊社トビラシステムズでございますが、名古屋に本社を置くIT企業でございます、特殊詐欺をゼロにするということを目指している企業でございます。

代表は明田といいまして、彼の祖父が原野商法に引っかかってしまったことを助けたいという思いでプロダクトを開発しておりまして、後述いたしますが、今では利用者数としては1500万人以上の方に御利用いただいているサービスを作っている会社でございます。

簡単ではございますが、弊社の軌跡を紹介させていただきます。

2010年10月に迷惑電話フィルタというものの開発に着手しておりまして、2年後の2012年6月に迷惑電話フィルタの「トビラフォン」というものを開発して、販売開始しております。

2015年3月に警察庁と特殊詐欺電話に関する覚書を締結させていただいておりまして、2016年3月には、3大キャリア全てのオプションサービスとして提供を開始しております。

少し飛びますけれども、2021年10月に280blockerというアドブロックのほうも、会社を吸収合併しておりまして、サービス開始しております。

その他、弊社としましては、特殊詐欺やフィッシング詐欺に関するレポートを毎月発行しておりまして、独自に啓蒙活動を行っております。僭越ではございますが、情報開示とともに、ふだんやり取りをさせていただいております警察様とか省庁様、キャリア様、パートナー企業様という方々にも展開をしておりまして、非常に御興味ですとかいろいろな情報交換を行わせていただいているかなと考えております。

弊社の特殊詐欺を防ぐ方法としては、独自の情報データベースを築いておりまして、特殊詐欺等と迷惑電話をブロックする仕組みを提供しております。弊社の迷惑電話情報データベースに関しましては、特殊詐欺に関する電話をブロックしまして、電話自体がかからない仕組みを提供しております。従来ですと、例えば電話をブロックしようとしますと、怪しい電話がかかってきますとまず出て、迷惑電話として登録すると2回目をブロックしたりといったものはございますけれども、弊社のサービスに関しては、まだ一度も出たことのない未知の電話番号であったとしても初回からブロックすることができますので、そもそも怪しい電話に出ないことができる唯一のサービスなのかなと自負しております。

展開としましては、先ほどお話ししましたように、モバイル向けに展開をしております、各キャリア様に我々のほうから提供しているサービスがございまして、あとはアドブロックの280blockerというものを紹介しております。

その他に関しましては、固定電話向けのサービスとして、例えば中部電力様ですとかJ:COM様、auひかり様等々と連携をしまして、お電話を買い換えたときとか回線を契約したときに、我々のサービスに入っていただくような仕組みを提供しております。

また、ビジネスフォン向けという形で、会社の電話に対して取付けをする機械であったりとか、スマートフォンで利用できるビジネスフォンアプリを提供しております。

少し話は変わりますが、特殊詐欺自体はなかなか減少しないと言われておりまして、そういった要因について、我々のほうでまとめておりますので御報告させていただいております。一番左の絵でございまして、特殊詐欺自体の認知度に関しましては、ニュースでも日々行われておりまして、皆様が知っているという状況かなと思っております。

ただ、真ん中にありますように、被害に対する意識に関しましては、自分は被害に遭わないと思っていたという方と、どちらかといえば自分は被害に遭うと思っていた、ほとんどの方が、全く自分は被害に遭わないとお考えなのかなと思っております。認知度が高いにもかかわらず、非常に当事者意識がないというところが問題なのかなと考えております。

こういったことを受けまして、結局、認知はしているが誰もが全く被害に遭わないと思っておりますので、グラフの一番右でございましてけれども、対策を取っている方はほとんどいっしょらなくて、要は誰も対策をしていないのでなかなか被害が減少しないのではないかなと思っております。

弊社の固定電話に向けた迷惑電話情報サービスの遷移を少し御紹介させていただきます。

もともとは電話機に外づけする形で、装置を販売しておりまして、家庭用電話機に後づけで迷惑電話の防止機器を装着するという外づけ型で販売を開始しております。その後に、一体型という形で呼んでおりますけれども、電話機自体にそういった機能を具備した商品も販売しております。

さらに進化しておりまして、電話自体を回線で替える、例えばNTT様から、恐縮ですがKDDI様に替えるとかというときに替わる機械があるのですけれども、その機械の中に内蔵するような形のものが今出ております。

最も新しいパターンとしましては、ネットワーク型という形で、機械は何もなくて、お客様のほうが回線を変更した場合、もしくは途中でこういったサービスが欲しいといったときに、メールとか電話でもすぐに申し込めるサービスも展開させていただいております。ですので、より簡単に、より現環境を変えない状況でサービスの利用開始が可能な状況になっています。

そもそもの迷惑電話の防止システムについて御紹介させていただければと思っております。

弊社の迷惑電話情報データベースに関しましては、当然、弊社が集めた膨大なデータを

基にブロックする仕組みでございますが、集める手法としましては、先ほど申しましたように、各サービスで月次で利用いただいている方は1,500万人以上ユーザー様がいらっしゃいますので、そういった方々が使っている情報をログとして頂くような情報で番号を集めております。あとは警察様とも提携しておりまして、日々データを頂くような状況になっています。あとは弊社のほうで2010年からずっと独自に集めているような情報収集もしておりまして、SNSやURL等々に関しても独自調査でデータを集めております。

こういった情報で日々集めた膨大なデータベースを保有しておりまして、これを各種サービスへそのまま展開しますと、いろいろな電話番号がひたすら止まってしまうということになりますので、弊社としては、集めるという部分に関しても評価いただくことはあるのですけれども、これを精査して、最適であると思われるデータベースを日々更新しながら提供するというところに対して御評価をいただいているのではないかと考えております。

少し話が替わりますが、280blockerという商品も展開しておりまして、こちらはウェブブラウジング上に表示される情報から、広告のブロックルールによりまして広告を特定して、広告をブロックするというようなサービスになっております。昨今、怪しい広告に関しても多くなってきておりますので、先ほどの電話と同様に、怪しい情報自体がもうそもそも見えないという状況でございますので、何か怪しいものがあつたとしても、そこに引っかかるというリスクを減らせるのではないかと考えております。

サービスの今後の見込みですけれども、サービスの利用機会の拡大に関しては当然弊社としても常に考えておりまして、今既に展開いただいているところに関してではなく、新規でサービスとして取り扱いいただくようなキャリア様とか、例えば扱ってみようと思われるような販売店様等々に対するサービスの御紹介に関しては行わせていただいております。

あとは、さらに既存のお取り扱いサービスの御利用者様増加のために、啓蒙活動やプロモーション等々をパートナー様、警察様、省庁様等と連携をしながら行っております。

2に関しては、新規・既存ともに御利用を開始いただいた後に利用継続いただくために、新しい機能の追加や情報収集をしてアップデートを常に行っております。

今、御紹介したもの以外にも、新規で何かお役立ていただけるようなサービス展開ができないかというふうにして、サービスの開発に関しても常にアンテナを立てながら行っております。

最後に4つ目ですけれども、AIの活用に関しても当然広く考えておりまして、直近ですと各種DB作成に活用したりとか、音声認識を応用して活用するようなことも考えております。

弊社サービスが消費者契約に関して寄与できると考える機能について御紹介させていただけるのかなと思っております。

先ほどから特殊詐欺にというお話をしておりましたが、詐欺に対する電話番号はたくさん保有しているのですけれども、詐欺電話ですと完全にブラックな犯罪につながる電話ですので、犯罪グループに関しては番号をどんどん替えていく傾向が強いのですが、なかなか

か消費者契約系の営業活動等に関してはグレーなものも多いものですから、こういったものも電話番号も非常に保有しておりまして、類似の効果があるのではないかなと思っています。

例えば家庭用電話サービスに関しては、迷惑な電話自体かかってくるということをそもそも抑えるようなことが機能としてございますし、例えば怪しい電話に出てしまって、御高齢者とかが何か物を買ってしまったときに、後ほど発着信の履歴から情報を確認して、御家族が何かフォローするようなことができるような通信履歴管理等々も家庭電話用サービスのほうには付いております。

法人向けに関しては、小さい会社様とかには消費者契約系の話があることはあるかと思うのですが、先ほどのものに加えまして、通話の録音だったりとか、ただ履歴だけではなく、音声としてもデータを残すことが可能になっております。

IVRと言われるような、怪しい電話がかかってきたときに自分では出ないで違う番号に誘導するようなことであったりとか、例えば違う番号に転送してしまうような条件転送のような機能に関しても、法人向けにトビラフォンBizに関しては有しております。

同様に、トビラフォンcloudという法人向けのアプリサービスに関しても、同じになっていきます。

モバイル用に関しては、同じく迷惑電話のフィルタに加えましてSMSのブロックもありますので、怪しい要件のSMSが来た場合に関しては、こういったものもブロックできる可能性を備えております。

少し飛びますけれども、下のほうに関しては先ほど申しましたように、280blockerに関しては広告表示を物理的に削除しますので、クリックで誘導されて、引っかかるようなことに関しては抑止できるのではないかなと考えております。

実際に、前頁を進めるに当たっての課題として弊社の方で考えているものでございますが、まずは特殊詐欺同様に、ユーザー様の当事者意識がなかなか低いのではないかなというところが大きい課題感かなと考えております。被害や困り事に巻き込まれてしまう可能性は誰でもあり得るのですけれども、自分が流されてしまったりすることに関しては拒否感があるような方々が年齢問わず、特に高齢者に関しては多いと聞いておりますので、ユーザーの当事者意識というところに関してはなかなか変えるのは難しいかなと思いつつ、大きな課題かなと考えております。

2つ目はコストかなと思っておりまして、ユーザーさん目線で見ますと、昨今、非常にコスト意識が高いことから、明らかにというものに関してはお金は出されるかと思いますが、当事者意識が低いということも鑑みて、セキュリティーサービスに対して残念ながら前向きではない方々が多いのかなと考えています。

今度、事業者様目線で見たとくも、上記等々から利益性がよいサービスとはなかなか捉えられないことが多いものですから、意義的にはやってみたいなという事業者も非常に多いのですけれども、サービスの導入に対して、コストで見た場合に前向きではない事業者

様が多いことに関しては課題感かなと思っています。

また、導入いただいた事業者様に関しても、広告宣伝費をかけて積極的なサービスの拡販は行っていないこともございますので、いろいろな部分においてコストが関係して、この辺に関しては課題感かなと思っています。

最後に、導入の手間もやはりあるのかなと思っておりまして、サービスが変遷しておりますという話はしましたが、特に家庭用電話機に設置する装置においては、今、御利用の電話に外付けで機械を付けないといけないという部分がありますので、手間を考えるとそこが原因となって導入が進まないということがございます。弊社としても、例えば消費行政の補助金等々を活用いただくような自治体様と連携したりとか、ケーブル局様と連携するような施策を複数展開はしたのですけれども、現状においては想定より普及は進んでいないかなと考えています。

非常に足早ではございますが、弊社のサービスの概要説明をさせていただきました。

以上となります。ありがとうございます。

○橋田座長 ありがとうございます。

坂倉様からの今の御発表を踏まえて、質疑応答、意見交換をしたいと思います。御発言のある方は、挙手又はチャットでお知らせください。よろしくお願いします。

では、田中委員、お願いします。

○田中委員 田中です。

大変貴重な取組と技術やサービスについて御教授いただき、どうもありがとうございます。

このページとも少し関係しているのですけれども、6ページをもう一度見せていただいてもよろしいでしょうか。手口の認知度は、オレオレ詐欺ではほぼ100%に近いけれども、被害に対する意識では、4分の3ぐらいは自分は遭わないと思っていたということで、いわゆる認知バイアスのようなものが示唆されているようなグラフかなと思います。例えばニュースとかで特殊詐欺の報道があっても、被害に遭っているな、でも自分は大丈夫と思うような認知バイアスは、楽観主義バイアスとかコントロールの錯誤などと呼ばれる人間の認知的な傾向としてあるのですけれども、これについて御質問です。こういった非常に有益な技術やサービスを消費者をエンパワーすることにつなげていくためには、そういった機能が自分にとって必要だと消費者自身が思うプロセスが必要になってくるかと思います。もし消費者が自分だけは大丈夫だと思っていると、せっかくいい技術が世の中にあっても、例えば先ほどもモバイル向けのアプリケーションの御説明がありましたけれども、アプリケーションがインストールされないとか、デフォルトで入っていてもオフにされるとか、削除されてしまうとか、そういったことが考えられるかと思います。

これに対応するためには、こういった技術の必要性を消費者と共有するというプロセスが必要になってくると思うのですけれども、何かそのためにされている工夫とか課題があれば教えていただけないでしょうか。例えばアプリケーションをプラットフォームに置く

ときに、キャッチコピーとか、文言をこういうふう工夫されているとか、そういったものがあれば教えていただけると幸いです。

○坂倉氏 ありがとうございます。

おっしゃるとおり、私どもに関しては、二軸かなと思っておりまして、消費者の方々の意識をとという部分に関しては、我々も例えば啓蒙活動をしたりとか、現場でいろいろな情報を収集されていらっしゃる方々とお話をしてどう伝えるか、どう進めるかということに関しては日々考えながら、各々で発表していかないと、と考えております。

ただ、ある意味それこそニュースでも連日やっておりますし、意識としては非常にあるはずなのですが、ここは個人的な感覚もありますが、お伝えしていくことが難しいのかなと思っておりまして、もう一つは、おっしゃいましたように、デフォルトでユーザー様のほうが意識をしないような状況下において、各種サービスの中に組み込まれているようなところまで持っていくことができれば、意識をしない状況に実は裏側に我々のものがあって、怪しい電話とか消費者契約系の電話をブロックするとか、こういったことができるのではないのかなというのは、私の立場からは考えております。

○田中委員 どちらかというと、消費者の意思決定を担保するためには、オプトインよりはオプトアウト設定にしていくほうが望ましいというようなお考えになりますでしょうか。

○坂倉氏 現在はそのように考えてしまっているのかもしれないですけども、ずっと10年以上にわたって消費者の方々にはお伝えしてきたつもりですし、徐々に浸透しているのかなと思いつつ、限界もあるのかなと思ひまして、おっしゃるとおりかなと考えております。

○田中委員 ありがとうございます。

○橋田座長 ありがとうございます。

ドライブレコーダーの普及率は50%以上だそうで、トビラシステムズさんのユーザーさんは1,200万人とおっしゃいましたが、やはり被害の迫力が違うということなのかもしれないですね。

次に、原田委員、お願いします。

○原田委員 御発表ありがとうございました。

私の方から幾つか、非常に興味深かったので御質問させていただきたいのですけれども、よろしく願いいたします。

まずは5ページです。電話の特殊詐欺を防ぐ方法として、私は今回のトビラシステムズさんのサービス自体は大賛成なのですが、いろいろ乗り越えるべき課題があったのではないかなと思って、そういった質問なのですが、まず1つは、迷惑情報データベースは警察から提供された特殊詐欺に使われた電話番号と書かれておりますけれども、例えば民間の会社の方々がこれを使うことになると、電気通信のサービスですと利用の公平性とか、また別の法律に引っかかる点はなかったのかどうかとか、通信の秘密とか、電気通信事業法の方の問題点が何か課題としてなかったのかどうかという点。

あと、最後のほうに、固定電話、家庭用の電話機には難しいということでしたが、アナログ電話はおそらくもうすぐ終わりになって、IP電話かなんか、要はデジタル化するというのをNTTの東と西で一斉にやられると思うのです。なので、距離によって通話料が変わらなくなっていくというような動きになっていると思いますけれども、そういうところで今のアナログ電話ではなくて、IP電話やひかり電話みたいに仕組み自体が変わってしまう、NTTさんによって変わってしまうということで、こういうものをより入れやすくなるというようなことができるようになるのかどうかという点。

いっぱい先にしゃべってしまっていて申しわけないのですが、8ページのショートメッセージに関するほうに関しましては、我々は消費者相談を受けているのですが、フィッシングメールかなにかで届くショートメッセージの電話番号は、要は過去の被害者に乗っ取りをしてしまった電話番号から発信をされていくということで、発信された電話番号自体は善意の第三者の電話番号ということになると、それをまたブロックすることになりますと、ブロックされた側は全く分からない、乗っ取られたままで、その電話番号が他のユーザーに使われたときに、それがずっと残ってしまうという可能性はないのかどうかという点が一つ。

9ページのアドブロックの仕組みは非常にいいと思うのですが、できる限りで結構ですが、どんな方法でブロックするのかと、あとは不適切な広告が出ないようにするというのは非常にいいことだと思うのですが、他の広告に差し替えられるということであればまだ分かるのですが、全く消してしまうということになると、そっちの事業者側というか広告を出しているサイト側の方で何か問題というか、要は広告収入が得られないということになりますので、そっちの方から何か問題がないのか。アドブロックのアプリはいろいろありますけれども、大体ユーチューブとかあいうところに出てくる広告とかをブロックしたりとかすると、またそっち側の方で対策をされてしまうということで、そういった点で別の広告が出るのではなくて、全くブロックしてしまうと、そっち側の方でクレームになったりとかしないのかどうかというところ。

それと先ほどの御質問にあったところみたいに、ユーザーさんに自主的にやってもらうということになると、どうしても自分は関係ないと思ってしまう。例えば個人間取引のメルカリみたいなものも、今、エスクローサービスというのがデフォルトになっているのです。昔、黎明期の頃のオークションはエスクローサービスを有料で提供していたのですが、自分は被害に遭わないだろうということで、損保会社が加入しても、全然それを払ってまで使うユーザーさんがいなかったの、結局損保会社さんが全部手を引いてしまったのですが、メルカリさんみたいなところが強制的にエスクローシステムを導入したことによって、それが当たり前になって、安全な個人間取引ができたということになりますと、やはり消費者の方で選んでもらうとすると、さっきの認知バイアスではないのですが、本人が選ばうとはしないということで、先ほどの電話の話のように、デフォルトでシステムを組み込むことができる可能性が今後出てくるのかどうか。

いっぱい質問してしまいましたが、お願いいたします。

○坂倉氏 誠に貴重な御意見ありがとうございます。

まず、1つ目の電気通信事業法の部分に関してなのですが、キャリア様とか各省様との関係でいろいろと協議も重ねて、確かにハードルはあったのですが、最終的にはエンドユーザー様に同意をいただくという前提において進めておりますので、ここに関してはクリアしているかなと考えております。

御質問の回答になっておりましたでしょうか。

○原田委員 要はユーザーさんから自主的にやっているから、利用の公平性は通過ができるということですか。

○坂倉氏 はい、その認識でございます。

2つ目の電話自体がおっしゃいますように、IP化していったり、変化していくことに関しての我々のサービスの組み込みの可能性が上がっていくということに対してなのですが、我々も変化点と捉えておまして、NTT様を中心として各キャリア様とお話はしておまして、1つ大きなポイントかなとは考えております。

ただ、特に家庭電話において少しネガティブな意見も当然ございまして、電話自体の数に関してはシュリンクの傾向値がございますので、どちらかという減っていくものに対して当然ある程度の投資が各社様で必要でございまして、言い方は悪いですが、この投資がそもそも見合うのかどうかというところに関してはかなり慎重な議論になっておまして、そこに我々としても意義や意味を踏まえて御提案を続けたいといけないかなと思ひまして、提案を続けているところでございます。

○原田委員 ただ、今までどおりの固定電話、自宅電話を高齢者こそ使ってしまうのかなと。若い人はもう固定電話なんかは家に持たないと思いますけれども、高齢者はまだずつとそこにしがみついてしまいそうな気がするので、高齢者にはまだ要るかなと。

○坂倉氏 おっしゃるとおりです。まさしく我々もそこを警察の方とも話をする中で非常にポイントかなと思っております。言い方はよくないのですが、犯罪グループとかこういった悪質な営業電話をかけるような企業からすると、従来の電話の持ち主が、どんどん若い方は携帯とかの方に抜けて行きますので、高齢者が残っていきますので、ある意味だましやすいいリストになっているとかいうことを言う方もいらっしゃいますので、利用者が減っていたとしても、保護するという観点からは弊社サービスのようなもの、当社の思い込みも当然ありますけれども、うまく広げていければいいかなとは考えております。

○原田委員 心強いです。

○坂倉氏 ありがとうございます。

フィッシング詐欺の件に関しましては、別の者から回答させていただいてよろしいでしょうか。

○柘植氏 トビラシステムズ、柘植と申します。

フィッシングの担当をしております。私のほうから回答させていただきます。

おっしゃるとおりSMSの中でフィッシングの手口の大きなものを占めるものとして、マルウェアに感染してしまった人、一般の第三者の人たちがばらまいてしまうということがありますが、おっしゃるとおりそのお電話番号からのSMSを全てブロックしてしまうと、実際には正規のメッセージをブロックしてしまうこともありますし、あるいは別の方が後々その番号を使ったときにブロックしてしまうというようなことも当然ながら考えておりますので、送信元の電話番号を用いて一律にブロックということは現在やっていないところです。それよりは、誘導されるようなURLですとか、どのような文章を書いているのかとか、そういったところに重きを置いてのフィルタリングを実施しているところでございます。

○原田委員 ショートメッセージの中身自体も加味してブロックをするということですね。
○柘植氏 そうです。

○原田委員 例えばそれこそAIではないのですけれども、自動的にブロックすることで、さっきの話で申し訳ないですが、通信の秘密みたいなものは侵さないで、このようなURLが載っていたらブロックするみたいな、そういうイメージでいいですか。通信の秘密は侵さないということですね。

○柘植氏 そうです。立てつけ上は通信の秘密を侵しているものではなくて、SMSのフィルタリングに関しては、ユーザー様から同意を得たものであるのと、あと端末に到達した後、アプリケーションでそれをチェックしてフィルタリングするという形になりますので、そのときの中身自体ではないという点があります。

○原田委員 同意を取って、中の部分で自動的にフィルタリングするみたいな、LINEさんみたいな感じですね。

○柘植氏 LINEの中身を私は詳しく把握していないのですけれども、そういった形かと思えます。

○原田委員 ありがとうございます。

○坂倉氏 ありがとうございます。

次の280blocker、広告ブロックの件に関しても別の担当から回答させていただいてよろしいでしょうか。

○佐々木氏 トビラシシステムズの佐々木と申します。よろしくお願いいたします。

広告に関しては、不適切な広告だけではなく、そうではない広告もブロックしてしまうとクレームなどにもつながってしまうのではないかなという御質問であったかなと思うのですけれども、御指摘のとおり、今の広告ブロックの仕組みの中で、明確にあるこういう広告のみを出すというような部分をブロックしたりとかフィルタしたりということであれば問題ないのですけれども、ネットワークを通じて、1つの広告の枠の中でターゲティング等された状態で様々な広告が表示されるといったような中では、一つにはアダルトな広告が出ることもありますし、もしくは先日ネットで検索した洋服の広告が出るようなこともあるかなと思います。

今のフィルタの力ですと、枠そのものをブロックするとか見えなくするという事にな

るかなと思います。その枠の中で特定のものだけを狙ってブロックするということは、頑張ることができるのですが、できないケースも多いかなと思います。そういったところは今のところ技術的な限界もあって、一律にブロックされるような状態になっているかなと思います。今のところ、それについて何かしら明確なクレーム等につながっているようなことはないのですが、機能といたしまして、私どものアプリですと、例えばホワイトリストを登録するような機能もございまして、例えばよく見るこのサイトはそんなに広告が煩わしくはなくて、広告収入で活動されているので応援したいみたいなケースですと、ホワイトリストに登録していただくといったようなことも可能な仕組みを御提供しております。

○原田委員 そうなのですね。ありがとうございます。私から聞くと非常に心強いサービスだなと思って、見たくない、特に違法性の高い広告なんかは見ないほうがいいと思いますので、このサービス自体はとてもいいなと思う反面、逆に向こう側からしてみたら広告を見てもらえないということで、広告収入が減ったりとか、また別の手口、たちごっこみたいなことになったりとかするのかなというところをまた一方でちょっと懸念したので、今のところ、要は他の広告に差し替えではなくて、その広告ごと消えるという仕組みということですね。

○佐々木氏 はい、そうなります。

○原田委員 ありがとうございます。

○坂倉氏 ありがとうございます。

最後の御質問で、意図的に我々がうまく取れているかなのですが、エスクローシステムというのは、御質問の意図としては、基本的にはユーザー様で選んでいただくわけではなく、デフォルトサービスとして展開していくほうがいいのではないかと御指摘でよろしいでしょうか。

○原田委員 そうですね。さっきのエスクローのように、当初からあったサービスなのですが、当初は有料だったので誰も選択しなかったのですが、非常に安全性が高い取引の仕組みだったので、事業者側の方が強制的にその仕組みを取り入れたことによって、今、デフォルトは個人間取引はエスクローになったというような歴史があるものですから、そういう安全性の高いものはそういうものに取り入れてしまうみたいな形でも、それが当たり前なんだみたいなデフォルトの仕組みがやはり必要になってくるのかなというのを改めて自覚したということです。ありがとうございます。

○坂倉氏 ありがとうございます。

弊社としても当然、おっしゃいますようにユーザー様としては普通に付いているようなものの状況でお納めしたいなと考えておりますということは常にやっているのですが、視点は違うのですが、他にもう少し何か便利な機能があれば、こういったところに興味を持っていただいて入っていただけるのではとか、いろいろな視点から導入や拡大について考えておりますので、また啓蒙しながら考えていこうかなと改めて思いました。ありが

とうございます。

○原田委員　こちらこそありがとうございました。

○橋田座長　では、鳥海委員、お願いします。

○鳥海委員　興味深いお話ありがとうございました。

280blockerについてお聞きしたいのですけれども、最近ですと広告に関しても詐欺広告とかは、例えばフェイスブック上で前澤社長の詐欺広告が話題になったり、そういうのが結構あったような気がするのですけれども、こういったアプリケーションでブロックが可能なのかというのを教えていただきたいなと思います。特に私はAndroidユーザーなのでAndroidのことになってしまうのですけれども、サンドボックスとかを使っていて、なかなか外部のアプリから特定のアプリに対して操作するのは難しいと思うのですけれども、そういったものはどうやって回避されているのか、あるいはブロックそのものをどこのレベルでやっているのかをもしよろしければ教えていただけますでしょうか。

○佐々木氏　トビラシステムズの佐々木です。御質問に対してお答えさせていただきます。

広告ブロックの仕組みにつきましては、まずiOSであるか、Androidであるか、iPhoneであるか、Androidのスマホであるかによって、できることとできないことが異なっておりまして、その辺りを踏まえて御説明をさせていただきます。

まず、iOS、iPhoneのほうにつきましては、ウェブブラウザのSafari上で表示されるウェブ上のコンテンツについて、ここの部分を消すといったようなきめ細かいブロックを指定をすることができまして、その機能を使いますとかなり細かな粒度でここの部分のこの広告を消すといったようなことが可能になっています。

それとは別に、iPhoneの中で、今のお話だけですとSafariで表示される場合のウェブサイトでしか効果がないのですけれども、それ以外のアプリの場合、例えばGoogle Chromeを使った場合だとか、もしくはフェイスブックなどのアプリを使った場合はどうなるのかということになりますと、こちらにつきましては同じアプリの中でDNSブロックによる広告フィルタという機能がありまして、こちらの機能を使ったブロックを行っています。こちらは先ほど申し上げたような、このサイトのこの部分を消すといったような細かい指定をするようなことが原理的にできない仕組みとなっておりまして、広告を表示するための通信を妨害して、阻害して、広告の表示をブロックするといったような仕組みとなっております。この場合ですと、なかなかきめ細かいブロックが難しいといったような課題がありますけれども、かなりの広告は消すことができる。ただし、アプリによっては消すことが難しいといったようなケースもございまして、なかなか一様にはいかないといったところがございます。

Androidに関しましては、今、iOSのiPhoneのほうで御説明した後者のほう、DNSを使ったブロックと似たような仕組みでAndroidのほうは弊社の場合ですと機能を実現しているというような形になっておりまして、メリット、デメリットに関しても、先ほど申し上げたようなメリット、デメリットがAndroid側にもあるといったような形になっておりますの

で、様々なアプリの広告表示の通信をブロックして、表示されないようにするといったような仕組みとなっております。

○鳥海委員 ありがとうございます。後者のDNSブロックのほうのお話ですけれども、アプリを入れたときにDNSの設定自体を書き換えている形になるのですか。

○佐々木氏 これもまたiPhoneとAndroidでそれぞれ技術的には違った話になってくるのですけれども、おおむね本来のDNSが行う通信とは異なる通信によってブロックするといったような形になっております。

○鳥海委員 本来というのは、各アプリが行っているということなのか、例えばAndroidだったらAndroidのスマホそのものが行っているという形。

○佐々木氏 Androidを例に取りますと、Androidの本来のDNSサーバーではなく、弊社が用意している現サーバーで名前解決を行うようにして、ここでフィルタを行っているというような仕組みであります。

○鳥海委員 そうすると、アド以外のものもたまたま同じサーバー上で何か処理されていたりすると、それもブロックされてしまうという理解でよろしいですか。

○佐々木氏 おっしゃるとおりです。なので、先ほどきめ細かなフィルタが難しいといったような点もそこに起因しておりまして、他の機能も併せて妨害すると、例えばサービスやアプリの利用が成り立たなくなるような、通信まで妨害してしまうとサービスやアプリ自体が使えないとなっておりますので、そういったものは仮に広告に関わる場合であってもブロックができなくなるといった制約がございます。

○鳥海委員 分かりました。ありがとうございます。そうすると結構いろいろ難しいなという気はするのですけれども、その辺は技術的には解決はかなり難しいところなのでしょうか。

○佐々木氏 どのような通信が行われているのかをかなり詳細に調べながら、可能な限りの点を探っていくといったようなところが日々の活動になるかなと思っております。

○鳥海委員 通信まで確認されるということですか。

○佐々木氏 そうです。アプリやウェブサイトがどのような通信を行っているかといったようなところを確認していった、ここまでの通信に関しては広告表示に関わる通信に限られるのでブロックしても大丈夫かなとか、そういったような判断の仕方になるかなと思います。

○鳥海委員 通信そのものを見るとすると、DNSだけではなくて、本当に実際の通信まで、スマートフォンの中でどこかで横取りして見ているという感じになるということでしょうか。

○佐々木氏 今、通信の中身を見ると言ったのは、DNSもブロックすべき通信を調べるために社内でラボ環境のようなところで通信の中身を確認しているといったような形になります。通信の中身を見てブロックしているというわけではなくという意味合いです。

○鳥海委員 通信の中身を見るわけではなくて、事前に学習しておいてという。

○佐々木氏　そうです。調査段階ではそういうこともしているという意味です。

○鳥海委員　分かりました。ありがとうございます。

○橋田座長　トビラシステムズの皆様、どうもありがとうございました。

この後、関連する議論も出てこようかと思いますので、もし差し支えなければ引き続き御参加いただけますと幸いです。

では、次に参ります。消費者向けにセキュリティーソフト等を提供されているBBソフトサービス株式会社様から御発表をお願いしたいと思います。20分程度で、BBソフトサービス株式会社の池谷様、御発表をお願いいたします。

《2. ②事業者ヒアリング（BBソフトサービス株式会社）》

○池谷氏　BBソフトサービスの池谷と申します。よろしくお願いします。

資料を共有させていただきます。

私どもの会社概要及びこの後詳しく御紹介させていただきます詐欺ウォールの事業について御説明させていただきたいと思います。

まず、私は、BBソフトサービスのプロダクト本部、PR企画部、サポート企画部を兼務しておりまして、主に詐欺ウォールのプロダクトマーケティング、PR、及びカスタマーサポートの部門を見させていただいております。本日はよろしくお願いいたします。

本日は、会社の概要、インターネット詐欺の背景・実情、詐欺ウォールの御紹介、消費者支援への有効活用という形でお話を進めさせていただきたいと思います。

まず、会社概要ですが、私どもはソフトバンクグループのグループ企業でございまして、親会社はSB C&S社でございます。85名の会社規模の企業でございます。

「AIとITサービスを通じて人と社会を『みまもる』」という事業ビジョンの下、私どもはセキュリティーソフトウエアのSaaS事業とIoT事業、及び法人事業の3本柱の事業体を軸に展開をさせていただいている企業でございます。

事業ビジョンとしましては、私どものサービスで家族のライフスタイルを見守るをメッセージに、それを届けるサービスのプラットフォームとして事業を展開しております。

私どもの会社も第19期を迎えまして、2,600万サブスクリプションライセンスの実績を作っております。サブスクリプションといえば、もう今や当たり前の契約形態ですが、私どもは創業時からサブスクリプションモデルを国内に展開をしており現在も右肩上がりの成長を継続しております。

最初に、インターネット詐欺、トビラシステムズ様は電話の詐欺というメッセージでございましたけれども、私どもはネットの世界の詐欺の範疇でございまして、そちらの背景を皆さんも御存じのところだと思いますが、改めてお話をできればなと思っております。

こちらはIPAさんのデータとフィッシング対策協議会様のデータを活用させていただきまして、およそ10年前、皆様も御記憶にあるかなと思いますが、ウイルスマルウェアが消費者様の一番の脅威だった時代があったと思います。今、見ますと、フィッシングを主とするインターネットの詐欺が消費者様の最大の脅威に変化してきているといったところが見てとれるかなと思っています。

こちらは面白いアンケート結果があったので共有させていただきました。セコム様がアンケートを取られていて、日本人の不安に関する意識調査というアンケート結果でございます。不安に感じることはたくさん世の中にあると思うのですが、ストーカーとか、虐待とか、いじめとか、セクハラとか、そういうジャンルもちろん入ってはいるものの、1位になっているのが何とフィッシング詐欺でした。消費者様の意識も大分変わられてきたなといったところでございます。

こちらは大分ニュースに取り上げられていましたので皆さんも御存じかもしれませんが、2023年度のクレジットカードの不正利用、その中の番号を盗用された被害の額だけを抽出した数字になりますが、504億円という結果で過去最悪となり、年々過去最悪経過を更新しているという状況でございます。これも主たる理由はやはりフィッシング詐欺かなとも見てとれます。

次からは、私どもがオリジナルで取ったデータのアウトプットになります。大手ブランドを語るフィッシングサイトランキングというものを、この後も御紹介しますインターネット詐欺レポートという形で、毎月のネット詐欺サイト出現傾向や対策を発信しており、その中でこのようなランキングを作っています。これは大手ブランドを語るフィッシングがどれぐらい出たかというものをブランドごとにランキングしたデータになっておりまして、2022年を見ますと三菱UFJニコス様、三井住友銀行様、国税庁様をかたるフィッシングサイトが上位に来ておりまして、昨年2023年におきましてはイオン銀行様、私どものグループのソフトバンクが第2位、三井住友カード様、アマゾン様というようなランキング順位となりました。年毎に傾向は変わりますが、2023年は特徴的な点は、短期集中的に狙われるようなフィッシングが横行してしまっていて、イオン銀行様は特に6月、7月ぐらいに集中的にフィッシングがばらまかれたというようなことが起きたことが影響し、年間を通じ第1位になったといった結果です。本原因は読み切れませんが、犯罪者側の心理や時事背景といったものを分析し傾向を認識することが大事なかなと思っています。

また別のオリジナルデータとしまして、ネット詐欺と言ってもいろいろなカテゴリー、ジャンルがございますので、カテゴリーごとにどのぐらい手口、被害があったのかというところを集計しておりますが、昨年は偽販売、違法販売というジャンルの詐欺サイトが6割を超えるような割合でございまして、次いでフィッシングという結果です。上位の2つが毎度多いカテゴリーとなり、また、偽ソフトウェアと真ん中ぐらいにあります、いわゆるサポート詐欺とも言われていて、パソコンが危険に侵されているようなアラートを出して、そこから恐怖をあおり、詐欺サイトへ誘導するようなやり口です。これは昨年も結構多い

傾向でしたので、ポイントも上がってきているといったような結果でございました。

ネット詐欺とひとえに言ってもいろいろなカテゴリーがございまして、この後、詳細は御説明させていただきますけれども、皆様がよくお耳にされるようなもの以外にもございます。私どもは10個のカテゴリーに分類いたしまして、それを消費者様にわかりやすい情報としてお届けすべく、集計分析をさせていただいています。

最後にアンケートの結果、これは私どもが外部機関に依頼をして取ったアンケート結果になりますが、お伝えしたいのは左側のネット詐欺に遭遇したことがある、51%です。2人に1人の方が被害に遭ったもしくは身近に感じた・遭遇したといった結果になりますので、こういったデータからもすごく身近な脅威であると見てとれます。

これを踏まえまして、私どもが開発、販売をしています詐欺ウォールという商品を具体的に御紹介をさせていただきたいと思っています。

詐欺ウォールという商品は、日本国内に特化しています。日本国内のネット詐欺サイトを自動検知して、自動警告（アラート）をするネット詐欺専用のセキュリティーソフトウェアです。

詐欺ウォール事業は、2006年から本格的に強化をさせていただきまして、最初は私どものグループのヤフージャパン様と組ませていただいて、当時、ヤフープレミアムというような会員サービスがあったかと思いますが、その中に無償で御提供するような形のビジネスモデルでスタートいたしまして、その後、ソフトバンクのスマホ向けにセキュリティーオプションとして御採用いただき、そこから多くのお客様に御利用いただきだしたというような背景でございます。

2013年には警察庁様と連携協定を結ばさせていただきました。これは私どもだけではなくて、セキュリティーベンダー各社が、警察庁様で集約した危険サイトのURLをセキュリティー製品に反映していきましょうという取組でございまして、その中の一社として私どもも参画させていただきました。

2014年に詐欺レポート、毎月情報を発信するような取組を開始させていただきました。

2018年には、この後も御紹介しますが、検知するエンジンにAIの機能を搭載いたしまして、より効率的に検知をするような仕組みということでパワーアップさせていただきました。

最近では、2022年には無償のウェブサービスとして簡易的にURLの危険度を判定するようなサービスを展開また、直近ではソフトバンクのスマホ向けのセキュリティーオプションもリニューアルされまして、その中に詐欺ウォールのエンジンを採用いただいたと、そのような形で事業を拡大させていただいております。

これは今、御紹介した警察庁様との取組のお話ですが、写真は前代表ですが、もともとは2013年に大阪府警様が始められたものに賛同し、同年の12月に警察庁様のほうが主幹になりまして、各ベンダーに供給をするような取組という流れで、小さいですが大手セキュリティーベンダーさんのロゴも見られると思いますが、セキュリティーベンダーと一緒に

このような協定を締結し、協働で世の中の詐欺をなくしていきましょうというような大きなネットワークで対策を施していったというような取組でございます。

詐欺ウォールは、冒頭申し上げましたとおりWindows、Android、iOS、Macという端末からインターネットサイトを閲覧する際、危険な要素が少しでもあれば、真ん中にあるような警告画面を表示して、注意喚起、警告をするというようなソリューションでございます。機能的には非常にシンプルですが、こちらはサイト自体を遮断するのではなく、あくまでも警告をするだけでございます。その後はお客様、消費者の判断となりますが、基本的には対象サイトは閉じていただくことを推奨しております。

裏側ではどのようにサイトをチェックしているのかを説明する図ですが、最初はスミッシングやフィッシングメールを入り口として、そのメールに記載してあるURLをタップするような動きをすると思います。向かって右のように公式のサイトに飛べばもちろん問題ないのですが、偽サイトである可能性もございますので、そのサイトを検知するために、ブラックリスト、AI、ヒューリスティックという3つの検知エンジンを瞬時に動かしまして、そのサイトをチェック、判断しているというような挙動になっています。

実際、当然ソフトウェアやアプリケーションですので、全くパフォーマンスに影響がないわけではありませんが、0.5秒以下ぐらいの体感的にはあまり感じられないぐらいのスピード感で判定をするような技術を搭載しております。この辺が非常に製品の強みと思っています。この3つのエンジンで一つでも危険な要素があれば、警告画面を表示するというような仕組みでございます。

冒頭、10個のカテゴリーを定めているというお話をさせていただきました。その内訳となります。上の3つは危険性の高いサイト、アダルトサイト、違法アップロードサイトですが、このサイト閲覧や利用は違法行為のおそれがあるサイトになります。ですので、我々の考え方としては、当然、個人情報や金銭を搾取される可能性ももちろんありますが、利用者、消費者様側が犯罪に加担する可能性も秘められているようなサイトと考えております。向かって右側にあるように、詐欺サイトというよりは危険なサイトですというメッセージを警告画面として表示しております。

下の7つはメジャーな詐欺サイトでございますが、一方的に第三者からだまされるというような詐欺サイトとなり、向かって右下ですが、詐欺の疑いがありますといったようなメッセージを警告画面で表しております。

3つのAI、ブラックリスト、ヒューリスティック検知エンジンで、AIのところは機械学習を活用し、効率的に検知するために、その過程の一部の特許取得しておりますので、こちらを今後もさらなる強化していこうと取り組んでおります。

詐欺サイトを判定する機能という意味では、競合他社様も機能としては搭載しております。ではなぜ詐欺ウォールなのかといったところを表したものが、検知テストの結果となります。このテスト手法は、警察庁様から競合他社各社様に展開しているリストの中から100URLをランダムに抽出し、それを各社製品で閲覧したときに検知するかどうかを集計し

た結果になります。詐欺ウォールは94.4%となり、これは2023年4月から翌年3月までの1年間の平均結果になりますが、非常に高い数値を出すことができています。競合他社様をみますと平均で37%程です。この差が私どもの検知エンジンの精度の高さであり、一番強みと考えています。

第三者評価という意味では、特許庁様や、全国PTA協議会様からお墨付きをいただいております。全国PTA協議会様では青少年のスマホ利用はどんどん若年化していますので、青少年向けの対策も必要です。ですから、こういう製品をフィルタリングと併せて御採用いただくのも有効ではないかというプレゼンをさせていただきまして、推薦をいただいたという背景です。

あと、お客様のカスタマーレビュー、私はカスタマーサポートの部門も見ておりますが、お客様からもこういう警告画面が出て助かったというようなレビューをたくさんいただいております。

公的団体も警察庁様ほかブラックリスト共有などの連携関係もございますので、信頼をいただいているかなと思っています。

右下の私どもの製品に賛同いただいた多くの販売パートナー様がいらっしゃいます。販売チャンネルに関しましては、我々自社ECサイトがもちろんございますが、その他にもアマゾン様や、ソフトバンクの通信キャリア、ソフトバンクキャリア以外の通信キャリアである全国のインターネットサービスプロバイダー（ISP）様、電力系ISP様、あとは地域のケーブルテレビ局様でのネットサービスのCATVプロバイダー様にも多くこの製品を販売いただいております。

あと、パソコンメーカー様です。大手の国産PCベンダー様の中には、パソコンの初期段階にこの製品をプリインストールしていただいて、購入後すでにこの製品が搭載されているというような取組、また家電量販店様も、パッケージ商品を陳列販売していただいておりますと、全国多くの販売チャンネルにて取り扱っていただいております。

私どものグループのソフトバンクの方では、セキュリティパックプラスというオプションと、直近、リニューアルリリースされたセキュリティOneというスマホ向けのセキュリティーオプションに危険サイトチェックという機能があり、これを動かしている裏側は詐欺ウォールのエンジンが動いております。多くのソフトバンクの回線・スマホ利用者様に詐欺ウォールを御利用いただいている実績がございます。

これも当然だろうと思われるかもしれませんが、お客様、利用者様からすると、国内のサポート、日本人のサポートというのは非常に安心されますので、国内に拠点を置きまして、電話やメールを中心としたサポートで安心・安全をお届けしております。

こちらまでが商品の御紹介でございまして、ここからは本日の本題に入らせていただきます。

私どもが考えます消費者様側にアプローチしたいメッセージを3点挙げさせていただきました。まずは今日お話しさせていただいたようなネット犯罪の基本的な知識と、最近の

流行といったものの情報は、面白い話ではありませんが知識として持っていただきたいです。

2点目は、先ほどトビラシステムズ様の御指摘もありましたけれども、ネットの世界も同じく自分自身は大丈夫だという根拠のない自信を持っていらっしゃる方がたくさんいらっしゃいます。ですが、非常に巧妙になっている点は、リテラシーが高い方でも、お若い方でも被害を受ける可能性は十分あるということを理解していただくというのはやはり重要かなと思っています。

未然防止の意識です。対策はいろいろございますがまずは事前知識付けが重要ですので是非私どもの取組としましては、冒頭申し上げましたインターネット詐欺リポートのような情報を多く発信していきたいと思っています。過去こういうことが起きて、今後どういうところに気をつければよいかというような情報のつくりになっておりますので、こういったものを是非読んで意識を高めていただく目的として配信をさせていただいています。

あとはネット詐欺講座という形で、消費者様と面と向かって脅威を知っていただく機会をいろいろなパートナー様と組ませていただきながら、企画し、運営しています。私どもはソフトバンクのグループでございますので、ソフトバンク側のCSR活動に参加する機会もございます。

どうやったら自分事として感じていただけるか、その一つの施策としまして、ネット詐欺被害を疑似体験をしてもらおうと考えました。実際に被害に遭ってしまったら問題ですので、実際に疑似の世界で体験をもらおうというような思いがありまして作ったコンテンツがこちらでございます。これは偽販売サイトをお題にしました疑似体験ができるような動画コンテンツとなり、動画を動かしていくと、メールが来てURLをタップした、安いと思って買物をしてみたというふうに順繰りポイントポイント进行操作していただきながら物語は進んでいきます。結果的に物が届かないとか、違うものが来たとか、そんな被害になるというようなところが体感できるものになっています。

より身近に自分事として考えていただくために、自分の中のイメージと抱き合わせていただくために、こういったコンテンツを作りながら一緒に見ていただく、その取組は非常に効果的に反応いただいておりますので、実はこれの第2弾、第3弾を今、準備していたりもしますので、こういったものを拡大展開していきたいなと思っています。

あと、これも先ほど少しお話ししましたが、無料のウェブサービスで詐欺サイトチェッカーというものを公開しています。この入力窓にちょっと怪しいなと思ったURLをコピー・アンド・ペーストしていただいて、チェックを押していただくと、さっきの3つの検知エンジンの一つのブラックリストエンジンで、チェックいたしまして、既知の詐欺サイトかどうかを判定します。もしそこにヒットすれば危険ですよというような結果をその画面上に返すというものになっております。簡易チェックですので、100%チェックできるかというものではありませんが、意識する癖をつけていただくために怪しい疑いチェックしてください。これは有効対策として無料のものでありますのでどんどん使っていただきたいなと思って

います。

そのような取組を中心にやらせていただいておりますが、我々なりにもいろいろな課題があって、思いどおりにいかないケースもよくございます。ソフトウェアやアプリケーションは、買ったら有効になっていると勘違いしてしまっている消費者も結構多く当たり前ですがセットアップしなければ有効になりませんので、各セキュリティーベンダー様も共通の課題であるかなとも思います。より簡単にセットアップするための努力、これは私どもも課題として認識しておりますし、昔は倍ぐらいあったセットアップ手順も半分に削減させてまいりました。カスタマーサポートの問合せの第1位は初期設定、設定方法ですので、こういったものをより簡易にしていけるというのは、やはり自助努力をしていかなければいけないかなと思っています。

販売方法にもよりますが、買ったものの初期設定していないが故に商品が有効に働いていない状況を打開するために利用率を促進するという動きも、長らく私どもが取り組んでいる課題です。そこで利用促進のため、お客様へのアプローチとしてソフトウェアからプッシュ通知ができる機能がございまして、今、有効になっていませんよとか、詐欺情報を送ってあげるとか、今、警告がどのくらい出ているのですよみたいな情報を配信しております。ただそれに反し、サポートに入ってくるのは警告画面が煩わしいと、邪魔だと、消してくれと、そのような問合せも結構多くて、そこはお客様とのコミュニケーションと、私どもが歯がゆいところですが、より親身に考えていただけるように、お客様に寄り添った配信を考えなければいけないというのは日々取り組んでいるところでございます。

こちらが最後のスライドになりますが、冒頭にありましてとおり、消費者様が自分事として脅威に思ってくださいとあったところですが、冒頭のアンケートにもございましたけれども、脅威と思っていながらも何もしていないというお客様が多くいらっしゃって、どうやったら意識をしていただけるのだろうというのがすごく難しい課題でもございまして、詐欺ウォールという事業において、ブランドコンセプトも含めどのようにお客様にメッセージを与えていくべきかどうか、そんなことを思いながらブランドコンセプトの再構築も考えています。やはりメッセージの仕方によってはしっかり感じ取っていただけると私は信じておりますので、その努力を惜しまずこの辺りも展開強化していきたいなと思っております。

私どもからのプレゼンテーションは以上となります。

○橋田座長 ありがとうございます。

ただいまの池谷様からの御発表内容を踏まえまして、質疑応答、意見交換をしたいと思います。御発言のある方は挙手またはチャットでお知らせください。

では、原田委員、お願いします。

○原田委員 お願いします。非常に興味深かったので、図々しくて失礼します。

セキュリティーソフトを入れると、私は消費者相談なので、商売上、詐欺サイトを毎日のように見るのですけれども、このサイトは詐欺の可能性がありそうですよと言ってくれるの

は10回に1回ぐらいで、大体素通りして詐欺サイトに行けてしまうという悲しさがあるので、御社のサービスだったら9割方弾いてくれるのだらうなと思うと、それはそれで商売的には不便かもしれないのですけれども、消費者的にはいいのかなと思いました。

特に問題に多いのが、おっしゃっていただいたサポート詐欺というやつです。あなたのパソコンがとかと言って電話をかけさせるという手口で、最初からポップアップ広告であなただのパソコンは脅威に侵されていますよというような、あれ自体を防ぐということですか。それとも、それに警告を出すということでしょうか。

○池谷氏 それ自体は侵入を防ぐものではありませんで、ユーザー様から危険なサイトに飛ぶときにチェックするだけのものですので、それ自体はそういうことはできないです。

○原田委員 そうなのですね。電話をかけさせてしまうではないですか。そうすると、電話をかけてしまったらもうあまり機能しないということですか。

○池谷氏 もちろんです。もうそっちからはリアルの世界になります。ただ、その先に、またここに何かを振り込んでくださいというような偽サイトのURLをメールか何かで御案内するケースもございますので、その際はまた働くかと思います。

○原田委員 広告が出てしまって、大体最近では電話をかけてしまって、電話口のほうで誘導されてしまうと。そのときに、使ってしまうツールがさっきみたいに普通の電話とか、あとは遠隔操作アプリとか見守りアプリみたいな、アプリ自体に問題があるわけではなくて、それを使って遠隔操作されてしまうとか、サポート詐欺もそうですけれども、勝手に第三者が取り除きましたから5万円の電子マネーを買ってこいとかというふうに言われるのですけれども、遠隔操作アプリとか、普通にストアにはあるのだけれども、使い方によっては怪しく使われてしまうとか、そのようなことに対してのサポートとか警告とかというようなことはできるのでしょうか。

○池谷氏 あくまでも今申し上げたとおりで、シンプルに危険なサイトへ行ったときに、その危険なサイトが本当に危険かどうかを判断するのみになりますので、その過程においてはいろいろあると思うのですけれども、そこまで防ぐものではないです。

○原田委員 あくまでリンク先というか飛んだ先が詐欺サイトもしくは何か情報を抜き取ろうとしているサイトかどうかを判断するというような感じなのですね。ありがとうございます。特にフィッシングとかメールもそうなののですけれども、昔はそんなにしょっちゅう来るものではなかったのですが、結局普通に被害者が多いということは、それだけみんな受け取ったことがあるということになると、メールアドレスとかショートメッセージの番号とかこういうものが闇に流通といいますか、そういうような形で流通してしまっているのでしょうか。メールの部分については何をもって判断しているのでしょうか。フィッシングのメールとかも判断するのですか。

○池谷氏 フィッシングメールですとかスミッシングメールを判定するものではございません。

○原田委員 リンク先が怪しいか。

○池谷氏 そこにURLが記載されていますので、そこを押してしまった後です。

○原田委員 そうするとメールそのものは入ってしまうのですが、要はあくまでリンク先が怪しいかどうかというところで判断していただくことによって、また詐欺が防げるというような。

○池谷氏 おっしゃるとおりです。

○原田委員 ありがとうございます。ちゃんと機能が分かれるわけですね。

○橋田座長 では、森座長代理、お願いいたします。

○森座長代理 御説明ありがとうございました。

大変いいサービスを展開されていると思います。原田さんのお尋ねと重複するのですが、要はランディングページの危険性を判断されるサービス、ランディングページの危険性について警告をされるサービスだと理解したのですが、そうしますと例えばフィッシングだったらメールで来るのかなと思っていますし、サポート詐欺、あとポップアップの広告みたいなものと理解しているのですが、御社のサービスの及ばないところで、窃取の不安、電話をかけられてしまったらしようがないという話でしたけれども、このところをもうちょっとこうすればそうはならないのにと。もちろんランディングページ側での危険判断というのはすごくすばらしい効果を発揮していると思うのですが、手前でやられてしまうと悔しいことに手が出せないということになるわけですので、ここをもうちょっとこうしてくれればいいのにみたいなことがございましたら、ランディングまで行く手前でこうしてくれればいいのにという御意見がありましたらこの検討会に共有いただけると大変有り難いのですが、いかがでしょうか。よろしくお願いします。

○池谷氏 御質問ありがとうございます。消費者様がこうしたらいいのかという意味ですよ。

○森座長代理 プラットフォームでも、広告事業者でも、もちろんランディングページの開設者自体は単なる悪者なので、ここにどうにかしろと言っても駄目だと思うのですが、そこだけではないのだと思うのです。例えばメールフィルタリングみたいなことなのかもしれませんし、あるいは広告事業者なのかもしれませんし、悪い人が単独でやられている話ではないですし、もしかしたら他の介入が可能ということもあるかもしれないなと思ひまして、それでお尋ねをしているわけでございます。

○池谷氏 ありがとうございます。

先ほど大手ブランドを語るフィッシングサイトランキングということをお紹介させていただきましたけれども、やはり企業様側もサイトのつくりですとか、詐欺サイトに乗っ取られないような取組というのは当然ながらされていると思いますし、こういう大手のブランドさんは今、当然のようにトップ画面でフィッシング詐欺に注意してくださいという案内を掲載されていますので、そういう取組は継続的に啓発されるべきかと思います。ですので、何か特別な対策があるかということ、なかなか今はいちごこの状況で難しいとは思いますが、ユーザーコミュニケーション、パートナー様も自社の抱える会員様

に注意を呼びかけていただく、事前の意識と対策みたいなものをしっかりつけていただく、これに尽きるかなというふうには思っています。

私どもも詐欺ウォールという最終手段のアラートですけれども、それを使わずともまずはURLを怪しんでくださいとか、その先に行かないでくださいとか、行くときは公式のアプリからとか、公式のページからブックマークにしておいてそこから入ってくださいとかそういうことを一生懸命呼びかけておりますので、そういうお客様とのコミュニケーションを密にして意識を高めていただく、そういったことが一番重要かなと考えています。

すみません、お答えになっているかどうか心配ですが、いかがでしょうか。

○森座長代理 分かりました。ありがとうございました。フィッシング詐欺の場合は、成り済まされた側からの周知啓発みたいなことで、御案内のとおりだと思うのですが、スマホのMN0を含めたアクセスプロバイダーもかなりいろいろ対策を検討されていて、フィッシング詐欺の対策検討会みたいなことをされていて、報告のほうはどうなっているかというのは分からないのですが、そういったこともあるのかなと思ひましてお尋ねをした次第ですが、何となく分かりました。ありがとうございました。

○池谷氏 ありがとうございます。

○橋田座長 ありがとうございます。

他の方いかがでしょうか。

では、山口委員。

○山口委員 貴重なお話ありがとうございました。

私のほうからは技術的な質問というよりは、少し漠然とした質問になってしまうかもしれませんが、御社のケースであれ、トビラシステムズさんのケースであれ、恐らくビジネスの根幹になっているのは、いかにデータを収集して、それを学習して、適用するかというプロセスそのものにビジネス的な価値があると認識した上での御質問になるのですが、例えば御社の場合であれ、トビラシステムズ様の場合であれ、警察庁様からのデータが共有されていて、それを基に御自身たちでもデータを集めて学習をすることによって精度が上がっているというところがあると思うのです。そうすると、消費者保護の観点から見たときに、例えば関係企業団体のようなものを作って、同じように巨大なDBを構築しようと。消費者保護のためにそういったDBを構築しようという動きが将来的にないわけではないと思うのですが、まずそもそも業界としてそういう動きがあるのかないのかが質問の1点目になります。

もう一つとしては、もしそういう動きがあるとする、恐らく今申し上げたように企業様が今までの自分たちの努力である意味培ってきたデータであったりだとか資産であるものをある意味、公的に提供することになった場合に、ある程度今までの利益担保であったりだとか、DB共有を促されるような企業様が、それだったら参画してもいいかなと思う仕組みがある程度ないと、みんなでDBを集めましょう、役に立つからこれを公開しましょうと言ってもなかなか世の中としては動かないだろうなと思っております。なので、企業様

の観点から見たときに、こういった企業支援とか企業保護の形があると、消費者のために世の中で大きなDBを構築して、それをオープン化していこうという動きになる可能性があるかを、あくまで御社の御意見で構いませんのでお聞かせいただければと思います。

○池谷氏 ありがとうございます。

1番目の団体ネットワークの御質問ですけれども、具体的にはそういうものがあるということではございませんで、あくまでも私どもは営利企業として、一つの事業として展開をさせていただいているのがまず実態でございます。ただ、世の中のために私どももネット詐欺ゼロ社会へというようなメッセージをビジョンに掲げているところもございますので、被害がなくなることが一番の目的だと思っています。

警察庁様とお話ししたときにもあったのですけれども、一企業がどれだけ努力してもできることは限られているのだと。警察庁様もそうだし、その啓発ネットワークを広げていくことが世の中から撲滅していくために一番大事なのだというお話をさせていただきまして、そういう取組になるべきだと私どもも考えています。

唯一近いところで申し上げますと、2つ目の御質問の延長なのですけれども、ブラックリストに御理解いただいてありがとうございます。私どもが警察庁さんから頂いたものもあれば、私どもが自社ネットワークで収集しているものもたくさんございまして、それがビッグデータとしてデータベース化されています。このリストを使って実現させている我々のブラックリストエンジンと呼んでいるもの、これを他の企業様でも御活用いただけないかということで、それを違う業態の皆様にも使っていただけるような施策、共創の御提案みたいなものは取り組んでいるところでございます。ですので、例えばあるEC事業者様、クレジットカード業界様、そういったところが自社のお客様にサービスを提供する際に、危険なサイトをチェックするためのサービスを付加価値として提供されるような、取組が少しずつできていけばいいかなと思っていろいろな業界様とお話をさせていただいているという実態はございます。

○山口委員 ありがとうございます。

○橋田座長 池谷様、ありがとうございました。

この後、関連する議論も出てこようかと思しますので、差し支えなければ引き続き御参加いただけますと幸いです。

では、次に消費者向けにプライバシー保護アプリ等を提供されている株式会社DataSignさんから御発表をお願いいたしたいと思います。では、太田様、20分程度で御発表をお願いします。

《2. ③事業者ヒアリング（株式会社DataSign）》

○太田氏 ありがとうございます。

株式会社DataSignの太田から御紹介をさせていただければと思います。

今日はBunsinというアプリの御紹介でございます。

まず自己紹介としまして、DataSignという会社で代表をさせていただいております、あとは個人のエンパワーメントをテーマに掲げておりますMyDataJapanの常務理事もさせていただいております、先ほど広告ブロックの話もありましたけれども、DataSignはもともとブロックされる広告側の事業をやっておりまして、そこに広告用のデータを消費者に無断で集めて販売するということをやっております、今は改心しまして、データ活用の透明性確保と個人を中心とした公正なデータ活用を実現するためにDataSignを作っております。

DataSignのミッションですけれども、「だれもが公正に安心してパーソナルデータを活用できる世界を実現する」ということで、この「だれもが」というのは生活者も含まれておりますし、企業も含まれている。企業も生活者も現在なかなかパーソナルデータをうまく活用できるという状況、特に日本においてはそういう状況なのかなというところで、ちゃんと公正にそういったデータが使われるようなものを目指しております。

DataSignでやっていることなのですけれども、プロダクトとして企業向けのwebtruというものと個人向けのBunsinというものもやっておりまして、あとはR&Dで分散型のアイデンティティーとかいろいろなことをやっております。BunsinもR&Dの一環みたいな感じでやっているのですけれども、今日はBunsinのほうをメインで御紹介したいと思います。webtruはちょっとだけ説明をします。

まずはwebtruのほうなのですけれども、同意管理ツールと売り出しております。これは最近Cookieの同意しますかみたいなものでちょっとうざいポップアップが出てくると思うのですけれども、それに類するものでございます。我々のwebtruはあまりうざくないような形でそれを実現しようと思って頑張っております、いろいろな企業さんに、消費者から同意を得たりとか、同意を得るではなくてオプトアウトしたりだとか、パーソナルデータの利用について通知とか公表を行うためのものを生成するツールとして御活用いただいております、ちょうど先ほど詐欺ウォールさんのウェブサイトを見たらwebtruが導入されております、ありがとうございます。

どういふものかといいますと、導入しているウェブサイトによって見え方は違うのですけれども、例えばDataSignのサイトでも自社の製品をもちろん導入しております、あなたのプライバシーというような形で、ウェブサイトを訪れると、あなたのプライバシーが設定できそうなボタンが左下に出てくるようになっております。訪れた消費者が、これが出てきてちょっと押すとプライバシー設定と出てきまして、最初、1段階目、2段階目、3段階目なのですけれども、まずは一番左の画面が出てきて、大まかなカテゴリー、広告利用とかアクセス解析利用、パーソナライズ利用でパーソナルデータを収集していますよと。嫌な人はこのチェックボックスを外して設定を保存すれば、そういったデータ収集が行わ

れなくなりますよという機能を提供しております。

ドリルダウンができて、アクセス解析のところを見ると、例えばアクセス解析にはGoogleアナリティクスを使っていますよというのが分かって、それをまたクリックをしますと、GoogleアナリティクスというのはGoogleが提供していて、どういう情報を送信していて、何に使っているかというのが見られるようなものを提供しております。こういう機能をウェブサイト運営している企業が自社で一つ一つ作るというのは結構大変なので、我々のwebtruでは、ウェブサイトwebtruを導入いただければこういったものが自動で生成されて、消費者に対してこういった通知であったり、オプトアウトの機会であったり、同意であったり、そういったものを提供できるというものになります。

webtruの説明としては以上になります。

Bunsinの説明になるのですが、Bunsinというのは、あなたの「身代わり」アプリと書いてありますが、現在、メールアドレスをいっぱい作って、例えばアマゾンに登録するときはアマゾン用のメールアドレスを生成してそれを登録しようとか、ビックカメラオンラインのときはこのメールアドレスを生成して登録しようとか、そういうことができるものです。どういうふうにするかをお見せしたほうが早いので、今、DataSignのお問合せフォームが映っていると思うのですが、例えばこういうお問合せをするときとか会員登録をするときとかにメールアドレスを入れてくださいと言われることが多いと思うのですが、自分の本当のメールアドレスを教えるのは嫌だなと思ったときに、Bunsinはアプリだけではなくて、Googleエクステンション、Chromeのエクステンション、Edgeのエクステンションで提供しております。ここでBunsin生成というボタンを押して、例えばDataSignに提供するのであればDataSignにして、転送先を自分のメールアドレスにして作成するとメールアドレスが発行されますので、これをコピーして貼り付けると、これがDataSignに提供したメールアドレスということで、こちらに残ってくるということです。

これはDataSignにしか提供しないメールアドレスとして、こうやってデータベースに残っていきます。この問合せフォームはメールアドレスだけ入れればいいので、これで問合せをすると、ここに送られてきたメールが自分の先ほどの本当のメールアドレスに転送されてきて、その転送されてきたメールに返信をすると、ちゃんと送信元はもともと提供したメールアドレスになるということで、自分の本当のメールアドレスを隠しながらメールのやり取りができるというようなものを提供しております。

このように自分の本当のメールアドレスではなくて、ダミーのメールアドレスを作って提供することで、転送して自分のメールアドレスを隠しながら相手とやり取りができる。先ほどの例では、DataSignに提供したメールアドレスはDataSignにしか提供していないので、例えば先ほどのDataSignに提供したメールアドレスに対して、DataSignに登録したはずなのに何かよく分からない詐欺サイトっぽいところからメールが来たなというのが分かるようになります。そうするとDataSignが漏えいしたのか、第三者提供したのかということが消費者側で検知することができるようになるという考え方のものがございます。

現在はメールアドレスだけなのですけれども、今後、電話番号とかクレジットカード番号とか住所とか、CookieはもうサードパーティCookieはなくなって必要ないのですけれども、そういったものに対してもメールと同様、提供先ごとにダミーのものを生成して、転送して、本当の情報は隠すことができるというものを提供していきたいと考えております。

電話番号は難しそうという話は後ですのですけれども、クレジットカードは一部このようなバーチャルクレジットカードを提供しているようなサービスがあったりしますので、実現は可能なのですけれども、まだ僕らのほうでは提供できておりません。電話番号はちょっと難しくて、住所もここに書いてあるとおりの私書箱みたいにしておいて、そこを誰かが転送するというものなのですけれども、こちらも転送サービスというよりは、メルカリのメルカリ便みたいに形で送付先を隠して送ることができる。そういうものをサードパーティとして提供できないかということを考えております。

また、最近こういったメールアドレスとかクレジットカードとか電話番号というのはダークウェブに流れることが結構多くて、提供したメールアドレスとかクレジットカード番号、電話番号とかがダークウェブに流れていないかを常に監視して、それがダークウェブに流れたら通知して無効化するというようなことも予定として考えているところでございます。

このBunsinというサービス、今はメールアドレスだけなのですけれども、今後電話番号とかクレジットカード番号にも広げていきたいなというところと、もう一つ、今後の展望としましては、Digital Identity Walletというものに進化していきたいと思っております。考え方としては、自分の最小限の情報だけ渡せばいいよと。例えばメールアドレスが必要というのも、別に本当のメールアドレスでなくてもデータのやり取りができればそれでいいよねと。それで最小限のものだけ渡せばいいという考え方のもので、先にこちらのDigital Identity Walletとはというスライドで御説明します。

例えば本人確認するときに、13歳以上の確認とか、18歳以上の確認のほうが分かりやすいと思うのでそちらから説明をすると、今、例えば18歳以上を確認するということをオンラインでやろうとすると、免許証の画像とかを撮って、マイナンバーカードの画像とかを写真で撮って、自分の顔をぐるぐるしたりとか、カードの厚さを写真に撮ったりとか、そういう面倒くさいことをして本人確認をして、そこに書いてある生年月日が18歳以上だったら18歳以上だよねということをしないと、本当に18歳以上かどうかということは確認ができないのですけれども、これをVerifiable Credentialsと呼んでいるのですけれども、暗号学的に検証可能な形で18歳以上を確認できるような仕組みが今、ヨーロッパを中心に広がってきておりまして、その仕組みを使って最小限の情報、先ほどの自分の顔写真とか住所とかも載った画像とかを渡すのではなくて、暗号学的に自分が18歳以上であることを証明できるデジタル証明書を提供して、それで18歳以上を確認していく。そういったことができるような技術を今、別のプロジェクトで作っていますので、それをBunsinの中に取り込んでいくということを考えております。ですので、ここに書いてあるように金融機関

で本人確認をするときとか、18歳以上を確認するとき、SNSで最近ですとLINEさんとかは18歳以上が確認できないと使えない機能があったりして、キャリアの18歳以上確認機能とかを使っておりますけれども、それをもうちょっと分散型で、本人が自分の意思で証明書を中央に知られることなく提供していく、証明していくということができるよう技術を取り込んでいきたいなと考えております。

Bunsinは、そのデータを提供するときに、例えば18歳以上の証明書と共にメールアドレスとかも提供するのだけれども、そういうときはBunsinの機能を使って、その提供先に固有のメールアドレスを発行して会員登録をしていく。そうすると、自分の本当のメールアドレスも自分の本人確認情報も他の情報も渡すことなくサービスの利用ができて、かつ、企業側も余分な個人情報を持つことなくサービスの提供もできるし、利用する人が適切な利用者なのかということの確認もできるということで、こういったことが実現できないかと考えております。

ここにPDSと書いておりますけれども、パーソナルデータストアというところに自分の証明書だとか、もっと言うと18歳以上とかの証明のデータが少ないものであればスマホの中にローカルに保存ができるのですけれども、例えば自分のパーソナルヘルレコードとか、自分の購買履歴とか、そういったものはデバイスの中に全部入れておくというよりは、クラウドの中に保存をして、その中から必要なデータを取り出して、必要な企業に渡していくことができるような仕組みを今、構築しているところでございます。

こういう仕組みを作ると、Bunsinのところに自分の情報がどんどん集まってくる。自分のデバイスの中であつたり、パーソナルデータストアに自分の情報がどんどんたまってきます。今までは企業が持っていたものですが、それが自分の情報として自分のパーソナルデータストアとかデバイスの中に入ってきますので、そのデータに対して脳みそを付けてあげれば、文字どおり自分の分身ができるのではないかとということでBunsinという名前をつけているのですけれども、そうすることで例えば会員登録するときにプライバシーポリシーを見るのは面倒だから読んでおいてとか、例えば購買履歴とも連動することによって、家で最近、歯磨き粉とかを買いますけれども、歯磨き粉をいついつ買っているから、そろそろなくなるから勝手に代理で買っておいたよとか、そういう面倒くさいことはパーソナルAIに任せて便利になることができます。そういう構想で今、Bunsinの開発をしております。

そのサービスを展開していくに当たっての課題なのではございますけれども、まずDataSignをどうやって信頼すればいいのかという問題があるかなと思っております。Bunsinもですが、今、DataSignが中央集権的にサービスを提供していて、メールの転送をしているので、メールの中身もDataSignが見ようと思えば見えてしまう。その中身に依拠して、その中身を分析して広告を出しますよとかもやろうと思えばできてしまう。要するにGoogleのGmailみたいなものです。そういうこともやろうと思えばできてしまうのですけれども、そういうことはしないよということは言っているのだけれども、生活者とかからしてみると、本

当にしないのとか、DataSignは信頼できる企業なのということをどうやって信頼すればいいのかというのが、なかなか担保が難しい。

その担保のために我々DataSignは、冒頭に説明しなかったのですが、過去に情報銀行の認定を取得しておりまして、情報銀行というものの認定を取得して信頼性を獲得すれば、中央集権的なところであっても一定の信頼は得られるかもしれないなということで取得していた経緯がありましたが、paspitというサービスだったのですが、サービスとしてもあまりうまくいかなかったもので、そこは終了しております。

中央集権的なところをどうやって信頼するかという方向性ではなくて、そもそもサービス自体を分散化して、DataSignに依存しなくても自分でサーバーを立ててもいいし、自分の信頼できる企業があるのであれば、その企業がサーバーを立ててやっているようなところを使えばいいというような感じで、分散化をするということも考えられるのですが、その場合、依存をしないということは、そこにお金を払わなくてもいいということになってしまうので、ビジネスモデルの構築が難しいですよということになってしまいます。

先ほどパーソナルAIを、あえてこっち側、分かりにくいですがこっちをデバイスとして見てみますが、デバイス側にパーソナルAIを持って、サーバー側に持たないような仕組みで考えようというのを考えているのですが、そもそも分散型AI、脳みそがそれぞれの消費者の手元にある状態というのは、サーバーに大きな集中型AIがあるよりも、明らかに性能的に劣るというところに対して、分散化というのはなかなか難しいなというところが課題として思っております。分散の部分と集中型の部分をうまく組み合わせて、プライバシーにも配慮しながらこういった機能を提供していこうというのが、ちょうど先週か今週Appleさんから発表されまして、Private Cloud Compute、PCCというものが発表されまして、正に今の最適解としてはAppleさんがそういうものを提供して利用するという形になるのかなと思っております。

もう一つの課題としては、僕らは消費者側から消費者のエンパワーメントをするであつたりとか、データ最小化をして必要なデータを取らないようにしようとか、ちゃんと自分のデータはPDSに入れられるようにしようとか、そういうことをやっているのですが、そもそもそういう権利が日本においては個人にはないというところがあるので、幾ら企業に最小限のデータだけしかあげないと言っても、いやいやもっとデータをくれないとサービス提供しないよとか、自分のデータを下さいと言っても、お金がかかるのであげませんとか、あげるのであればお金を下さいみたいなことになって、そもそもその権利が法的に担保されていないので、企業がこういう仕組みに参加してくるメリットが少ないというかな状態です。なので、こういった取組がなかなか進んでいかないなど。要するに個人側が自分のデータを管理して、必要最小限のデータを提供して、サービスの提供を受けるといようなムーブメントがそもそも起きにくいというところがあります。

最後はおまけみたいなものなのですが、Bunsinの電話番号がなぜできなくなった

かというところで、セキュリティーVSプライバシーというところは、個人のエンパワーメントというところと結構関わってくるのかなと思っておりまして、これはほんの一例ですけれども、050番号に対しての本人確認厳格化とかいろいろなことがあって、もともとBunsinの電話番号のサービスを提供しようと思って準備を進めていたのですけれども、その頃は050に対して厳格な本人確認はなかったもので、050番号、1つの番号が100円以下で発行ができたのですけれども、現在いろいろありまして1つの050番号を発表するのに400円とか500円とかかかってしまう。そうするとサービスとして成り立たなくなって、要するにBunsinの電話番号にかけるために原価として400円とか500円かかるとサービスとしては1,000円ぐらいかからないといけないみたいな形になると、そこまで払うまでではないなというところもあるので、なかなか難しいところでございます。

これは書き過ぎかもしれませんが、要するに本人確認の厳格化というところでコストが上がってしまっているというところは犯罪等の防止には必要なのですけれども、それに伴って、例えば本人確認を厳格化しよう、厳格化しようとしていくと、そもそも何かのサービスを使うときに、今まではライトに、そんなに自分の情報を提供せずに利用できていたものが提供できなくなってきたりとか、利用できなくなってきたりとか、そういったことは個人のエンパワーメントというところとぶつかる部分が出てくるのではないかなというところで、このところを課題として書かせていただきました。

私からは以上となります。ありがとうございました。

○橋田座長　ありがとうございました。

では、ただいまの太田様からの御発表を踏まえて、質疑応答、意見交換をしたいと思います。御発言のある方は挙手またはチャットでお知らせください。いかがでしょうか。

では、原田委員。

○原田委員　他の発言者の方の間に、私がまたすごく興味深かったので御質問を幾つか。

すごくど素人的な質問なので非常に申し訳ないのですけれども、教えていただければ幸いです。1つは、メールアドレスを分身化することでしたけれども、逆に言うと、悪用される可能性がないのかなということを思ってしまいまして、匿名性を高くするためにあえて悪用するというところでやったときに、本当のアドレスはDataSignさんのほうにあるわけなので、そういった情報はどういう条件の下に開示されるのかとか、悪用されないための対策がもしあれば教えていただきたい。

特に他のサービス、電話番号とかも今後は御検討されているということなので、分身するということは悪用されるというところと表裏一体な気がするので、匿名性を高くするために悪用されない仕組みを並行で考えたときに、どのようなことを御検討されているのかというのが1点。

もう一つは、非常に興味深かったのは12ページ以降の付録ではありますけれども、DIWという仕組みです。すごくとんでもないど素人的な質問で申し訳ないのですけれども、こういうものは、いわゆる自分の個人情報とかそういった情報をブロックチェーン上に置いて、

要は書換えとかが他人にできないような感じで保管して、それを他の企業さんとかでも一緒に使うというようなイメージでしょうか。教えていただければと思います。

○太田氏　ありがとうございます。

1点目の悪用を防ぐにはどうするかというところなのですが、私の認識が間違っていたらあれなのですが、悪用というのはこうやってメールアドレスとかダミーのものを使えるので、例えば消費者側が悪用をするということを止めるにはどうするかと。

○原田委員　そういうことです。

○太田氏　ありがとうございます。

今、そういう仕組み、現状はないです。なので、例えば何かに応募するときに、1つのメールアドレスにつき1回応募できますよとか、そういうのがたまにあったりしますけれども、そういうところに1人がBunsinを使ってめちゃくちゃメールアドレスを生成していっぱい応募するということはできてしまうというようなことになります。そこら辺が先ほどのセキュリティと個人の権利のところのせめぎ合いで、それは個人の権利側を強くし過ぎだろうみたいなところがあると思うのですが、今はそういうのを防ぐ仕組みはありません。

では、その仕組みをどうやって防ぐのですかというところに出てくるのが、正に2番目のDIWで、御質問としてはブロックチェーンを使って共有していくのかというところであったのですが、結論から言うと、ブロックチェーンは関係ないと言ってしまうとちょっと語弊があるかもしれないのですが、ブロックチェーンは使っても使わなくてもどっちでもいいというものになります。そこが肝なのではなく、どちらかというと証明書を発行する人が秘密鍵という暗号学的な鍵があるのですが、それで署名をするというところが大事なポイントで、この署名をしたものがちゃんと本人に渡って、本人が署名されたものを誰かに渡すことによって証明することができるというところが、DIWに関連する技術の基本的なところになっておりまして、その鍵を検証するための公開鍵、要するに本当にこの秘密鍵で署名されましたかというのを確認するために公開鍵が必要なのですが、その公開鍵をブロックチェーンで管理するのか、別のところで中央集権的に管理するのが、管理せずにWalletの中だけやるのかというのは、結構仕組みによって自由でできるというところでございます。

○原田委員　結構いろいろな使い方が考えられるということですか。

○太田氏　仕組みとしては、いろいろな仕組みを使えるものではあるのですが、先ほど申し上げたように、今は例えば先ほどの応募するとかというユースケースにおいても、1人のメールアドレスにつき1回の応募ですよというのが昔は多くて、最近は電話番号にしましょうということで、自分の本人確認にメールアドレスとか電話番号とかを使うというところがそもそも違うよねというところでDIWというのが出てきていて、電話番号とかメールアドレスとかを使わずに、自分が本人ですよということだけを暗号学的に証明をすることができるので、そうするとメールアドレスも電話番号も渡すことなく本人ですよと

ということが証明できて、何も渡さずに本人が確認できて、サービスが利用できるということで、個人側からしてみれば、最小限の情報でサービスが利用できて、このサービスを提供するほうも最小限の情報だけでちゃんと適切な人か判断ができると。

○原田委員 追加の説明でとてもよく分かりました。ありがとうございます。

○橋田座長 今の話は、本人認証と個人のプライバシーとか自由をどうやって折り合わせるかという話だと思いますけれども、1人がたくさんメールアドレスを作って、たくさん応募するとかということを防がないといけないケースがあるので、そういう場合には、ちゃんと二重に応募してきていないということを確認できるような認証を使う必要がある。その他の場合にはそうでもないというようなことが全て暗号学的な認証でもってできるようなインフラがあれば、電話でも何でもそれでいけるということ、技術的な可能性としてはそういうことなのだろうと思いますけれども、そういうインフラをどうやってみんなの合意の下で作るかというところが大変ということですね。

○太田氏 おっしゃるとおりです。

○橋田座長 では、次に森座長代理、お願いします。

○森座長代理 御説明ありがとうございました。

私はwebtruもBunsinも大変すばらしいサービスだと思って以前から使わせていただいておりますが、質問1点と意見が2つありまして、まずお尋ねしたいのは、資料の10ページに本当のデータというのがありまして、CookieIDというのが入っているので、これはどういうことなのかなと思いましたので、これを御説明いただければと思います。

それから、意見として、これは皆様に申し上げることなのですが、最後のところにありましたデータ提供の最小限、3番のデータミニマイゼーションとか、あとコントローラビリティ、消費者がコントロールできる、そういうことが法制度上でできていない。これは前回御説明いただきましたマネーフォワードの瀧さんのお話の中にもありましたけれども、これが消費者に対するエンパワーを法制度的に支えるということであって、この検討会の大きなテーマであろうと思っています。これをどのように現実のものとしていくということが非常に重要なことなのではないかなと思っています。

恐らくはミニマイゼーションとコントローラビリティ、コントローラビリティは自分のデータに対するコントローラビリティですけれども、恐らくそれ以外の選択、消費者による選択みたいなことの実効化ということもこの検討会の大きなテーマで、それについては毎回話していくべきことなのかなと思っています。

意見のもう一つは、匿名性と050番号のところとか、さっきの複数のメールアドレスのところなのだと思いますけれども、電話番号の本人確認というのは、電話番号が重大犯罪に利用されるようになってきますと必要なことになってきましたので、それはどうしてもやらざるを得ないと思っています。他方で、メールアドレスをたくさん作って、何か懸賞に応募するとか、それはフリーのメールアドレスがあればみんなやりますので、それをどこまで禁止というか、どこまで制限すべきなのかというのは、比例的に考えていいと思うのです。

ただ、全体として、今、全体の傾向がどんなふうになっていっているかというのと、ある程度匿名でサービスなりプラットフォームなりを利用することは許されつつも、最終的に誰かが、ベンダーが本人確認はしっかりしているというのが全体的な傾向なのではないかなと思っています。それを典型と言っていいのかわかりませんが、電子商取引の分野で長い間課題になっていた特商法とクラウドソーシングの関係で、本当はサービス提供者なり販売者は氏名とか住所とかを表示してサービス提供する、物販をすることが特商法上求められているわけなのですけれども、それをクラウドソーシングでやるとなると、似顔絵を描いてあげますとか、翻訳をしてあげますとか、ちょっとしたサービスを提供するのに本名から何からさらしてという話なのかということは以前から問題になっておりましたけれども、その点は特商法の解釈によって、その場合は個々のベンダーが氏名と住所を出していなくても、クラウドソーシングのプラットフォームがしっかり本人確認できていればよいというようなことになったと理解していますので、誰かは分かっているけれども、そして例えば050番号が悪用された場合には警察が捜査に乗り出しますのです、そのときにはその人の真の情報を持っている誰かはいますけれども、表面には出てこないというのが今の傾向なのではないかなと思っていますので、比例的なものであるべきである。つまり、重大犯罪に利用される電話番号の本人確認はしっかり、そうでないものについては程々にいいと思いますが、全体的な傾向としては、誰かがしっかり本人確認をしていて、そのサービスの利用は匿名でできるというのが一般的な傾向なのかなと思いました。

先ほどの御質問について教えていただければと思います。よろしくお願いします。

○太田氏　ありがとうございます。

CookieIDは、歴史的にというか、最近サードパーティCookieというものが問題になって、何が問題になっているかというのと、複数の事業者が同じCookieIDを参照できてしまうということが問題視されております。これはメールアドレスとか電話番号と一緒に、最近はCookieが使えなくなるのでメールアドレスとか電話番号を企業間で共有して、ターゲティングしていこうというのが広がっておりますけれども、もともとCookieもそういう仕組みで、企業間で共有ができて、そこに対してターゲティング広告を打てるという性格のものである、それを企業ごとに別のCookieIDを発行していこうというものになります。要するにファーストパーティCookieしか使えないようなブラウザをBunsinで提供するというような計画で考えておりました。

Google Chromeでは大分遅れてはいますけれども、サードパーティCookieに関しては、Chromeも開始することを予定しておりますし、Safariではもう使えなくなっているというところもあって、そういったブラウザを提供することは今のところは考えておりませんが、もともとはそういったところも考えておまして、似たような考え方で、先ほど言い忘れたのが、サードパーティCookieが使えなくなることによって、メールアドレスとか電話番号がトラッキングの識別子として使われていくというところの対抗手段としても、Bunsin

というのは個人的には考えておりまして、個人的に電話番号での認証が増えているというのはあって、その電話番号が本当に認証だけに使われるのかと思うと、それはフェイスブックでも一部報道されていましたが、識別子として使っていたりとか、あと最近、アドテクの事業者のUnified ID 2.0では、電話番号も識別子として使おうというのが公式に仕様が出来上がったりとかしているというところもありますので、そういったものをちゃんと個人側で識別されないように、自分のデータを守るという意味でこういったBunsinみたいなサービスを使えるというふうになっていくといいなと個人的には思っているところでございます。

以上です。

○森座長代理 ありがとうございます。

CookieIDというのは、ブラウザの持っているサードパーティCookieを書き換えるみたいなことなのでしょうか。

○太田氏 書き換えるというよりは、もうそのサイトに行ったときに消去するという事です。一旦そのサイトに行っても、離れてしまったら消去してしまう。

○森座長代理 サードパーティとのやり取りでサードパーティCookieが入りますけれども、それはその後で消されてしまって、次にそのサードパーティにアクセスしたときには、サードパーティのサーバーから見れば初回アクセスのように見えるという状態にする。

○太田氏 おっしゃるとおりです。

○森座長代理 ありがとうございます。よく分かりました。

あと、太田さんのおっしゃいましたメールアドレスと電話番号の脅威というのはこの検討会でも重要なインプットだと思ってしまして、メールアドレスが漏えいして怖い、電話番号が漏えいして怖いということですが、識別子として名寄せ用にすごく使われていますので、いろいろなデータがこれに紐づいて集められるということは、この検討会としても重要なインプットとして承ろうと思います。どうもありがとうございました。

○太田氏 ありがとうございます。

○橋田座長 太田さん、ありがとうございました。貴重な御報告をいただきました。

では、その次に進みたいと思います。最後の議題ですが、消費者を支援することに活用できるデジタル技術に関する取組の募集について、意見交換をしたいと思います。

それでは、事務局より御説明をお願いします。

《2. ④消費者を支援することに活用できるデジタル技術に関する取組の募集について》

○江口企画官 資料4を御覧ください。

消費者を支援することに活用できるデジタル技術に関する取組の募集についての御提案でございます。

「1. 趣旨」として、本専門調査会におきましては、消費者契約の場面において、消費者を支援することに活用できるデジタル技術の現状と見通し、個々の消費者にパーソナライズするAIの検討及び社会実装に向けた課題等を整理し、取りまとめることを予定しております。

第2回の会合から事業者ヒアリングを行っていただいておりますが、消費者が本専門調査会の取りまとめ結果を参照することを想定しますと、できるだけ多くの情報が掲載されていることが望ましく、ヒアリングを行う事業者以外の取組についても可能なものについては併せて掲載することが望ましいと考えております。

そのため、事業者等の取組を広く募集してはいかがでしょうかという御提案でございます。

「2. 提案要領等」は、参考資料1の募集要領（案）、2の提出様式（案）でございます。

「3. の募集期間」としては、6月中を目途に開始し、9月13日を締切りとすることを考えております。

「4. 募集要領」につきましては、内閣府消費者委員会ウェブサイトに掲載することを予定しております。

「5. 今後の進め方（案）」ですが、本日の専門調査会で御提案させていただき、御承認をいただきましたら、準備が整い次第、募集を開始させていただきたいと考えております。つきましては、消費者を支援することに活用できるデジタル技術に関する取組の募集について、本専門調査会での御承認をお願いいたします。

以上です。

○橋田座長 ありがとうございます。

ただいまの御説明への御質問等がございましたらお願いいたします。御発言のある方は挙手またはチャットでお知らせください。

私、このタイトルが少しだけ気になっていて、消費者を支援するという言い方なのですが、けれども、消費者を支援する技術というのはあらゆる技術がそうなので、支援より保護のほうが伝わりやすいのではないかという気がしたのですけれども、皆さんいかがでしょうか。

森座長代理、お願いします。

○森座長代理 ありがとうございます。

どういう用語を使いましょうかというやり取りをしだすと結構ややこしいことになりますので、本当にあくまでも御参考の意見として申し上げますが、この際ですので、エンパワーというあまり耳なじみがない言葉ですけれども、そのまま使ってしまったいいのではないかという気もしております。そんな気もしなくもないように思います。

以上です。

○橋田座長 やや大胆な御意見ありがとうございました。なるほどと思いました。

他の方がいかがでしょうか。他のポイントに関する御意見でももちろん結構です。

○森座長代理 もう一つ申し上げてよろしいでしょうか。

○橋田座長 お願いします。

○森座長代理 ありがとうございます。

「消費者契約の場面において」は限定的であり過ぎると思います。今の太田さんの説明とかも正にそうだったと思うのですけれども、結局、契約ではなくて、バックグラウンド的にやられていると言うとまた怒られるのですけれども、情報収集もされて、それがひもづけられて、自由に使われていると。今度見せてくれと言ったら見せてくれないみたいなそういう話になっていますので、「消費者契約の場面において」というのは取っていただいて、消費者被害の現状を踏まえて、消費者の消費生活のデジタルの局面においてというのでしょうか、消費者がデジタル社会で生活する上で消費者を支援することに活用できるというふうにさせていただいた方が、用語は全然こだわりませんけれども、要は消費者契約に限定しないということが重要だと思います。

○橋田座長 ありがとうございます。

タイトルにエンパワーすると入れるというお話もありましたが、趣旨の1行目にエンパワーするという表現があって、2行目は支援するというふうになっているのですけれども、エンパワーの意味をもうちょっと説明したほうがいいかなという気はしますけれども、いかがでしょうか。被害という話があるので、被害を防ぐとか何とかということで分かるかもしれませんけれども。

原田委員。

○原田委員 被害も大事なのですけれども、被害とともにやはり加害者と表裏一体というのは、要は成り済まされてしまうと、自分のショートメッセージの電話番号で人に迷惑をかけるということになると、被害なのか、加害なのか、被害、加害というのが一線で引きにくいというところもあったりするので、なかなか被害とかという言葉を出してしまうとまたちょっと違うかなと個人的には思いました。

○橋田座長 森座長代理、お願いします。

○森座長代理 私も原田さんに賛成です。なりすましもそうですし、被害というよりは、それこそ選択肢を与えられていないとか、あるいは契約書、利用規約が分かりにくいとか、被害とまでは申しませんが、やはり消費者が搾取されている状況があるわけですので、ちょうど山本先生にチャットにお書きいただきましたけれども、私も原田さん同様、被害ではないかなとは思いました。

○橋田座長 被害ではなくて、何ですかね。

○森座長代理 消費者に選択を取り戻すというか、消費者の主体性を回復するというか、そういうことを含んでいると思うのです。それがパラダイムシフトだと思っていますので、そう書いていただいてもいいと思います。消費者に主体性を回復するとか、消費者の選択

を取り戻すとか、そういうふうに書いていただいてもいいと思います。

○橋田座長 ありがとうございます。確かに保護はパターンナリスティックな感じがします。

他に御意見ありますでしょうか。

どうぞ。

○荒井委員 エンパワーするというようなところで、なるほどと思ってお話を伺っていたのですが、募集要領のほうを拝見すると被害防止のような例が多く見受けられるように思いまして、これらもとても重要なと思うのですが、是非より積極的な支援のような例も入れられると、より分かりやすくなるかなと思いました。

コメントです。

○橋田座長 ありがとうございます。

タイトルと文章のほうは、エンパワーするとかもう少し積極的といいますか、パターンナリスティックではない表現を使って、でも内容は正しく伝えないといけないということと、例に関しては今、荒井委員から御指摘があったように、被害だけではなくて、もう少し積極的な例があるといいですねということです。

他は何か御意見ございますか。よろしいでしょうか。

○小林事務局長 被害だけにとどまらないエンパワーの例として例えばどのようなものがあるかという具体例があれば、聞かせていただきたい。

○橋田座長 被害ではないエンパワーとして何か思い付く方はおられますか。

お願いします。

○森座長代理 それはここまでのいろいろな御説明にもありましたように、詐欺とかそういうのは被害だと思うのですが、そうではなくて、利用規約が全体として不利なものになってしまっていてとか、分かりにくいとか、同意疲れのことなんかもそうです。読まずにクリックしているだけであることとか、あとデータの最小限性が守られていないこと、さっき太田さんの御説明にありました、いろいろな場面で、ソーシャルログインの場面でどんなデータが、例えばフェイスブックでログインするとき、ログインと書いてあるのをを使うときに、フェイスブックから、これから使おうと思っているアプリにどんなデータが行っているのか分かりません、これから使おうと思っているアプリからフェイスブックにどんなデータが来ているのか分かりませんというようなこととか、あとまさしく外部送信ですね。webtruを使えば、自分のウェブのアクセス履歴、今、私は昨日の野球の結果を見ているわけですが、この私のアクセスがどこに送信されているのかは分かりませんが、そういうことについての透明性を確保したいとか、それについて選択したいとか、そういう希望があるわけです。あるいは、自分のデータについてどんなものを持っているのか見たいとか、あるいは消してほしいとか、それは被害ではないと思うのです。正に今までお金で損をすることと健康被害が発生することだけが消費者問題だと考えてこられたわけです。すごく申し訳ないのでありますが、はっきり言って消費者委員会でもそうでした。そうではなくて、もう少しデジタルにおいて問題となっていることを何とかし

ようというのがパラダイムシフトなのだから、パラダイムシフトに従った記載ぶりにすべきということです。

○橋田座長　ありがとうございます。

先ほどの複数のIDを使い分けるとか、データミニマイゼーションというのは分かりやすいと思います。それから、消費者がいろいろなサービスに関するダッシュボードみたいなインターフェースにアクセスできて、それを自ら管理できるとか、全体を把握できるとかいうふうなことも分かりやすい例になるかなと思いました。

他は何かございますでしょうか。

お願いします。

○田中委員　被害というのももちろん問題の一つに含まれると思うのですが、予防とか未然に防ぐということもあると思うので、リスクという言葉を使ってもいいのかなと思います。消費者がデジタル環境で様々なリスクにさらされるようになってきた中で、エンパワーをして、リスクに主体的に対応するのを支援するというような印象を個人的には抱いていますので、リスクが一つの用語なのかなという印象を受けました。

以上です。

○橋田座長　ありがとうございます。

リスクと、逆に言うと機会損失みたいなこともあり得ると思うので、ちゃんとその機会を捉えられるみたいな例もあるといいのではないかと思います。

他はよろしいでしょうか。

ありがとうございます。ということで、募集することとしてよろしいでしょうか。御異論はないと思いますので、進めたいと思います。募集の準備が整いましたら、募集を開始いたします。具体的な取り扱いと応募案件の取りまとめ作業は、座長と事務局に一任いたしたいと思います。募集結果については、後日、御報告をいたします。

事務局におかれましては、募集に向けた準備をお願いいたします。

最後に、事務局から連絡をお願いします。

《3. 閉会》

○江口企画官　本日は、長時間にわたりありがとうございました。

次回の会合につきましては、確定次第、御連絡させていただきます。

以上です。

○橋田座長　では、本日はこれにて閉会とさせていただきます。

お忙しいところ、御参集いただきまして、ありがとうございました。

以 上