利用者情報に関するワーキンググループ（第16回）

令和６年11月25日

【小玉利用環境課課長補佐】　それでは、定刻となりましたので、ただいまから利用者情報に関するワーキンググループ第16回会合を開始させていただきます。

事務局を務めます総務省利用環境課の小玉と申します。本日もお忙しい中、お集まりいただきましてありがとうございます。

前回、前々回に引き続きまして、電気通信事業者における利用者情報の取扱いに関するヒアリングのため、本日はKDDIから中塚情報セキュリティ本部、セキュリティ管理部長、楽天モバイルから本田Division Managerにお越しいただいています。また、個人情報保護委員会にオブザーバーとして御参加いただいています。

山本主査は14時までの御参加となるため、それ以降の議事進行は生貝主査代理にお願いをいたします。

また、森構成員は14時半までの御参加となります。呂構成員は、少し遅れての参加となります。

それでは、これ以降の議事進行は山本主査にお願いしたいと存じます。山本主査、どうぞよろしくお願いいたします。

【山本主査】　承知いたしました。どうぞよろしくお願いいたします。

電気通信事業者における利用者情報の取扱いに関するヒアリングを実施いたします。本日はKDDI様、それから楽天モバイル様より順番に御発表いただきます。前回と同じく事業者様のプレゼンにつきましては公開、その後の質疑応答は非公開で開催させていただきます。傍聴者の皆様におかれましては、御承知おきいただければと思います。

それでは、早速ですけれども、KDDIの中塚部長から御説明をお願いいたします。御準備のほう、いかがでしょうか。

【中塚氏】　それでは、私のほうから始めさせていただきたいと思います。改めてKDDI情報セキュリティ本部で部長を務めさせていただいております、中塚と申します。このたびは、当社の取組について御紹介する貴重な機会をいただきまして、本当にありがとうございます。

昨今の情勢を踏まえると、業務委託先における事故に該当する事案が多いと認識してお

ります。当社でも電気通信事業をはじめとする様々なサービスを展開しておりますが、当該業務を行う上で業務委託は欠かせないものとなっております。本説明上では、お客様の情報を利用者情報と表現させていただいておりますが、利用者情報を守る上で業務委託先の管理監督が非常に重要と考えております。本日の説明で、業務委託先の管理監督に焦点を当て、当社の取組について御紹介させていただきたいと思いますので、よろしくお願いいたします。

こちらが本日の目次となっております。まずは、利用者情報保護の取組としまして、当社の中で大前提となってございますセキュリティポリシー、プライバシーポリシーについて説明させていただきます。当社では情報セキュリティの確保を目的とした方針として、セキュリティポリシーを定めております。利用者情報を含めたあらゆる情報に対する適切な管理を重要な経営課題として認識し、情報セキュリティ確保のための方針を定めております。

主な内容としましては、情報セキュリティ管理体制、情報セキュリティ対策の実施、社内規定の整備、教育の実施、適切な業務委託先管理の実施、法令遵守などを定めており、当該ポリシーに基づいて利用者情報を適切に取扱い、情報セキュリティの確保を推進しております。これらのポリシーに基づいた情報セキュリティ確保のために、経営層をメンバーに含む情報セキュリティ委員会をトップとして、セキュリティガバナンスの体制を構築してございます。

具体的には、本委員会でセキュリティ対策を決定した上で、各本部の代表が参加する簡易の会議体で本決定内容を指示、伝達し、情報セキュリティ強化施策として全社に展開しております。当社ではセキュリティポリシーと合わせて利用者情報の保護を目的とした方針として、KDDIプライバシーポリシーを定めております。利用者個々人に関するデータの重要性を認識しており、その利用者、利用者情報の保護の徹底を図るための方針を定めております。主な内容としましては、適切な利用者情報の取扱い、データの取得、利用目的、利用するデータ、第三者との連携、安全管理措置などを定めており、当該ポリシーに基づいて利用者情報を適切に取扱い、利用者情報の安全確保に取り組んでおります。

また、お客様より安心してお客様の情報を当社に預けていただけるよう、当社のホームページ上でプライバシーポータルというページを公表しており、当該ホームページ上でデータの利用目的や外部委託を含めたデータ連携の詳細について説明し、透明性の確保を実施しております。

先ほど御説明させていただいたポリシーに基づいて、適切に利用者情報を取り扱っているところではありますが、これらのポリシー体制に基づいて、業務委託先の管理監督を実施しております。ここからは、当社における業務委託先の管理監督に関する取組について御紹介いたします。

まずは、当社における業務委託先の管理監督の全体像について御説明いたします。当社における業務委託先の管理監督は、１つ、事前確認、２つ、契約、３つ、監査の３つで構成されております。事前確認では、業務委託先として適格性を確認し、契約においては、当社と同等のセキュリティレベルを確保し、その後の監査においては、そのセキュリティレベルが維持できていることを確認しております。なお、当社における利用者情報に関する取扱いの委託代表例としましては、サービスの利用者情報について、当社の携帯販売代理店やコールセンター等で取扱いを実施してございます。

初めに、事前確認のステップについて御説明いたします。当社の社内規定に基づき、業務委託元部門が業務委託先の適格性の事前確認を実施しています。具体的には、情報セキュリティ部門が事前に用意した所定のチェックシートに基づいて、各委託元部門が業務委託先と連携して確認し、適格性を判断しております。確認事項としましては、契約内容、教育、運用体制等となり、具体的には、利用者情報保護覚書の締結が可能かどうか。年１回以上の教育を実施しているか。セキュリティ関連規定に従った運用や自己管理体制が整備されているか。安全管理措置として、例えば入退室の管理やシステムアクセスの適切な認証を実装しているかなどを確認しております。これらの確認をもって、各委託元部門において、当該業務の委託元の的確性を評価、判断しております。

次に、契約のステップについて御説明いたします。当社では、事前確認でチェックした内容を業務委託先で実施いただけるよう、安全管理措置などの基本的事項を業務委託契約に盛り込むとともに、利用者情報の預託がある場合は個別に覚書を締結しております。これらの契約内に利用者情報の適切な取扱いに関わる情報を記載することで、業務委託先における安全管理措置などを担保しております。これらの契約に含まれる事項として、安全管理措置として、アクセス管理、持ち出し手段制限、外部不正アクセス防止、秘密保持としまして、第三者及び業務上知る必要のない従業者への開示、漏えいの禁止、再委託の条件として、当社から委託先間の契約で定める義務と同等の義務の実施や再委託時の当社に対する書面での事前承認の必須化、再委託先の監督として預託情報の安全管理に関する監督といった内容を契約に明記しております。

次に、監査のステップについて御説明いたします。当社では、業務委託先監査と称していますが、この業務委託先監査において、当社の規定に定めるセキュリティレベルが確保されていることを継続的に確認しております。具体的には、事前確認と似たような流れとなっておりますが、情報セキュリティ部門が事前に用意した所定のチェックシートに基づいて、セキュリティレベルを業務委託元部門が監査するという流れになります。この監査において、業務委託元部門における不適切事項が発見された場合は、業務委託先に対して是正を依頼しております。これらの監査において、情報セキュリティ体制や規程の遵守状況、安全管理措置の実施状況について確認しており、基本的には立入りでの監査を年に１回以上の頻度で実施しております。

最後に、業務委託先における安全管理措置として、具体的にどのような項目を定めているかについて御紹介いたします。外部からの不正アクセスや内部不正による持ち出しを防止する対策として、物理的な安全管理措置と技術的安全管理措置を定めており、物理的な安全管理措置としましては、入退室の制限、監視カメラの設置、また、それらのログの取得、預託情報の施錠管理やワイヤーロックの実施などを定めております。また、技術的な安全管理措置としましては、利用者情報を取り扱う環境のシンクライアント化や外部記憶媒体の利用制限、アクセス制限、権限制御、アクセスログ・操作ログの取得、クラウドサービス利用の制限、通信の暗号化、OSソフトウエアのアップデート、システムアクセスの認証などを定めております。

これらの項目を業務委託先の選定時に確認し、契約で担保し、監査で確認することによって、当社が業務委託先に預託する利用者情報が業務委託先においても適切に取り扱われるよう取り組んでおります。

最後に、これまで御紹介した取組をもって、業務委託先の管理監督を実施しているところではありますが、これが最終形とは認識しておらず、日々、これらの活動を把握、評価し、改善につなげることで、より適切な業務委託先の管理監督が実現できると考えております。業務委託先の管理監督に限らず、当社の情報セキュリティを継続的に改善していく体制を構築しておりますので、これらの体制の取組を通じ、引き続きお客様の情報を適切に取り扱うことができるよう邁進してまいります。

以上で発表を終わらせていただきます。どうもありがとうございました。

【山本主査】　ありがとうございました。続きまして、楽天モバイル、本田Division Managerより御説明をお願いいたします。

【本田氏】　楽天モバイルの本田です。本日は当社の業務委託先管理について御紹介させていただく機会をいただきありがとうございます。

早速ですが、始めさせていただきます。次のスライドお願いいたします。まず、楽天モバイルだけではなくて、楽天グループの情報セキュリティガバナンスに関して、説明を一番始めにさせていただきます。

次のスライドお願いします。楽天グループの中に楽天モバイルをはじめ、様々な業種、業態のグループ会社が集まって構成されておりますけれども、楽天グループ全体としての情報セキュリティレベルを担保するために、楽天グループの本社の専任部門による情報セキュリティガバナンス構造というものを構築し、運営をしている形で、グループ全体のセキュリティを担保する形になっております。グループ共通のセキュリティポリシー、それからITソリューション、従業員が使うパソコンであるとか、それから、そのパソコンの中で動く様々なセキュリティに関するソリューション、ここは各社、各事業で選定されるわけではなくて、グループ共通のインフラにのっとって選定されるという形で、技術的にも体制的にもセキュリティを担保するというコンセプトで運用をさせていただいています。

次のスライドお願いいたします。さきに説明させていただいたコンセプトにのっとって、ISMSのグループ全体で取得をするという形でコントロールをしております。楽天モバイルをはじめ、全グループ内で45社がISMSを取得し、同じセキュリティの水準にのっとった事業を運営しているという形でセキュリティを担保しております。

次のスライドをお願いいたします。セキュリティポリシーに関しましても、グループ共通のセキュリティポリシーというものを頂点として、各事業に沿った事業法、そういったもの肉付けしながら、各グループ会社の社内のポリシーに落とし込んでいくというコンセプトでポリシーを構築しております。最上位にある楽天グループの共通のセキュリティポリシーは、ISO27001といった世界共通のセキュリティ基準が盛り込まれた内容になっておりまして、対してグループ、各社の情報セキュリティポリシーというのは、各事業における事業法が反映されており、楽天モバイルでは電気通信事業法上の安全管理措置やTCAの安全管理基準、そういったものが楽天モバイルの規定の中には盛り込まれているというような形で、全体とのバランスを取っている形です。

次のスライドをお願いいたします。では、ここで楽天モバイル株式会社の情業務委託のセキュリティ管理について説明させていただきます。

次のスライドお願いいたします。こちらは概略になります。左側のほう、図の左側のほ

うが契約部門と、それから委託先の事業者、対して、点線で囲まれた中というのが管理部門による調達申請のプロセスを構築している絵となっております。具体的には、購買部門と法務部門、セキュリティ部門がそれぞれの責任を担いながら、安全な契約、委託先との契約を担っていくという形で運営をしておりまして、法務部門がまず、契約内容をレビューした後、情報セキュリティ部門によるセキュリティの審査を実施するというプロセスとなっております。

セキュリティ審査は情報セキュリティに係る業務委託先審査マニュアルというマニュアルを、これグループ共通のものがありまして、こちらに沿って実施をしていきます。審査対象となるのは、機密情報を取り扱う委託先事業者、それからクラウドサービスの場合もこのプロセスの対象になります。委託対象というのは、委託先の事業者、それからサービス単位ではなくて、あくまで契約単位で実施をして、チェックシートを取得し、業務内容をレビューしながら、データベースに対してその内容を登録をしていくという方法を取っております。ですので、同じ事業者であっても、契約が新しい契約になる、取り扱う情報が変わるとか、それから事業する場所、オペレーションする場所が変わるというような場合には、全てチェックシートを１から回すという形で情報を集めております。データベースに収容された情報に関しては、年次で定期的な棚卸しの内容でチェックをしていくというような形で、継続的な運用を担保しているという形になります。

次のスライドお願いいたします。こちらは社内向けに展開されているマニュアルの抜粋という形になりますけれども、こういったフェーズで委託管理をしていくということが社員にも示されています。必ず委託先申請プロセスマニュアルというものに沿って委託審査を行うので、導入準備のところから、それを見越した話というのを事業者と進めてくださいということと、それから委託先審査のマニュアルを参照すること、当然、審査においては日数がかかるので、それも踏まえた計画を立てること。それから委託審査終了後も、契約が終了するまでは定期的なチェックの対象になるということが明記されております。

次のスライドお願いいたします。ここで、委託先の事業者選定のポイントという形で、提示されている内容を一部抜粋して紹介させていただきますと、まず、委託先の企業の選定に関してはセキュリティの認証を取得している事業者を選定することを強く推奨をしております。それから、再委託に関して。これは必ずしも、全て禁止はしていませんが、再委託、再々委託先にも機密情報を委託される可能性があることから、必ず一次の委託先と同じセキュリティ基準を有すること、さらにこれを、再委託の有無というのは必ず委託先

に確認をして、必要な手続を取ることというのを明記させていただいています。

次のスライドお願いします。そして、通常の委託先事業だけではなくクラウドの場合、クラウドに関しては、通常の委託先に比してより技術的な観点で確認をする項目というのを定めておりまして、具体的には契約先の提供するサービスレベル、バックアップとか冗長性の定義、この辺りが当社の要求水準を満たしていること、それから、情報セキュリティ対策も同様に当社、社内のポリシーと同等の定義があること。それから、さらに情報に関しては当初の所有権を確認した上でサービス提供のために利用し、情報の機密性が維持されることということを明記、担保するように努めております。

次のスライドお願いいたします。こちらが情報セキュリティチェックシートの項目の抜粋ということになります。委託先に関しては大きく３つ、全社的な情報セキュリティ体制について、それから、作業場所、委託業務に関する情報セキュリティについて、こちらは主に物理的なセキュリティに関して聞く項目になっております。さらに、機密レベルの高い情報を取り扱う場合のセキュリティについては、２つに比して、より詳細な内容を聞いていくという形で、ここは濃淡をつける形で運用させていただいております。一方で、クラウドSARSサービスの利用者に関しては、上記委託先、作業型に比して技術的な観点で10項目の大項目でヒアリングをするという形で、チェックシートを構成させていただいています。

次のスライドをお願いいたします。一旦契約が始まりましたら、１年に一度データベースから抽出する形で事業者に対して変更がなかったか、この辺りを確認するという運用を全契約に対して徹底しています。

次のスライド、お願いいたします。委託終了時に関しては、マニュアル上にこのような記載を掲示させていただいておりまして、必ず情報の破棄と、それから破棄証明を取得すること。それから、委託先でサーバーやシステムを利用している場合には、アクセス権及びパスワードを直ちに削除､または破棄することというのを明記させていただいています。

以上が当社の委託先管理に関する運用の御説明となります。これで終わりになります。ありがとうございました。

【山本主査】　ありがとうございます。

それでは、２社のプレゼンにつきまして、質疑応答に移りたいと思います。まずは、KDDI様の御説明につきまして、質疑を行います。先ほど御案内したとおりですけれども、質疑応答は非公開で実施いたします。傍聴者の皆様におかれましては、本日の傍聴は以上と

なります。それでは、事務局におかれましては、非公開設定への切替えをお願いいたします。

【小玉利用環境課課長補佐】　了解いたしました。

お時間を取りました。大丈夫でございます。どうぞよろしくお願いします。

【山本主査】　ありがとうございます。それでは、KDDI様からの御説明につきまして、構成員の皆様から御意見、御質問をいただきたいと思います。御発言希望の方はチャットにてお知らせいただければと思います。いかがでしょうか。

それでは、呂さんお願いいたします。

【呂構成員】　弁護士の呂です。大変丁寧に御説明いただきまして、誠にありがとうございました。私からは２点御質問させていただければと思います。１点目として、今回のヒアリングの背景の一つとして、外部サービスの利用契約について、個人データの委託がないと考えてしまったことが事案の発生につながったケースがあったのですが、KDDI様におかれては、業務委託契約と外部サービスの利用の契約とで類型的に分けて、個人データの取扱いの委託の有無を振り分けるといった発想はされておらず、業務委託契約も、外部サービスの利用契約も全て、個別の事案に応じて個人データの委託の有無を判断されているという理解でよろしいでしょうか。２点目として、年１回以上立入検査を行われていることで、実際の件数も非常に多く、大変手間とコストのかかることを実施されていて素晴らしいと思いました。立入検査のときにもチェックシートを用いて検査されるということで、これは単なるインタビューをして終わりという以上に、委託先の嘘を見抜くといいますか、何か工夫などがあれば御教示いただければと思いました。

以上の２点です。

【山本主査】　ありがとうございます。それでは、KDDI様お願いいたします。

【山崎氏】　お世話になっております。KDDIの山崎と申します。御質問ありがとうございます。プライバシーを担当しております、山崎のほうから１点目の部分について回答させていただきます。

１点目は、まさに呂先生から御指摘があったとおり、類型的に明確に分けているというわけではなく、業務委託として出てきたものについて、一件一件個別の案件を精査して、契約書を確認したり、サービスの利用規約等を確認し、サービスの構成を見ながら個人データの取扱いがあるか、ないか、ある場合については、どういうセキュリティ対策の措置が講じられているのか、個人情報保護法上の委託として整理ができるような内容になって

いるのかというのを確認した上で、これが適切にできるのかどうかというのを判断して、足りない部分があれば、新たな契約を結ぶとか、別のサービスに切り替えるといったような、そういった形で運用しております。１点目の点については、以上とさせていただきます。

【中塚氏】　２点目ですけれども、チェックシートでチェック、インタビュー以上のことをやっているのかということですが、現地に行った際に、しっかり現地、現物を確認するようにしておりまして、例えばいろいろな資料ですとか、現物だったりということをしっかりと確認をして、先ほどお話ししました、言葉は悪いですけど、うそがないようにというか、しっかりと監査に行った者が監査をしてくるといったことを実施しております。

【呂構成員】　ありがとうございました。

【山本主査】　よろしいでしょうか。それでは、森さんお願いいたします。

【森構成員】　御説明ありがとうございました。私も呂先生とほぼ同じですので、重複を避けつつお尋ねするのですが、先ほどもありましたけども、年１回の立入検査ということで、しっかりやっていただいていると思います。

私がお尋ねしたいのは、委託先選定のタイミングです。このときは御説明上はチェックシートということだと思うのですけども、選定のタイミングの際にKDDIさんからお仕事をいただきたいということで、割とチェックシートにはチェックをしてしまうのだと思うのですけども、そこで何がしか出入りの業者さんがチェックをしてしまいがちであるということについて、本当にチェックされたとおりだろうかという確認ができるようになるものだろうかと、どうしてもなかなか見抜きにくいのではないかと思っていまして、それ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。

【山本主査】　ありがとうございます。それでは、KDDI様、お願いいたします。

【中塚氏】　質問ありがとうございます。業務委託先監査を対面でやることによって、事後的にうそというか、そういったところを確認することもでき、そういったことをしっかりやることで、チェックシートのほうにしっかりと過去の動静だとか、現行の状況を把握、反映させておりますので、そういったところから複合的にしっかりとチェックできるような形でやっております。

【森構成員】　ありがとうございました。

【山本主査】　ありがとうございます。それでは、木村さん、お願いいたします。

【木村構成員】　主婦連合会の木村です。御説明ありがとうございます。大変丁寧にい

ろいろ対応をなさっていることはよく分かりました。私からは２点質問させてください。

１点目は、契約について御説明いただきましたが、作業が終了したとか、不適切なことで終了したときの契約解除について、御説明いただけませんでしょうか。例えばどのように情報を削除するとか、社としての方針とか方法があれば教えてください。

２点目は、利用者もこういうことを知らないといけないと思うのですけれども、資料の４ページにプライバシーポータルということで書いてあるのは理解したのですけども、御社から利用者に、これをどのように利用者にお知らせしているか教えてください。よろしくお願いいたします。

【山本主査】　ありがとうございます。それでは、KDDI様お願いいたします。

【山崎氏】　御質問ありがとうございます。１点目の契約のところと、あと終了時にどうしているのかというところについて、まずは回答させていただきます。

契約終了時については、まず、契約をするときに、契約終了した場合にはデータを削除してください、物理的に渡すものであれば、そのデータを返してくださいというような返却、削除の取決めをした上で契約をしております。最後に、終了するときに削除の証明書とか、やり方は様々、ケース・バイ・ケースであるのですけども、それを削除したとか返却したという証明書を取り交わすことで終わるというような形を徹底するという形で対応しております。

【木村構成員】　必ず書面でということですね。

【山崎氏】　そうですね。原則書面で取り交わす形になっています。

２点目のプライバシーポータル等、どういった形で利用者、お客様にお伝えしているかという点なのですけども、これも様々やり方はあるかとは思っているのですが、大きなところとしては、規約の同意をしていただくとか、使っていただく場面において、規約では、文字でたくさん書いてあってなかなかイメージしにくい部分があると思うのですけども、この先、さらにもう少し詳しく知りたい方はという形で、規約の中からプライバシーポータルに誘導というか、リンクをさせていただいてそこで見ていただくと、そういった形で規約とイメージをセットで見ていただくといったような、そういった形で御案内をするようにしております。

【木村構成員】　分かりました。ありがとうございます。利用者に分かりやすいように工夫していただいていることはとてもいいと思いますので、利用者にさらにアピールする形になるといいと思います。ありがとうございます。

【山本主査】　ありがとうございます。それでは、寺田さんお願いいたします。

【寺田構成員】　よろしくお願いいたします。JIPDECの寺田と申します。よろしくお願いします。丁寧に御説明いただきまして、ありがとうございます。問題を起こさないように様々な対策を取られているということをよく理解いたしましたが、一方で、どんなにリスクマネジメントを強化しても問題は起こり得ると、そういった考え方を前提にするのも重要だと思っています。その上で、２点お聞きしたいと思います。

まず、１点目が、委託先にどのような責任を持たせるかということです。委託先に真摯に対応していただくためには、それなりにちゃんと委託先にも一定の責任を負わせる必要があると考えられます。委託先が問題を起こしたときに、恐らく契約書の中では損害賠償といったようなものが入っているかと思いますが、それ以外に何らかの責任を負わせるということを、例えば取引の停止をするとか、そういったことも考えていらっしゃいますでしょうか。

それから、２点目が、実際にインシデントが起こってしまったという場合の対策について、被害を最小化するとか２次被害を防ぐ、そういった対策というのはどのようになっているのかについて、お聞きしたいと思います。大体委託先に責任があるよといった形で契約書には書かれているかと思いますが、なかなか委託先だけで全て解決できる、あるいは、委託先が自己の責任を最小化しようとするような動きを取ったりということもあり得ると思いますので、こういったことが起きないように、委託元のKDDIさんとして何らかの対策というものを考えていらっしゃるでしょうか。

以上２点になります。よろしくお願いいたします。

【山本主査】　ありがとうございます。それでは、KDDI様お願いいたします。

【山崎氏】　御質問ありがとうございます。まず、１点目の委託先にどのような責任を持たせるかというところについて、山崎のほうから回答させていただきます。

こちらですけども、契約をするときの契約書に損害賠償とか、そういったところは明確に規定するというものは大前提としてあります。それ以外にも、委託先への依頼事項として締結する部分があり、代表的なところでいうと、漏えい時に、速やかに報告することであったり、それを委託先に運用していただくことを明記する条項を入れているのが一般的にやっておるところになります。

その上で、我々がお願いしている事項を守っていただけないといった場合には是正をお願いするというところも委託元の権利として入れておき、さらに、それでも改善が見られ

ない場合には、取引を停止するといったようなところを契約上、担保して、委託先にも、言わばガバナンスを効かせるというようなやり方をしているというのが委託先の責任という観点で、我々がやり取りしている内容となっております。

【山本主査】　ありがとうございます。寺田さん、いかがでしょうか。よろしいですか。

【寺田構成員】　ありがとうございます。２点目のインシデント起きた場合の、委託先と委託元、KDDIさんと責任の分解のところというのがまだお聞きできていないのですが。一般的に委託先が何らかの問題を起こした場合は、全て委託先の責任だよという形になる、契約書でもそう書かれていると思うのですが、なかなかそれで解決できない場合というものが非常に多いように思っていますので、そういったインシデントが起きた場合に、委託先が何らか問題を起こした場合に、委託元として何らかの対策みたいなものというのは考えていらっしゃるでしょうかという質問になります。

【中塚氏】　業務委託先でもログを取得していたりということで、当該ログを我々も一緒になって調査したり、原因や影響範囲などを特定した部分、適切な対策を実施できるようにということで、我々も委託先に寄り添いながら、一緒に対応するような形で対処しているといったような状況となってございます。

【寺田構成員】　分かりました。ありがとうございます。

【山本主査】　ありがとうございます。それでは、生貝さんお願いいたします。

【生貝主査代理】　大変丁寧に御説明いただきありがとうございました。私からは１点、KDDI様も非常に様々なグループ会社、多く持っていらっしゃいますけれども、その中で委託先の管理ということも含めて、グループ会社で、グループ全体として協力して取り組んでいる、あるいは一緒に行っているといったようなことがあれば、教えてください。よろしくお願いいたします。

【山本主査】　ありがとうございます。それでは、KDDI様お願いいたします。

【中塚氏】　KDDI、中塚でございます。KDDIグループの中で、KDDIグループガバナンスという営みをやっておりまして、各子会社をしっかりとキャッチアップしながら、本体が支援しながらということで、しっかりとKDDI全体のグループガバナンスを下げないように、上げるようにということで、日々取り組んでいるといった次第となっております。

【生貝主査代理】　分かりました。ありがとうございます。

【山本主査】　ありがとうございます。それでは、太田さんお願いいたします。

【太田構成員】　DataSignの太田です。御説明ありがとうございました。私からは２点

質問させていただきます。１点目は、呂さんの質問への追加質問のような感じなのですが、もう回答いただいているかもしれないですが、僕が完全に理解できなかったので確認させてください。

業務委託先との契約のところです。利用者情報の預託がある場合とない場合みたいなので場合分けをされていましたけれども、利用者情報の預託がある場合というのは、個人データの取扱いがある、取扱いがないに関わらず、同じ契約内容で同じ対応を行うということでよろしいでしょうかというのが質問の１点目です。

２点目ですけれども、これは６ページのところです。契約のところで、当社同等のセキュリティレベルを確保と書いてありまして、かつ再委託先にも同じ、同等の義務の実施みたいなのが８ページ目に書いてあるのですけれども、要するに、御社のセキュリティレベルと同等レベルで委託先、再委託先もちゃんと確保されていることを契約で担保するということだと思うのですけれども、普通に考えてというか、イメージ的にはKDDIさんのセキュリティレベルと販売代理店と、代理店の末端である店舗みたいなところまで、全てがKDDIさんと同じセキュリティレベルですというのは、結構かなりハードルが高いんじゃないかと感じたんですけれども、これは、例えば入退室管理とかに関しても結構店舗レベルだと厳しいかと思ったんですけれども、これはコストをかけて、御社、KDDIさんのセキュリティレベルを同等にするという取組を行っているということなのでしょうかというのが２点目の質問でございます。以上です。

【山本主査】　ありがとうございます。それでは、KDDI様、お願いいたします。

【山崎氏】　御質問ありがとうございます。１点目のデータの取扱いの部分については、山崎のほうから回答させていただきます。

こちらですけども、御質問の趣旨としては、預託があり、なおかつ、個人データの取扱いがある、預託はしているけども、個人情報保護法上の取扱いがない場合、さらに分水嶺というのがあるのじゃないかという御質問だと理解しました。

個人データの取扱いがあるのかないのかというところも内部の審査というか、チェックの中でチェックをして、それに応じて適切な対応を求めるというような、そういった形になってございます。

【太田構成員】　ありがとうございます。１点目についてはよく分かりましたが、もうちょっと突っ込んで聞きたいなと思ったのが、取扱いがあるないというのをどういう点で判断をしているかというのが、もしあれば教えていただけますでしょうか。

【山崎氏】　ありがとうございます。それもケースにもよるというところではあるとは思うのですけども、通常、我々が契約する際にはセキュリティのレポートを確認したり見たり、利用規約を確認したり、あとは、そこから読み取れない場合に、情報の取り扱い方法を直接確認した上で、必要な対応をお願いしていくという、そういう流れになっています。

【太田構成員】　ありがとうございます。１点目に関しては大丈夫です。

【山崎氏】　２点目は中塚のほうから回答させていただきます。

【中塚氏】　中塚でございます。御質問ありがとうございました。先ほどの御質問ですけれども、基本的にKDDI、当社の非常に重要なデータを扱っていただくといったようなこともありますので、基本的には、我々と同等のものを求めるといったことでお願いしている次第です。

【太田構成員】　ありがとうございます。では、もう委託先、再委託先まで、本当にKDDIさんと同等のところのコストをかけて、ちゃんと実施しているということを担保するようにしているということですね。

【中塚氏】　はい、そうなります。

【太田構成員】　ありがとうございます。

【山本主査】　ありがとうございます。太田さん、よろしいでしょうか。

【太田構成員】　はい、大丈夫です。

【山本主査】　ありがとうございます。それでは、江藤さんお願いします。

【江藤構成員】　一橋大学の江藤祥平と申します。私からは大きく３点お伺いさせていただければと思います。

まず、お示しいただきました資料の７ページの情報セキュリティ教育について、具体的な内容をもう少し御教示いただければと思っております。違反事例について、人為的なエラーに基づくものが多いということで、私も教育、あるいは研修というものの重要性について認識しております。お伺いしたいのは、いわゆる委託先、あるいは再委託先における研修内容について、どの程度把握されていて、どの程度の要求をされているのかということを御教示ください。具体的には、御社のコンテンツを提供するというようなこともあるのか、あるいは、いわゆる動画を閲覧するというのではなく対面での教育実施、あるいは理解度の確認、そういった具体的な内容まで求めておられるのかという点について御教示ください。

２つ目は委託先の選定に関わる話です。委託先の選定時におけるチェックシートにおける確認の運用ということですけれども、こちらは仮にチェックシートの要求を満たさない場合には不十分であるとして委託を断るのか、それとも、委託先にそれを是正させて最終的には委託契約に至るという運用が常態化しているのかという点について、御教示ください。併せまして、再委託の場合、事前承諾が必要ということですけれども、こちらのほうも事前承諾をしないという運用が実際にあり得るのか、それとも、チェックシートを満たす内容であれば、最終的には事前承諾に至っているのかということも御教示ください。

３点目、細かい点ですけども、事前にいただきましたアンケート、３－２のところでシステムアクセスの認証方法について、知識認証、所持認証、生体認証のいずれか、または複数を組み合わせた認証とございます。このいずれか、あるいは複数、どちらを採用するかというのは、これはどのような情報を扱っているかによって求められる認証の度合いというのが異なってくると､そういった理解でよろしいのか御確認いただければと思います。

以上、３点よろしくお願いします。

【山本主査】　ありがとうございます。それでは、KDDI様、お願いいたします。

【中塚氏】　質問ありがとうございます。まず、教育につきましてですけれども、主にe－ラーニング等を使いながら、まず、情報セキュリティの基本のキから、また事故の話だとかというところも含めて、幅広く教育するようなことで委託先、再委託先についての教育をお願いしています。必要に応じて、弊社側のコンテンツを提供するといったところが一つ目の答えとなってございます。

それから、２つ目の質問ですが、満たさない場合の対応についてですけれども、ここは基本的に、満たさない場合については契約をしないといったようなことで徹底してございます。再々委託時についても同様といったようなことで徹底してございます。

それから、システムアクセス認証のいずれか、複数の部分につきましては、ケース・バイ･ケースというような形になると思いますので､御理解いただければと思っております。

【山本主査】　江藤さん、いかがでしょうか。

【江藤構成員】　ありがとうございます。研修ですけれども、私もいろいろな個人情報を大学で扱うので、e－ラーニングで研修を受講することも多いですけれども、例えば、研修内容によっては倍速再生が可能になるであったり、あるいは知識確認が求められないものだったり、そういったものですと、どうしても実際に個々人が徹底して個人情報の重要性について認識しているかと言われると、心もとないところもあるなと思ってふだん受講

しておりますので、最も重要な個人情報を扱う最前線の情報取扱者が、徹底してコンテンツ教育を受けるということは非常に重要だというように、お話をお伺いして思いました。

私からは以上です。

【中塚氏】　ありがとうございます。テストなんかで確認をしたり、それからしっかりと研修が終わったことについて提出で確認したりもしていますので、そこら辺も徹底していることを、追加として補足させていただければと思います。

【山本主査】　ありがとうございます。一通り御質問、御意見を承ったかなと思いますけれども、改めてという方がいれば、チャットにてお知らせいただければと思います。いかがでしょうか。よろしいでしょうか。

ありがとうございます。そうですね。私も、皆さんの御質問でほぼ伺いたいことはカバーできていて、特に追加でというのはないのですが、１点最後のところの、お答えにくいところかもしれませんけども、研修のところについてご質問させていただきます。この研修ですが、どういった人間観を前提とされているのでしょうか。また、今いろいろテストをして、その効果を確かめるというところがありましたけれども、どういう研修、伝え方というのが効果的なのかというところについて、何か御知見があればぜひ教えていただきたいなと思います。

というのも、性悪説に立ったときに、法的な制度がこうなっていますということを教えても、あまりピンと来ないというか、あまり効き目がないような感じがいたします。どちらかというと、事故が起きるとあなたにもこんな不利益がありますよという脅しじゃないですけれども、ネガティブな帰結を伝えるとか、そういうのが効果的ということもあるかもしれない。伝え方なども心理学的にいろいろあるのかなと思ったので、その辺り、何か御知見があればお聞かせいただきたいなと思いますが、いかがでしょうか。

【中塚氏】　御質問ありがとうございます。研修といっても、いろいろなレベルの方に一様に研修するわけじゃないのでなかなか難しい部分もありますけれども、やはりメリハリといいますか、そういった罰則のものを伝えるべき研修もありますし、先ほど申しましたとおり、基本のキの部分をやるといった部分もあったり、あとは、各所におけるリスクなんかを持ち寄って、部署間での各種のリスクを相互に知るといって気づきを得るといったような研修もやってございます。

【山本主査】　ありがとうございます。いろいろ工夫して取り組まれているということはよく分かりました。ありがとうございます。

それでは、KDDI様、ありがとうございました。こちらにて御退出となります。改めて御礼申し上げます。ありがとうございました。

【中塚氏】　どうもありがとうございました。失礼いたします。

【山本主査】　それでは、KDDI様の御退室が完了次第、楽天モバイル様の質疑応答となります。事務局にて設定をお願いいたします。

【山本主査】　それから、生貝さん、私が、次の予定がどうしても出なければいけないということで、ここでバトンタッチでもよろしいですか。

【生貝主査代理】　承知しました。

【山本主査】　よろしくお願いします。ありがとうございます。

【小玉利用環境課課長補佐】　それでは、生貝先生、準備ができました。

【生貝主査代理】　ありがとうございます。それでは、山本先生に代わりまして、しっかり務めさせていただきます。生貝でございます。

それでは、早速でございますけれど、楽天モバイル様の質疑応答に移らせていただきたいと思います。御説明について、構成員の皆様から御意見、御質問ありましたら御発言、チャットのほうに、その旨を書き込んでいただければと思います。よろしくお願いいたします。それでは、寺田さん、よろしくお願いいたします。

【寺田構成員】　よろしくお願いいたします。JIPDECの寺田と申します。よろしくお願いいたします。

【本田氏】　よろしくお願いたします。

【寺田構成員】　非常に丁寧に御説明いただきありがとうございました。問題を起こさないように様々な対策をされているということ、よく理解できました。とは言っても、どんなにリスクマネジメントを強化しても問題というのは起こり得る、そういったことを前提にすると、幾つか御質問させていただきたいことがあります。

３点あるのですが、１点目は、委託先にどれだけの責任を持たせるのかというのが非常に重要なことなのかなと思っています。委託先が問題を起こしたときに、多分契約書では損害賠償とか、そういった内容が入っているかと思いますが、それ以外に何らか責任を負わせるような、例えば、取引を停止しますとか、そういった内容といったものも考えていらっしゃいますでしょうか。また、これまでに問題を起こした委託先があればですが、そういったことがあったのかどうか、問題を起こした委託先がもしあったという場合には、どういった責任の負わせ方というのをされたのかということについて教えていただければ

と思います。

それから２点目になります。今度は、実際にインシデントが起きてしまったという場合の対策について教えていただきたいなと思います。被害を最小化するとか、２次被害を起こさないように対策といったことを、どういったことをされているのかということになるのですが、委託先がやらかしてしまった場合には、基本的に委託先の責任ですよという形にはなっていると思いますが、なかなか委託先だけでは対応できない、あるいは、委託先が問題を矮小化しようとかといったことも起こり得るので、そういったことに対して何らかの対策といったものは考えていらっしゃいますでしょうかというのが２点目です。

３点目になります。再委託に関してですが、再委託に対して、楽天モバイルさんと委託先との間で契約の内容とか、そういった条件と同等とされているというふうに書かれていましたが、一方で、再委託先に対して監視監督であったりとか、そういった形での立入りであったりとか、特に立入調査、そういったことはされていますでしょうかと、以上３点よろしくお願いいたします。

【生貝主査代理】　楽天モバイル様、よろしくお願いします。

【本田氏】　ありがとうございます。まず、インシデントに係る御質問からお答えさせていただきますと、当然インシデント等は委託先において発生いたします。報告を、委託先で発生したものを、それを委託している部門、主管部門が受けて、我々のところに報告というものが入ってまいります。それを我々セキュリティ部門のほうで確認を行って、その原因と､それから再発防止策が十分であるかということの確認を行うわけですけれども、その報告において不十分と思われたもの、それから、何度も同じような類型の事故、ある程度、繰り返してしまうような事業者に関しては、実地に主管部門だけではなくて、セキュリティ部門として赴いて何が起きているのか、何でその再発防止策が有効でなかったのかということを詳しくヒアリングをするということを行っております。

それによって、例えば当社のほうで委託先が使ってもらっているシステムであるとかオペレーションそのものに何らかの無理が生じているのではないかというような場合には、システム部門に対してセキュリティ部門から調整をかけて、オペレーションをより合理的にできないかといった調整をしながら、事故の再発に対して、委託先のみならず当社としても積極的に関わるということを行っております。

それと、委託先が何らか事故を起こして、それがあまりにも合理的ではない、当社として委託業務をお任せできないといった場合には、これは当然契約の打切りということも視

野に入れて対応しますし、契約にもそういったことというのははっきりとうたわれております。ですので、損害賠償のみならず、契約そのものを打ち切ることは契約書に明示されているものの、私が知る限りですが、内容を適用して契約を打ち切ったという事例は現在のところ、私の知る限り、当社では発生しておりません。

それから、再委託に関して、こちらは実際には再委託先に関する管理監督については、委託先が全責任を負うということを契約、並びに再委託に関する覚書というものに明記させていただいているものの、当社として再委託先まで立入りを行って確認をするということは、これまで行った事例はございません。ただし、これに関しても絶対にしないというわけではなくて、状況に応じて、我々としても積極的にそこに対して確認に赴くということはやぶさかでないと考えておりますので、もしそのような場面があれば適切に対応したいと考えております。

【寺田構成員】　ありがとうございます。

【生貝主査代理】　どうもありがとうございます。それでは、呂構成員お願いいたします。

【呂構成員】　大変丁寧に御説明いただきまして、ありがとうございました。まず前提的なことについて御質問させていただいた上で、追加の質問をさせていただくかもしれません。契約の類型を、業務委託契約と外部クラウド利用契約に分けられているということですけれども、この分け方はどういった基準に基づいているでしょうか。

【本田氏】　契約というよりも、チェックのスキームを２つに分けているということになります。まず、その前提で、契約そのものが２つに分かれるのではなくて、あくまでデータの委託というものは、形が異なりますので、通常の業務委託と、それからデータを委託するSaaSのようなシステムを提供する事業者に対するものと２つに分けているというイメージになります。

まず、この点は御質問の御認識と合いますでしょうか。

【呂構成員】　そうですね。ヒアリングシートも拝見していて、こちらの項目１－２．で、個人データの委託をしている場合の契約形態が業務委託契約と外部クラウド利用契約大別される旨記載されていたので、これに対応して、チェックも委託作業型とクラウドサービス型で対応されているのかなと思ったのですが。

【本田氏】　そこはおっしゃるとおりです。そのとおりです。

【呂構成員】　分かりました、ありがとうございます。このヒアリングの趣旨として、

定型的な外部のサービスを利用するような場合、それはクラウドを使う場合も、そうではない場合もあるかもしれないですけども、そういった場合に、個人データの委託ではないと整理してしまって、個人データの委託先の監督が十分でなかったという事案が生じた、ということが背景にあります。そういったケースとの関係で、御社におかれて、契約を類型的に振り分けて、さらにその振り分けに基づいて個人データの委託の有無を御判断されるというプロセスや基準をどうされているのか把握したかった、というのが質問の趣旨になります。御社の場合は、業務委託か外部クラウドかという点は、単純に外部のクラウドのシステムを使っているか否かで分けられているということになるでしょうか。

【本田氏】　そうですね、例えば当社の中の一事業部門が、何らかSaaSサービスを使うという場合には、クラウドのほうのチェックシートのみを提出してもらうという形になりますし、もし委託先があって、かつ委託先がSaaSのサービスを使うという場合には両者のチェックシートを回収するという形になります。

【呂構成員】　ありがとうございます。そうすると、サービス内容から物理的に判断していらっしゃるのであって、定型的な約款に基づくサービス利用契約なのでこちらに振り分ける、などといった話ではないということですか。

【本田氏】　ではないです。利用容態に……。

【呂構成員】　分かりました。その上で、業務委託契約の場合も、外部クラウド利用契約の場合も、両方とも個別の事案に応じて個人データの委託があるかどうかを御判断されているということですか。

【本田氏】　そうですね、確認をしています。

【呂構成員】　ありがとうございます。いわゆるクラウド例外に該当して、個人データの取扱いがない、といった整理をされるかどうかというのも、個別の事案に応じて御判断されているのでしょうか。

【本田氏】　そうですね。おっしゃるとおりです。

【呂構成員】　よく分かりました。ありがとうございます。私からは以上です。

【生貝主査代理】　ありがとうございます。それでは、太田構成員、お願いいたします。

【太田構成員】　ありがとうございます。私からは２点質問をさせてください。

説明いただいた資料の９ページ目で、ISO2001とかを取得している企業は審査がスムーズに進行しますということが書いてあると思うのですけれども、これ具体的にはISMS取得企業であれば審査項目が減ったりとか、チェックリストの項目が減ったりするということ

でしょうか、というのが１点目の質問です。

２点目は、これはすごく細かい話なのかもしれないのですけれども、10ページ目のところに契約先、一番最後、契約先は当社の情報に対する当初の所有権を確認した上で、サービス提供のためにのみ利用し､情報の機密性を維持することと書いてあるのですけれども、所有権の確認というところが僕的に引っかかりまして、所有権の確認というのはどうやってやっているんだろうかというのが気になりまして、まず、所有権を確認し、サービスの利用のためにのみ利用されるか確認ということで、何かいろいろとチェック項目があると思うのですけれども、所有権を確認というのはどういう確認なのかなというのを聞きたいと思いました。以上です。

【本田氏】　ありがとうございます。まず、１点目、チェックシートとそれから情報セキュリティに関する認証取得の関係なのですけれども、これは非常にシンプルで、チェックシートの構成上、一番初めのほうで委託先に対して、情報セキュリティに関する認証取得をしている場合、ISO27001と、それからPCI DSSとか、そういったものです。そういった幾つかの例示とともに、それらに適合している場合はチェックシートの１から10まで答えて、あとのものに関しては答える必要はありませんというような形の構成を取っていまして、ですので、取得しているものに関しては、取得している27001の基準に関する質問というのをわざわざすることはないだろうという判断の下でチェックシートを構成しているという形で省力化を図っているというのがコンセプトになっております。

この点はまず､シンプルな回答になるのですけど､申し訳ありません､所有権のところ､こちらに関しては､持ち帰りでの回答させていただきたいのですが､よろしいでしょうか。

【太田構成員】　了解いたしました。ありがとうございます。

１点目に関して深掘って質問をしたいのですけれども、ISMSを取得している企業だったら、ここのチェックはしなくてもいいよみたいな感じだということなのですけれども、セキュリティレベル、ISMSを取っているからセキュリティレベルが高いのかというと、そうでもないような気が僕はしていて、例えばバックアップしていますか、冗長化していますかみたいなところで、例えばISMSの場合はバックアップを取っていないけれども、そのリスクをトップマネジメントとして、許容しますとしてしまうと、別にバックアップを取っていなくてもISMS認証は取得できるみたいな、要するにマネジメントシステムとして、トップマネジメントがリスクを許容するみたいな判断をしていると、セキュリティレベルは低いけど、一応マネジメントシステムとしては回っているみたいな状況になることがある

のかなと思っていて、そこら辺でチェックリストと齟齬が生じるような、齟齬が生じるというか、答えなくていいよと言っているけども、そこの基準に達していないみたいなことが起こり得るのではないかなと思ったのですけれども、その部分は、何かそういうことが起きないようになっているイメージですか。

【本田氏】　いや、ここはもう御指摘、おっしゃるとおりだと思っておりまして、必ずしも全ての委託先に関して、ISMSを取得していれば簡易的なパス、確認のみでパスするというわけではなくて、それでも取扱う情報がシビアなものである。それから、クラウドの事業者、システムをある程度の規模で運用している場合には、当然それ以上の詳細なことというのをヒアリングしていくような構成になっております。ですので、あくまで大ざっぱなところでは､認証取得企業というところで間引く質問というのはあるのですけれども、取り扱う情報とサービスの内容によっては、個別具体的に確認をするような構成にもなっております。なので、そういった形で担保するということで、必ずしも認証が全てを賄ってくれるというコンセプトではございませんということを補足させていただきます。

【太田構成員】　ありがとうございます。よく分かりました。

【生貝主査代理】　ありがとうございます。そうしましたら、森構成員、お願いいたします。

【森構成員】　御説明ありがとうございました。よく分かりました。私は委託先の選定のところ、契約の締結段階のところについてしたいと思いますけれども、基本的にはチェックシートを使ってということですけれども、チェックシートでやるとなると、業者の皆様はもちろん、楽天モバイルさんと契約したいということなので、チェックしがちになると思うのですけども、その辺をどのように、これは本当にチェックのとおりやっているのだろうかと、紙だけかもしれないですけども、実際に紙のとおりだろうかというように確認できるようになっているのかと。インセンティブとしては、実際にやっていなくてもチェックしがちだと思うのですが、そこのところを見破れるように、何かそういう工夫がありますでしょうかということについて、もしあれば教えていただければと思います。よろしくお願いします。

【本田氏】　御質問ありがとうございます。この点に関して、セキュリティという面では、必ずしも一律、こういった形で虚偽なチェックシートの内容というのを補完できるようにしようというような手段というのは、今のところ一律ではございませんが、ただし、ある程度扱う情報が大量にある、サポートセンターとかそういったところと新たな取引を

結ぶというような場合には、実地に赴いて確認をするといった手順というのを、事業部門と連携をしながら対応した事例というのはございます。

【森構成員】　なるほど、場合によってはチェックリストだけではなく、実査といいますか、実際にどうなっているのかというのを見に行かれるということですか。

【本田氏】　そうです。

【森構成員】　分かりました。ありがとうございました。

【生貝主査代理】　よろしゅうございますか。それでは、江藤構成員、お願いいたします。

【江藤構成員】　一橋大学の江藤祥平と申します。本日は大変分かりやすく御説明いただきまして、どうもありがとうございます。私からは簡単に、大きい点は一つと、細かな点で２点、お伺いできればと思います。

１つ目は委託先、また、再委託先における情報取扱者の研修、教育内容についてお伺いできればと思います。リソース配分の観点から限界があるかもしれませんが、御社の情報コンテンツについて、例えば委託先に提供されるようなことはとあるのでしょうか。また、再委託先における研修内容というのは、これは委託先と再委託先との契約の間で決まっているように思いますけれども、その点についても、御社のほうで把握されているか否かについて、お聞かせいただければと思います。

２点目は、事前にいただきましたアンケート、２－11と２－12の点で、いわゆる外部サービスの利用や親会社、連結子会社におけるものの内数についての件数であったり、個人データ取扱い委託先における契約違反の件数について、非開示とさせていただきますということで、そのように承知しているのですけれども、こちらのほうは、数としては無論把握はされているんだけれども、何か契約等々の状況によって開示することが差し支えると、そういう認識で正しいのかについて、御教示ください。

３点目は、先ほどの太田委員の質問とも関わるのですけども、いただきました資料の10ページで、当社の情報に対する当社の所有権という類いですけども、研究者の身では、思わず所有権という言葉がここに出てしまうと気になってしまって、一応データは無体物なので、所有権は観念し得ないということなので、所有権と言われると、どういう趣旨かなというように確かに少し混乱するところもありましたので、何かここでおっしゃる意味での所有権というのは、先ほど太田構成員がおっしゃったように、内容を明らかにしていただけるとありがたいなと思っておりましたが、そちらについては、また追って御回答いた

だけるということですので、私のほうではコメントにとどめさせていただければと思います。では、よろしくお願いします。

【本田氏】　ありがとうございます。まず、教育に関して、こちらは委託先でも個人情報、並びに機密情報を取り扱う事業者に対しては当社の機密情報に関する区分、こちらを基にした資料というのは提供させていただいています。情報の機密レベルに応じた３段階、全部で公開情報も含めると４段階の機密レベルを定めていて、それぞれ評価される利用用法というのはこういう形ですよということを明記した資料を展開し、それに基づいた教育というのが実施されるという形で理解、共通した理解というのを担保するようにとしております。中でも通信の秘密に関しては、特に当社は通信事業者ですので、その点に関しても理解が及ぶような資料の構成に努めております。

２点目、件数に関して、こちらは特に違反のあった件数に関して、記述をということでヒアリングシートに書いてあったのですけども、違反というところが、果たしてどこまでが違反だろうかというところで考えが及んでおらず、例えば情報漏えいの件数という形であれば厳密にカウントしていますし、インシデントとして、再発防止までフォローアップするというのは先ほど申し上げたとおりですけれども、一方で、軽微なルール違反的なもの、あるいは漏えいまでは至らないけれども、ヒヤリ・ハットみたいな事案というのも、これは報告はされてきまして、そういったものまで含めると、件数としてどこまで計上して御報告差し上げるべきなのかというところが私では判断できず、後者に関しては、完全に把握、件数まで把握し切れて、吸い上げる仕組みがあるかというと、そこまでは全体的に及んでいないかなというのが正直なところでございます。インシデントとヒヤリ・ハットであるとかインシデント未満である情報漏えいに達していないものであったりというところはスコープから外れておりますので、そういった形でモニタリングをしているということが御説明になります。

以上で御回答になっておりますでしょうか。

【江藤構成員】　どうもありがとうございます。確かに２点目の契約違反の事例については、我々も意見をお互いに出し合って、この質問に至った記憶があるのですけれども、契約違反件数ということでしたら少し曖昧ですので、次年度以降、質問の内容を工夫するなどして、より会議に即した回答をいただけるような質問へと改めていければと思っております。どうもありがとうございます。

【本田氏】　ありがとうございます。

【生貝主査代理】　ありがとうございました。それでは、木村構成員、お願いします。

【木村構成員】　主婦連合会の木村です。御説明ありがとうございます。まず、資料で、委託終了に関して書いてあるのですが、実際にはどのようにされているのかというところです。書類をやり取りしているのか、立入りをしているのか、委託終了についてどのように確認されているのかというのが１点目の質問になります。

２点目ですけれども、ヒアリングシートを拝見しまして、利用者にこういうふうに知らせるというURLがありましたので、そちらを拝見しました。そうすると確かにきちんと書いてあるのですけれども、文字だけなので印象としては分かりにくいと感じたのが正直なところなのですけれども、利用者に関して、もう少し分かりやすく伝えるということをする予定はありますでしょうか。あと、利用者にはどういう機会に、どのように伝えているかということを教えてください。よろしくお願いいたします。

【本田氏】　ありがとうございます。まず、契約終了時、こちらに関しても基本的には書面と、それからアカウントを消しましたねとか、それから、破棄証明書を出してくださいねというような形のチェックシートみたいなものを適用することで担保をしている形です。

一方で、例えば販売代理店であるとか、それからコールセンターに関しては、実際に物件退室時に、完全に情報がなくなっているかというところは目で、目視で確認をするというのが、それぞれ主管部門のほうで実施されておりますので、そういった形で残留物がないといったことまでは目で確認するということも併せて行っております。

まず、１点目のお答えになりまして、２点目、お客様向けの個人情報の扱いに関する御説明に関して、こちらに関しては日々、分かりにくいというところがあれば、改善を試みるという取組はしているものの、御指摘のとおり分かりにくい点があろうかということは思います。こちらに関しては、改善を日々重ねていくしかないわけですけれども、変更、それから何かサービスの側でも新たなサービスが取り扱われることによって、個人情報の取扱いが変わるというようなことがあれば、これは約款の変更という形でユーザーに対する周知をメール等、有効な形で行うというのが定められた手順にのっとって実施をしているという認識でおります。

【木村構成員】　メールにて、利用者にお知らせするという理解でよろしいですか。

【本田氏】　そうですね、メールをはじめとする有効な手段を通じてお届けしています。お客様の登録された連絡先に対して、必要な変更内容を適切な方法でお伝えする形となり

ますので、基本的にはメールを使用することが多いかと思います。

【木村構成員】　分かりました。ありがとうございます。

【生貝主査代理】　ありがとうございます。それでは、これで１巡分は御質問いただいたかと思いますが、ほかにさらに御質問とコメント等あればと思いますが、いかがでしょうか。よろしいですか。

そうしましたら、私から一つだけ、少しマクロな質問ですけれども、楽天様のグループとしては、通信モバイル事業にまさに５年ほど前ですか、本格的に参入をされて、そして、もしあればですけれど、その前と後で、つまり、まさに通信事業者としての情報を多く扱うようになった中で、グループとしてという形になるかもしれず、また、委託先の管理監督だけには限られないと思うのですけれども、まさにこういったプライバシー、個人情報、利用者情報のガバナンスで何か変わったということが、プラクティスでも、あるいは何か意識や考え方という意味でもあれば教えていただきたいなと思ったのですが、いかがでございましょうか。

【本田氏】　やはり正直申し上げて、通信の秘密を取り扱うというところで責任の重さというのが増したというところは、我々、隣で仕事をしているプライバシーの主管部門も、情報セキュリティの部門も、当然我々としては認識を強めなければいけないですし、従業員に対する説明もより強めていかなければいけないと日々認識をしているところです。ここは大きく、これまで通信の秘密を取り扱う前と後で一番変わったのはそこだと思っておりますので、グループ全体に対して、楽天モバイルで取り扱っている情報は通信の秘密であって、厳重な管理とルールにのっとって取扱いが必要であるということを伝えることが大きく変わった部分かなと認識をしています。

【生貝主査代理】　どうもありがとうございます。承知しました。

それでは、ほかに特に御質問、御意見等ございませんようでしたら、この辺りで意見交換を終了させていただきたいと思います。

それでは、最後に事務局から連絡事項をお願いできればと思います。

【小玉利用環境課課長補佐】　事務局でございます。生貝先生ありがとうございます。

本日の議事録につきましては、事務局で作成の上、皆様にお諮りをいたしました後に公表することとします。

以上でございます。

【生貝主査代理】　ありがとうございます。

それでは、楽天モバイル様、ヒアリングのほう丁寧に御対応いただきまして、ありがとうございました。

以上で、利用者情報に関するワーキンググループ第16回会合を終了とさせていただきます。本日は皆様方、お忙しい中御出席をいただきまして、ありがとうございました。

以上