参考資料17-1

利用者情報に関するワーキンググループ（第14回）

令和６年11月12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14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です。皆様、お忙しい中、本日もお集まりいただきましてありがとうございます。

本日は、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、NTT東日本から石井情報セキュリティ推進部長、NTT西日本から萬本セキュリティ＆トラスト部長にお越しいただいております。また、個人情報保護委員会にオブザーバとして御参加をいただいています。

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。よろしくお願いいたします。

本日から３回にわたり、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、まず事務局から本ヒアリングの趣旨について御説明いただき、続いて、NTT東日本様、NTT西日本様より順番に御発表をいただきます。事業者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にて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、事務局から御説明をお願いいたします。

【小玉利用環境課課長補佐】　再び事務局でございます。ありがとうございます。

資料14－１に基づきまして、電気通信事業者における利用者情報の取扱いに関するモニタリングについて、簡単に御説明させていただきます。

１ページ目をお願いします。１つ目のオレンジの枠ですけれども、これまで申し上げてきたとおり、総務省では、「電気通信事業における個人情報等の保護に関するガイドライン」において、電気通信事業者による情報の取扱いについて定期的にモニタリングをするということになっております。

さて、２つ目のオレンジの枠でございますが、同ガイドラインの第13条３項ですけれども、電気通信事業者は、個人データ等の取扱いを委託する場合に、委託先において当該個

人データ等について安全管理措置が適切に講ぜられるよう、委託先に対し必要かつ適切な監督を行うこととしております。しかしながら、近年、電気通信事業者の業務の委託先を通じて利用者情報が漏えいするという事案が複数発生しています。

具体的には、その下の点線の部分ですけれども、２つの事例を挙げさせていただいています。2023年、NTTドコモがインターネット接続サービス等の販売支援業務を委託している会社から、顧客情報を含む業務情報が不正に持ち出されたという件。あるいは、NTT西日本がテレマーケティング業務を委託していた会社、この会社に対して、コールセンタシステムを提供していた、また別の会社から2014年から2022年にわたり顧客情報が不正に持ち出されていたという事案もございました。

こうした事案があったことから、今回、電気通信事業者の委託先における利用者情報の取扱いについて確認を行うため、今後３回にわたってモニタリングを行わせていただくというものでございます。具体的には、NTT東日本様、NTT西日本様、ドコモ様、ソフトバンク様、KDDI様、楽天モバイル様に対して実施させていただくというものでございます。

２ページ目をお願いいたします。主なヒアリング項目といたしましては、大きく３つの観点がございます。

第１は、委託先の監督ということでございます。ここには具体的に、右に書かれているように、委託先選定時における委託先候補の安全管理措置等の確認方法ですとか、委託契約における、安全管理措置の実施あるいは秘密保持等の定めの有無ですとか、あるいは委託先における個人データの取扱状況の把握の方法ですとか、個人データの取扱いを伴う外部サービス、いわゆるクラウドサービスなども含みますけれども、そういった外部サービスの利用を行う場合について、個人データの取扱いの委託としてきちんと認識しているかということが含まれています。

第２は、安全管理措置でございます。大きく分けて、外部、内部とございますけれども、委託先において、外部からの不正アクセスによる漏えいを防ぐための安全管理措置ですとか、あるいは内部からの不正持ち出しによる漏えいを防ぐための安全管理措置がございます。

最後に、その他としていますけれども、例えば、委託に関する説明を利用者に対して行っているか、適切にされているかというような観点もございます。

３ページ目は、電気通信事業者６社に、今回、ヒアリング対象でございますが、記入を依頼しましたヒアリングシートでございます。詳細は割愛しますが、前に述べた観点が網

羅的に溶け込んでおります。

１ページ飛ばしていただいて、５ページ目でございますけれども、御参考までに、ガイドライン第13条３項の解説を抜粋しています。冒頭から申し上げますと、電気通信事業者は、個人データ等の取扱いを委託する場合には、委託先において当該個人データ等について安全管理措置が適切に講ぜられるよう、委託先に対して必要かつ適切な監督をしなければならないということがまず大きな趣旨としてございますと。具体的なお話として、電気通信事業者は、自らが講ずべき安全管理措置と同等の措置が講ぜられるように監督を行うものということを規定しています。

また、ガイドライン解説は、さらに具体的に書いていて、電気通信事業者は、取扱いを委託する個人データ等の内容を踏まえて、個人データが漏えいした場合に本人が被る権利ですとか利益の侵害の大きさを考慮して、委託する事業の規模、性質、あるいは個人データの取扱い状況に起因するリスクに応じて、３つの措置を大きく挙げております。すなわち、１つ目が、適切な委託先の選定であり、２つ目が、委託契約の締結であり、３つ目として、委託先における個人データ等の取扱いの状況をきちんと把握することを講じるということでございまして、こうした３つの項目は、既に少しだけ御覧いただいた３ページ目のヒアリングシートにも溶け込んでいるところでございます。

最後に、スケジュールでございます。少し戻っていただいて、４ページ目でお願いできればと思いますけれども、想定スケジュールですが、本日、そして、11月15日、そして、25日とヒアリングを実施し、年内に向けて取りまとめをさせていただければと存じます。

御説明は以上でございます。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した。

それでは、続きまして、NTT東日本、石井部長より御説明をお願いいたします。

【石井氏】　NTT東日本の石井です。資料を共有しますので少々お待ちください。

資料の共有のほう、大丈夫でしょうか。

【山本主査】　見えております。よろしくお願いします。

【石井氏】　それでは、早速ですけれども、本日はこのような貴重な機会をいただきまして、大変ありがとうございます。第14回の利用者情報に関するワーキングという形の中で、我々NTT東日本における業務委託を中心に、契約、及び、その契約の中でお客様情報をどうやって取り扱っているかというところをより具体的にお話しさせていただきたいと思っております。よろしくお願いいたします。

ここは目次でございます、先ほど話したところでございますので割愛させていただきます。

では、早速ですが、我々NTT東日本の電気通信事業がどういったものかに関しましては、皆様、もう既に御存じだとは思いますけれども、おさらいという形、イメージがより湧くということを想定しまして、お話をさせていただきたいと思います。

大きく電気通信事業と、それに関する附帯の業務及びその目的を達成するための目的達成業務がございます。電気通信事業に関しましては、皆さん、もうイメージどおり、いわゆる音声の伝送サービス、いわゆる電話です。あと、データ伝送サービス、いわゆるインターネット等のアクセス、あと、専用サービス、これは企業の一般専用線という形で使われることが多くございます。あとは電報です。この４つを電気通信事業という形で我々は営んでいるというのが実態でございます。

それに加えまして、附帯及び目的達成として、例えば、料金をお支払いいただくような料金回収であったり、または昔の電話機の販売、通信機器の販売であるとか、いわゆる電気通信事業を実際に行っていくために必要なほかの業務を附帯業務・目的達成業務という形で実行しているというのが実態でございます。

続いて、では、先ほどの電気通信事業をどのような形で行っているかといいますと、やはり業務委託というものは存在しています。電気通信サービスの申込みであるとか、または解約、開通みたいな、いわゆるサービスを活かしたり、またはサービスを停止したりというような場合の処理を委託するケースが多くございまして、こちら、情報としましては、契約者様のお名前や御住所、電話番号等の取扱いに関して我々の連結子会社に委託しているというのが一つございます。

続いて、真ん中の段になりますけれども、実際、サービスを御利用していただいているお客様のサービスが、いわゆる故障であるとか、うまく動いていないというのが分かった際、当然直しに行ったり、運用中のフォローをしますので、故障対応等を行うものに関して、また契約者様の御氏名であるとか住所、連絡先等、これも連結子会社に委託しているというケースがございます。

最後、電報です。これに関しては配達がありますので、ここをいわゆる連結子会社に委託しているということがございまして、電気通信事業を実施していく中でも、各種委託を実施しているというのが実態でございます。

では、そういった委託をする際に、当然我々電気通信事業をしっかり営んでいく中では、

お客様の情報というものを非常に大切にしておりますので、その情報をいかに守っていくかというところで言いますと、運用で守るのは後でまた話をしますけれども、まずはルールとして、我々も３万人強のNTT東日本グループ会社社員がいますので、その方々がしっかりルールを守れるような体制をつくらなければいけないということで、いわゆる仕掛けをしっかりつくっているというのが実態です。

下のところにありますとおり、規程、基準、マニュアルとありますけれども、規程はいわゆる日本国憲法みたいなもので、こうあるべきだというのが書かれています。基準が、民法とか商法、セキュリティに関する取扱い等を定めたもので、マニュアルが実際のルールや運用をいかに実施していくかというのを分かりやすく書いたものなので、このマニュアルをちゃんと読んでいけば、基本的には、新しく来られた方であるとか、違う部署に行っても、ああ、こういう対応をすればいいんだなというのが分かるように、そういった仕掛けを工夫しながら整えることによりまして、大きな会社ではありますけども、そういった情報をしっかり守るという風土が根づくように、まずは規定等からしっかりつくり上げるというのを第一に考えております。

では、具体的に、規程や基準、マニュアルというものがどういったものかというのは、この右に書いてありますとおり、基本規程を考えるのが規程の部分ですし、基準に関しては、業務委託先の選定とか遵守事項、または情報セキュリティに関する契約の要点であるとか、あと、情報の取扱いの管理、マネジメントの状況の確認方法等に関してしっかり実施しなさいというのをこの基準のところで書かせていただいているところでございます。

最後、マニュアルのところでは、先ほども言いましたが、いわゆるセキュリティルールとして、使用する様式や、チェックシートなどがありますので、様式類等を規定したり、締結前、締結時及び契約中、契約終了時の各フェーズでいろいろな実施事項を定めているというのがマニュアルに書かれているものでございます。

では、先ほどのマニュアルに書かれている締結前、締結時、契約中、契約終了時に関して、どのようなルールがあって、具体的に何をしているかというのが次のページからの説明になります。

ここで書かせていただきましたとおり、契約前、締結時、契約中、契約終了時に何をしているかというところでございますが、まず契約前、いわゆる委託先の選定のタイミングでございます。ここに関しましては、我々の扱っている貴重な情報をしっかり取り扱うことができるかということを確認するということで、チェックシートをつくることによりま

して、均一的な対応が取れるような対応を取っているところでございます。

２番目、締結時に関しましては、右側にありますが、「お客様情報の保護及び秘密保持に関する覚書」を別途、契約とは別に覚書を結ぶという形を取っておりますので、これも締結として均一的にしっかりお客様情報を守れるということを加味して対応させていただいております。

続いて、３番目、契約中。これに関しては、契約中にしっかりそこのセキュリティが保たれているか、お客様情報がしっかり守られているかというのを点検することによって対応しており、その点検シートを定めています。

最後、契約終了時、金輪際、我々のお客様情報を扱わないということをしっかり確認するために返却・廃棄することが当然大事でございますので、返却・廃棄について委託契約終了時の対応について覚書で定めており、廃棄、終了しますということを書面でいただくという形を取っているというのが、この４つのサイクルで対応させていただいております。

では、さらに細かい話になりますけれども、委託前の選定に関しては、具体的にどういうことを聞いているのかというのがこのページでございます。２つ目の黒いところに書いてある「主な確認項目」とありますけれども、管理体制、いわゆるマネジメント体制が会社としてしっかり取れているのかというところであったり、情報の管理、情報が生まれてから、つくられて、廃棄されるまでどういった管理がなされているか。及び、新規で入ってこられる方々に対して、または、期中に、どういった教育をしてセキュリティのレベルを上げようとしているか。あとはアクセス権限、必要最低限の方に必要な情報だけが渡るような権限管理がされているか。あと、外部脅威対策であるとか、あと、事故対応、有事の際のインシデント対応等のチェック項目がございますので、こういったところをチェックして、ここが必然的に適切な委託会社であるかというのを判断するようにしております。

続いて、契約締結時でございます。契約締結に関しましては、この覚書の中にいろいろな項目を入れております。ここではまず安全管理措置、あと、次のページ以降、また、秘密保持であるとか再委託の条件はお話しさせていただきますけど、まず安全管理措置に関してでございます。安全管理措置ということに関しましては、先ほどのチェックシートと同じでございますけれども、組織的なルールがちゃんと制定されているかであるとか、点検の頻度がどうなっているかであるとか、セキュリティのマネジメント体制が取れているかというのをしっかり確認するというのがまず一つございます。

続いて、先ほどの育成のところになりますけれど、人として、従事社員に関する研修を

実施しているかというのが覚書に入っています。

続いて、環境面で言いますと、入退室の制限とか入退室管理がなされているかというのを確認したり、あと、先ほども話しましたアクセス権の必要最低限というところを確認するというのがございます。

最後、自社に関係なく外国で扱っていないか、越境ですね。こういった情報をどう扱っているのかを確認するのも安全管理措置の中で実施しているという状況でございます。

続いて、契約締結の中で、もう一つ、必須で入れる項目として秘密保持というのがございます。これはいわゆる御存じのとおり、業務に当たって知り得た情報をほかに使わない、いわゆる守れと守秘義務を課すものでございますけれども、業務上、必要以上に取らない、知らない、知ろうとしないであるとか、または漏らさないみたいなことをしっかりと事項として書き添えた上で契約を結ぶということを実施しております。

続いて、再委託先です。再委託に関しては、委託先が再委託を選定する際に我々が委託先に対応しているような同じチェックシート、チェック項目の内容をしっかり再委託先の適切な選定をするように規定しているというところ。及び、我々委託元が委託先へ実施しているのと同じようなところで言うと、書面を必ず結ぶようにしていますので、我々委託元に委託先から必ず書面が返ってきて、再委託先と契約してよろしいかというのを伺った上で許可をするというようなやり方を実施しております。これも契約として覚書の中に記載する項目でございます。

最後、再委託先の監督に関する事項でございますが、ここに関しましては、いわゆる提供とか取得、目的外の禁止であるとか、秘密保持、点検等に応じる義務を書かせていただいているところで、再委託先に関しても我々委託元が委託先に実施することと同じように、委託先が再委託先に実施するということを実施しております。

あと、最後でございますけれども、契約中と契約終了時、契約中に関しましては、冒頭申し上げましたとおり、いわゆる点検ということを実施しますが、点検シートに基づいた対応を実施するということ。あと、委託先に対して年１回の立入検査ということを実施しております。

あとは、再委託先に対しては、委託先への履行を確認する中で、再委託先のお客様情報等の取扱いを把握、監督するということを実施しております。

最後は契約終了になりますので、先ほど冒頭申しました、委託終了時の確認書、ファイルなど削除しましたということを提出させて、しっかり確認するということを実施してお

ります。

こういった動きをしっかり入り口から出口まで、我々としてはルールを決めながら運用をしっかり実施していくことによりまして、お客様情報を確実に守れるような委託を実施しているということでございます。

NTT東日本からの報告は以上となります。

【山本主査】　ありがとうございました。

続きまして、NTT西日本、萬本部長より御説明をお願いいたします。

【萬本氏】　NTT西日本の萬本です。資料共有させていただきます。

冒頭、事務局からございましたとおり、マーケティングアクトProCXという会社及びNTTビジネスソリューションズという、両方とも連結子会社なのですけども、こちらでお客様情報漏えいを起こしました。関係する全ての皆様に多大な御迷惑をおかけしましたことを改めて深くおわび申し上げます。

この当該事案についてですけども、NTT西日本からProCXへ、アウトバウンドテレマーケティング業務を委託していました。ProCXは、その業務において、ビジネスソリューションズが提供するコールセンタシステムを利用する中で漏洩を発生させてしまったものになっております。

契約形態としては、正しくは、NTT西日本とProCXの間は業務委託契約、ProCXとビジネスソリューションズの間は、コールセンターのシステムを利用するというサービス利用契約プラス個人データ取扱い委託という形でした。従来から、業務委託の場合については、当然ながら個人データの取扱い委託に該当するという認識がありましたので、そのような対応をしていましたが、業務委託ではない外部サービスを利用する場合というケースにおいて、個人データの取扱い委託には該当しないと誤認していたと言うと言い過ぎかもしれないんですけども、該当しないという認識の下で業務を行っていたということから、今回、改めて対策を行っているという状況になっております。

外部サービスによるProCXからビジネスソリューションズへの個人データの取扱いなどについては、ProCXから当社へ報告するように求めていなかったというところと、個人データをビジネスソリューションズにおいて取り扱っている事実を把握できていませんでした。

これらの点を踏まえまして、外部サービス利用時においても、個人データの取扱い委託となる場合には安全管理措置を講じる必要がある旨を契約書に明記するなど、法に則ったルールに改めるとともに、委託先事業者の皆様には、改正後のルールを反映した契約に変

更いただき、適宜必要な措置を講じていただくように対応を進めているところです。

さらに言うと、NTT西日本グループとして、今後同様の事案を再び発生させることがないように、大切なお客様の情報を扱う会社として自覚を持つ、委託先管理の取組を一過性の、一時的な対策にするのではなくて、継続的に自分事として社員一人一人がちゃんと実施していくことを通じて、セキュリティファーストカンパニーになることを目指していきます。

では、今回のヒアリングの御説明をさせていただきます。委託先に対する監督ということで、全体像になってまいります。

委託契約の締結前と締結時と締結後にどのようなことを行っているのかといったところになってまいります。

今回の漏えい事案を踏まえまして、業務委託には当たらない外部サービス利用時においても、個人データ取扱い委託となる場合がありまして、その場合には安全管理措置を講じる必要がある旨を契約書に明記するなど、法に則ったルールに改めています。

委託契約締結前につきましては、個人データの取扱い委託に対する当社監督事項として、委託先が、当社が要求する安全管理措置を履行できる委託先かどうか。委託契約の締結前にチェックシートを用いて確認を行っております。

委託契約の締結時につきましては、当社が要求する安全管理措置実施を義務づける契約書、覚書を締結しております。さらに、委託契約締結後において、当社が要求する安全管理措置を実行できているかどうか。契約締結後に立入検査や実査を含めて、ヒアリングを含めて、確認を行っております。

ここからにつきましては、それぞれヒアリング項目に、Qとして書かれているものに対するアンサーという形で御回答させていただければと思っております。

初めに、個人データの取扱いの委託について、どのような情報を、どのような事業者に委託しているのか。代表的なものを可能な範囲ということなので、まず弊社からそれぞれ委託をかけている内容としまして、これは先ほどのNTT東日本ともほとんど内容的には一致しているのですけども、電気通信サービスの申込み、解約手続というところで、個人データとして、契約者氏名、住所、電話番号等を事業者へ委託しております。

同様に、電気通信サービスの故障対応について、同じように事業者B。電報の配達について、事業者Cといった形で、代表例として、大きくはこのような委託を行っております。委託先との間の契約形態、外部サービス事業に対する認識ということで、Qのところで、個人データの委託について、もしくは再委託について、委託先との契約形態にどのような種別

があるのか。ここにつきましては、委託先との契約形態について、業務委託、外部サービス利用。外部サービス利用の中でもクラウドサービスとクラウドサービス以外という種別がございます。再委託先についても同様になっております。

さらに個人データの取扱いの委託先のうち、業務委託に対して、従来より個人データの取扱い状況を監督していましたが、外部サービス提供事業者に対しての対応が不十分だったというところで、今回の漏えい事案を受けまして、外部サービス提供事業者の個人データの取扱い状況について監督を強化しております。

次に、委託先の選定というところですけども、個人データの取扱いを委託する場合において、委託先の選定に当たって個人データを適切に取り扱うためにどのような安全管理措置を行っているかといったところですけども、契約締結前に、委託先事業者における個人データの取扱いに関わる情報管理体制であったり、研修の実施、事業者の環境、アクセス権の管理、外部脅威の対策、越境移転確認、事故対応などの項目を遵守しているか、チェックシートを用いて確認することとしています。

さらに、研修に関する確認というところも、ここの中ではないですけど、ほかの項目でQがありましたので、御回答になってくるんですけども、研修に関する確認につきましては、お客様情報管理に関する研修を少なくとも年１回求めることにしています。その中で、個人情報保護規則等で情報管理研修の実施に関する規定を盛り込んでいること、研修実施計画書・カリキュラム・受講者名簿等・研修の実績を提示できるようにしていること。研修内容は、情報管理について基本事項を盛り込んだ適切な内容であるようにしていることについて確認を行っております。

続きまして、個人データの取扱い委託契約において、安全管理措置の実施、秘密保持、再委託の条件、再委託先の監督等に関する事項を定めているかといったところですけども、このように定めております。

安全管理措置につきましては、お客様情報保護のために必要になってくる組織的・人的・物理的・技術的・外的環境把握に係る安全管理措置の遵守。秘密保持に関しましては、業務遂行に当たり委託先が知り得た情報の守秘義務の遵守を求めています。再委託先の条件、監督については後ほど説明します。

そのほかのQで出てきているものについて、契約書以外の方法に実運用上行っているものはあるかについてです。実際に実運用上行っている措置としましては、委託先事業者における個人データの取扱いに係る情報管理体制、研修、事業所環境、アクセス権管理、外

部脅威対策、越境移転確認、事故対応等の項目を遵守しているか、ヒアリング等によって確認することとしています。

個人データの取扱い状況についてどのように把握し、監督を行っているか。監査・点検の内容、方法及び頻度といったところですけども、個人データの取扱いについて、以下のとおり把握、監督を行っています。

把握項目としまして、まず個人データの取扱状況の把握・監督方法ということで、定期的に個人データ管理の各種対応の履行状況の確認を行っております。そして、事務所への立入検査等を実施しております。点検項目につきましては、こちらは委託先選定時のチェック項目と同様です。

再委託先の監督ですけども、委託先が再委託先の履行状況を調査・確認する。当社による再委託先の監督といったところで、そもそも再委託に当たっては当社の事前の書面による同意が必要となっている上で、当社が委託先と締結する覚書と同等の覚書を委託先と再委託先で締結することを義務づけておりまして、さらにその上で事務所への立入り、直接調査・報告等を行っているという状況になっております。

頻度につきましては、１年に１回、立入検査を実施するといったところで進めております。

委託先への物理的・技術的安全管理措置についてです。外部からのアクセス防止としましては、例えば個人データにアクセスする場合の従業員の認証等を実施しています。内部からの不正持ち出しの防止としましては、外部ストレージへのアクセスが可能にならないような措置を実施していたり、保守作業端末から情報が取り出せないような措置を実施していたり、保守作業端末に外部記録媒体を接続してデータを持ち出すことが可能にならないような措置を行っていたり、振る舞い検知を入れていたり、ログチェックを実施したりといったことを行っております。

最後に、個人データの取扱いの外部委託に関して利用者への説明をどのようにしているのかといったところと、あとは、漏えいした情報がインターネット上に流通していないかの確認をどうしているのかといったところになっております。

個人データの取扱いの利用者への説明ですけども、プライバシーポリシーにおいて、個人情報の取扱いを外部に委託する場合には、守秘義務契約の締結等により委託先においても適正に取り扱われるよう管理、監督をしますと記載して、公式のホームページで公開しております。

最後に、漏えい発生後の対応として、インターネット上に情報が漏えいしていないかのパブリックモニタリングであったり、ログ等による漏えいによる発生原因を調査するフォレンジック等を行っております。

NTT西日本としては以上となっております。

【山本主査】　どうもありがとうございました。

それでは、これまでの御説明につきまして質疑に移らせていただきます。先ほど御案内しましたとおり、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、本日の傍聴は以上で終了となります。事務局は非公開設定に切替えをお願いいたします。

【小玉利用環境課課長補佐】　ありがとうございます。大丈夫でございます。非公開設定に切り替えました。

【山本主査】　承知いたしました。それでは、ただいまの御説明につきまして、構成員の皆様から御意見、御質問ありましたら御発言いただきたいと思います。この質疑応答の場には、NTT東日本様、NTT西日本様の双方が参加しておりますので、御意見、御質問の際には、NTT東、西、両社に対してか、どちらか一方かについてお示しいただけると幸いです。チャット欄に御発言いただきたい旨を書き込んでいただければと思います。それでは、よろしくお願いいたします。

早速ありがとうございます。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。両社の皆さんに対しての質問とさせていただきたいのですが、両社とも当然、事前のいろいろな規程であったり、そういったものというのはしっかりとできていること、それに関しては多分大きな問題はないだろうと思っていますが、これの実効性に関して幾つか疑問があります。

その中でも、特にというところですが、結局、最終的には委託先に真摯に対応してもらわないと駄目だということで、何らかの責任をちゃんと委託先にも負わせる必要があるのだろうと思っています。その中で、委託元として委託先が何らか問題を起こしたときにどのような責任を負わせるのかということをあらかじめ決めていらっしゃいますでしょうか。また、そのことについて委託先に伝えていらっしゃいますでしょうか。

契約の中に何らか書かれていると思うのですが、それに関してさらに、これまでに問題を起こした委託先に責任を負わせたことがありますかということと、責任を負わせたことがある場合には、どのような責任を実際に負わせたことがあるのかといったことについてお聞きしたいと思います。

私からは以上です。

【山本主査】　ありがとうございます。それでは、両社ということでしたので、NTT東日本様、それから、西日本様、順番にお答えいただければと思います。よろしくお願いいたします。

【石井氏】　NTT東日本の石井です。まず委託先がもし不適切な対応をしてしまったときの対策に関しましては、覚書の中にいわゆるペナルティーといいますか、損害賠償の項目を必須項目で入れるようになっています。ですので、そういったお金の面という形だけではないですけれども、ある程度の一定の歯止めが利くような項目は必ず入れて対応するということは実施しているというところで実効性を高めています。それ以外で言いますと、年１回の立入り点検において、実際行って、話をして、紙上だけの関係にならないとか、そういったことも当然大事だと思いますので、そういった営みは取っているというところで、実効性をいかに上げていくかということに注力して対応させていただいている状況でございます。

【寺田構成員】　ありがとうございます。

【山本主査】　ありがとうございます。

それでは、NTT西日本様、お願いいたします。

【萬本氏】　NTT西日本、萬本です。先ほどNTT東日本からもありましたとおり、契約書上で、ペナルティ条項も記載しておりまして、実際に立入検査の中で、不適合のところがあったときに、それを是正したりというのを行っています。

【山本主査】　ありがとうございました。

寺田さん、いかがでしょう。何かコメントがあれば。

【寺田構成員】　ありがとうございます。実効性の部分でいくと、やはりもっと厳しい何かがないとつらいのかなという気はしています。やはり委託先からすると、怒られただけで済みましたというのではつらいような気がするので、もう少しその辺りは今後厳しくしていくということは検討されているでしょうか。

【山本主査】　では、追加の御質問ということですので、NTT東日本様、いかがでしょうか。それでは、NTT西日本様からお願いできますか。

【萬本氏】　NTT西日本、萬本です。先ほどちょっと申し上げましたとおり、実際に契約締結中に立入検査を行っていく中で、本来すべき対策というのが取れていないときはちゃんと対策をその場で実行していただくように、是正措置というか、そういったものを行っ

ていくようにはしていますので、賠償のところで請求額を上げるとか厳しくするというよりは、どちらかというと、実際の対策面の中で、我々が提供する環境だったら我々のほうがちゃんとそういう環境をつくる。委託先でその環境をつくらないといけない場合は、委託先に足りていないものをちゃんとお金を出してもらって構築していただくという考え方でやっております。

【山本主査】　ありがとうございます。

NTT東日本様、いかがでしょうか。

【石井氏】　NTT東日本も事前の審査やチェックはやっており、その中で、よりセキュリティ対策というものに重きを置くことで実施してもらうように、委託先にも当然ながら対応していけば、実効力は上がっていくと思いますし、例えばですけれども、我々弊社のシステムをしっかり使ってもらえれば、我々がしっかり監視して、彼らが何か悪さしたときにもパッとアラームが上がってくるというような対応が取れますので、極力、我々のシステムを活用することで、実効性を上げていく。厳しく対応するというよりは、セキュリティが守られるように、しっかり我々は安全サイドに入るようなところにうまく誘導をかけていくという営みを我々としては実施していく中で、トータルとして安全性が高まっていけばいいかなと思いながら強化していきたいというふうに考えております。

【寺田構成員】　ありがとうございました。私のほうは大丈夫です。

【山本主査】　ありがとうございます。

それでは、森さん、お願いいたします。

【森構成員】　ありがとうございます。御説明ありがとうございました。私から、お二方に１点と、NTT西日本さんに２つ御質問したいと思います。よろしくお願いします。

１点目はお二方にということですけども、私が実務に疎いということもありまして、契約前のチェックリストでということですけれども、チェックリストということになりますと、取引をしたいベンダーがたくさんいる。NTTさんと取引したいベンダーがたくさんいると思うんですけども、チェックリストなので、「できていないけど、全部チェックを入れておこうか」みたいなことにならないとも限らないと思うんですが、その辺りをどのようにコントロールされているのかということをお尋ねしたいと思います。

あと２つはNTT西日本さんにお尋ねしたいのですけども、漏えいの案件を念頭に置いておりますけれども、１つは、グループガバナンスのようなものがないのでしょうかということでございます。今回は、委託先ということで、委託先についてどうしているかという

ことを一般的に御説明いただいたのだと思いますけども、他方で、本件は、この漏えいの件は、どちらもやはりNTTという名前を使ったビジネスであって、それで、社会的信頼性というのはNTTの３文字によって強力に発生すると思いますので、グループ内ガバナンス、グループ内共通ガバナンスみたいなことがあるのか、ないのか。あるとしたらどんなものなのかということを教えていただきたいと思います。

それからもう１つは、これもNTT西日本さんに伺いたいのですけども、やはり本件は、漏えい自体は、数は多かったとはいえ、誰でも漏えいするという状況、時代であるのかなと思っておりまして、問題は事後的なところで、すぐに分からなかったというところが問題ではなかったかと私は個人的には思っております。そういう意味で、ProCXさんが、漏えいしているのじゃないかという指摘を受けて、調査をされたと思うんですけれども、調査をして、一旦は漏えいがないという内部的な結論に至った。そして、しばらくたってからまた外部から、警察から指摘を受けてという経緯だったと思いますけれども、調査をされたり、調査した結果として問題なかったということをNTT西日本さんとして報告を受けておられたかどうか。報告を受けられて、もし受けられていればですけども、どのように対応されたかということを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、NTT東日本様、お願いいたします。

【石井氏】　NTT東日本の石井です。契約前に関しましては、先ほど申しましたとおり、チェックリストを用いてということになるのですが、結局、森さんがおっしゃられるとおり、杓子定規な対応をしていれば、形上だけで、丸、丸で終わってしまうというようなケースは当然あろうということは想定されます。では、実際何をやるかというと、チェック項目をより具体的なアクションにつながるようにかなり細かく書いてあるというのが一つと、あと、我々は契約のときに、立入りで見に行ったり、または、契約が始まれば、期中、先ほど言いましたとおり、年間１回、点検に行くことにはしていますというところで、うそがあれば、そこでちゃんと見抜くという力を養っていく。その中で、結果的に大事なのは、我々社員が情報を本当に守ろうと思って、気持ちを込めて対応しているか。またはスキルを持った上で、契約の本当の穴を見抜ける、彼らが言っている、うそを見抜けるかというところが大事になってくるのではないかと思っていて、我々社員の意識に甘さがあると多分ぼけると思っていて、どちらかというと、我々は今、何をやろうと思っているかというと、我々社員のレベルやスキルをしっかり上げていくことで、そういった担保をできるよ

うなところをしていきたいなと思っておりまして、だまされないようにしっかり我々も力をつけていくというところをしっかり強化しているというようなことを実施しています。

【山本主査】　ありがとうございます。

それでは、NTT西日本様、お願いいたします。NTT西日本様に関しましては追加の質問もありましたので、そちらも併せて御回答いただければと思います。

【萬本氏】　１点目につきましては、先ほどNTT東日本からもありましたとおり、契約締結前ですけど、しっかりヒアリングを行うということもそうですし、社員の人たちが、一人一人が情報というのをしっかりと大切に扱うのだという気持ちを持ってやるということも大事ですし、期中の中で点検を、立入検査して、できているかどうかというのを確認していくということが大切だと思っています。

２つ目のグループガバナンスの話ですけども、規程類とか、先ほどのマニュアルとか規則とかそういったものについては、基本的にNTT西日本でつくったものに基づき、各グループ会社で、それをベースにして併せて規程類をつくっていっています。

なおかつ、今回、７月からセキュリティ＆トラスト部というのをNTT西日本の中につくったのですけども、NTT西日本の中のセキュリティ＆トラスト部がグループ全体のセキュリティガバナンスも見るようになっていますので、実態としてはどういうことかというと、例えばグループにセキュアFATというセキュアドPCを配布して、それで業務を行っていただいているんですけども、セキュアFATの挙動を、セキュリティ＆トラスト部において24時間365日監視しています。今回の不正事案を受け、内部不正の検知項目を追加して、確認しています。また、電気通信サービスについては、全て監視を行い、適切な運用がなされているかというところを見ていますので、その意味で、グループ全体としてもガバナンスを利かせているというのが現状です。

最後に、３点目のところですけども、もともとProCXが対応していたものについて、正直言うと、ＮＴＴ西日本に報告が上がってきていなかったというところが、これがまず第一、一番問題だと思っています。警察が入った後にこの報告が上がってきまして、そこで初めてＮＴＴ西日本として把握して、調べ始めました。その中で当時第三者的に、私は調査を行った側の立場ですけども、以前公表した社内調査委員会報告書にこれらの経緯を全部赤裸々に記載しています。

なぜこんなことが起こってしまったのかというところですが、電気通信サービスについては、しっかり監視をするなど、種々の対策をやっているんですけども、電気通信サービ

ス以外の各グループ会社の個別の事業についてはそこまでグループガバナンスが利かせられていなかったというか、監視できていなかった部分があって、各グループ会社が独自のサービスを行っていた。そこの領域まで踏み込んで、ちゃんとガバナンスを利かせないといけないなというのが今回の反省点であると思っています。

以上となります。

【山本主査】　ありがとうございます。森さん、いかがでしょうか。追加でも。

【森構成員】　御事情、よく分かりました。グループガバナンスはあったけれども、電気通信事業以外のところを適切に入れられていなかったということだったと思いますので、納得いたしました。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、次に、木村さん、お願いいたします。

【木村構成員】　木村です。御説明ありがとうございます。やはり１回、利用者の情報など出てしまうとなかなか、回収ということもできないですし、利用者にとってみては不信感が募るというところで、大変皆さん努力されていることはよく分かりました。漏えいについて質問したいのですけど、まずNTT東日本さんに、説明資料ではなくて、もう一つの資料で、「漏えい発生後の対応」とあるんですけれども、漏えい後の発生の対応について、NTT西日本さんのほうで、漏えい発生後に、漏えいした情報がインターネット上に流通していないかどうか検知する仕組みをもって運用していますとありますが、NTT東日本さんもこういうシステムをもって対応なされるということなのでしょうか。もしくは漏えいする前に、年に１回の点検とあるのですけれども、それ以外に何かモニタリングをするようなことはあるのかというのをNTT東日本さんにお伺いしたいと思います。

それからNTT西日本さんには、漏えいした情報がインターネットに流通していないかを検知する仕組みをつくって運用していますと。これは漏えい発生前もこういうことはなさるのかどうかお伺いしたいと思います。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、NTT東日本様からお願いいたします。

【石井氏】　NTT東日本です。まず漏えいが、本当に悲しいかな、出てしまった場合ですけれど、モニタリングであるとか、あと、OSINT調査はするようになっています。

ただ、当然ながら、出ないようにするためにしっかりルールであるとかセキュリティ対策というのは、我々としてはしっかり強化していきたいと思っていますので、そういうと

ころでも我々としても引き続き頑張っていこうと思っております。

【山本主査】　ありがとうございます。

木村さん、この点、いかがでしょうか。

【木村構成員】　もちろん出ないにこしたことはないのですが、ただ、いくら取り決めていても出てしまうことはあるかもしれませんので、そこをどう防いでいくのかというのも御検討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。

NTT東日本様、今の件、今の木村さんからの御発言に対してコメント等があればと思いますけど、なければ、そのまま次に行こうと思います。

【石井氏】　そうですね。出ないにこしたことはなくて、当然我々も出ないことになるように対応はしておりますし、よりシステム的な対応をすることのほうが、今、我々、ルールとしては、いわゆる人が見てとか、人がチェックしてという、かなり人力で、当然社員の育成も兼ねてボトムを上げようとはしておりますけれども、なかなかこの手の対応は、言い方は悪いですけれど、マネジメント上はどこか抜けるケースというのはあるのだろうというふうに思っているのは事実ですので、そこをいかに機械的に、何か変な作業をしたらアラームが上がるとか、または、作業をするにしても、必ず誰かが承認して、機械的に対処しないと次の工程に進まないとか、そういったものをいわゆる、危ない、リスクが高そうな業務であるとか行為に関して導入していくということで何とか防ぐというところを、しっかり対策としてお金をかけながらやっているというような状況でございます。

【木村構成員】　引き続き対策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、NTT西日本様、お願いいたします。

【萬本氏】　情報漏えい発生前の対策としては、たくさんやっていることはあるんですけども、例えばサイバーセキュリティ対策として、恐らくこれはバグがあるなとか、脆弱性があるなみたいな情報はやはりそれなりに開発者のサイトで出回ることがあるので、そういったところの情報を持って、それが正しいのかどうかを確認した上で、早めに対策を打てるものは対策を行っていくみたいな、ゼロデイが起こる前にプロアクティブに対応するみたいなこともやっていますし、そもそも内部不正みたいなものについては、先ほども申し上げましたとおり、内部不正に関する不正検知ルールみたいなものを追加して、それぞれの人たちが業務を行っているパソコンで何か不正な動きをしていたりすると、それを

検知して、アラートとして上げて、本人に、「こんなことしてなかった？」という確認を取ったりというのはできるような仕組みとかを導入していたりもしています。

【木村構成員】　分かりました。ありがとうございます。また考えられないような、いろいろな落とし穴というと変ですが、穴みたいなのがあるかと思いますので、ぜひまた対応を引き続きよろしくお願いいたします。

【石井氏】　かしこまりました。

【山本主査】　ありがとうございます。

それでは、江藤さん、お願いいたします。

【江藤構成員】　江藤と申します。本日は御説明ありがとうございました。私からは４点、質問がございまして、最初の１点目は、NTT西日本さんに、残りの３点は、NTT西日本さんとNTT東日本さん両方にお伺いできればと思います。

まず１点目、NTT西日本さんにですけれども、今回起きました漏えいの事故についてですけれども、外部サービス利用については委託に当たらないという認識だったということで、それが一つの事故の原因であったり、あるいはそれを気づくことに遅れたということに関わっていたと認識しているんですけども、今回の事故ですけども、例えば実際にこれが委託に当たると認識して、適切な契約書の定めをして、そして、今、委託元、さらには委託先における監督を徹底していれば防げていた事案だとお考えになるのか。それとも、どうしてもこういったことは持ち出しの事案ですので、ヒューマンエラーと言うのですかね。故意のエラーですけども、そういったものはどれだけ技術的、管理的なシステムが発展したとしてもどうしても防げないので、研修などを徹底する、あるいはしっかりとしたアクセス権限を付与するなどでしか防ぐことができないという事案なのかという点について、実務上の感覚も踏まえて教えていただければと思います。

２点目は、NTT東日本さんとNTT西日本さん両方にお聞きしたいんですけども、いわゆる再委託先を選定する際に、事前の同意が必要という運用だということでしたが、この際、事前に同意するかどうかを決定する際のレベルですかね。その選定のレベルというのは、御社が委託先を選定するものとやはり同じくらいのレベルのものを要求されているのでしょうか。これをお伺いする趣旨というのは、どうしても再委託の場合には、委託先から、こういったものを使いますということで、御社のほうに情報が入るのではないかと思っていて、選定のプロセスというのはある程度済んでいるようにも思いますので、その際に、ただの形式的な審査にとどまらず、実質的な審査までなされているかどうかということを

教えてください。

３点目は、外部記録媒体による持ち出しですけれども、これはNTT西日本さんのクエッションネア３－２、事前に御提出いただいた３－２を拝見いたしますと、「保守作業端末のみならず、委託業務にあたっては、原則、外部記録媒体利用を禁止しており、やむを得ず使用する場合は、事前に当社の許可を得ることを定めています」とあります。この「やむを得ず使用する場合」というのが、具体的に実務的にはどういうところを想定しておられるのかというのをNTT西日本さんにお伺いできればと思います。

また、同じ３－２の外部記録媒体の記述について、NTT東日本さんでは、電子媒体への出力規制を行うという記述がありますけれども、このことの具体的な意味についても簡単に教えていただければと思います。

長くなって恐縮ですけれども、最後は、アクセス権限の付与と、この認証の方法についても実務的運用ですけども、具体的にこれは認証というのを行う際にはいわゆる、私たちですと例えばカード認証とかパスワード認証、生体認証、IC認証、いろいろあると思うんですけども、どういった認証システムを取られているのかという点、また、アクセス権限というのは、いわゆるプロトコルで言うところのレベル４、３、２、１のような形で、それぞれの役職に応じて、どの程度の範囲でアクセスできるかというのをきめ細やかに設定されているのかという点についても教えていただければと思います。

以上、長くなりましたが、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、NTT西日本様にまずお願いいたします。

【萬本氏】　一番初めに御質問されたのというのが、今回のような事案について、今後起こり得るのかどうかといった話だったと思うのですけども、今回起こった事案というので、一番問題だと思っているのは、実際に犯行に及んだ人がやっている業務というのをマネジャーの人たちがしっかり管理ができていなかったものだという理解をしています。その意味で、人というところのマネジメントができていなかった。技術的な対策についてはもう既に入れ込んでいて、ログチェックというのはずっと行っていますし、共用のアカウントを廃止して、個々のアカウントに切り替えていますし、USBのような外部媒体の持ち出しというものはアクセス制限をかけていますし、そういった技術的な対策を行っていて、なおかつ先ほども申し上げましたとおり、個々の人たちが作業する端末、セキュアFATのほうで、内部不正も含めて、検知ルールを追加して、監視を行っているので、今現在、じゃあ、できるかと言われると、ほとんどのシステムではできない状態になっていると思って

います。ただ、ちょっと問題なのが、先ほども少し申し上げましたけども、子会社が行っている個別のサービスで、なおかつ、電気通信サービス以外の個別のサービスで、まだそこの監視まで行き届いていないものもやはり少なからずあるので、それらで情報漏えいが起こらないかというところについては、今まさに対策を進めているところになっています。その意味で、人という面と技術という面の両方で、今、対策を進めていますので、基本的には、ただ、技術的な対策でUSBの持ち出しを不許可にしているとか、多要素認証を使って、本人以外の人に成りすましができないようにしているとかいろいろな対策を打っているのが実情です。

２つ目の再委託に関しては、基本的には委託と同じルールに基づいてやっているので、具体的に言うと、例えば帝国データバンクの何点以上の委託先のみと契約するとか、幾つか検査項目とかもあるので、そういったところのチェック項目をクリアしたところじゃないと再委託先としては認められないとなっています。

３つ目の外部媒体、原則禁止で、やむを得ない場合という、その「やむを得ない」というのはどういうケースかというところですけど、例えば閉域で運用しているシステム同士をつないでデータを渡さないといけないときとか、要は、インターネットにつなぐほうが危険なので、閉域で運用しているんですけども、閉域で運用している間のデータを受渡しとかするときに、どうしてもUSBを使わざるを得ないケースがあるので、今、弊社としてどうしているかというと、今、データブリッジという製品とか、それは何かというと、USBのポートにそれぞれデータ転送する元と先のPC同士とかサーバー同士を接続して、そこの間だけデータを受け渡し、決まったデータだけ受け渡すといったことを行っていて、できる限りUSBメモリーみたいに、なくしてしまったり、容易に運べたりするものについては使わないようにしているというのが今の実情です。

最後に、アクセス権限ですけど、先ほど申し上げましたとおり、基本的には多要素認証を導入していますので、多要素認証で行って、成りすましとかを防ぐということをやっていたりしています。権限についても、マネジャーというか、どちらかというと、業務上割当てられた権限というのですかね、例えばオペレーターの人の権限はオペレーターの、その範囲のデータしか見えないようにしているとか、そういった形で権限管理とかをやっていたりしています。

以上でございます。

【山本主査】　ありがとうございます。

それでは、NTT東日本様、お願いできますでしょうか。

【石井氏】　NTT東日本の石井です。先ほどのNTT西日本の萬本さんとほぼ同じになるんですけれど、まず契約のレベルをどうしていますかというところですが、委託契約自体を当然承認する方がいらっしゃるんですが、その方が委託先も本当に間違いないかというのを確認するようにしていますので、委託先の承認だけレベルを落とすとかそういったことは一切ございません。ただ、形骸化するだろうとか、出来レースだろうということは危惧されますので、期中の点検に関しても必ず点検結果を見て、情報適正利用管理者を配置しており、情報適正利用管理者が見て問題ないという形になりますので、そういうところもミックスしながら、変なところと契約しないようにはしているという形でございます。

続いて、３－２のUSB、電子記憶媒体への出力規制というところでございますが、ソフトで止めるというのと、あと、物理的に閉塞するという感じですね。

NTT西日本さんと同じで、全てが必ず100％、閉められるものではないのはそのとおりですので、極力そういった閉める端末を多くして、この端末しかUSBは扱えませんよという最小限まで絞り込んだ環境下で運用対処をしていくということを実施することで、極力漏えいというのを避けていきたいと思っているというのがやり方でございます。

最後、４つ目のアクセス権限はNTT西日本の萬本さんと全く同じ回答になると思いますので。オペレーターであるとかダウンロードできる権限を極力絞り込んだ中で対応していくというやり方をしております。

【山本主査】　ありがとうございます。

江藤さん、いかがでしょうか。追加でも。

【江藤構成員】　とてもよく分かりました。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す。

すみません。私、今のお話を聞いて、ちょっとお聞きできればと思ったのが、NTT西日本様の検知システム、要するに、不穏な動作、動きをしていないかどうかをチェックするシステムというのと、NTT東日本様、今、御発言があった、閉めるというか、要するに、アウトプットというか、エクスポートできないようにするという仕組み。これは違うものになるのでしょうか。すみません。そこは技術的なところが分からなかったもので。

【萬本氏】　恐らく違うもののことを言っていると。

【山本主査】　違う。なるほど。

【萬本氏】　私が言っていた検知については、例えば10メガ以上のファイルを移そうと

したときにアラートが上がるとか、例えば退職１か月、退職者が１か月ぐらい前からはファイルのアップロード、ダウンロード、両方とも常に見張っておくとか、そういった検知のディテクトのほうを言っていて、東の石井さんが言われていたのは、どちらかというと、初めから、検知ではなくて、対策としてUSBを閉塞しておくとか。

【山本主査】　すごくプリミティブな仕方というか、そういう感じになるということですか。

【萬本氏】　そうですね。はい。

【山本主査】　ありがとうございます。これはNTT東日本様、すみません。私が伺っていなかったというか、聞き逃しているかもしれませんけど、この検知の仕組みについては、NTT東日本様は今、導入されているという理解なのでしょうか。

【石井氏】　そうですね。NTT西日本さんと同じですけど、先ほど私のほうで、自社システムに極力誘導していくようにすることで、大きく守りにいくという話をさせていただきましたが、自社システムであれば検知システムが入っておりますので、そこで検知するということも加味して守りにいく、大きく守りにいきたいという対応をしておりますので、我々も同じようなことを考えて実施している状況です。

【山本主査】　分かりました。

【石井氏】　あと、機器に関しては、個別ソフトだというのは萬本さんがおっしゃるとおり、別だと思っています。

【山本主査】　よく分かりました。ありがとうございます。

それでは、呂さん、お願いいたします。

【呂構成員】　御説明ありがとうございました。大変充実された監督体制を敷いていらっしゃるということがよく分かりました。その上で、NTT西日本様への御質問が一つと、あと、両社様への御質問が２つあります。１つ目、NTT西日本様への御質問ですが、漏えい事案に関するお話で、業務委託の場合には個人データの取扱い委託に該当する認識があった一方で、外部サービス利用の場合には、個人データの取扱い委託には該当しないという認識だったということですが、例えばクラウド例外に当たると思っていたとか、むしろ制度面で分かりづらいところがあったなど、何かこのように解釈してしまっていた理由などがあれば教えていただければと思いました。

２つ目、これは両社様への御質問ですけれども、委託先に対する立入検査を期中に必ず１回行われているということで、実際の件数も非常に多いですし、かなりコストのかかる

ことを実施されていて、素晴らしいと思いました。立入検査については、実際にお話しされて、うそを見抜くことが重要と考えていらっしゃるというコメントもあったのですが、どのくらいの深さで調査するのでしょうか。訪問して、委託先を選定するときと同様のチェック項目を単にインタビューすることにとどまらず、実際にシステムや入退室の管理状況を見るといったことまで行われているのかという、調査の深度についてお伺いしたく思いました。

３つ目も両社様への御質問ですけれども、再委託先の監督はやはり非常に難しい問題だと思っていますが、再委託先に対しても立入検査ができるようにしているということではあるのですが、これは御社におかれて実際に再委託先に対して立入検査を実施されたり、あとは委託先から再委託先に立入検査を実施させたりしているのでしょうか。再委託は関係がリモートに、遠くなればなるほど難しい問題だと思いますが、その辺りの実際の運用状況についてお伺いできればと思いました。お願いいたします。

【山本主査】　ありがとうございます。本質的なお話かなと思いました。

では、NTT西日本様、お願いいたします。

【萬本氏】　一番初めが外部サービスで、業務委託とは違って、ちゃんと認識が持てていなかったという点について、そもそもルールになっていなかったこと自体がおかしかったと認識しています。当然クラウドサービスを使ったら、データをそこにアップロードするというのも当たり前のことですし、そこから何らか漏えいが起こるという可能性があるからです。なぜそういうことが起こったのかというと、サイバーセキュリティを見ていた部署と規程を見ていた情報セキュリティ部というのはまた別に存在していて、組織が分かれていたことで、今回そういった事案が起こった一因はあると思っていたので、今回、セキュリティ＆トラスト部というのは、情報セキュリティとサイバーセキュリティを一つにした部署をつくったんですね。その意味で、もともと私は認識がありましたし、ルール化されていないのはおかしいと思っていたので、今はルール化しております。

【呂構成員】　ありがとうございます。大変よく分かりました。その後の部署を編成して、改善につなげたということについてもよく分かりました。ありがとうございます。

【萬本氏】　２つ目以降のところですね。立入りでうそを見抜けるのかどうかというところですけれども、実際に我々、今、セキュリティ＆トラスト部が実査を行っていって、各委託先のところとか、あと、自社内のシステムというのを実査しながらヒアリングとかをやっていて、そのノウハウを今度、業務委託を実施する現場の人たちにもノウハウを渡

してあげたり、あとは、もしできないのだったら、一緒にそれを確認しに行ったりというのをやっているのが今の実態です。

その意味で、見抜けるかと言われると、やはり経験というか、ノウハウを持っていないとなかなか難しい話なので、チェック項目だけでやる部分も当然ながらあるのですけども、重要なシステムとかの委託についてはしっかり我々も一緒になって、できているかどうかのチェックを含めて行っているというのが現状です。

最後３点目、再委託先の立入りについてですけども、こちらも実際やっておりまして、たとえば、今回のProCXとビジネスソリューションズについては、当然ながら、立入りどころか、対策も含めて委託元のNTT西日本で、対策のシステム面、技術面のコンサルも行い、実際にそれが運用上できているかどうかの確認も行っていますし、今、ログのチェックも行っています。

以上となります。

【呂構成員】　ありがとうございます。大変よく分かりました。

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

【石井氏】　NTT東日本のほうですが、立入検査のうそを見抜く力というのはやはりなかなか、おっしゃるとおりで、例えば点検項目も表面上確認することが書いてあるだけだと、杓子定規な対応となってしまうと思うんですけれど、実は我々のチェックシートは、目視により何とかシートを確認しろと、言い方はあれですが、具体的に結構書いています。ですので、これを見て、ちゃんと実施していると我々は信じていますので、それなりのレベルでうそを見抜く力は上がっていっているのだろうと思っているというのが一つです。

続いて、再委託先、ここに関しては我々も今、委託先に、基本的には同じことを実施してくださいということでお願いしている形なので、今後、我々としてもそこを強化していく、または、実際に我々も情報セキュリティ推進部として、先ほどのNTT西日本の萬本さんがおっしゃられたような調査を実施していますので、サンプリングで調査したり、再委託先に関しても、今後はより強化していくということを考えていかなければいけないと思っております。

【呂構成員】　ありがとうございます。大変よく分かりました。

【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。ありがとうございます。まず両社に３点、質問

がありまして、NTT西日本さんに１点、追加質問がございます。

まず１点目ですけれども、安全管理措置についてですが、去年の12月に、個人情報保護委員会の個人情報保護に関する法律についてのガイドラインの一部が改正されて、安全管理措置の対象として、個人データとして取り扱うことを予定しているものも含まれるということが明確化されたのだと思いますが、これはウェブスキミングに対する対応だと思いますが､このガイドラインの改正に対して追加的な安全管理措置を実施されたりですとか、委託先チェックシートのチェック項目を増やしたりですとか、そういった対応は何かされましたでしょうかというのが１点目です。

２点目ですけれども、個人データの取扱いの委託先については、御説明いただいたとおりしっかりと管理されているということは分かったのですけれども、個人データの取扱いの委託とはしていないけれども、個人データとか個人情報にアクセスできる事業者、アクセスしようと思えばできてしまう事業者に対してはどのように管理されているのだろうかというところが気になりました。

３点目、委託先の選定についてですけれども、両社ともチェックシート等を用いて確認しているということですが、確認の結果、審査NGになる割合はどの程度あるのだろうかというのが気になりました。あと、もし委託先として利用している、利用中の委託先が、委託先チェックでNGになった場合は、それが改善されるまではどういう対応をされているのだろうかというのが知りたいです。

最後に、NTT西日本さんに対して質問ですけれども、今回の情報漏えいに関して、委託先に対して改正後のルールを反映した契約に変更をいただいたというお話をされておりましたけれども、割と外資系企業、特に外資系のクラウドサービスはなかなか個別契約に対応してくれないみたいなのは僕も経験としてはあるのですが、そういったものも含めて、こういった改正後のルールを反映した契約に変更されるときに問題となったようなことがあれば、漠然とした質問で申し訳ないのですが、何か問題となったことがあれば教えていただければと思います。

以上です。

【山本主査】　ありがとうございます。

それでは､NTT東日本様からお願いできればと思うのですけれども､よろしいでしょうか。

【石井氏】　NTT東日本、石井です。まずウェブスキミング等の個人情報保護法の変更に関して、昨年12月のタイミングで変更されたことによりまして、私が冒頭説明させていた

だいた、三角形での基準とかマニュアルとかありましたけれど、あの中の基準を変えています。マニュアルの中にある、いわゆる様式のチェックシートに関しては、我々の個人情報保護ルール等に包含されていましたので、特に運用上、何か大きな変更点はございませんでしたので、そこのところは引き続き対応していくという形の中で守っていけるというふうに対応を決断しておりますというのが１点でございます。

続いて、２点目の個人データの委託、ここ、言い方が難しいですが、委託、個人情報に触れるのだけど、委託としていないみたいな、表現が難しいんですが、もし、例えば具体的に、私が違ったら申し出ていただければいいと思うんですけれど、クラウドサービスみたいな形で、いわゆるサービス利用契約で締結していて、実は個人データをクラウド事業者が触れちゃうんだけど、我々が気づかなかったというようなケースなのかなというふうに思って、簡単に答えをさせていただくと、そのケースは事前に必ず見つけて、個人情報の移転があるのであれば覚書を結んでくださいという言い方をしていますので、いわゆる利用規約だけではない、我々のルール側に倒してくるという対応を今しています。今回の調査でも、そういったところをちゃんと調べて対応している実態を確認しているという状況です。

最後、３つ目、委託先のチェックシートによる審査NGについてですが、割合等に関しては、我々、情報セキュリティ推進部では会社全体を一元的に把握できていません。各組織の契約対応の中で、何回も何回も往復しているということはあるとは思うのですが、その割合までは把握していません。ただ、我々が把握しているチェックシートの中では、いわゆる改善予定日はいつですか、駄目な場合はいつから直りますかというのを必ず記載するようになっていますので、その中でこの項目であれば、いわゆる何月までに直れば、では、いいです、ローンチまで間に合うので大丈夫とか、そういう判断を多分したりしながら実際は対応しているのだと感じておりますというのが回答になります。

【山本主査】　ありがとうございます。

それでは、NTT西日本様、お願いいたします。

【萬本氏】　１点目、２点目については、NTT東日本の石井さんがおっしゃってくださったとおりです。３点目のところですけども、実態としては、それぞれ委託先NGになるケースの場合は、委託先、ここにしようとか、切り替えて、現場のほうで契約しないといけないので、切り替えていっているので、その意味で、オーケーのものしか我々としては見ていないですし、途中段階で、ここは駄目だったというところまでのパーセンテージとか取

っているわけではないので、申し訳ないのですけども、そこの割合というのは分からないというのが実態です。

最後の外資系クラウド事業者が個別契約を締結してくれない件については、クラウド例外の考えに基づき、個人情報を取り扱っていない事業者と判断し個別契約を締結しないケースはございます。

【太田構成員】　ありがとうございます。今の点に関して、要するに、クラウド例外、取り扱っていないから違いますみたいな話を、先ほどの個人データの取扱いの委託とはしていないが、個人データや個人情報にアクセスしようと思えばアクセスできる事業者みたいなふうに置いているのですけれども、じゃあ、そういったのは一応把握はしていて、個人データの取扱いの委託として契約を結んだり､チェックシートは通っていないけれども、ちゃんと把握はして、管理はされているという認識で合っていますでしょうか。

【萬本氏】　リストで管理しています。

【太田構成員】　それはNTT東日本様も同様ということでしょうか。

【山本主査】　NTT東日本様、いかがでしょうか。

【石井氏】　我々のほうは、調査をして、今のところ、そういったクラウド例外になるような契約はないという、クラウドサービスですけど覚書を結んでいるケースしかなかったので、今のところ、変なことにはなっていないというところなのですが、それを全てデータベースとして、この契約を毎年更新して、これはクラウド例外なのにやっていないという管理まではまだできていないです。

【太田構成員】　ありがとうございます。もう１点追加で質問ですけれども、先ほどのNTT西日本さんの御回答では､委託先チェックでNGとなったから､もう委託先を切り替えるみたいなお話をされていましたが､NTT東日本さんの場合は､いついつまでに対応するみたいなのを確認しているというお話だったのですけれども､その｢いついつまでに対応する｣の対応するまではNGの状態で委託先を利用するというようなイメージでしょうか。

【石井氏】　NTT西日本と同じように､別の委託先を考えるとか､対応を変えるというのもありますし、どうしてもそこがノウハウを持って代えがたしという状況であれば、スケジュールを遅らせるか、または最悪、どこまでリスクがあるかというのを考えながら、全ての項目、100％できなきゃいけないというものではなくて、必須・推奨項目というのも当然契約の中にありますから、その重みを考えながら、リスクテイクしながらやっていくということもあると認識しております。

【太田構成員】　ありがとうございます。以上です。

【山本主査】　ありがとうございました。

それでは、引き続き、生貝さん、お願いいたします。

【生貝主査代理】　丁寧な御説明ありがとうございました。一つは、森先生から先ほどあったグループガバナンスについてお伺いしようかと思ったのですけれども、それは既にお答えいただきましたので。もう一つは、今回、特に、NTTビジネスソリューションズへの派遣社員の方が直接的な、こうした行為を行ってしまったということ、同様のケースはやはり古くは､それこそベネッセでしょうか｡あるいはさきの東京都のHER－SYSの件含めて、やはり生じる場合があるのかなと思います。

そうしたときに､当然やはり､特にコールセンターに関わるようなところを含めて､様々な外部のお力というのをスポット、短期で人材をおかりしてくることというのは大変重要であり、ただ、他方で、やはりそれまでに受けている訓練ですとかエクスパティーズ、あるいは時間の短さといったようなところを含めて、やはり少し違ったトレーニングや対応というのを受け入れる元のほうでもしていかなければならないことがあるのかなと想像したときに、特に派遣会社さんですとか、そういった方たちとのやりとりですとか、あるいは、スポットで来ていただける社員の方々に対する特別なトレーニングといったようなことを、何か特に気をつけていることですとか、仕組み上、つくっていることがあれば教えていただければと思います。

【山本主査】　では、西日本様、お願いいたします。

【萬本氏】　そもそもコールセンターのようなところに関しては、例えばスマホなどの持込みを禁止しているとか、持ち込む鞄は透明な鞄じゃないと駄目とか、業務に入る前に当然ながら情報セキュリティの研修、勉強会を行ってから、同意書を取って、本人がそういう情報の漏えいをしないことであったり、あと、業務上知り得た情報を外でしゃべったりしないなどを順守する誓約書を書いてもらいますし、勉強会もしますし、先ほど言ったとおり、技術的な対策で監視カメラを置いていたりとか、その人の作業記録というのが残っていたり、録音されていたり、いろいろな対策をやっているというのが実態です。

【生貝主査代理】　ありがとうございます。特に一つ重要な論点かと思いましたので、お伺いいたしました。ありがとうございます。

【山本主査】　ありがとうございます。

ほかはいかがでしょうか。生貝さん、以上で大丈夫ですか。はい。ありがとうございま

す。

一応私の見る限り、１周は終えたのかなと思うのですけれども、まだ時間はございますので、追加で御質問、コメントがあればと思いますけれども、いかがでしょうか。

はい。では、寺田さん、お願いいたします。

【寺田構成員】　何度もすみません。もちろん問題を起こさないようにすることが最も重要であることは間違いないのですが、どんなにリスクマネジメントを強化しても、やはり問題は起こり得るという、そういう考えというのがやはり必要なんじゃないかなと思っています。

その際に必要なことというのは、いかに被害を最小化するか、二次被害を防ぐか、被害対策はなかなか難しいと思いますが、そういったことを考えないといけないと思うのですが、この辺に関して、委託先と何らか契約というのは結ばれていますでしょうか。もっとも、これは全て委託先の責任でちゃんとやれよと言っても、規模の問題も含めて相当難しい問題だと思いますので、委託元であるNTTさんでも何らかの対策というのが必要になるのかなと思っていますが、その辺りというのはどのようになっていますでしょうか。これは両社にお聞きしたいと思います。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、NTT東日本様、いかがでしょうか。

【石井氏】　おっしゃるとおりで､極力起きないように我々としては対策を打ちながら、正直、悲しいかな、起きるときは起きるというふうに、それは我々も理解して、マネジメントをしています。ですので、起きないことを想定するというよりは、起きることを想定した中で対策を取っていくというのも実態としてはあります。

委託契約に関しては、まず覚書の中で、委託先に対して何か有事、インシデントがあれば速やかに我々に報告する義務を必ず負うように、それは契約書の中に記載することによって意識づけをしっかりするというところで、まず最低限の担保は取っていますし、我々社内の中も多分、委託先、委託をやっている方々は業務が中心ですので、その影響がどこまで出るかというのはなかなか、情報漏えいに関しては分からないところがあります。その際は、逆に我々情報セキュリティ推進部のほうにすぐにエスカレーションするというのは、もうこれは日々訓練していますので、情報を我々としてもすぐ収集しながら、あまり影響が大きくならないように我々としても対策を取っていくというようなことを心がけております。

【山本主査】　ありがとうございます。

それでは、NTT西日本様、いかがでしょうか。

【萬本氏】　先ほどNTT東日本の石井様からあったとおりだと私も思いますし、西としても同じことをやっているのですけども、もともと委託先で環境も整備した上で、全部、業務も含めて渡しているケースについても、先ほど言ったセキュアFATみたいなものをこちらで貸与して、その上で業務をしてもらうことによって、そもそも情報漏えいを起こさないようにして、御指摘いただいたのは事後の話ですけど、事前の防御も高めるような営みも現在進めていたりはしています。

【寺田構成員】　ということは、事後の対策というのはそれほど強化されていない。ということはないとは思うのですけども。

【萬本氏】　いえいえ。そういう意味で、NTT東日本の石井さんがおっしゃってくださったとおりで、事後のところについては、ちゃんと契約上、縛っていたり、そこについてもいろいろやってはいるものの、事前も含めて、併せてセットでやっているという形です。

【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。

ほかの方、いかがでしょうか。

もしなければ、私のほうから。非常に単純な質問をさせていただければと思います。研修が具体的にどのようになされているのかということと、研修をしたり、同意書を取るような意識づけみたいなことを一方でやるというところはあるかと思うのですけれども、これの効果はどうなんでしょうか。テストをするわけではないと思うのですけれども、どれぐらい効果があるというふうにお感じになっているかということが１点目です。

これは非常に定性的な話なので難しいかもしれませんけれども、どういう研修をすれば、そのような意識が高まっていくとか、その辺の御経験やお考えがあれば伺いたいと思います。さはさりながら、さっき生貝さんからもあったとおり、派遣の方ですとか、スポットでという方はなかなかその意識が醸成されにくい。また、性悪説じゃないですけれども、そもそも持ち出そうという意図、目的を持って入ってきてくるというところでは、あまりそういう意識づけみたいなことは効果がない。そういうところでは、システムによって縛っていく、検知システム、アーキテクチャで縛っていくということが重要になると思います。実際には研修のような意識づけとの組合せなのかなと思って伺っていましたが、このシステム的な管理も今後非常に重要になってくるというところで、それを妨げる要因はど

こにあるのかを伺いたいです。例えば、同じシステムを使わせれば、委託元がリアルタイムで委託先､あるいは再委託先をモニタリングできるということだと思うのですけれども、これが進まない理由、これを阻むものが何なのかと。システムを共有すれば、グループで一体的にモニタリングしていけると思うのですけれども、現状、そうなっていない理由というのは、単にコストだけの問題なのか、もうちょっと違う理由があるのか。その辺り、ちょっと伺えればなと思いました。

すみません。雑駁な御質問ですけれども、NTT東日本様、いかがでしょうか。では、NTT西日本さん、先にオンにしていただいたので、すみません。NTT西日本様からお答えいただければと思います。

【萬本氏】　まず研修についてですけども、今回、我々、漏洩事案を発生させたこともあり、今までも経営層向けとか、管理者向けとか、全社員向けとか、システム主管、業務主管向けとか、いろいろな階層別で情報セキュリティに関する研修というのをやっていたのですけど、今回、新しい研修を導入しまして、何かというと、先ほどのチェックシートを〇、〇として、「オーケー」と言って、最後、「サインを書いて」と言われて、サインを書く管理者の方、担当部長とか部門長クラスの方ですけど、そういった方々に、自分が持っているシステムであったり、情報というのがそもそも漏えいした場合であったり、内部不正で持ち出された場合、どういうことが考えられるのか。持ち出し方、どういうものがあるのか。リスクとしては何が考えられるのか。どういう対策を打つべきなのかみたいなのを自分で考えてもらって､それをお互い持ち寄って､グループディスカッションをして、発表していただく研修を新しく立てつけました。

今まで結構､担当者任せになっていたり､派遣社員任せになっていたりというのが結構、問題の技術的な対策以外のところの人という部分、もともと情報セキュリティ、人とルールと技術の３つをバランスよく、ちゃんと見ていくことですけど、人というところがどうしても弱くなってくるので、研修で自分事として扱ってもらうという考え方の定着化を図っています。あとは、どうしても派遣社員の人たちとか含めて、ちゃんとその人とコミュニケーションを取って、業務を見ているかというと、すぐ入れ替わるから、まあ、いいやとなってしまうケースは多いと思うのですよね。

なので、しっかりコミュニケーションを取ってもらうようにするといったところを研修の内容に加えました。その結果、今まで業務主管とかシステム主管といった人たちが、研修をすると大体、四、五百人ぐらい出ていたのが、今、2,000人ぐらい出るようになってい

るので､大分意識は変わってきているのではないかなと思いますというのがまず一つです。

２つ目がモニタリング。さっきも、我々ずっとモニタリングをするようにしていて、監視して、対応していますし、そもそも派遣社員の人たちは、さっきも言っていたとおり、センターに入る前に入り口に監視カメラがあって､スマホなどの持込みができないように、ボックスの中に、全部鍵とかも含めて入れ込んで、透明なバックの中に持ち込むものだけを全部入れて持ち込むという、物理的なセキュリティ対策もやっていますし、アクセス権の設定で、その人がアクセスできるお客様情報というのは、自分が扱うものにしか行かないようにしていたり、そういう技術的な対策を行っていますし、誓約書といった形で、自分が知り得たものを出さないことも書いていますし、幾つかの、人に対する教育、技術的な対策、物理セキュリティを組み合わせてやっているのが今の実態です。

【山本主査】　ありがとうございます。検知システムが働くようなシステムを委託先でも使ってもらえれば、委託元がリアルタイムでモニタリングしていける。そういう意味では、委託先にはそれを使ってもらうということが重要かなと思ったんですが、ここ、全てがそれを使っているわけではないという、さっき御回答もあったかと思うんですけど、その辺の理由というのはどの辺りにあるのかというところはいかがなのでしょうか。

【萬本氏】　業務を丸投げしていた部分があるというのも一つの原因じゃないかと思っていて、ちゃんと業務を責任持って、環境まで用意した上で、そこのマネジメントを含めてちゃんと見るという考え方を持ってやっていけば、恐らくできる部分が多いと思うんですよね。さき程も申し上げましたとおり、丸投げ体質みたいなところがあったりすると、もう全部投げちゃったから、もう相手の責任だみたいな、そういったマネジメントの仕方をすると、さっきおっしゃられていたように、委託先のほうが勝手に全部やって、モニタリングもしないし、何をやっているのか分からない状態になるというのが実態じゃないかなとは思います。

【山本主査】　ありがとうございます。大変よく分かりました。特に研修のところの、ある種、ハッカソン的なというか、非常に能動的な研修のプログラムについても御紹介いただいて、大変勉強になりました。ありがとうございます。

それでは、NTT東日本様、いかがでしょうか。

【石井氏】　我々も人に関しては非常に大事だと思っていまして､研修に関しては当然、年１回とか、あと、新規で入ったタイミングで必ずやるということは、それはルール化しているというのは、先ほど申したとおりですけれど、実際、研修の資料とか、このレベル

を合わせていかなきゃいけないと思っていますので、我々はその資料も共有して、これを使って、こういう研修をしたほうがいいというのは、ある程度併せながら対応させていただくことで、各人のセキュリティレベルを必ず上げていこうというところが、地道なやり方ですけれども、あるかなと思います。また、権限については派遣の方とか、就業する業務にあわせて必要最小限の権限しか与えないようにしています。すべての人に危険な行為が可能な権限は与えない。萬本さんもおっしゃられたような環境的な対策とか、携帯を持っていかないとか、そういうことはしっかり実施しながら、先程のような対応を取っていくことで担保しているというのがやり方かなと思います。

続いて、システム面のところですけれど、我々も、理想としては、本来、我々が全て管理できる状況下において委託できているのが、正直言うとやりやすいし、安心だしというのはあると思います。ただ、委託先の業務の効率性とか、委託先がこういうふうに考えたとき、俺たちはこうやりたいんだというのを我々がそこまで強制できるものではないのが事実なので、例えばで言いますと、我々が持っているデータベースのある業務システム等は、我々が張り出して、お貸し出しするようなことでしっかり担保するんだけれども、彼らが加工して使うようなOA端末、いわゆる普通のパソコンとか個人の端末、これらに関して、そこまで我々縛りをかけて、同一環境下に持っていきたいというふうに動いてはいるんですが、そこまでなかなか進まないのは、やはり先ほどのお金の面であるとか、各社が持っている資産なのに、我々がその上にかぶせて、この端末を使えというふうに言い切るとか、なかなか難しいというのも実態としてはあると思っていますので、方向としては進めたい方向だけれども、なかなか進まない実態というのはそういうところにもあると感じます。

【山本主査】　大変ありがとうございました。よく分かりました。ありがとうございます。

まだもうしばらく時間ありますけれども、ほかの方、いかがでしょうか。もう少しここは詳しく聞きたいとか、せっかくの機会ですので、何かあればと思いますが、いかがでしょうか。よろしいですかね。今のところ、特にお手が挙がっていないように思いますけれども、よろしいでしょうか。

それでは、NTT東日本様、それから、NTT西日本様、本当にありがとうございます。お取組、大変よく分かりましたし、今後とも利用者情報の保護につきましては、できる限り対策を講じていただきたいと、引き続き保護のレベルも引き上げていただければと思います

ので、引き続きどうぞよろしくお願いいたします。ありがとうございました。

それでは、事務局から連絡事項をお願いいたします。

【小玉利用環境課課長補佐】　事務局でございます。次回の会合ですけれども、11月15日、今週の金曜日でございます。13時から、NTTドコモ、ソフトバンクのヒアリングを予定しております。

本日の議事録につきましては、事務局で作成の上、皆様に御確認いただいた後、例によって公表することを予定しております。よろしくお願いします。

以上です。

【山本主査】　ありがとうございます。

それでは、予定していた時間より少し早いですが、以上で、利用者情報に関するワーキンググループ第14回会合を終了とさせていただきます。本日はお忙しい中、御出席いただきまして、どうもありがとうございました。

以上