資料16－4

大手通信事業者における個人データの委託先の監督等について

〇昨今、電気通信事業者において、委託先を通じて大量の個人データの漏えいが発生する事案が複数発生しております。

〇個人データの取扱いを委託する場合には、委託先の選定、委託契約の締結及び委託先における個人データ等の取扱状況の把握等、委託先に対する必要かつ適切な監督を行う必要がありますが、昨今の事案においては、

・個人データの取扱いの委託が行われているにもかかわらず、委託先と再委託先の間の契約が業務委託契約ではなく、外部サービス利用契約であったことから、再委託の事実の把握や再委託先における個人データの取扱状況の把握が十分に行われていなかったケース

・個人データの委託先（再委託先を含む。）において、外部のクラウドストレージへのアクセスや外部記録媒体の利用が可能となっており、それらを通じて個人データが不正に持ち出されるなど、物理的安全管理措置、技術的安全管理措置等が不十分となっていたケース

など、委託先の監督が不十分であることに起因して、個人データの漏えいが発生しているケースが見受けられました。

〇特に、外部サービス利用契約については、同様の契約形態に伴う個人データの取扱いの委託が他の事業者においても行われていることが想定されるところ、個人データの取扱いを伴う外部サービス利用契約に係る認識や個人データの漏えい対策等を確認するため、今般、大手通信事業者における状況についてヒアリングを行うこととしました。

〇つきましては、以下の各項目について、委託先の監督に関する貴社の取組・状況をご記載ください。

社名		楽天モバイル株式会社
１．委託先について		
1-1.	個人データの取扱いの委託（再委託）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	以下の委託業務において、契約者の氏名・住所・電話番号・メールアドレス等の取り扱いを委託しています。 ・店舗の運営に係る代理店業務

	いるのか、代表的なものを可能な範囲で記載すること。	・サポートセンター業務 ・郵送に関する業務
1-2.	個人データの委託（再委託）について、委託先との間の契約形態にはどのような種別があるか（業務委託、定型のサービス利用規約に基づくもの等）。	大別して以下 2 種の契約形態があります。 ・業務委託契約 ・外部クラウド利用契約
２．委託先の監督について　※1-2 の契約種別毎に異なる場合は、種別毎に一般的な内容を記載すること（様式別途でも可）。		
（１）外部サービス利用に対する認識		
2-1	個人データを取り扱う情報システムに外部サービスを活用する場合において、当該外部サービスの提供者が当該個人データを取り扱う場合、個人情報保護法上の委託に該当するものとして扱っているか。	個人情報保護法上の委託に該当するものとして、扱っております。
2-2	2-1 の回答が「個人データの委託として扱っている」の場合、個人データの取扱いの委託先における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ついて、契約上どのように担保されているか（外部サービス利用	個人データの取扱いの委託先における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ついて、委託先と締結する「個人情報の取扱いに関する覚書」で定めることで担保しております。以下に、覚書における記載の例を示します。 ---------- ◆安全管理措置について（甲：楽天グループ株式会社　乙：委託先）

	契約又はそれに付随する覚書等における標準的な記載の例を示すこと）。	原契約の目的を達するために委託される個人データを、違法な取扱いから保護するため、取扱いに係るリスク及び保護される個人データの性質に対して適切な技術的及び組織的安全管理措置を講じること、並びに、甲より当該技術的及び組織的安全管理措置にかかる基準が提示された場合、当該基準を遵守すること。なお、甲及び乙による別途の合意がない限り、甲が、データ内容の正確性の確保に努めるものとする。さらに、外国において個人データを取り扱う場合、当該外国の個人情報の保護に関する制度等を把握した上で、個人データの安全管理のために必要かつ適切な措置を講じるものとする。 ―――――――――――――――――――――――――――――――――――― ◆再委託の条件、再委託先の監督等について（甲：楽天グループ株式会社　乙：委託先） 乙は、甲の事前の書面による承諾を得ることなく、甲から委託された業務の一部または全部を委託してはならないものとする。乙が本覚書に基づく業務を甲の承諾を得て再委託する場合、乙は、再委託再委託先に本覚書で乙に課されているのと同等の義務を書面により義務付けるものとし、再委託先が当該書面に基づく個人データ保護の義務を履行しないときは、乙は当該不履行につき直ちに甲に報告するとともに、再委託先の義務の不履行については甲に対し全責任を負う。
2-3	個人データの取扱いの委託先が、当該個人データを取り扱う情報システムに外部サービスを活用する場合において、当該外部サービスの提供者が当該個人データを取り扱う場合、個人情報保護法上の再委託に該当するものとして扱っているか。	個人情報保護法上の再委託先に該当するものとして扱うこととしています。

2-4	2-3 の回答が「個人データの再委託として扱っている」の場合、個人データの取扱いの委託先による再委託先の監督や、貴社による再委託先の監督について、契約上どのように担保されているか（外部サービス利用契約又はそれに付随する覚書等における標準的な記載の例を示すこと）。	以下に、覚書における記載の例を示します。 ---------- 乙が本覚書に基づく業務を甲の承諾を得て再委託する場合、乙は、再委託再委託先に本覚書で乙に課されているのと同等の義務を書面により義務付けるものとし、再委託先が当該書面に基づく個人データ保護の義務を履行しないときは、乙は当該不履行につき直ちに甲に報告するとともに、再委託先の義務の不履行については甲に対し全責任を負う。
（２）委託先の選定		
2-5	個人データの取扱いを委託する場合において、委託先（再委託先を含む）の選定にあたり、個人データを適切に取り扱うための安全管理措置が講じられているかについて確認を行っているか。確認を行っている場合、具体的にどのような項目を、どのような方法で確認しているか。 ※1-2 の種別で差異がある場合には、それぞれ記載すること。	当社では、委託先の選定にあたり、個人データを適切に取り扱うための安全管理措置が講じられているかを確認するため、委託先にセキュリティチェックシートへの回答をお願いしております。 <委託作業型> ①全社的な情報セキュリティ体制について（確認項目：20 項目） ②作業場所・委託業務に関する情報セキュリティについて（確認項目：9 項目） ③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（確認項目：14 項目） ＜クラウドサービス型＞ ①情報セキュリティおよび個人情報保護管理体制（確認項目：9 項目） ②サードパーティー管理（確認項目：4 項目） ③アクセス制御（確認項目：6 項目） ④アプリケーションセキュリティ（確認項目：2 項目） ⑤運用セキュリティ（確認項目：10 項目）

		⑥データ管理（確認項目：4 項目） ⑦情報セキュリティインシデント対応（確認項目：3 項目） ⑧ネットワークセキュリティ（確認項目：4 項目） ⑨物理セキュリティ（確認項目：8 項目） ⑩コンプライアンス（確認項目：3 項目）
2-6	個人データの取扱いの委託先の選定にあたり、委託先（再委託先を含む）における教育体制（教育対象の社員の範囲、研修の有無、理解度の確認、研修内容の見直し、頻度等）について、どのようなものを求めているか。 ※1-2 の種別で差異がある場合には、それぞれ記載すること。	委託先と締結する「個人情報の取扱いに関する覚書」にて以下を定めており、かつチェックシートでも教育の実施につき確認を行っている。 ---------- 以下の事項を担保すること a. 乙の従業員（甲から提供を受けた個人データを取り扱う者に限る。本覚書で許容される範囲において、再委託先も含む。以下本号において同じ）が個人データの機密性を認識していること b. 乙の従業員が個人データの取り扱いに関する教育を受講していること c. 乙の従業員が本覚書に基づく乙の義務並びに従業員個人の職務及び義務について認識していること d. 個人データにアクセスする乙の従業員の信頼性を乙において合理的に確認した上で個人データへアクセスさせること
（３）委託契約の締結		
2-7-1	個人データの取扱いに係る委託契約（再委託契約を含む）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。 ※1-2 の種別で差異がある場合には、それぞれ記載すること。	2-2 記載の内容と同じ。個別具体的な事項はチェックシートでカバーされている。

2-7-2	自社の個人データの取扱いを委託している場合において、1-7-1 のとおり委託契約（再委託契約を含む）に定めた事項について、契約書締結以外の方法により実運用上行っている措置はあるか。 ※1-2 の種別で差異がある場合には、それぞれ記載すること。	当社では、契約書締結以外の方法では、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して、委託先との契約形態に関わらず、全ての委託先に対して、2-5 と同様の情報セキュリティチェックシートを用いて審査をしております。
2-8	個人データの取扱いの委託先が再委託を行う場合、委託先に対してどのような対応を行っているか（再委託を承諾する基準等の再委託条件、委託先による再委託先の管理監督の実施状況の把握方法等）。 ※1-2 の種別で差異がある場合には、それぞれ記載すること。	「個人情報の取扱いに関する覚書」にて、再委託先にも委託先と同等の条件の適用を義務としている。
（４）個人データの取扱いの委託先における個人データの取扱状況の把握		
2-9	個人データの取扱いの委託先（再委託先を含む）における個人データの取扱状況について、どのように把握し、監督を行っているか。 ※1-2 の種別で差異がある場合には、それぞれ記載すること。	委託先(再委託先を含む)における個人データの取扱状況について、委託先との契約形態に関わらず、2-5 と同様の情報セキュリティチェックシートで把握しております。また、年に 1 度、委託先に対して 2-5 と同様のチェックシートの記載内容に変更がないか確認を行っております。

2-10	個人データの取扱いの委託先（再委託先を含む）における個人データの取扱いの監査・点検の内容、方法及び頻度並びに 2023 年度の実施件数（書面点検・立ち入り調査の各件数）。 ※1-2 の種別で差異がある場合には、それぞれ記載すること。	当社では、委託先（再委託先を含む）における個人データの取扱いについて、2-9 で回答した通り、委託先との契約形態に関わらず、年に 1 度、委託先に対して 2-5 と同様のチェックシートの記載内容に変更がないか書面点検を行っております。2023 年度の実施件数は [redacted]件となり、立ち入り調査は行っておりません。書面点検の内容は以下の通りです。 ---------- <書面点検の内容> ・委託先(再委託先を含む)の業務場所が当社社内の場合 ①全社的な情報セキュリティ体制について（確認項目：5 項目） ②作業場所・委託業務に関する情報セキュリティについて（確認項目：2 項目） ・委託先(再委託先を含む)の業務場所が委託先等の施設の場合 ①全社的な情報セキュリティ体制について（確認項目：20 項目） ②作業場所・委託業務に関する情報セキュリティについて（確認項目：9 項目） ③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（確認項目：14 項目）
（５）個人データの取扱いの委託及び再委託の実施状況		
2-11	電気通信事業に係る個人データの取扱いの委託先及び再委託先の件数。 （内数として以下を記載） ・外部サービスの利用 ・親会社、連結子会社に係るもの	電気通信事業に係る個人データの取扱いの委託先及び再委託先との契約を[redacted]件、締結しております。 外部サービスの利用や、親会社・連結子会社に係るものの内数については、[redacted]

2-12	個人データの取扱いの委託先（再委託先を含む）における、個人データの取扱いに係る契約違反の件数（2023 年度）。 ※1-2 の種別で差異がある場合には、それぞれ記載すること。	[redacted]
３．その他		
（１）物理的・技術的安全管理措置		
3-1	委託先（再委託先を含む。）において、外部からの不正アクセスによる個人データの漏えいを防ぐため、どのような安全管理措置を講じているか。特に、個人データにアクセスする場合の従業員の認証等、技術的安全管理措置をどのように講じているか。	外部からの不正アクセスによる個人データの漏えいを防ぐため、委託先には当社の PC およびネットワークを提供し、その利用をお願いしております。 当社の PC およびネットワークには、技術的安全管理措置として以下の 2 つのセキュリティソリューションを導入しております。 また、委託先が自社の PC およびネットワークを使用して当社の情報にアクセスする際には、リモートデスクトップ経由での接続をお願いしており、その際の操作ログは保存しております。 ---------- [redacted] [redacted]

3-2	委託先（再委託先を含む。）において、内部からの不正な持ち出しによる個人データの漏えいを防ぐため、どのような安全管理措置を講じているか。特に、実際に不正な持ち出しを行おうとした場合に、それを阻止するための物理的・技術的安全管理措置をどのように講じているか 少なくとも以下の内容については、具体的に対応状況の回答をお願いします。 -許可されていない外部ストレージへのアクセスが可能となっていないか - 保守作業端末にダウンロードが可能になっていないか - 保守作業端末に外部記録媒体を接続し、データを持ち出すことが可能になっていないか - セキュリティリスクが大きいと想定される振る舞いを即時に検知できているか - 各種ログ等の定期的なチェックは十分か	委託先における、内部からの不正な持ち出しによる個人データの漏えいを防ぐため、技術的安全管理措置としては、3-1 の回答の通り、2 つのセキュリティソリューション[redacted]を導入した PC およびネットワークを委託先に提供しております。 また、物理的安全管理措置に関しては、当社が以下の通りに定めており、委託先の業務場所が当社外にある場合は、2-5 のセキュリティチェックシートを通じて、当社の定める物理的安全管理措置が適切に施されているか確認しております。 具体的な対応状況についても以下に記載いたします。 ---------- ＜物理的安全管理措置＞ (1)情報システムのインフラの物理的境界線には、許可を得ていない者が立ち入ることはできません。 (2)当社の施設に立ち入るスタッフ及び訪問者に ID バッジを発行する等、適切かつ分かりやすい識別方法を確立し、関係者のみが当社の施設に入館できるよう承認手順を作成しております。 (3)情報を取り扱う区画を定義し、適切な入退室管理により保護することや、物理的な訪問者記入帳や電子的な監査証跡を確実に利用してモニタリングを実施しております。 (4)機密性の高いパーソナルデータを取り扱う、全ての区画には、侵入検知システムを設置しております。 (5)施設への不正侵入を防止するため、物理的な障壁を設けております。 (6)無人の機密性の高いパーソナルデータを取り扱う区画は物理的に施錠して定期的に点検しております。 (7)自動消火装置、閉制御の専用空調設備、無停電電源装置（UPS）をサーバルームに設置しております。

		(8)外部のサポートサービス担当者に立ち入りを許可する区画を制限しております。 ＜対応状況＞ ・許可されていない外部ストレージへのアクセスが可能となっていないか →[redacted]により、許可されていない外部ストレージへのアクセスを検出しております ・ 保守作業端末にダウンロードが可能になっていないか →[redacted]により、ダウンロード防止に努めております ・ 保守作業端末に外部記録媒体を接続し、データを持ち出すことが可能になっていないか →[redacted]により、データの不正な持ち出しを防止しております ・ セキュリティリスクが大きいと想定される振る舞いを即時に検知できているか →[redacted]実装をしており、検知に努めております ・ 各種ログ等の定期的なチェックは十分か →各種ログのチェックを十分に行い、内部からの不正な持ち出しによる個人データの漏えい防止に努めております
（２）委託に関する利用者への説明		
3-3	個人データの取扱いを外部へ委託することについて、利用者に対してどのような説明を行っているか。	当社では、個人データの取扱いを外部へ委託することについて、Web サイト上で説明しております。Web サイトリンク、説明箇所は以下の通りです。 ---------- ＜Web サイトリンク＞ 電気通信事業における個人情報の取扱いについて

		https://corp.mobile.rakuten.co.jp/guide/privacy/telecom/index.html#privacy04 ＜掲載箇所＞ 個人情報等の利用　－　4.委託先等による利用
（３）漏えい発生後の対応		
3-4	漏えいの発生後の対応として、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を検知したり、作業者の記録を保存し漏えいの発生原因を特定したりすることができるよう、措置を行っているか。	漏えいの発生後の対応として、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を検知したり、作業者の記録を保存し漏えいの発生原因を特定したりすることができるよう、サイバーセキュリティを担っている部署にて対応しております。