

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

○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。

○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、委託先と再委託先と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。

○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。

○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。

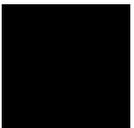
社名	株式会社NTTドコモ	
1. 委託先について		
1-1.	個人データの取扱いの委託（再委託）について、どのような情報を、どのような事業者へ委託して	※例えば、「コールセンター業務を行う者に契約者の氏名、電話番号等を委託」のように、委託の目的ごとに括った形で、委託する個人データの件数の多いものを数例ご記載ください。

	いるのか、代表的なものを可能な範囲で記載すること。	<p>※大手通信事業者として、他の業界と比較し特徴的と考えられる委託先や委託する情報があれば、そのような例もご記載ください。</p> <ul style="list-style-type: none"> ・キャリアショップや量販店等の運営に係る代理店業務：契約者の氏名・電話番号・住所等の情報取扱いを委託 ・コールセンター・サポートセンター業務：契約者の氏名・電話番号・住所等の情報取扱いを委託 ・契約者に対するテレマーケティング業務：契約者の氏名・電話番号等の情報取扱いを委託 ・ダイレクトメール送信に関する業務：契約者の氏名・住所等の情報取扱いを委託
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）。	<p>※1-1の回答にかかわらず、個人データの委託全般についてご回答ください。</p> <ul style="list-style-type: none"> ・A:業務委託契約 ・B:ドコモ以外の事業者が提供する定型の利用規約に基づく外部サービス利用（外部サービス提供事業者が個人データを取扱う場合）
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	<p>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（※）、個人情報保護上の委託として取り扱っている。</p> <p>※外部サービス提供事業者が個人データを取り扱うことになる場合のみ</p>

	該当するものとして扱っているか。	
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）。	委託契約において委託先（再委託先を含む）と締結する確認書の遵守事項にて安全管理措置、秘密保持、再委託の条件、再委託先の監督に関する事項を定め、担保している。（具体的な記載については2-7-1の回答に記載の通り） なお、以降で回答している社内ルールが要請する委託先（再委託先を含む）の監督状況のモニタリングを今後、強化していく。
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として取り扱っている。

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）。	委託先に対して、再委託がある場合は再委託先と情報管理に関する確認書（2-2 の回答の確認書）を締結することを要求し、委託先は再委託先より署名済みの確認書を取得する。 委託元は、委託先へ再委託先から確認書を入手したことを確認することで再委託先の情報管理を担保している。 ※「外部サービス利用契約」「業務委託契約」による違いなし。
(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。	・委託先に対して、契約前に立ち入り調査を実施している。立ち入り調査では「管理体制」「従業員の教育」「再委託の条件」「情報事故の有無や緊急連絡体制の確認」「情報の取扱管理の確認」の確認を実施している。 ※「外部サービス利用契約」「業務委託契約」による違いなし。
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	委託先に対しては、契約時の業務開始前研修および定期研修の実施を義務付けている。 求める教育体制の詳細は以下のとおり。 ・研修の有無： XXXXXXXXXX

	<p>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。</p>	<ul style="list-style-type: none"> ・ 頻度 : [REDACTED] ・ 対象の社員の範囲 : [REDACTED] ・ 研修内容の見直し : [REDACTED] ・ 理解度の確認 : [REDACTED] <p>※「外部サービス利用契約」「業務委託契約」による違いなし。</p>
<p>(3) 委託契約の締結</p>		
<p>2-7-1</p>	<p>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。</p>	<p>委託契約において委託先(再委託先を含む)と締結する確認書の遵守事項にて安全管理措置、秘密保持、再委託の条件、再委託先の監督に関する事項を定めている。具体的な記載については下記の通り記載している。</p> <ul style="list-style-type: none"> ・ 安全管理措置 : [REDACTED] ・ 秘密保持 : [REDACTED] ・ 再委託の条件 : [REDACTED] ・ 再委託先の監督 : [REDACTED] <p>※「外部サービス利用契約」「業務委託契約」による違いなし。</p>
<p>2-7-2</p>	<p>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、2-7-1の</p>	<p>2-5と同様となります。 ※「外部サービス利用契約」「業務委託契約」による違いなし。</p>

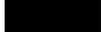
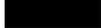
	<p>とおり委託契約（再委託契約を含む）に定めた事項について、契約書締結以外の方法により実運用上行っている措置はあるか。</p> <p>※1-2の種別で差異がある場合には、それぞれ記載すること。</p>	
2-8	<p>個人データの取扱いの委託先が再委託を行う場合、委託先に対してどのような対応を行っているか（再委託を承諾する基準等の再委託条件、委託先による再委託先の管理監督の実施状況の把握方法等）。</p> <p>※1-2の種別で差異がある場合には、それぞれ記載すること。</p>	<p>委託先が契約前に再委託先へ立ち入り調査を実施している。その際、業務委託元である当社は、委託先担当者と同行する。</p> <p>※ 立ち入り調査確認内容は 2-5 と同様</p> <p>※ 「外部サービス利用契約」「業務委託契約」による違いなし。</p>
<p>（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い状況の把握</p>		
2-9	<p>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状況について、どのように把握し、監督を行っているか。</p> <p>※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。</p>	<p>委託先における個人データの取り扱い状況について、下記の対応を行っている。</p> <p></p> <p>※ 「外部サービス利用契約」「業務委託契約」による違いなし。</p>
2-10	<p>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、</p>	<p>委託元において、委託業務に関する業務フローを作成し、委託先と各フローでのリスクの想定やそれに対する対策について検討実施している。</p>

	<p>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）。</p> <p>※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。</p>	<p>検討結果よりリスクに合わせたセキュリティ対策を作成し、それを踏まえて契約前及び契約中に立ち入り調査を実施している。立ち入り調査では「管理体制」「従業員の教育」「再委託の条件」「情報事故の有無や緊急連絡体制の確認」「情報の取扱管理の確認」等を確認している。</p> <p>・立ち入り調査：■■■■件</p> <p>※ 書面調査は不可。立ち入り調査を義務付けている。</p> <p>※「外部サービス利用契約」「業務委託契約」による違いなし。</p>
--	---	---

(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	<p>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。</p> <p>(内数として以下を記載)</p> <ul style="list-style-type: none"> ・外部サービスの利用 ・親会社、連結子会社に係るもの 	<table border="1" data-bbox="860 679 1904 858"> <thead> <tr> <th></th> <th>1-2 の種別 A</th> <th>1-2 の種別 B</th> <th>合計</th> </tr> </thead> <tbody> <tr> <td>委託先</td> <td>■■■■</td> <td>■■■■</td> <td>■■■■</td> </tr> <tr> <td>再委託先</td> <td>■■■■</td> <td>■■■■</td> <td>■■■■</td> </tr> <tr> <td>合計</td> <td>■■■■</td> <td>■■■■</td> <td>■■■■</td> </tr> </tbody> </table> <p>■■■■</p> <p><親会社、連結子会社に係るもの></p> <p>親会社：■■■■件、連結子会社：委託先■■■■件、再委託先■■■■件</p>		1-2 の種別 A	1-2 の種別 B	合計	委託先	■■■■	■■■■	■■■■	再委託先	■■■■	■■■■	■■■■	合計	■■■■	■■■■	■■■■
	1-2 の種別 A	1-2 の種別 B	合計															
委託先	■■■■	■■■■	■■■■															
再委託先	■■■■	■■■■	■■■■															
合計	■■■■	■■■■	■■■■															
2-12	<p>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）。</p> <p>※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。</p>	<p>■■■■</p>																

3. その他		
(1) 物理的・技術的安全管理措置		
3-1	<p>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。</p>	<p>【委託先に当社システムを使用させる場合】</p> <p>■業務委託先での管理情報の取扱いに際しては、業務委託先と情報事故の防止その他安全管理に関して実施する旨を定めた確認書を締結している。</p> <p>■当社システムを使用させる場合、当社が予め下記措置等を施した上で使用させている。</p> <ul style="list-style-type: none"> ・  ・ ・ ・ <p>【その他業務委託の場合】</p> <p>■業務委託先での管理情報の取扱いに際しては、業務委託先と情報事故の防止その他安全管理に関して実施する旨を定めた確認書を締結している。</p> <p>■当社システムを利用させる場合と異なり、当社より予め措置を施すことができないことから、委託先のシステム等に応じた対策を施している。</p> <p>■確認書では業務委託先での安全管理について「個人情報の保護に関する法律についてのガイドライン（通則編）」で規定する基本方針の策定、個人データの取扱いに係る規律の整備等の実施を義務付けており、これに沿った物理的、技術的安全管理措置を義務付け、業務委託元である当社と委託先にて対策を検討及び策定する</p>

<p>3-2</p>	<p>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</p> <p>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。</p> <ul style="list-style-type: none"> -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 	<ul style="list-style-type: none"> ■業務委託先での業務にあたっては契約前に業務フローを作成し、フロー上でのリスク分析及び対策案の検討を当社と業務委託先会社の間で実施している。 ■対策策定時は、当社にて各作業で考えられるリスクと対策に関する資料を作成し、それをもとに確認を行っている。 ■お客様の個人データの不正な持出を防ぐ仕組みとしては以下の内容を義務付けている <ul style="list-style-type: none"> ・  ・  ・ 
<p>(2) 委託に関する利用者への説明</p>		

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。	<p>公開しているプライバシーポリシー (https://www.docomo.ne.jp/utility/privacy/) において、以下のように表示し、利用者へ説明しています。</p> <p>-----</p> <p>7. パーソナルデータの取扱いの委託 当社は、販売・受付業務、故障修理業務、料金・与信関連業務、Web サイト・システム運営業務、イベント・キャンペーン等の実施業務、データ加工・分析業務、その他の業務において、パーソナルデータの取扱いの全部または一部を委託する場合があります。この場合、当社は、パーソナルデータを適正に取扱うと認められるものを選定し、適切な監督を実施します。</p>
(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。	<p>漏えい発生後には、 インターネット上での漏えい情報の流通がないか確認を行っている。</p> <p>作業者の記録については、 をルールとして制定している。</p>