

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	西日本電信電話株式会社	
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いるのか、代表的なものを可能な範囲で記載すること。	<ul style="list-style-type: none"> ・電気通信サービスの申込、解約受付手続きを行う者に、契約者の氏名、住所、電話番号等の取扱いを委託（連結子会社■■■■■に委託） ・電気通信サービスの故障対応を行う者に、契約者の氏名、住所、電話番号等の取扱いを委託（連結子会社■■■■■に委託）

		・電報の配達を行う者に、電報本体及び配達先の氏名、住所、電話番号等の取扱いを委託（連結子会社■■■■■■■■■■に委託）						
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>以下の種別があります</p> <table border="1"> <thead> <tr> <th>種別</th> <th>内容</th> </tr> </thead> <tbody> <tr> <td>種別 A</td> <td>業務委託</td> </tr> <tr> <td>種別 B</td> <td>外部サービス利用■■■■ ・クラウドサービス ・クラウドサービス以外の外部サービス</td> </tr> </tbody> </table> <p>■■■■■■■■■■</p>	種別	内容	種別 A	業務委託	種別 B	外部サービス利用■■■■ ・クラウドサービス ・クラウドサービス以外の外部サービス
種別	内容							
種別 A	業務委託							
種別 B	外部サービス利用■■■■ ・クラウドサービス ・クラウドサービス以外の外部サービス							
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。	個人データの取扱いの委託として扱うこととしています。						

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）と締結する覚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、担保しています（具体的な記載については2-7-1の回答に記載の通り）
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	委託先と締結する覚書において、以下の通り担保しています。 ■委託先による再委託先の監督 ・委託先が再委託先の履行状況を調査・確認 ■当社による再委託先の監督 ・委託先が実施した再委託先に関する調査・確認内容を当社が確認

	する覚書等における標準的な記載の例を示すこと)。	
(2) 委託先の選定		
2-5	<p>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。</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>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かかる、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、チェックシートを用いて確認を行うこととしています。</p> <p><1-2の種別Bの場合> 委託契約当事者となる外部サービス提供事業者の情報の取扱い有無の事前チェックや再委託先に対する管理強化を検討しています</p>
2-6	<p>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。</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>お客様情報管理に関する研修を少なくとも年1回実施することを委託先等に求めることとしています。</p> <p>そのうえで、下記について確認を行っています。</p> <ul style="list-style-type: none"> ・個人情報保護規則等にて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の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 <p><1-2の種別Bの場合></p>

		委託契約当事者となる外部サービス提供事業者の情報の取扱い有無の事前チェックや再委託先に対する管理強化を検討しています
(3) 委託契約の締結		
2-7-1	<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。</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>個人データの取扱いの委託に関する覚書を委託先との間で締結し、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担保しています。</p> <p>■安全管理措置</p> <ul style="list-style-type: none"> ・お客様情報保護のために必要な組織的・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 <p>■秘密保持</p> <ul style="list-style-type: none"> ・業務遂行にあたり委託先が知り得た情報の守秘義務の遵守 <p>■再委託の条件</p> <ul style="list-style-type: none"> ・当社の書面による事前同意が必要 <p>■再委託先の監督</p> <ul style="list-style-type: none"> ・委託先が再委託先の履行状況を調査・確認し、その調査結果を当社が報告を受け把握する

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。	2-5に記載の内容を確認しています。
-------	--	--------------------

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>委託先に対して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把握の方法については、以下の対応を求めています</p> <p>■再委託を承諾する基準等の再委託条件</p> <ul style="list-style-type: none"> ・ 当社の事前の書面による同意を必要としている ・ 当社が委託先と締結する覚書と同等の内容の覚書を委託先と再委託先で締結することを義務付けている <p>■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</p> <ul style="list-style-type: none"> ・ 当社は、委託先及び再委託先に対して、定期的に個人データ管理の履行状況の報告を求めることができ、また、事務所等に立入り、直接調査・報告を求めることができるとしている
<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>		

<p>2-9</p>	<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。 ※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>以下の通り把握、監督しています。</p> <ul style="list-style-type: none"> ■当社による委託先の個人データの取扱い状況の把握・監督方法 <ul style="list-style-type: none"> ・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しており、事務所等に立入点検を実施している ■委託先による再委託先の監督 <ul style="list-style-type: none"> ・委託先が再委託先の履行状況を調査・確認 ■当社による再委託先の監督 <ul style="list-style-type: none"> ・定期的に個人データ管理の各種対応の履行状況の報告を求めることができ、また、事務所等に立入り、直接調査・報告を求めることができるとしている
------------	--	--

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、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>	<ul style="list-style-type: none"> ・委託先による個人データ管理の各種対応の履行状況に関する報告書により確認を行っており、加えて、少なくとも年1回事務所等への立ち入り点検を実施している（点検項目は2-5記載の項目） ・委託先が再委託先の個人データ管理の各種対応の履行状況を調査・確認（少なくとも年1回） <p>・2023年度実施件数 立ち入り調査 ■件、書面点検 ■件</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"> <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>		1-2 の種別 A	1-2 の種別 B	合計	委託先				再委託先				合計				<p>うち、</p> <p>[Redacted]</p> <p>[Redacted]</p>	
	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>[Redacted]</p>																		

<ul style="list-style-type: none"> - 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 	質問	回答
	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	当社が許可していないオンラインストレージサービス等のインターネットサービス に接続できないように 技術的安全管理措置を講じなければならないと定めています。
	保守端末にダウンロードが可能になっていないか	[Redacted]
	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	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。 [Redacted]
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]	

		各種ログ等の定期的なチェックは十分か	
(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。	プライバシーポリシーにおいて、「個人情報（以下略）等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、監督します。」と記載し、公式 HP 上で公開している。	
(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。