

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	ソフトバンク株式会社	
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、どのような事業者へ委託	※例えば、「コールセンタ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。

	<p>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。</p>	<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> <p>代表的な委託の例：</p> <p>例① コンシューマ向け事業 委託先：コールセンター事業者 委託情報：携帯電話役務等の契約者個人情報（契約者番号、契約者名、契約者電話番号、契約者メールアドレス、料金プラン、請求金額、対応履歴等） ※当該問い合わせ顧客のみ参照可能なシステムへのアクセス権を付与</p> <p>例② コンシューマ向け事業 委託先：請求書印刷事業者 委託情報：携帯電話役務の契約者個人情報（契約者名、契約者住所、ご契約プラン、請求金額等）</p> <p>例③ コンシューマ向け事業 委託先：携帯電話の販売代理店事業者 委託情報：携帯電話役務の契約者個人情報（契約者番号、契約者名、契約者電話番号、契約者住所、課金情報等） ※弊社顧客対応システムへのアクセス権を付与</p> <p>例④ 法人顧客向け事業 委託先：コールセンター事業者 委託情報：法人向けサービスの法人契約担当者個人情報（契約者番号、会社名、窓口担当者名、連絡先電話番号、連絡先メールアドレス、契約プラン等）</p>
--	------------------------------------	--

		<p>例⑤ 法人顧客向け事業</p> <p>委託先：法人契約携帯のヘルプデスク事業者（キッティング、MDM等）</p> <p>委託情報：法人契約者情報、利用者個人情報（会社名、携帯利用者名、利用者電話番号、利用者メールアドレス等）</p>
1-2.	<p>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>	<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> <p>種別A) 個別契約（SB（委託元）→業務委託先）に基づく契約 →業務委託契約等に加え、弊社ひな形の【個人情報の取扱の委託に関する覚書】（以下個人情報委託覚書と略）を一律で締結を社内ルール化</p> <p>種別B) 定型サービス約款式の（提供者（委託先）→SB（委託元））一律の契約 ※種別Aと同様、覚書締結を求めることとしているが、事業者によって拒否されるケースは個別に確認</p>
<p>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）。</p>		
<p>（1）外部サービス利用に対する認識</p>		
2-1	<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</p>	<p>外部サービスの利用が、個人データの第三者提供、委託等個人情報保護法 法第27条および法第27条（第5項）に該当するかを事前に確認を行った上で、扱っている。</p>

	<p>上の委託に該当するものとして扱っているか。</p>	<p>なお、業務委託を行う際の委託先に対して、【個人情報委託覚書】においても、委託に外部サービスの利用を含むことが明確となるよう、以下のように注記を行っている。</p> <p>第9条（委託先の監督） 1 乙は、甲の事前の書面等による承諾を得ない限り、個人情報等の取扱いの全部又は一部を第三者に委託（第三者が提供するクラウド・SaaS等外部のシステム・サービスの利用を含む。また、委託が数次にわたって行われるときは再委託以降のすべての委託を含む。以下同様とする。）してはならない。</p>
<p>2-2 【別紙 非公開 希望】</p>	<p>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）。</p>	<p>「個人データの委託として扱っている」場合、当社は以下の項目を契約上担保している。 なお、項目については令和2年個人情報保護法改正時に、見直しを行ったもので、個人情報保護法「第4章第2節の規定の趣旨に沿った措置」を網羅している。</p> <p><安全管理措置の実施> 【個人情報委託覚書】 第6条（安全管理措置） 第7条（外国で個人情報等を取り扱う場合の特則） 第8条（従業者の監督）</p> <p><秘密保持> 標準的には2つの契約に規定している。 ・業務委託契約に機密情報全般の取り扱い ・個人情報の委託覚書に個人情報等の取り扱い</p>

		<p>【業務委託契約】 第 17 条 (機密情報の取扱)</p> <p>【個人情報委託覚書】 第 4 条 1 項 (利用目的による制限、第三者提供の制限、不適正利用の禁止、適正な取得)</p> <p><再委託の条件、再委託先の監督> 【個人情報委託覚書】 第 9 条 (委託先の監督)</p> <p>※契約・覚書における標準的な記載内容については、別紙参照。</p>
2-3 【別紙 非公開 希望】	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。	<p>再委託に該当するものとして扱っている。 なお、契約書類【個人情報委託覚書】においても、委託に外部サービスの利用を含むことが明確となるよう、別紙のように注記を行っている。</p> <p>第 9 条 (委託先の監督)</p> <p>※覚書における標準的な記載内容については、別紙参照。</p>
2-4 【別紙 非公開 希望】	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	<p>再委託の原則禁止、実施の場合は、当社の事前承諾を必要としている。</p> <p>【個人情報委託覚書】 <再委託時の当社の事前承諾必須> 第 9 条 (委託先の監督)</p>

	<p>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）。</p>	<p>〈再委託先の監督〉 第9条（委託先の監督）2項、3項</p> <p>※覚書における標準的な記載内容については、別紙参照。</p>
<p>（2）委託先の選定</p>		
<p>2-5 【非公開希望】</p>	<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。 ※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>〈1-2の種別Aの場合〉 ※1-2で分類いただいた種別ごとにご記載ください。以下同じ。</p> <p>〈1-2の種別Bの場合〉</p>
<p>2-6</p>	<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Aの場合〉 委託先において、委託業務を行う従業者に対し、業務開始時および年1回以上の定期的な情報セキュリティ/個人データの取扱いに関する教育の実施を義務化している。 当社業務エリアへ入場する委託先については、契約時に当社情報セキュリティに関する教育教材を配布し、入場前に内容確認を行うよう義務化している。 さらに、個人データを取り扱う委託先に対し、業務における情報の取扱い等に関する教材を提供し、定期的な教育実施の確認を行っている。</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><1-2の種別Bの場合> 委託先において、委託業務を行う従業者に対し、業務開始時および年1回以上の定期的な情報セキュリティ/個人データの取扱いに関する教育の実施を求め、実施状況を確認している。</p>
<p>(3) 委託契約の締結</p>		
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。 ※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><1-2の種別Aの場合> 契約に定めている。 なお、各項目の記載内容は、設問2-2~2-4をご参照ください。</p> <p><1-2の種別Bの場合> 種別Aと同じ。 (但し、弊社契約を拒否するベンダーの場合、個別にベンダー側文書（利用規約や安全管理文書）の記載箇所を確認している)</p>
2-7-2	<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、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。</p>	<p><1-2の種別A・Bの場合共通> 契約書締結以外の方法としては、契約に盛り込まれた事項が適切に担保されるかを確認するための確認を行っている。</p> <ul style="list-style-type: none"> ・契約書に基づき取り扱う委託先の担当者の事前確認 ・セキュリティチェック（具体項目については2-5参照） ・教育体制のチェック（具体項目については2-6参照） <p>加えて、リスクに応じた措置を行っている。</p> <ul style="list-style-type: none"> ・特にリスクが高いと思われる事案(例：コールセンター、代理店)： <ul style="list-style-type: none"> -現地へのオンサイト確認、委託先の責任者と取扱状況についての面談等

		<ul style="list-style-type: none"> ・ 弊社に委託社員が常駐する場合： - 当社の情報取扱規程に従い、データ機密区分ごとに取り扱環境の設置 - 指定場所から情報を持ち出す際の申請・審査・承認プロセス - 操作端末の監視等 <p>なお、契約締結後については、（４）に記載のとおり、年１回以上の委託先における安全管理措置の状況のヒアリングを実施、契約時からの環境変化の確認、および、安全管理上追加で必要な内容の確認を実施している。</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：1-2の種別 A/B、再委託先：1-2の種別 A/Bの場合></p> <ul style="list-style-type: none"> ・ 契約に定めており、設問 2-7-1 と同じ対応を行っている。 <p><再委託の対応条件></p> <p>【個人情報委託覚書】</p> <p>第 9 条（委託先の監督）</p> <ul style="list-style-type: none"> ・ 当社の事前の書面等による承諾を得ない限り、再委託を禁止。 <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"> ・ 当社が再委託を承諾した場合、委託先と同様な契約上の規定（委託先の監督義務全般）を再委託先にも義務としている <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等></p> <ul style="list-style-type: none"> ・ 委託先が再委託先の個人情報等の取扱方法等について、契約時に書面にて提示させること等により、再委託状況の把握。再委託先が再々委託を行う場合以降も、再委託を行う場合も、同様の行為を委託先に義務化している

(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い状況の把握		
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><1-2の種別Aの場合></p> <p>弊社外で個人データを取り扱う委託先（再委託先を含む）については、原契約の終了に至るまで年1回以上、書面により当社に委託先での個人データの取扱い状況の報告を求めている。また、リスクに応じ、その一部についてはインタビューや実査を行い、課題を知得した場合には、改善指示、教育・指導を行っている。</p> <p>具体的な確認項目の例：</p> <ul style="list-style-type: none"> ・ 個人データの取扱い体制、規程の変更状況 ・ 個人データ取扱者の変更、教育の実施状況 ・ 再委託先の変更状況、取扱い状況（契約、安全管理措置の確認） ・ 個人データを取り扱う業務エリアの一般業務エリアとの分離状況 ・ 個人を識別した入退室制限・記録・監視の状況 ・ 入退室時の持出持込制限の状況 ・ サーバやクライアントの技術的対策状況（ネットワークの分離、アクセス制限、マルウェア対策、外部への持出制限、ログ取得、監視等） ・ データ保存国・アクセス国の変更状況 ・ アクセスログの記録状況等 <p>また、弊社内で個人データを取り扱う委託先については、上記に加えて、実際の取扱い作業時には当社が立ち会うなどの社内ルールが遵守されているかの確認を行っている。</p> <p>（例：システム保守部門で商用サーバにアクセスする場合など）</p>

		<p><1-2の種別Bの場合> 個人データを取り扱う SaaS 委託先（再委託先を含む）については、原契約の終了に至るまで年1回以上、書面により委託先での個人データの取扱状況の報告を求めている。また、リスクに応じ、その一部についてはインタビューや実査を行い、課題を知得した場合には、改善指示、教育・指導を行っている。</p> <p>具体的な確認項目の例：</p> <ul style="list-style-type: none"> ・ SaaS 事業者による当社データへのアクセス制限の変更状況 ※当社の依頼がない限りアクセス不可 ・ データ保管環境（リージョン）の変更状況 ・ 海外移転（会社所在国、サーバ設置国、アクセス国）の変更状況 ・ ネットワーク監視、不正持出監視の状況 ・ データの暗号化の状況 ・ 脆弱性管理、定期的な脆弱性診断の実施状況 ・ 第三者認証取得状況 ・ SaaS の設定確認（認証機能、接続元制限、ログ取得等）の状況等
2-10 【非公開希望】	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。	<1-2の種別Aの場合> <1-2の種別Bの場合>

(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 【非公開希望】	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	<table border="1" data-bbox="862 279 1899 454"> <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 data-bbox="862 494 1377 582"><親会社、連結子会社に係るもの> ○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 【非公開希望】	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。	<p data-bbox="862 614 1198 646"><1-2の種別Aの場合></p> <p data-bbox="862 742 1198 774"><1-2の種別Bの場合></p>																
3. その他																		
(1) 物理的・技術的安全管理措置																		
3-1 【非公開希望】	【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。	
3-2 【非公開 希望】	<p>【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</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されていないか -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	
(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。	<p>当社のホームページ各所にて、当社個人データの委託に関する方針、安全管理措置を定期的実施すること、また、外国の委託先について説明している。</p> <p>① プライバシーセンター パーソナルデータの保護に関する方針</p> <p>委託 当社は、各種サービス等の問い合わせ対応業務、設備メンテナンス業務、料金関連業務その他の業務において、パーソナルデータの取り扱いの全部または一部を委託する場合があります。 当社は、業務委託先（サプライヤーを含む）にプライバシーポリシーの遵守を求めます。業務委託契約を締結する際は、業務委託の相手としての適格性を十分に審査します。業務委託契約には、安全管理措置、秘密保持、再委託の条件、その他のパーソナルデータの適正な取り扱いに関する事項について定めます。委託期間中においては、定期的な業務状況のモニタリング等を実施することにより、当社の業務委託先を適切に監督しています。 業務の受託に伴って委託元から提供（預託）されたパーソナルデータについては、これを委託元と当社との間で締結する契約の目的の達成に必要な範囲内で利用します。</p> <p>と、委託先の監督全般の方針を説明。</p>

		<p><u>②プライバシーセンター 所在が外国にあるパートナー企業への業務の委託</u></p> <p>ソフトバンクは、お客さまにより良いサービスを提供するため、パートナー企業に業務を委託し、海外でお客さま情報を取り扱う場合があります。海外においても、ソフトバンクと同等の安全管理措置が取られるよう管理しています。</p> <p>海外パートナー企業への業務の委託 ソフトバンクは、当該パートナー企業に対して、個人データの取り扱いについて我が国の個人情報取扱事業者に求められる要件と同水準の措置を講じるように求めています。</p> <p>として、海外への委託の安全管理措置について説明。</p> <p><u>③情報セキュリティポリシー</u></p> <p>7 業務委託先の管理体制強化</p> <p>業務委託契約を締結する際には、業務委託先としての適格性を十分に審査し、当社と同等以上のセキュリティレベルを維持するよう要請していきます。また、これらのセキュリティレベルが適切に維持されていることを確認し続けていくために、業務委託先を継続的に見直し、契約の強化に努めます。</p> <p>と、セキュリティレベルの維持について、説明している。</p>
<p>(3) 漏えい発生後の対応</p>		
<p>3-4</p>	<p>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</p>	<p><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検知></p>

	<p>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>	<p>当社では、個人データに限らず当社に関係する情報が意図しない形でインターネット上に流通していないか、Threat Intelligenceの活用や当社リサーチャーによるダークウェブのモニタリングにより、漏えい情報を検知している。漏えいした情報の検知はそのモニターの活動に含まれる。</p> <p><作業者の記録を保存し漏えいの発生原因を特定> 当社では、対象データを取り扱う作業者を限定したうえで、その作業のサーバ等のアクセス記録やPCの作業記録などをすべて取得し、監視チームおよびAI活用により操作ログをチェックしている。漏えいの疑義はリアルタイムで検知し、専門チームでの調査およびフォレンジック対応を行っている。</p>
--	--	---