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結果

２０２４年12月27日

事　　務　　局

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

○「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、同ガイドラインの遵守状況及び電気通信事業者による情報の取扱いについては、定期的にモニタリングを行い現状を把握することとされている。

（参考）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（令和４年個人情報保護委員会・総務省告示第４号）

（ガイドラインの見直し）
第５２条　本ガイドラインについては、社会情勢の変化、国民の意識の変化、技術動向の変化等諸環境の変化を踏まえ、必要に応じ見直しを行う。
２　本ガイドラインの遵守状況及び電気通信事業者による情報の取扱いについては、前項の本ガイドラインの見直しに必要な限度において、定期的にモニタリングを行い現状を把握することとする。

○同ガイドラインにおいて、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、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いるが、近年、電気通信事業者の業務の委託先を通じて大量の利用者情報が漏えいする事案が複数発生。

（参考）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（令和４年個人情報保護委員会・総務省告示第４号）

（従業者及び委託先の監督）
第１３条　（略）
２　（略）
３　電気通信事業者は、個人データ等の取扱いの全部又は一部を委託する場合は、その取扱いを委託された個人データ等の安全管理が図られるよう、委託を受けた者に対する必要かつ適切な監督を行わなければならない。

（参考）委託先を通じた大規模な漏えい事案について

○NTTドコモ
【発生時期】 2023年3月30日　【漏えい件数】 約596万件
【事案概要】ドコモが「ぷらら」および「ひかりTV」の販売支援業務を委託している㈱NTTネクシアにて業務に従事していた元派遣社員が、業務に使用しているパソコンから個人として契約する外部ストレージへアクセスし、顧客情報を含む業務情報を不正に持ち出したもの。

○NTT西日本
【発生時期】 2014年4月～2022年3月　【漏えい件数】 約120万件
【事案概要】 NTT西日本が新サービスやオプションサービスを顧客に案内するテレマーケティング業務を委託する過程において、顧客情報の漏えいが発生。具体的には、NTT西日本がテレマーケティング業務を委託していた㈱NTTマーケティングアクトProCXに対してコールセンタシステムを提供していたNTTビジネスソリューションズ㈱の元派遣社員（同システムの運用保守を担当）が、NTT西日本の顧客情報を不正に持ち出していたもの。

⇨ 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、NTT東日本、NTT西日本、NTTドコモ、ソフトバンク、KDDI、楽天モバイルに対し、モニタリングを実施。

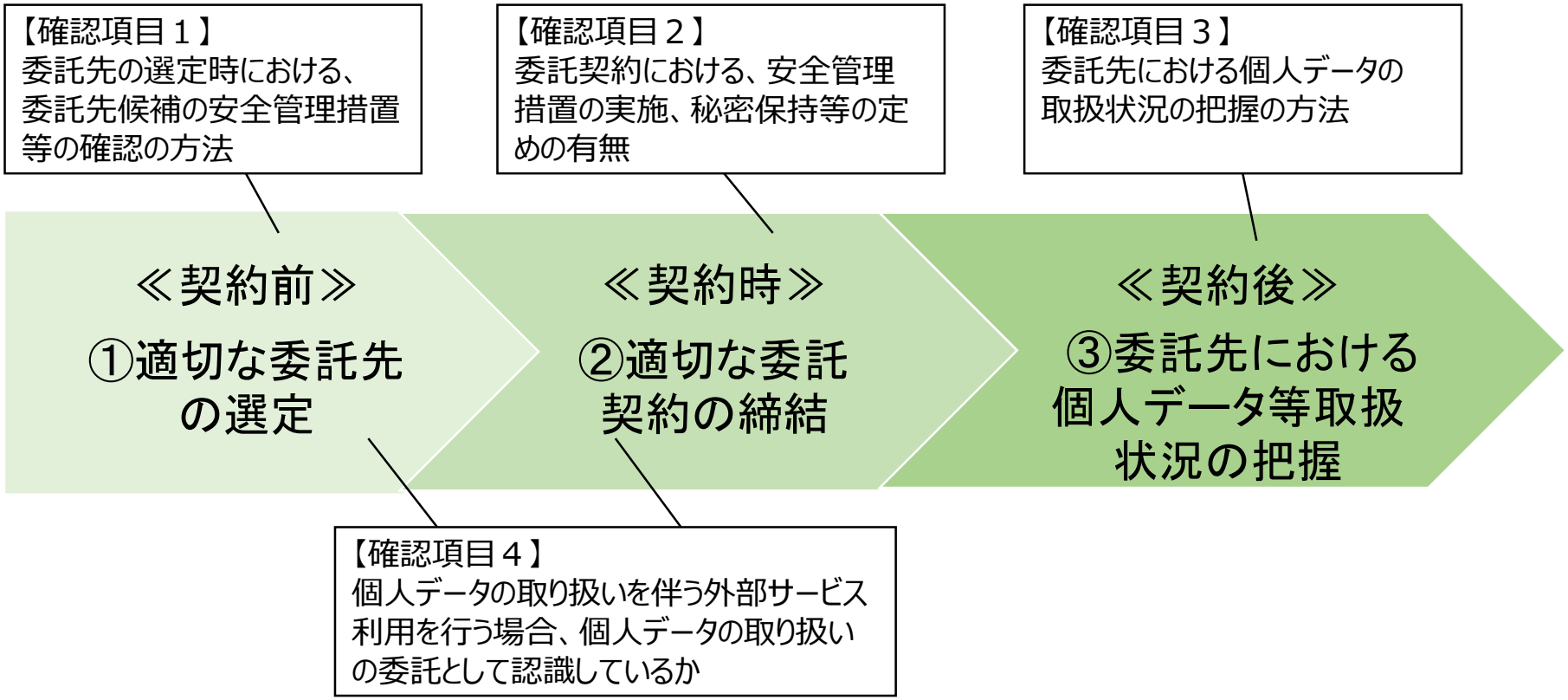
電気通信事業者モニタリングの確認項目

○ ガイドライン第13条第３項において、電気通信事業者は、個人データの取扱いを委託する場合は、その取扱いを委託された個人データの安全管理が図られるよう、委託を受けた者に対する必要かつ適切な監督を行わなければならないとされている。

○ 具体的には、ガイドラインの解説において、①適切な委託先の選定、②適切な委託契約の締結、③委託先における個人データ等取扱状況の把握を電気通信事業者に求めており、それぞれについて確認（確認項目１～３）。

○ 併せて、過去の漏えい事案を踏まえ、外部サービスの利用に関して確認（確認項目４）。

■モニタリングの確認項目１～４



電気通信事業者モニタリング結果（確認項目１）

確認項目１．委託先の選定時における、委託先候補の安全管理措置等の確認方法

＜モニタリング結果＞

各社とも、委託先の選定にあたって、安全管理措置が実施されることについて、あらかじめ、委託先の管理体制等の確認に加え、必要に応じて個人データ等を取り扱う場所に赴く又はこれに代わる合理的な方法により確認を行っている。

■事業者の説明の概要（特段の記載がない限り、業務委託契約、外部サービス利用契約による差異はなし。）

＜NTT東日本・西日本＞

- 委託先選定時に、チェックシートを用いて、委託先における個人データの取扱いに係る管理体制、研修、アクセス権管理等の項目の遵守状況を確認（※）。
- 必要に応じて契約前に立入り調査を実施。

※外部サービス利用の場合、当該事業者の個人データの取扱い有無の事前チェックや再委託先に対する管理の強化を検討している。

＜NTTドコモ＞

- 委託先選定時に、委託元が業務フローを作成の上セキュリティ対策を実施し、その内容を立入り調査で確認。
- 立入り調査では、セキュリティ対策に加え、委託先の管理体制、従業員教育、インシデント体制の有無等も確認。
- なお、委託先を通じた漏えい事案を踏まえ、安全管理措置の確認項目へ委託先のシステム環境についての対策を追加、及び従業員教育に用いる研修コンテンツへの反映を行っている。

＜ソフトバンク＞

- 委託先選定時に、管理体制、漏えい対策、インシデント対応、教育等の安全管理措置の実施状況の確認を実施。
- 必要に応じて契約前に立入り調査を実施。

＜KDDI＞

- 委託先選定時に、チェックシートを用いて、契約内容、教育、運用体制等を確認。
- 必要に応じて契約前に委託先にヒアリングを実施。

＜楽天モバイル＞

- 委託先選定時に、チェックシートを用いて、全社的な情報セキュリティ体制、作業場所・委託業務に関する情報セキュリティ、教育等について確認（※）。
- 扱う情報が大量にある契約を新たに結ぶ場合など、必要に応じて立入り調査を実施。

※クラウドサービスの場合は、情報セキュリティ及び個人情報保護管理体制、アクセス制御、各種セキュリティ等について確認。

確認項目２．委託契約における、安全管理措置の実施、秘密保持等の定めの有無

＜モニタリング結果＞
各社とも、委託契約又は覚書等において、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規定している。

■事業者の説明の概要（特段の記載がない限り、業務委託契約、外部サービス利用契約による差異はなし。）

＜NTT東日本・西日本＞

- 委託先と、個人データの取扱いの委託に関する覚書を締結し、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定めている。

＜NTTドコモ＞

- 委託契約において委託先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。

＜ソフトバンク＞

- 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（※）。

※個別の委託契約によらず、外部サービス利用契約のような、定型サービス約款に基づく契約の場合、個別にベンダー側の利用規約や安全管理に関する文書の記載箇所を確認している。

＜KDDI＞

- 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、再委託の監督を定めている。

＜楽天モバイル＞

- 委託先と、個人情報の取扱いに関する覚書を締結し、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定めている。

確認項目３．　委託先における個人データの取扱状況の把握方法

＜モニタリング結果＞

各社とも、定期的に監査（年１回の立入り調査等）を行う等により、委託契約で盛り込んだ内容の実施の程度を調査した上で評価している。

再委託については、委託元が、委託先が再委託先に実施する立入り調査に同行したり、直接、再委託先へ立入り調査を行うことができるようにしている事業者も見受けられた。

■事業者の説明の概要（特段の記載がない限り、業務委託契約、外部サービス利用契約による差異はなし。）

＜NTT東日本＞

- 委託先による自主点検の履行状況確認を行うことで、個人データの取扱状況の把握、監督を実施。
  - ✓ 点検シートに基づく自主点検結果を委託先から受領し、履行状況を把握、監督
  - ✓ 委託先に対して年１回の立入り調査を実施し、履行状況を確認
  - ✓ 再委託先に対しては、委託先への履行状況確認の中で、再委託先での個人データの取扱状況を把握、監督

＜NTT西日本＞

- 以下の通り把握、監督を実施。
  - ✓ 少なくとも年1回、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、委託先に立入り調査を実施
  - ✓ 再委託先に対しては、委託先への履行状況確認の中で、再委託先での個人データの取扱状況を把握、監督
  - ✓ 委託先を通じた漏えい事案を踏まえ、委託元も、再委託先に対して、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るようにするとともに、再委託先に立ち入り、直接調査・報告を求めることができることとしている。

＜NTTドコモ＞

- 委託先に個人データを貸与する際は「取扱管理簿」を作成し記録を保持している。
- 委託先に対して定期的に立入り調査を実施（１年を超える継続契約の場合年１回実施）するとともに、委託先が再委託先に実施する立入り調査に、委託元も同行することとしている。

＜ソフトバンク＞

- 社外で個人データを取り扱う委託先については、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立入り調査を行い、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。
- 委託先の個人データ取扱担当者を社内システムに登録し管理している。
- 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社員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。

＜KDDI＞

- チェックシートに基づき、委託先のセキュリティレベルを監査するとともに、立入り調査で年に１回以上の頻度で確認。

＜楽天モバイル＞

- 委託先における個人データの取扱状況について、チェックシートで把握。
- また、年に1度、委託先に対して上記のチェックシートの記載内容に変更がないか確認を実施。
- 状況に応じては、再委託先に対して立入り調査を実施を検討。

確認項目４．　個人データの取り扱いを伴う外部サービス利用を行う場合について、個人データの取り扱いの委託として認識しているか

＜モニタリング結果＞
　各社とも、個人データを取り扱う外部サービスを活用する場合、個人情報保護法上の個人データの取扱いの委託として扱っている。

■事業者の説明の概要

＜NTT東日本＞
- 個人情報保護法上の個人データの取扱いの委託として扱っている。

＜NTT西日本＞
- 委託先を通じた漏えい事案を踏まえ、現在は個人情報保護法上の個人データの取扱いの委託として扱っている。

＜NTTドコモ＞
- 個人情報保護法上の個人データの取扱いの委託として扱っている。

＜ソフトバンク＞
- 個人情報保護法上の個人データの取扱いの委託として扱っている。

＜KDDI＞
- 個人データを取り扱う外部サービスの提供形態によるが、個別の事案ごとに法令に則った対応を行っている。

＜楽天モバイル＞
- 個人情報保護法上の個人データの取扱いの委託として扱っている。

電気通信事業者に関するモニタリング結果（その他：構成員からのご意見）

【委託関係の在り方について】

- 委託先、再委託先に関わる対応については、委託元各社とも必要条件を満たしたうえで、さらに追加的な対策を進めていることを評価する。特に書面だけではなく必要に応じて立入り調査を行っている点、委託元のシステムを委託先に利用させることを進めている点などは、積極的に対策を進めているものとして高く評価できる。
- 一方で委託先におけるインシデント対策について、委託元と委託先の関係は主従ではなく協調であるという考え方によって責任の所在の明確化とそれにともなった責任の取り方、取らせ方が甘くなってはいないか。委託先が委託元のグループまたはグループ関連企業であったり、委託元の営業秘密や重要なノウハウを知り得る状態にあることは少なくないと考えられ、そのような場合には厳しい対応が取りにくくなるのではないか。委託元においても、協調すべきことと責任の所在に基づく規律とは明確に分けた対応を進めることを望む。
- 上記２ポツ目のような状態を防止するため、法的な対応も必要と感じている。現状はインシデントがあった場合の責任は委託元に集中しているが、委託先にも責任を負わせることが必要ではないか。EUのGDPRにおいてはコントローラーとプロセッサーという定義の元、パーソナルデータを実際に取り扱うプロセッサーにも強い責任を負わせている。委託元が安全管理を強化・改善することは、もちろん重要なことであるものの、それによって委託先が委託元に依存する（委託元の指示にのみ対応する）、委託元によって守られているといった考えにより、自助努力が損なわれないようにする必要がある。そのためには、委託先の責任は委託元だけではなく、パーソナルデータの委託先にもあることを明確にするなど、委託関係の在り方そのものについての見直しも必要ではないか。これにより、社会全体としての安全管理意識の底上げも図れると考えられる。

【委託先における個人データの取扱状況の把握方法について】

- 委託先に対して年1回またはそれ以上の頻度で立入り調査を行っていることは、特筆すべきことである。とりわけ利用者情報の厳重な管理が求められ、リソースも豊富な大手電気通信事業者ではあるものの、委託先に対して立入り調査まで行うことは、望ましいことではあるが、難しいことでもある。したがって、確認項目３のモニタリング結果に、定期的な監査の具体的な内容の一例として、年1回またはそれ以上の頻度で立入り調査を行っていることを記載してはどうか。

参考資料

（参考）電気通信事業者向けヒアリングシート

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。

1-2 個人データの取扱いの委託（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）。

２．委託先の監督について

（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。

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）。

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。

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）。

（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。

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。

（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。

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、2-7-1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。

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）。

（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。

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）。

（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

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）。

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。

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。

（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。

（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。

（参考）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の解説①

「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（令和４年個人情報保護委員会・総務省告示第４号）の解説」（抜粋）

3-4-6　委託先の監督（第13条第3項関係）

第13条（第３項）
３　電気通信事業者は、個人データ等の取扱いの全部又は一部を委託する場合は、その取扱いを委託された個人データ等の安全管理が図られるよう、委託を受けた者に対する必要かつ適切な監督を行わなければならない。

電気通信事業者は、個人データ等の取扱いの全部又は一部を委託（※1）する場合は、委託を受けた者（以下「委託先」という。）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しなければならない。具体的には、電気通信事業者は、第12条に基づき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、監督を行うものとする（※2）。

その際、委託する業務内容に対して必要のない個人データ等を提供しないようにすることは当然のこととして、取扱いを委託する個人データ等の内容を踏まえ、個人データ等が漏えい等をした場合に本人が被る権利利益の侵害の大きさを考慮し、委託する事業の規模及び性質、個人データ等の取扱状況（取り扱う個人データ等の性質及び量を含む。）等に起因するリスクに応じて、次の（1）から（3）までに掲げる必要かつ適切な措置を講じなければならない（※3）。

なお、通信の秘密に係る個人情報については、通信当事者の同意又は違法性阻却事由がなければ提供してはならないことに留意する必要がある（3-7-4（第三者に該当しない場合）参照）。

（1）適切な委託先の選定

委託先の選定に当たっては、委託先の安全管理措置が、少なくとも法第 23 条及び本ガイドラインで委託元に求められるものと同等であることを確認するため、「9（別添）講ずべき安全管理措置の内容」に定める各項目が、委託する業務内容に沿って、確実に実施されることについて、委託先の体制や規程等の確認に加え、必要に応じて個人データ等を取り扱う場所に赴く又はこれに代わる合理的な方法による確認を行う等により、あらかじめ確認しなければならない。

また、外国にある第三者に個人データの取扱いを委託する場合、委託元は、委託先を通じて外国において個人データを取り扱うこととなるため、委託先が所在する外国の個人情報の保護に関する制度等を把握した上で、委託先の監督その他の安全管理措置を講じる必要がある。

（2）委託契約の締結

委託契約には、安全管理措置（委託先において個人データ等を取り扱う者（委託先の作業者以外の者を含む。）を明確にすること、委託先において講ずべき安全管理措置の内容等）、秘密保持、再委託の条件（再委託を許すかどうか並びに再委託先を許す場合は再委託先に個人データ等を適正に取り扱っていると認められる者を選定すること、再委託を行うに当たっての電気通信事業者への文書による事前報告又は承認及び再委託先の監督に関する事項等。なお、二段階以上の委託を許す場合は同様に再々委託先等の選定、監督に関する事項等を定める必要がある。）、委託契約終了時の個人データ等の取扱い（個人データ等の返却、消去等）、契約内容が遵守されなかった場合の措置（例えば、安全管理に関する事項が遵守されずに個人データ等が漏えいした場合の損害賠償に関する事項、安全管理措置の不備が発見された場合の解約等）その他の個人データ等の取扱いに関する事項を適正に定めることが適当である。また、委託先における委託された個人データ等の取扱状況を委託元が合理的に把握することを盛り込むことが望ましい。

（参考）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の解説②

(3) 委託先における個人データ等取扱状況の把握

委託先における委託された個人データ等の取扱状況を把握するためには、定期的に監査を行う等により、委託契約で盛り込んだ内容の実施の程度を調査した上で、委託の内容等の見直しを検討することを含め、適切に評価することが望ましい。

また、委託先が再委託を行おうとする場合は、委託を行う場合と同様、委託元は、委託先が再委託する相手方、再委託する業務内容、再委託先の個人データ等の取扱方法等について、委託先から事前報告を受け、又は承認を行うこと、及び委託先を通じて、又は必要に応じて自らが、定期的に監査を実施すること等により、委託先が再委託先に対して本条の委託先の監督を適切に果たすこと、及び再委託先が第12 条に基づく安全管理措置を講ずることを十分に確認することが望ましい（※4）。再委託先が再々委託を行う場合以降も、再委託を行う場合と同様である。

【委託先に対して必要かつ適切な監督を行っていない事例】

事例 1）個人データ等の安全管理措置の状況を契約締結時及びそれ以後も適宜把握せず外部の事業者に委託した結果、委託先が個人データ等を漏えいした場合

事例 2）個人データ等の取扱いに関して必要な安全管理措置の内容を委託先に指示しなかった結果、委託先が個人データ等を漏えいした場合

事例 3）再委託の条件に関する指示を委託先に行わず、かつ委託先の個人データ等の取扱状況の確認を怠り、委託先が個人データ等の処理を再委託した結果、当該再委託先が個人データ等を漏えいした場合

事例 4）契約の中に、委託元は委託先による再委託の実施状況を把握することが盛り込まれているにもかかわらず、委託先に対して再委託に関する報告を求めるなどの必要な措置を行わず、委託元の認知しない再委託が行われた結果、当該再委託先が個人データ等を漏えいした場合

（※1）「個人データ等の取扱いの委託」とは、契約の形態・種類を問わず、個人情報取扱事業者が他の者に個人データ等の取扱いを行わせることをいう。具体的には、個人データ等の入力（本人からの取得を含む。）、編集、分析、出力等の処理を行うことを委託すること等が想定される。

（※2）委託元が第12条が求める水準を超える高い水準の安全管理措置を講じている場合に、委託先に対してもこれと同等の措置を求める趣旨ではなく、委託先は、第12条が求める水準の安全管理措置を講ずれば足りると解される。

（※3）委託先の選定や委託先における個人データ等取扱状況の把握に当たっては、取扱いを委託する個人データ等の内容や規模に応じて適切な方法をとる必要があるが、例えば、必要に応じて個人データ等を取り扱う場所に赴く又はこれに代わる合理的な方法（口頭による確認を含む。）により確認することが考えられる。

（※4）委託元が委託先について「必要かつ適切な監督」を行っていない場合で、委託先が再委託をした際に、再委託先が不適切な取扱いを行ったときは、元の委託元による法違反と判断され得るので、再委託をする場合は注意を要する。

（参考）個人情報保護法

第25条　個人情報取扱事業者は、個人データの取扱いの全部又は一部を委託する場合は、その取扱いを委託された個人データの安全管理が図られるよう、委託を受けた者に対する必要かつ適切な監督を行わなければならない。