監督責任

目的

監督責任とは「委託先からの情報漏えいを防止する」ことが目的です。情報漏えい事故のニュースなどから見ても明らかですが、情報漏えい事故の原因が委託先にあったというケースは多いです。委託先を原因とする事故の問題は、情報セキュリティにおいては、事故の原因が委託先にあったとしても、委託元が責任を免れることができない、という点にあります。これは、マイナンバーを取り扱う上でも同様です。

では、個人情報を含む業務を委託する場合、委託先で情報漏えいが発生しないようにするにはどのようにしたらよいでしょうか。身近な例に置き換えてみます。

うさちゃん（ウサギ）を飼っている人が海外旅行に行くシーンを思い描いてください。

今回の海外旅行は、とある理由でうさちゃんを連れて行けないとしましょう。飼い主は、海外旅行で不在になる間、うさちゃんの面倒を見てくれる人を探さなければなりません。ペットホテルという手段もあるでしょう、親類や友人、知人という手段もあるでしょう。さて、どうやって選びましょうか。おそらく、快く引き受けてくれて、ある程度信頼できる人、間違っても、たまねぎを食べさせたりしない人。そうです。うさちゃんのお世話の"心得"がある人を選ぶはずです。

さて、ようやくある程度信頼して預けることができる友人が見つかりました。友人も快諾してくれました。次は何をするでしょうか。多分、うさちゃんのお世話の方法を伝えるでしょう。食事のタイミング、種類と量、散歩の時間、リードの種類や長さ等々、盛りだくさんです。さすがに友人は"心得"がある人です。すべて、メモをして、シャンプーの種類まで聞いてきました。この人でよかった。飼い主は安心して、準備にかかる費用とお礼を包んで渡しました。

やっと準備が整いました。飼い主は海外旅行に出かけます。今回は長旅です。うさちゃんに手を振るときは辛かった。でも、心配はありません。信頼できる人がお世話をしてくれていますから―

そう思ったのも2、3日。大事なうさちゃんが気がかりになってきました。病気になっていないだろうか、友人はしっかりと食事、散歩などのお世話をしてくれているだろうか。

友人に電話をかけます。友人は大丈夫だと言っていますが、どうにかしてうさちゃんの大丈夫な姿を見る方法は無いでしょうか。そうです。写真です。本当は動画が良かったのですが、この際仕方がありません。友人に依頼し、写真を送ってもらいました。元気そうなうさちゃんの写真を見て、飼い主は安心です。それから、2日に1回写真を送ってもらえるように友人に依頼しました。

その後、安心して海外旅行を楽しみ、帰国後、元気なうさちゃんと再会することが出来ました。

さて、飼い主は、無事にうさちゃんと再会を果たしたわけですが、今回の飼い主の対応には次の3つのポイントが考えられます。

- 信頼できる人を選んだこと
- 条件を伝え、合意をとったこと
- 状況を確認したこと

このうちのどれかが欠けていた場合には、もしかしたら、うさちゃんは病気になっていたかもしれません。

監督責任の話に戻りましょう。
法令では、個人情報を含む業務を委託する場合、その適切な扱いについて事業者に様々な制約や条件が課せられており、外部にその業務を委託する場合でもそれは変わりません。そのため、委託先で情報漏えいなどの事故が発生した場合は、委託元の管理監督責任を免れられず、また重大な欠陥があった場合は、委託元に対して制裁が科される可能性もあります。

そんなリスクを回避するためにも、業務の委託を行う場合は、先ほどの例と同様の観点で、委託先に対する監督責任として、以下の3点の要件を満たす対処を行う必要があります。

- 委託先を適切に選定する
- 委託先と安全管理措置に関する内容を含めた契約を締結する
- 委託先における特定個人情報の取扱状況を確認する

求められる要件と手法

1 委託先を適切に選定する

この要件は、情報を適切に取り扱うと想定される委託先を選ぶことで、情報漏えいのリスクを低減するためのものです。
委託先を選ぶための基準を制定することが必要になります。例えば、ISO27001を取得している企業を選定する、チェックリストを事前配布して『安全管理措置』の項目対処が満たせている企業を選定するなどの条件を基準として制定することができるでしょう。
なお、マイナンバーガイドラインにおける事前確認項目の観点例は次となります。

事前チェック観点	対応安全管理措置
設備	物理的安全管理措置
技術水準	技術的安全管理措置
従業者に対する監督および教育の実施状況	人的安全管理措置
経営環境	組織的安全管理措置

『安全管理措置』の遵守状況を確認するには、『安全管理措置』の項目に基づいてチェックシート等を作成し、確認することが望ましいでしょう。
なお、事業内容や各種法令の変更時にあわせて選定基準の見直しを行うことに留意しましょう。

2 委託先と安全管理措置に関する内容を含めた契約を締結する

この要件は、選定した委託先に対して、具体的な情報の取り扱い方法等を盛り込んだ契約を締結することで、委託先に情報の適切な管理を実施させるためのものです。契約内容に含める条項としては次のものが挙げられます。

- 秘密保持の義務
- 事務所内からの個人情報の持ち出し禁止
- 個人情報の目的外利用の禁止
- 再委託における条件
- 情報漏えい事案が発生した場合の委託先の責任
- 委託契約終了後等の個人情報の廃棄又は返却
- 委託先従業者に対する監督および教育
- 契約内容の遵守状況の報告

再委託、再々委託に関する注意点
マイナンバー法では、委託先がさらに業務の再委託を行う場合には、必ず最初の委託元からの許諾を得る必要があります。（マイナンバー法　第10条（再委託））委託が繰り返された場合（再々委託）も同様です。そのため再委託、再々委託を行う場合は、常にエスカレーションして委託元の了解が取れるよう、契約書等に条項を盛り込んでおくことが望まれます。

3 委託先における特定個人情報の取扱状況を確認する

この要件は、委託先において情報がどのように取り扱われているか、という点について状況を確認することで、委託先における情報の適切な管理の欠陥、欠落等を検出し、漏えい事故を未然に防止するためのものです。
あらかじめチェックリストを作成しておき、監査を実施する、報告を受ける、といった方法が挙げられます。いずれの手法をとる場合でも、少なくとも、年1回は取扱状況を確認することが必要です。
対処の手法と取得できる記録をご紹介します。

手法の例	取得できる記録の例
自ら委託先の取り扱い状況を確認する （監査を実施する）	チェックリスト
委託先から取り扱い状況の報告を受ける （チェックリストや報告書等で報告を受ける）	チェックリスト 報告書

手法の例	取得できる記録の例
委託先者を自らの監督下である事務所の取扱区域に配置し日常的に監督する	日報

繰り返しになりますが、適切に監督するために必要な措置を講じず、又は、必要かつ十分な監督義務を果たすための具体的な対応をとらなかった結果、特定個人情報の漏えい等が発生した場合、番号法違反と判断される可能性があります。『安全管理措置』の遵守状況は確実に確認するようにしてください。