

(5) 外部委託先の監督方法

本節では、業務を実施する上で発生する外部委託について、個人情報保護を徹底させるためにどのような対策を行っているかということについて取り上げている。自らの事業所内における対策や従業員教育等には力を入れていても、事業体の違う外部委託先に対する監督は必ずしも容易ではなく、関与の程度や方法、そもそもの選定のあり方などについて事業者の事例を紹介している。

例えば、そもそも個人情報保護対策を適切に行っている事業者しか外部委託先として選定しないことを明確にして、自社で独自の認定制度やチェック制度を構築している事例(⑨)、認証の有無や委託業務の内容でグループ分けを行い、チェックの要否の判断を分けている事例(⑫)などを紹介している。

また、業務委託中に、適切な管理が継続されているかどうかを確認するために委託元として立ち入り検査を実施しているような事例(⑧)、委託元部署担当者だけでなく法務部も委託先に同行して委託元部署担当者、委託先両社に注意喚起を促している事例(⑭)を紹介している。中には検査だけに止まらず、実効性のある改善計画の策定まで求めるような事例(⑤)もある。そして、上記を契約のライフサイクルを通じて実施するという意味で、契約前・契約締結時・契約中・契約後にそれぞれチェックを実施しているような事例(⑬)も紹介している。

一方で、“管理”という姿勢ではなく、パートナーシップと外部委託先事業者における個人情報保護の取組を具体的に支援するような取組(合同勉強会の開催など)を行っている事例(①)、パートナー会社の経営層向けの意識喚起の機会を設定しているような事例(⑮)、社内点検時に委託先企業の担当者にも同行してもらい、自社の個人情報保護に向けた取組を知ってもらうような取組を行っている事例も紹介している(⑩)。

なお、一部、業務を受託されている側からみた、委託先の監督に対する協力事例や対応事例(⑦)なども紹介している。

本節で紹介している取組事例

- 4-(5)-①：委託先を集めての合同勉強会開催により委託先との意識を共有し、さらに定期的監査及び是正後のフォローアップ監査を実施
- 4-(5)-②：委託先から定期的に「報告書」や「証明書」を取得し、さらにモニタリングを実施
- 4-(5)-③：委託業務ごとに年1回以上の定期検査を実施
- 4-(5)-④：個人情報取扱い業務を委託している業者に対する立ち入り検査の実施
- 4-(5)-⑤：業務委託先へはチェックシートを送付。不備項目には改善計画の提出を求め、原則6ヶ月以内に改善できなければ契約を終了
- 4-(5)-⑥：書類発送は監査済みの外部委託先を利用
- 4-(5)-⑦：委託元へ個人情報保護のあり方を提案
- 4-(5)-⑧：取扱情報・事業者規模に応じたチェックリストを作成。立ち入り検査を実施
- 4-(5)-⑨：協力会社に対して独自の認定制度を導入
- 4-(5)-⑩：派遣社員からは直接誓約書をとらずコピーで対応
- 4-(5)-⑪：内部点検の際に委託先職員に同道してもらい、自社のチェックの厳しさを伝える
- 4-(5)-⑫：委託先については認証の有無、委託業務の内容などでグループ分けを実施
- 4-(5)-⑬：契約前、契約締結時、契約中、契約後、それぞれの場面に応じて個人情報の安全管理措置を確保
- 4-(5)-⑭：社内の各部署の外部委託時には法務部が同行チェックすることで意識付け
- 4-(5)-⑮：パートナー会社の経営層向けの意識喚起の機会を設定

4-(5)-①【委託先を集めての合同勉強会開催により委託先との意識を共有し、さらに定期的監査及び是正後のフォローアップ監査を実施】

(小売業（通販等）：約 520 人)

- ・H社では年3~4回、委託先を中心として、毎回約40社から70~80人程が参加する「個人情報保護対策合同会議」を行っている。参加者の多くは個人情報保護責任者であり、各社の取組についての意見交換やヒューマンエラーに関する事故事例の検証を行い、安全対策議論を共有している。
- ・委託先グループごと（業種ごと）にディスカッションを行い実情に沿った議論になるようにしている。また議事録を参加企業へ必ずフィードバックしていることで、危機意識を高める効果がある。
- ・外部委託先の情報取扱い管理の検証のため、現地へ赴き「外部監査」を年1~2回実施し、実態を把握し不備や是正を指摘・指導し、是正後のフォローアップ監査も行っている。

4-(5)-②【委託先から定期的に「報告書」や「証明書」を取得し、さらにモニタリングを実施】（小売業（通販等）：約 520 人)

- ・H社では委託先からは「個人情報保護報告書」を毎月提出してもらっている。
- ・外部委託先に預託された個人情報を破棄した場合、廃棄証明書を必ず提出してもらうようにしている。
- ・個人情報保護に関する教育やシステムの整備についても報告してもらっている。
- ・専任担当が適宜、委託先の作業現場までチェックに行っている。

4-(5)-③【委託業務ごとに年1回以上の定期検査を実施】（信用業：約 3,700 人)

- ・I社では委託業務ごとに、年に1回以上の定期検査を実施している。
- ・担当部署においてチェックシートを使用したリスク評価を実施し、必要に応じ業務の見直しや委託先への改善指導を実施している。

4-(5)-④【個人情報取扱い業務を委託している業者に対する立ち入り検査の実施】

(信用業：約 3,700 人)

- ・I社では個人情報を取り扱う業務を委託している業者（印刷会社等）に対しては、委託先の作業場所単位での立ち入り検査を実施している。
- ・検査ツールは委託先による自己評価シートと、自己評価シートの回答結果を現地で検証するためのチェックシートの2種類を使用する。
- ・シート内の各設問は点数評価（3点~1点）を行い、1点の項目がある場合は委託で

きないこととしている。

4-(5)-⑤【業務委託先へはチェックシートを送付。不備項目には改善計画の提出を求め、原則 6 ヶ月以内に改善できなければ契約を終了】（信用業：約 700 人）

- ・J 社では業務委託先の選定基準として、プライバシーマーク又は ISMS など客観的に評価される認証を取得しているか、認証の取得がない場合には過去にプライバシーマーク、ISMS 認証を剥奪されていないこと、過去に個人情報の漏えい・紛失等の事故を起こしていないこと、委託業者内に適切な情報管理体制が整っていることを条件としている。
- ・委託の際には個人情報の取扱状況に応じた覚書を委託先と交わす。再委託が発生する場合も、委託先と再委託先との間で同様の覚書を交わさせる。
- ・委託先に対しては、「安全管理措置評価用シート」を用いて評価を行なっている。評価結果で個人情報保護に不備がある項目については委託先から改善計画書（任意フォーマット）を徴収し、原則 6 ヶ月以内に改善出来なければ契約を終了する。

4-(5)-⑥【書類発送は監査済みの外部委託先を利用】（信用業：約 700 人）

- ・J 社では利用者への利用明細等の発送を外部委託している。委託先については監査を行っている。

4-(5)-⑦【委託元へ個人情報保護のあり方を提案（※）】

（情報サービス業（コールセンター等）：約 1,900 人）

- ・Q 社では情報管理については、同社から顧客に対して提案する場合もある。時間やコストがよりかかるため顧客から実施しなくてもよいといわれる場合もあるが、同社からは実施した方がいいと提案している。
- ・逆に、顧客からの厳しすぎる要求に対しては交渉する。社内でも決まりや約束事があるため、それにそぐわない場合には業務を断る場合もある。リスクの高い仕事は請けられないという姿勢を見せる場合もある。

（※）ここでは委託元との関係についての取組を取り上げた。

4-(5)-⑧【取扱情報・事業者規模に応じたチェックリストを作成。立ち入り検査を実施】

(その他サービス業(冠婚葬祭): 約 70 人)

- ・V社では委託先として、返礼品を取扱う百貨店、サーバ管理業者、位牌製作事業者等がある。規模は百貨店が最も大きく、位牌製作事業者は個人経営がほとんどである。
- ・返礼品を取り扱う百貨店へは参列者の送付先リストを渡し、発送からリストの破棄まで委託している。
- ・委託先を「取扱情報」と「事業規模」に応じてランク分けし、チェックリストを作成した。チェックリストにはランク別の20～50項目の必須項目がある。委託先にはすべて立ち入り検査も実施している。
- ・個人情報保護に関する覚書も交わしている。

4-(5)-⑨【協力会社に対して独自の認定制度を導入】

(その他サービス業(印刷・広告): 約 11,000 人)

- ・X社では、委託業務でダイレクトメールの発送を行う際、再委託先を、社内と同程度のセキュリティ確保をしていると認めた認定協力会社に限っている。認定のための検査は半日程度の立ち入り視察で実施している。現在全国で十数社が認定会社となっている。認定先については今後も増やしていきたい。現在は、個人情報管理に厳重を要する特定業務に限ってこのような取扱いにしている。
- ・委託先の中には、セキュリティ確保のために立ち入り検査に応じられないというケースもある。その場合、同社の作業をしているときに立ち入り検査をさせてもらうよう依頼する。
- ・委託先には取引基本契約書、個人情報保護についての覚書を交わしている。

4-(5)-⑩【派遣社員からは直接誓約書をとらずコピーで対応】

(その他サービス業(印刷・広告): 約 11,000 人)

- ・X社では派遣社員からは直接の誓約書を取ることなく、派遣会社がとった誓約書等のコピーで対応している。
- ・派遣社員、パート、アルバイトでも個人情報を取り扱う場合は、すべて教育の対象である。テストやアンケートで受講状況をチェックしている。派遣社員からは「受講しました」という書面へのサインもとってはいない。

4-(5)-⑪【内部点検の際に委託先職員に同道してもらい、自社のチェックの厳しさを伝える】

(その他サービス業(教育・学習支援): 約 180 名)

- ・ケ社では、内部点検の際に、委託先企業の職員を同道している。自分たちがどれほどキッチリしているかということを見せることで、要求される水準を示すことができ、

暗に個人情報保護に関する努力を促すことができていると考えている。

4-(5)-⑫【委託先については認証の有無、委託業務の内容などでグループ分けを実施】

(その他サービス業(印刷・広告)：約 1,400 名)

- ・コ社では、プライバシーマーク、ISMS を取得していない事業者については、外部委託先として適切か否かのチェックを年に 1 度以上行うようにしている。
- ・主管事業部と相談して、(個人情報の適切な保護の観点から問題が多いため) 委託を行わなくなった事業者もいる。監査時に問題点を指摘し、対応を要請したにも関わらず、対応を要請した点についての改善が見られないような企業である。
- ・社内イントラネット上に、委託可能事業者リストを掲示している。
- ・委託先企業については、2 段階で分けている。「データを渡してよい(処理を任せてよい) 事業者」と「封入・封緘などの事後処理だけを委託できる事業者」である。
- ・また、具体的なミスがあった場合は、臨時で監査に行くようにしている。

4-(5)-⑬【契約前、契約締結時、契約中、契約後、それぞれの場面に応じて個人情報の安全管理措置を確保】(製造業：約 26,000 人)

- ・サ社では技術力や情報セキュリティ一般も含め、外部委託先を格付け評価している。格付けでは、プライバシーマークや ISMS の認証を取得しているかどうかも評価項目のひとつである。また、格付けは低い、この企業を使いたい、という要請が現場からあったときは購買部門が委託先に対して直接改善要求をおこなう。
- ・契約に一般的な守秘義務条項などの項目を設けている。また、この契約時に、携帯電話・ノート PC を同社同様の基準で管理すること、個人情報を含む秘密情報を台帳で管理すること、従業員教育の実施、顧客からサ社に要求があった場合に限られるが、個人情報を廃棄した証明として廃棄証明書を提出することなどを求めている。
- ・年に一度同社による外部委託先向けの情報セキュリティ研修会を実施している。研修終了時点でテストをおこなっている。研修会へは、約 6 割の委託先企業が参加している。参加しない企業とは基本的に契約を行わないこととしている。
- ・契約中は購買部門が定期的に情報セキュリティ対策の状況確認を実施し、確認結果に基づいた是正計画と、実施指導、是正実施内容の確認を行っている。
- ・事後評価では情報セキュリティ状況確認、情報セキュリティ事故対応などをもとに評価を行っている。重大な事故が発生した場合や、改善が見られない場合には、取引の見直しや新規発注停止なども必要に応じて実施している。

4-(5)-⑭【社内の各部署からの外部委託時には法務部が同行チェックすることで意識付け】

(製造業：約 2,000 人)

- ・ス社では外部委託に際しては、「個人情報取扱適性判定書」を作成しており、社内規程、管理責任者、第三者認証取得有無、入退室管理、システムセキュリティ、再委託有無・再委託先管理方法、過去の漏えい事故の有無などについて、チェックした上で委託を行う。委託先選定の際には、委託先に立ち入り検査を行い、委託担当部署と法務部が同席した上で実施している。
- ・立ち入り調査に法務部が立会うのは、担当部署に、法務部が確実にチェックしていることを認識させると同時に、委託先に対して「個人情報に対する意識の高い会社」であることを印象付けるといったねらいがある。
- ・委託先企業がプライバシーマークなどの認証を取得している場合には、「認証の更新や評価を受けた」、という報告も毎年確認させてもらうようにしている。
- ・「個人情報取扱報告書」という書式を用意しており、委託期間中においても、委託先の状況をチェックしている。その他にも、打ち合わせで敢えて先方の会議室を利用させてもらったり、先方の執務室に入らせてもらったりして視察し、セキュリティの運用状況について評価している。

4-(5)-⑮【パートナー会社の経営層向けの意識喚起の機会を設定】

(情報サービス業(ソフトウェア)：約 5,500 人)

- ・セ社では年に 1 度、パートナー会社の経営層の方に来訪を依頼し、弊社の施策や事故事例の話をするような機会を設けている。最近では特に「機密」の概念が変わってきていることについて重点的に説明している（例：かつて、作業記録は機密情報ではなかったが、作業記録に個人名が含まれていると、個人情報、機密情報として扱われるようになってきた）。