東京海上日動リスクコンサルティング（株）
情報グループ
主任研究員　岡安 禎司

「個人情報の保護に関する法律についての経済産業分野を対象としたガイドライン」の改正内容と業務委託時のリスク管理について

２００８年２月２９日付けで、「個人情報の保護に関する法律についての経済産業分野を対象としたガイドラインの策定」が改正され、３月１日付けで施行された。
今回の改正では、業務の外部委託先からの個人情報漏洩が頻発していることを受け、業務委託に関わる記述を中心にガイドラインの見直しが図られている。財団法人　日本情報処理開発協会がまとめた資料（参考文献１）では、プライバシーマーク認定事業者の２００６年度報告事故のうち４４．３％が委託先や協力会社、提携先等で発生しており、業務委託を行う際にはより慎重な対応が必要となってきている。今回のガイドライン改正のポイントと、業務委託に関するリスク管理のあり方について記述する。

１．「経済産業分野を対象としたガイドライン」の位置づけ

個人情報保護法は、民間の事業者における個人情報の取扱いに関するルールを定めているが、これは各事業分野に共通する必要最低限のルールとなっているため、事業分野の実情に応じたより具体的なガイドラインが各省庁によって定められている。その中で、経済産業省が策定している「経済産業分野を対象としたガイドライン」には、以下のような特徴がある。

①広い事業分野に適用されるガイドライン

現在、各省庁にて２２分野３５ガイドラインが策定されているが、本ガイドラインは、広く経済産業分野の事業全般に適用されるものであることから、事業を営む上で参照すべき基本的なガイドラインと位置づけられる。

②法執行上の基準

本ガイドラインは、経済産業大臣が法を執行する際の基準となるもので、法の規定違反として「勧告」「命令」及び「緊急命令」の処分を行う際には、ガイドライン上の「しなければならない」と明記された必要措置が講じられているかが判断基準となる。

③具体的事例による解説集

本ガイドラインでは、個人情報保護法の要求事項ごとに具体的事例をあげて解釈を説明しており、個人情報保護の具体的な対策水準を考えるための解説集という面もある。

経済産業分野を対象としたガイドラインは、個人情報保護法全面施行（２００５年４月）前の２００４年１０月に策定され、その後２００７年３月に「個人情報の取扱いに関する過剰反応」に対する見直しを中心とした改正が行われた。今回は２回目の改正となり、２００７年１２月から改正原案に対する意見募集が行われ、２００８年２月に新たなガイドラインが公表された。

２．今回の改正のポイント

外部委託先からの個人情報漏洩が頻発していることを踏まえ、今回の改正では「委託先、再委託先に対する委託元の監督責任の在り方について」ガイドラインの見直しが図られている。

改正の主なポイントは以下の通りである。

（１） 委託先に対する必要のない個人データの提供の禁止

「委託先に対して業務に必要のない個人データを提供しないようにすること」が明記された。

（２） 委託先に対する「必要かつ適切な監督」の内容の明確化

「必要かつ適切な監督」には、具体的に下記の３項目が含まれると明記された。

① 委託先を適切に選定すること

委託先の選定にあたっては、委託する業務の内容に応じて少なくとも個人情報保護法第２０条で個人情報取扱事業者が求められている安全管理措置と同等の措置が講じられていることを合理的に確認することが望ましいとされている。例えば委託開始時にチェックリストを用意し確認を行ったり、客観的な基準による第三者認証（例えばプライバシーマーク）を取得しているかなどを確認した上で委託先を選定することが考えられる。さらにこれらの確認は契約更新などのタイミングで適宜再実施することが望ましいとされている。

② 委託先との間で必要な契約を締結すること

委託先との間では契約を締結し、その中に委託先における個人データの取扱状況を合理的に把握する方法を盛り込むことが望ましいとされている。経済産業省のガイドライン説明資料（参考文献２）には、「個人データの取扱いを委託する場合に契約に盛り込むことが望まれる事項」として具体的に以下の項目があげられている。

- 委託元及び委託先の責任の明確化
- 個人データの安全管理に関する事項
- 個人データの漏えい防止、盗用禁止に関する事項
  - 委託契約範囲外の加工、利用の禁止
  - 委託契約範囲外の複写、複製の禁止
  - 委託契約期間
  - 委託契約終了後の個人データの返還、消去、廃棄に関する事項
- 再委託に関する事項
  - 再委託を行うに当たっての委託元への文書による報告
- 個人データの取扱状況に関する委託元への報告の内容及び頻度
- 契約内容が遵守されていることの確認（例えば情報セキュリティ監査なども含まれる）
- 契約内容が遵守されなかった場合の措置
- セキュリティ事件、事故が発生した場合の報告、連絡に関する事項

③　委託先における委託された個人データの取扱状況を把握すること

委託先における個人データの取扱いを把握する方法としては、たとえばチェックリスト等を整備しその記録内容を確認したり、適宜報告を受けたりするなどの方法がある。また委託先を訪問調査したり、監査を行うことも個人データの取扱状況を把握するための手段の１つとして考えられる。

今回の改正では「再委託先についての監督責任」について具体的な事例が追記された。今後業務委託を行う事業者は、委託先に「再委託の有無」を確認し、再委託先も含めた監督を行うことが必要となってくる。

３．外部事業者への業務委託を行う際のリスク管理について

外部事業者へ業務委託を行うのにあたっては、今後よりいっそう慎重な個人情報の取り扱いと、実効性がある委託先の監督が求められる。しかし委託元が一方的に委託先に対して個人情報保護の対策を要求するのではなく、両者間で個人情報取扱いに関るリスクを相互評価・共有していくことが必要である。委託先と委託元の両者が業務委託開始時に個人データの取扱い手順やルールを協議したり、委託開始後も報告や振り返りの機会を設けていくことが大切である。

外部事業者へ業務を委託する際は、個人情報の取扱いに関わるリスクだけでなく、以下のようなリスクも考えられる。

- 委託先への業務ノウハウの流出
- 委託コストのブラックボックス化
- 委託先の倒産、買収・営業譲渡などによる業務撤退、中断
- 反社会的組織への業務委託による社会的批判　　など

外部事業者へ業務委託をすることによるメリットを最大限に享受するためには、個人情報の取扱いに関わるリスクだけではなく、上記のようなリスクも含めた上で「委託先選定→契約・委託開始時→委託作業期間中→委託終了時」という業務サイクルの各フェーズについてリスク評価を行なっていく必要がある。さらに、業務委託開始後はＰＤＣＡサイクルをまわしながら各種リスクの軽減を図っていくことも大切である。

業務委託を行う際に必要となる個人情報保護の対策は、こうした「外部事業者へ業務委託をする際のリスク管理」の一環として検討していくことが必要である。

以上

（第 172 号　2008 年 4 月発行）

【参考文献】

１．（平成１８年度）「個人情報の取扱いにおける事故報告にみる傾向と注意点」
2007 年 6 月 11 日　財団法人　日本情報処理開発協会プライバシーマーク推進センター
http://privacymark.jp/news/20070611/jikohoukoku_H18_20070611.pdf
２．経済産業省・個人情報保護ガイドライン等概要資料（平成 20 年 2 月 28 日現在）
http://www.meti.go.jp/policy/it_policy/privacy/080229guidline-gaiyou.pdf