東京海上日動リスクコンサルティング（株）
情報グループ
主席研究員　　近森　健三

個人情報保護対策とリスクコントロール

第３回　外部委託先の管理

■外部委託に伴うリスクと管理の必要性

一般的な企業の場合、外部への業務委託を全くなしに事業運営を行うことは考えにくい。法律上の制約などの理由による場合もあろうが、一般的には専門的なノウハウの活用、コストセーブ、リスク移転などを目的として外部への業務委託を実施している場合が多いと思われる。しかしながら、外部委託にはこのようなメリットばかりではなく、例えば以下のようなリスクがあることを認識しておかなければならない。

・ 不適切な委託先の選定
・ 契約内容の不備
・ 委託先へのノウハウの流出
・ 委託コストのブラックボックス化
・ 委託先の倒産、買収・営業譲渡等による業務撤退
・ 委託先における善管注意義務違反、履行遅延等の契約義務違反
・ 委託先における不正行為、過失

特に、個人情報保護の観点からは委託先の不正行為や過失による個人情報の漏洩・流出は大きなリスクとなり得る。外部委託のメリットを最大限に享受するためには、「委託先選定⇒契約⇒委託開始⇒委託終了」の業務サイクルに合わせたリスク管理が求められる。

■委託先管理における必須項目

「行政機関の保有する個人情報の適切な管理のための措置に関する指針について」の第８-４において外部委託管理についての規定があるが、同項においては委託先管理の具体的な内容についてはあまり触れられていない。この点に関し、「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するガイドライン」が参考になる。同ガイドラインのⅡ．２（３）４)「委託先の監督」では、「必要かつ適切な監督」が行われていない状況とは以下のような事項を怠った場合としている。逆に言えばこれらの項目が「必要かつ適切な監督」を実現する上での必要条件と解釈できる。

・契約締結時及びそれ以降も定期的に安全管理措置の状況を把握すること

・安全管理措置の内容を委託先に指示すること
・再委託の条件を指示すること
・委託後の委託業務の履行状況を確認すること

このほか、業務委託先との契約終了後においても、委託先での業務遂行状況が適切であったかどうかの評価を行い、継続契約の適否や契約の内容などにフィードバックすることも付随的に必要であると考えられる。以上をまとめると、委託先管理において最低限必要な事項は以下の４点と言える。

〔選定〕委託先の適切な選定
〔契約〕再委託条件を含む安全管理措置条項を盛り込んだ契約
〔監督〕契約締結時及びその後の定期的な安全管理措置の状況把握
〔評価〕委託業務終了後（あるいは定期的な）委託先の評価

■委託先の選定

委託先における安全管理のレベルにバラツキが生じないよう、委託先選定に関する統一的な基準を定めておく必要がある。もとより外部委託については前述したメリットを享受することを目的としているため、まずは委託先の業務遂行能力面（パフォーマンス）を評価する必要があるが、これに加え、安全管理という観点から情報セキュリティ評価を盛り込む。つまり、この二つの観点で評価基準を設ければ良いことになる。

情報セキュリティ面の評価項目としては、プライバシーマークやＩＳＭＳ（情報セキュリティマネジメントシステム）などの第三者認証の取得状況や内部管理体制、事故歴、賠償責任保険（個人情報漏洩保険）加入状況などが考えられる。尚、ＩＳＭＳについては、認証取得の対象が特定の部門や業務に限定されているケースが一般的であるため、委託する業務が認証の対象となっているかどうかの確認が必要である。

また、委託先の故意や重過失が原因で個人情報漏洩事故が発生した場合、委託元が負担した費用を委託先に求償することになるが、委託先が十分な資力を持たない場合には、委託元が負担した費用を回収できずに財務状況が悪化することになりかねない。このようなリスクに備え、個人情報漏洩保険などに加入している委託先を選ぶ、あるいは委託先に個人情報漏洩保険の加入を義務付けることも検討しておきたい。

■委託先との契約

当然ではあるが、委託先の従業員は委託元との間に直接的な雇用関係が無い。従って、委託先を通じて間接的にコントロールすることで安全管理の遵守を求めざるを得ない。しかし、いくら委託先に対して「安全に管理して欲しい。」と口頭や文書で要請しても、委託先が了解していなかったりその内容が具体性を欠いたりしている場合には、適切な管理は期待できない。また、個人情報漏洩が発生した場合の責任の所在もあいまいとなるおそれもある。従って、委託の際には、委託先に課すべき安全管理義務条項を盛り込んだ契約を取り交わすことによって強制力を働かせる必要がある。

前述した「行政機関の保有する個人情報の適切な管理のための措置に関する指針について」の第８-４においては、以下の事項を契約に明記することが求められている。

①個人情報に関する秘密保持等の義務
②再委託の制限又は条件に関する事項
③個人情報の複製等の制限に関する事項
④個人情報の漏えい等の事案の発生時における対応に関する事項
⑤委託終了時における個人情報の消去及び媒体の返却に関する事項
⑥違反した場合における契約解除の措置その他必要な事項

このうち、再委託については特に留意を要する。業務が孫請けに再委託されてしまうと一次委託先以上に管理が困難となるし、実際の漏洩事例を見ても、再委託先や再々委託先から個人情報が漏洩しているものが少なくない。とはいえ、委託業務の内容によっては再委託を認めないと不都合が生じる場合も考えられる。従って、契約においては原則は禁止とし、以下を満たすことを条件として例外的に認めるとしておくと良い。

・再委託を行う場合には事前に書面にて委託元の許可を得る。
・再委託先に対して、自社が本委託業務契約上負っている義務と同等以上の義務を課す。
・再委託先の監督責任を負う。
・再委託先が更に委託を行う場合も同様の義務を負う。

しかし、これらの義務を委託先に負わせたとしても、再委託によるリスクがなくなるわけではない。事前に届出を受けたとしても無制限にこれを認めることは避け、委託先の選定基準に照らし合わせて、再委託を認めるかどうかを判断する必要がある。

■委託先の監督

契約を締結すれば晴れて委託業務は開始となるが、契約条項に様々な安全管理措置に関する条項を盛り込んだからといって安心はできない。委託元は、委託先が契約に定めた安全管理措置を確実に実施しているかどうか監督しなければならない。

委託先の業務状況を把握するためには、委託先から個人データの取扱い状況について定期的に報告を受ける、委託先に赴いて直接監査を行う、あるいは外部の第三者に委託先の情報セキュリティ監査（注）を依頼しその結果の報告を受ける、などの措置が必要である。尚、これらの行為を確実に実施できるよう、契約書に報告の義務や監査の権利を盛り込んでおくことが望ましい。（注：情報セキュリティ監査は経済産業省の制度である。同制度は民間企業や政府、地方自治体等の情報セキュリティ対策の監査を目的としており、情報システムのみならず情報資産全体のセキュリティマネジメントを対象として監査がなされ、情報セキュリティレベルを客観的に評価できるものとして有用である。）

■委託先の評価

委託業務が終了したら、当該委託先が適切に業務を遂行したかどうかについて評価を行うべきである。また、長期間（１年以上）に亙り継続して業務を委託する場合は、委託業務契約の更新のタイミングに合わせ、少なくとも年１回以上定期的に評価を実施する。この評価の第一の目的は、当該委託先の評価結果を実績として記録し次回以降の委託先選定（もしくは当該委託先との契約継続可否の判断）のための参考情報とすること、第二の目的は、評価結果をフィードバックすることによって委託先管理全体のレベルアップを図ることである。

評価項目は、基本的には選定時の基準と同様に、パフォーマンス面と情報セキュリティ面の２つの観点となる。情報セキュリティ評価の項目としては、例えば、ルールの理解度・徹底度、リーダー・要員の資質、安全管理措置の遵守、事故・不備の発生、監査時の結果、指摘事項の改善状況などが挙げられる。

次回（第四回）は、個人情報漏洩時の対応について述べてみたい。

出典：特定非営利活動法人ネットワークリスクマネジメント協会発行
NRAメールマガジン『啓・警・契』第１０７号
URL：http://www.nra-npo.jp/

（第 89 号　2006 年 1 月発行）

