外部委託及びクラウドにおける情報セキュリティマネジメントシステム適合性評価の利用

日本ヒューレット・パッカード株式会社　佐藤　慶浩

組織における情報セキュリティ対策における課題のひとつが外部委託における機密保護対策である。
外部委託を一意に検討することは具体性を欠くことになり難解になる。解決するには外部委託する業務をいくつかの観点で細分化して、それぞれの特徴を踏まえた上で課題を整理する必要がある。また、委託先に課すべき義務だけに着目し、委託元のすべきことについて明確にしないと実現性を欠く対策となる点にも注意が必要である。
その他にも注意すべきことはあるが、ここでは、主としてこれら２点に着目して、外部委託における情報セキュリティ対策の課題の整理と改善のための検討を行う。
なお、本稿では、情報セキュリティ対策のうち機密性の保護だけについて論ずることにする。完全性と可用性の保護についても別途検討する必要があるが、本稿では取り扱わないものとする。
様々な業務態様を一意に取り扱ってしまうという失敗の代表例が、委託先に対してＩＳＭＳ認証やプライバシーマーク認証の取得を単に求めるような行為である。ＩＳＭＳ認証については、認証取得の取得対象部門の範囲と内容は適用宣言書で特定されている。委託先の情報セキュリティ対策状況を確認するための質問票に、「貴社はＩＳＭＳ認証を取得しているか？」という項目を入れている場合があるが、ＩＳＭＳ認証は部門単位であり、「会社が認証取得している」という表現をすることは、そもそも禁止されている。それに相当する適切な表現は、「全部門が認証取得している」となるが、委託した業務を実施する部門と関係ない部門に対しても認証取得を要求していることになる。また、ＩＳＭＳ認証は情報セキュリティ対策のレベルを一定に保つものではない。リスク評価に基づいて適切なリスク対応をするというマネジメントシステムが構築されていることが認証の対象である。言い換えると、リスク対応としての対策レベルを低くして、高いリスクがあるとしても、それを認識・評価した上で受容するという判断をしているのであれば、対策レベルは低いままでも認証の取得は不可能ではない。そのため、「ＩＳＭＳ認証を取得しているか？」とだけ委託先に質問するのは愚問である。一方、プライバシーマークについては、取得は法人単位であり全部門が認証取得の対象に限られている。しかし、適用対象については、選択が可能である。例えば、個人情報を含むデータ保存に関する業務について、プライバシーマーク取得している事業者が委託元として、プライバシーマーク取得しているデータセンター事業者を委託先として、外部委託する場合に、委託元はデータ保存については自社で実施していないとして認証取得の対象範囲外とすることができ、委託先はデータの内容は委託先のみが知り得るもので委託先にとっての個人情報には該当しないとして対象範囲外とすることができる。これの全体を見ると、個人情報を含むデータ部分は、委託元と委託先のどちらにおいてもプライバシーマークによる対象ではないということが起こり得る。
これらの例からもわかるとおり、委託元が委託先に、ＩＳＭＳ又はプライバシーマーク認証取得を求める際に、認証取得部門や業務、対象情報の範囲を個別に指定しない限り、単にその取得を求めるだけでは不十分となることがある点に注意しなければならない。
また、それらを指定したとしても、認証の取得は委託発注前の実績を問うものであり、外部委託する業務が定型業務ではない限り、事前に取得している業務手順とこれから発注する業務手順との相違による影響を踏まえなければならない。

以上のことから、外部委託における情報セキュリティ対策は、これから発注する委託業務においてどのような対策を講ずるのかを明確にすることが必要である。
そのためには、外部委託の業務をいくつかの観点で細分化して、それぞれの課題を整理することが考えられる。
以下に、いくつかの観点での課題をあげる。

(1) どのような契約で実施するのか？（派遣か請負か←How）

委託契約を類別するのに情報セキュリティ対策の観点でまず重要なことは、派遣か請負かかの違いである。派遣であれば日々の業務作業の指示と監督は委託元にあるため、業務と同様に情報セキュリティ対策の指示及び監督は委託元とするのが現実的である。一方、請負であれば委託元が委託先の作業者個人に直接作業指示をすることは法律上認められていないため、必要となる情報セキュリティ対策については委託先企業が最終的な指示をすることしかできない。そのように、作業者への直接の指示は委託先しかできないが、請負業務の指示と同様に、委託元がリスク対応の判断をした上で必要な対策について、作業者個人ではなく委託先企業に対して対策を指示することはできる。ただし、その場合には、指示した対策について請負義務が生じ、また対価の対象ともなるのであって、指示していない対策について、委託先が必要に応じて適宜補完することを求めることは、委託元の利己的な行為と考えられ適切ではない。
委託元の作業場所で委託業務を実施する請負業務では、偽装請負との関係で問題となる場合がある。実質は、委託元が作業者に日々の作業指示を行っている場合は、情報セキュリティ対策の指示も委託元が行うのが現実的である。それにもかかわらず、契約形態が請負であることを理由に対策指示を曖昧にするといった本末転倒を回避するため、契約形態を実態に正す必要がある。
（委託する業務を実施する作業場所については、派遣であれば委託元、請負であれば委託先であれば比較的単純であるが、委託元で実施する請負業務については、注意が必要である。
なぜなら、請負については、いわゆる偽装請負として問題化しているとおり、委託元が作業者に日々の作業指示をしているような実態で派遣業務となっている場合には、契約形態にかかわらず、情報セキュリティ対策の作業指示は委託元がしなければ現実的ではない。しかしながら、そのように定めると、派遣業務を請負として偽装することが明らかとなってしまうことから、それをあいまいにするというのは、本末転倒である。それならば、契約形態を派遣に正す必要があると考えるべきである。）

(2) どこで業務を実施するのか？（委託元作業場所か委託先作業場所か←Where）

派遣であれば当然であるが、請負の場合でも、委託元作業場所で業務を実施させるのであれば、そこでの物理的（施設的）情報セキュリティ対策は、委託元が実施するしかない。社員に対して十分である対策が、非社員に対しても有効であるかのリスク評価は委託元の責任であり、その対策が不十分であるにもかかわらず、委託先社員が事故を起こしたときに請負としての監督責任を一方的に問うのは適当ではない。

(3) どの時点を保証させるのか？（注意義務か結果責任か←When）

外部委託の情報セキュリティ対策については、委託元の理想としては、特段に何も具体的な対策を指示することなく事故が起きないという結果を委託先が保証してくれることを期待したいであろう。一方で、委託先としては、受注時点で顕在化していない未知の脅威に備える対策までを講じることを見積もることはできず、ましてや事故の結果生じる予測不能な規模の損害の賠償を保証することは現実的ではないと考えるであろう。

現実的な範囲で考えるならば、委託元が委託先に対して、委託する業務を仕様化して検収条件を定めるように、情報セキュリティ対策として講じるべき注意義務を明示的に指示することで、委託先による実施に不備があれば業務委託の債務不履行責任を問い、指示内容に不足があったのであれば、一方的に委託先の責を問えないということになるであろう。
このことは一見、委託元にとって不利のようであるが、仮に結果責任をいくら求めても、それは事後的な金銭賠償でしか担保されず、本来なされるべきは、事故発生を未然に防ぐための対策に力点が置かれることの利益に着目すべきである。結果責任を偏重すれば、委託先としては未然防止対策を講じるよりも、むしろ、リスクを転嫁する、すなわち保険に加入するなどに対策原資を割り当てるという経済原理が働き得ることも憂慮するべきである。
したがって、外部委託先において必要となる対策は、委託元が仮に外部に委託しないとすれば、どのようにリスク評価し対応するかを自身で検討し、それに基づいて講じるべき対策が何であるかを決定し、それを委託先に示すことが基本である。
(4) どちらがリスク評価するのか？（業務専門性を有するのが委託先か委託元か←Who）
委託元がリスク評価と対応選択に基づいて情報セキュリティ対策を決定して指示するのが基本であるが、委託する業務の専門性を委託元が有していない場合には、それは逆に現実的ではなくなる。この場合には、業務の専門性を有する委託先がリスク評価から対策決定までの一連のことを実施する方が、効果的な対策を期待できることになる。
この場合には、委託する業務の実施能力を評価するのと同様に、情報セキュリティ対策の実施能力を評価することに手間をかける必要がある。
(5) どの種類のデータを取り扱う業務を実施するのか？（個人情報を取り扱うソフトウェア開発の例←What）
委託する業務の種類は多種多様であり、それぞれに特定するリスクを検討しなければならないが、ここではＩＴシステムのソフトウェア開発で個人情報を取り扱う場合において、日本固有の問題があることを例にあげる。
ソフトウェア開発の検収時の受け入れ検査ではテストデータが必要となるが、個人情報を処理するソフトウェアの場合には、テスト用の個人情報が必要になる。
このとき、実際の個人情報をテストに用いることは、情報セキュリティ対策として好ましくないが、ソフトウェアの受け入れ検査としては品質確認の精度を高めるのに役立つ。このことは、アルファベット文字しかない欧米では、容易にテストデータを生成できるのに対して、外字や名寄せ、文字コードの問題を持つ日本では、実際の個人情報を使うより確実なことはないという違いがある。
委託元企業として好ましくない実際の個人情報を使うという手法は、委託先側のみでなく委託元担当者にも誘惑を与える。なぜなら、実際の個人情報ではなく、テストデータを使って受け入れ検査を合格させた後に、実際の個人情報でソフトウェアの不具合が生じた場合には、瑕疵担保を課していたとしても業務に悪影響が出れば、受け入れ検査の委託元担当者の責任が問われかねないからだ。
一般的に、実際の個人情報をテストに使うことを禁止している場合には、本来、委託元がそのような情報を委託先に提供しない限り、違反は起こりにくい。ところが、ここで示したように、委託元の担当者にとっても利点があると違反が起こりやすくなる。
この問題を解決するためには、日本語特有のテスト用の個人データが工業標準規格などのような第三者的な立場で用意され、それを用いたテストによれば、委託元担当者と委託先の双方の責任が軽減される必要がある。

委託元と委託先の利害関係が一致せずに、双方のけん制効果が生じる問題は顕在化しやすいが、ここで示したような例では、組織として実態が把握しにくくなりやすい。委託元企業は、決定した対策が、委託先ばかりではなく、自社の委託発注担当者にとっても過度の負担になっていないかを十分注意する必要がある。

(6) 誰が対策を実施するのか？（←Who）

外部委託の情報セキュリティ対策を考える場合、業務を実施するのが委託先であることから、対策の実施者が委託先に限られるかのような錯覚をしやすい。しかし、保護すべき情報は委託元の情報であることから、一次的な情報取扱者は委託元であり、対策の最初の実施者は委託元であると考えるのが自然である。委託する業務に必要のない情報を取り扱わせないようにするのは、委託元の責任であり、業務に必要最小限の情報だけに使用を制限するようにしなければならない。業務に必要のない情報までを委託先に提供しておきながら、それらの余分な情報の保護までを委託先に求めることは、委託元の情報セキュリティ対策として無責任である。

したがって、外部委託の情報セキュリティ対策は、委託元と委託先双方で実現することは当然である。

以上のことから、外部委託における情報セキュリティ対策の改善として以下のことが言える。

①派遣と請負は実態に即して区別した上で、派遣業務については、委託元が情報セキュリティ対策の責任を持つべきである。

②作業場所についての物理的（施設的）情報セキュリティ対策の責任は、派遣か請負かや、委託元か委託先かにかかわらず、その場所の所管者が持つべきである。

③請負業務においては、結果責任だけを偏重することなく、リスク評価、対応選択、対策決定については、委託元が実施して委託業務と同様に委託先に具体的に指示することを基本にするべきである。

請負業務において、業務の専門性を委託元が有していない場合に限り、委託先にリスク評価、対応選択、対策決定を依頼することができる。ただし、その場合にも結果責任に過度の保証を求めてしまうことで、リスク軽減としての未然防止よりもリスク転嫁がリスク対応として選択されることにならないように注意すべきである。

④外部委託において、委託元が実施すべき対策についても予め委託先に対しても明示すべきである。これに委託元が違反している場合に委託先がそれを報告又は相談しやすいような環境整備をすべきである。

⑤外部委託において、委託先のＩＳＭＳ認証やプライバシーマーク認証の取得の有無を参考にする場合には、それらの認証対象範囲に注意しなければならない。委託する業務と無関係の業務については、無意味な確認か過剰な要求になるからである。また、委託する業務が委託先にとっての定型業務ではない場合には、業務を委託するより前の時点での認証取得の効果についても注意すべきである。

⑥請負業務において、個人情報を含むソフトウェア開発を委託する場合には、実際の個人情報をテストに使わないとするのであれば、その動作確認をするためのテストデータが標準化されることが期待される。さらには、外部委託に限らない問題ではあるが、同一の日本語に対して複数の日本語コード体系を併用しているという特異な状態を改善することも、動作確認に実際の個人情報を用いるという悪慣習の是正には一助になるものと考えられる。