第３回 クラウドサービスの安全性評価に関する検討会 議事概要

日時 ： 平成 30 年 11 月 22 日（木） 15 時 00 分～17 時 00 分
場所 ： 経済産業省 別館２階 235 各省庁共用会議室
議題 ： 情報と情報システムのクラス分け・監査主体等について

１．情報と情報システムのクラス分け・監査主体等について、事務局より説明

２．委員からの主な意見は以下のとおり。

【管理策について】
○あるリスクに対して対応方法が複数存在しうる中、管理策で特定の対応方法まで規定するのか、目標という形で規定するのか、その書き方を整理していく必要がある。
○政府としては期待するコントロールレベルを示し、プロバイダ側がそのレベルに相当する管理策を実装しているということを責任をもって説明するという仕組みが必要ではないか。
○管理策を抽象的に設定すると、監査人の質によって監査結果にばらつきが生じる懸念がある。他方、管理策を詳細に設定すると対応コストが上がるため、セキュリティが前提だが、費用対効果も考慮して粒度を検討すべき。
○クラウドの技術革新に対応するために、管理策に上位基準と下位基準を設けて、下位基準を柔軟にアップデートする体系とすると良いのではないか。
○必須の管理策と選択的な管理策とに分けて、選択的な管理策については、選択肢を設けるほかに、管理策として期待したい水準を例示するのも良いのではないか。
○クラウドは変化するものであるので、技術革新を阻害しない程度の管理策を固定し、その具体的な対応策の解釈作業を一定期間ごとに行うことも考えられるのではないか。
○調達前の安全性評価の枠組みの中に入ってこない SLA の部分については、SLA の例などがあると使いやすくなるのではないか。

【情報と情報システムのクラス分けについて】
○情報システムのクラス分けを行う場合、「業務単位」ということでは幅が広い表現となるので、粒度を明確にした方がよい。
○業務ありきになり過ぎて、全く異なるシステムを一つのシステムとして構築する場合が見受けられるが、そういった場合にはシステムそのものを分けるという考え方も示すべき。
○クラウドとオンプレミスでは可用性の概念が異なるため、十分検討が必要である。

【監査主体について】

○実務的な観点と品質担保の観点から、監査主体は法人単位で担うことが現実的ではないか。

○法人単位で担う場合であっても、法人に所属する個人についても、特定の認定資格を保有していることを要件に含めることを考えておいた方が良い。

○監査スキームを維持・担保するために、資格・研修等を通じて監査人の品質を確保することが必要である。監査スキームを維持・担保する組織づくりも検討する必要があるのではないか。

○監査を担う主体の要件として、既存の国内の認定制度も参考にできるのではないか。

【その他（フレームワーク等）について】

○監査という言葉が示されているが、諸外国では認定・認証の仕組みを採用している。今回のフレームワークの位置づけを確認すべき。

○海外の場合、民間認証機関を活用する第三者適合性評価活動を、あくまで二者監査の代行と位置づけて、二者監査と第三者適合性評価の中間にあたる認定制度を採用しているのではないか。

○求める基準と、評価結果の基準に差があった場合に、全く使えないということとなるのか、あるいは継続的なチェックを行うということで使用することとするのかなど、整理が必要。

○認定後のサービス変更について、サービス全体を再監査するのか、あるいは変更部分のみを監査するのか等、方法・対象を整理すべき。

○評価制度を経たサービスについて、評価を経たものであれば、安全性については調達の際にそれだけでよいものとするのか、再度中身を見比べる必要があるのか、という部分については明らかにするとよい。

○過去の事例を用いてもよいので、今回のフレームワークに則ってプロバイダがクラウドサービスを構築した場合に、費用がどの程度変化するのかのシミュレーションを行うべき。

○クラウドを活用に際して管理策を実施してセキュリティを高めた場合でも、オンプレミスの場合よりも費用が安くなるというような実例を示していくことが重要。

（以上）