第５回 クラウドサービスの安全性評価に関する検討会 議事要旨

日時 ： 平成 31 年 2 月 12 日（火） 17 時 00 分～18 時 30 分
場所 ： 経済産業省 本館２階 西３共用会議室
議題 ： 監査の枠組み、登録されるサービス、シミュレーションについて

1. 監査の枠組み、登録されるサービス、シミュレーションについて、事務局より説明

2. 委員からの主な意見は以下のとおり

【監査手続について】

〇外部監査における標準監査手続は、直接評価を行う場合の手続と、内部監査結果を間接評価する場合の手続とで異なってくる。両者の手続の違いを識別して、きちんと定義しておく必要がある。いずれも、既存の監査技法をどのように参考とし、利用するかが重要。

〇監査の時点で有効でなくとも、プロバイダに継続的に改善を求めるということも想定されるのではないか。

〇監査とは、ある時点でできているか、できていないかを評価する、一種の健康診断のようなもの。継続的に改善しているような場合には、改善してから評価を受けるべき。監査の時点でできていなければやはり不適正となるのではないか。

〇サンプリング数の議論は、既存の監査基準を参考にしながら検討していくのが良いのではないか。

〇コストを下げるために少ないサンプルで見るということもルールとしてはあり得るが、それは必然的に運用を行っているプロバイダの信頼性が少し下がるということになる。これはある種の決めの問題。

〇監査の効率化に向けて、IT 技術を活用した監査の電子化・自動化を検討していくべき。

〇監査を行う領域によって自動化がしやすいところとそうでないところがある。また、監査を自動化するにあたっては、被監査側が電子化・自動化に対応しているかという部分も関係してくるので留意が必要。

〇クラウドサービスの安全性評価における「安全性」とは、政府が許容できないリスクに対して、プロバイダが適切に対応しているということであり、想像もできないようなリスクへの対応まで求めるものではない。想定されるリスクに対応していくためにどのような管理が必要か、その管理が有効に機能しているかという位置づけのものであると理解すべき。

〇そもそもセキュリティ対策を実施する責任はプロバイダにあり、プロバイダは内部監査でサービスが安全であることを確認したうえで、自らのサービスが安全であることを宣言するというのが、セキュリティ監査全般のベースとなる考え方である。

【内部監査について】

〇内部監査の重要性が増しているが、日本の内部監査部門には、組織における位置づけ・能力・リソースといった点で海外に比べると弱い部分も存在する。

〇プロバイダの中には、日本国内に内部監査機能を有していない場合もある。その場合のやり取りを海外にある本社側に行わせるのかどうかを含めて検討していかなければならない。

〇内部監査と外部監査のコストについて、単純に外部監査は内部監査よりも高いというロジックではないのではないか。単価が同じ人間が実施すれば工数が同じということになり、社会的に見ればコストは変わらないはずである。

〇内部監査のメリットは、多様な監査要求がある中で、同じ項目について他の監査結果を使っても良いとした場合に、作業の重複が回避できるところにある。そのあたりのロジックをしっかりと整理しないといけない。

〇内部監査についても自動化を図ることで、コストの効率化も実施していけるのではないか。

【クラウドサービスの動的な要素について】

〇統制目的に対してプロバイダが実装した技術の有効性を、監査人が評価できるのかという問題がある。新技術が出てきた場合には、中立的な機関で技術検証を行って、適当な技術の例示として追加していく必要があるのではないか。つまり、基準自体は変わらないが、解釈が動的に変わっていくということになるのではないか。

〇実際に制度を運用してみると、ガバナンスの変化など、その都度監査が必要かどうかを判断する必要が出うる。制度立ち上げから 3 年間くらいは、運営を見守る仕組みを含めて、手厚い対策をとるべきではないか。

〇制度が動的な変化に対応できず、政府がレガシーシステムしか使えない、ということは避けるべきなので、変化への対応については継続的に検討していく必要がある。

〇ビジネスモデルが変化して従量課金等のモデルが出てきており、政府としてそうしたサービスを調達することも想定されるため、そういった調達のあり方そのものも継続的に検討すべき。

〇技術評価・検証を行うホワイトラボの設計・カバー範囲等について検討を進める必要があるのではないか。

〇ホワイトラボは、各省庁連携した形で作っていかないとうまくいかないのではないか。また、グローバルとどう連携していくかという視点も含めたグランドデザインを作っていく必要がある。

〇時代とともにクラウドに関するリスクも変わるため、制度運用の中にリスクの検討を行うための仕組みを設け、基準改訂と同じようなタイムスパンでリスクの見直しも行うべきではないか。また、想定していないリスクが発生した場合の対応も考えるべきではないか。

【シミュレーションについて】

〇シミュレーションは本登録に向けた事前評価とは性格が異なる点を明確にしておく必要があるのではないか。

〇監査品質を高めることは良いが、クラウドサービスのコストメリットが圧縮されてしまうとサービス利用に対するモチベーションが圧縮されてしまう。品質とコストとの調整を意識してシミュレーションを実施してほしい。

【その他】

〇監査を行うことで今までよりコストが上がり得るが、セキュリティがしっかりとしたサービスであれば、多少コストが上がっても採用するということを、政府からプロバイダ側へ示すことが重要である。

〇行政側の手続や体制を整えていく際に、それに係るコストも忘れずに検討を進めていく必要がある。

〇クラウドサービスとオンプレミスでシステム構築のアーキテクチャは大きく異なる。オンプレと同じアーキテクチャでクラウドを構築しようとすると高コストになる。クラウドとしてのアーキテクチャや構築手法を考え、登録されるクラウドサービスをどのように使っていくかも研究していく必要がある。

〇SaaS は特に多様性があるため、SaaS に対応した管理基準や監査基準についても多様性が求められる。管理基準や監査基準をどのように適用していくかについては今後検討が必要である。

（以上）