第２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 10 月 19 日（金）　10 時 00 分～12 時 00 分
場所　：　総務省（中央合同庁舎第２号館）10 階第１会議室
議題　：　クラウドサービスの安全性評価の枠組み等について

１．クラウドサービスの安全性評価の枠組み等について、事務局より説明

２．国内の認証制度について、委員より説明

３．委員からの主な意見は以下のとおり。

【フレームワーク・プロセスについて】
○クラウドサービスの安全性評価における問題は、グレーの評価になることが多く、各省庁がホワイトリストに載っていないクラウドサービスを調達する際の扱いについても検討した方がよい。
○現在のシステム調達の細かなプロセスとのマッチングを適切に実施しないと制度の実効性確保が厳しくなる。
○調達単位によって調達プロセスの方法が変わってくることも考慮すべき。
○国が最終的に監査主体を決めるとしても、その認定に関する審査活動は、専門機関が国にも民間にもあるので、そういう組織を活用した方がよい。
○安全性評価の枠組みにおいて、SIer が間に入ったときに、それをどのように活用するのかということを考えておいた方がよい。

【整備文書について】
○調達前の管理基準と更新時の管理基準の双方で差が生じると、極端に言えば、運用時点では、調達前の管理基準は無視してよいというメッセージを与えてしまうことになりかねない。
○安全性評価のスキームそのものの方向性については、全く異論はない。日本において、IT 監査のリソースが量的に少ないことを考えると、文書類の充実が必要で、熟練していない監査人でも文書類を見てきちんと監査できるようにならなければいけない。
○海外の政府認証制度の例にもあるように、細か過ぎる基準を出すと、それだけ内部コストが負担になってしまうので、実際の審査コストが安くても制度が回らなくなってしまう可能性がある。

【技術の活用について】
○監査費用を抑えるために、IT を使ったデータ収集の自動化を考えておくことはとても重要である。
○技術の評価・検証について、試験をそれぞれの会社が全て個別に実施するのは大変な作業であり、不可能な場合が多い。第三者機関として信頼できる評価結果を示すホワイトラボのようなものが重要。

【その他】

○マイクロサービスの形態で新しいサービスをいろいろと生み出せるような API を切り出しておいて、ベンチャーを活性化して、それらをダイナミックに組み合わせてサービスを構成していくというクラウドネイティブの考え方や、モニタリング機能の業界標準化の動きを取り込むのかどうかが今後大きな判断になる。

○監査人を育てる仕組みについて考慮しなければ、監査人がボトルネックになって、ホワイトリストに載るクラウドサービスの数が必然的に制限されていくことになり得る。

○自治体での活用を考えた場合、地方でデータセンターを運営している事業者も多く存在する。厳しい基準を作った場合、その認証を取得できるのは、大手の事業者となる。地方でデータセンターを運営しているような中小の事業者のところまで考えて、基準のレベル感について適切に決めていく必要がある。

○コストを抑えることが大変重要であることは理解しているが、国の調達ということを考えたときに、セキュリティリスクがあって、それに対応していくことが必要になる事態もあり得る。コストのことばかり考えていると、もともとの目的である政府として大事なデータをどう守っていくのかという部分が達成できないということが起こってしまう。

○きちんと情報の分類を考えながら、やるべき事はしっかりやるという仕組みの中で、どのようにコストを抑えられるのかを考えるべきで、コストを抑えたいからといって順番が逆になるようなことになってはいけない。

（以上）