第４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 30 年 12 月 17 日（月） 10 時 00 分～12 時 00 分
場所 ： 経済産業省 本館２階 西３共用会議室
議題 ： 中間整理

１．中間整理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
【責任分界点について】
○政府機関、プロバイダ、監査人の責任分界点がある。
○プロバイダ側が、自社のサービスとしてどこまで見ているかを明確化するしかないのではないか。
○監査のほうは責任分界点の議論は難しく、保証のレベルの話になるのではないか。
○監査については、管理基準に対して実際にコントロールが設計されているかという「整備状況」の評価と実際に適用されているかという「運用状況」の評価の２種類があり、後者まで行うべきではないか。
○プロバイダの自己宣言書に基づいて監査を行うことを想定した場合、そのフォーマットとして海外の事例も参考になるのではないか。
○管理基準の解釈に幅が生じないように、プロバイダとカスタマの定義をモデル等で整理することが重要。
○複数プロバイダのサービスを組み合わせる場合の責任分界点がどうなるのかも整理するべき。
○サプライチェーンの問題やSaaSを含むサービスの組み合わせを想定すると複雑になるので、議論の対象を絞って進めていくべきではないか。
○政府調達においてシステムを構築することが多いSIerの位置づけについて議論するべき。
○単純には、SIerがサービスを提供するときにはその用いるクラウドサービスが評価済みリストに載っていることを求めるというふうに整理をすることも考えられる。
○SIerがリスク込みで検討した結果、政府が直接契約を行う方が好条件の場合も出てきうる。

【管理基準について】
○管理基準というのは調達前と更新時で変わらないが、更新時に管理基準の中でどれだけの基準適合性を見るかは場合によって変わるかもしれない。
○政府機関が管理基準に対して想定する対策例を残しておくことが重要。
○政府と民間、民間の中でも企業にごとに情報のクラス分けに違いがあり、政府の管理基準を参考に民間独自に基準をつくることも想定されるので、何を想定した管理基準かを明確にすると民間に広まる際に使いやすくなるのではないか。

【監査基準、監査期間について】
○監査を行う者同士の横のつながりにより、技術進歩等に応じた、監査手続きの相場観が醸成されるような仕組み作りをすることが重要。
○監査の更新期間と、監査の際に見る対象期間にギャップが生じる可能性があるので、これらの関係を整理する

必要がある。
○管理策が決まると、プロバイダは自身がそれに適合していることを証明するという気持ちで宣言をし、その宣言が信頼できるかどうかを監査人が調べるという構図は、結論としては変わらない。
○今後の議論だが、既存制度の認証・監査結果については弾力的に援用できるようにするべき。
○監査を行う際にテクノロジーを有効に活用することが重要であり、これはまさしく事業者が工夫できる領域。ただし、監査として自動化ができない範囲も存在することに留意が必要。

【評価済みクラウドサービスのリストについて】
○監査、自己言明に要する時間軸や更新期間を踏まえて、リストの有効性について整理する必要がある。
○評価済みリストに載っていないクラウドサービスを利用したい場合の扱いを整理する必要がある。仮にそのようなサービスの利用を認める場合でも、調達側にこの制度と同等以上の安全性評価を求めることを最低限するべきではないか。
○載っていないクラウドを使うとき、リスクアクセプタンスということもやはり考えていかなければいけない。
○BCPの関係で単なるバックアップサイトとしてクラウド業者を使うケースを、同じように評価するのかという論点もあるのではないか。

【クラウド技術の特徴について】
○クラウドの世界、ITの世界は技術が進み、セキュリティ等に対しても対策はどんどん変わっていくことが想定される。
○イノベーティブなテクノロジーが多く出ることを期待したいので、監査基準を細かく縛ることでこれを阻害することは避けるべき。
○ベンダーロックインの問題についても検討をするべき。

【その他】
○本検討会で検討されている制度は政府がクラウドサービスの安全性評価のために監査・検査を行うものであり、認証制度ではなく、既存の民間認証制度とは異なるという点を明確にするべき。
○システムのセキュリティの監査は民間でも不十分な部分があるので、民間での品質管理に関わる産業の育成にもつながるとよい。
○政府主導で体制の整備と試行を行うことで、重要インフラ分野に対する見本になっていくとよい。
○IaaS、PaaS、SaaSの切り分けを効率的に行うことは難しいが、典型的なモデルのようなものを想定する必要があるのではないか。
○実際に制度を運用する場合の時間、コスト、スケジュール感などを早期にシミュレーションするべき。
○SLAというのは、目標値未達の場合には料金を取らないだけとも言える。この場合、監査が可能な範囲と実際のサービスの間にギャップが残りかねない。
○特に地方でデータセンター、IaaS、PaaSを提供する事業者については、審査等に要するコストの影響が気になる。

（以上）