第 9 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 ： 令和元年 12 月 3 日（火） 17 時 00 分～19 時 00 分
場所 ： 経済産業省別館 2 階 227 各省庁共用会議室
議題 ： 監査シミュレーションに関する報告、調達・構築関連調査に関する報告、とりまとめ（案）について

1. 監査シミュレーション結果について事務局より説明

2. 調達・構築関連調査について委託先事業者より説明

3. とりまとめ（案）について事務局より説明

4. 委員からの主な意見は以下のとおり。

【とりまとめ（案）の記載について】
○調達と、その後の運用における基準が今まで大体バラバラであるのが一般的であったが、これらを一体としてやることは政府としても初めてに近い取り組みではないかというのを、少ししっかりと書いたほうがよいのではないか。
○重大な統制の変更について、例えば、基盤部分を変更しているにも関わらず統制変更を行わず、制度側に届出がなされないというケースも想定される。届出等の対応を求めるのは、正確には、重大な統制の変更が発生した場合ではなく、重大な統制の変更が必要とされる環境の変化が発生した場合ではないか。そのように読み取れるように記載を工夫すべき。
○監査主体登録基準に関して、クラウドコンピューティングに関連する知見も監査人に求める要件として追記すべき。
○制度立ち上げに向けたスケジュールに関して、引き続き管理基準や監査手続の作成を行っていかなければならない。必要な検討は決められた時間内に実施しなくてはならないが、2020 年秋から登録簿の運用を始めるというのは時間的に厳しいのではないか。しっかりとした制度を構築するためにもあまり性急に検討を進めることはできないのではないか。
○技術変化や ISO の改訂等を踏まえて管理基準の見直しを行っていくことを考えると、数年に一度程度の頻度で大幅な見直しが発生するということを念頭に置いておくべき。
○監査コストの低減に向けて引き続き検討を行う旨入れていただきたい。

【今後の詳細な基準等の整備について】
○サービスが登録取消しになった場合、利用者側ですぐに他のサービスに移行するということは難しい。実務を考えれば、そのまま使い続けることになることが想定されるが、その場合のリスクは誰が負うのかも整理を行う必要がある。
○登録簿に登録されたサービスに重大なインシデントが発生した場合、誰がどのような手順で再調査を行うのか、また、その場合に登録簿上のステータスはどうなるのかという点についても検討しておく必要がある。
○制度立ち上げ時の経過措置の適用期間、軽微な発見事項の場合には登録が認められるということだが、その判断基準も整理いただきたい。
○長期的な制度運用を考えたときに、監査主体によって品質のばらつきが生じないよう、品質確保のための仕組み作りを行うことが重要。例えば、監査人に対して監査の実務にまで踏み込んだ研修の受講を必須とする、実務を行う際に参照できるようなガイドラインを作成する等、具体的に検討を行う必要がある。

【制度活用側における論点について】
○諸外国ではクラウドサービス調達・構築時のセキュリティ上の留意事項も整理している。日本においても、本調査結果を踏まえて、クラウドネイティブのシステムアーキテクチャ、ゼロトラストのネットワークセキュリティモデル、DevOps 等を前提とするセキュリティ上の留意事項を整理する必要がある。
○本制度はあくまで事実を提供するものであり、調達側で言明書等に記載されている事実に基づいて判断を行うことが前提となっているが、言明書等は読み慣れていない人にとってはハードルが高い。文書類の読み方の手引きやベストプラクティスを整理することも検討すべき。
○例えば、IDS、IPS を仮想マシンで作る場合のようにクラウドの仮想化が進んだケースも検討できると、セキュリティ監視サービスの契約のあり方等の見直しにつながりうる。そこまで踏み込んだ検討とできると良い。
○ISO/IEC 27017 では、CSP だけではなくカスタマ側で実施すべきことも定義されているので活用頂きたい。
○クラウドの場合、ユーザー側でもリアルタイムにサービスの運用状況を確認することができる。そのような機能を活用してユーザー側での利用のあり方についても検討を行う必要がある。政府全体のクラウド政策にもつながる話であることも認識して検討いただきたい。
○政府全体として調達後の運用部分もしっかりと見る仕組みを整備する必要があるが、そのためには、調達側で情報システムやクラウドコンピューティングの技術に精通した人材を確保し、待遇面、キャリアパスなども改善していかなければならない。

【その他】
○審査で確認する資料量が膨大となることが想定される。審査を滞りなく実施するために、事務手続とシステムの整備も進めておく必要がある。
○ユーザー、CSP、SIer、監査人、コンサルタント等、本制度に関係する人々が理解できるような制度としていかなければならない。
○調達関連の調査結果は政府のシステムを対象に実施されているが、報告書において示される利用者側の心構えは民間でも参考になる。
○制度運用の実務を担う主体とも上手く連携していただきたい。

【とりまとめ（案）の扱いと、今後の検討について】
○とりまとめ（案）の扱いは座長一任とし、事務局と相談ののち、パブリックコメントを実施する。
○今後の基準等の詳細な検討は WG にて検討を行い、政府において最終的な決定を行うものとする。

（以上）