第８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 10 月 28 日（月） 10 時 00 分～12 時 00 分
場所 ： 経済産業省別館 11 階 1111 各省庁共用会議室
議題 ： 中間とりまとめからの進捗と立ち上げに向けたポイント、制度における評価の考え方、監査結果と登録の関係について、期間の考え方、「他のクラウドサービスを利用したクラウドサービス」の登録の在り方について、管理基準 WG 報告、監査 WG 報告、シミュレーションの状況

1. 事務局説明資料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。

【制度における評価の考え方について】
○通常、調達側が登録結果を踏まえて調達時の要件を検討する際、セキュリティに対して保守的になるので、「この管理策はいらない」という事が言えずに、非効率なものとなりかねない。登録簿ができた後でも、こうした発注側と調達側の要件のすり合わせという問題は残るので、登録簿を活用した調達の際の留意事項のようなものも引き続き検討いただきたい。
○本制度は CSP がどのようにセキュリティ対策をしているかのファクトを提供するものであり、調達側はそれに基づいて判断を行わなければならないが、こうした情報のレポートは読み慣れた人でないと理解するのが大変。調達側が報告書を読み解く際のプリンシプルのようなものもあわせて検討する必要がある。
○これまでの政府調達は、一度調達すると後はプロバイダに任せきりだった。これがクラウドになると、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ようになるので、一度監査を受けたら終わりではなく、継続的にサービスの利用方法を見直すようにしなければならない。

【期間の考え方について】
○サービスが登録抹消になった場合を想定して移行期間のようなものも設けておかないといけない。そうでないと、ユーザーからすると、登録が抹消された途端に認証されていないサービスを利用しているというような事態が生じてしまう。諸外国の制度等も参考にしながら、登録保留や一時停止等のステータスを設けることも検討いただきたい。
○「基準日」や「言明の対象期間」等の用語の定義を明確に行い誤解のないようにすべき。

【「他のクラウドサービスを利用したクラウドサービス」の登録の在り方について】
○クラウドのサプライチェーンには、SaaS/PaaS/IaaS という上下のサプライチェーンと、ID 管理やセキュリティマネジメント等一部の機能について他のクラウドサービスを利用するような横のサプライチェーンがある。これまでの議論においては、前者の登録の在り方が整理されてきたが、後者のようなサービスは必ずしも単体で登録されるとは限らないので、こうしたサービスの在り方についても検討を行う必要がある。

【管理基準 WG 報告について】
○可用性の観点から管理基準を確認いただきたい。事業継続に関して言えば、ISO は非常にマクロな意味でのコンティニュイティを要求している一方で、SP800-53 はミクロな観点から要求している。クラウドサービスの運用において可用性が問題になるような事例を想定して必要な対策が含まれているか確認いただきたい。

【監査 WG 報告について】
○言明書等に記載される情報の開示範囲を詳細に検討すべき。
〇SaaS を調達する際には、SaaS の監査報告書だけではなく基盤側の報告書も必要になると考えられるが、調達側で基盤側の報告書まで請求できるのかという点も検討していただきたい。
○本制度はユーザー企業も注目している。登録されたサービスに関する情報が民間に対してどこまで公開されるのか、具体的なイメージがあると良い。
○「重大な変更」には、統制環境の変更だけはなく、システム構成の大幅な変更も含まれる。そのことが分かるように記載すべき。
○ある CSP が複数のサービスを登録する場合、すべてのサービスにおいて同じ監査手続を実施しなければならないのか。管理策によっては組織として一度監査をすれば済むものもあるので、既に登録されているサービスがある場合には追加部分だけを監査するといったように柔軟な対応が認められるべき。
○CSP の企業としての存続やサービスの継続性といった点も登録簿の信頼性という観点からは重要となるので、この点についても制度として検討しておくべき。
○管理策をしっかりやっているかということの確認と、そもそも登録申請を受け付けるかどうかの確認は概念が異なる。後者は管理基準とは別に整理を行うべき。

【シミュレーションの状況について】
○監査コストに関して、IaaS や PaaS といった基盤部分と SaaS では対象となる管理策の内容が異なるはずであり、その点も含めて検討いただきたい。また、運用状況評価の効率化等を含めて、工数削減に向けて引き続き検討を行っていただきたい。
○監査コストは監査項目と監査人の単価で決定される。前者は管理策数によって決まり、後者はクオリティとのトレードオフ。その中でどこまで効率化できるかということだが、サンプリングやローテーション等の監査の手法を組み合わせることでコスト削減の余地はある。ただし、あまり大胆なことをするほどリスクが高まるということも認識しておくべき。
○本制度に対する CSP の関心は非常に高く、登録簿に載ることでサービスの信頼性を世の中に対して示すことができると考えている CSP もいる。そういう意味では、監査に係る費用もそのために必要なコストということで、必ずしもそのまま府省庁のサービスに対して配布されるというものでもないと考えられる。

【その他】
○これまで日本においては第三者評価や監査はあまり行われてこなかった。これには、大丈夫であると自己宣言している内容を盲目的に信用することや、業務執行部門などの企業の第一線のクオリティが高いということにより、ある程度中で社会が成り立っていたという背景がある。しかしながら、昨今のセキュリティ事案を見ている限り、そういった論理がもう成り立たない状況になっている。今回の制度に限らず、第三者評価をインフラの中に組み込んでいく必要がある。

（以上）