第６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 3 月 1 日（金） 15 時 00 分～17 時 00 分
場所 ： 総務省（中央合同庁舎第２号館）８階 第１特別会議室
議題 ： 中間とりまとめ（案）について

1. WG における検討状況について、WG 座長より説明

2. 中間とりまとめ（案）について、事務局より説明

3. 委員からの主な意見は以下のとおり。

【中間とりまとめ（案）について】
〇今回、よい議論が出来ている部分を反映いただいていると思う。今後の活動として、制度ができたということで終わらせず、「実行可能性」が大事。
〇クラウドはまず運用が主体であり、変化を覚悟しなければならないという点をしっかり認識した文面になっているのは非常によい。

【今後の制度の立ち上げについて】
〇実効性のある制度とするためには、制度立ち上がりの時点で一定程度主要なプロバイダが参加していることが非常に大事になる。そのためには、プロバイダや監査主体を含めて準備を行っていく必要がある。
〇制度立ち上げに要する期間や監査主体の数に限りがある一方で、立ち上げ時に一定数のサービスを登録しておきたいという点を踏まえると、工夫して準備を進めていく必要がある。
〇今回の制度に対する民間ユーザー側からの期待も大きい。早く立ち上げ、ロケットスタートを切ることが出来る仕組み作りをしていただきたい。
〇過去の制度立ち上げ例では、企業規模やその事業範囲によって異なるが、新しい基準で監査を行うとなると、内部監査に６～8 か月、その後、外部監査への適合可否の調査に１～２か月、外部監査で３～４か月と、ほとんど１年掛る。
〇プロバイダが登録プロセスを進める上での事実上の前提条件が内部監査であり、2020 年秋に制度開始を目標とするのであれば、プロバイダに早めに方針を示しておく必要がある。
〇時間がかかるという点は理解できる一方で、クラウドのこの時代で２年後に登録に載るとなると、使いものになるのか、という話にもなり得る。スピード感をもって進めてほしい。

【基準におけるサプライチェーンの考え方について】
〇基準においてクラウドサービスのサプライチェーンを考える際、クラウドサービスカスタマは必ずしも政府機関とならないのではないか。例えば、IaaS を PaaS 事業者がこれを使う際には、PaaS 事業者はカスタマになるのではないか。
〇既存の認証制度として、クラウドサービスカスタマの認証制度が存在しているように、プロバイダであると同時にカスタマの側面があるという点は理解。
〇（一方、基準はあくまでも政府からプロバイダに要求するものであり）政府から見れば SaaS プロバイダが IaaS のプロバイダを使っているか否かは関係がなく、政府が求める基準を満たしている SaaS であることだけが確認できればよいので、政府からの視点においては SaaS プロバイダをカスタマとして見る必要はないということ。

〇政府とプロバイダとの間の責任分界点を明確にした上で、プロバイダ側で実施すべき部分について、政府が求める基準を満たしているかどうかを政府が確認することとなり、サプライチェーンについてはプロバイダが責任をもって対応するということ。

【サービスの粒度について】

〇登録簿に載るサービスの粒度と、調達側で使いたいと考えているサービスの粒度が必ずしも一致しないのではないか。

〇基本的にクラウドサービスは、プロバイダが自分のサービスを定義し、範囲を決めてカスタマに提供しているため、それを１つの単位として監査を行う。監査を受ける際に示した管理範囲等がサービスの範囲と一致しているかどうかということは非常に重要な問題であり、厳しく見る。

〇他方、調達側で考えているサービス範囲が監査対象からはみ出る部分については個別のカスタマ側で確認するということ。標準的な部分についてはここまでできている、という以上のことを制度でくみ取ろうとすると複雑になり過ぎ、非常に個別のケースに振り回されることになる。

【監査について】

〇調達者として仕様書を作り、提案に対して判断するという立場から、監査報告書に何が記載され、誰にどのようなタイミングで開示するのか、また、登録簿には監査報告書そのものが載せられるのか、あるいはサマリーだけを載せるのかという点も検討しなければならない。

〇他の監査制度・認証制度で使用した資料等を活用することで、監査の効率化が図られる。他の機関がチェックした資料等を共有するためのルールを設定しておく必要があるのではないか。

〇当面の間、毎年更新監査を行うとなると、コストを含めてプロバイダ側の監査対応の負担が大きくなる。事業者側の負担がなるべくないような形で、なおかつセキュリティを担保しなければいけないという中で、どのように更新監査を行っていくのか留意が必要。

〇監査コストは最終的には調達コストに反映される。政府機関はそこを踏まえてセキュリティに対するコストを払い、結果として安心を買うというのが今回の制度の趣旨である。必ずしもプロバイダの負担を重くするものではない。

〇セキュリティ対策や監査を行うと当然コストが発生する。これをいきなり民間で行うとうまくいかないが、まずは政府で経験値を貯めて民間に展開するというように位置付けるのであれば、コストの増加分は必要な投資であるということになる。

〇コストは調達側で負担するというのは前提だが、そのためには、登録されたサービスが実際に使われるようにしていかないといけない。

【その他】

〇新しい技術に対応できるような仕組みが必要だが、それは制度をどこまでも柔軟にするという事ではない。

〇制度が悪用される可能性についても留意する必要がある。特に、監査部分については、技術専門家による助言や監査業務の第三者への委託などが検討されているが、信頼できる専門機関を早めに設ける必要がある。プロバイダは機微な情報を提出する必要があるが、信頼できるところでないと資料を出したくない。

〇「登録簿」という名称について、何を登録するのかがわかるような名称とすべき。

〇レガシーシステムをクラウドに移行するというのは理想だが、非常にコストが掛る。まずは、レガシーシステムがないところからクラウド利用を進めていき、その中で制度も使っていくという事ではないか。

4. 中間とりまとめ（案）の扱い。

議論を踏まえた中間とりまとめ（案）の取り扱いについては座長一任とし、事務局と相談の上、パブリックコメントを実施することとなった。

（以上）