第１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 8 月 27 日（月）　10 時 00 分～12 時 00 分
場所　：　経済産業省　本館 17 階　第１共用会議室
議題　：　今後の検討における詳細な論点等について

議事概要　：
１．今後の検討における詳細な論点等について、事務局より説明

２．委員からの主な意見は以下のとおり。
【検討の枠組】
○クラウドサービスを利用することになる情報の範囲の設定によって議論の範囲が大きく変わる。
○ガイドラインをつくるだけでなく、運用のプロセスと体制をどうつくるかということが重要。
○データ連携や競争原理、グローバル性とグローバル連携も考慮すべき。
○調達コストや申請コストもかかる。こういった費用や仕組みの整理も必要。
○政府でガイドラインや指針がまとめられて民間に提供されることは有効だが、大きくまとめて一つのガイドラインとなると使い勝手が悪い。そのレベル分けや、想定する利用形態の検討が必要。
○すでに、国際規格に基づく民間の認証制度が存在する。既存の民間レベルの適合性評価制度が最大限活用されるように議論すべき。
○これから新しいクラウドサービスを提供する際に技術の透明性について開示するという観点と、開示にあたってクラウドサービスを受ける側である企業の情報管理についても、しっかりしたものでないといけないという観点について、論点に含める必要がある。
○責任分界点については、クラウドを提供する側とクラウドを利用する側に加えて、監査する人や認証を出す人の責任がどこまでなのかという部分についても併せて検討する必要がある。
○調達要件の仕組みを作る際に、該当する事業者やサービスについてのホワイトリストのようなものを提供する仕組みにすることも考えられるのではないか。
○今後、民間でも同じように使えるようにすることを考えた場合には、コンプライアンス疲弊しないかどうか心配。企業の経営的なストラクチャーやプロセスの中に導入できるか意識して検討する必要がある。
○諸外国の制度の一部には、技術的な詳細を記載し、それが少し変わっただけで、その基準をまた書き換えるため、その前に取得した認証の賞味期限が非常に短いものになってしまうという技術進歩の問題がある。特にクラウドの世界では、このような問題をどのように担保するかが大事。
○基本的には、過剰な負担にならないよう、国際標準の枠組みの中で実施しながら、クラウド事業者がある程度自社やサービスのセキュリティのレベル感を説明できるようにする仕組みを検討する必要がある。
○さまざまな規定・ガイドラインがあって、実効性がないということが課題になっている。そのような状況で、更に新たな規定・ガイドラインを作ることがないようにするべきである。限られた期間内で、すべてについて検討することはできないので、何かに絞って検討する必要がある。
○調達基準やガイドラインの運用という言葉が出ているが、基準の運用の手前に、クラウドはシステムとして運用するところに価値がある。契約後の契約内容がしっかり履行できているのかという点が一番大切。

【具体的な基準等の策定について】

○サイバー空間上での情報の集まりだけでなく、クラウドサービスを運用するデータセンターの基準も重要。

○使い方によって基準の中身が異なるため、IaaS、PaaS、SaaS を切り分けて検討する必要がある。

○認証とした場合の対象が何かという点で、おそらくサービスを個別に見る必要があるが、それを提供している組織について、何も見なくてもよいということにはならない。

○実際に基準を作って運用していくことを考えると、物理的な話については、単純なデータセンターの立地場所の話以外にも、実際に使っている機材がどういうものであるかなど、実装上のところにまで踏み込まざるを得ないのではないか。

【実効性の確保について】

○調達後の契約に対するフレキシビリティや、どうサポートし、どう監視していけるかというところまで考えなければ実効性は出ない。また、基準自体もフレキシブルである必要がある。

○組織については、クラウド事業者が必要な要件を満たしていることを、認証によって判断するということがあってもよいが、使うクラウドサービスについては、サービスごとに、政府の要求仕様を満たしているかどうかを確認しなければいけない。その確認の方法は監査になるのではないか。

○監査について、既存の監査の仕組みを利用するという話であれば問題はないが、新たに別の基準を使って監査することになった場合には、監査の仕方やレベル感によってかなりの差が生じるため簡単な話ではない。チェックリストや監査手続き等の標準化が必要となる。

○認証の仕組みや要件・基準を満たしているか確認する仕組みに実効性を持たせるような具体的な手続をきちんと採り入れていかないと、基準を作ってもなかなか運用されないということがあるのではないか。

○情報や情報システムのクラス分けについては、概念を決めるだけでなくて、どのような情報はどれに該当するのかという事例集やリストをかなりきちんと作らないと、そのとおりに運用ができなくなる。

（以上）