

## 「クラウドサービスの安全性評価に関する検討会 中間とりまとめ(案)」 に対する意見

[提出者名]	在日米国商工会議所 (The American Chamber of Commerce in Japan)
[意見]	
<p>(ページ番号は中間とりまとめ(案)の中でコメントする箇所を示しています)</p> <ul style="list-style-type: none"><li>● (全体)日本には数多くのグローバルなクラウドサービスプロバイダー(CSPs)が存在していることを踏まえ、在日米国商工会議所(ACCJ)は政府が日本語と同様に英語でもパブリックコメントのプロセスを実施することを要望します。さらに、パブリックコメントの対象となる法令案等の英語版を発出することで、コメント提出に向けた検討や議論が促進されるものと考えます。</li><li>● (全体)製品/サービスの適用範囲は会社によって異なる可能性があるため、CSPs が評価のためにクラウドサービスにおける製品/サービスの単位を指定できるかどうかを明確にする必要があると ACCJ は考えます。</li><li>● (P7、参考図3)参考図3の説明が不明瞭であるため、この図についてさらに説明を加えていただくようお願いします。</li><li>● (P7 25 行目)情報システムが要求する可用性を満たすためには、複数の CSPs によるサービスを組み合わせて 1 つのサービスを構築する可能性が非常に高いと考えます。そのようなシナリオ下では、いずれかの CSP によって提示されたサービスレベルアグリーメント(SLA)が適切な測定値ではない可能性があります。SLA の測定方法自体も異なる場合があります。むしろ、可用性に関しては、特定の数値要件を提示するのではなく、完成した情報システムの SLA を指定するか、もしくは各 CSP が明確な SLA を保持しているかどうかを確認するほうがよいのではないかと考えます。</li><li>● (P10、8 行目)「運用状況まで踏み込んだ制度とすること」との表現がありますが、CSPs の業務を妨げる可能性のある詳細な要件を過度に記載することは推奨しません。このような運用上のステータスは、すでにクラウドサービスの一部として含まれています。</li><li>● (P10、16 行目)1 つの提案依頼書(RFP)に異なるレベルの複数の業務システムが含まれている場合、フレームワークの適用方法はどうかお示しいただくよう要望します。</li><li>● (P10、21 行目)「監査」におけるサービス単位の定義を明確にしてくださいようお願いします。</li><li>● (P11 参考図 5)CSPs が監査実施のタイミングと頻度を指定できるかどうか、あるいは監査主体が登録時に監査の有効期限を設定することができるのか明確化していただくよう要望します。</li><li>● (P11、参考図 5)監査主体については、CSPs が政府によって選定された候補の中から指名できる方がよいと考えます。</li><li>● (P11、7 行目)どのクラウド/サービスの単位が監査の対象となっているか明確にする必要があると考えます。</li></ul>	

- (P11、参考図 5) 監査が必要な項目は原則として管理基準に含まれ、個々のプロジェクトに対する追加の監査は最小限となるべきです。そうでなければ、事前に監査を実施することのメリットは非常に限られたものになるでしょう。
- (P11、参考図 5) 監査手続きは、データセンターに物理的にアクセスすることなく、文書を通じても実施できるようにすることを強く推奨します。例えば、既存の Service Organization Control (SOC2) コンプライアンスレポートや文書を確認することなどが挙げられます。
- (P12 15 行目)「その(監査)費用は政府の調達費用に反映される」という現在の計画に従うと、一部のグローバル CSPs はデフォルトではそのような商業的取り決めを持たず、またグローバルで整合性と透明性を維持するという観点から、追加の監査費用を顧客に請求できないため、さまざまな CSP 間で不公平が生じる可能性があります。
- (P12 17 行目)「システム調達全体としてクラウドサービス導入前よりも費用が下がるよう、制度設計する必要がある」と述べられていますが、そのような明示的な記述は避けた方が良いと考えます。パブリッククラウドサービスを採用する際の費用削減は数ある重要なメリットのうちの 1 つですが、運用費用の削減はすぐには実現しない可能性があることに加え、高いセキュリティなどといったその他のメリットも優先度を下げられるべきではないためです。
- (P13 20 行目) 仮に「物理的な基準」として日本データセンター協会のデータセンターファシリティスタンダードなどの日本国内のルールが適用された場合、グローバル CSPs では、データセンターの物理的な位置を開示することや情報を提供することは困難です。この点に関して、ACCJ はグローバルスタンダードとの整合性を図るためにそうした基準が取り除かれることを強く推奨します。
- (P15 - P20) 監査プロセスが英語でも実施可能となることを強く要望します。グローバルな CSPs は海外の本社と頻りにコミュニケーションをとる必要があります。日本語でのコミュニケーションが要求されると、目に見えないコストが発生し、グローバル CSP と国内企業との間に不公平な競争環境が生じることを懸念しています。監査費用の増加は、最終的には日本国民の税負担の増加につながるため、ACCJ はこれらの費用を最小限に抑える方法について慎重かつ真剣に検討すべきであると考えます。
- (P16 24 行目)「(監査主体の)国内に法人登録があることを要求」とされていますが、日本で作成および取得された記録のみですべての監査プロセスを実施するのは非効率的であると考えます。CSPs が監査プロセスの特定の部分を海外での実績に置き換えることができれば、より効率的になることが期待できます。これにより、従うべきグローバルスタンダードが生み出され、グローバルな CSPs だけでなく、将来的にグローバルに事業を展開することを計画している日本企業にも裨益するでしょう。
- (P17 24 行目) CSP が管理基準を満たすことができない場合には、関連するサービスのみが登録簿から削除され、基準を満たす他のサービスは登録簿に登録されたままになるという理解が正しいかご確認いただくよう要望します。