AICPA「SOC 2」Guide Working Group: Chair（起草委員長）インタビュー和訳要約

Q1.SOC1・SOC2 報告書とは？

AICPA が編み出したSOC1・SOC2 報告書により、企業は外部委託先における内部統制のデザインと運用の有効性についての理解が可能となります。SOC1 報告書は、SSAE16（旧 SAS70）に準拠した保証報告書です。SOC1 報告書では、外部委託先における財務報告に係る内部統制が取扱われます。日本では、JICPA/監査・保証実務委員会実務指針第 86 号（旧 18 号）が、SOC1 報告書に該当します。

SOC1 報告書では、外部委託先における財務報告に係る内部統制のみが報告対象になるという制限があります。AICPA では、SOC1 報告書の報告対象を財務報告目的以外にも拡大するか、財務報告目的以外を対象とする別の報告書を準備する必要があると考えました。このような経緯で、SOC2 が編み出されました。SOC3 は、Trust サービス（SysTrust、WebTrust）の改訂版になります。

Q2. 財務報告目的以外の保証報告書が必要とされる理由

SOC2 が必要とされる理由は二つあります。一つはアウトソーシング・サービスの利用、特にクラウド・サービス利用の増大です。もう一つは、ガバナンス（G）、リスク管理（R）、コンプライアンス（C）、すなわち、GRC の重要性が高まっていることです。この GRC 重視の考え方は、アウトソーシング・サービスを利用する企業だけでなく、サービス提供側である外部委託先でも浸透してきています。これは、企業の内外を問わず、GRC の重要性が高まっていることを意味します。この二つが、財務報告目的以外の報告書が必要とされる理由です。

SOC2 では、セキュリティ、可用性、処理のインテグリティ、機密保持、プライバシーの五つの観点から内部統制を評価します。

Q3. 外部委託リスクと GRC

企業は業務を外部へ委託することにより、特定のビジネス・リスクが解消されるという認識を持っています。一方で、当該リスクは外部委託先における新たなリスクとなります。当該リスクは外部委託先における対応が必要となります。このため、大手金融機関のみならず、様々な業界で、ベンダー・リスク・マネジメントが一般的となりつつあります。

ベンダー・リスク・マネジメントは、外部委託先におけるリスクの評価と対応です。外部委託先で起こり得るリスクを特定し、委託会社側でのユーザー統制として対応したり、外部委託の際に必要な統制を適用してもらうことも可能です。外部委託先が内部統制を適用しなかったり、内部統制が有効に運用されないこともあるため、委託会社は外部委託先における内部統制が有効に運用されていることを何らかの形で確認する必要があります。

SOC2 がこれに対応しています。SOC2 では、外部委託先の内部統制が有効に運用されているという証を委託会社に提供することができます。

Q4.SOC2 開発上のポイント

検討を重ねた結果、SOC2 では、業務オペレーション、コンプライアンスだけでなく、内部統制に柔軟に対応することが、SOC2 報告書利用者にとって重要であるとの認識に至りました。SOC1（SSAE16）報告書を利用している委託会社に対して、従前と同レベルの情報を提供することの必要性についても検討し

ました。委託会社では、SOC2 においても、従前の SAS70 と同様に、外部委託先の監査人が実施した内部統制の評価手続とその結果に関する情報を必要としています。委託会社が SOC2 報告書を利用しやすいよう、SOC1 報告書の様式を踏襲しました。SOC2 における内部統制の評価基準として、既に馴染みのある Trust サービスの原則と規準を選びました。Trust サービスの原則と規準とは、セキュリティ、可用性、処理のインテグリティ、機密保持、プライバシーです。これは、過去 10 年間、SysTrust、WebTrust で利用されてきた経験の裏付けがあり、統制項目が網羅されている証となります。

Q5.SOC2 レポートの利用状況

SOC2 レポートは、AICPA からガイドが公表されて 1 年余りですが、クラウド・サービス、とりわけ、IaaS,SaaS に関する分野での利用が急速に伸びています。他にも、コールセンター、インターネット上のオンライン自動化ソフトなど、SOC1（SSAE16）レポートでは対応できなかったサービスで利用され始めています。

これらの企業は、過去に SOC1 報告書では対象とすることができなかったリスクを含めることに価値を見出しており、特にクラウド業界においてその傾向が顕著です。AICPA では、CSA（クラウド・セキュリティ・アライアンス）と連携して、クラウド・コントロール・マトリックス（CCM)に対して、SOC2 を利用してどのように評価できるかを提示する予定です。これは、クラウド・ユーザーの SOC2 レポートの理解促進に繋がるため、AICPA と CSA との連携は、SOC2 にとって非常に重要です。

日本における金融機関向け IT サービスでは、金融情報システムセンター（FISC）の要求事項に細心の注意を払っているため、金融機関向けサービスを提供する外部委託先が FISC の要求事項を遵守していることについて、SOC2 レポートをいかに活用できるかということも重要なポイントです。SOC2 は、クラウド・ユーザーや金融機関が、CCM や FISC の要求事項に対する遵守状況を評価する際の一つの手段を提供するものであると考えています。

Q6. SOC2 の今後

SOC2 は、公表されて日が浅いフレームワークです。今後は、委託会社と外部委託先両者のニーズや新たな課題への対応が必要となります。

現在、SOC2 が対応すべき課題は、IT に関する技術革新への対応です。SOC2 は保証報告書に関するフレームワークですから、他の様々な内部統制のフレームワークに対応できるはずです。CSA（クラウド・セキュリティ・アライアンス）や金融情報システムセンター（FISC）の要求事項への対応等に加え、SOC2 形式の保証報告書に適用できそうな他の統制フレームワークを検討していきたいと思います。多種多様な新しいフレームワークに適用できることに喜びを感じながら、他の機関と連携していくつもりです。

2012.12.20

＜Chris Halterman＞
◇アーンスト・アンド・ヤング（米国）／エグゼクティブディレクター
◇AICPA（米国公認会計士協会）／SOC 2 Guide Working Group : Chair