第 34 回研究大会講演録
特別講演

クラウド環境における SOC 保証業務 ～ SOC 2 保証報告書の有効利用～

SOC Assurance Service in Cloud Environment
-Effective Use of SOC 2 Assurance Report-

遊馬 正美
Masami Asuma

EY 新日本有限責任監査法人 シニアパートナー

クラウド環境においては、SOC（System and Organization Controls）保証業務である米国公認会計士協会（AICPA）の SOC2 をはじめとして、国内でもさまざまな制度が存在している。本講演では、これらの制度における基準と枠組み、報告書の構成、用途等について、ISMAP との関係も含めて説明が行われた。講演内容は以下のとおりである。

公認会計士が行う保証業務には、財務諸表監査、内部統制監査等の他に SOC3 の日本版となる Trust サービスの検証業務、保証業務実務指針 3402 に基づく委託業務に係る受託会社の内部統制の評価業務などがあり、さらに AUP と呼ばれる合意された手続業務などがあるが、SOCR（System and Organization Controls Reporting - 受託業務に係る内部統制の保証報告書）は、一般的に業務を外部に委託している場合に、委託先における委託業務に係る内部統制の状況を把握し、その有効性の評価に利用するための報告書である。

SOCR には国際基準、米国基準、日本基準がある。最初に出たのは財務報告目的の米国基準である SAS70 である。日本基準では旧 18 号が相当し US-SOX、JSOX の登場とともによく出回るようになった。情報システムに関しては米国で SysTrust、WebTrust といった Trust サービスが始まって、その後 SOC3 という呼称となり、日本では SysTrust、WebTrust のライセンス契約による Trust サービスが約 2 年前に始まった。2011 年には財務報告目的の国際基準として ISAE3402 ができ、米国でも SOC 1、SOC 2、SOC 3 という呼称が使用されるようになった。SOC1 は財務諸表監査、内部統制監査に、SOC2、SOC3 はセキュリティにフォーカスしたものになっている。

委託元 A 社が外部委託先 B 社に業務を委託している場合、A 社が B 社（受託会社）の内部統制を評価する方法としては、「受託会社から保証報告書を入手する方法」「受託会社を訪問して直接監査する方法」「他の監査人を利用する方法」の 3 つがあるが、US-SOX、JSOX 以後は委託会社も外部委託先の内部統制状況の理解と評価が求められるようになったため、保証報告書の利用が促進された。受託会社が受託会社確認書（きちんと内部統制をデザインして運用しているという宣言書）、システム記述書（どういったコントロールがあるかという記述書）を用意し、受託会社監査人は独立した監査人としてこれを監査した結果の報告書を添付して保証報告書にまとめ、委託会社に利用してもらうという形である。このフレームワークを利用するメリットとしては、受託会社側は、内部統制に関する煩雑な問合せを効率化でき、委託会社側は委託先管理の効率化ができるところにある。

保証報告書の構成を Type2 の例でみると、報

告書は独立した受託会社監査人の保証報告書、受託会社確認書、内部統制そのものの内容であるシステム記述書、監査人が実施した運用状況評価手続とその結果に関する記述の 4 つのパートからなる。最後の監査人のパートには、例外事項が発生した場合、その例外事項も記述される。その他、5 つ目のパートとして評価対象期間後に大きな事象が発生して報告書の内部統制そのものに影響を与えた場合などに「会社からのその他の情報提供」が追加される場合もある。Type1 の場合は運用状況評価手続とその結果に関する記述は含まれない。Type1 報告書はある一時点における内部統制のデザインに関する報告書であり、Type2 は一定期間における内部統制のデザインおよび運用状況に関する報告書である。なお、ISMAP については、最初の特例期間中は Type1 的な整備状況評価の報告書が用いられ、特例期間終了後は Type2 的なものに移行していくことになっている。

SOC1 と SOC2・SOC3 の大きな違いとしては、SOC2・SOC3 は対象リスクとして、セキュリティ、可用性、処理のインテグリティ、機密保持及びプライバシーという、Trust サービス規準における 5 つのクライテリアがあることであり、SOC2・SOC3 保証業務では最低限セキュリティ（コモンクライテリア）を対象にしなければならず、それ以外は任意である。クラウドサービスベンダーの SOC2 保証報告書は主にセキュリティと可用性が対象となり、機密保持が加わる場合もある。またプライバシーはボリュームが大きく重いものになるため、実務ではあまり見ない。財務報告目的の SOC1 の場合は、アクセス管理はセキュリティに対応するが、可用性、機密保持などは対象外であるため、SOC1 だけではさまざまなコンプライアンスをクリアする上で足りないという場合に、SOC2 も併せて入手することが多い。最近では金融情報システムセンター（FISC）の安全対策基準にも SOC2 という言葉が見られるようになった。また ISMS との違いとしては、現地の往査や報告書のボリュームも SOC2 が圧倒的に多く、開示も ISMS は認証取得の証明書だけだが、SOC2 では詳細な内部統制を確認することができるという大きな違いがある。

SOC 2+ 保証報告書は、Trust サービス規準以外の規準を付加するものであり、日本では一般的には FISC の安全対策基準が使われることが多い。また個人情報保護関連でマイナンバーのガイドラインが使用されることもある。

ISMAP に関しては、クラウドサービス事業者を ISMAP 監査機関（監査法人が主）が監査し、その報告書に基づいて ISMAP 運営委員会に申請、その結果によって ISMAP クラウドサービスリストに公表されるという流れだが、SOC1、SOC2 との比較でいうと SOC1 は委託会社等限定された先にだけ開示されるが SOC2 は潜在的な利用者も開示対象となる。一方 ISMAP はクラウドサービス事業者と運営委員会のみ開示対象であるため、内部統制の詳細な内容については SOC2 保証報告書が必要となる。そのため ISMAP と SOC2 は今後も共存していく関係になるものと考える。

（内藤　裕之　記）
（2020 年 11 月 6 日開催）