クラウドセキュリティに関する第三者評価・認証制度の概要
ISO/IEC 27017認証、SOC2およびSOC2+

アドバイザリー事業部　エグゼクティブディレクター　佐藤芳克

▸ Yoshikatsu Sato
公認情報システム監査人、公認内部監査人。外資系証券会社、国内大手コンサルティングファームを経て現職。情報セキュリティ監査、ISO認証取得支援、データセンター事業者・クラウドサービス事業者の受託業務に係る内部統制の保証業務（SOC1・SOC2）など、ITリスクに関するアドバイザリー業務に従事。

Ⅰ　はじめに

2015年12月15日、国際標準化機構（ISO）および国際電気標準会議（IEC）はクラウドサービスに関する情報セキュリティの国際規格として、ISO/IEC 27017：2015（以下、ISO/IEC 27017）を発行しました。既に、幾つかのクラウドサービス事業者は、この規格認証への対応を開始するなど、新たな動きが見られています。

これまでクラウドセキュリティに関する第三者評価として、主に「SOC2」が利用されてきました。SOC2は、米国、日本をはじめ、世界各国で広く利用されている評価制度です。

本稿では、「ISO/IEC 27017認証」と「SOC2」の特徴を整理するとともに、クラウドサービス事業者および利用者が、これらの評価・認証制度を検討・利用する場合に考慮すべきポイントについて解説します。

Ⅱ　ISO/IEC 27017

1. 規格の特徴

ISO/IEC 27017は、情報セキュリティ管理策の実践の規範であるISO/IEC 27002にクラウドサービス固有の事項を追加したものです。認証取得に向けては、ISO/IEC 27001が要求する、情報セキュリティマネジメントシステム（ISMS）が確立していることが前提となります。

2. 認証制度

日本では、一般財団法人 日本情報経済社会推進協会（JIPDEC）がISO/IEC 27017認証に係る新たな制度として、「ISMSクラウドセキュリティ認証」の認定審査の開始を発表しました。認証を取得した組織には、認定マークが入ったCertificate（認証登録証）が発行されます。

Ⅲ　SOC2の概要とISO/IEC 27017認証との比較

1. SOC2の概要

SOC2は、米国公認会計士協会（AICPA）が定めた評価の規準である「Trustサービスの原則と規準」に基づき実施されます。Trustサービスの原則と規準は、「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」の五つで構成され、SOC2では、この中から一つ以上を選択（複数選択可能）し、評価が行われます。

評価の結果は、詳細な報告書（SOC2保証報告書）としてまとめられ、サービスの利用者（想定利用者を含む）がこれを利用することができます。

2. ISO/IEC 27017認証との比較

(1) 評価の規準、難易度

ISO/IEC 27017が国際的な標準規格であるのに対し、Trustサービスの原則と規準はAICPAが定め

▶表1　対比表　ISO/IEC 27017 vs SOC2

	ISO/IEC 27017認証	SOC2
評価の規準	国際的な標準である国際規格	AICPAが定めたTrustサービスの原則と規準
難易度	比較的容易	高難度
Outputと利用者	▸ Certificate（認証登録証など） ▸ 認定証は不特定多数に向け、公開可能	▸ 詳細な報告書（整備、運用されている具体的な手続が示される） ▸ 報告書の利用はサービスの利用者（想定利用者を含む）に制限
訴求効果	▸ 情報セキュリティに対するマネジメントの仕組みが、一定のレベルで存在することを訴求できる ▸ ただし、ISO認証取得は比較的容易であることから、大きな効果は期待できない場合が想定される	▸ 高難度であることの認識が浸透しつつあり、相応の評価が期待できる ▸ 報告書は各種の監査、法規制等に係る検査などに利用することができる

た規準です。TrustサービスのISO/IEC 27001やISO/IEC 27017と多くの部分で関連性があり、これらの要求事項をより具体化、高度化したものです。従って、ISO/IEC 27017認証とSOC2を比較した場合、取り組みに関する難易度は、一般的に、後者の方がより高くなるとされています。

(2) Outputと利用者

SOC2保証報告書は、「(評価を実施した) 監査人の意見」「(クラウドサービス事業者の) 経営者の確認書」「システムの記述」および「監査人が実施した運用評価手続とその結果」の四つのパートで構成されます※。

「システムの記述」のパートには、事業者がクラウドセキュリティのためにデザイン（整備）し、運用する内部統制の仕組みが詳細に記述されます。これは、クラウドサービスの利用者にとって、非常に有用な情報ですが、ISO/IEC 27017のCertificateには、こうした情報は含まれません。

(3) 訴求効果

前述のように、日本では今後、「ISMSクラウドセキュリティ認証」の制度運用が本格化すると思われます。ただし、ISMS（ISO/IEC 27001）の認証取得が比較的容易であり、既に一般化していることを踏まえると、この認証取得による訴求効果は、あまり期待できない場合も考えられます。

一方、SOC2は高難度であることの認識が浸透しつつあり、また、SOC2保証報告書は各種の監査、法規制等に係る検査で利用されるなど、大きな効果が期待できます。（<表1>参照）

Ⅳ　SOC2+

SOC2はTrustサービスの原則と規準に、任意の評価規準を追加することができます（SOC2+）。米国では既に、医療保険の相互運用性と責任に関する法令「HIPAA」や、米国国立標準技術研究所（NIST）が発行する連邦政府情報システムにおける推奨セキュリティ管理策である「NIST SP 800-53」を追加するなど、積極的な取り組みが見られます。

日本でも今後、金融機関向けには「金融機関等コンピュータシステムの安全対策基準」（FISC：金融情報システムセンター）、マイナンバー事業者向けには「特定個人情報の適正な取扱いに関するガイドライン」（個人情報保護委員会）を追加するなど、利用者のニーズに合わせた、より最適な報告書（SOC2+保証報告書）へのカスタマイズが期待されています。

Ⅴ　おわりに

ISO/IEC 27017認証、SOC2、SOC2+と見てきましたが、これらは、それぞれに特徴があり、クラウドサービス事業者および利用者は、各自の目的に合わせて活用することが重要です。

情報セキュリティマネジメントシステムがまだ十分に構築できていないクラウドサービス事業者は、まずはISO/IEC 27017認証に向けた取り組みから始め、段階的にSOC2、SOC2+へステップアップする成長モデルが良いでしょう。また、クラウドサービスの利用者は、サービスの利用目的、用途を踏まえて、クラウドサービス事業者に、どのレベルの第三者評価・認証を求めるのか、検討することが大切です。

※　特定期間における運用状況を評価するType2の場合