ISMS クラウドセキュリティ認証の概要

一般財団法人日本情報経済社会推進協会
情報マネジメントシステム認定センター
センター長　　星　昌宏

この度 JIPDEC が新たに開始する「ISMS クラウドセキュリティ認証」は、ISMS の認証規格である JIS Q 27001(ISO/IEC 27001)に加え、ISO/IEC 27017:2015 に基づいたクラウドサービス固有の追加事項に考慮したうえでの ISMS 認証、すなわちクラウドサービスを扱う組織の ISMS 認証である。

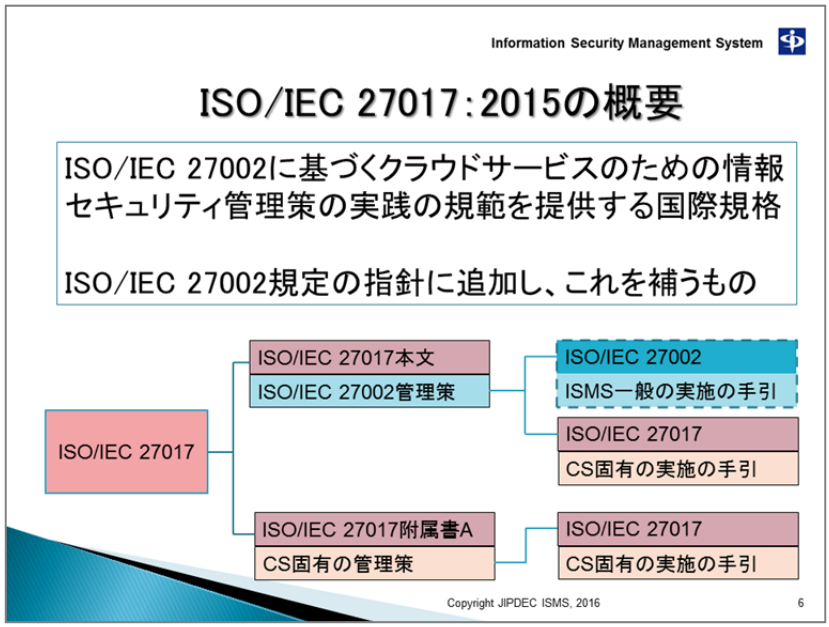
■ISO/IEC 27017 発行の経緯

ISO/IEC 27017 は、正式名称を「ISO/IEC 27002 に基づくクラウドサービスのための情報セキュリティ管理策の実践の規範」という。認証基準ではなく実践の規範（ベストプラクティス）であり、そのまま認証の要求事項にはならないので、そこをつなぐ仕組みとして JIPDEC が「JIP-ISMS517-1.0」という認証基準を新たに設け、これを用いた認証を行うこととした。

昨今、クラウドサービスの利用が盛んになる一方で、たとえばサーバ内のデータ消失や、意図しない者とのデータ共有等の事例が出て来ており、クラウドサービス利用における情報セキュリティの不安が高まっていた。そうした中、2011 年に、ISO/IEC 27002（ISMS 実践のための規範）と整合性をとったかたちで「クラウドサービス利用のための情報セキュリティマネジメントガイドライン」が経済産業省から出され、ISO/IEC への提案の末、国際標準化が決定し、2015 年 12 月 15 日に ISO/IEC 27017:2015 が発行された。

■ISO/IEC 27017 の概要・構成

ISO/IEC 27017 は、ISO/IEC 27002（ISO/IEC 27001 に対するベストプラクティス）規定の指針に、クラウドサービス固有の事項に関する指針を追加・補足する位置づけとなっている（図 1)。実際にクラウドサービスのための ISMS を構築する際には、リスクアセスメントの結果をふまえて必要な管理策を決定し、それを 27002 やこの 27017 に示す管理策と比較することで、必要な管理策の見落としがないかを検証することになる。



（図 1）

ISO/IEC 27017:2015 の構成は以下の図のとおりである（図 2)。
0～4 は 27017 独自の内容であり、5～18 は 27002 と同じ構成になっている。

（図 2）

このうち「1.適用範囲」において、ISO/IEC 27017 は、クラウドサービスの提供及び利用に適用できる情報セキュリティ管理策のための指針を示しており、この指針の管理策及び実施の手引きは、クラウドサービスプロバイダ及びクラウドサービスカスタマの両方に

対して提供されるものであると定められている。例えば他社の IaaS を利用して、その上に構築したサービスを更に他社に提供するような場合、つまり一方ではカスタマ、他方ではプロバイダであるような場合には、両者の立場で認証を取得することが求められる。

追加の実施の手引の例として「18.1.1 適用法令及び契約上の要求事項の特定」では、クラウドサービスカスタマは「クラウドサービスプロバイダにどの国の法律が適用されるのか」を考慮することが望ましいとし、他方、プロバイダはカスタマに、クラウドサービスに適用される法域を知らせることが望ましいとしている。

■ISMS クラウドセキュリティ認証について

今回新しくスタートする ISMS クラウドセキュリティ認証は、ISMS（ISO/IEC 27001）認証を前提としている。つまりマネジメントシステムとして PDCA を回す部分は ISMS 本体であり、その中で、適用する管理策に対応した ISO/IEC 27017 の実施の手引が参照されるという枠組みになっている。当認証の対象は、クラウドサービスを提供している組織（クラウドサービスプロバイダ）、または、クラウドサービスを利用している組織（クラウドサービスカスタマ）のいずれか、あるいは両方である組織であり、その組織が提供または利用するクラウドサービスの分類（IaaS、PaaS、SaaS）は問わない。

また、ISMS クラウドセキュリティ認証の認証基準は、ISO/IEC 27017:2015 に基づく要求事項「JIP-ISMS517-1.0」である。この JIP-ISMS517-1.0 は、ISO/IEC 27017 を要求事項として扱うための基準である。JIP-ISMS517-1.0 は現在ドラフトの段階であり、実際にこの要求事項に基づいて認証が開始されるのは、2016 年 8 月以降となる予定である。