ISMS 適合性評価制度
クラウドセキュリティ認証の概要

2015 年 11 月 16 日

一般財団法人日本情報経済社会推進協会
情報マネジメント推進センター

１．背景

クラウドサービスの本格的な普及に伴い、国内外のクラウドサービスにおいて大規模な障害や機密情報漏えいの発生など、リスクが顕在化しており、クラウドサービスに求められるセキュリティ要求事項を明確化することの重要性が認識されつつある。また、クラウドサービス向けの国際規格として、ISO/IEC 27017(Code of practice for information security controls based on ISO/IEC 27002 for cloud services：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）が、近日中に発行される見込みである。

このような状況を踏まえ、クラウドセキュリティに対する市場の期待も高いことから、日本セキュリティ監査協会などの関連機関等と連携して、クラウドサービスのセキュリティ維持・向上のため、ISMS 適合性評価制度において、クラウドセキュリティの認証を開始することを決定した。

２．クラウドセキュリティ認証

クラウドセキュリティ認証とは、ISMS（ISO/IEC 27001）認証を前提として、クラウドサービスの情報セキュリティ規格（ISO/IEC 27017）を満たしている組織を認証する仕組みである。

組織は ISO/IEC 27017 を適用することによる情報セキュリティマネジメントに基づいて ISO/IEC 27017 に基づくリスク対応をすることとなる。前提となる ISO/IEC 27001 においては、クラウドセキュリティリスクを含む情報セキュリティリスクを特定し、内外の情報セキュリティ技術・環境に応じてセキュリティ対策を講じることができる。また、個々の具体的なセキュリティ対策については、組織におけるリスクアセスメントの結果に応じてリスク対応することとなるので、個別のセキュリティ技術も含めた効果的なセキュリティ対策を実施することができる。

ISO/IEC 27017 とは

ISO/IEC 27017 は、セクター（分野）固有の規格である。具体的には、次の事項が規定されている。

・ISO/IEC 27002 規定の管理策に対する追加の実施の手引
・クラウドサービスに関連する追加の管理策及び実施の手引

これらの管理策及び実施の手引は、クラウドサービスについての情報セキュリティリスクアセスメントの結果に応じてリスク対応を実施するためのセキュリティ対策を提供する。

クラウドセキュリティ認証を取得のためには図に示す要件を満たす必要がある。

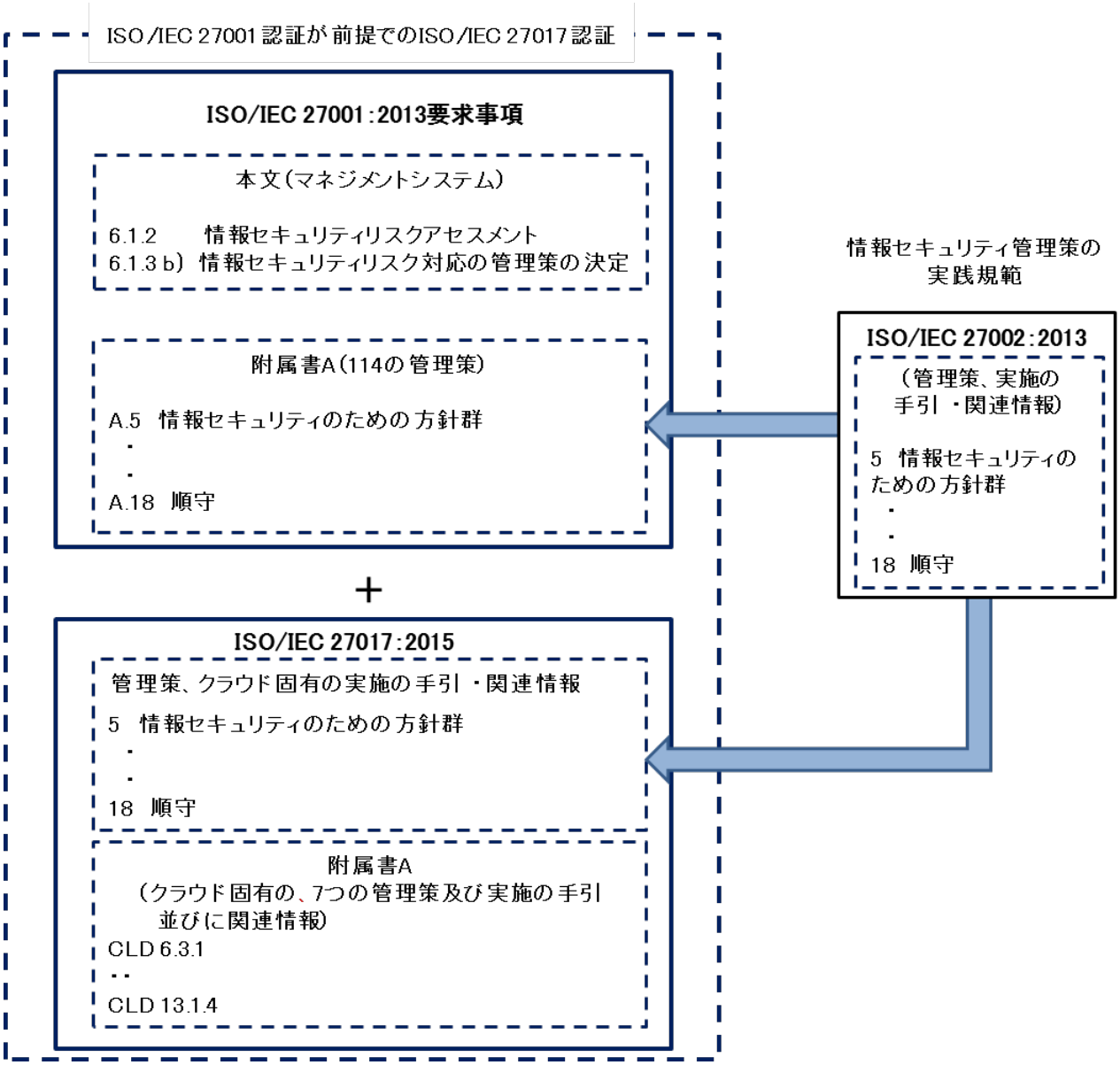

図　クラウドセキュリティ認証の要件

３．アドオン認証

アドオン認証とは、ISMS（ISO/IEC 27001）認証を前提として、特定の分野固有の規格を満たしている組織を認証する仕組みである。アドオン認証のためには、別途定める要件を満たすことが必要となる。

なお、クラウドセキュリティ認証については、セクター（分野）固有の規格として ISO/IEC 27017 を用いる。

以上