ISO/IEC 27017:2015 に基づく ISMS クラウドセキュリティ認証について

2016 年 8 月 1 日

一般財団法人日本情報経済社会推進協会
情報マネジメントシステム認定センター

【ISMS クラウドセキュリティ認証とは】

ISMS クラウドセキュリティ認証は、JIS Q 27001:2014(ISO/IEC 27001:2013)に適合した ISMS(情報セキュリティマネジメントシステム)において、その適用範囲内に含まれるクラウドサービスの提供もしくは利用に関して、クラウドサービス向けの国際規格である ISO/IEC 27017:2015 に規定されるクラウドサービス固有の管理策が実施されていることを認証するものである。

ISO/IEC 27017:2015:
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)

【ISMS クラウドセキュリティ認証のための新たな認証基準（要求事項）の策定】

ISO/IEC 27017:2015 は、クラウドサービス固有の情報セキュリティ管理策及び実施の手引を追加するガイドライン規格であり、ISMS 構築時に用いられる認証基準(要求事項)の類ではない。その点では、情報セキュリティ管理策の実践のための手引である JIS Q 27002:2014(ISO/IEC 27002:2013)と同様の位置付けとなる。

組織がクラウドサービス固有の情報セキュリティを含めた ISMS 認証を取得するためには、組織が ISO/IEC 27017:2015 の内容を取り込むための基準が必要である。このため、ISMS クラウドセキュリティ認証のための新たな認証基準として「ISO/IEC 27017:2015 に基づく ISMS クラウドセキュリティ認証に関する要求事項 JIP-ISMS517-1.0」を策定した。

なお、これは ISO/IEC 27001:2013 に対する追加の要求事項であるため、ISMS クラウドセキュリティ認証を希望する組織は、ISO/IEC 27001:2013 及び JIP-ISMS517-1.0 への適合が求められる。

【認証の対象となる組織】

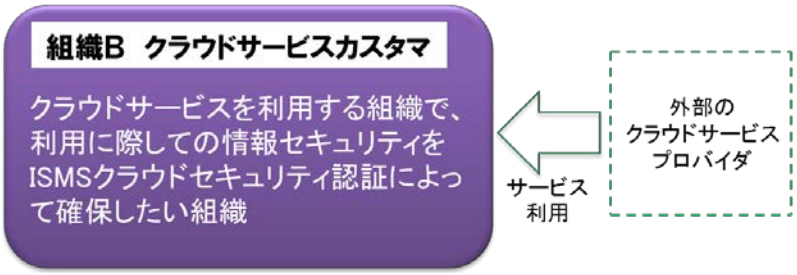
ISMS クラウドセキュリティ認証においては、次に示すように、クラウドサービスを提供している組織（クラウドサービスプロバイダ）、又はクラウドサービスを利用している組織（クラウドサービスカスタマ）のいずれか、あるいはその両方である組織が認証の対象となる。

なお、提供又は利用するクラウドサービスの種類(IaaS、PaaS、SaaS)は問わない。

・ケースA：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）

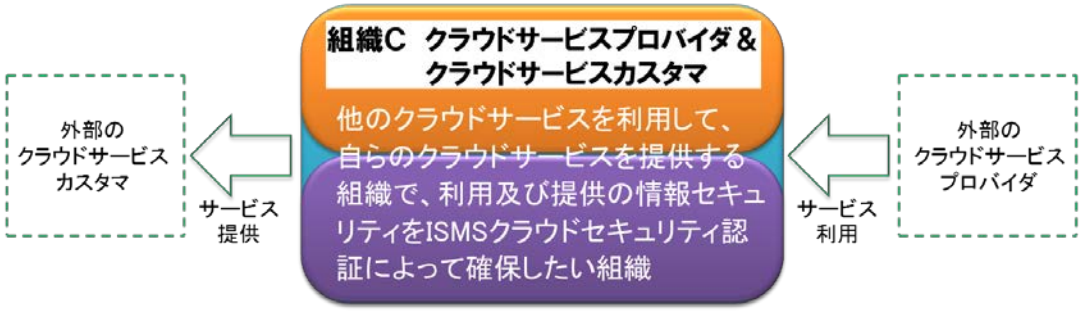
＊クラウドサービスの提供先（クラウドサービスカスタマ）の認証取得とは独立して認証を取得できる。

・ケースB：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）



＊利用するクラウドサービスの提供者（クラウドサービスプロバイダ）の認証取得とは独立して認証を取得できる。

・ケースC：クラウドサービスを利用及び提供している組織（クラウドサービスプロバイダ＆クラウドサービスカスタマ）



＊クラウドサービスプロバイダが自らのサービスを提供するに当たり、別のクラウドサービス（他組織が運用しているクラウドサービス）を利用している場合は、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の要求事項を満たすことで、認証を取得できる。

例：他組織の IaaS を利用した SaaS 型のクラウドサービスプロバイダの場合

‘SaaS’としてのサービスプロバイダに対する‘クラウドサービスプロバイダの要求事項’及び‘IaaS’の利用者としての‘クラウドサービスカスタマの要求事項’を満たす必要がある。

以上