ISO/IEC 27017:2015 に基づく クラウドセキュリティの構築のポイント

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
審査グループ　リーダ　　野中　武志

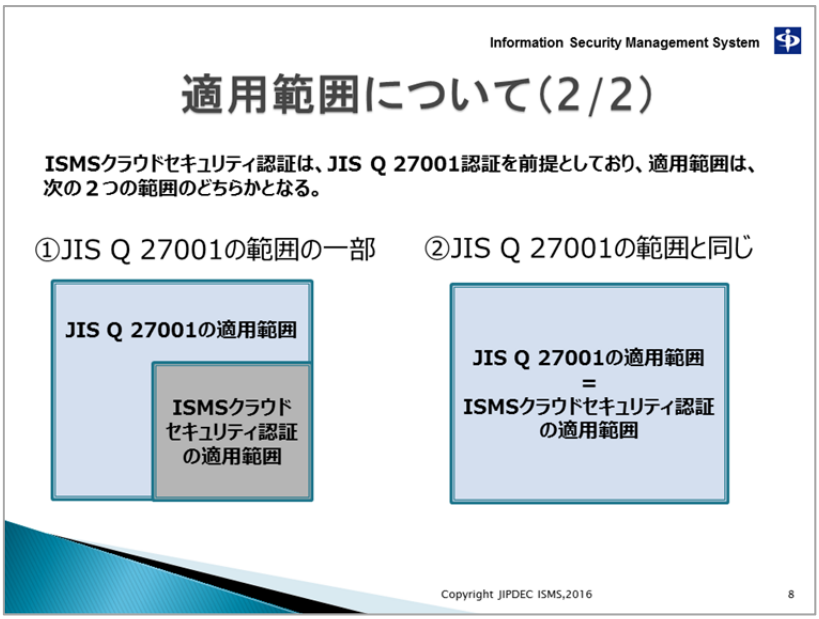
ISMS 認証のベースである ISO/IEC 27001 と、ISO/IEC 27002 に基づくクラウドサービスのための情報セキュリティ管理策の実践の規範（ベストプラクティス）である ISO/IEC 27017 を結びつける存在である、JIP-ISMS517-1.0（「ISO/IEC 27017:2015 に基づく ISMS クラウドセキュリティ認証に関する要求事項」）について解説する。

■ISMS クラウドセキュリティ認証取得のための要求事項

ISMS クラウドセキュリティ認証にあたって順守しなければならない要求事項とは、JIP-ISMS517-1.0 の 4 章にある基本的要件のことを指す。この要求事項は、適用範囲・情報セキュリティリスクアセスメントおよびリスク対応・内部監査の 3 つの内容に大別される。

■適用範囲とリスクアセスメントについて

ISMS クラウドセキュリティ認証は、JIS Q 27001 認証を前提としているため、JIP-ISMS517-1.0 における適用範囲は、JIS Q 27001 の範囲の一部か、JIS Q 27001 と同範囲かのどちらかとなる（図 1）。



（図 1）

リスクアセスメントの実施については、基本的には 27001 における方法と同様でよいが、ISMS クラウドセキュリティ認証では、クラウド特有のリスクを見直すことがポイントとなる。ISO/IEC 27017 はあくまで管理策を洗い出した内容であるため、まずはその前段階として、リスクの洗い出しを行う必要がある。ISO/IEC 27017:2015 の附属書 B には、ITU-TX.1601 (2014) や Cloud Computing Security Risk Assessment:2009 ENISA など、リスクの洗い出しに関連する参考文献のリストがあるので、参考にしていただきたい。

■技術的リスク：仮想化環境におけるリスクについて

仮想化環境では、さまざまなリスクが考えられる。たとえば、アクセス権設定の不備による環境全体の乗っ取りといった職務分掌の欠如によるリスクや、特権パーティションからあらゆるサービスが制御可能となり脆弱性の単一障害点となる、といったことが例として挙げられるだろう。また、仮想化サーバ構築にあたり、通常ネットワーク（レイヤ 2）に精通しておらず、冗長性や VLAN などを意識した設計に不慣れなサーバ管理者によるネットワーク設計により、ネットワーク運用ポリシーやセキュリティポリシーとのズレが生じてしまうなど、さまざまなケースが考えられる。仮想化環境のネットワークにおける問題に関しては、PCI DSS V3.1 でも管理策が挙げられているので、こちらも参考にしていただきたい。

■適用宣言書について

JIP-ISMS517-1.0 における適用宣言書の書き方については、JIP-ISMS517-1.0 の A.4 適用宣言書の例示を参考にしていただきたい。本クラウドセキュリティ認証は、JIS Q 27001 に基づく ISMS 認証をベースとしているため、「27001 のある管理策は実施していないが、その管理策に紐づく 27017 の管理策は実施している」というようなケースはないという点に留意が必要である。

クラウド情報セキュリティについて、技術面での深掘りだけではなく、組織全体としてどうマネジメントを行うのかということに焦点をあてて対策を行うことが、当認証の狙いである。