JIS Q 27001:2014 への移行に関する説明会　質疑応答内容

2014 年 10 月 28 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

Q1：管理策におけるプロジェクトマネジメントについて
管理策におけるプロジェクトマネジメントの範囲とは、企業単位、企業が決めた範囲でいいのか。また、プロジェクトの定義は有期性の業務と一般では言われているが、どのようなスタンスと理解すればいいのか。

A1：JIS Q 27001:2014 の附属書 A の「A.6.1.5 プロジェクトマネジメントにおける情報セキュリティ」に関連してプロジェクトマネジメントついて説明します。JIS Q 27001:2014 を実施するプロセスにおいて、管理策を選定する際の参考として用いるための手引について規定した JIS Q 27002:2014 の 6.1.5 では、「プロジェクトの特性にかかわらず、一般にあらゆるプロジェクトに適用される。例えば、中核事業プロセス、IT、施設管理，その他のサポートプロセスのためのプロジェクト…」とあります。対象とするプロジェクトは組織がリスクを考慮して決め、審査員は組織が決めたプロジェクトに対して審査を行います。

Q2：管理策におけるサプライチェーンの内容について
ICT サプライチェーンの内容は、当社と共同で物を販売している会社との管理なのか。
また、仕入れを行っているだけで転売も何もしていない場合には、サプライチェーンをどのように理解すればいいのか。

A2：JIS Q 27001 附属書 A.15 が適用されます。A.15 は JIS Q 27001:2006 の A.6.2.3 及び A.10 にあった第三者との取引を対象としています。情報セキュリティマネジメントは、自分自身で対応できる項目と第三者に依頼しなければできない項目とがあり、第三者に依頼しなければできない項目を一つの管理策にまとめています。ICT サプライチェーンは二者間のチェーンとクラウドサービスを含めていますが、セキュリティを保つうえで必要な供給者を組織が定め、要求事項を科すことが必要であれば策定し、対応すればよいでしょう。

Q3：リスクアセスメントについて
「資産にとらわれなくてもよい」との説明だったが、今後、見直すにあたっては、資産にとらわれないリスク分析の方法あるいはヒントを頂きたい。

A3：資産ベースのリスクアセスメントは、それを扱う複数の部署で個別に扱うことが多いと思います。資産ベースの分析では、その置かれた局面、どの時点で扱うかによって重要度が変わる資産などの対応に難しい面があります。プロセスを踏まえてみると、リスクは業務の流れの中で問いやすいため、プロセスの流れの中で資産を考えるのも一つの方法です。また、個人情報のようにライフサイクルを意識したリスクアセスメントを行う方法もあります。

以上