参考資料4－2

ISO27001関係資料

ISO／IEC27001－情報セキュリティマネジメント

ISO規格27000ファミリーは、組織の安全な情報管理に役立ちます。

この規格の使用は、財務情報、知的財産、従業員情報などの情報セキュリティの実施に役立ちます。

ISO／IEC27001は、情報セキュリティマネジメントシステム（ISMS）の要件を定める最もよく知られた規格です。

ISMSとは

ISMSは、企業の機密情報の安全を保持するためのマネジメントに対する体系的なアプローチです。ISMSには、リスクマネジメントプロセスの適用により、人、プロセス、ITシステムも含まれます。

ISMSは、全ての分野における中小および大企業の安全な情報管理に役立ちます。

ISO／IEC27001の認証

他のISOマネジメントシステム基準と同様に、認証を得ることはできますが、義務的なものではありません。ある組織はISO／IEC27001に含まれるベストプラクティスから利益を得るために実施を選択していますし、他の組織はISO／IEC27001に沿っているということで顧客を安心させるために実施しています。

International Organization for Standardization ホームページより

仮訳：厚生労働省

JIPDECホームページより引用

情報セキュリティマネジメントシステム(ISMS)適合性評価制度の概要

2014年4月14日

1. ISMS適合性評価制度の創設

我が国では情報処理サービス業のコンピュータシステムが十分な安全対策を実施しているかどうかを認定する制度として、昭和56年7月20日通商産業省告示342号による「情報システム安全対策実施事業所認定制度」(以下、安対制度という)があった。安対制度では、集中管理されていた情報システムの施設・設備等の物理的な対策に比較的重点がおかれていたが、技術的対策だけでなく人的セキュリティ対策を含む組織全体のマネジメントを確立する必要性がでてきた。

こうした状況を受けて、経済産業省では「情報セキュリティ管理に関する国際的なスタンダードの導入および情報処理サービス業情報システム安全対策実施事業所認定制度の改革(平成12年7月31日)」を公表するとともに、従来の安対制度を平成13年3月31日をもって廃止することを決定した。

この安対制度の廃止に伴い、技術的なセキュリティのほかに、人間系の運用・管理面をバランス良く取り込み、時代のニーズに合わせた新しい制度として、情報セキュリティマネジメントシステム(Information Security Management System:以下、ISMSという)適合性評価制度を創設することとなった。ISMS適合性評価制度は、わが国全体の情報セキュリティ強化のため、また安対制度廃止後の受け皿として、2002年4月から本格運用を開始した。

2. ISMS適合性評価制度の目的

インターネットの急速な普及を背景に、わが国においても情報セキュリティ政策会議が提示する法規の整備、技術的な検証、重要インフラの情報セキュリティ対策等を積極的に推進しているところである。
しかしながら、その一方では、セキュリティ対策の不備に起因する機密情報や個人情報の外部への漏洩、コンピュータウイルス、不正アクセス行為やシステムダウンによる事業の中断などさまざまなセキュリティ事故などが相次いでいる状況である。
こうした情報セキュリティへの意識が高まる中で、組織として情報セキュリティマネジメントを確立するためには、技術的なセキュリティ対策と組織全体のマネ ジメントの両面から取り組む必要がある。ISMS適合性評価制度は、国際的に整合性のとれた情報セキュリティマネジメントに対する第三者適合性評価制度であり、本制度は、わが国の情報セキュリティ全体の向上に貢献するとともに、諸外国からも信頼を得られる情報セキュリティレベルを達成することを目的としたものである。

3. ISMS適合性評価制度における認証基準

ISMSの認証基準JIS Q 27001:2014(ISO/IEC 27001:2013)は、ISMS適合性評価制度において、第三者である認証機関が本制度の認証を希望する組織の適合性を評価するための基準である。

・JIS Q 27001:2014 情報技術ーセキュリティ技術ー情報セキュリティマネジメントシステムー要求事項
(ISO/IEC 27001:2013 Information technology ーSecurity techniquesーInformation security management systemsーRequirements)

－組織がISMSを構築するための要求事項をまとめた国際規格である。

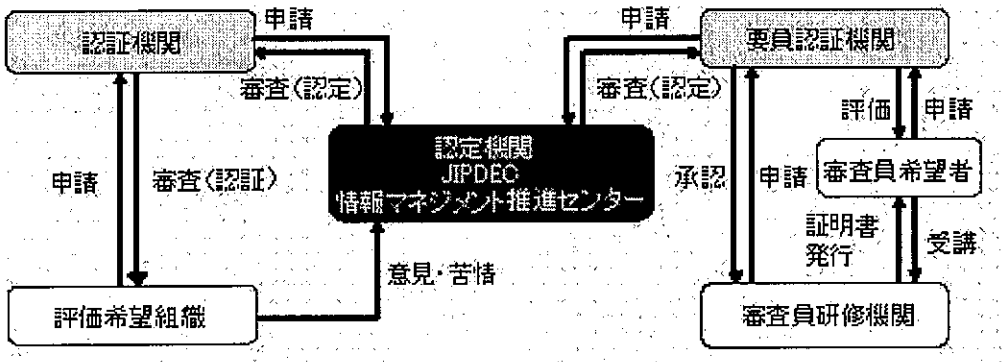
※ JIS Q 27001は、ISO/IEC 27001の制定発行に伴って、日本工業標準調査会（JISC）により日本工業規格（JIS）として制定された国内規格であり、内容は、ISO/IEC 27001を忠実に日本語に翻訳し、国際規格との整合性が厳密に保たれている。
2006年3月にJIS Q 27001:2006（第1版）発行後、ISO/IEC27001:2005の改訂に伴いJISも改訂が行われ、2014年3月にJIS Q 27001:2014（第2版）が発行された。

4. ISMS適合性評価制度の対象範囲

ISMS適合性評価制度のパイロット事業（平成13年度事業）では、対象範囲を主として情報技術関連分野（情報処理サービス業を含む）としていたが、平成14年4月の本格運用からはこの制限を外し、全ての業種・業務分野を対象範囲とした。
ISMSは、情報技術関連の業種だけでなく、全ての業種を対象に情報セキュリティに対するマネジメントシステムの認証を行うことが可能であるが、情報の管理は業務に密着しており、情報資産の洗い出しやリスクアセスメント等に関して審査するにはその分野の専門性が必要である。

5. ISMS適合性評価制度の運用

ISMS適合性評価制度は、組織が構築したISMSがJIS Q 27001（ISO/IEC 27001）に適合しているか審査し登録する「認証機関」、審査員の資格を付与する「要員認証機関」、及びこれら各機関がその業務を行う能力を備えているかをみる「認定機関」からなる総合的な仕組みである。なお、審査員になるために必要な研修を実施する「審査員研修機関」は要員認証機関が承認する。



[Home]

Last modified: Mon Apr 14 11:10 JST 2014