JQAは、次期ISO 14001改定案(CD2)をこうみている

自主的なイニシアチブを通じた環境遂行能力のさらなる向上を目指す

2013年4月に公表された「環境にやさしい企業行動調査(環境省)」によれば、環境課題に対応する上で重視する事項の上位に、経営活動と環境配慮行動を統合した戦略的な対応、ステークホルダーへの対応、経営責任者のリーダーシップ、組織体制とガバナンスの強化、バリューチェーンにおける環境負荷低減があげられています。次期ISO 14001は、わが国で環境課題に対応する組織が重視する考え方と同じ方向性の中で、従来からの国際規格であるISO 14001の底流に流れる考え方を踏襲しながらも、環境遂行能力のさらなる向上を目指した議論が進展しています。

①トップマネジメントの関与

環境に限ったことではありませんが、ISOマネジメントシステムにおける成功の鍵はトップマネジメントの関与であるといわれています。さらなる向上を目指すために、トップマネジメントのコミットメントを重視し、経営に環境活動を取り込み、意思決定を行う上での立ち位置について、経営の視点から掘下げられています。

②遂行能力の向上した結果は環境パフォーマンスでも計る

現行のISO 14001では、要求事項として環境パフォーマンスについて直接規定していません。これは、環境マネジメントシステムを改善することで、その活動の結果として環境パフォーマンスが改善されていく、という考えによるものです。しかし現実には、環境マネジメントシステムは問題なく運用されているがその成果が期待通りに上がらない、という状況が見られることがあります。改定案では、環境マネジメントシステムのパフォーマンスと環境パフォーマンスの双方を扱うとしています。

③ISO 14001独特の改定ポイント

独特の改定ポイントとしては、ライフサイクルに配慮したバリューチェーンの管理があげられます。一般に事業活動、製品、サービスはバリューチェーンのプロセスに沿って展開されています。このため環境の改善も、組織内部に留まらず、マーケットや多様なステークホルダーが一緒になって、今までの枠組み、制度、商慣習を変えながら、全体的なイノベーションを図ることで取り組みの成果があがっています。次期ISO 14001も、そのような経験や、時代的、社会的な要請を取り込んだ規格になっています。

審査の現場で見込まれる変化とは

審査の現場では、これまで以上にトップマネジメントの意向と環境マネジメントシステムのパフォーマンス、その結果としての環境パフォーマンスを向上させる努力とが合っているかどうかが浮き彫りにされ、それらの結果がどうフィードバックされてPDCAが回っていくかが、より明らかになると見ています。

また、活動の広がり、事業活動を俯瞰した全体的な取り組みが期待される規格になったことで、例えば工場だけが認証取得している場合では、会社全体での意思決定との連動や、中長期的な経営計画での位置づけなどに、どう配慮するかが焦点になっていくでしょう。

業務改善という視点から

環境パフォーマンスを向上させる上で大事なことは、節約によるコストメリットの出る目標のみならず、事業プロセスにISO14001の要求事項を組み込み、本業の中で経営的に取り組んでいくことだと考えられます。環境パフォーマンス向上のために、事業に直結した形で課題を設定し、戦略的に、課題によっては中長期的な計画を立て、継続的な向上を見込んだ目標を立てて取り組んでいくことが重要です。例えば環境負荷低減の施策に業務改善の視点を取り入れ、評価尺度をうまく設定すれば、パフォーマンス改善に有効に働きます。IT化で業務の効率化を図ったら結果的に紙ごみが減った、節電につながったというケースがありますが、業務改善という継続的な活動が環境への好影響を生んでいる例といえます。またバリューチェーンの管理においても、ITや流通改革を活用して在庫や物流をスリム化することは、環境パフォーマンスの面でも成果を生むと考えられますし、優れた製品やサービスは社会の環境負荷低減に大いに貢献することでしょう。

JQA環境審査部長　小笠原康治

5. パフォーマンス重視

今回の改定では、パフォーマンスが強く意識されている。9章「パフォーマンス評価」をはじめ、随所にパフォーマンスという用語が用いられ、従来以上にパフォーマンスをきちんと評価してコミットすることが要求されるようになった。そこでは成果を出す姿勢が明確に打ち出されており、組織は、自分たちが意図した成果にどこまで到達するかはっきりさせ、それを戦略として構築し、先を見据えたマネジメントにつなげていくことが求められる。

組織にとっては、「とりあえずISO」を離れて、ISOを取得する意味、目標を考えながら取り組むことが、より促されることになる。

6. 効率化の視点から

審査のためのドキュメント作成など、時代を経て陳腐化した作業はどんどんなくせばよい。文書管理もIT時代にふさわしく、文字文書だけではなく、図版、画像、映像、デジタル情報を含む幅広い情報として管理することができるようになった。これらは、7.5項「文書化した情報」に述べられており、こういう点でも使い勝手のよい規格になることが見込まれる。

■ 表3： ISO/CD 14001:2013の構成（赤字は固有要求事項）

- 0 序文
- 1 適用範囲
- 2 引用規格
- 3 用語及び定義
- 4 組織の状況
  - 4.1 組織及びその状況の理解
  - 4.2 利害関係者のニーズ及び期待の理解
  - 4.3 環境マネジメントシステムの適用範囲の決定
  - 4.4 環境マネジメントシステム
- 5 リーダーシップ
  - 5.1 リーダーシップ及びコミットメント
  - 5.2 環境方針
  - 5.3 組織の役割、責任及び権限
- 6 計画
  - 6.1 リスク及び機会への取組み
    - 6.1.1 一般
    - 6.1.2 環境側面の特定
    - 6.1.3 順守義務の決定
    - 6.1.4 著しい環境側面と組織リスク及び機会の決定
    - 6.1.5 行動のための計画
  - 6.2 環境目的及びそれを達成するための計画策定
    - 6.2.1 環境目的
    - 6.2.2 目的達成のための計画
- 7 支援
  - 7.1 資源
  - 7.2 力量
  - 7.3 認識
  - 7.4 コミュニケーション
    - 7.4.1 一般
    - 7.4.2 内部コミュニケーション
    - 7.4.3 外部コミュニケーション及び報告
  - 7.5 文書化した情報
    - 7.5.1 一般
    - 7.5.2 作成及び更新
    - 7.5.3 文書化した情報の管理
- 8 運用
  - 8.1 運用の計画及び管理
  - 8.2 バリューチェーンの管理
  - 8.3 緊急事態への準備及び対応
- 9 パフォーマンス評価
  - 9.1 監視、測定、分析及び評価
    - 9.1.1 一般
    - 9.1.2 遵守評価
  - 9.2 内部監査
  - 9.3 マネジメントレビュー
- 10 改善
  - 10.1 不適合及び是正処置
  - 10.2 継続的改善
- 附属書(A、B、C)

規格改定情報： ISO/IEC 27001

■ ISO/IEC 27001:2013発行までのスケジュール

2009年5月	2009年10月	2011年10月	2012年7月	2013年7月	2013年10月
NWIP	WD	CD	DIS	FDIS	IS

ISO/IEC 27001は情報セキュリティマネジメントシステムの中核規格に
—ISO/IEC 27000ファミリーはクラウドセキュリティなどの要素を加え時代のニーズにこたえる

ISO/IEC 27001:2013の発行

情報セキュリティマネジメントシステム(ISMS)のための要求事項ISO/IEC 27001は、2013年10月に改定版が発行された。この改定(*7)の趣旨を整理すると以下のとおりになる。

- ISO/IEC 27001がISMSの認証に使用される基準であることを考慮し、2005年版を基本的に継承した。
- ISO/IECマネジメントシステム規格を作成・改定する際に採用することが決められたマネジメントシステム規格の共通要素を採用した。
- ISO/IEC 27001の6章「計画」に記述されている情報セキュリティアセスメント及び情報セキュリティリスク対応並びにこれらの実施について、リスクマネジメントのガイドライン規格ISO 31000を適用した。
- 2005年から現在までの情報セキュリティとビジネス環境の変化が考慮され、ISO/IEC 27001を通信、金融、クラウドコンピューティング事業などの分野別ISMS認証制度の要請に対応できるようにした。

改定のポイントと審査での変更点

共通要素に従って、後述の1章～10章の章立てになっている(表4)。この流れで改定のポイントや審査での変更点を見ていく。

●適用範囲の決定

ISO/IEC 27001の2005年版では適用範囲は組織が定めるだけでよかったが、2013年版では、なぜその適用範囲にしたのか、根拠を明らかにし、文書化した情報として明示することが求められ、4章「組織の状況」で述べられている(*8)。このことは、従来の審査で触れてこなかったわけではない。JQAでは、審査の際に適用範囲を決めた理由を聞いていた。その上で、例えばインターネットのファイアーウォールを境界(バウンダリー)として、ファイアーウォールの内側でセキュリティ対策が取られ、保たれているかどうかを見るという審査を行っていた。従来から境界をどこに置くかがポイントであったが、根拠を明示することで、実際の運用がより明瞭になる。

●組織のリスクと情報セキュリティリスク

今回の改定では、6章「計画」(*9)で、2通りのリスクについての要求事項が入っている。一つは、ISMSが成果を出すうえで直面する全社的なリスクであり、組織の評判や存続にかかわるリスクである。もう一つは情報セキュリティリスクである。情報セキュリティリスクは従来通りの情報に対するリスクのことを示している。どの組織でも事業存続のための活動を日常的に行っている。それを明示したものととらえればよい。例えば、従業員の年齢構成などもリスクの一つとなり得る。

●アクションプランの作成

6章「計画」ではまた、情報セキュリティ目的を確立し、それをどうやれば達成できるかのアクションプランの作成も求められる。

現行版と比較して具体化されており、測定可能であることが要求され、計画、実施、レビュー、改善によるPDCAサイクルが明確になっている。達成度の判定が可能であり、達成へ向けたアクションプラン、進捗管理が明確ならば、これまでの年度目標のようなものでも問題はない。

●用語の削除とその対応

6章「計画」では、「脅威」「ぜい弱性」、リスク対応の選択肢における「受容」「回避」「移転」といった用語が削除されている。ただし削除されたからマネジメントシステムも変えなければいけないということではない。今までに作り上げてきたリスクアセスメント手法が十分であると考えるなら、変更の必要はない。

●管理策の変更

附属書Aにおける管理策は、技術の変化に対応した変更がなされた。管理策の総数は、133から114へと減少している。

改定版への移行期間と手続き、JIS発行時期

改定版への移行期間は2年(2015年9月末まで)となった。

JQAでは現在移行審査を受付けている。移行審査は定期審査あるいは更新審査に合わせて受審すれば追加工数はない。

移行審査を受ける際には、改定版に基づく新規、追加要求事項の運用実績(数ヵ月)が必要とされる。この実績に基づき、改定版による内部監査、マネジメントレビューの実施、および適用宣言書の改版も必須である。

ご希望により、業務相談、予備審査も実施する。なお、JIS Q 27001の発行時期は2014年3月が見込まれている。■

■ **表4: ISO/IEC 27001:2013の構成** (赤字は固有要求事項)

- 0 序文
- 1 適用範囲
- 2 引用規格
- 3 用語及び定義
- 4 組織の状況
  - 4.1 組織及びその状況の理解
  - 4.2 利害関係者のニーズ及び期待の理解
  - 4.3 情報セキュリティマネジメントシステムの適用範囲の決定
  - 4.4 情報セキュリティマネジメントシステム
- 5 リーダーシップ
  - 5.1 リーダーシップ及びコミットメント
  - 5.2 方針
  - 5.3 組織の役割、責任及び権限
- 6 計画
  - 6.1 リスク及び機会に対処する活動
    - 6.1.1 一般
    - 6.1.2 情報セキュリティリスクアセスメント
    - 6.1.3 情報セキュリティリスク対応
  - 6.2 情報セキュリティ目的及びそれを達成するための計画策定
- 7 支援
  - 7.1 資源
  - 7.2 力量
  - 7.3 認識
  - 7.4 コミュニケーション
  - 7.5 文書化した情報
    - 7.5.1 一般
    - 7.5.2 作成及び更新
    - 7.5.3 文書化した情報の管理
- 8 運用
  - 8.1 運用の計画及び管理
  - 8.2 情報セキュリティリスクアセスメント
  - 8.3 情報セキュリティリスク対応
- 9 パフォーマンス評価
  - 9.1 監視、測定、分析及び評価
  - 9.2 内部監査
  - 9.3 マネジメントレビュー
- 10 改善
  - 10.1 不適合及び是正処置
  - 10.2 継続的改善
- 附属書A(規定)管理目的及び管理策

(*7)
ISO/IEC 27001 は 2005 年に発行され、2008 年から定期的な見直しを開始する予定であったが、ISO マネジメントシステム規格の共通要素採用の決定を待つかたちで改定が行われた。

(*8)
4.1 項(組織及びその状況の理解)で内部及び外部の課題を決定し、4.2 項(利害関係者のニーズ及び期待の理解)で ISO/IEC 27001 にかかわる利害関係者を決定する。そして 4.3 項(ISMS の適用範囲の決定)で内部及び外部の課題と利害関係者の要求事項を考慮し、適用範囲を決定し、文書化した情報として明示する。

(*9)
6.1 項(リスク及び機会に対処する活動)の 6.1.1 項(一般)では、ISO/IEC 27001 の計画策定時にリスク及び機会の決定が要求される。リスクはマイナス面だけではなく、プラス面も含む。6.1.2 項(情報セキュリティリスクアセスメント)では情報についてリスク特定・リスク分析・リスク評価の実施が求められ、6.1.3 項(情報セキュリティリスク対応)ではリスク対応プロセスを文書化した情報で明確にすることを求められる。

JQAは、ISO/IEC 27001改定をこうみている

ISO/IEC 27001改定が組織に与える影響は?

いままでのISO/IEC 27001は、管理策にマネジメントを追加してできている構造という印象があり、概念的にもやや整理できていないように見えていました。例えば、違いがわかりにくい「ISMS基本方針」と「情報セキュリティ基本方針」を定義することが求められていたことなどです。今回の改定で、一連の情報セキュリティマネジメント(ISMS)の規格のISO/IEC 27000ファミリー(*10)の中で、ISO/IEC 27001は他の規格との関係もすっきり整理され、ISO/IEC 27000ファミリーの中核規格となりました。

ICT技術は目まぐるしく変化しており、クラウドコンピューティングを始め、インフラ制御システムに関する情報セキュリティのリスクは広がり続けています。このようなビジネス環境と直結した情報セキュリティマネジメントは、ICT企業だけでなくさまざまな組織から注目され、守るだけではなく、情報を活用するセキュリティへの展開を予感させます。

改定でISO/IEC 27001は、「How to」ではなく、「What」が中心になりました。今後、ISMS規格が個人情報、クラウドや通信などに広がっていくことを想定し、拡張性を持たせ、汎用性を高めた反面、どのように構築するか、具体的に何をすればいいかが、わかりにくくなっているように思えます。

今回の改定を振り返って注目しているポイントは以下のとおりです。①ISMSの認証規格として2005年版の継承。②マネジメントシステム規格の共通要素採用によるマネジメントシステム規格間の整合。③組織の内外の課題と利害関係者のニーズ及び期待を考慮した適用範囲の決定。④組織のプロセスへのISMS要求事項の統合。⑤リスクマネジメント規格ISO 31000との整合。

組織がISO/IEC 27001:2013に移行するために必要なことは?

ISO/IEC 27001:2013への移行は、いまある形をなるべく生かし必要最小限の変更で考えてください。現行の基準の方が詳しいところは捨てずに利用してもよく、過剰な部分は整理しスリム化してもいいかもしれません。

具体的な準備は、まず、組織のセキュリティに関する内外の課題を意識していただくと同時に、ISMSを実施しビジネスで何を成し遂げたいのか、ビジネス上どういうメリットを得ようとしているのかを意識していただきたいと思います。それを踏まえて、ISMSの適用範囲は正しいのか、方針はこれでいいのか確認していただきます。次に、目的を達成するための計画をきちんとつくり、パフォーマンスを評価と有効性の測定を行います。さらに、社内ルールについて管理策を中心に新旧の基準のギャップ分析を行い、リスク分析と結び付けて採用、不採用を明確にします。

2013年版への移行審査を受けるための必須事項は、①適用宣言書を2013年版に全面改定すること、②2013年版に適合するISMSを運用し、内部監査、マネジメントレビューを実施することです。また、規格改定を機に、①マンネリ化、形骸化してしまったシステムのムリ・ムダを洗い出し、現在の組織のニーズに合わせて見直しを行うことや、②ISO 9001やISO 14001など他のマネジメントシステムとの統合運用を視野に入れ、組織全体のマネジメントシステムの見直しを行うことを推奨します。

審査機関としての対応は?

この改定後もJQAの審査は大幅に変わることはありません。ISO/IEC 27001の審査は組織のビジネスプロセスに沿って行うことになりますが、JQAは10年以上前から、組織のビジネスプロセスに沿って組織のビジネスや経営をふまえたプロセス審査を行っており、大幅な変更は必要ないのです。また、共通要素の採用で他のマネジメントシステムとの統合運用が容易になり、新たに組織の戦略に必要なマネジメントシステムを追加導入する負荷も小さくなります。

JQAでは移行審査の受付を開始しています。ご心配があれば、事前に業務相談、予備審査サービス(いずれも有料)のご利用も可能です。移行期間についてのお知らせはJQAのWebサイトで別途公開します。

JQA情報セキュリティ審査部長　江波戸啓之

(*10)
ISO/IEC 27000 ファミリー(情報セキュリティマネジメントシステムに関する国際規格;作成中規格含む):ISO/IEC 27000(概要及び用語)、ISO/IEC 27001(要求事項)、ISO/IEC 27002(管理策の実践のための規範)、ISO/IEC 27003(実施の手引)、ISO/IEC 27004(測定)、ISO/IEC 27005(情報セキュリティリスクマネジメント)、ISO/IEC 27006(監査及び認証を行う機関に対する要求事項)、ISO/IEC 27007(監査のための指針)、ISO/IEC TR 27008(管理策の監査員のための指針;技術報告書)、ISO/IEC 27010(部門間及び組織間コミュニケーションのための情報セキュリティマネジメント)、ISO/IEC 27011(セキュリティ技術ー ISO/IEC 27002 に基づく電気通信組織のための情報セキュリティマネジメント指針)、ISO/IEC 27013 (ISO/IEC 27001 及び ISO/IEC 20000-1 の統合的実施の手引)、ISO/IEC 27014 (情報技術のガバナンス)、ISO/IEC TR 27015(金融サービスのための情報セキュリティマネジメントの指針;技術報告書)、ISO/IEC 27016(組織の経済的側面)、ISO/IEC 27017(クラウドコンピューティングサービスにおける ISO/IEC 27002 に基づく情報セキュリティ管理策実践のための規範)、ISO/IEC 27018(クラウドコンピューティングサービスのデータ保護制御の実践のための規範)