テクノファNEWS 第134号
2018年6月10日 発行

テクノファNEWS

Technology Transfer

ニュース・ダイジェスト

ISO9004:2018発行される

ISO9004:2018 Quality management -- Quality of an organization -- Guidance to achieve sustained success（品質マネジメント-組織の品質-持続的成功を達成するためのガイダンス）が2018年4月に発行された。世界の企業の平均的な寿命は縮まっているが、中には数百年近く生存している企業もある。急速に変わる世界でどうやって存在し続けていくのか。その疑問に答えを出す目的でISO9004は発行された。

2018年の企業長寿予測によると、スタンダード・アンド・プアーズ総合500種株価指数（S&P500）の平均的な会社はたった12年しか続かない。時価総額が少なくとも61億ドルの大企業500社は、新しいテクノロジー、経済ショック、手強い競争相手など、今後の課題に的確に準備できないことが、会社が終焉する主な理由である。

新たに発行された「ISO9004:2018 品質マネジメント- 組織の品質- 持続的成功を達成するためのガイダンス」は、世界中で最も長く続いている企業のうちの何社かの秘密と戦略を明らかにし、他の組織がそのような課題に備えると同時に組織のパフォーマンスを最適化することを目的にしている。

この規格を開発したISO委員会の幹事であるCharles Corrie氏は、「当規格の目的は組織が生き残るのを助けることである」と述べている。「企業倒産は、市場の変化、競争、または新しいテクノロジーに効果的に適応しないことが原因であることが多い」と彼は述べている。

「ISO9004は、世界中の最も成功している企業のうちの何社かの戦略、ベストプラクティス、及び経験を活かして、規模またはジャンルを問わずすべての企業にガイダンスを提供する。これには、今後の課題やここに至るまでに業績を高めてきた方法が含まれる。」

本規格は、以前のガイダンスを基に構築したISO9004:2009の改訂版であり、組織がそれらの品質マネジメントシステムの最大限の可能性を引き出すことにより全体の業績を改善することを助ける。

それは、組織が、組織の展望、目標（使命）、価値、及び文化というより広いコンテキスト（背景）での戦略、方針及び目的の調整（アラインメント）や展開などのトピックに取り組むことによって、ISO9001（品質マネジメントシステム）より優れた次のレベルに移るのを助ける。

ISO9004は、専門委員会ISO/TC176 品質マネジメント及び品質保証、分科委員会SC 2 品質システムにより開発された（委員会の幹事はイギリスBSI）。規格は各国の標準化団体またはISOストアから購入できる。
https://www.iso.org/news/ref2275.html

ISO/IEC27000情報セキュリティー規格が改訂される

ISO/IEC27000:2018は、2018年2月に改訂された。この規格は、情報セキュリティマネジメントシステム（ISMS）の概要を説明し、ISMSのISO/IEC 27001ファミリー規格でよく用いられる用語と定義を規定している。

ISO/IEC27000ファミリー規格には12を超える規格があるが、この規格は、ISO/IEC27000ファミリー規格に欠くことのできない専門用語をすべてまとめている。

ISO/IEC27000:2018は、共同専門委員会ISO/IEC JTC 1 情報技術、分科委員会SC 27 ITセキュリティ技術（ドイツのISO委員機関であるDINが事務局）により開発された。各国の標準化団体またはISOストアから購入できる。
https://www.iso.org/news/ref2266.html

OHSAS18001から新しい国際規格であるISO45001に移行

世界では、労働災害からくる致命的疾患のために、毎日何千もの命が失われている。これらは、防ぐことができた、あるいは防ぐべきであった死であり、今後は防がなければならない。ISO45001は、組織がまさにそれをすることを手助けすることをめざす。ISO/PC283/WG1リーダーKristian Glaesel

氏とBSIのCharles Corrie氏が、新しい規格を使ってどのように最善の安全をもたらすかを教えてくれる。

● ISO45001は何ですか？

ISO45001は、世界初の労働安全衛生を扱う国際規格であり、OH&Sのパフォーマンスの改善を望んでいるすべての組織のためのただ一つの明確な枠組みを提供する。組織のトップマネジメントは、それを使って従業員と訪問者に安全で健全な職場を提供することをめざす。これを達成するためには、人の身体、精神、認識の状態への悪影響を軽減することによって、疾病や負傷、そして極端な場合死をもたらす恐れのあるすべての要素を管理することが不可欠である。ISO45001はそれらの側面すべてを扱っている。

ISO45001は、従来のOH&Sのベンチマークだったに基づいているが、改訂版または最新版ではなく、新しい全く異なる規格であり今後3年の間に段階的に導入される予定である。従って組織は、労働安全衛生について現在の考えや仕事のやり方を変える必要がある。

● OHSAS18001とISO45001の大きな違いは何ですか？

違いは多くあるが、OHSAS18001はOH&Sのハザードや他の内部の問題を管理することに焦点を合わせているが、ISO45001は組織とそのビジネス環境の相互作用に焦点を合わせていることが主な変化である。2規格はまた以下のようにも異なる。

・ISO45001はプロセスベースである－OHSAS 18001は手続きベースである
・ISO45001はリスクと機会を考慮する－OHSAS 18001はただリスクだけを扱う
・ISO45001は利害関係者の見解（考え）を含む－OHSAS18001は含まない

これらのポイントは労働安全衛生マネジメントのとらえ方の重要な変化を表している。OH&Sはもう「スタンドアロン」として扱われず、持続的成功な組織を運営する要素として捉えなければならない。2規格は構造では異なっているけれども、OHSAS 18001に従って確立されたマネジメントシステムは、ISO45001の構築の強固な基盤になる。

● OHSAS18001の認証を取得しているが、どうやって移行を開始するのか？

OHSAS18001から移行する際には、新しいマネジメントシステムそのものが確立できるように、「地固めをする」必要がある。以下の順番に従うなら、移行へ向かってうまく進むことになるでしょう。

1. あなたの組織のビジネスに影響を及ぼすかもしれない外部要因及び内部要因、利害関係者（あなたの組織の活動に影響し得る個人または組織）の分析を行い、あなたのマネジメントシステムにこれらのリスクがどのように管理できているかを自問してください。
2. あなたのマネジメントシステムは何を達成するために確立されたかを考えながら、マネジメントシステムの範囲を決定してください。
3. プロセス、リスク評価/リスクアセスメントを確立、プロセスの重要評価指標（KPIs）の設定に、1、2の情報を使ってください。

以上の情報をOHSAS18001に適応させると、新しいマネジメントシステムの基礎が出来上がる。

● ISO45001が初めてなら何を知る必要がありますか？

ISOマネジメントシステムについてどのくらい知っているかによる。ISO45001は附属書SL（共通テキスト）を採用することにより、同一構造、同一コアテキスト、同一用語と定義が使われ、ISO9001:2015（品質マネジメントシステム）やISO14001:2015（環境マネジメントシステム）などの他のISOマネジメントシステム規格と共通化されている。すでに共通テキストに精通しているのなら、ISO45001の多くはなじみがあるだろうから、システムの「足りない部分」を補う必要があるだけである。

そうでなければちょっと難しいかもしれない。ISO45001をふつうの本として読めば理解しにくい。具体的な条項がどう関連し合っているかをすべて理解しなければならない。規格の可能性を十分に引き出す優れた研修コースを見つけることを勧める。そのプロセスにおいてコンサルタント会社のサービスを利用することも考えられる。

● ISO9001とISO14001両方の認証を取得した統合システムを有している。他のマネジメントシステムと一緒にどのようにISO45001を使うことができますか？

ISOマネジメントシステム規格に共通の枠組（共通テキスト）は、新しいマネジメントのトピックを組織の既存のマネジメントシステムに統合するのを容易にするために慎重に開発された。例えば、多くの組織がOH&SMSと環境MSを同じ機能で管理していることから、ISO45001はISO14001にかなり同様な規定を持っている。

● ISO45001をどのように利用するのですか？

組織の多くは効果的なOH&Sマネジメントシステムを確立するためにISO45001を使用し、認証書を取得する組織はわずかではないかと予想している。ISO45001の中には、認証を得るための要求事項は何もない。労働安全衛生マネジメントシステムを整え、ベストプラクティスを実行することで多くの恩恵を得ることができる。ISO認証は、外部の関係者に規格を完全に満たした組織であることを実証する公式な承認にすぎない。

ISO45001を正しく実行するなら受ける恩恵は尽きることがない。規格はOH&Sのリスクを扱い、管理することを義務付けると同時に、OH&Sマネジメントシステムが常に有効であるために絶えず変化し

続ける組織の状況に継続的改善を要求している。さらに、世界的規模で現行の法律に従うことを確実にする。これらの手段をすべて同時に行うことにより、組織の戦略目標を達成し続けながら、保険料負担を減らすことから従業員の士気を高めることまで、結果として恩恵を多く受け、組織の「働くのに安全な場所」であるという評判を確立することができる。
https://www.iso.org/news/ref2271.html

ISO45001―知らなければならないこと

OHSAS18001から新しい国際規格であるISO45001に移行するにはいくつもの課題があるかもしれないが、綿密な計画を立て、チェックし、取り組むことで、組織、その従業員、及びすべての利害関係者は、改善された労働安全マネジメントシステムの恩恵を享受するだろう。

数値を見れば、なぜ労働安全衛生が重要なのかは明らかである。ILO（国際労働機関）によると、業務上の事故、負傷、及び職業病により、毎年約278万人が亡くなっている。ILOは、労働安全衛生の実施が悪いと経済にかかる負担は、年間全世界の国内総生産（GDP）の3.94%と推定されると主張している。

EU-OSHA（欧州労働安全衛生機関）の長官であるChrista Sedlatschek氏もまたフィナンシャル・タイムズ紙の中で次のように書いている。「仕事関連の健康障害と負傷による経済的損害は、EUのGDPの3%から5%に相当すると推定される。」

テクノロジーや人工知能の進歩によって仕事と職場の性質は、大きく変化しておりこれが大きな課題となっている。グローバル・ウェルネス研究所は、仕事は以前より変わりやすく、人々が共同で行うものになっているとして、新しいテクノロジーについて労働者に習得させる必要性を強調している。研究所のWellness at Workリポートは、次のように述べている。「企業が今後も存続し続け成功するために、労働環境及び労働文化を働く人々の価値観、モチベーション及び健康ニーズに合わせなければならない。」

◆ 協力して一つになること

企業は、生産性を高め、収益性を改善し、全従業員の福祉を向上させようと努力(奮闘)しているが、自社の労働安全衛生マネジメントシステムをもっと注意して見るべきである。労働安全を扱う国家規格や認証スキームをめぐる何年にもわたる混乱の結果、国際的合意である労働安全衛生評価シリーズ（OHSAS）のプロジェクトグループが生まれた。グループには、各国の標準化団体、学界、認定及び認証機関、及び労働安全衛生機関の代表者が集められた。イギリスの標準化団体であるBSIグループが事務局を提供した。

BSIに協力し、OHSASプロジェクトグループの代表を務めるTrevor Dodd氏は、OHSAS18001により経営層のコミットメント及び関与が改善され、訓練及びコミュニケーションも改善されたと述べている。で、どうして新規格なのですか？Dodd氏は次のように説明する。「事故及びインシデントが低下したが、世界がより複雑に、相互につながっていくにつれて、労働安全衛生もまた、時代とともに変化して新しいISO規格が求められた。労働安全衛生に関するすべての側面である資源、能力、業務管理、パフォーマンス評価、継続的改善に合わせて、リーダーシップ、協議と参加、ハザードの特定、リスク及び機会の評価などに触れている。」

◆ 課題に取り組むこと

ISO45001は、ISO9001品質やISO14001環境などの他のISOマネジメントシステム規格と共通の構造になっている。OHSAS18001からISO45001への移行には、3年間の移行期間がある。しかし、Long氏は、構造が変わっているので意外と時間がないかもしれないと警告している。

フランスの国立調査安全研究所（INRS）のCatherine Montagnon氏は、新規格により「階層化されたコントロールに従って、ハザードを取り除き、リスクを最小限にするための手段が強化された」と考えている。彼女は、認証制度だけでは、労働環境の安全衛生の改善には至らず、トップマネジメントがコミットメントを明確にしただけで終わる危険があると指摘する。「労働条件の改善には、社会的対話の強化及びすべての階層の働く人々の関与に基づいたグローバルなアプローチが必要である。働く人々とその代表者は、改善の可能性の特定、リスクアセスメントに貢献し、行動計画の開発及び実行に携わるべきである。」と、彼女は言う。

◆ より明確なメッセージ

Montagnon氏は、グローバル化及び国の経済構造の変化により「世界中で労働安全衛生の文化を高める」ことが難しくなると警告する。彼女はリスク及び機会を詳しく説明する。「国家間の格差がリスクであり、国家間の矛盾を大きくしている。労働安全衛生へのアプローチが、欧米先進国（例えば、米国、カナダ、ヨーロッパ、オーストラリアなど）のニーズや期待に焦点を合わせていて、他の国のニーズや期待には合っていないこともリスクである。しかし、労働安全衛生マネジメントシステムに対する国際的に認められた要求事項に裏打ちされた労働安全衛生の文化の構築は機会であると明確なメッセージを出したい。」

Long氏はこのようにまとめる。「認証書を取得することは価値であろうが、それだけのためではなく、ISO45001を組織の事故防止に役に立たせる活動がISO45001の恩恵を最大に受けることになる。」
https://www.iso.org/news/ref2270.html

個人情報マネジメントシステム要求事項 JIS Q 15001:2017とマネジメントシステム

(株)テクノファ 情報セキュリティ関連コース 講師
(有) インターギデオン　川辺　良和

1. はじめに

プライバシーマークの要求事項である個人情報保護マネジメントシステムJIS Q 15001:2017（以下、本規格）が2017年12月20日に改訂・公表された。本規格は、2017年5月30日に全面施行された改正個人情報保護法への対応として注目されており、本規格の改訂、それに続く2018年1月12日のプライバシーマーク付与適格性審査基準の改訂・公表と続くことになるが、ここでは、本規格の特徴とISMS等他のマネジメントシステムとの関連について述べる。

2. 個人情報マネジメントシステム要求事項JIS Q 15001:2017の特徴

（1）共通マネジメントシステムフレーム（HLS）の採用

本規格の特徴として、ISOマネジメントシステムフレームの共通化が挙げられる。本規格は、統合版ISO補足指針の付属書SLに規定する上位構造（HLS）を採用、本規格箇条0.2で「他のマネジメントシステム規格との近接性」として記され、他のマネジメントシステム規格と共通のフレームで構成されている。

本規格の構成と、JIS Q 27001：2014情報セキュリティマネジメントシステム（ISMS）の構成との対比を表2に示すが、共通フレーム（HLS）は、具体的には、1.適用範囲、2.引用規格、3.用語及び定義、4.組織の状況、5.リーダーシップ、6.計画、7.支援、8.運用、9.パフォーマンス評価、10.改善の構成であり、表2の通り、規格本文は4.3～4.4、6.2、8.2～8.3における「個人情報保護」か「情報セキュリティ」のみの相違となっている。

本規格はISOのJIS化でなく、JIS規格改訂で共通フレーム（HLS）を採用した結果、マネジメントシステム要求事項を記した本文と、管理策を記した付属書A（規定）以下とに分離された。

表2を見ると、規格本文に付属書A,B,C,Dが追記されているが、付属書A「管理目的及び管理策」は、旧規格JIS Q 15001：2006箇条3に定めた要求事項の改訂であり、付属書B「管理策に関する補足」は、旧規格の解説に相当する管理策に関する補足説明になっている。

付属書C「安全管理措置に関する管理目的及び管理策」は、ISMS規格の付属書Aに相当する管理目的及び管理策の包括的なリストといえる。

付属書D「新旧対応表」では、旧規格の「事業者」を新規格で「組織」に、以下「代表者、事業者の代表者」を「トップマネジメント」、「リスクの認識、分析」を「個人情報保護リスクアセスメント」に、「（リスクの）対策」を「個人情報保護リスク対応」に、「残存リスク」を「残留リスク」に、「実施及び運用」を「運用」に、「教育」を「認識、教育」に、「点検、代表者による見直し」を「パフォーマンス評価」に等と表記している。

（2）個人情報保護法改正に伴う追加・変更

本規格は、個人情報保護法改正に伴って発生した改訂規格とも言えるものであり、実際に本規格の巻末の解説3.2には、個人情報保護法改正に伴う要求事項として追加又は変更された項目として、次の内容が掲げられている。

a）“特定な機微な個人情報”を“要配慮個人情報”に変更した。
b）旧規格では“個人情報”としていた要求事項の一部を「個人データ」に変更
c）“開示対象個人情報”を“保有個人情報”に変更
d）外国にある第三者への提供の制限の追加
e）第三者提供に係る記録の作成などの追加
f）第三者提供を受ける際の確認
g）匿名加工情報の追加

以下、規格本文、及び付属書Aのポイントを旧規格との対比しながら述べることにする。

3. 個人情報マネジメントシステム要求事項JIS Q 15001:2017規格本文の内容

＜3. 用語及び定義＞

用語及び定義は、「3.1組織」から「3.47リスク所有者」までを規定しているが、個人情報保護マネジメントシステム以外の旧規格にはなかった「リスク」関係や「測定量」関係の用語など、多くの用語を規定している。

＜4. 組織の状況＞

この項目については、関係する要求事項として「3.3.2法令、国が定める指針その他規範」、「3.3.1個人情報の特定」が挙げられる程度で明確に該当する項目はなく、本規格で要求事項になった項目と言える。「4.1組織及びその状況の理解」、「4.2利害関係者もニーズ及び期待の理解」、「4.3個人情報保護マネジメントシステムの適用範囲の決定」、「4.4個人情報保護マネジメントシステム」から構成されている。

組織の状況として、内外の課題及び利害関係者とそのニーズを把握し、個人情報保護マネジメントシステムとしての適用範囲を決定・文書化してマネジメントシステムへと展開するフレームが規定されている。

＜5. リーダーシップ＞

旧規格の「3.3.4資源、役割及び権限」、「3.2個人情報保護方針」が、本規格では「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」として構成されている。特に、旧規格が1つであった個人情報保護方針について、5.2.1内部向け個人情報保護方針と5.2.2外部向け個人情報保護方針に分けて規定されている他、附属書A3.2.1、A3.2.2で管理策としてより詳細に定められている。

＜6. 計画＞

旧規格の「3.3計画」、「3.3.3リスクなどの認識、分析及び対策」、「3.3.6計画書」が本規格では、「6.1リスク及び機会に対処する活動」、「6.2個人情報保護目的及びそれを達成するための計画策定」から構成されている他、附属書A3.3.3、A3.3.6で管理策としてより詳細に規定されている。

本項目は、リスクに関する計画の要求事項であり、運用として実施は「8.運用」の中でリスク要求事項として定められている。

＜7. 支援＞

旧規格の「3.3.4資源、役割、責任及び権限」、「3.4.5教育」、「3.3.7緊急事態への準備」、「3.5個人情報保護マネジメントシステム文書」が、本規格では、「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」から構成されている他、附属書A3.3.4、A3.4.5、A3.3.7、A3.5に管理策として詳細に規定されている。

旧規格の「3.4.5教育」及び「3.3.7緊急時対応」は規格本文では、教育ではなく「7.3認識」、緊急時対応ではなく、「7.4コミュニケーション」として規定されている点に注意が必要である。

また、「3.5個人情報保護マネジメントシステム文書」が記録も含めた「7.5文書化した情報」として規定されている。

＜8. 運用＞

旧規格の「3.4実施及び運用」、「3.4.1運用手順」が「8.1運用の計画及び管理」、「8.2個人情報保護リスクアセスメント」、「8.3個人情報保護リスク対応」から構成されている他、附属書A3.4.1、A3.3.3で管理策として詳細に定められている。

＜9. パフォーマンス評価＞

旧規格の「3.7点検」、「3.7.1運用の確認」、「3.7.2監査」、「3.9事業者の代表者による見直し」に相当する要求事項が、本規格では「9.パフォーマンス評価」として包括的に規定された。「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」から構成されている他、附属書A3.7.1、A3.7.2、A3.7.3で詳細に規定されている。

＜10. 改善＞

旧規格の「3.8是正措置及び予防処置」から、「10.1不適合及び是正処置」、「10.2継続的改善」に変更されている他、附属書A3.8で詳細に規定されている。旧規格の予防措置の用語はなくなったが、考え方としては、是正処置と継続的改善により予防措置を講ずることに繋がると理解できる。

4. 個人情報マネジメントシステム要求事項JIS Q 15001:2017付属書Aの内容

ここでは、個人情報に係る要求事項の中心であった旧規格3に相当する付属書Aに規定された要求事項について、追加・変更された内容を中心に記載する。

＜A3.2個人情報保護方針＞

A3.2.1内部向け個人情報保護方針とA3.2.2外部向け個人情報保護方針として記載されている。

＜A3.3.1個人情報の特定＞

組織は、特定した個人情報については、個人データと同様に取り扱わなければならないが追加された。

＜A3.3.3リスクアセスメント及びリスク対策＞

組織は、現状で実施し得る対策を講じた上で、未対応部分を残留リスクとして把握し、管理しなければならないが追加された。

＜A3.4.2.1利用目的の特定＞

組織は、利用目的の特定に当たっては、取得した情報の利用及び提供の範囲を可能な限り具体的に明らかにするよう配慮しなければならないが追加された。

＜A3.4.2.3要配慮情報＞

旧規格の「特定な機微に個人情報」は、要配慮情報として個人情報保護法を踏まえた記載となり、e)その他の規定が追加された。

＜A3.4.2.7本人に連絡又は接触する場合の措置＞
旧規格の「本人に直接アクセスする場合の措置」に相当する内容として記載されている。
＜A3.4.2.8個人データの提供に関する措置、A3.4.2.9匿名加工情報＞
個人データとして記載されている。また、A3.4.2.8.1外国にある第三者への提供の制限、A3.4.2.8.2第三者提供に係る記録の作成、A3.4.2.8.3第三者提供を受ける際の確認、並びにA3.4.2.9匿名加工情報は、改正個人情報保護法対応として新たに追加された。
＜A3.4.3.1正確性の確保＞
組織は、個人データを利用する必要がなくなったときは、当該個人データを遅滞なく消去するよう努めなければならないが追加された。
＜A3.4.3.2安全性の確保＞
付属書C参照が追記され、ISMSの付属書Aに相当する管理策として追加された。
＜A3.4.3.4委託先の監督＞
委託を受ける者を選定する基準には、少なくとも委託する当該業務に関しては、自社と同等以上の個人情報保護の水準にあることを客観的に確認できることを含めなければならない、及び契約の要求事項として、h)契約終了後の措置が追加された。
＜A3.4.5認識＞
旧規格の教育は、箇条7.3との係わりを踏まえ、認識となった。
＜A3.5.1文書化した情報の範囲＞
d)内部規程に定める手順上で使用する様式が追加された。
＜3.7パフォーマンス評価＞
旧規格の点検は、パフォーマンスの評価となり、旧規格の事業者の代表者による見直しは、運用の確認、内部監査の後に「3.7.3マネジメントレビュー」として位置づけされた。
＜A3.7.1運用の確認＞
個人情報保護管理者は、トップマネジメントによる個人情報保護マネジメントシステムの見直しに資するため、定期的に、及び適宜にトップマネジメントにその状況を報告しなければならないが追加された。

5. JIS Q 15001:2017とISMSを中心とする他のマネジメントシステムとの関係

本規格は、個人情報保護マネジメントシステムPMSの要求事項であり、付属書C「安全管理措置に関する管理目的及び管理策」は、ISMS規格の付属書Aに相当する管理目的及び管理策の包括的なリストになっている旨を述べた。個人情報自体が情報として位置づけられるため、ＩＳＭＳ規格の管理策はＰＭＳでも有効活用可能といえる。
個人情報保護対策や管理策は、ＯＥＣＤのプライバシーガイドライン８原則である「収集制限の原則」、「データ内容の原則」、「目的明確化の原則」、「利用制限の原則」、「安全保護の原則」、「責任の原則」、「公開の原則」、「個人参加の原則」をベースとしているが、この中で「安全保護の原則」は情報セキュリティとの接点といわれており、附属書C、「安全管理措置に関する管理策のリスト」として位置づけられる所以ともいえる。

個人情報保護法改正により、個人を識別できる情報としての個人情報の定義が明確化された。他のマネジメントシステムを取得・運用する組織においても、取引先や社員情報、採用予定者や、退職者情報等の個人情報を利・活用していることから、個人情報の適切な管理はコンプライアンス上も欠かせない。具体的には、管理すべき個人情報を特定し、適切に管理することは、マネジメントシステムを超えて重要であり、内部監査としての監査チェックポイントとしてモニタリングすることが必要と言える。ここでは、内部監査のチェックリストの例を表1に掲げる。

表1　個人情報保護に係る内部監査チェックリストの例

- **管理すべき個人情報を特定し適切な個人情報保護教育を実施しているか。**
- **遵守すべき個人情報関連法令、国が定める指針その他規範を特定し、周知、運用管理しているか。**
- **マイナンバーの取扱い、ルール策定と運用は適切か。**
- **採用応募者情報の管理は適切か。**
  - **→取得目的を明確にして本人の同意を得ているか。**
  - **→第三者提供・利用についての取り扱いは適切か。**
- **退職者情報の取扱いは開示請求等、本人の権利への対応を含め適切か。**
- **退職者のアカウント無効化などについて、適切な取扱いをルール化し運用しているか。**
- **懸賞・プレゼント・応募者情報の取扱いは、子供等が応募者のケースも含め適切か。**
- **株主情報の取扱いは株主優待製品の故障・部品の注文などの問合せも含め適切か。**
- **健康診断・組合員等、要配慮情報の取扱いは適切か。　　など**

表2　JIS Q 15001:2017個人情報マネジメントシステムと
JIS Q 27001:2014情報セキュリティマネジメントシステムの要求事項の構成の対比

	JIS Q 15001:2017個人情報保護マネジメントシステムの構成	JIS Q 27001:2014情報セキュリティマネジメントシステムの構成
	0　序文　　0.1　概要 0.2他のマネジメントシステム規格との近接性	0　序文　　0.1　概要 0.2他のマネジメントシステム規格との両立性
	1.適用範囲　2.引用規格　3.用語及び定義	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　**個人情報保護**マネジメントシステムの適用範囲の決定 4.4　**個人情報保護**マネジメントシステム	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	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 6.2　**個人情報保護**目的及びそれを達成するための計画策定	6.1　リスク及び機会に対処する活動 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	7.1　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
8.運用	8.1　運用の計画及び管理 8.2　**個人情報保護**リスクアセスメント 8.3　**個人情報保護**リスク対応	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	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	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	管理目的及び管理策
附属書B(参考)	管理策に関する補足	－
附属書C(参考)	安全管理措置に関する管理目的及び管理策	－
附属書D(参考)	新旧対応表	－
	参考文献　解説	参考文献　解説

■筆者紹介■

川辺 良和氏（ISMS主任審査員 システム監査学会理事）
有限会社インターギデオン 代表取締役

●テクノファ担当セミナー
- プライバシーマークと改正個人情報保護法 ～マネジメントシステムへの影響～（TT65）
  JRCA　ISMS審査員CPD登録コース
- 情報セキュリティにおける内部監査コース（TT33）
  JRCA　ISMS審査員CPD登録コース

●著書
- システム監査基準解説書(経済産業省監修 共著)
- システム監査白書(通産省監修1995-2000共著)
- システム監査技術者育成カリキュラム(中央情報教育研究所 共著)
- システム監査技術者育成テキスト下巻(中央情報教育研究所 共著)
- プライバシーマーク制度における監査ガイドライン(日本情報処理開発協会 共著)
- システム監査Q＆A110((財)日本情報処理開発協会 共著)
- システム監査技術者入門(コンピュータエージ社 共著)
- システム監査技術者試験午後重点対策(アイテック社)

テクノファ最新ニュース

Technology Transfer

JRCA登録 CPDコース
プライバシーマークと改正個人情報保護法
～マネジメントシステムへの影響～

2017年5月30日に10年ぶりに個人情報保護法が改正され、12月20日にはプライバシーマーク要求事項のJIS Q 15001:2017が公表されました。

本コースでは改正個人情報保護法を解説するとともに、プライバシーマークやマネジメントシステムへの影響などについて演習を交えて解説します。

●こんな方にオススメ

・プライバシーマーク事務局・推進者
・情報セキュリティ担当者
・改正個人情報保護法の内容とマネジメントシステムへの影響を把握したい方

コースID：【TT65】
時　間：9:30～17:00
料　金：32,400円（一般）
　　29,160円（会員）

日程：
No.3 ： 2018年 6月18日(月) 大阪
No.4 ： 2018年 7月13日(金) 東京
No.5 ： 2018年 8月 6日(月) 川崎
No.6 ： 2018年 9月25日(火) 東京
No.7 ： 2018年10月18日(木) 大阪

毎月各地で開催、10月以降は下記参照ください
https://www.technofer.co.jp/isotrg/tt65/

内部監査員コースのご案内

明解なテキストと実践演習、経験豊富な講師の指導で定評のある内部監査員2日間コースです。

●ISO9001内部監査員2日間コース（コースID：TQ31）
●ISO14001内部監査員2日間コース（コースID：TE31）
●ISO/IEC27001内部監査員2日間コース（コースID：TT31）
●ISO22000内部監査員2日間コース（コースID：TQ38）
●労働安全衛生内部監査員2日間コース（コースID：TS31）
●IATF16949内部監査員2日間コース（コースID：TQ35）
●JIS Q 9100航空宇宙内部監査員2日間コース（コースID：TQ37）
●JEAC4111内部監査員2日間コース［講師派遣型セミナー］（コースID：TQ45）

知識、経験のない方でも理解しやすいマネジメントシステム規格解説の講義と、内部監査に必要な知識・技能を習得していただく、講義と実践的なケーススタディで、即戦力の内部監査員として活躍していただくカリキュラムをご提供しています。

企画・編集／株式会社テクノファ
〒210-0006 川崎市川崎区砂子１-10-２　ソシオ砂子ビル
TEL:044-246-0910 FAX:044-221-1331
ホームページ⇒http://www.technofer.co.jp/