JQA

一般財団法人 日本品質保証機構
マネジメントシステム部門

企画センター
〒101-8555　東京都千代田区神田須田町1-25　JR神田万世橋ビル17F
TEL.03-4560-5710／FAX.03-4560-5760

ISO関西支部
〒532-0003　大阪府大阪市淀川区宮原4-1-9　新大阪フロントビル2F
TEL.06-6393-9040／FAX.06-6393-9056

ISO中部支部
〒450-0003　愛知県名古屋市中村区名駅南1-24-30　名古屋三井ビルディング本館9F
TEL.052-533-9221／FAX.052-533-9279

ISO東北事務所
〒024-0051　岩手県北上市相去町山田2-18　北上オフィスプラザ5F
TEL.0197-67-0031／FAX.0197-67-0033

ISO九州事務所
〒812-0011　福岡県福岡市博多区博多駅前3-2-8　住友生命博多ビル11F
TEL.092-432-4810／FAX.092-432-4811

URL　https://www.jqa.jp

JQAマネジメントシステム情報誌 ISO NETWORK 2021 Vol.33
2021年2月発行

JQAマネジメントシステム情報誌

2021
Vol.33

ISO NETWORK

特集

一般財団法人 日本品質保証機構

特集 第一部

新型コロナウイルスの感染症拡大を踏まえて、改めてISO 9001を考える

新型コロナウイルス感染症の拡大により、業種を問わずテレワーキングが積極的に導入されるなど、企業の多くが従来とは仕事のやり方を大きく変更する必要に迫られている。このような状況下での品質マネジメントシステムの運用について、審査事業センター 品質審査部 部長（審査事業センター 副所長）の大久保 友順に聞いた。

審査事業センター
品質審査部 部長
（審査事業センター 副所長）
大久保 友順

新型コロナウイルスの感染症拡大を受けて

過去にも重大な災害を経て企業が大きな変化に直面することはありましたが、今回のコロナ禍は今なお進行しています。いつ収束するか分からないという点で、これまでに類を見ない事態です。こうした状況のなかで、ISO 9001に取り組む企業はそれぞれ品質マネジメントシステムに必要な変更を加えながら、品質管理・品質保証を追求しています。審査では、こうした外部環境の変化を受けて行うマネジメントシステムの変更点は焦点となります。企業と対話しつつ、粗探しはせずにマネジメントシステムが意図した結果を達成できているかを注意深く確認しています。

ISO 9001では変更の要求事項が規定されています。これは、品質マネジメントシステム自体が、状況に応じた変更に柔軟に対処できる「生きた」マネジメントシステムであることを意図しています。今回のような事態でも、マネジメントシステムの変更を適切に管理・運用していけば、事業本体に及ぶドラスティックな変化にも十分に対処することができ、事業運営の大きな助けになるでしょう。審査を通じて、ISO 9001の認証を取得している企業は、自社が定めた変更管理のルールを適用して、業績回復につなげることができていると実感しています。

この重大な局面でもISO 9001の本質をしっかり見つめ、生きたマネジメントシステムとして、柔軟かつ自在に運用してください。次では、箇条ごとに審査上のポイントを説明します。

審査で注目するポイント

箇条4　組織の状況

適用範囲は、箇条4.1（組織及びその状況の理解）、箇条4.2（利害関係者のニーズ及び期待の理解）を考慮して決定します。これまで5カ年計画などの中長期計画のタイミングで、企業の状況や利害関係者のニーズ・期待の変化を確認して適用範囲の見直しを行うことが一般的でした。5カ年計画の場合、5年サイクルの間でも企業の環境は大きな変化がありませんでしたが、それがコロナ禍では、1年間で大きく変化している企業があり、変化のサイクルが短縮されていると感じています。

また、企業によっては、業績に大きく影響を受けるような事業環境の変化に伴い、今までとは異なるビジネスを取り入れることで、顧客が大きく変わる場合があります。例えば、テレワーキングの普及により印刷物やコピーの需要が減ったために、印刷会社など紙媒体を扱う企業が、テレワーキングで需要が伸びる情報関連ビジネスに取り組むといったことが起きています。この場合には、取引先が変わり企業を取り巻く外部・内部の課題や利害関係者のニーズも変わるので、適用範囲の見直しも視野に入ってきます。同様に飲食業や流通業など、従来は対面で業務を行ってきたサービス業が、対面を避けることにより業務形態が大きく変わる場合には、適用範囲の見直しが必要となることがあります。

適用範囲が変わらない企業でも、箇条4.2（利害関係者のニーズ及び期待の理解）が大きく変わる場合があります。例えば、テレワーキングの導入に伴って従業員の在宅勤務などの勤務体系が変わる場合や、従来のプロセスから変わる場合などの状況変化です。審査では、プロセスレベルの変更があった場合には、規格に定められている変更管理が行われたかを確認します。

箇条5　リーダーシップ

リーダーシップに関しては、後の箇条6（計画）、箇条7（支援）、箇条8（運用）で要求される計画や資源、運用などの変更について、トップマネジメントがしっかり関わって対応できているかが重要です。特に、テレワーキングが常態となりコミュニケーション方法が大きく変わるなかで、箇条5.2.2（品質方針の伝達）で述べられるコミュニケーションが適切になされているかを審査では確認します。

箇条6　計画

箇条6.1（リスク及び機会への取組み）に関しては、コロナ禍という緊急事態に対処し品質マネジメントシステムの意図した結果を妨げかねないリスクを回避または最小化することが重要ですが、リスクを機会にする考え方に立って何にどう取り組むかも欠かせない視点です。

事例としては、マスクの販売業があります。従来は、消耗品である不織布製の使い切りマスクを中国から輸入し、低価格で供給するビジネスでした。コロナ禍が世界に広がる時期には中国からの製品供給が遮断されてしまいましたが、国内のマスク販売業者は知恵を絞り、繰り返し使用できる綿などでできた洗えるマスクを製品化して市場を作り出していきました。不織布マスクの供給遮断というリスクを、新たな洗えるマスクの販売という機会に変えたのです。中国から不織布の素材が入ってこないので国内で製造できるメーカーを発掘し対処した企業もあります。現在は低コスト化し国内で安定供給できるようになり、供給元の多様化というリスク分散になりました。

こうした取り組みのなかでは、供給元が変わることなど

によるリスクを評価しつつ、これまで3～6か月かけて製品の出荷承認をしていたものを1～2か月に短縮して出荷できる仕組みに変更するなど、マネジメントシステムの変更を進めスピード感のある対応につなげています。審査では、このような変更が箇条6.3（変更の計画）に基づき行われたかを確認します。

箇条6.2（品質目標及びそれを達成するための計画策定）については、コロナ禍では、年初に立てた品質目標を変えざるをえないケースがあります。例えば、企業のなかには箇条6.1（リスク及び機会への取組み）に基づき品質目標を立て阻害要因として市場クレームを設定し市場クレーム率を品質目標のKPIとしている場合があります。しかしコロナ禍による売上減で、その母数が大幅に減ってしまうとクレーム率はとても達成できない大きな数字になってしまいます。このように、経営環境が大きく変わった場合は、KPIの妥当性を含めて再検討が必要です。

箇条6.3（変更の計画）については、品質マネジメントシステムやプロセスを変える場合は、変更が計画的な手法で行われているかを確認します。コロナ禍で、従来の業務が変わっている場合があります。例えば、対面で行われていた営業活動に、ネットによる営業活動も追加されている場合などは、プロセスを追加したり、営業の仕組みを追加しています。このような場合は、箇条6.3（変更の計画）による要求事項の確認が必要となります。注意したいのは、いかなる変更でも、変更前と同じく要求を満たしていることです。箇条6.3（変更の計画）　b）にある、マネジメントシステムが完全に整っている状態でなければなりません。

箇条7　支援

箇条7.1（資源）では、品質マネジメントシステムの活動を行う上で必要な資源の提供に関する要求事項です。例えば、物流業界ではテレワーキングの普及や外出回避などによりネット販売などが伸びていることを受け、物流量の増加や納期の変更に対応しなければならないという状況にあります。また、製造業では、緊急事態宣言後は、海外から日本に物資が届かなくなった時期があり、製品の素材の供給元を変えるという大きな変更が見られました。審査では、このような状況下であっても、品質マネジメントシステムの活動を行う上で必要な資源4M（Man（人）／Machine（機械）／Material（材料）／Method（方法））が提供されているかを確認します。

箇条7.2（力量）では、密を避けるための対応策として、検査員を多能工化する動きが進んでいます。例えば、今まで寸法測定に3人、電気測定に2人が専門的に携わってきた場合、コロナ禍では5人全員が同時出勤することが難しいため、それぞれの専門分野を超えて、寸法検査・電気検査の両方をできるように教育・訓練して資格を与えるといった対策が必要になります。人員の減少は4M（Man（人）／Machine（機械）／Material（材料）／Method（方法））に関わる変更です。審査では、この4Mに関わる変更が品質管理の方針や目的どおりに行われているかを確認します。

箇条7.3（認識）では、熟練技能の伝承などが対象となります。従来のOJTのように、直接現場で教育することが困難になった現状を踏まえ、マニュアルを電子化して保存することや、熟練者による作業の様子を映像として保存するなどの対応が進んでいます。

箇条7.5（文書化した情報）では、大企業で進んできた電子化とネットワークの共有化が、中小規模の企業にも広がっていることが特徴的です。例えば検査記録をネット管理すれば、検査者と承認者が違う場合でも紙に出力して判を押す必要がありません。これは業務の効率化という面からも重要なことです。審査では、文書化した情報の電子化とネットワークの共有化がマネジメントシステムに取り込まれているかを確認します。

このほか審査では、箇条7.4（コミュニケーション）のテレワーキングの導入などで大きく変化したコミュニケーションの仕組みや、箇条7.1.3（インフラストラクチャ）における情報通信技術の変化が、マネジメントシステムにどのように取り込まれているのかを確認します。

「密を避ける」観点から、今まで10人で行ってきた業務を7人で行うために、IoTの技術を取り入れていく企業が増えています。品質保証の世界でも、徐々に自動測定器の導入が進みつつあります。人間が測定してデータを書き留めるという作業をなくし、人を介さない検査手法が確立してきています。さらに製造業の分野では、先進的な検査として消耗部品の交換時期を予見する傾向管理も進展しています。このような新しい手法を採用した場合には、その変更がマネジメントシステムに反映されていることが求められます。

箇条8　運用

箇条8.1（運用の計画及び管理）では、製品・サービスの提供に関する要求事項を満たすことと箇条6.1（リスク及び機会への取組み）で決定した取り組みを実施するためのプロセスの計画、実施、管理を求めています。加えて、意図しない変更によって生じた結果をレビューし、必要に応じて有害な影響を軽減する処置をとることも求めています。審査では、意図しない変更によって生じた結果のレビューがなされているか、必要に応じて有害な影響を軽減する処置がとられているかを確認します。

箇条8.2（製品及びサービスに関する要求事項）では、顧客の要求事項を確認するコミュニケーションの手段が、従来のフェイス・トゥー・フェイスから情報機器を介したテレワーキングになってきていますので、顧客の要求を的確に把握できるよう注意が必要です。

箇条8.3（製品及びサービスの設計・開発）では、製品・サービスの設計・開発の計画や管理、変更について述べています。このうち、特に製品・サービスの設計・開発の変更について、例えば製造業において、製品に使用する素材を海外から輸入していたところ、コロナ禍により供給が遮断されたというケースがあります。この場合、代わりとなる素材を調達するために、供給元の再選定を迅速に行い、製品に使用する素材を変更しなければなりません。また、供給元の再選定にかかる時間を考慮すると、製品の信頼性評価に要する期間を短縮する必要があるかもしれません。審査では、短期間で製品・サービスの設計・開発に関する変更が実施された場合でも、その変更に伴うリスクを評価し、適切な処置を施しているかを確認します。

箇条8.4（外部から提供されているプロセス、製品及びサービスの管理）では、仕入れ先や供給元の変更点について注目します。例えば、これまで年1回は現地に赴き監査していたものができなくなるなどの状況が生まれています。現地で確認できない以上、供給元の検査工程がどう決められたのか、その手法はどうなっているのかといった品質保証の仕組みをリモートで確認し評価する仕組みを形成することが必要です。

箇条8.5（製造及びサービス提供）では、製造とサービスの提供現場での変更管理について注目します。変更の例としては、製造業において検査工程の人数を減らす一方で、検査工程に従事する一人あたりを多能工化するといったケースが想定されます。審査では、このような変更が箇条8.5.6（変更の管理）に基づき、きちんと管理されているかを確認します。

箇条9　パフォーマンス評価

箇条9.1（監視、測定、分析及び評価）では、コロナ禍での変化の対応や方針、目標に対する活動について注目します。以前から、製造業における傾向管理などの手法により、品質保証に関する問題が起きてからではなく、問題が発生する前にデータから傾向を分析して、必要な設備を調整するなど、問題の予防に力を入れる企業が増えています。こうした取り組みがコロナ禍で大きく促進され、予防に関わる人材の育成や、教育システムの変更などにもつながっています。今後もこのような取り組みをする企業が増えてほしいと考えます。

箇条9.2（内部監査）については、より詳細な情報をカバーするために、下記のコラムで解説します。

箇条9.3（マネジメントレビュー）では、マネジメントシステムが企業の目的や製品およびサービスにとってふさわしいものであること、プロセスや製品およびサービス品質の主要な側面をすべてカバーしていること、品質目標をはじめとしたマネジメントシステムの計画が達成されていることを確実にするために、トップマネジメントは、あらかじめ定められた間隔でマネジメントレビューを実施することが求められます。今年は、特にコロナ禍の影響により、企業のマネジメントシステムに影響を及ぼす外部・内部の課題に変化が生じやすいため、この変化に伴うマネジメントシステムのあらゆる変更の必要性について評価されているかを審査では確認します。

箇条10　改善

箇条10（改善）では、顧客満足を向上させるために、取り組む3つの主要な改善対象を示しています。3つの主要な対象とは、不適合を防止するためのプロセス、既知および予想されている要求事項を満たすための製品およびサービス、そして品質マネジメントシステムです。コロナ禍で、顧客や取引先が変わったもの、新たな製品やサービスを展開しているもの、生産体制が変わったものなどがあります。箇条9（パフォーマンス評価）で、パフォーマンスを監視・測定・分析・評価されていますので、是正処置、継続的改善につなげられている企業こそが、ISOを活用された組織的に強い力を持ったマネジメントシステムとなります。審査では、その継続的改善の組織力の力強さを見たいと考えています。 ■

Column

ISO 9001内部監査のポイント

コロナ禍では内部監査も大きく様相が変わってきています。実際に現場を見て監査するこれまでのやり方ができなくなった場合に、どのように考え、アプローチしていけばいいか、浮き彫りにしてみたいと思います。

事業所間の移動が制限される企業では、テレワーキングの仕組みを活用して、リモート監査に変えることは差し支えありませんので、業務も変わっているという観点からも、内部監査は必ず実行してください。

従来の対面方式の内部監査では、規格の箇条順でチェックするスタイルが中心だったと思いますが、そのやり方では時間もかかり、現場を見ないと難しい。ポイントを絞って効率よく目的を達しているか確認する方法を、工夫して見つけていくことが大切です。

例えば製造業では、今年「この工程で不良が出た」「こういう市場クレームが出た」「製品実現の工程順序やプロセス順序を変えた」といった事柄をサンプリングしながら、設計や製造で目的が達成できているかを確認する内部監査のスタイルが多く見られます。

このように内部監査を行うとしても、重要なプロセスは時間をかけてしっかり見ていく必要があります。リモート会議や電話等で構いませんので、必ず当事者とのインタビューは行ってください。仕事のやり方に無駄がないか、品質方針や目標が現場に浸透しているかなどは、インタビューを通じて把握することができます。こうして情報をきちんと集めた上で、マネジメントシステムが確実に履行されているか、何か変えるべきところはないのかなどを内部監査のアウトプットとすることが大切です。

内部監査は会社のマネジメントシステムのチェック機能という位置付けです。会社の内部で変更のあったところは、社内だからこそよくわかることがあると思います。今年はコロナ禍の影響で、特に企業のマネジメントシステムに影響を及ぼす外部・内部の課題や利害関係者のニーズ・期待に変化が生じやすく、そうした変化に伴う課題や改善点をうまく抽出してほしいと考えます。

内部監査に完璧を求めすぎても、体制上の制約などで難しい場合もあります。JQAの審査が内部監査の延長線上に位置し、マネジメントシステム上で変化のあった部分を相互チェックするかたちが望ましいと思います。内部監査は審査と一体化するものと考え、わからないことがあればJQAへ相談してください。

■ 参考　ISO 9001:2015の構成

特集 第二部

新型コロナウイルスの感染症拡大を踏まえて、改めてISO 14001を考える

新型コロナウイルス感染症の拡大が多くの企業に深刻な打撃をもたらすなか、この変化をチャンスと捉えている企業も見受けられる。ここでは、新型コロナウイルス感染症の流行下におけるISO 14001審査の3つの視点を紹介するとともに、環境マネジメントシステムを活用することで企業の持続的な成長につなげるためのヒントや、リモートでの取り組みが進められている内部監査における留意点などについて、審査事業センター 環境審査部 部長の山田 衛に聞いた。

審査事業センター
環境審査部 部長
山田 衛

新型コロナウイルスの感染症拡大を踏まえて、ISO 14001審査で注目する点

時代の変化がトップマネジメントの認識を変えた

コロナ禍によって、世界は大きく変化しました。日本政府は脱炭素社会やサーキュラーエコノミーへの移行を加速し、環境と経済の好循環を加速するための取り組みの強化を明らかにしています。

ビジネスの現場に生じた大きな変化の一つとして、在宅勤務などの働き方改革が進展し、オフィスや工場で働く人が少なくなったことがあげられます。これにより各拠点（サイト）での環境負荷は低減する一方、テレワーキングの現場となる従業員の家庭におけるエネルギー使用量や廃棄物の排出は増大しています。人々の価値観や行動様式が変化するなかで、自動化、IoT、タッチレスなどをキーワードにした新たなビジネスの機会も生まれています。ISO 14001審査のトップインタビューを通じて、ニューノーマルに向かう変化を、環境の視点で捉えることで成長につなげようとしている経営者が多いと実感しています。

コロナ禍を受けてJQAが審査で注目する点

企業のトップの多くは、サプライチェーンと現場の仕事の変化が大きいと捉えています。例えば、あるオフィス機器メーカーでは、取引先のオフィスから人がいなくなることでビジネス機会が減少しました。仕事の現場においても、工場の生産量の減少や、感染症拡大防止に向けてテレワーキングが進行することにより、各サイトの現場でマネジメントシステムを運用する人の数が減少しています。JQAでは、企業が取り組むべき課題や方向性の発見に貢献すべく、コロナ禍における審査の重点ポイントとして「①変化への対応」「②方針・目標に対する活動」「③コミュニケーション」の3つの視点を取り入れています。

重点ポイント①「変化への対応」

変化を成長につなげるには、変化によるマイナスの影響をいち早く発見し、予防するための処置を実施することが重要です。テレワーキングが進行するなか、工場などで法令違反などを起こさないためには、限定された要員でマネジメントシステムを効果的に維持する必要があります。マネジメントシステムの適切な運用に対して、審査では稼働中の設備だけでなく稼働を停止している設備のメンテナンスや点検をどのように行っているか、廃棄物処理のアウトソーシング先などが稼働停止している場合の工場内における廃棄物保管状況、行政への報告状況など、変化に対してどのように対応しているかについて検証します。

重点ポイント②「方針・目標に対する活動」

コロナ禍における企業の外部・内部の変化に対応するには、方針や目標の妥当性に対する評価を行う必要があります。オフィスへの出勤率や工場の稼働率が低減すれば、電気の使用量も少なくなり、CO_2排出量の削減目標を容易に達成することが可能となります。こういった状況においては、目標そのものの妥当性についてレビューするとともに、新たな目標を策定する必要性についても検討することが求められます。外部・内部の状況の変化に応じた適正な目標の設定は、環境マネジメントシステムの実効性を高めるための活動の活性化につながることが期待できます。

コロナ禍では、商談のリモート化により車の使用を減らすことや、イベントのバーチャル化を推進するといった環境パフォーマンスに直接的に寄与する目標を設定することが可能です。また、環境マネジメントシステムの適用範囲を拡大することによって、活動を活性化することも期待できます。例えば、電力使用量に起因するCO_2排出量は、前述のように各サイトでは減少しても、テレワーキングを行う従業員の家庭などでは増加します。こういった状況を受け、より積極的なCO_2排出量削減につなげていくには、工場などのサイトから直接排出するCO_2（スコープ1）、電力使用に伴って発電所などから間接的に排出されるCO_2（スコープ2）に加え、サプライチェーン全体のCO_2（スコープ3）を適用範囲にすることも一つの方法です。スコープ3は、サプライヤーの材料製造に伴う環境負荷や、省エネ製品などによる社会全体の環境負荷低減効果も適用範囲としており、この考え方を従業員の家庭における環境負荷に拡大することで、新たな目標や取り組みの方向性が見えてくる可能性もあります。（右注記参照）

SDGs（持続可能な開発目標）を、環境マネジメントシステムのPDCAサイクルに取り込むことも有効と考えます。省エネ製品による気候変動への対応やリサイクル製品によるサーキュラーエコノミーへの貢献を方針や目標として策定し、製品やサービスの開発・普及に取り組むことを成長のためのチャンスと捉えている企業も少なくありません。これら国際的な基準や目標をどのように考慮して活動に展開しているかについても、審査で検証します。

重点ポイント③「コミュニケーション」

審査を通じて、多くの企業がコミュニケーションを課題としていると実感しています。従来はフェイス・トゥー・フェイスで行っていた業務上のコミュニケーションと同様の効果を、リモート環境においても実現する必要があるためです。すべての従業員にテレワーキング用のパソコンを貸与するなど、全社的なデジタル化に踏み切る企業も増えています。また、これまでは社内の現場やサプライヤーに出向いて行っていた監査などを、リモートで行うための仕組みづくりなども重要になっています。

次のページではコロナ禍でのISO 14001審査のポイントを要求事項に沿って説明します。

注記

温室効果ガス（GHG）排出量と報告に関する国際的な基準「温室効果ガス（GHG）プロトコル～事業者の排出量算定及び報告に関する標準～」にて、企業活動の上流（原料の製造など）から下流（製品の販売など）までの全体を通し、自社の直接排出量（自社の工場・オフィス・車両など）（スコープ1）、エネルギー起源の間接排出量（電力など自社で消費したエネルギー）（スコープ2）、その他の間接排出量（その他のサプライチェーン全体の排出量）（スコープ3）の3つのスコープに分け、それぞれの排出量算定を求めている。

コロナ禍のISO 14001審査

箇条4　組織の状況

コロナ禍の緊急事態では、取締役会などにおいて「外部・内部の課題」「利害関係者のニーズ及び期待」に関する変化およびその対応についての議論が行われているはずです。その結果がマネジメントシステムに適切に反映されているかどうかを審査では注目しています。課題評価をタイムリーに行い、マネジメントシステムに反映することで、事業プロセスとマネジメントシステムの統合につながることが期待できます。

箇条5　リーダーシップ

新型コロナウイルスの影響で企業の外部・内部の状況が一変し、これまでの価値観や既成概念が崩れた感があります。箇条5（リーダーシップ）に関する審査では、前述の「重点ポイント①『変化への対応』」に関連して、企業の外部・内部の課題をどのように取り込み、経営的判断をしているかについて確認するとともに、社内外への対応についてリーダーシップをどのように発揮しているかを検証します。また、先行きが不透明な状況で、設備投資や人材育成に対する考え方や、将来のビジネスプランと持続可能性との関連についても確認します。

箇条6　計画

変化をチャンスに変えていくには、従来の延長線上で環境負荷低減を図るだけでなく、リスクと機会という視点に立ち返り、マネジメントシステム自体の見直しを図ることが重要です。テレワーキングの拡大によって電力使用量の削減目標を達成したことを成果として捉えるのではなく、定期的なレビューのタイミングを見直すことで新たな目標を設定し、新たな働き方の推進に着手することも、活動の活性化につながると考えます。審査では、コロナ禍における外部・内部の変化をリスクおよび機会としてどのように反映し、取り組みにつなげているかについて確認します。

箇条7　支援

新型コロナウイルスの感染症拡大予防といった直接的な対応だけでなく、コロナ禍による影響と気象災害などを関連づけながら検証し、リスクに対応するための仕組みづくりを行うことは、環境マネジメントシステムのみならず、事業継続計画(BCP)としても重要です。例えば、ある企業でこれまでは大雨などによる設備の異常事態に即応できるよう、そのための力量を持つ専任者が毎日出勤していたが、テレワーキングの拡大により週1回の出勤になったとします。この企業で異常事態発生の可能性があれば、専任者の出勤日を待つのではなく電話やネットで対応するための仕組みを構築するといったことがリスク発生の予防につながります。従来は専任者が目視で検査していたことをセンサーによる監視に変更するなど属人的な要素を排除すること、さらに休業期間中や夜間の対応について検証することも安全の担保になります。審査では、これら仕組みづくりに伴い、箇条7（支援）に生じた変更を計画、管理しているかを確認します。

箇条8　運用

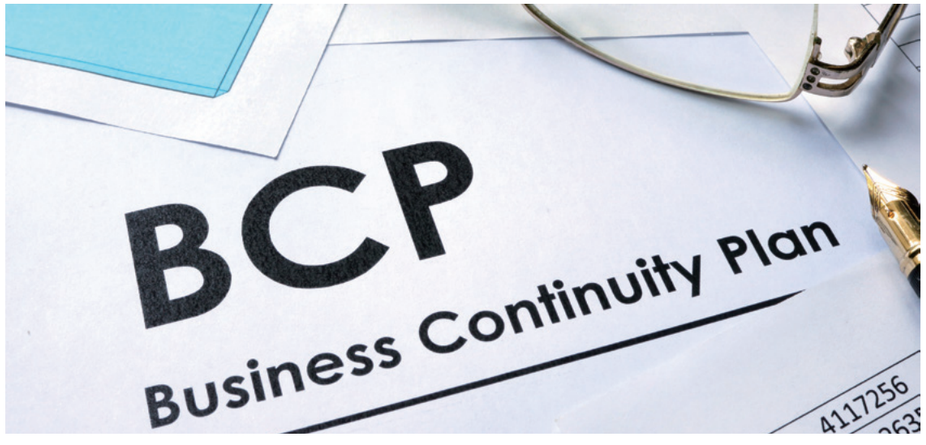
新型コロナウイルスの影響により、人員の減少や仕事の内容が変化するなかで、従来の運用ルールが有効に機能しているか、ルールそのものの見直しを図っていく必要もあります。EMS委員会の開催頻度が少なくなっているケースや、リモートで開催される場合もあると考えられます。審査では、状況の変化に対して、運用ルールが適切に変更され、実効性が伴っているかについて確認します。

箇条9　パフォーマンス評価

監視・測定においては、意図した成果を達成するために監視測定の対象を決定し、その結果に応じて環境パフォーマンスを継続的に改善するための処置につなげることが求められています。コロナ禍において環境目標の見直しを行った場合は、求められるパフォーマンスレベルも変化している可能性があり、審査では目標と監視・測定ポイントの整合性やタイミングの適切性を確認します。

箇条10　改善

改善は、企業の意図した成果や環境方針・目標を達成するために、環境マネジメントシステムの課題や改善すべき点を特定し、必要な取り組みを推進することが求められています。コロナ禍における先行きが不透明な状況のなか、企業が持続的に成長するために、環境マネジメントシステムをどのように活用しているか。具体的には、企業の外部・内部の課題決定プロセスからリスクと機会への取り組みに対する目標管理や監視測定、内部監査、並びにマネジメントレビューといった一連のPDCAを効果的に回すことによって、企業の環境パフォーマンス向上や継続的改善がどのように実現されているかについて確認します。■



Column

ISO 14001内部監査のポイント

コロナ禍で、内部監査をリモートで実施する企業が増えています。しかし、例えば製造業では騒音や異臭などのサイト特有の環境状況をリモートで確認することが困難な項目もあり、これまで現場で確認していた内容をいかにリモートで効果的に確認するかが課題であり、検討が必要です。

JQAの審査では、リモートによる内部監査が、これまでの現場訪問による監査と同様に適正に行われているのかを重視します。企業にとって内部監査のポイントは、現場のオペレーション状況の確認と、業務の効率化や汚染の予防などの環境負荷の低下につなげるための情報を収集することにあります。経営者が適切な判断を行うためのリモート内部監査はどうあるべきか。今後は、それぞれの企業がJQAの審査を有効に活用し、自社の内部監査の方法を検証して改善に向けた活動を推進することが重要となります。

■ 参考　ISO 14001:2015の構成

特集　第三部

新型コロナウイルスの感染症拡大を踏まえて、改めてISO/IEC 27001を考える

新型コロナウイルス感染症の流行により、企業の状況や利害関係者のニーズなどに変化が生じている。情報セキュリティ分野においては、テレワーキングの新規導入や、従来はテレワーキングの対象外だった従業員への導入拡大が、最も影響が大きいところといえるだろう。コロナ禍での情報セキュリティマネジメントシステムの審査のポイントについて、審査事業センター 情報審査部 部長の宮下 卓士に聞いた。

審査事業センター
情報審査部 部長
宮下 卓士

審査で注目するポイント

箇条4　組織の状況

東京では、オリンピック時の出勤抑制を意識して、テレワーキングの導入・準備をしていた企業もあり、テレワーキングに対応したマネジメントシステムの構築をすでに進めていましたが、これまでテレワーキングに未対応であった企業や業務においても、急遽対応せざるを得なくなったことがコロナ禍での2020年度の特徴です。

◎審査の視点とチェックポイント

テレワーキングの導入等により業務プロセス自体が変化すれば、リスクも変化し、マネジメント対象も変わります。コロナ禍においてマネジメントシステムを変更した企業も多く、ISO/IEC 27001の審査に際しては、企業の状況を含め実情に応じてマネジメントシステムが変更され新たなリスクが定義されているか、リスクに対応する方策が確実に実施されているかどうかが、確認のポイントとなります。

それらの点は利害関係者が企業に期待するところであり、企業が外部変化に対応してリスク対策を講じていくことは、企業として利害関係者のニーズを監視している証左にもなります。

ただし、コロナ禍は突然起きたことであり、企業は細かいリスク分析をしてマニュアルの書き換えを行うより先に、目の前に起きている課題に対応しながらリスクをまとめテレワーキングの体制をつくるなど、事業継続の方策を実現化する必要がありました。そのため、リスク分析が不十分なところがあると考えられます。箇条4に限ったことではありませんが、一年近くが経過してテレワーキングの運用体制が多少落ち着いたところで当時構築したシステムを今一度見直し、リスクなどを整理し直すことが必要です。ISO/IEC 27001では、テレワーキングに伴う情報セキュリティの管理策について、取引先とデータをやりとりする場合なども含め、あらかじめ規定されています。テレワーキング導入に伴うマネジメントシステムの変更や、手順書に新規項目を追加する場合は、本規格を参照することで網羅的に管理できるようになっています。

なお、マニュアルの書き換えについては、早急に行ったかよりも、現状の手順の内容が全員に伝わっていることが重要です。テレワーキングを導入

し、順守されるべき規則を新規につくった場合、それがWebポータルなどに明示されて周知されているか、縦系列で漏れなく伝達されているかなどは、注意するポイントとなります。認識が共有され、ガバナンスが働いている状態であれば、文書への反映に多少のタイムラグがあっても大きな問題とはなりません。

箇条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

箇条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）では、適用範囲を定義するために、外部と内部の課題、利害関係者のニーズ、外部組織で実施する活動とのインターフェースと依存関係を考慮して、境界と適用可能性を決定することが規定されています。テレワーキングの導入により、ネットワークを含む情報システムに対して変化が発生していることが考えられます。

◎審査の視点とチェックポイント

テレワーキング等により企業の人員が会社外から企業の情報システムにアクセスする場合でも、企業の内部にいる人員が企業の情報システムにアクセスすることと同等にマネジメントされた状況にあると考えられる限りは、テレワーキングの実施場所に関する適用範囲を大きく変更する必要はないと考えます。

Web会議を使用する場合も、その仮想空間を企業の拠点として考えることができます。ただし、他社の提供するクラウド上のサーバや、各種のクラウドサービスなどを利用することを、適用範囲に含めて考慮しておく必要があります。

企業の情報システムに外部のネットワーク経由でアクセスする場合は、適用範囲を定義し直し、VPN、アクセス権の付与、各端末の認証、自宅の通信環境の確認等のセキュリティ対策を講じている必要があります。

登録活動範囲については、企業、業務内容、場所、論理的なネットワーク構成が現状に即した内容となっているかを確認します。

箇条5　リーダーシップ

コロナ禍でのテレワーキングの整備は、必ずトップマネジメントのコミットメントに基づいています。トップマネジメントがどのような過程で方針変更を決定し指示を出したか、情報セキュリティについても経営層の了解を得ているか、ということを確認します。

非常時であり、トップマネジメントの意思決定がWeb会議システム上などで行われたこともあると考えられます。審査においては、定型的なマネジメントレビューでなくとも、方針変更を決定した役員会、経営会議等がマネジメントレビューに当たると考えます。方針決定に至る時系列の流れについては、審査時に確認しています。

附属書A.6　情報セキュリティのための組織

コロナ禍においては、ISO/IEC 27001 の箇条6.1（リスク及び機会に対処する活動）や箇条6.1.2（情報セキュリティリスクアセスメント）、附属書A.6.2（モバイル機器及びテレワーキング）に関する部分が特に大きく変化しました。これまで附属書A.6.2（モバイル機器及びテレワーキング）を不採用だった企業も採用するようになっています。

附属書A.6.2（モバイル機器及びテレワーキング）はモバイル機器とテレワーキングに関するセキュリティを確実にする目的で定められたもので、在宅で勤務しテレワーキングの場所から会社のサーバなどの情報にアクセスして業務を行う場合に加え、社内のネットワークだけではなく外部のインターネットを経由して会社のネットワークに入る場合も扱っています。

附属書A.6.2.1（モバイル機器の方針）では、モバイル機器を用いることで生じるリスクを管理するために、方針およびその方針を支援するセキュリティ対策を採用することが推奨されています。この方針は附属書A.5.1.1（情報セキュリティのための方針群）に示された実施の手順を参考に策定します。

また、附属書A.6.2.2（テレワーキング）では、テレワーキングの場所でアクセス、処理、保存される情報を保護するために、方針およびその方針を支援するセキュリティ対策を実施することを求めています。

◎審査の視点とチェックポイント

自宅から会社のサーバなどの情報にアクセスして業務を行ったり、インターネットから会社のネットワークに入るケースが激増しています。テレワーキング導入に関しては、附属書A.6.2.1（モバイル機器の方針）に示されるとおり、モバイル機器の使用に伴うリスクに関する管理方針を立て、その方針に則ったセキュリティ対策が採用されているかに着目して審査します。

特に、会社から貸与された装置ではなく、個人のパソコンを使って会社のネットワークにアクセスする場合、個人のパソコンであっても会社のルールや機能を確実に履行することが求められます。これに関するモラル教育は、ISO/IEC 27001の箇条7（支援）、箇条7.2（力量）、箇条7.3（認識）、箇条7.4（コミュニケーション）を参照してください。

テレワーキングの場所でアクセス、処理、保存される情報の保護については、附属書A.6.2.2（テレワーキング）で示すように情報保護の方針を立て、その方針を実現するセキュリティ対策が実施されているかを確認します。また、在宅勤務をする上での操作マニュアルが整備されているかも確認します。

箇条9　パフォーマンス評価

箇条9.1（監視、測定、分析及び評価）では業務が滞りなく効率的に回る体制がとられていることを求めていますが、運用が変われば監視項目や測定方法も変更されます。例えば、テレワーキングが基本となった場合の出退勤管理やEラーニングについて、Webサイト上で報告・集計できるシステムを構築するなど、変化に応じた監視、測定、評価システムを整備することも必要になる場合があります。

機械的に測定できるものは良いのですが、テレワーキングの実施場所、作業中のPC画面や出力したドキュメントが第三者に見られない対策の実施状況などは、自己申告になる可能性が高くなり、確認が難しいためできる範囲での対応にならざるを得ないと考えます。

また、社内のネットワークに比べて自宅の通信環境は整備されておらず、サーバにアクセスする場合の応答率の悪化も見られました。インタビューでは、次に同様の事態が発生したときのために、どこまで、どのように投資をしてリスク対応をしていくのかを確認する場合があります。

内部監査も、開催時期の延長、Web会議での開催など、テレワーキングによりフェイス・トゥー・フェイスの実施が難しいこともあります。Web会議システムで実施する場合、電子化された記録の閲覧は容易ですが、紙での記録、現場の状況などは難しくなります。Webカメラを使って現場や紙記録を確認する、今回の重

点監査ポイントを確認可能な内容に限定する、など内部監査計画の見直しも必要となります。

箇条10　改善

今回、テレワーキングを導入された企業は、環境の変化が発生しています。企業に影響を及ぼすリスクや機会の変化の可能性もあり、新たなリスクや機会に対して対処することが必要となるでしょう。また、情報資産の洗い出し、情報セキュリティリスクアセスメント、情報セキュリティリスク対応も実施することが必要です。

箇条4（組織の状況）でも述べましたが、テレワーキングが導入されたことにより、適用された管理策の内容が適切なのか、確認して見直すことも必要です。

附属書A.11　物理的及び環境的セキュリティ

テレワーキングの実施にあたっては、会社のモバイル機器を自宅に持ち帰るケースも多く見られました。これについては附属書A.11.2.5（資産の移動）および附属書A.11.2.6（構外にある装置及び資産のセキュリティ）を参照します。

附属書A.11.2.5（資産の移動）では管理策として、装置や情報またはソフトウェアは事前の許可なしで構外に持ち出さないことが記されています。管理策の実施にあたっては、持ち出しを許可された従業員や外部利用者を特定すること、持ち出し期限を設定して返却が設定どおりであったかを検証すること、持ち出しと返却を記録すること、そして、資産を扱う者や利用する者については識別情報や役割、所属を文書化し、資産の返却時に文書も返却することを要求しています。

附属書A.11.2.6（構外にある装置及び資産のセキュリティ）では、構外にある資産の管理策として、構外での作業に伴った、構内での作業とは異なるリスクを考慮に入れてセキュリティを適用することが求められています。

◎審査の視点とチェックポイント

会社のモバイル端末を自宅で使用する場合には、附属書A.6（情報セキュリティのための組織）で規定している情報の保護に関するリスクや、附属書A.13（通信のセキュリティ）に記載のある外部ネットワークを使用することに伴うリスクに加え、紛失等のリスクについても考慮しておく必要があります。審査においては、これらの項目について従来は記載する必要がなかった企業も、必要に応じて本箇条を追加して資産に対するリスクの把握に努めているか、また、それらのリスクに対する対策を講じて、それを周知し実践しているかを確認します。

構外にある装置および資産には、会社から貸与しているIDカードも含まれます。毎日通勤している状況であれば、もし紛失してもすぐに気づくことができますが、長期間、自宅でのテレワーキングが続き、IDカードを使用する機会がないままであると、紛失しても気がつかず、対処が遅れる可能性があります。審査ではそういったリスクを想定し、常駐している契約先社員への貸与分も含め、IDカードの保管状況を定期的に確認するなど、紛失時に早期発見できる仕組みができているかにも着目します。

附属書A.12　運用のセキュリティ

情報処理設備の運用における管理目的と管理策を定める附属書A.12（運用のセキュリティ）では、操作手順書、変更管理、容量・能力の管理、開発環境・試験環境・運用環境の分離についての指針を示し、これらに則ってセキュリティを保った運用を行うことを求めています。

◎審査の視点とチェックポイント

社内においてはセキュリティと可用性を適切なバランスで保つことが可能ですが、テレワーキングで自宅から接続する場合には、当初規定していたとおりに運用できるとは限りません。在宅勤務が増え、セキュリティ強度を多少下げても可用性を優先した企業もあると思いますが、審査では、その際にセキュリティリスクアセスメントをどのように行い、トップマネジメントの許可を得て構築したのかというプロセスを確認します。

緊急事態宣言を受けてのセキュリティリスクアセスメントは、短時間での実施にならざるを得なかったと思われますが、運用から一年近くが経っていますので、妥当性はあるか、機密性に問題はないかなどを、再度確認してください。

また、在宅勤務中のセキュリティをどこまで要求するのかも考えるべき課題です。家族が同じ空間にいるとき、あるいはシェアオフィスなどを利用して業務を行う状況ではセキュリティ面への影響が大きく、自宅内に独立した空間を確保できない場合、どのようにセキュリティ対策を講じているかが重要です。

プリントアウトした書類の扱いについても同様です。本来は自宅での出力を不可能にするシステムが必要ですが、コストもかかります。やむを得ず出力した場合、シュレッダーで処理する、溶解処理するなど、従来の会社のルールの適用がどのようになされているかは確認すべき点だと考えています。

附属書A.13　通信のセキュリティ

附属書A.13.1.1（ネットワーク管理策）では、システムおよびアプリケーション内の情報を保護するためにネットワークの管理と制御を行うことを求めており、考慮すべきことの一つとして、公衆ネットワークまたは無線ネットワークを通過するデータの機密性・完全性や、

ネットワークを介して接続したシステムおよびアプリケーションを保護するために、特別な管理策を確立することを求めています。

◎審査の視点とチェックポイント

テレワーキングではWeb会議システムが頻繁に使われますが、公衆ネットワークまたは無線ネットワークを経由して会社のネットワークにアクセスする場合は、附属書A.13.1.1（ネットワーク管理策）に記されている内容を考慮する必要があります。ここでは公衆ネットワークまたは無線ネットワークを通過するデータの機密性・完全性や、ネットワークを介して接続したシステムおよびアプリケーションを保護するための特別な管理策を確立しているかが問われており、それらが適切に実施されているかが審査のポイントとなります。

また、細かい点ですが、例えば自宅でWi-Fiを使って無線LANに接続する場合、パソコンとルーター間の暗号化の機能が脆弱であると、第三者に見られてしまう危険性があります。そのような点も含め、ネットワーク管理策に変更があった場合、マネジメントシステムも実情に応じた変更をしているかどうかを確認します。

また、2020年4月の緊急事態宣言発出直後には、テレワーキングの増加の影響で通信会社の

ネットワーク負荷が高まり、通信スピードが著しく悪くなることがありました。また、マンションなどは、在宅勤務者が多くなり、共有の通信設備の負荷が高まったことで通信スピードの問題が発生したこともあります。この件に関しては、企業側で対応できることは限られていますが、可用性を確保するために、業務方法の変更（例:通信時間を減らす、データをまとめて夜間帯に取得しておく）などが必要と思われます。

附属書A.15　供給者関係

附属書A.15（供給者関係）では、外部のサプライヤーがアクセスできる企業の資産、情報を保護するために、サプライチェーンにおける情報セキュリティの管理目的および管理策を定め、サプライヤーと合意しておくことを求めています。

◎審査の視点とチェックポイント

テレワーキングを導入しているのはサプライヤー、協力会社も同様です。自社に関しては情報セキュリティマネジメントシステムを構築していても、協力会社の対策状況まで確認していない企業が多く、取引先調査でテレワーキングに関する調査項目を設けていない例も見受けられます。附属書A.15.1（供給者関係における情報セキュリティ）で求めているように、協力会社でテレワーキングを行っている場合は、協力会社の通信・運用のセキュリティ管理策についても確認し、リスクの状況に応じた対応をすることが必要です。

附属書A.17　事業継続マネジメントにおける情報セキュリティの側面

附属書A.17（事業継続マネジメントにおける情報セキュリティの側面）では、情報セキュリティ継続を企業の事業継続マネジメントシステムに組み込むことを求めています。コロナ禍においては、特に附属書A.17.1.1（情報セキュリティ継続の計画）および、附属書A.17.1.2（情報セキュリティ継続の実施）に関して、必要に応じた見直しに取り組んだ企業が多く見られます。

◎審査の視点とチェックポイント

事業継続を意図して緊急的にマネジメントシステムを変更した場合、情報セキュリティもそれに対応して変更されています。審査においては、変更の方針やプロセス、具体的な内容について明文化されていない場合でも、インタビューをして確認します。

附属書A.12（運用のセキュリティ）で述べたセキュリティと可用性の兼ね合いの問題も、事業継続という視点から、アクセシビリティの確保をどこまでのレベルとするかを検討しておく必要があります。

コロナ禍の審査方法

ISO/IEC 27001の場合、可能な限り現場審査を実施したいと考えています。

これは、入退管理装置のログ記録、その装置の利用者登録状況、日々の記録は現場でないと確認が難しいことや、現場で室内の状況など幅広く確認することで、大きなリスクとなり得るぜい弱な箇所の発見につながるためです。

その反面、審査の実施に際しては、企業の方々と審査員の接触を極力減らすことにより、罹患リスクを下げることが重要です。

接触を少なくするための取り組みとして、JQAでは、企業の希望に基づき、手書き記録や管理システムは現場で確認しつつ、それ以外の要員へのインタビューや電子記録の確認などはWeb会議システムを利用して行うことが可能です。

また、審査員が企業には一切訪問せず、Web会議システムのみで審査を実施することも可能です。ただし、この場合には、企業側にて現場をカメラで映していただくことや手書き記録などはその場で撮影いただくなどの対応が必要となります。

新型コロナウイルス感染症の収束に関して、先行き不透明な状況ではありますが、早期に通常どおりの現場審査を実施できることを願っています。

Column

ISO/IEC 27001内部監査のポイント

テレワーキングが常態化している企業では、内部監査や審査をリモートで行うケースも増えています。

内部監査で業務環境等の確認を行う場合、相手の自宅の状況を見ることはできないため、口頭で聞くしかありません。Web会議システムで実施する場合には、画面共有機能などを活用し、デスクトップのウイルス対策ソフトやWindowsのアップデート、アクセス権などのアクティブディレクトリを確認することは可能です。しかし、核となる画面構成はWeb会議システムでは提示しづらいため、出社してチェックする方がよい場合があります。

また、記録されている対策や成果は画面共有でも確認できますが、実際の業務の非効率な点などは記録ではなかなか把握できません。そのためリモート監査であっても、やはりインタビューが重要となります。

リモートでインタビューを行う場合、対面でのインタビューとは異なる視点が加わることで、従来以上に経営面の本質に迫る課題が洗い出される可能性もあります。情報機器についても、従来と異なる使い方がされるようになったことで、情報セキュリティに関わるインシデントにつながる情報が拾える場合もあります。

内部監査の結果はトップマネジメントに報告されるため、内部監査員が得た気づきは、改善の種になります。そういった気づきを通して、可用性と機密性のバランスを整えていくことが重要です。

■ 参考1　ISO/IEC 27001:2013の構成

- まえがき
- 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
- 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
- 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 不適合と是正処置
  - 10.2 継続的改善
- 附属書A（規定）管理目的及び管理策

■ 参考2　ISO/IEC 27001:2013 附属書A（規定）管理目的及び管理策の構成

- A5. 情報セキュリティのための方針群
  - A.5.1 情報セキュリティのための経営陣の方向性
    - A.5.1.1 情報セキュリティのための方針群
    - A.5.1.2 情報セキュリティのための方針群のレビュー
- A6. 情報セキュリティのための組織
  - A.6.1 内部組織
    - A.6.1.1 情報セキュリティの役割及び責任
    - A.6.1.2 職務の分離
    - A.6.1.3 関係当局との連絡
    - A.6.1.4 専門組織との連絡
    - 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
  - A.6.2 モバイル機器及びテレワーキング
    - A.6.2.1 モバイル機器の方針
    - A.6.2.2 テレワーキング
- A.7 人的資源のセキュリティ
  - A.7.1 雇用前
    - A.7.1.1 選考
    - A.7.1.2 雇用条件
  - A.7.2 雇用期間中
    - A.7.2.1 経営陣の責任
    - A.7.2.2 情報セキュリティの意識向上、教育及び訓練
    - A.7.2.3 懲戒手続
  - A.7.3 雇用の終了及び変更
    - A.7.3.1 雇用の終了又は変更に関する責任
- A.8 資産の管理
  - A.8.1 資産に対する責任
    - A.8.1.1 資産目録
    - A.8.1.2 資産の管理責任
    - A.8.1.3 資産利用の許容範囲
    - A.8.1.4 資産の返却
  - A.8.2 情報分類
    - A.8.2.1 情報の分類
    - A.8.2.2 情報のラベル付け
    - A.8.2.3 資産の取扱い
  - A.8.3 媒体の取扱い
    - A.8.3.1 取外し可能な媒体の管理
    - A.8.3.2 媒体の処分
    - A.8.3.3 物理的媒体の輸送
- A.9 アクセス制御
  - A9.1 アクセス制御に対する業務上の要求事項
    - A.9.1.1 アクセス制御方針
    - A.9.1.2 ネットワーク及びネットワークサービスへのアクセス
  - A.9.2 利用者アクセスの管理
    - A.9.2.1 利用者登録及び登録削除
    - A.9.2.2 利用者アクセスの提供
    - A.9.2.3 特権的アクセス権の管理
    - A.9.2.4 利用者の秘密認証情報の管理
    - A.9.2.5 利用者アクセス権のレビュー
    - A.9.2.6 アクセス権の削除又は修正
  - A.9.3 利用者の責任
    - A.9.3.1 秘密認証情報の利用
  - A.9.4 システム及びアプリケーションのアクセス制御
    - A.9.4.1 情報へのアクセス制限
    - A.9.4.2 セキュリティに配慮したログオン手順
    - A.9.4.3 パスワード管理システム
    - A.9.4.4 特権的なユーティリティプログラムの使用
    - A.9.4.5 プログラムソースコードへのアクセス制御
- A.10 暗号
  - A.10.1 暗号による管理策
    - A.10.1.1 暗号による管理策の利用方針
    - A.10.1.2 鍵管理
- A.11 物理的及び環境的セキュリティ
  - A.11.1 セキュリティを保つべき領域
    - A.11.1.1 物理的セキュリティ境界
    - A.11.1.2 物理的入退管理策
    - A.11.1.3 オフィス、部屋及び施設のセキュリティ
    - A.11.1.4 外部及び環境の脅威からの保護
    - A.11.1.5 セキュリティを保つべき領域での作業
    - A.11.1.6 受渡場所
  - A.11.2 装置
    - A.11.2.1 装置の設置及び保護
    - A.11.2.2 サポートユーティリティ
    - A.11.2.3 ケーブル配線のセキュリティ
    - A.11.2.4 装置の保守
    - A.11.2.5 資産の移動
    - A.11.2.6 構外にある装置及び資産のセキュリティ
    - A.11.2.7 装置のセキュリティを保った処分又は再利用
    - A.11.2.8 無人状態にある利用者装置
    - A.11.2.9 クリアデスク・クリアスクリーン方針
- A.12 運用のセキュリティ
  - A.12.1 運用の手順及び責任
    - A.12.1.1 操作手順書
    - A.12.1.2 変更管理
    - A.12.1.3 容量・能力の管理
    - A.12.1.4 開発環境、試験環境及び運用環境の分離
  - A.12.2 マルウェアからの保護
    - A.12.2.1 マルウェアに対する管理策
  - A.12.3 バックアップ
    - A.12.3.1 情報のバックアップ
  - A.12.4 ログ取得及び監視
    - A.12.4.1 イベントログ取得
    - A.12.4.2 ログ情報の保護
    - A.12.4.3 実務管理者及び運用担当者の作業ログ
    - A.12.4.4 クロックの同期
  - A.12.5 運用ソフトウェアの管理
    - A.12.5.1 運用システムに関わるソフトウェアの導入
  - A.12.6 技術的ぜい弱性管理
    - A.12.6.1 技術的ぜい弱性の管理
    - A.12.6.2 ソフトウェアのインストールの制限
  - A.12.7 情報システムの監査に対する考慮事項
    - A.12.7.1 情報システムの監査に対する管理策
- A.13 通信のセキュリティ
  - A.13.1 ネットワークセキュリティ管理
    - A.13.1.1 ネットワーク管理策
    - A.13.1.2 ネットワークサービスのセキュリティ
    - A.13.1.3 ネットワークの分離
  - A.13.2 情報の転送
    - A.13.2.1 情報転送の方針及び手順
    - A.13.2.2 情報転送に関する合意
    - A.13.2.3 電子的メッセージ通信
    - A.13.2.4 秘密保持契約又は守秘義務契約
- A.14 システムの取得、開発及び保守
  - A.14.1 情報システムのセキュリティ要求事項
    - A.14.1.1 情報セキュリティ要求事項の分析及び仕様化
    - A.14.1.2 公衆ネットワーク上のアプリケーションサービスのセキュリティ考慮
    - A.14.1.3 アプリケーションサービスのトランザクションの保護
  - A.14.2 開発及びサポートプロセスにおけるセキュリティ
    - A.14.2.1 セキュリティに配慮した開発のための方針
    - A.14.2.2 システムの変更管理手順
    - A.14.2.3 オペレーティングプラットフォーム変更後のアプリケーションの技術的レビュー
    - A.14.2.4 パッケージソフトウェアの変更に対する制限
    - A.14.2.5 セキュリティに配慮したシステム構築の原則
    - A.14.2.6 セキュリティに配慮した開発環境
    - A.14.2.7 外部委託による開発
    - A.14.2.8 システムセキュリティの試験
    - A.14.2.9 システムの受入れ試験
  - A.14.3 試験データ
    - A.14.3.1 試験データの保護
- A.15 供給者関係
  - A.15.1 供給者関係における情報セキュリティ
    - A.15.1.1 供給者関係のための情報セキュリティの方針
    - A.15.1.2 供給者との合意におけるセキュリティの取扱い
    - A.15.1.3 ICTサプライチェーン
  - A.15.2 供給者のサービス提供の管理
    - A.15.2.1 供給者のサービス提供の監視及びレビュー
    - A.15.2.2 供給者のサービス提供の変更に対する管理
- A.16 情報セキュリティインシデント管理
  - A.16.1 情報セキュリティインシデント管理及びその改善
    - A.16.1.1 責任及び手順
    - A.16.1.2 情報セキュリティ事象の報告
    - A.16.1.3 情報セキュリティ弱点の報告
    - A.16.1.4 情報セキュリティ事象の評価及び決定
    - A.16.1.5 情報セキュリティインシデントへの対応
    - A.16.1.6 情報セキュリティインシデントからの学習
    - A.16.1.7 証拠の収集
- A.17 事業継続マネジメントにおける情報セキュリティの側面
  - A.17.1 情報セキュリティ継続
    - A.17.1.1 情報セキュリティ継続の計画
    - A.17.1.2 情報セキュリティ継続の実施
    - A.17.1.3 情報セキュリティ継続の検証、レビュー及び評価
  - A.17.2 冗長性
    - A.17.2.1 情報処理施設の可用性
- A.18 順守
  - A.18.1 法令及び契約上の要求事項の順守
    - A.18.1.1 適用法令及び契約上の要求事項の特定
    - A.18.1.2 知的財産権
    - A.18.1.3 記録の保護
    - A.18.1.4 プライバシー及び個人を特定できる情報(PII)の保護
    - A.18.1.5 暗号化機能に対する規制
  - A.18.2 情報セキュリティのレビュー
    - A.18.2.1 情報セキュリティの独立したレビュー
    - A.18.2.2 情報セキュリティのための方針群及び標準の順守
    - A.18.2.3 技術的順守のレビュー

ひとつでも多くのご意見を、審査サービスの改善につなげます

審査後アンケートを通じて、受審組織の審査サービスに対するニーズを的確に捉え、さらなるサービスの改善を推進していきます

JQAでは2021年1月、審査後アンケートを刷新した。刷新の目的や内容について、品質推進室 室長の今井 礼介に聞いた。

品質推進室 室長
今井 礼介

JQAでは、受審組織のニーズを満たした審査サービスを提供するために、審査後アンケートを集計・分析し、サービス改善に役立てています。
これまでのアンケートを分析すると、JQAの審査サービスにおいても、サービス品質の6つの要素（正確性・迅速性・柔軟性・共感性・安心感・好印象）が受審組織の満足度に強く影響しているとわかりました。
より受審組織のニーズを満たした審査サービスを提供するには、このサービス品質の6つの要素を取り入れたアンケートの設計が必要であると考え、審査後アンケートを見直しました。

JQAの強みや課題を明らかにするアンケート設計

新しいアンケートは、シンプルに4つの設問で構成されています。「Q1. あなたは、今回のJQAの審査サービスを他社へどの程度おすすめしたいと思いますか?」「Q2.『おすすめ度:0-10点』の点数をつけるうえで、以下の項目はどのように影響しましたか。」という内容の2つの設問に加え、Q2.を補足する2つの自由回答に記入することでアンケートは完了します。

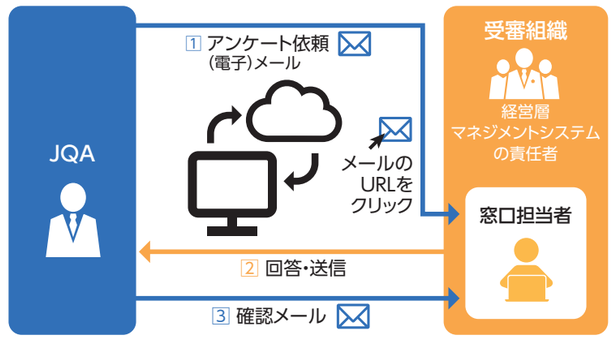
新しいアンケートは、受審組織の満足度とその満足度に影響した項目を紐づけることによって、JQAの強みや課題を明らかにする設計です。
例えば、Q1.で審査に対する満足度が高いと回答した受審組織が、続くQ2.の「2 審査計画など、対応の柔軟さ」「6 話のわかりやすさ」「8 審査員の経験・知識に基づく有用なコメント、貴社からの質問に対する的確な応答」などの項目がQ1.の満足度にプラスに作用したと回答した場合、それらはJQAの強みであり、強化していく事項と捉えることができます。逆にQ1.の満足度にマイナスに作用した項目は、JQAが改善すべきポイントであることがわかります。

■ 図1　審査後アンケートの回答画面

すべての受審組織からの回答を期待

審査後アンケートの回答数を多く収集することで、受審組織のニーズをより正確に分析できます。新しいアンケートでは、より多くの方に回答していただけるように、回答者の負担を極力小さくしました。回答想定時間は10分程度とボリュームを減らし、アンケートフォームへのアクセスもメールに記載したURLをクリックする方法に変更しています。審査後アンケートの流れは、図2のとおりです。

■ 図2　審査後アンケートの流れ



アンケートの分析結果に基づき審査サービスを改善

新しいアンケートは、審査サービスの改善に向けたPDCAサイクルを回すためのCに相当するものです。受審組織が期待する項目の抽出・検証のためのツールとして活用し、JQAの審査サービスの強化点・改善点を抽出し、満足度を高めていきます。JQAは、アンケートの分析結果に基づき、受審組織の意向を汲んだサービスの改善に引き続き取り組んでいきます。■