R70 古紙パルプ配合率70%再生紙を使用

VEGETABLE OIL INK

本誌は、印刷インキに「植物油インキ」を使用し、古紙パルプ配合率70%再生紙へ水なし印刷方式で印刷しています。水なし印刷方式は仕上がりが美しく、有害物質を含む排水を出しません。

Vol.30（通算67号）不定期刊　2019年3月発行
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　〒101-8555　東京都千代田区神田須田町1-25

JQA マネジメントシステム情報誌

2019 Vol.30

ISO NETWORK

特集Ⅰ

入門 労働安全衛生マネジメントシステム ISO 45001

第一部 安全で健康的な働き方の実現に向けて

第二部 いかにして効果的な労働安全衛生マネジメントシステムを構築するか



特集Ⅱ

いまから取り組む製造業の情報セキュリティマネジメント

第一部 まずは身の丈にあったシステムから

第二部 JQAと始める情報セキュリティマネジメントの第一歩

一般財団法人 日本品質保証機構

JQA マネジメントシステム情報誌
ISO NETWORK
2019 Vol.30

Contents

当誌に関するご意見・お問い合わせ先
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　ISO NETWORK編集部
東京都千代田区神田須田町1-25　JR神田万世橋ビル17階　〒101-8555

特集Ⅰ 入門 労働安全衛生マネジメントシステム ISO 45001

第一部　安全で健康的な働き方の実現に向けて

発行から約1年、注目が高まるISO 45001

働き方改革、ダイバーシティの推進、グローバル化など、社会環境の変化を成長につなげることを目的に、安全で健康的な職場環境づくりに注力する組織が増えています。このような動きが顕著になるなか、労働安全衛生マネジメントシステム（OHSMS:Occupational Health and Safety Management System）に関する初のISOマネジメントシステム規格として2018年、ISO 45001が発行されました。この特集記事では、ISO 45001に基づき効果的な労働安全衛生マネジメントシステムを構築・運用するためのポイントを、ISO 45001の要点である「リスク及び機会」を中心に解説します。

審査事業センター
環境審査部
労働安全衛生審査グループ
グループ長
松倉 宏行

審査事業センター
環境審査部
労働安全衛生審査グループ
齊藤 俊彦

審査事業センター
環境審査部
労働安全衛生審査グループ
志村 吉彦

ISO 45001は、組織が社会の変化に対応するための国際規格

企業経営者の意識が変化している

2018年3月にISO 45001が発行されて以来、多くのお客さまよりお問い合わせをいただいています。お客さまが新たにISO 45001を取り入れようというケースは大きく2つに分けられます。一つは、トップマネジメントが労働安全衛生活動のマンネリ化・形骸化に対して危機感を抱いており、このままでは事故が起きかねない、もしくはすでに事故が起きていることから、活動に喝を入れるためにISO 45001を活用しようと考えているケースです。もう一つは、これまでも労働安全衛生活動を行っていたが、ISO 45001の発行を機会に労働安全衛生のPDCAサイクルを回し、企業体質の変革につなげていこうと考えているケースです。

通常、組織がISO認証を取得する理由として「認証取得を企業のアピールポイントとして活用する」ことが多くあげられますが、前述した2つのようなケースを受けてISO 45001に取り組もうとしている組織が増えてきているのは、企業経営者の労働安全衛生への意識が変化している証拠ではないかと考えます。

社会の大きな変化が企業評価の基準も変えた

企業経営者の労働安全衛生への意識が変化している背景には、社会の大きな変化があります。2015年の国連サミットでは、2030年までの国際目標として持続可能な開発目標（SDGs:Sustainable Development Goals）が採択されました。SDGsは17の目標を掲げており、「すべての人に健康と福祉を」「ジェンダー平等を実現しよう」「働きがいも経済成長も」といった、働き方改革やダイバーシティの推進などと関連の深い目標が含まれています。企業がSDGsに紐づいた取り組みを強化する一方で、企業の環境（Environment）・社会（Society）・ガバナンス

■ 図1　ISO 45001：2018の構成

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 働く人及びその他の利害関係者のニーズ及び期待の理解
　4.3 労働安全衛生マネジメントシステムの適用範囲の決定
　4.4 労働安全衛生マネジメントシステム
5 リーダーシップ及び働く人の参加
　5.1 リーダーシップ及びコミットメント
　5.2 労働安全衛生方針
　5.3 組織の役割、責任及び権限
　5.4 働く人の協議及び参加
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 危険源の特定並びにリスク及び機会の評価
　　6.1.3 法的要求事項及びその他の要求事項の決定
　　6.1.4 取組みの計画策定
　6.2 労働安全衛生目標及びそれを達成するための計画策定
　　6.2.1 労働安全衛生目標
　　6.2.2 労働安全衛生目標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
　　7.4.1 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
　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
　　8.1.1 一般
　　8.1.2 危険源の除去及び労働安全衛生リスクの低減
　　8.1.3 変更の管理
　　8.1.4 調達
　8.2 緊急事態への準備及び対応
9 パフォーマンス評価
　9.1 モニタリング、測定、分析及びパフォーマンス評価
　　9.1.1 一般
　　9.1.2 順守評価
　9.2 内部監査
　　9.2.1 一般
　　9.2.2 内部監査プログラム
　9.3 マネジメントレビュー
10 改善
　10.1 一般
　10.2 インシデント、不適合及び是正処置
　10.3 継続的改善

（Governance）への取り組みを評価し、長期的視点で投資先を選定するESG投資も拡大しています。従来、企業の価値は、売上高や総資産といった経済的側面を中心に評価されていましたが、社会が変化したことで評価基準も様変わりしたのです。

労働安全衛生にもある「日本の常識は世界の非常識」

社会の大きな変化として、SDGsのほかにグローバル化があげられます。今後は外国人労働者の受け入れが拡大すると考えられます。また、事業拡大のために海外進出する企業も増えていきます。これまでの日本の労働安全衛生は特殊な文化のなかで発展してきたものであり、グローバル化を推進するには、多様な人々が働くことを前提とした国際標準に基づく労働安全衛生の仕組みの構築が必要です。

労働安全衛生における日本と世界の違いは、「誰が安全を守るのか」という考え方に如実に表れています。日本では、「自分の身は自分で守る」という考え方が基本です。例えば日本の伝統的な活動の一つである危険予知（KY）は、実際に起きた事故の経験に基づき、危険が潜んでいる作業などを予想し、事故を未然に防ぐよう行動するという活動です。つまり、自分自身の行動が基本になることから、日本では「身を守ることができるように教えますから、自分の身は自分で守りましょう」という教育をしています。

一方、世界標準となっているリスクアセスメントにおいては、リスクを低減する主体は個人ではなく組織です。そのため、「組織が身を守ってあげますから、ルールに則った行動をしてください」という教育が行われます。現在は日本においても厚生労働省の指針の下、リスクアセスメントの取り組みが進められていますが、文化の違いを認識した上で労働安全衛生の仕組みを構築しておかなくては、グローバル化を推進することは困難です。

企業が社会的責任を果たしていくには、取り組みを推進する人材の確保やバリューチェーンの管理が重要な課題です。人手不足が深刻化するなかで必要な人材を確保し、会社を存続・発展させていくには、働きやすい職場づくりは大前提です。ISO 45001は、組織自らが安全で健康的な職場を実現するための規格であり、また、外部委託先の管理を要求するなど、社会の変化を取り入れた規格です。

リスクアセスメントが労働安全衛生を強化する

ISO 45001は箇条7.2（力量）の項目で、「危険源を特定する能力を含めた力量を備えていることを確実にする」ことを求めていることから、負傷や疾病を引き起こす潜在的な危険源を把握できる力量を備えた人材の育成が必要です。そのためには、KYやヒヤリハットという労働安全衛生活動が馴染んでいる現場に、リスクアセスメントの考え方を導入することが重要になります。

KYやヒヤリハットとリスクアセスメントはアプローチが異なります。KYは実際に起きた事故から危険を予知する活動であり、ヒヤリハットは自分自身が危険を感じた経験がもとになっていることから、これらは後追いの活動（再発防止）であると言えます。一方、リスクアセスメントは、事故を起こすポテンシャルを持っている回転体、熱源、電圧などの危険源に対して、それらが普段人間が足を踏み入れない場所に存在していても、全てを洗い出すことが原点です。その上で人間の作業と接点があるかどうかを評価し、人間が触ると死亡する可能性があるもの、触ったとしても影響の少ないものといった重篤性を見積もり、洗い出したリスクは許容可能か否かを評価します。

リスクアセスメントは、これまでに事故が起きた・起きなかったではなく、危ないものがあるか・ないかを起点とする事故防止（予防）の考え方であり、これを導入することは、日本の労働安全衛生の強化につながると考えられます。

効果的な労働安全衛生マネジメントシステムの構築と運用に向けて

労働安全衛生マネジメントシステム構築のポイントは3つ

ISO 45001に基づく労働安全衛生マネジメントシステムは、現状の業務活動を通じて安全で健康的な働き方を実現するための取り組みです。そのため、構築の際には、①トップマネジメントのコミットメント、②全体がわかっている人と現場の仕事がわかっている人がチームを組む、③新たなことに取り組むという意識を持たない、つまり認証取得のみを目的とした取り組みを行わないことが重要です。

具体的には、トップマネジメントのコミットメントとして、組織の事業プロセスへのISO 45001の要求事項の統合を確実にします。また、部課長や安全衛生委員会のメンバーなど組織全体の業務活動がわかっている人は、実際に現場で働いている人とチームを組み、既存の業務活動がISO 45001のどの要求事項に対応するか、少し手を加えれば要求事項に適合する活動はないか、そして形骸化している活動があれば、それをなくすことはできないかという検討をします。

新たなことに取り組むという意識ではなく、トップマネジメント指揮の下、現状の業務活動の見直しをすることで、実際の業務活動とかけ離れたマネジメントシステムが構築されることを防止します。

■ 図2　労働安全衛生マネジメントシステム構築の3つのポイント

①トップマネジメントのコミットメント

②全体がわかっている人と現場の仕事がわかっている人がチームを組むこと

③新たなことに取り組むという意識を持たない、認証取得のみを目的と考えないこと

労働安全衛生マネジメントシステムの立ち上げには、現状の見直し作業はもちろんのこと、事務局を担当する方や安全衛生委員会のメンバーなどは、あらかじめISO 45001について学習しておく必要があり、マンパワーが必要です。

しかし一旦、仕組みが構築されると、その後のマネジメントシステムの運用は安全衛生委員会のルーティンワークの範囲に入りますので、従来のマンパワーで回していけるようになると考えます。ISO 45001がシステム運用段階において要求している人材は多くはありません。「労働安全衛生マネジメントシステムが規格の要求事項に適合することを確実にする」「労働安全衛生マネジメントシステムのパフォーマンスをトップに報告する」という2つの仕事の担当者を任命することを要求しているだけです。これを裏返すと、お目付役と情報を収集してトップへ報告する役割を担う事務局は必要であるものの、活動を逐一サポートする必要があるシステムを構築するのではなく、マンパワーをかけずに回せるシステムの構築が可能であることを示唆しています。

戦略的視点で組織の「リスクと機会」を決定

労働安全衛生マネジメントシステムを通じて、働く人の負傷と疾病を防止し、安全で健康的な職場の提供を実現するためには、事前に想定し得るリスクなどに対して、あらかじめ対応策を講じることが重要です。

ISO 45001では、箇条6（計画）にてリスクと機会への取り組みを要求しており、2つの特徴があります。

第一の特徴は、組織の置かれた状況に応じて、戦略的視点で取り組むべき「リスク及び機会」(箇条6.1 リスク及び機会への取組み)を組織が主体的に決定し、PDCAサイクルを回す仕組みの構築を要求している点です。

戦略的視点での対応については、①組織内の課題、組織外の課題を洗い出し、組織の事業上の課題を決定すること、②働く人と利害関係者からの要求事項に対し、対応が必要なものを決定することが求められます。このプロセスは、ステークホルダーとの対話を通じて重要な取り組み（マテリアリティ）を特定している企業には親和性の高いものであり、働き方改革やダイバーシティの推進は、戦略的視点での対応に該当すると考えられます。

第二の特徴は、2015年版ISO 9001、ISO 14001と大きく異なり、リスクと機会が4つに細分化された点にあります。具体的には、「労働安全衛生リスク」「労働安全衛生マネジメントシステムに対するその他のリスク」（箇条6.1.2.2）、「労働安全衛生機会」「労働安全衛生マネジメントシステムに対するその他の機会」（箇条6.1.2.3）に分けられました。

このうち、労働安全衛生リスクと労働安全衛生マネジメントシステムに対するその他のリスクの違いについては、人体へのリスクが労働安全衛生リスク、ベテラン事務局員の退職のような経営上のリスクが労働安全衛生マネジメントシステムに対するその他のリスクと捉えるとわかりやすいと思います。

具体的に、リスクと機会の決定および取り組みの計画策定は、次の手順で策定します。

①「組織内外の課題」「働く人と利害関係者の要求事項」および「労働安全衛生マネジメントシステムの適用範囲」をもとに、組織の置かれた状況に対応した4つリスクと機会を決定します。

②労働安全衛生リスクについては、リスクアセスメント手法を用いて評価します。一方で、労働安全衛生マネジメントシステムに対するその他のリスクは、リスクアセスメント手法を用いる必要はなく、抽出したその他のリスクについて、重要度や優先度に基づいて取り組むか、取り組まないかを評価します。

③労働安全衛生機会と労働安全衛生マネジメントシステムに対するその他の機会については、労働安全衛生パフォーマンス向上の可能性や期待できる恩恵などに基づいて取り組むか、取り組まないかを評価します。

④組織が取り組むべきと決定したリスクと機会に対して、実際の業務活動のなかでの取り組み方法と取り組んだ結果の有効性を評価する方法を計画します。

リスクと機会の決定、およびその取り組みの計画の策定には、組織の置かれた状況に応じて、戦略的な視点で自分たちの組織におけるリスクと機会は何か、決定したリスクと機会にどう取り組むかを考える必要があります。これにより、働く人の負傷と疾病を防止し、安全で健康的な職場の提供を実現するために、優先的に対応すべきリスクと機会を特定できるため、注力すべき活動とそれ以外の活動が明確になります。

「機会」を見逃さず上手にお金を使う

ISO 45001に関するご質問で最も多いのは、「リスク及び機会における機会とは何ですか」というものです。これまでの労働安全衛生には、「機会」という概念がなかったためです。まず、労働安全衛生機会について、ISO 45001では組織、組織の方針、プロセスまたは組織の活動の計画的変更を考慮に入れた、労働安全衛生パフォーマンス向上のための取り組みの好機という意味です。計画的変更とは、生産性向上のための設備導入といった、お金や時間などの資源の投入が伴うものであり、経営者の関与が不可欠です。

■ 図3　組織の状況に応じた「戦略的視点での対応」

組織が安全で健康的な職場を提供するために、
1）組織の事業上の課題を決定
- ●社内の課題
- ●社外からの課題

2）働く人および利害関係者からの要求事項に対し、対応が必要なものを決定
- ●法令、働く場所（事業場）、施主など
- ●労働条件、作業環境など
- ●その他

労働安全衛生活動に取り組む目的の明確化
⇒取り組む必要性の評価へ

■ 図4　組織の置かれた状況から「リスクと機会」を決定

1）組織の事業上の課題を決定（考慮する事項）
- ●社内の課題
- ●社外からの課題

2）働く人および利害関係者からの要求事項に対し、対応が必要なものを決定（考慮する事項）

3）労働安全衛生に関する4側面で決定（必須）
- ●労働安全衛生リスク
- ●労働安全衛生マネジメントシステムのリスク
- ●労働安全衛生機会
- ●労働安全衛生マネジメントシステムの機会

具体的な労働安全衛生機会として、以下のような改善・見直しの事例があげられます。

①製造ラインの移設時に、狭く高い作業場からの落下防止策や、地下ピット内の作業で頭が天井に当たらないようにするなどの改善を講じた。
②自動機など新たな設備の導入の際に、既存設備の不具合改善を実施した。
③設備の自動化の際、手の挟まれ・切創が多く発生している装置の再設計や運用方法の見直しを行った。
④組み立てエリアの拡大工事の際、出荷場の屋根を伸ばすことで、夏場の暑熱対策を図った。
⑤二人作業を一人作業に変更する際、作業員が倒れるなどの異常を発見する監視装置や警報装置を導入した。
⑥生産設備の増設工事の際、騒音管理区分IIのコンプレッサーを囲む壁を設置し、生産エリアの騒音を低減した。

企業においては、重大事故が発生していないのに安全性向上だけの目的で設備投資をするのは容易ではありません。しかし、製品の改良や生産性向上などを目的とした設備投資を労働安全衛生パフォーマンス向上のための取り組みの好機として捉えれば、安全性向上を目的とした設備投資への意思決定も容易になると考えます。

また、労働安全衛生マネジメントシステムに対するその他の機会については、労働安全衛生マネジメントシステム改善の好機であり、ISO 45001の附属書では「システム改善戦略に取組む」ことが要求されています。ここでは「戦略」がキーワードであり、機会の評価方法を確立し、取り組むべきか・取り組むに値しないことなのかを判断しながら、戦略的にマネジメントシステムを改善していくことがポイントです。

具体的には、以下のような取り組みがあげられます。

①過去の災害・重大ヒヤリハットの原因分析・評価結果を年度計画に落とし込み、月次で機械設計手順書の改訂、リスクアセスメント手順書に危険源を追加することなどを行った。
②非定常作業の手順書を月次で計画的に作成し、手順書をもとに教育を実施した。
③未熟練労働者に災害が多いという分析結果を受けて、未熟練労働者への教育のプロセスを見直した。

このような分析・評価に基づいた計画的な活動を行うことで、労働安全衛生マネジメントシステムが改善されていきます。

「リスク及び機会」への取り組みは、労働安全衛生活動のマンネリ化・形骸化の打破に役立つ

冒頭で、労働安全衛生活動のマンネリ化・形骸化に危機感を抱いている企業がISO 45001に注目していると述べました。マンネリ化・形骸化が起きる原因としては、長年、日本固有の労働安全衛生活動を続けることによる「やらされ感」によるものや、労働安全衛生経験スタッフの退職などから起こる労働安全衛生活動の硬直化があげられます。

前述のとおり、ISO 45001に基づきリスクと機会を決定し、その取り組みの計画を策定するためには、組織の置かれた状況に応じて、戦略的な視点で自分たちの組織における取り組むべきリスクと機会は何か、決定したリスクと機会にどう取り組むかを考える必要があります。これにより、働く人の負傷と疾病を防止し、安全で健康的な職場の提供を実現するために、優先的に対応すべきリスクと機会を特定できるため、注力すべき活動とそれ以外の活動が明確になります。

そして、実際に取り組みの計画に基づきマネジメントシステムを運用した結果を評価し、改善点を次年度の計画に反映していくというPDCAサイクルを回すことで、労働安全衛生パフォーマンスが向上します。

これら一連の取り組みは、長年、日本固有の労働安全衛生活動を続けている組織にとっては刺激となり「やらされ感」の解消につながります。また組織の置かれた状況に応じて優先的に対応すべき事項が明確になるため、労働安全衛生活動の硬直化の解消につながり、結果、労働安全衛生活動のマンネリ化・形骸化の打破に役立ちます。

ISO 45001には「安全に健康的に仕事をする」という当たり前のことが書かれている

少子高齢化が進行し、日本では人手不足がますます深刻になっています。企業では、AIや自動化によって生産性を向上させるとともに、働く人が常に健康で安全に力を発揮してもらえるようにすることが大切です。

ISO 45001を読み込めば読み込むほど、「安全に健康的に仕事をしましょう」という当たり前のことが書かれていることがわかります。書かれていることは、言われてみれば当たり前のことであるものの、改めて言われると「こういうことなのか」という気づきにつながることもあります。また、ISO 45001は、お金と人手をかけずにパフォーマンスを向上させようという規格であることもわかります。本腰を入れて労働安全衛生マネジメントシステムを構築したい組織には大きな発見があったり、自分たちではできていると思っていた労働安全衛生に関する活動などが、ISO 45001の要求事項と照合すると抜けていたりと、思い込みからの脱却につながることもあるでしょう。

厚生労働省の5年間の調査では、事故の96%は再発であるというデータがあります。事故や災害は、設備や段取りの変更点で起きることも多く、そういった変化点をしっかりと管理できるのは、気づきや思い込みからの脱却につながるというメリットに加え、ISO 45001に基づく労働安全衛生マネジメントシステムのメリットであると考えます。

第二部　いかにして効果的な労働安全衛生マネジメントシステムを構築するか

ISO 45001の特長は、戦略的にリスクと機会を分析することで組織としての注力ポイントが明らかになり、効果的に労働安全衛生パフォーマンスを向上できる点にあります。ここでは、ISO 45001の要求事項をどのように読み解けば、事業プロセスと一体化した労働安全衛生マネジメントシステムが構築できるのかを、逐条解説の形でご紹介します。

ISO 45001要求事項の解説

箇条1　適用範囲
ISO 45001の目的

箇条1（適用範囲）には、ISO 45001による労働安全衛生マネジメントシステムの意図する成果として、組織の労働安全衛生方針のもと、労働安全衛生パフォーマンスを継続的に改善し、法的要求事項とその他の要求事項を満たし、労働安全衛生目標を達成することが含まれると明示されています。組織は、この労働安全衛生マネジメントシステムが意図する成果をベースに、組織として何を目指すのか、組織が意図した労働安全衛生マネジメントシステムの成果を明確にすることが必要となります。

そして、組織が意図した労働安全衛生マネジメントシステムの成果を達成するために、組織の内外の課題、働く人とその他の利害関係者のニーズおよび実際の活動を考慮して適切な適用範囲を決定し、労働安全衛生に関連する「リスク及び機会」を特定後、それらに優先的に対応するための計画を立ててPDCAサイクルを回す、ということが労働安全衛生マネジメントシステムの全体の流れとなります。

箇条2　引用規格

ISO 45001では引用規格がないことが示されています。

箇条3　用語及び定義
全ての人が対象、“worker”は「働く人」

ISO 45001では、規格の箇条に従って用語を定義しています。そのなかでは、ISO 45001がトップマネジメントから管理職、非管理職まで組織の管理下で働く全ての階層、種類の人を対象とするため、「働く人」という用語を用いています。また、一般的なリスクと機会に加えて「労働安全衛生リスク」と「労働安全衛生機会」が定義されています。一般的なリスクと機会は、「労働安全衛生マネジメントシステムに対するその他のリスクとその他の機会」と定義されています。

箇条4　組織の状況
外部・内部の課題を把握し、適用範囲を決め、システムを構築する

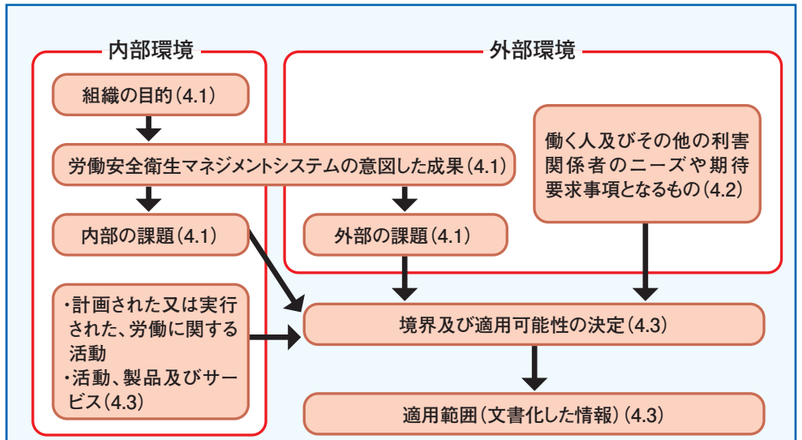
箇条4.1 組織及びその状況の理解
箇条4.2 働く人及びその他の利害関係者のニーズ及び期待の理解

労働安全衛生マネジメントシステムは、インプットをアウトプット（成果）に変換するプロセスの集合体です。箇条4.1（組織及びその状況の理解）および箇条4.2（働く人及びその他の利害関係者のニーズ及び期待の理解）は、インプットについての要求事項です。組織の目的に関連し、労働安全衛生マネジメントシステムの意図した成果に影響を与える外部・内部の課題、働く人とその他の利害関係者が企業に向けるニーズ・期待を経営的な視点で把握し、マネジメントシステムを展開するためのインプットの決定を要求しています。ここでいう組織の目的とは、「製造業であれば〇〇の供給によって社会に貢献する」という、企業理念などに表現されているものです。また、「労働安全衛生マネジメントシステムの意図した成果」とは、安全で健康的な職場の実現、負傷・疾病の防止ということを意味します。利害関係者には、お客さま、サプライヤーはもちろん、労働基準監督署のような行政機関も含まれます。

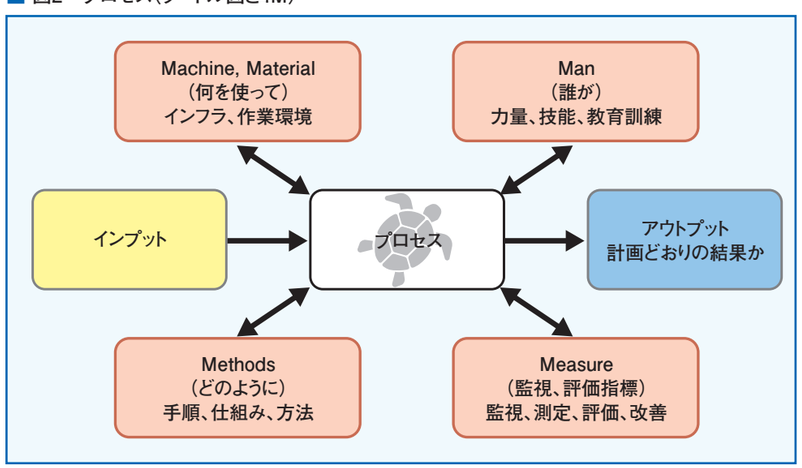
箇条4.3 労働安全衛生マネジメントシステムの適用範囲の決定

労働安全衛生マネジメントシステムの適用範囲を決定する際には、「外部及び内部の課題を決定」（箇条4.1）すること、「働く人及びその他の利害関係者の要求事項を考慮」（箇条4.2）すること、そして「労働に関連する、計画又は実行した活動を考慮に入れる」こ

■ 図1　箇条4.1～箇条4.3のまとめ



■ 図2　プロセス（タートル図と4M）



とが求められます。この場合の「計画」とは未来の活動といった意味であり、「実行した活動」とは、過去および現在の活動を意味します。つまり、現在、過去、未来における活動を考慮に入れて適用範囲を決定することが要求されます。また「考慮に入れる（take into account）」とは、「考慮する（consider）」とは異なり、必ず取り組まなくてはならないということを意味します。

お客さまからは、「製造部門のみを適用範囲にしたい」というお話を伺うこともありますが、箇条4.2（働く人及びその他の利害関係者のニーズ及び期待の理解）で述べたような幅広い利害関係者との折衝などを考えると、適用範囲を製造部門に限定するのではなく、組織全体で取り組むことが必要です。

■ 図3　リーダーシップ及びコミットメントの一覧

トップマネジメントがリーダーシップ及びコミットメントを「実証」する。

a) 安全で健康的な職場と活動の提供に対する全体的な責任
b) 労働安全衛生方針・目標と組織の戦略的方向性との両立
c) 組織の事業プロセスと労働安全衛生マネジメントシステム要求事項の統合
d) 労働安全衛生マネジメントシステムに必要な資源が利用可能
e) 労働安全衛生マネジメント及び要求事項への適合の重要性の伝達
f) 意図した成果の達成
g) 労働安全衛生マネジメントシステムの有効性に寄与するよう指揮、支援
h) 継続的改善の推進
i) 管理層の役割を支援
j) 労働安全衛生文化の形成・主導・推進
k) インシデント、危険源、リスク及び機会の報告をするときに報復から働く人を擁護
l) 協議及び参加のプロセスを確立、実施
m) 安全衛生に関する委員会の設置と支援

箇条4.4 労働安全衛生マネジメントシステム

この箇条は労働安全衛生マネジメントシステムの構築を要求しています。労働安全衛生マネジメントシステムはプロセスの集合体です。プロセスとは手順ではなく、インプットをアウトプットに変換するための、相互に関連または相互に作用する一連の活動です。プロセスとは、11ページの図2のように4M、つまり、何を使って（Machine，Material）、誰が（Man）、どのように実現し（Methods）、結果をどのように評価するか（Measure）を考えると理解しやすくなると思います。

箇条5 リーダーシップ及び働く人の参加
「働く人の参加」に重点が置かれていることがポイント

箇条5.1 リーダーシップ及びコミットメント

箇条5.1（リーダーシップ及びコミットメント）では、トップマネジメントがリーダーシップとコミットメントを「実証」することを要求しています。実証とは口で言っているだけではなく、きちんと実行することです。図3の「リーダーシップ及びコミットメントの一覧」のうち、特に注意が必要なのは、j)、k)、m)です。

j）労働安全衛生文化の形成・主導・推進は、多少時間のかかる取り組みです。文化は短期間で醸成できるものではありませんから、普段からトップマネジメントが先頭に立って、労働安全衛生に目の届いた経営を行い、働く人がやっていいこと・やってはいけないことを常識的に判断できるような文化を作りあげ、浸透させることが必要です。

k）については、ヒヤリハットをはじめとするインシデントや危険源の報告などを行った際に、報復行為から働く人を擁護することです。往々にして、報告者は周囲から「報告しなければ何もしなくて済んだのに」と責められることがあるので注意が必要です。

m）については、日本では50名以上の会社は衛生委員会、それより大きい会社は安全衛生委員会を設置することが労働安全衛生法で求められています。

箇条5.2 労働安全衛生方針

安全で健康的な労働条件を提供すること、危険源を除去して労働安全衛生リスクを低減することなど、ISO 45001は多くのコミットメントを求めています。また、働く人の協議及び参加へのコミットメントも求められていることから、トップマネジメントが一方的に方針を決めるのではなく、従業員と協議を行い、参加してもらうことを重視していることがわかります。

また、決めた方針は、文書化、組織内への伝達、利害関係者が入手可能にすること、そして常に妥当かつ適切なものに更新していかなければなりません。組織の内部や外部の状況は刻々と変化しますから、今の時代にフィットしたものにしておく必要があります。方針は作りっ放しで額に入れて飾っておくものではないということです。

ところで、ISO 45001をはじめとするISOマネジメントシステム規格には、文書を「維持する（maintain）」「保持する（retain）」という用語が使われています。文書の維持とは、作業手順など必要に応じて改訂を行い、最新の状態を保つことを意味します。文書の保持は、記録のために内容を不変に保つことを意味します。ISO 45001では文書化した情報を維持して保持することを求められる場合があります。1つの文書を維持して保持することはできませんから、これは2つ以上の文書のことを示していることを意味します。

箇条5.3 組織の役割、責任及び権限

役割、責任の割り当ては会社組織では当然のことですが、ISO 45001は、最低限2つの役割に関して責任と権限を割り当てることを要求しています。一つは規格要求事項へ適合することの責任と権限、もう一つは労働安全衛生パフォーマンスをトップマネジメントへ報告する責任と権限です。ISO 45001では、「管理責任者を任命する」という要求事項は無くなりましたが、事実上、管理責任者に相当する役割が必要であることを示しています。

箇条5.4 働く人の協議及び参加

「協議」と「参加」は、箇条3（用語及び定義）で定義されています。「協議」は、意思決定の前に意見を求めることで、求めた意見をどのように処理するかまでは要求していません。一方、「参加」は意思決定に関与することで、意思決定の場で意見を述べる、採決時に手を上げる・上げないなどを意味しています。

この箇条は、労働安全衛生マネジメントシステムの成功のために重要な働く人の協議と参加について定めたものです。働く人が協議・参加するために、その参加の障害や障壁を決定して取り除く、もしくは最小化することなどが求められます。箇条の文中には、注記2として「言語若しくは識字能力の障壁」とありますが、これには外国人労働者が当てはまると解釈できます。

ここまで、組織の状況を大きな視点で評価し、労働安全衛生マネジメントシステムの基本となるインプットとアウトプットを特定することと、トップマネジメントの責任が明確になりました。

箇条6（計画）では、組織の状況の変化を予測し、働く人および労働安全衛生マネジメントシステム双方にとってのリスクと機会を継続的に決定するプロセスを扱います。

箇条6 計画
2種類のリスクと2種類の機会に取り組む

箇条6.1 リスク及び機会への取組み
箇条6.1.1 一般

この箇条は、「労働安全衛生マネジメントシステムの意図した成果」を達成すること、「望ましくない影響」を防止・低減すること、および「継続的改善」するために取り組む必要のあるリスクと機会を決定するプロセスを要求しています。

リスクと機会を決定する際には、箇条4.1（組織及びその状況の理解）、箇条4.2（働く人及びその他の利

害関係者のニーズ及び期待の理解）と箇条4.3（労働安全衛生マネジメントシステムの適用範囲の決定）を考慮し（consider）、かつ箇条6.1.2.1（危険源の特定）で特定した危険源、下の図4にある2種類のリスクと2種類の機会、箇条6.1.3（法的要求事項及びその他の要求事項の決定）で決定した法的要求事項とその他の要求事項を考慮に入れます（take into account）。

■ 図4　2種類のリスクと2種類の機会

- 労働安全衛生リスク(6.1.2.2)
  危険な事象またはばく露の起こりやすさ、負傷および疾病の重篤度との組合せ。(従来からのいわゆるOH&Sリスク)
- 労働安全衛生機会(6.1.2.3)
  労働安全衛生パフォーマンスの向上につながり得る状況または一連の状況。
- 労働安全衛生マネジメントシステムに対するその他のリスク(6.1.2.2)
  OHSMSの確立、実施、運用および維持に関係するリスク。
- 労働安全衛生マネジメントシステムに対するその他の機会(6.1.2.3)
  OHSMSを改善する機会。

■ 図5　危険源の特定

- 危険源を継続的に先取りして（ongoing and proactive）特定するプロセスを確立、実施、維持。
- 考慮に入れる（これらだけに限られない）。
  ・作業編成、社会的要因、リーダーシップおよび組織の文化
  ・定常的および非定常的な(routine and non-routine)活動および状況
  ・緊急事態を含む、過去の関連のあるインシデントおよびその原因
  ・起こり得る緊急事態
  ・働く人、請負者、来訪者、周辺の人々、直接管理しない場所で働く人
  ・その他の課題
  ・労働安全衛生マネジメントシステムの実際の変更、または変更案
  ・危険源に関する知識、および情報の変更

箇条6.1.2 危険源の特定並びにリスク及び機会の評価

箇条6.1.2.1 危険源の特定

この箇条は、労働安全衛生リスクに関する危険源を特定することから始まります。ISO 45001は、現在明確になっていない、または潜んでいる危険源に対して継続的に先取りして（ongoing and proactive）特定するプロセスを確立、実施、維持することを求めています。危険源の特定にあたっては、作業編成、社会的要因、リーダーシップや定常的および非定常的 (routine and non-routine）な活動と状況を考慮に入れます。このうち、定常的および非定常的な活動と状況を考慮に入れなくてはならないのは、定常的あるいは非定常的な作業によって、危険の度合いが異なるためです。また、ほかにも考慮に入れる項目として、事故や火災、転倒などの緊急事態（20ページ 箇条8.2参照）を含む過去のインシデントとその原因、実際に働く人や同じ職場にいる請負者、来訪のお客さま、職場の周囲にいる人、組織が直接管理しない場所で働く人などがあります。直接管理しない場所で働く人とは、例えば運送会社では公道を走行しているドライバー、システムエンジニアリング会社では客先で作業しているエンジニアなどを意味します。

箇条6.1.2.2 労働安全衛生リスク及び労働安全衛生マネジメントシステムに対するその他のリスクの評価

この箇条は、2種類のリスク（労働安全衛生リスク、労働安全衛生マネジメントシステムに対するその他のリスク）の評価を行うことを要求しています。

労働安全衛生リスクとは、特定した危険源から生じる人体に対するリスクであり、リスクアセスメント手法によって評価することが求められます。労働安全衛生マネジメントシステムに対するその他のリスクについては、マネジメントシステムの確立、実施、運用および維持に関するその他のリスクを決定・評価することが求められます。

これら2種類のリスク評価については、要求される詳細度が異なります。労働安全衛生リスクについては、どのくらいのリスクレベルで、どういったリスク修正対策を適用するのかというリスクアセスメント手法に基づく詳細な評価が必要です。一方、労働安全衛生マネジメントシステムの確立、実施、運用および維持に関するその他のリスクについては、リスクを評価して取り組むべきか否かを決定します。ここではリスクアセスメント手法によるリスクの評価は求められていません。

箇条6.1.2.3 労働安全衛生機会及び労働安全衛生マネジメントシステムに対するその他の機会の評価

この箇条は、2種類の機会（労働安全衛生機会、労働安全衛生マネジメントシステムに対するその他の機会）の評価を求めています。具体的には、方針、活動の計画的変更を考慮に入れた労働安全衛生パフォーマンス向上の労働安全衛生機会と、マネジメントシステムを改善するその他の機会を評価します。

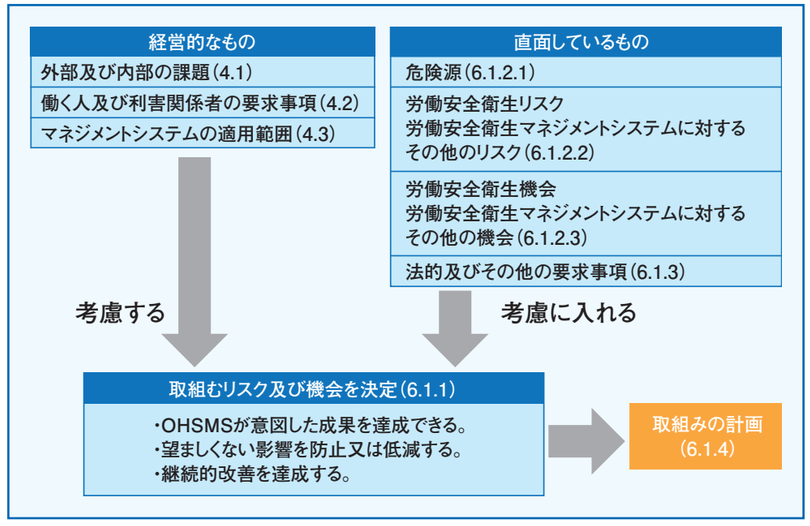
ここで、「機会（opportunity）」についてご説明しておきます。ISO 45001における機会とは、何かを可能にする時期または一連の状況のことであり、日本語では機会というよりも好機といった方がわかりやすいと思います。例えば、方針や活動の計画的変更があるときは、効率的にお金・時間を使えることから、労働安全衛生パフォーマンスを向上させる好機です。パフォーマンス向上活動そのものは機会ではありません。ISO 45001は、組織や活動の変化に合わせて労働安全衛生パフォーマンスを向上する活動を行うことを推奨しています。

箇条6.1.3 法的要求事項及びその他の要求事項の決定

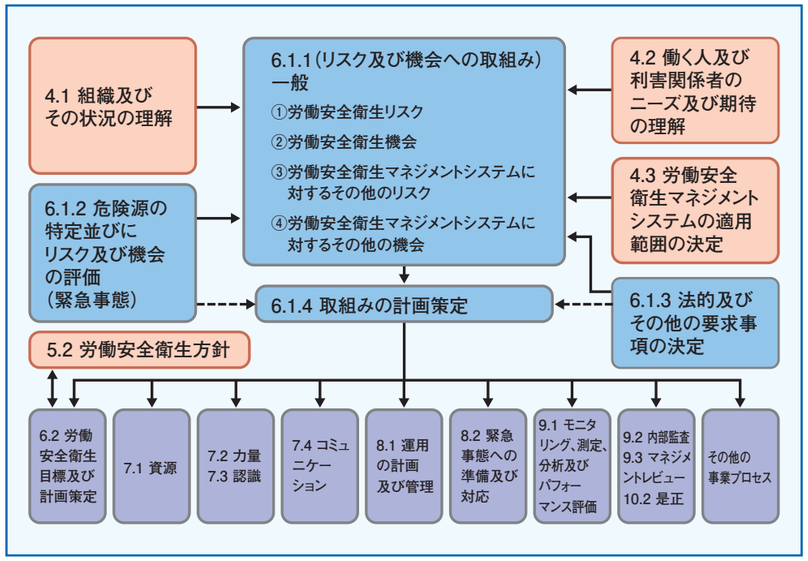
この箇条は、箇条6.1.2（危険源の特定並びにリスク及び機会の評価）を受けて、法的要求事項とその他の要求事項を決定することを要求しています。単に法的要求事項を決定するだけでなく、コミュニケーションが必要となるものの決定を要求しているのは、法的な外部コミュニケーションとして行政機関に対する届出や報告を意識しているからだと思われます。

ここまでの流れをまとめたのが、この下の図6です。「外部及び内部の課題」「働く人及び利害関係者の要求事項」「マネジメントシステムの適用範囲」を考慮するとともに、「危険源」「労働安全衛生リスク、労働安全衛生マネジメントシステムに対するその他のリスク」「労働安全衛生機会、労働安全衛生マネジメントシステムに対するその他の機会」ならびに「法的及びその他の要求事項」を考慮に入れ（必ず取り入れ）、その上で取り組む必要のあるリスク及び機会を決定します。

■ 図6　取組むリスク及び機会を決定



■ 図7　取組みの計画策定のまとめ



箇条6.1.4 取組みの計画策定

この箇条は、決定したリスク及び機会、法的要求事項とその他の要求事項、ならびに緊急事態の3つについて、自分たちで状況を判断し、何をすべきか、どのように取り組むかを考え、実施し、有効性を評価することを要求しています。また、この箇条は、決定したリスクと機会、法的要求事項とその他の要求事項、ならびに緊急事態について、労働安全衛生活動ではなく、その他の事業プロセスで取り組んでいいということを明確にしています。

ここまでを図にしたのが、上の図7です。箇条4.1（組織及びその状況の理解）で決定した組織の内外の課題と、箇条4.2（働く人及びその他の利害関係者のニーズ及び期待の理解）で決定した働く人と利害関係者のニーズと期待、箇条4.3（労働安全衛生マネジメントシステムの適用範囲の決定）で決定した適用範囲を考慮し（consider）、箇条6.1.2（危険源の特定並びにリスク及び機会の評価）で特定した危険源と評価した2種類のリスクと2種類の機会、箇条6.1.3（法的要求事項及びその他の要求事項の決定）で決定した要求事項を考慮に入れ（take into account）、箇条6.1.1（一般）で要求されているリスク及び機会を決定します。そして箇条6.1.4（取組みの計画策定）にて、決定したリスク及び機会、法的要求事項とその他の要求事項、ならびに緊急事態にどのように取り組むかを決定していきます。

箇条6.2 労働安全衛生目標及びそれを達成するための計画策定

箇条6.2.1 労働安全衛生目標

この箇条は、労働安全衛生目標を関連する部門および階層で確立することを求めています。労働安全衛生方針との整合性や、PDCAサイクルを回すために、測定可能もしくはパフォーマンス評価可能であることがポイントになります。また、目標を立てる上で考慮に入れる内容として、法的要求事項とその他の要求事項、リスクと機会、働く人との協議の結果、モニタリング、必要な人に情報を伝達することなどが要求されますので、取り組みの状況と照らし合わせて目標を更新することが必要です。

箇条6.2.2 労働安全衛生目標を達成するための計画策定

この箇条は、目標達成を計画するために必要な要素の決定を要求しています。具体的には、実施事項はもちろん、必要な資源（ヒト・カネ・モノ）、責任者、達成期限、結果の評価方法を決定する必要があります。そして最も重要になるのは、取り組みを事業プロセスに統合する方法を決定することです。目標に対して新たに取り組みを始めてもいいですが、ISO 45001は、ほかに行っている取り組みがあれば統合できないかなど、効率的な取り組みを計画することを要求しています。

箇条7 支援
働く人が力量を備えるための支援を行う

箇条7.1 資源
箇条7.2 力量

箇条7.1は、必要な資源（ヒト・カネ・モノ）を決定し提供しなさいという、いわば当たり前のことを述べています。箇条7.2は、負傷や疾病の発生といった労働安全衛生パフォーマンスに影響を与える働く人に必要な力量を備えさせてくださいということです。パフォーマンスに影響を与える働く人には、現場で働く人も管理・監督者も含まれ、それぞれに必要な力量も異なります。

また、重要なこととして、働く人に危険源を特定する能力を含めた力量を備えさせることも求められています。危険源を特定する能力とは、現場での危険を認識して危険源には近づかない、すなわち安全に作業する能力を備えていることとご理解いただけば結構です。

箇条7.3 認識

この箇条は、組織が働く人に対して認識させておかなくてはならない事項を示しています。組織の労働安全衛生方針や目標はもちろん、労働安全衛生パフォーマンスが向上したらどのような便益があるか、マネジメントシステムの要求事項に適合しない、すなわちルールに適合しないとどのような不利益があるか、さらには働く人に関連するヒヤリハットをはじめとしたインシデントとその調査結果、働く人に関連する危険源や労働安全衛生リスクアセスメント、ならびに決定した管理策（18ページ 箇条8.1.2参照）まで、きちんと認識させておくことが求められています。

なかでも重要になるのは、「重大な危険から働く人が自ら逃れることができることおよびそのような行動を取ったことによる不当な結果から保護されるための取り決め」という項目です。危ないと思ったら逃げることができる権利があること、そして逃げることによって非難されないということを働く人が認識できる教育が組織に求められます。具体的には、荷崩れが起きたときには、自分で支えようと思わないで逃げることなどを意味します。

箇条7.4 コミュニケーション
箇条7.4.1 一般

コミュニケーションには、内部と外部両方のコミュニケーションがあります。ここで要求しているのは、内部と外部両方に共通するコミュニケーションプロセスの確立、実施、維持です。プロセスを確立する際に決定すべき項目として、コミュニケーション活動の内容、実施時期、対象者や方法が示されていますが、実施時期が示されていることで、例えば労働基準監督署などへの報告を意識していることが窺えます。また、プロセスを確立する際に考慮に入れるものとして、性別や言語、それぞれの人の持っている文化、識字能力、心身障害（disability）などの多様性や、法的要求事項とその他の要求事項が求められます。ほかには、内部や外部からのコミュニケーションを図ろうとしてきた場合は、無視せずに対応することを要求しています。

箇条7.4.2 内部コミュニケーション

さまざまな階層および機能間で内部コミュニケーションを行い、変化があった場合には連絡、伝達することを要求しています。また、継続的に働く人からの提案などをきちんと扱い、労働安全衛生マネジメントシステムの改善につなげることも要求しています。具体的には提案制度のようなものと考えてください。

■ 図8　箇条7.2 力量

次の事項を実施
- 労働安全衛生パフォーマンスに影響を与える働く人に必要な力量を決定
- 働く人が（危険源を特定する能力を含めた）力量を備える
- 力量を身につけ維持するための処置、有効性の評価
- 文書化（力量の証拠）（保持）

■ 図9　文書化した情報一覧

箇条	文書化した情報の概要
4.3	労働安全衛生マネジメントシステムの適用範囲（利用可能）
5.2	労働安全衛生方針（利用可能）
5.3	役割、責任及び権限の割り当て（維持）
6.1.1	リスク及び機会 リスク及び機会を決定し、取組むために必要なプロセス及び処置（維持）
6.1.2.2	労働安全衛生リスクの評価方法及び基準（維持・保持）
6.1.3	法的要求事項及びその他の要求事項（維持・保持）
6.2.2	労働安全衛生目標及びそれらを達成するための計画（維持・保持）
7.2	力量（保持）
7.4.1	コミュニケーションの証拠（保持）
8.1.1	プロセスが計画どおりに実施されたという確信（維持・保持）
8.2	緊急事態に対応するためのプロセス及び計画（維持・保持）
9.1.1	モニタリング、測定、分析及びパフォーマンス評価の結果 機器の保守、校正又は測定の検証の記録（保持）
9.1.2	順守評価の結果（保持）
9.2.2	監査プログラムの実施及び監査結果（保持）
9.3	マネジメントレビューの結果（保持）
10.2	インシデント又は不適合の性質及びとったあらゆる処置 とった処置の有効性を含めた全ての対策及び是正処置の結果（保持）
10.3	継続的改善の証拠（維持・保持）
A7.5	法的要求事項及びその他の要求事項への取組みの計画、及びこれらの処置の有効性の評価（含めることが望ましい）

箇条7.4.3 外部コミュニケーション

外部コミュニケーションについては、法的要求事項とその他の要求事項を考慮に入れて、労働安全衛生マネジメントシステムについてコミュニケーションを行うことが求められます。法的要求事項を考慮に入れるという要求から、労働基準監督署などへの報告・連絡・届出が意識されていることが窺えます。

箇条7.5 文書化した情報
箇条7.5.1 一般
箇条7.5.2 作成及び更新
箇条7.5.3 文書化した情報の管理

箇条7.5は、文書化した情報に関する要求事項です。これは他のISOマネジメントシステム規格と同じで、組織の管理すべき情報を適切な識別と記述のもと、紙や電子媒体など適切な形式で作成、更新するということです。情報は必要なとき、必要なところで、入手可能であり、十分に保護されていることを求めています。また外部から入手した文書を必要に応じて識別して管理することも求めています。労働安全衛生に関する外部文書には、労働基準監督署から発行された指導票や、化学物質のSDS（安全データシート）があります。

箇条8. 運用
4Mを意識してプロセスをつくる

箇条8 運用
箇条8.1 運用の計画及び管理
箇条8.1.1 一般

運用段階では、12ページで述べた4Mを意識しながら、プロセスを計画、実施、管理、維持することが求められます。具体的には、プロセスに関する基準の設定、基準に従ったプロセスの管理、文書化した情報の維持・保持、働く人に合わせた作業の調整が必要です。このうち、文書化については、プロセスが計画どおり実施されたことに確信が持てる必要最小限のもので良いとしています。また、作業の調整とは、より安全に、より働きやすくする調整を意味します。

複数の事業者が混在する職場では、他の組織とマネジメントシステムの調整が求められます。これは、建設もしくは造船所のような大規模な事業場だけではなく、複数の会社の従業員が同じ職場で同時に働く場合が該当します。

箇条8.1.2 危険源の除去及び労働安全衛生リスクの低減

この箇条では、危険源による負傷や疾病のリスクを低減するために、管理策の優先順位によって、危険源の除去と労働安全衛生リスクを低減するプロセスを確立、実施、維持することが求められます。この管理策（control）とはリスクを修正する対策のことで、複数の管理策（controls）から優先順位の高いものを実施することです。リスクマネジメントの世界では優先順位が決定されており、①危険源の除去②危険性の低いプロセスや操作、材料、設備への代替③工学的対策の実施、もしくは作業構成の見直し。工学的対策とは、カバーやインターロック（安全装置）などのハードウエア的な対策。これらが実施できない場合は、④教育訓練や表示、注意喚起などを含めた対策を行います。教育訓練（training）とは、座学での教育では不十分とされています。また、それもできない場合は、⑤適切な個人用保護具を使いなさい、という5段階の優先順位の下、リスクを低減することを要求しています。

箇条8.1.3 変更の管理

この箇条は、労働安全衛生パフォーマンスに影響を及ぼす計画的な、暫定的および永続的変更の管理をするプロセスの確立を求めています。変更管理プロセスの目的は、既存の製品やサービス、プロセスの変更をはじめ、法的要求事項とその他の要求事項の変更や、危険源および労働安全衛生リスクに関する知識または情報の変化などがあった際に、これに伴い発生する新たな危険源や労働安全衛生リスクを抑制し、労働安全衛生を向上させることです。このうち、例えば法的要求事項とその他の要求事項の変更としては、従業員の人数が増えて、安全衛生委員会の設置が義務化されるなどがあげられます。

これらは意図した変更、計画的な変更ですが、意図しない変更や変化もあります。例えば、災害に遭って工場の様子が変わったなどの変更です。このような管理できない変更は、その結果をレビューし、有害な影響を低減することが求められます。

箇条8.1.4 調達
箇条8.1.4.1 一般

この箇条では、製品およびサービスの調達を管理するプロセスを確立、実施、維持することを求めています。これは、調達する製品やサービスが自分たちの労働安全衛生マネジメントシステムに適合するよう、事前に評価などを実施し、危険なものには対応するということを意味します。化学物質などでは当たり前に要求されることですが、これが調達の管理の基本です。

箇条8.1.4.2 請負者

この箇条は、同じ職場で一緒に働いている、労働安全衛生マネジメントシステム対象外の請負者（contractors）の活動に起因する労働安全衛生リスクの評価とその管理プロセスについての要求です。この箇条の対象は広く、請負者が組織に影響を与える活動や業務と、組織が請負者に影響を与える組織の活動や業務、そして職場のその他の利害関係者、お客さまなどの来訪者に影響を与える請負者の活動や業務が含まれます。

また請負者の選定には、請負者選定に関する労働安全衛生基準を定めて適用しなければなりません。これは組織の労働安全衛生マネジメントシステム対象外の人に対しても、労働安全衛生のために、組織やマネジメントシステムの取り決めに従う約束事を入れておくということであり、一緒に働く人を無視してはならないという内容でもあります。

■ 図10　箇条8.1.3 変更の管理

- 労働安全衛生パフォーマンスに影響を及ぼす、計画的な、暫定的および永続的変更の実施および管理のためのプロセスを確立。
  - ・新しい製品、サービスおよびプロセスまたは既存のそれらの変更
    - ― 職場の場所および周囲の状況
    - ― 作業の構成
    - ― 労働条件
    - ― 設備
    - ― 労働力
  - ・法的要求事項、およびその他の要求事項の変更
  - ・危険源および労働安全衛生リスクに関する知識または情報の変化
  - ・知識および技術の発達
- 意図しない変更によって生じた結果をレビュー

箇条8.1.4.3 外部委託

外部委託とは、一般的な意味での外部委託であり、製造業が自ら製造した部品のめっき工程を外部委託する場合などを意味します。ISO 45001は、外部委託に関しても機能とプロセスの管理を要求しており、法的要求事項とその他の要求事項に適合しているかの管理や外部委託の取り決めが労働安全衛生マネジメントシステムの意図した成果の達成に適切であることが求められます。

またこの箇条は、自らの発注によって、外部委託先の社員などが負傷・疾病することを未然に防いでいると解釈することができます。

箇条8.2 緊急事態への準備及び対応

この箇条は、事故や火災、転倒など労働安全衛生上の緊急事態への対応プロセスを確立、実施、維持することを要求しています。具体的には、応急処置（first aid）の用意を含めた緊急事態の計画的な対応を確立します。そして計画的な対応に関する教育訓練（training）を提供し、計画的な対応をする組織の能力について定期的にテストと訓練を行いますが、ここでの訓練は、教育訓練よりもハードな訓練（exercise）が求められます。また、テストと訓練後はもちろん、不幸にして事故など緊急事態が発生した場合には、パフォーマンスを評価して、必要に応じて対応計画を改訂します。さらに、全ての働く人に自らの義務や責任に関わる情報を伝達するほか、マネジメントシステムの対象外となる請負者、来訪しているお客さま、消防署などの緊急時対応サービス、労働基準監督署などの行政機関、そして地域社会にも関連情報をきちんと伝達します。

これらの対応プロセスを策定するにあたっては、利害関係者である地域社会、近隣の工場、消防機関などのニーズや能力を考慮に入れ、利害関係者の関与を確実なものにしなければなりません。

箇条9 パフォーマンス評価
トップマネジメントからアウトプットを引き出す

箇条9 パフォーマンス評価
箇条9.1 モニタリング、測定、分析及びパフォーマンス評価
箇条9.1.1 一般

パフォーマンス評価を行うにあたり、モニタリングおよび測定の対象を決定する必要があります。対象になるものには、法的要求事項とその他の要求事項の順守の程度、危険源およびリスクと機会に関わる活動・運用、労働安全目標達成に向けた進捗、運用およびその他の管理策（controls）の有効性などが含まれます。管理策の有効性については、カバーやインターロック（安全装置）などが外され無効化されていないか、表示・警告をした貼り紙が剥がれていないか、読みにくくなっていないかなどのモニタリングが求められます。さらに、モニタリングや測定、分析、評価の方法、評価基準、モニタリングの実施時期も事前に決定しておくことが求められます。

このパフォーマンス評価の目的は、労働安全衛生マネジメントシステムの有効性を判断することです。パフォーマンスが上がっていなければ有効性は低く、どこかに改善点があることがわかります。なお、この箇条では、測定機器の校正、検証、使用、維持を確実にすることも要求されます。

箇条9.1.2 順守評価

順守評価は、パフォーマンス評価の一つです。パフォーマンス評価は、法的要求事項とその他の要求事項の順守の程度をモニタリングすることを求めていますが、ここでは法的要求事項とその他の要求事項の順守を評価するためのプロセスを確立、実施、維持することを求めています。また、順守状況に関する知識や理解を維持することも求めています。自分たちの組織の状態を把握した上で、順守評価の結果を記録として保持しなさいということです。

箇条9.2 内部監査
箇条9.2.1 一般

内部監査は、あらかじめ定めた間隔で実施することが求められます。1年に1回、半年に1回といった間隔で、要求事項への適合と、実際に労働安全衛生マネジメントシステムが有効に実施され維持されているかを評価します。

箇条9.2.2 内部監査プログラム

内部監査を行うための監査プログラムを計画、確立、実施、維持することを求めています。各プロセスの重要性や、前回までの監査の結果を考慮に入れる（take into consideration）ことが求められます。監査基準や監査範囲を明確にすること、公平性の確保、結果を監査対象の管理者に報告すると同時に、関連する結果については働く人、利害関係者に報告することも求められます。利害関係者とは、関連する結果の報告ですから、例えば親会社からの求めがあれば応じるなどが考えられます。

ここでのポイントは、監査した結果をトップマネジメントに報告するだけでなく、共有することを要求している点です。また、監査の結果、不適合があれば改善に取り組むこと、有効性が低ければパフォーマンス向上のための継続的な取り組みを実施すること、監査の実施内容と結果を保持することなども要求されます。

■ 図11　箇条9.1.2 順守評価

- 法的およびその他の要求事項の順守を評価するためのプロセスを確立、実施、維持
- 以下を実施
  - ・頻度、方法を決定
  - ・順守を評価し、必要に応じて処置
  - ・順守状況に関する知識および理解の維持
  - ・文書化（順守評価の結果）（保持）

箇条9.3 マネジメントレビュー

監査の後は、結果をトップマネジメントに報告して判断を仰ぐマネジメントレビューです。マネジメントレビューで「次の事項を考慮」となっているのはインプット項目です。全てを網羅する必要はありませんが、「考慮」しながらトップマネジメントに報告を行ってください。

- 前回までのマネジメントレビューの結果と、そのためにとった処置の状況
- 外部・内部の課題の変化
  ニーズや期待、法的要求事項の変化なども含まれます。
- 方針や目標の達成度
- 傾向を含めた労働安全衛生パフォーマンスに関する情報
  「傾向を含めた」とは、今年の労災何件だけでなく、労災件数の推移をグラフや表にするなどを意味します。
- 資源の妥当性
  ヒト・カネ・モノが足りているか。
- 利害関係者とのコミュニケーション
  お客さまや労働基準監督署が含まれます。
- コミュニケーションの状況
  コミュニケーションは双方向ですから、「誰に○○を報告しました」「誰々より○○という指導をいただきました」となります。
- 継続的改善の機会
  これはシステムの継続的改善ですから、「こういうふうに変えるといい」というように提案を行うことです。

このようなインプットを受けて、トップマネジメントはアウトプットとして、次の全ての事柄について指示してください。

- ●労働安全衛生マネジメントシステムの継続的な適切性、妥当性および有効性
  トップから見た適切性や妥当性、有効性の結論です。
- ●継続的改善の機会
  インプットとして提案した内容に対する結論です。
- ●労働安全衛生マネジメントシステムのあらゆる変更の必要性
- ●必要な資源
  今の資源で十分か否かという決定です。
- ●もしあれば必要な処置
- ●事業プロセスとの統合を改善する機会
  組織の全体について最もよく知っているのはトップです。「この部門で行っている活動は、別の部門の活動と統合した方が効率が良いのではないか」など、トップの目線で無駄を省き効率を上げることを指示します。
- ●戦略的方向に対する示唆
  方針の変更などについても、きちんと指示してください。

これらのアウトプットを、働く人にきちんと伝達してください。

箇条10 改善
マネジメントシステムを継続的に改善する

箇条10 改善
箇条10.1 一般
箇条10.2 インシデント、不適合及び是正処置

インシデントとは、事故と事故になる前のもの、日本語ではヒヤリハットなどとも呼ばれています。事故などのインシデントが発生した場合、もしくは規格要求事項などの不適合があった場合には、遅滞なく対応してください。また、再発や他所での発生を予防するために、当事者や当事者のまわりの人に参加してもらって、是正処置を取る必要性を評価してください。

必要に応じて既存のリスクアセスメントをレビューします。このリスクアセスメントは労働安全衛生リスクの評価です。往々にしてリスクアセスメントの結果、安全だと判断された場所で事故は起きますので、リスクアセスメントが正しいかをきちんとレビューすることが重要になります。そして管理策の優先順位に従って処置し、対策を実施する前にもう1回、その対策を実施することに対するリスクアセスメントを行ってください。

また、是正処置を含めてとった全ての対策の有効性をレビューし、必要な場合は労働安全衛生マネジメントシステムを変更してください。その際に、手順やプロセスの変更が必要であれば実施してください。

文書化については、性質（nature）およびとった処置、有効性を含めた是正処置の結果を要求しています。事故の性質、例えば事故のタイプ、被災者の年齢、事故の起きた時間帯などを分類することは、統計的な処理や分析を行うためにも重要です。

箇条10.3 継続的改善

この箇条は、労働安全衛生マネジメントシステムを継続的に改善することを求めています。労働安全衛生パフォーマンスを向上させ、働く人の参加を推進し、継続的改善の結果を働く人に伝達することで、労働安全衛生マネジメントシステムを支援する文化を醸成してください。マネジメントシステムはプロセスの集合体ですので、プロセスを改善した記録が残ります。 ■

特集Ⅱ　いまから取り組む製造業の情報セキュリティマネジメント

第一部　まずは身の丈にあったシステムから

モノのインターネット(IoT)化や人工知能(AI)技術が製造業を含む産業全体に普及し、情報セキュリティマネジメントに取り組む重要性が高まっています。しかしながら、製造業においては、情報セキュリティマネジメントの取り組みが十分に浸透しているとはいえないのが現状です。第4次産業革命と呼ばれる技術革新による変化の中で、製造業はどのようなリスクにさらされているのか、対応するにはまず何から手をつけるべきなのか、ISO/IEC 27001主任審査員の川合浩司が解説します。

ISO/IEC 27001主任審査員
CSMS主任審査員
川合 浩司

製造業における情報セキュリティのいま

急速に高まる情報セキュリティ対策の必要性

あらゆる産業において品質管理やコストダウンのためのIT化が着実に進められてきましたが、近年急速に普及しているIoT化や人工知能は産業や社会を根底から変えると言われています。これに伴って情報セキュリティリスクも増大しており、対策を行うべき範囲は急速に拡大しています。

また、一つの企業が抱えるリスクのサプライチェーン全体への影響も考慮する必要があります。例えば近年では、情報セキュリティが堅牢なターゲットを攻撃するために、まずサプライチェーン内で比較的防御の甘い取引先を狙い、そこを踏み台にターゲットである企業を攻撃する手法が頻発しています。この場合、踏み台に利用された企業は結果的に加害者になってしまい、その後の取引に重大な影響を及ぼすことが懸念されます。

このように、情報セキュリティに関するリスクは一企業にとどまらずサプライチェーン全体に影響を及ぼすようになっているため、取引先に対して情報セキュリティの取り組みの強化を促す企業が増えています。実際に、取引先から情報管理の取り組みについて問われたことがあるという企業は多いのではないでしょうか。

情報セキュリティについての誤解

しかし、製造業においては、情報セキュリティマネジメントの取り組みが十分に浸透しているとはいえないのが現状です。

これには、情報セキュリティというと、「個人情報保護」に注目し「当社はモノ作りだから、それほど重要な個人情報は持っていない」と考えがちなことも一因としてあるかと思います。しかし多くの製造業では、取引先の情報、設計情報、品質情報、製造ノウハウなど、いったん漏洩すると事業に大きな影響を与える可能性がある情報を保有しています。それらの情報をしっかり守る

ことが求められているのです。

さらに、情報セキュリティというのは、情報漏洩対策に限ったものではありません。情報を必要なときに使用できるように管理することも需要です。例えば、生産ラインを動かす制御系システムのデータが壊れてしまうと生産ラインが止まってしまうというリスクが考えられます。「必要なときに使えるように情報を管理する」ということもまた、情報セキュリティにおいて重要な要素の一つです。

製造業の情報セキュリティとは何か

製造業が取り組むべき情報セキュリティとしては、①お客さまから預かった設計図などの情報や自社が保有している情報の機密性を保持すること、②自社の生産ラインを稼働させるための情報（受発注データなども含む）を必要なときに利用できるようにすることが考えられます。

①は自社の信頼と競争力に関わる問題です。製造業には外部に漏れてはならない情報が数多くあります。取引先から預かった情報が漏れれば、企業の信用は失墜します。そのほかにも、企業は競争力の源泉となる固有技術や知的財産、新製品の開発情報を保有しています。合併や買収、事業提携に関する情報もあるでしょう。これらの情報を共有する範囲を決め、許可された者以外アクセスできないようにしっかりと管理する必要があります。

②は生産の継続性に関わる問題です。生産設備を動かしている情報（例:加熱温度と時間・加工内容など）が壊れてしまえば、品質の低下や製品事故の原因になったり、生産ラインが止まってしまったりします。生産システムの多くがコンピュータによってコントロールされている現在、データが破壊されてしまうことのほかにも、サポートされていない古いソフトウェアで動いているパソコンのデータが使えなくなるなど、リスクにはさまざまなものが考えられます。増大するリスクへの対応の甘さは、製品の品質や生産活動そのものに多大な影響を与える可能性があります。

ISO/IEC 27001は変化する脅威に対応する仕組み

ISO/IEC 27001は、情報セキュリティマネジメントシステムを確立・実施・維持し、継続的に改善するための国際規格です。

情報セキュリティに取り組むうえでポイントとなるのは、リスクマネジメントの考え方です。情報技術の進歩は非常に速く、また企業の事業内容や製造体制も変化していきます。情報セキュリティ対策はある時点では最新、完璧の対策であったとしても、すぐに陳腐化したり実情にそぐわなくなったりする可能性があります。変化する環境に対応するために、ISO/IEC 27001には、想定される潜在的なリスクへの対策を選択し、継続的に改善していくPDCAの考え方が取り入れられています。

認証機関によるISO/IEC 27001の審査を受けることで、企業自身が気づいていないリスクに気づくということもあります。情報を取り巻く状況が激しく変化する中で、一つの企業だけで全ての変化に適切に対応するのは簡単なことではありません。審査を受けることで定期的に第三者の視点でチェックする仕組みが整いますから、情報セキュリティに取り組むうえで非常に有効だといえるでしょう。

また、ISO/IEC 27001の特長として、対策が必要な情報セキュリティリスクに対してどのように対応すべきかを示す管理策が、必要な対策の見落としを防ぐためにあらかじめ示されているということがあげられます。情報セキュリティのための方針群、組織、人的資源、資産、アクセス制御など14の箇条にわたって管理策が記載されており、ISO/IEC 27001に取り組む企業は、自社の状況や、情報セキュリティリスクに合わせて必要な管理策を参照することができるのです。

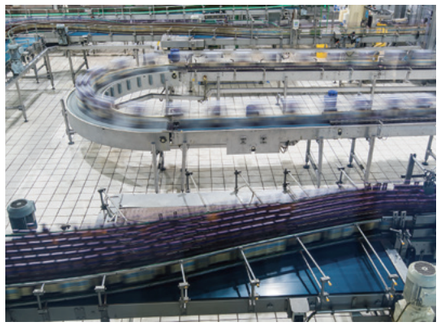
情報セキュリティマネジメントシステム構築のポイント「リスクアセスメント」

ここからは、情報セキュリティマネジメントシステム構築の重要なポイントである「リスクアセスメント」の進め方を解説します。

リスクアセスメントとは、情報セキュリティに関するリスクを洗い出し、その特性やレベルを分析・評価することです。まず自社が持つ情報および情報処理施設に関連するその他の資産（以下、情報資産）に関するリスクを明確にすることから始めるのが良いでしょう。

情報資産の一覧を作成し、分類する

情報資産に関するリスクを明確にするためには、そもそも企業がどんな情報資産を保有しているのかを洗い出す必要があるため、まず目録を作成します。企業は、設計図や注文書、顧客データのような情報そのもののほかに、そのような情報を取り扱うためのコンピュータシステム、ネットワークなどの情報資産を保有しています。これらの情報資産を棚卸しして一覧を作成します。個々のデータを十把ひとからげに並べるのではなく、それぞれの情報資産の特性（例:紙／電子データ、保管場所など）に応じて分類していくと、この次のリスク分析を行う上で良いでしょう。



最近は情報システム自体を外部の情報通信システム会社に委託したり、データのやり取りや保存場所としてクラウドのような外部のサービスを利用している

■ 図1　情報資産の例

分類	資産の例
ハードウエア	サーバ、クライアントパソコン、周辺機器、ネットワーク機器
ソフトウエア	OS、アプリケーション、ユーティリティ
データ	顧客情報、受注情報、経理情報
記録媒体	磁気記録、光記録、その他バックアップ
施設・設備	社屋、サーバルーム、空調設備、防火設備、電源装置
紙媒体・書類	契約書、手順書、規程集
人間	正社員、契約社員、顧客

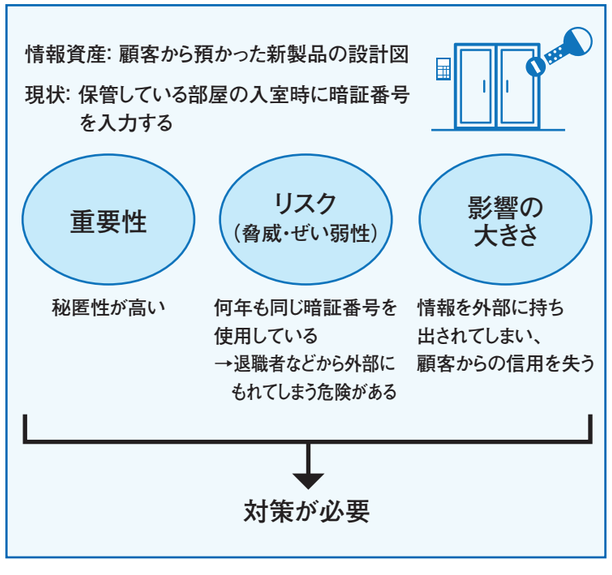
ケースも増えています。このように一見すると社内にはない情報も、企業の情報資産としてリストアップするのを忘れないように注意してください。

現状を把握し、リスク分析を行う

目録によって企業にどのような情報資産があるか明らかになったら、重要性、考えられる脅威、脅威に対するぜい弱性（つけこまれやすさ）、事故が発生した場合の影響の大きさなどの観点からそれぞれの情報資産を分析し、評価していきます。そして、優先順位の高い情報セキュリティリスクを特定します。

リスク分析によって、それまで気づかなかった現状に潜むリスクが明らかになることもあります。例えば、「データの受け渡しにUSBメモリやディスクなどの媒体を使っている」という運用がされており「ネットワークにつながっていないから問題になることはない」と考えていたとしても、媒体そのものが壊れたり紛失してしまったりする、あるいは媒体経由で生産システムがウイルスに感染するという脅威が発見されることもあります。全てのリスクに自力で気づくのは難しい面もあるため、まずはこのリスク分析の部分を外部の専門家に手伝ってもらうという方法も考えられるでしょう。

■ 図2　リスク分析の例



リスク分析の結果に基づいて対応方法を決める

分析の結果、それぞれのリスクに対して、どのような対応をとるのかを決めます。ここで参照するのが管理策です。企業は、リスク分析の結果明らかになった自社の状況に応じて「この管理策を実施する」「この管理策は状況に合わないので採用しない」という決定を行います。例えば、開発を全く行っていない企業であれば、開発に関する管理策を採用する必要はないでしょう。もちろん、企業の状況に合った管理策が規格に載っていなければ、他の方法を採用して対応します。

■ 図3　特定されたリスクへの対応の例

（図2の場合）

入室に使用する暗証番号に対する変更のルールを定めて実行する

（管理策 A.9.3.1）

企業によって抱えるリスクは異なりますから、リスク分析の結果、企業が具体的にどのような管理策を講じるのかはさまざまです。例えば「書類を鍵のかかるキャビネットに入れる」としている会社（A）もあれば、そうではない会社（B）もありますが、そのために会社（B）が直ちに要求事項に対して不適合となるわけではありません。会社（B）はキャビネットのある部屋自体の入退室を厳重に管理し、関係者以外の入室を厳しく制限しているためキャビネットに鍵をかける必要はない、という判断がされているのであれば、リスク分析の結果に基づいた対応がとられていると言えるでしょう。書類のセキュリティを確保するために「部屋の出入りの管理を厳重にする」、さらに「キャビネットに鍵をかける」など、どこまでの対策を行うことにしても、それがリスク分析の結果とひもづいていれば良いのです。

リスク分析の結果、「対策を講じない」つまり「リスクを受容する」、と判断することもまた対応方法の一つです。その場合も、そのリスクの持つ影響の大きさや発生可能性の高さ、対策にかかるコストといった要素を総合的に分析し、企業としての判断が対応方法に反映されていることが重要です。

ISO/IEC 27001の審査で認証機関は、このようなリスク分析の妥当性を重視しています。どのようにリスク分析を行い、その結果を反映した対応がとられているかがポイントとなります。

実施する管理策が決まったら、企業は管理策の適用状況（適用する管理策／適用しない管理策、その管理策を適用しない理由など）を記載した「適用宣言書」を作成します。適用宣言書を作成することで、その企業が情報セキュリティに関してどのような管理策を講じているのかが一目でわかるようになります。

トップのリードで身の丈にあったシステムを構築し、成果を上げる

情報セキュリティマネジメントシステムの担当者に必要なスキルとは

ISO/IEC 27001に基づいた情報セキュリティマネジメントシステムを構築し運用するには、マネジメントシステムに関する知見やスキルに加え、情報システムに関する知見やスキルも求められます。とはいえ、企業によっては両方の知見やスキルを兼ね備えた人材が確保できないこともあるでしょう。

その場合は、マネジメントシステムのスキルのある従業員とITの素養のある従業員とがペアを組んで進める方法が考えられます。もしISO 9001の認証を取得している企業であれば、その事務局担当者もしくは経験者とともに、情報システムの運用に携わってきた担当者が協力してシステムを構築すると効果的でしょう。

目的と範囲を明確にして外部のリソースも活用する

企業内部のリソースが足りない場合、コンサルタントやシステムインテグレーターなどのIT専門企業、近年経済産業省が養成を進めている中小企業向けの情報セキュリティ専門家などの外部リソースを活用する方法もあります。その場合、システム構築・運用のどの部分を外部リソースに依頼するのか、すなわち外部リソースに何を期待するのかを具体的に決めておくことが大切になります。認証取得までを段階的に考えると、「リスク分析の部分を手伝ってください」「具体的な手順書を作ってください」「手順書の作成と教育を行ってください」「内部監査のやり方のアドバイスをください」「登録審査をサポートしてください」というような依頼内容になっていくでしょう。ただし、外部リソースに任せっきりにしてしまい、企業の実情に合わない重たいシステムを構築してしまう危険性には十分注意してください。外部からのアドバイスを受けることの目的は、あく

までも最終的に内部リソースだけでマネジメントシステムを回せるようにすることにあります。

また、まず情報収集をするというのであれば、独立行政法人 情報処理推進機構（IPA）が提供するウェブサイトの情報セキュリティに関するコンテンツやセミナーなどのイベントは参考になるでしょう。もちろんJQAでも、新たにISO/IEC 27001の導入を検討している企業のためのセミナーや、業務相談や予備評価などのサポートサービスを用意しています。また、これから新たに情報セキュリティに取り組もうとする企業を対象とした「情報セキュリティ簡易診断」（→第二部 29ページ参照）のサービス提供も開始しました。企業の状況に応じて、適宜このような外部サービスを利用していくと良いでしょう。

トップマネジメントの判断のもと、メリハリをつけて取り組む

これは他のマネジメントシステムにも共通していえることですが、内部のリソースを活用するにしても、外部に委託するにしても、いずれにしてもうまくマネジメントシステムを構築・運用していくためにはトップマネジメントの理解と関与が不可欠です。トップの号令のもと、組織体制を作り、企業の状況に合った情報セキュリティの方針を定めて、全社をあげて取り組めるようにしなければなりません。

JQAの審査では最初に経営者へのヒアリングを行いますが、そこで、経営者がどれくらい本気なのか、セキュリティに対してどのような企業文化を持っているかなどを確かめています。「入札参加資格になっているからISO/IEC 27001の認証を取得する」「競合他社がやっているからうちもやる」というような判断で取り組み始めた企業もあるようですが、やはり、外部環境の変化に対応しながら継続的な改善を実践していくためには、経営者の本気の関与が重要だと思います。

最後に、ISO/IEC 27001の取り組みで成果を上げるために大切なことは、常に身の丈に合った情報セキュリティマネジメントシステムの維持に気をつけることです。

ISO/IEC 27001は現状を把握しリスクに優先順位をつけて取り組むものです。あまり難しく考えずに、トップマネジメントの判断のもとメリハリをつけて取り組み、身の丈にあったマネジメントシステムを構築しPDCAを回していくことで、少しずつレベルアップすることを目指すのが良いでしょう。 ■

情報セキュリティマネジメントに取り組まれる製造業のお客さまのお問い合わせ先

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
カスタマーリレーション部
TEL: 03-4560-5710
E-mail: ms-suishin@jqa.jp

※当機構は製造業を熟知した情報セキュリティマネジメントシステム審査員を擁しています。情報セキュリティ簡易診断を含めお気軽にお問い合わせください。

第二部　JQAと始める情報セキュリティマネジメントの第一歩

当機構は、これから情報セキュリティマネジメントに取り組み始める企業が、まず自社の状況を把握するために利用することができるツールとして「情報セキュリティ簡易診断」サービスを開始しました。このサービスの特長や期待される効果について、企画センター ソリューションビジネス開発部 部長の宮下卓士に聞きました。

企画センター
ソリューションビジネス開発部 部長
宮下 卓士

新サービス「情報セキュリティ簡易診断」開始

今回新しく「情報セキュリティ簡易診断」を開発した背景をお聞かせください。

宮下　当機構は情報セキュリティマネジメントシステム（ISO/IEC 27001）の審査を長く行っていますが、認証取得に関するお問い合わせ・ご相談を受ける中で、情報セキュリティに関する取り組みの必要性を感じていても、実際に何から始めるのか、どのような対策を講じたら良いのか、という悩みを持っていらっしゃる企業が多いと感じています。特に製造業の場合、品質管理・製造技術などの知見や経験は多くお持ちですが、情報セキュリティ対策となると、知見や経験がやや少ないため、情報セキュリティ対策が進捗していないことが多いようです。

そのような情報セキュリティ対策を検討して実施することが、難しいと感じている企業に、基本的なことをJQAと一緒に確認することから始めませんか、というのがこのサービスを開発した意図です。

例えば「敷地内への人の出入管理」「パソコン利用者の登録」など、業種を問わず一般的に企業が実施する情報セキュリティ対策の基本があります。このような基本となる事項を、専門性を有するJQAの診断員と一緒に確認することで、「こういうところの対策をしていけばいいのか」ということがご理解いただけると思います。

情報セキュリティ簡易診断は、どのような流れで進めるのでしょうか。

宮下　情報セキュリティ簡易診断は、専用の「診断チェックシート」使って行います。お客さまにはまずこのチェックシートに沿って自社の状況を自己点検していただきます。その後JQAの診断員がお客さまを訪問し、チェックシート・自己点検結果を基にお客さまの情報セキュリティ対策の取り組みを評価します。チェックシート・自己点検でわからないところがあっても、診断員が一緒に診断しますので問題ありません。わからないところをどんどん診断員に聞いていただければと思います。

■ 図1　簡易診断の流れ

STEP 1 お申し込み	お申込み受付後、診断実施日を調整
↓	
STEP 2 診断実施前	チェックシートに基づいてお客さまの状況をあらかじめ自己点検
↓	
STEP 3 診断当日	JQA認定診断員が訪問の上、チェックシートおよび自己点検結果を基に情報セキュリティ体制と運用・管理状況を診断

なお、このサービスに必要な日数と料金は、1日程度（約5時間）で、100,000円（税別）です。また、報告書は発行いたしません。

情報セキュリティマネジメントやISO/IEC 27001の知識がない状態でも受けてもいいのでしょうか。

宮下　全く問題ありません。ISO/IEC 27001の規格内容を見ても、具体的な情報セキュリティ対策のイメージがわかりにくいと感じる企業も多いでしょう。そのような企業にこのサービスを活用していただければ、情報セキュリティマネジメントの第一歩を踏み出していただくことができるサービスだと考えています。

このサービスを受けることで、どのような効果が期待できるでしょうか。

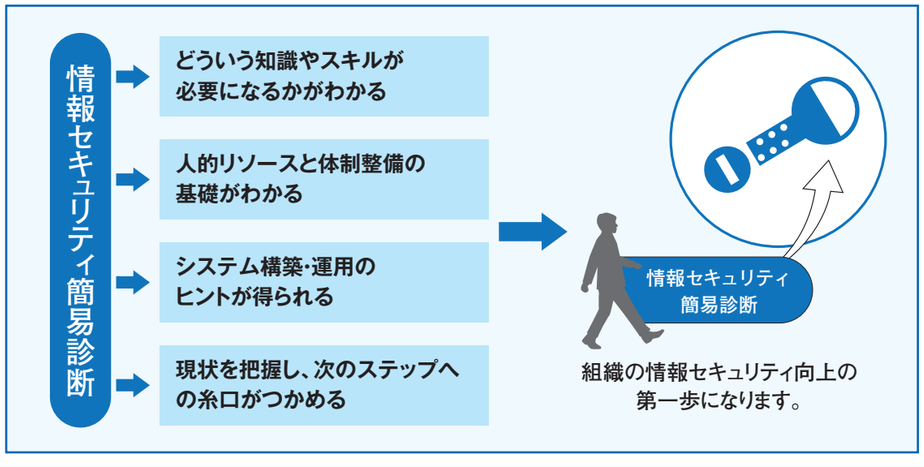
宮下　情報セキュリティ対策に取り組むために、何をすればいいのかが明確になる、ということがいえるでしょう。企業の情報管理の現状を把握し、情報セキュリティ対策のために必要になる知識やスキル、人的リソースと社内体制などについて、取り組むべきポイントとのギャップを明らかにします。現状何ができているのか、また逆に何が不足しているのかがわかれば、しっかりした情報セキュリティマネジメントシステムを構築する道筋が描けるようになります。このサービスを利用することで、結果的に大きく回り道することなくISO/IEC 27001の認証取得を見通すこともできるのではないかと思います。

■

■ 図2 こんな組織におすすめです

- **取引先から情報セキュリティの取り組みを求められている組織**
- **情報セキュリティ対策として、何から手をつけていいのかわからない組織**
- **情報セキュリティ対策の必要性を感じながらも、始めるきっかけがなかった組織**
- **ISO/IEC 27001の認証取得を検討している組織**

■ 図3　期待される効果



情報セキュリティ管理基準による診断チェックシート

情報セキュリティ簡易診断で用いるチェックシートは、経済産業省策定の「情報セキュリティ管理基準」のうちの「管理策基準」に基づいて、企業が情報セキュリティに取り組むための具体的なチェックポイントがわかりやすく解説されています。

■ 図4　診断チェックシート（抜粋）

項　番	解　説	確認内容	判定	メモ
6.2 モバイル機器及びテレワーキング				
6.2.1 モバイル機器を用いることによって生じるリスクを管理するために、方針及びその方針を支援するセキュリティ対策を採用する。	モバイル機器とは、スマートフォン、持ち出しするパソコン（無線を使ってインターネットに入ることを含む。）、ハンディターミナルなど、移動可能な機器を使う場合の会社としての方針（考え方）や使用方法などのルールを決めることです。 ここで言うモバイル機器を使用する上での方針は、5.1.1で記載した方針群の一つとなります。	モバイル機器を使用するための方針は作成しているか		
		モバイル機器を使用するための使用方法、禁止事項などルールを作成しているか		
7.3 雇用の終了及び変更				
7.3.1 雇用の終了又は変更の後もなお有効な情報セキュリティに関する責任及び義務を定め、その従業員又は契約相手に伝達し、かつ、遂行させる。	従業員、派遣社員、パートタイマー、アルバイトなど全ての従業員が、退職する場合や人事異動で部署が変わる場合、退職者や異動者が行うべき責任や追っている義務の内容を明確にして、その人に内容を伝えて、遵守させることです。 例えば、退職者する方に、仕事で知った取引先や製造物などの情報を、同業者に話すことは禁止する、退職してもその責任を所有していることを伝える、退職時に退職後の機密保持合意書に署名してもらうなどです。 また、人事業務から営業業務などに異動する場合に人事情報へのアクセスの必要性はなくなります。（管理職で、部下の情報を見ることはあるえますが）人事業務を行っていたときに知り得た従業員の情報などを他の従業員に話したりしてはいけないことを引き続き遵守することなどもあります。	退職時や異動時などに際して、情報セキュリティに対して引き続き所有する責任や義務を定めているか		
		上記で決定した責任や義務を従業員や（委託先などの）契約相手に伝達して、遂行させているか。		
8.1 資産に対する責任				
8.1.4 全ての従業員及び外部の利用者は、雇用、契約又は合意の終了時に、自らが所持する組織の資産の全てを返却する。	社員、契約社員、アルバイト、派遣社員といったあらゆる形態の従業員が、退職する場合は、全ての資産（パソコン、メールアドレス、職員手帳、社員証など）を返却することを要求しています。 直接雇用者のみならず、外部委託先なども対象です。 例えば、製品輸送を契約している運送会社に入門証を貸与しているが、その運送会社と運送委託契約が終了したときに入門証を回収する必要があります。 貸与品が、多いときなど貸与時に渡したものをリスト化して、受領サインをもらっておき、退職時にそのリストに基づいて返却物を確認することなどが、考えられます。	組織（会社）から離れる人々から、貸与した資産を全て返却させているか		
8.3 媒体の取扱い				
8.3.1 組織が採用した分類体系に従って、取外し可能な媒体の管理のための手順を実施する。	構築された分類体系に従って、媒体（HDD、USBメモリ、DVD、サーバのDISK装置など）に関する手順を構築することです。 8.2.1と8.2.3が、関連する対策です。 この項は、特に「取り外し可能な媒体」に対してですので、使用方法、使用者登録、暗号化、パスワード、持出、保管、データ復元を不可能にするなど、多岐にわたる管理方法を検討する必要があります。 これらの管理方法を検討して、管理方法を実施することとなります。	分類体系に従った取外し可能な媒体の管理手順が策定されているか		
		上記の管理手順に従って、取外し可能な媒体の管理が実施されているか		
11.1 セキュリティを保つべき領域				
11.1.1 取扱いに慎重を要する又は重要な情報及び情報処理施設のある領域を保護するために、物理的セキュリティ境界を定め、かつ、用いる。	サーバ、情報、製造技術（製造工程）、新規開発製品サンプル、顧客からの預かり品など情報や設備に対して、漏えい、盗難、火災や地震による破損などを起こさないために物理的な対策を講じることです。 設置の基準の例として、 ·ラックなどを設置している部屋は、上階の床下から、現在の床までの壁で囲う。 ·無窓とし、窓ガラスが有る場合は格子を設置し、飛散防止シートを貼る。 ·入室·退室の管理装置を設置する。 ·紙、サンプルなどの保管のため、中が見えない鉄製で、施錠できるロッカーを設置する。 ·敷地に不正侵入されないように外周に侵入センターを設置する。 ·死角や重要な部屋の出入口に監視カメラを設置する。 ·敷地への門や一般訪問者の建物出入口などに受付を設置し、社員や一般者の入門を管理する。 などが、考えられます。 新しいセキュリティ対策機器が、開発されるため、基準も見直していく必要があります。 設備投資がかかる事柄が多く、全てを設置しなければならないものではありません。投資計画に反映しながら、物理的対策を向上させていくことになります。	敷地、部屋、設備に関して物理的なセキュリティ対策を行う具体的な基準を定めているか		
		上記で定めた物理的なセキュリティ対策の基準に基づき、セキュリティ対策機器などを設置しているか		

「情報セキュリティ管理基準」は、業種や規模を問わず幅広い組織が適用できる実践的な情報セキュリティの規範として、国際規格ISO/IEC 27001およびISO/IEC 27002に準拠する形で策定された基準です。このため、簡易診断はISO/IEC 27001とも整合性を持っており、組織が情報セキュリティ体制を国際標準に発展させていくことにもつながります。