テクノファ News

No.150

2021 年 2 月 10 日 発行

1. ニュース･ダイジェスト

より良いコミュニティの構築

環境デザインによる防犯の国際規格（CPTED）が発行されました。

CPTED は、犯罪を減らし、コミュニティでの生活の質を向上させるために広く使用されている都市計画アプローチであり、違反を阻止し、住民の恐怖を軽減するように生活環境を設計するという概念です。

このような概念は 1970 年代から存在し、世界中の多くの防犯戦略で使用され、多くの成功を収めています。さまざまなガイダンスソースが存在しますが、国際的に合意された一連のガイドラインで最高のものをまとめたものは今までありませんでした。

ISO 22341（セキュリティと回復力－保護セキュリティー環境デザインによる防犯のガイドライン）は、特定の種類のテロ攻撃を含む犯罪を減らすための原則、要素、戦略、およびプロセス、新規または既存の都市建築環境における犯罪の脅威に対処します。

住宅地、商業地域、工業団地、教育機関、コミュニティパークなど、あらゆる種類のサイトを対象とするこの規格には、犯罪リスク評価のプロセスと認定されたセキュリティハードウェア製品の適用が含まれています。

規格を開発した専門家でプロジェクトリーダーである HyeonhoPark 博士は、CPTED の原則、概念、および用語を説明する国際的なガイダンスが必要であると述べました。

「十分に計画され、正しく実施されれば、CPTED は費用効果の高い方法でコミュニティの安全性と産業のセキュリティを向上させます」

「さらに、一部の国・地域では、たとえば建築規制の特定のセキュリティ基準を満たすための要件が導入されているため、CPTED の利害関係者と実務家は、基本的な原則、範囲、機関の役割、要素、戦略、およびプロセスを明確に理解することが重要です。」

URL: https://www.iso.org/news/ref2620.html

すべての人のアクセシビリティ

規格開発者向けの人間工学データが更新されました。

世界中で 10 億人を超える人々が何らかの形の障がいを抱えているため、製品、サービス、環境に誰もがアクセスできるようにすることが人権の基本です。その中で規格は強力な役割を果たします。そのため、ISO は ISO / IEC Guide71(規格におけるアクセシビリティ配慮のためのガイド)を開発しました。

Guide71 は、規格の開発者を対象としており、規格を開発または改訂するときにアクセシビリティの問題を確実に考慮するのに役立ちます。アクセシビリティの重要な要素は人間工学であるため、ISO には Guide71 のユーザーをサポートするための人間工学データに関するガイダンスもあり、更新されたばかりです。

ISO / TR 22411（ISO/IEC Guide71 を適用するための人間工学的データ）は、規格開発者が障がい者や高齢者の特性と能力を理解するのに役立ちます。

この技術仕様書は、すべて人間工学研究に基づいた、定量的データと知識だけでなく、および状況やタスクに特化したデータを提供します。データは、加齢の影響および、さまざまなタイプの人間の感覚障がい、身体障がい、および認知障がいの結果に焦点を当てています。

ISO / TR 22411 は、主に規格開発者を対象としていますが、エルゴノミストや設計者が、よりアクセスしやすい製品、システム、サービス、環境、および設備の開発をサポートするために使用することもできます。

この技術仕様書は、現在利用可能な新しく、より詳細なデータで改訂されました。さらに、この新版には、視覚障がいのある読者がよりアクセスしやすいように、図や表の代替テキストが付録に用意されています。

URL: https://www.iso.org/news/ref2612.html

CLEAN GREEN FISH

環境に優しいシーフードの選択は、新しい規格でより簡単になるでしょう。

消費者はよりエコロジカル製品を求めているため、CO^2 排出量を実証することは、競争力を獲得する方法のひとつです。現在、シーフードサプライヤーは、ISO 22948（シーフードのカーボンフットプリント－ナガスクジラの製品カテゴリルール（CFP-PCR））の発行により、まさにそれを行うことができます。

新しい規格では、ISO 14067：2018（温室効果ガス－製品のカーボンフットプリント－定量化の要求事項及び指針）で定義されているシーフードのカーボンフットプリントの計算と伝達に関する製品カテゴリルール（PCR）について詳しく説明しています。これにより、そのような製品の環境への影響をよりよく理解することができ、消費者にもそれを示すことができます。

このドキュメントで概説されている方法論は、ライフサイクルアセスメントと製品のカーボンフットプリントに関する ISO 規格の要件に基づいています。これにより、漁業または養殖から消費に至るまでのナガスクジラ製品のカーボンフットプリントの計算と連携が可能になり、漁業と水産養殖のバリューチェーンの両方から製品に関連することになります。

この規格の普及は、エネルギー消費を削減し、水産業の全体的な環境への影響を改善すると同時に、低炭素製品に対する消費者の需要を高めるための貴重なツールとして役立つことが期待されます。

URL: https://www.iso.org/news/ref2611.html

危険の回避

新しい安全標識の効果的な使用に関する新しい指針

安全標識が紛らわしい世界を想像してみてください。掃除された床を滑って転ぶことから、建設現場での悲劇的な事故に至るまで、誤解される安全標識は災害の元となります。

安全標識については国際的に合意された基準がいくつかありますが、それらが組織のリスク低減プログラムの一部であることを確認することは別の問題です。

新しく公開された ISO / TS 20559（グラフィックシンボル－安全色と安全標識－安全署名システムの開発と使用に関するガイダンス）は、プロセスにある程度の秩序と明確さを与えることにより、組織がまさにそれを行うのを支援することを目的としています。

リスクを低減することを目的としたコミュニケーションシステムを形成するための安全標識の実際の適用に関する推奨事項と説明が含まれています。

このガイダンスは、安全標識に関する国際的に合意された主要な下記の規格を補完するのに役立ちます。

- ISO 3864 シリーズ（図記号－安全色及び安全標識）の設計原則をカバー
- ISO 7010（図記号－安全色及び安全標識－登録安全標識）；
- ISO 16069（図記号－安全標識－安全路の案内システム（SWGS））；
- ISO 23601（安全識別－脱出及び避難計画標識）；
- ISO 17398（安全色及び安全標識－安全標識の分類，パフォーマンス及び耐久性）
- ISO 45001（労働安全衛生マネジメントシステム－要求事項及び利用の手引）

ISO / TS 20559 は、製品ラベルから避難経路の標識、機器のマーキング、標識の配置場所などの理解トレーニングまで、あらゆる種類の標識を対象としています。

URL: https://www.iso.org/news/ref2609.html

気温上昇

気候変動が大変な事態となっています。
しかし、私たちにできることはまだたくさんあります。

2020 年、COVID-19 によってもたらされた世界的な封鎖は、世界が温室効果ガス排出量を削減できることへの希望がありましたが、それは二酸化炭素排出量が多くなるのを止めるのには十分ではありませんでした。

2020 年は、最も激しい荒天が観測されたことを考えると、これは驚くことではありません。東南アジアでの壊滅的なサイクロンと台風、オーストラリアとカリフォルニアでの山火事、中央アフリカでの大洪水は、2020 年の中で記憶に残っていることでしょう。

ニュージーランドは最近、1800 以上の国・地域が参加して「気候非常事態宣言」を作成しましたが、温室効果ガスの排出量を削減し、地球の保護を開始するという政府の手厚い取り組みが見え始めています。

2015 年のパリ協定の 5 周年にあたり、行動を起こさなければならないのは政府だけでなく、個々の組織でもあります。あなたの会社は、環境への影響を減らし、ネットゼロ排出目標に貢献するために何ができるでしょうか？

きれいな緑の文化を育む

組織が環境に与える影響を確実にすることは最優先事項であり、戦略とプロセスのすべての側面で考慮されることは、前向きな変化の良い前兆です。あなたが現在どのように環境に影響を与えているかを知ることは、それがポジティブであろうとなかろうと、資源をより効率的に使う方法とあなたが行う活動のどれが最も悪い影響を与えているかを知るための基礎を提供します。

ISO 14001 などの環境マネジメントシステム（EMS）の基礎は、健全で客観的なプロセスを持っていることです。環境問題を特定、管理、監視、制御する方法を詳しく説明することで、多くの場合、資源のより効率的な使用、廃棄物の削減、管理、汚染の低減、さらにはコスト削減につながります。

また、効果的な EMS は組織横断的なアプローチを採用しているため、ある部門の成果を改善して、別の部門の成果が低下するということはありません。

カーボンフットプリントを計算する

測定できないものを変えることはできませんが、魚をスライスするように、切り分けて考える方法はたくさんあります。国際的に認められている方法論は、年次報告書を読むときに数値が比較可能になり、投資家や利害関係者にとって意味のあるものになるために役立ちます。

そのようなツールの 1 つは、ISO 14064 です。温室効果ガス（GHG）プロトコルに準拠し、ほとんどの GHG プログラムと互換性のある、3 部構成のこのシリーズは、温室効果ガス排出量の定量化、監視、および検証の仕様を示します。

これは、製品のカーボンフットプリントを定量化および報告するための要求事項、および指針を提供する ISO 14067 によって補完され ます。

具体的な行動を取る

組織が環境への影響の観点からどのように進んでいるかを明確にしている場合でも、どのような具体的な行動を取るべきかを知るのは難しい場合があります。フレームワークと一連の指針を持つことは、企業が効果的であるだけでなく、彼らが行うすべての文脈において意味のある行動を特定するのに役立ちます。

ISO 14080（温室効果ガス管理及び関連活動－気候変動対策行動に関する方法論の枠組み及び原理）などの基準は、気候変動との闘いにおいて会社が独自の一貫した比較可能な方法論を開発するのに役立ちます。これにより、目的の達成に役立つアクションとプロセスを特定、評価、正当化することができます。

ISO 14080 は、国連気候変動枠組条約（UNFCCC）や世界銀行などの主要な組織の意見を取り入れて開発されいるため、国際的な取り組みや目的に整合しています。

エネルギー効率を高める

組織が使用するエネルギーの種類と量は、CO^2 排出量に大きな影響を与える可能性があります。しかし、どこから始めればよいのでしょうか。

エネルギーを効率的に使用するためのいくつかの適切なポリシーを設定することは良いことですが、そのためには測定可能な明確な目標と信頼できるデータを生成する方法が必要です。また、改善のために絶えず見直す必要もあります。

それがすべて重く聞こえる場合は、それを実行する方法に関する明確なプロセスとガイドラインが役立つ可能性があります。例えば、ISO 50001（エネルギーマネジメントシステム－要求事項及び利用の手引）は、そのようなポリシー、測定、継続的改善をカバーするエネルギーマネジメントシステムを確立する方法を詳しく説明しています。また、スタッフ、クライアント、投資家、その他の利害関係者に、エネルギー効率をどれほど真剣に受け止めているか、そして適切なポリシーが実施されていることを示す方法でもあります。

よりクリーンでグリーンな未来に投資する

低炭素経済への移行、ひいてはより持続可能な未来の創造は不可欠ですが、簡単ではなく、多くの公的および民間投資が必要になります。その投資の一部は、「グリーン」ボンドの形で投資家に販売される債務として発行されます。そのような債券の発行者が信用できることを保証し、彼らが行う環境上の約束を果たす能力について評価されることが重要です。

ISO は、グリーンボンドが実際に何であるかを明確に定義し、プロジェクトと資金調達のための資産を指名するための要件を指定し、適格性、収益の使用と開示要件を指定し、保証オプションを説明することによって、この市場を後押しするのに役立つ一連の国際的に合意された標準に取り組んでいます。

ISO 14030 シリーズとして知られるこの基準は、債務を発行する者、それらを販売する引受人、発行者の信用力と環境上の利益に基づいて決定を下す投資家、およびそのエリアで法律を策定する際の政策立案者が使用することを目的としています。

しかし、これは ISO が行っていることのほんの一部です。現在、国連の持続可能な開発目標（SDG）13：気候変動対策に貢献する 732 の基準があります。

詳細については、標準と SDG13 および地球の保護に関する専用ページ（https://www.iso.org/sdg/SDG13.html）をご覧ください。

URL: https://www.iso.org/news/ref2607.html

WHAT A GREAT IDEA

発表されたばかりのイノベーションにおける知的財産を保護するための新しい基準。

オスカー・ワイルドは「模倣が最も誠実なお世辞になる」と言いました。しかしビジネスにおいては、競争相手があなたのやり方を真似て、先を行こうと逃げるようとするならば、それは慰めにはなりません。

今日の知識ベースの経済において世界規模でますます重要になっている知的財産（IP）は、あらゆる種類の組織にとって重要です。IP は、そのアイデアを「所有」して保護することができるからです。IP を活用して、投資の誘致と確保、競争優位性の向上など、多くのビジネス目標を達成できます。

イノベーションプロセスのすべてのステップで IP を管理することは、ビジネスとして理にかなっており、創造性を高めることができる真のインキュベーターを生み出すのに役立ちます。

ISO 56005（イノベーションマネジメント－知的財産管理のためのツールと方法－ガイダンス）は、組織が最良のアイデアを保護し、最大化するのに役立つガイドラインと戦略を提供します。

この規格は、IP マネジメントフレームワーク、リスクマネジメントツール、および IP 活用のための方法などを備えています。

これは、イノベーション管理に関する ISO 56000 シリーズで公開されている最新の規格です。

・ISO 56000（イノベーション・マネジメント－基本及び用語）
・ISO 56002（イノベーション・マネジメント－イノベーション・マネジメントシステム－手引）
・ISO 56003（イノベーション・マネジメント－技術革新協調のためのツール及び方法 －ガイダンス）
・ISO / TR 56004（イノベーション・マネジメントアセスメント－ガイダンス）

現在開発中のシリーズの他の標準は次のとおりです。（※2）

・ISO 56006（ イノベーション・マネジメント－戦略的諜報管理のためのツールと方法–ガイダンス）
・ISO 56007（ イノベーション・マネジメント－アイデア管理のためのツールと方法–ガイダンス）
・ISO 56008、イノベーション・マネジメント–イノベーション運用測定のためのツールと方法–ガイダンス

URL: https://www.iso.org/news/ref2605.html

KEEPING AN EYE ON INFORMATION SECURITY

IS ガバナンスの規格が更新されました。

企業の情報をデータ侵害やハッキングから保護することはますます複雑になり、多くの場合、それを正しく行うために多くのシステム、ツール、および人員が関与することになります。ただし、システム全体が効果的に管理されていない場合、機能するものと機能しないもの、およびすべてが組織構造と戦略にどのように適合するかを可視化するために、世界で最善の努力を尽くすと失敗につながる可能性があります。情報セキュリティ（IS）ガバナンスに関する国際的に合意された規格が改訂されました。

ISO / IEC 27014（情報セキュリティ, サイバーセキュリティ,プライバシー保護－情報技術のガバナンス）は、組織が ISO / IEC27001 に基づく情報セキュリティマネジメントシステム（ISMS）を評価、指示、監視、および伝達できる、情報セキュリティのガバナンスの概念、目的、およびプロセスに関するガイダンスを提供します。

規格を開発した専門家の ISO と IEC の合同ワーキンググループのコンビーナである Edward Humphreys 博士は次のように述べています。

「ISO / IEC 27014 のこの新版は、ISMS の適用範囲に組み込まれた情報セキュリティガバナンス活動の基本であり、組織全体のガバナンスのコンテキストであるため、ISO / IEC 27001 の重要なコンパニオンです。」

この規格は最近更新され、明確さと構造が改善され、新しい情報が追加されました。これは、ISO / IEC 27001（情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－要求事項）に準拠していると同時に、組織のより広範なガバナンス要件にも関連しています。

ISO / IEC 27014 には、同じ専門家委員会によって現在開発されている情報セキュリティに関する他のいくつかの規格が加わります。これらは

（※2 現在開発中のため、タイトルの和訳は仮で記載しています）
・ISO / IEC 27002（情報技術－セキュリティ技術－情報セキュリティ管理策の実践のための規範）
・ISO / IEC TS 27110（情報技術－サイバーセキュリティおよびプライバシー保護–サイバーセキュリティフレームワーク開発ガイドライン）

・ISO / IEC TS 27100（情報技術–サイバーセキュリティ–概要と概念）
・ISO / IEC 27005（情報技術―セキュリティ技術―情報セキュリティリスクマネジメント）

URL: https://www.iso.org/news/ref2604.html

環境の実態を正しく理解する

環境への影響を減らすことは、私たちが実際に環境に与える影響を測定することから始まります。環境情報を評価および検証するための ISO シリーズの主要な規格が改訂されました。

組織は、意思決定を導き、国の規制やインセンティブスキームを満たすために、ますます環境情報に目を向けていますが、そのためにはデータを検証し、信頼できるものにする必要があります。

ISO 14065（環境情報を妥当性確認及び検証する機関の一般原則及び要求事項）は、環境情報ステートメントの検証と検証を実行する機関の原則と要件を指定します。
以前は主に温室効果ガスの排出に焦点を当てていたこの規格は、温室効果ガスの声明、カーボンフットプリント・ウォーターフットプリント、環境ラベルの主張、CSR 報告書、グリーンボンドやその他の金融商品に関連する情報など、あらゆる形態の環境情報をカバーするように強化・改訂されました。
この規格は ISO / IEC 17029(適合性評価－妥当性確認機関及び検証機関の一般原則及び要求事項)に整合しており、プログラムの所有者、規制当局、認定機関、検証機関の能力を評価し、認識するための基礎を提供します。

URL: https://www.iso.org/news/ref2600.html

マネジメントシステム関連

ISO 14009:2020
（環境マネジメントシステム－設計と開発に材料循環を組み込むためのガイドライン）
【発行】2020 年 12 月 21 日
ISO 14065:2020
（環境情報を妥当性確認及び検証する機関の一般原則及び要求事項）
【発行】2020 年 12 月 1 日
ISO/IEC 27014:2020
（情報セキュリティのガバナンス）
【発行】2020 年 12 月 15 日
ISO/PAS 45005:2020
（労働安全衛生マネジメント－COVID-19 パンデミック下の安全な労働のための一般指針）
【発行】2020 年 12 月 15 日
JIS Q 21503:2021
（プロジェクト,プログラム及びポートフォリオマネジメント－プログラムマネジメントの手引）
【発行】2021 年 1 月 20 日
ISO 9000 及び ISO 9001 のシステマティックレビュー・今後の道
https://committee.iso.org/sites/tc176/home/news/content-left-area/news-and-updates/add-a-post-11.html

環境法規関連

労働安全衛生法施行令・労働安全衛生規則（改正）～ベンジルアルコールの追加～
【2020/12/2 公布・2021/1/1 施行】
ラベル表示、SDS 交付、リスクアセスメントを義務付ける物質に「ベンジルアルコール」を追加
https://www.technofer.biz/w1803/index.php/2020/12/02/post-6674/
水質汚濁防止法施行令（改正）～民泊事業者のちゅう房施設等を除外～
【2020/12/18 公布・12/19 施行】
旅館業のうち住宅宿泊事業に該当するものの用に供するちゅう房施設等を「特定施設」から除外
https://www.technofer.biz/w1803/index.php/2020/12/18/post-6770/
2019 年度の温室効果ガス排出量（速報値）～6 年連続減少
【2020/12/8 公表】
https://www.technofer.biz/w1803/index.php/2020/12/08/post-6725/
2019 年度の産業廃棄物の不法投棄等の状況
【2021/1/8 公表】
ピーク時（平成 10 年代前半）からは大幅に減少しているが、跡を絶たない状況
https://www.technofer.biz/w1803/index.php/2021/01/08/post-6886/

詳しくは弊社運営サイト「環境法規制 改正情報サイト」をご確認ください。
https://www.technofer.biz/w1803/
QR コードからもアクセス可能です。

2. 第 4 回 TF ニュース勉強会

「中小企業における情報セキュリティ対策の在り方」

加藤 道明 氏
・ローブライトコンサルティング株式会社 代表取締役
・株式会社テクノファ主任講師
ISMS リスクアセスメント有効活用コース
ISMS 監査・審査のための管理策の理解向上コース 担当

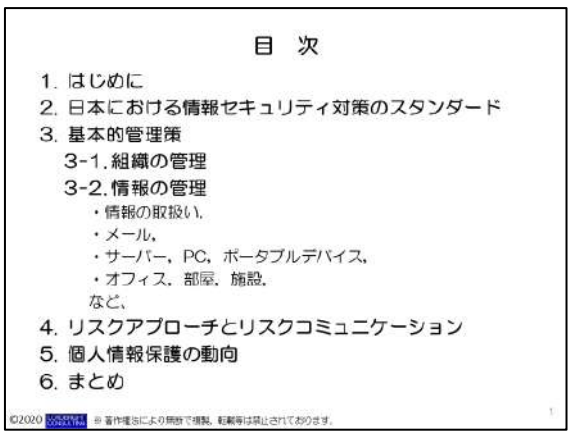
今回はテクノファの各種 ISMS セミナーの講師を長く担当し、また、日本の ISMS 黎明期から ISMS に携わり、主任審査員を務めている加藤様にお越しいただき「中小企業における情報セキュリティ対策の在り方」というテーマでご講演をいただく。

はじめに

ニュースの話題から入りたいが、ゲーム大手カプコンが 2020 年 11 月にランサムウエアで被害を受けたというニュースがあった。一部報道によるとランサムウエアの被害に遭い脅迫された企業の半数以上が身代金を支払っていたという。このような昨今の情報セキュリティに関する現状を共有したうえで本日の内容に入っていきたい。

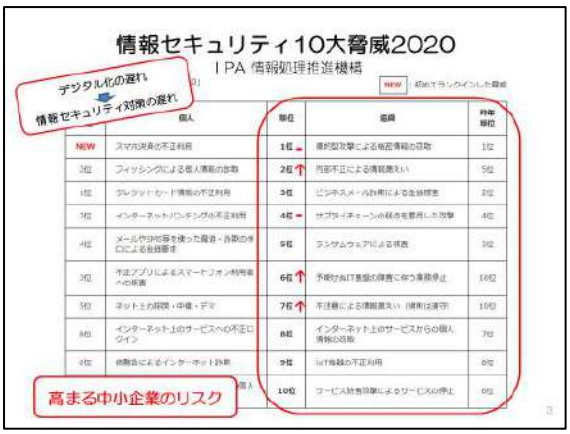
今や日本における情報セキュリティ対策は、ISO/IEC 27001 がベースになっていると言っても過言ではない。認証取得は 6,000 組織を超えたところで決して多くはないが、数々のガイドラインのベースが ISO/IEC 27001 をベースとしており、社会的には十分に認知されたと言えよう。また、今月 2020 年 12 月から ISO/IEC 27701（プライバシー情報マネジメントシステムのための ISO/IEC 27001 及び IEC/ISO 27002 への拡張 – 要求事項及び指針）を基準としたプライバシー情報マネジメントシステム（PIMS）の認証が始まった。新たな個人情報保護の在り方と考えてよい。本日はこの情報を含めてお伝えしたい。

本日の内容は下記の通りである。



ISO/IEC 27001 では、“管理策”という ISO 9001（QMS）や ISO 14001（EMS）では見られないものが入っている。また、リスクアプローチについて具体的な手法を要求しているのも ISO/IEC 27001（以下、ISMS と呼ぶ。）の特徴であろう。

では、はじめに、IPA（独立行政法人情報処理推進機構）「情報セキュリティ 10 大脅威 2020」（※3）から紹介したい。



IPA（独立行政法人情報処理推進機構）「情報セキュリティ 10 大脅威」とは、毎年、1 年間に発生した社会的に影響が大きかったと考えられる情報セキュリティにおける事案から、IPA が脅威候補を選出し、情報セキュリティ分野の研究者、企業の実務担当者などが審議・投票を行い、決定したものである。セキュリティ対策の普及を目的とした資料であり、同機構は、各企業・組織の研修・教育等に活用することを勧めている。左側の欄が個人への注意喚起、右側の欄が企業・組織への注意喚起である。。

この国におけるデジタル化（DX（デジタルトランスフォーメーション））の遅れ、ということについては政府の動きが加速していくと考えている。例えば今回のコロナ禍の中で、今どき FAX を使っているのは日本くらい、と騒がれたことをご記憶の方もいよう。一方で、紙で仕事を行っているうちには問題とはならなかったことが、電子化されることで問題になる部分もある。情報セキュリティも重要な課題となる。

では、「情報セキュリティ 10 大脅威 2020」について、具体的な説明に入っていきたい。右側の組織への注意喚起の中で、今、特に知っておいて欲しい 4 つについて説明する。

(※3) 2021 年 1 月 27 日に 2021 年版が公開されています

まずは、「**標的型攻撃による機密情報の搾取**」について説明する。
これは、偽メールを送り付け、偽サイトに誘導するなどし、ID やパスワードなどの情報を窃取するものである。例えば、銀行名で送られてきたメール。素人がパッと見ただけでは、本来の自分が利用している銀行なのか、偽メールなのかわからない。そのような中で、中小企業でも対策が取られるようになって来ている。
ISMS 審査の中で、よく目にする対策例としては、社内の IT スタッフが全社員に偽メールをわざと送り、受け取った社員側が偽メールを開かないかどうかをチェックする、という取り組みがある。

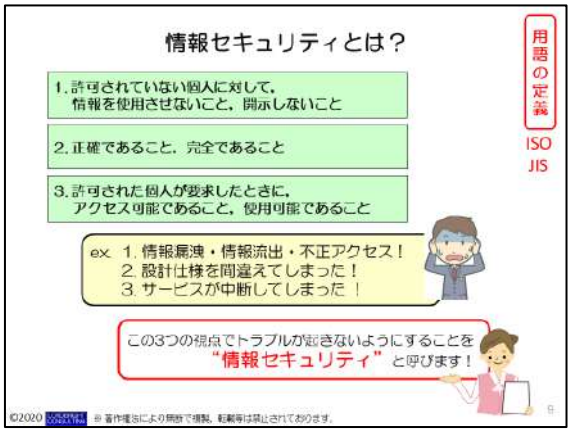
次に、「**内部不正による情報漏洩**」について説明する。
これは、文字通り、内部の者による情報漏洩である。それ以上の説明は必要ないであろう。企業に対する被害が顕在化し、持ち出した個人や持ち出した情報を無断使用した企業を相手取り損害賠償を裁判所に申し立てるというのが一般化しつつある。

次は、「**サプライチェーンの弱点を悪用した攻撃**」について説明する。
特定の業務を外部組織に委託している場合、業務委託先がセキュリティ対策を適切に実施していないと、業務委託元への攻撃の足がかりとして狙われる。セキュリティ対策を適切に実施していない業務委託先を狙って、そこから業務委託元の情報を盗み出す。業務委託先の問題意識が希薄であることを、国側も心配している。

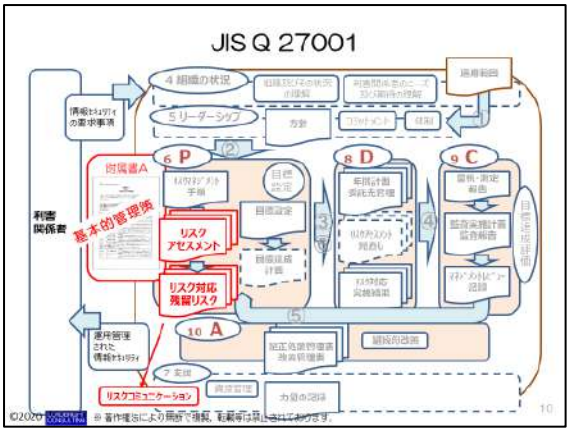
最後に、「**ランサムウエアによる被害**」について説明する。
感染すると、PC やサーバーに保存されているファイルを利用できない状態にされる。復旧と引き換えに金銭を要求される。冒頭に述べた被害である。被害に遭い脅迫された企業の半数以上が身代金を支払っているという事実を受け止めなければいけない。目の前の問題を手っ取り早く解決するために、支払い出来る額の請求なら払ってしまえ、という判断をしてしまう企業が意外とあるということである。

それでは、「日本における情報セキュリティ対策のスタンダード」について話しを進めていきたい。

日本における情報セキュリティ対策のスタンダード

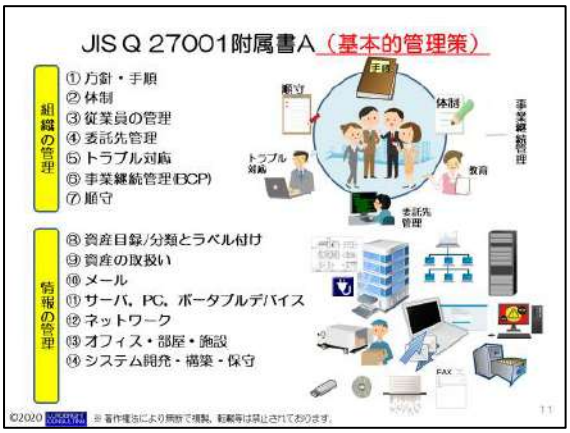


スライドの通り、3 つの視点でトラブルが起きないようにすることを**“情報セキュリティ”**と呼ぶ。一方で、ISMS の認証取得組織のレベルであっても、情報漏洩対策のみにとどまっているケースがある。仕事を正確にできない社員に、情報漏洩しないようにと言っても、いかがなものだろう。精神論ではなく、まずは正確に・定めた手順通りに仕事が出来る社員を育てる、そこまで含めて考えていかなければならない。



このスライドは ISMS の全体像・流れをイメージにしたものである。情報セキュリティを目的とした PDCA サイクルである。
ISMS では、朱色の部分をしっかり理解する必要がある。朱書きの部分では、基本的管理策の選択とリスクアプローチおよびリスクコミュニケーションが要求されている。この部分が「よくわからない」という方が多い。ISMS では、リスクはゼロにはならないということを前提にしている。セキュリティリスクをゼロにするということは、業務を止めるまたは組織を解散するということであり、一般的にはあり得ない。リスクを出来るだけ小さくし、リスクと付き合って行くということを考えなければならない。今回は、この部分に絞って、以降説明する。尚、その他の要素は QMS や EMS と同じと理解してよい。

基本的管理策



このスライドは、ISMS の附属書 A に記載されている基本的管理策をイメージにしたものである。上記に示す「組織の管理（①～⑦）」は、企業であれば、レベル差があるとしても、何かしらあるであるはずである。ゼロからではなく、この規格を利用し、点検すればよい。「情報の管理（⑧～⑭）」という部分

が ISMS においては特徴と言える部分になる。研修を受けに来られる方からは⑫のネットワークが難しい、とよく聞く。また⑭のシステム開発もハードルが高い。一方で、前述で紹介した脅威・被害は、むしろこれらの管理策の不備によるところが大きい。⑫、⑭がこの先の日本における大きな課題になると考えている。

では、基本的管理策の中身に入っていく。ここでは、勘違いしがちな点を中心に説明する。

上記スライドの「組織の管理」から説明する。

組織の管理

①方針・手順

これは社則、就業規則の延長と言える。多くの会社では、社則とは別立てにして、例えば"情報セキュリティ規程"という規定集を作っている企業が多い。ポイントは、社会の状況や自組織に変化があった場合、見直すことである。例えばランサムウエアによる被害などは数年前まではさほど問題になっていなかった。新たな脅威に対応できるよう見直しが必要になる。10 年前と同じ規程のままという組織に高い確率で遭遇するが、これは情報セキュリティ対策の在り方に反している。

研修会の受講者から「見直す事項がなくなって困っている」という話をよく聞く。前述で紹介した IPA が発信している情報に基づく見直しと点検は最低限行ってほしい。発信している内容には、必ず変化があるので有効活用してほしい。

また、規定した事項を関係者に周知するということは言うまでもない。

②体制

情報セキュリティでは、大多数の組織が社長をトップと定め対応している。法令によっては、違反時の処罰対象を組織の代表者としている影響もある。つまり、情報セキュリティ対策は、社員の問題というより経営陣の問題ということになっている。

次に、専門組織との連絡体制の構築が求められている。例えば、社内にランサムウエアのことが分かる人材がいなければ対策の取りようもない。まずは、情報の入手先として IPA を勧めている。また、少なくとも一人は IPA が発信していることを理解できる社員の育成をお願いしたい。ここに力を入れておらず、対策が出来ていない組織が目立つ。

その他、前述で紹介したランサムウエアによる被害など、身代金を要求（脅迫）された場合等は、警察への連絡も必要となる。問題が起きてからどこに連絡するか調べるのではなく、最低限、いざというときにどこへ連絡するか、具体的な連絡先一覧等を整備しておく必要がある。

③従業員の管理

ここでは、採用時／雇用中／離職・退職時といった３つの場面で留意すべき事項を求めている。採用においては、リスクに応じて関連する法規制や倫理に従い、採用希望者の履歴などを確認することを求めている。昭和の時代は日本でも大手企業を中心に素行を含め採用希望者のことを調べていた。しかし今は労働関連法令または個人情報保護法により、候補者の履歴確認には限界がある。ISMS のベースが英国であり、日本にはなじまない部分といえる。日本では「役員による面接等でチェックを行っています。」と答える組織が多い。

雇用中については、教育・訓練が中心になる。

離職・退職時の対応とは、組織に在籍中に知った情報は漏らさない、という誓約書を交わすことが一般的になった。

④委託先管理

過去、委託先も法人であり、委託先での不祥事の責任は委託する側にはない、という考えが一般的であった。しかし、現在の個人情報保護法では、委託する側の責任も求めている。委託する側による委託先の監視が求められている。委託先を訪問監査する組織も増えている。訪問監査までは出来ないとしても、チェックリストを渡し自己申告してもらう、という委託先の監視は広がりをみせている。

⑤トラブル対応

審査で必ずチェックするのがエスカレーション。現場で問題が起きた場合、上司に速やかに情報が伝わるかどうか。緊急連絡網が存在するのか、機能しているのかをチェックする。

忘れられがちなのが再発防止（是正処置）である。情報流出を繰り返す組織も散見される。情報セキュリティ対策は精神論ではうまく行かない。トラブルの原因を個人の理解不足とするのではなく、担当が変わっても再発しないような仕組みを取り入れることが必要となる。例えば、メールの誤送信の再発防止策として、クラウドを利用し、メールの利用を減らす企業が増えている。

⑥事業継続管理（BCP）

まず、BCP とは何だろうか。完全復旧の手順や設備を BCP と考えている組織が後を絶たない。ISO 22301（BCMS：事業継続マネジメントシステム）という規格がある。その規格を基準とするならば、それは少し違う。完全復旧は BCP の最終プロセスでしかない。バックアップシステムやシステム二重化などを提案したい、利害関係の中で偏った解釈が広まってしまったようだ。BCP とは、通常の活動が出来ない状況下に陥った際、何を優先し、それをどこまで行うかを決め、その為に何を準備し、どのように行うかといった手順を、あらかじめ検討立案し、定期的に演習し、有事に備えることである。その点を理解してほしい。今、コロナ禍の中で、各企業が取り入れているテレワークも立派な BCP と言える。また、BCP として、安否確認を PR する組織がある。その場合であっても電話番号等連絡先が最新であるか、連絡が着くか、定期的に演習して欲しい。

⑦順守

これには、法令順守と社内ルールの順守がある。審査では、不正アクセス禁止法、不正競争防止法、個人情報保護法、著作権法の４つが特定されていることを、必ずチェックされる。留意したいのが、これらの法律は毎年のように改正されることである。タイムリーに改正を把握し見直しを行って欲しいところだが、最低限、年に１度、改正されていないか確認し、必要に

応じて見直しを行って欲しい。その他の法令については組織の方で重視しているものを特定すればよい。

また、社内ルールの順守については内部監査とマネジメントレビューで充分に対応できる。

ここまでが「組織の管理」である。続いて「情報の管理」について説明する。

情報の管理

⑧資産目録／分類とラベル付け

資産とは、主に業務で取り扱う情報と情報を取り扱うために必要なハードウエア、ソフトウエア、設備などがそれにあたる。それらを棚卸し、台帳化するのが一般的である。それらを台帳化したら、情報を分類、例えば、社外秘かそうでないかを仕分けし、社外秘であることがわかるようにラベルを付け、また、それら情報にアクセス出来る従業者を設定する。情報セキュリティ対策は、どういう情報があるのか、どういうハードウエア、ソフトウエア、設備があるのかを把握し、管理することから始まる。

⑨資産の取扱い

資産を棚卸し、台帳化したら、次は、それら資産の取扱いについて、ルールを定める。対象は、社外秘のものになるであろう。例えば、社外の印刷物は鍵付きキャビネで保管する、などである。

暗号化については、ISMS 認証制度が始まった頃は、そこまでやる必要があるのか、と反発する組織もあったが、今ではメール添付ファイルの暗号化など、暗号化が身近な時代となった。

⑩メール

ISMS では、メールについてそれほど多くのことが言われているわけではない。宛先の確認、パスワード付き添付ファイルなどが主要な事項となる。また、メールを交わす相手との機密保持契約も忘れてはならない。

既に紹介したが、メールの誤送信防止策として、クラウドを利用し、メールの利用を減らす企業も増えている。ISMS を取得する組織にマザーズ上場の企業が増えているがそれらの企業ではチャットシステムの活用が広がっていると感じる。定められた人のコミュニティであれば誤送信のリスクを下げられる。

あと、パスワード付き添付ファイルについて、メール送信時に同時にパスワードが自動で生成され、同じ送信先に別途パスワードのみ送信される仕組みを取り入れている組織が多いが、これは止めよう、という流れが起きている。パスワードまで誤送信先に送ってしまっては暗号化する意味がない。

⑪サーバー、PC、ポータブルデバイス

パスワード管理は中小企業でもできていると感じる。Windows アップデートを知らない人はいなくなったと言ってもよい時代になったと思っている。ただし、Windows10 におけるアップデートは、これまでの Windows とは異なる部分も多い。自動で更新される更新プログラムもあるが、マニュアル操作が必要な更新プログラムもある。また、Microsoft Store でのダウンロードと更新も忘れてはならない。一度、見直しすることをお勧めする。

テレワークについては情報セキュリティを考慮したルール化と周知徹底が必要である。しかしながら、コロナ禍で急遽テレワークを導入した組織も多く、現在、どの企業も試行錯誤中であると感じる。今後、有効な管理策が続々と出てくるであろう。

⑫ネットワーク

情報セキュリティにおいて、内部犯行を除けば、ネットワーク、特にインターネットのリスクが最も高い。今は、通信機器に装備されたファイアウォールを管理し、簡単には侵入出来ないようにするのが一般的である。しかしながらこれも完ぺきではない。24 時間監視している組織はまだまだ少ない。米政府が企業に対し情報管理を厳しく要求する中、政府もこの点を気にしはじめている。不正アクセスを 100%回避することはできない。不正アクセスをいかに早く見つけ、ふさぐかが、被害を最小限にするといった意味で重要になる。とはいえ、正直、24 時間監視するとなると、コストもかかり、まだまだハードルがあるのも事実だと思う。もっと安く監視ができるようになる時代が来ることも待ち望んでいる。

⑬オフィス・部屋・施設

来客者の入退管理はもちろん、従業者の入退管理は基本中の基本。ただし、必ず電子錠が必要ということではない。最低限、いつ誰が出入りしたかの記録が残るようにすればよい。サーバー室や執務室などにセキュリティレベルを設定し、入退室の記録を手書きで台帳に記録するところから始めるのもよい。

また、中小企業であってもサーバーに UPS（無停電電源装置）はつけて欲しい。それにより停電等で電源供給がなくなってもサーバーをシャットダウンする時間がかせげ、データの損傷を防ぐことが出来る。サーバーの復旧というロスを無くすことが出来る。UPS も昔に比べて格段に安くなっている。通販でも購入出来る。取説をみて設置すれば悩むほどのコストはかからない。

⑭システム開発・構築・保守

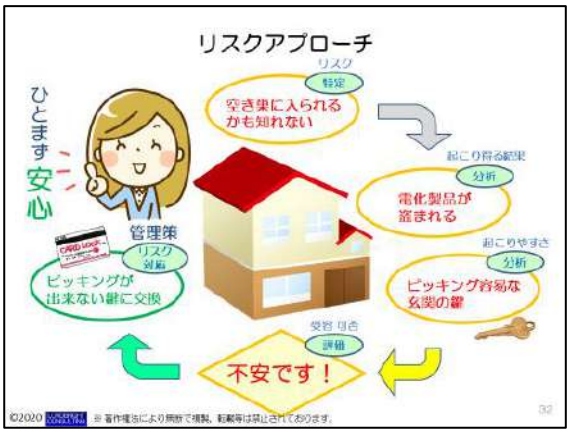
昨今、世間を騒がせている不正アクセスは、システム開発でのセキュリティ対策の不備によるところが大きい。実際、システムを開発する側、開発を委託している側問わずセキュリティ設計をどの程度やっているのか、そして、どのような残留リスクがあるのかを説明できる組織が少ない。そもそも、この国にシステムのセキュリティ設計が出来る SE はそう多くはない。これまでセキュリティに投資する企業も少なく、システムを提供する側もセキュリティの専門家を育成して来なかった。日本の課題ともいえる。これは、国も把握している。不正アクセスの事案が増え、企業に与えるダメージも大きくなる中で、どのように専門家を育てて行くか、教育をして行くか、今後の動向に留意したい。

「情報の管理」の説明は以上である。

次のスライドでは、ISMS を取得している組織での管理策のレベル差を示す。

ISMS では、管理策のレベルを要求していない。あくまで、管理策の視点である。どのレベルの対策を導入するかは、組織が決めることになる。上記スライドに示すベースラインで ISMS を取得する組織もある。高度なセキュリティ対策を施してから、審査を受けるという組織もあるが、まずは、ベースラインで審査を受けるということでも構わない。そうすることにより、中小企業でも大きなコストを抱えることなく認証を取得できる。「電子錠を付けないと認証取得できない。」とコンサルから言われたという話しを聞いたことがあるがそれは間違い。前述でも述べたように、まずは、台帳管理でも構わない。ISMS はマネジメントシステムであり、管理策も PDCA サイクルを回しながら、必要に応じて見直して行くものであることを理解して欲しい。

リスクアプローチとリスクコミュニケーション



このスライドは、リスクアプローチを教育するにあたり開発したスライドであり、研修をはじめ各所で使っているが好評。これがリスクアセスメントである。この例は、筆者自身が体験した事例であり、自宅での防犯対策を、ISMS に当てはめて整理しただけである。これで ISMS が要求するリスクアセスメントの要素を満たしている。組織では、対象を業務にし、どのようなリスクがあり得るか、洗い出し、特定して行けばよい。また、リスクは組織の事業や業務によって違ってくる。ISMS を取得した他社のリスクアセスメント結果を流用し、審査を受けてもうまく行かない。例えば、テクノファのような研修機関と大手銀行で、リスクが同じということはあり得ない。テクノファよりも銀行の方がより高いリスク対応が必要であろうことは容易に想像できるだろう。つまり、セキュリティでは、標準化よりも最適化、事業や業務、さらには事業規模に合った対策が必要ということである。

また、リスクコミュニケーションを忘れてはいけない。業務担当者と管理者でリスクに関する情報、特に残ったリスクを共有することが大事である。日本では、個人に依存した業務が多く、管理者が残ったリスクを知らないまま、業務が行われていることがある。現場の業務には例外が付きものである。残ったリスクは、必ず業務担当者と管理者で共有するようにして欲しい。業務担当者を管理者では決裁権も違うため、共有することで、また違ったリスク対応になることもある。

個人情報保護の動向

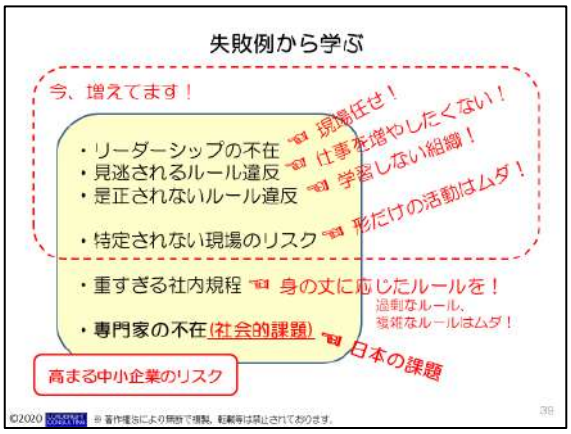
最後に、個人情報保護の動向に触れる。

2003 年に成立した個人情報保護法。この法律に基づき、個人情報保護ガイドラインがあり、それをサポートするのが JIS Q 15001 である。その認証制度としてのプライバシーマークが国内で普及し、現在 16,000 社を越える企業が認証取得している。そのような中、2019 年に ISO/IEC 27701（プライバシー情報マネジメントシステムのための ISO/IEC 27001 及び IEC/ISO 27002 への拡張 – 要求事項及び指針）という規格が制定された。また、今月 2020 年 12 月から一般社団法人情報マネジメント認証センター（ISMS-AC） によるプライバシー情報マネジメントシステム（PIMS）の認証が始まった。これは ISMS のアドオン認証。つまり ISMS の認証取得組織を対象に展開される。PIMS は、EU が 2016 年に発行し、2018 年適用開始した「EU 一般データ保護規則」（通称：GDPR）がベースとなっている。EU の GDPR 適用開始に伴い、日本の個人情報保護法もこれに準拠する方向になっている。自分の所属する審査機関も取り組む予定であり、現在、審査員の教育を行っている。

最後に

ISMS の認証制度において不正アクセスなどのセキュリティ事故をきっかけに認証停止になる組織が出ている。しかしながら、事故を起こしたから認証停止という訳でもなさそうだ。規格要求にあるリーダーシップや不適合の是正処置の適合性に課題がある組織は要注意である。また、内部のシステムであるか顧客向けシステムであるかを問わず、システム開発・運用・保守に関する規格要求への適合性についても今一度確認されることをお勧めする。

（次ページへ続く）



ISMS の認証制度が始まり 19 年、中小企業を中心にスライドの上の部分（点線枠）が増えてきているように感じる。リスクは下げることはできてもリスクをゼロにすることはできない。事故が絶対起きない組織などない。既に ISMS を取得している組織であれば、少なくとも、事故が起きても認証停止には至らないよう、規格要求事項は死守して欲しい。尚、ISMS では要求事項の除外を認めていない。組織の都合・判断で採用しないということは認められていない。また、認証を取得していない組織においては、リスクを下げるため、いざというとき、組織へのダメージを少なくするため、できる範囲の中で ISMS に取り組むことをお勧めする。

＜質疑応答＞

Q1：中小企業にとって認証取得の価値はどのように考えればよいか。

A1：ISMS に抵抗感を感じる経営者が多いようにみえるが、審査の現場では経営者から次のような声が多く聞かれる。
・社員の意識が変わった
・外部の方が年に 1 回来ることにより社内に刺激を与えることができている

Q2：法規制対応は大切なことであることは誰もが分かっているが実際の運用上ではいかがであろうか。

A2：近年は朝令暮改、法令が毎年のように変わる。そのためか法令順守が十分できていることを説明できる企業には残念ながらあまり遭遇しない。大変ではあるが、学習する姿勢がとにかく大事。これも完璧にはできないが、学習することでリスクを減らすということにつながる。

Q3：中小企業にとっての認証取得のハードルについて

A3：「管理策の事例」というタイトルのスライドで挙げたベースライン（赤枠内）でも ISMS を取得できる。プライバシーマークはやさしく、ISMS は難しいというのは誤解である。むしろ、ISMS の方が対策に幅を持てる。教育機関としても頑張ってほしい。自身が講師を務める講習会を受けるだけでコンサルタントに頼らずに認証取得ができたと言ってくださる受講者がいらっしゃった。大変ありがたい。

Q4：クリアデスクについて

A4：ISMS にしっかり取り組んでいる企業の机の上は本当にきれい（きれいにするのに 3 年程度かかる組織もあるが）。この話は、情報セキュリティというよりも躾。整理整頓の話し。近年は、スーツにネクタイを要求するよりも、職場の整理整頓を要求する企業が多いように感じる。

Q5：ISO 9001 の認証停止の話はあまり聞かない。ISMS で停止はそれなりにあると聞いて驚いた。もう少し状況を聞きたい。

A5：この数年、聞くようになった。1 つの審査機関で数社停止という話もある。停止になると隠すことは出来ず、組織の取引に影響を与えるはず。ISMS の取得が契約条件になっている組織も多い。認証停止についてもう少し話すと、そのきっかけは不正アクセスである。社会的問題を起こした企業に関する報道を耳にしたことがあると思うが、その企業が ISMS を取得している場合、当該審査機関として、事情を聞きに行かなければならない。しかし、説明した通り事故イコール認証停止という訳ではないようである。リーダーシップの不在や運用においてインシデントの発生時、修正のみが行われ是正処置（再発防止）が行われていない場合、認証停止になっているようである。マネジメントシステムの要求事項を満たしていない、有効でない、という判断である。

Q6：お客様から情報漏洩の覚書などを求められるケースが増えているが、それに伴うリスクについて、ISMS を取得すると何か変わるのだろうか。

A6：ISMS において、リスクコミュニケーションが求められている。しかし、何でも全てトップに上げよ、ということではなく、セキュリティ事故が起きたとき、当該担当者や管理者レベルではどうにもならないようなリスクについてトップとリスクコミュニケーションすることを求めている。その上でトップを含めリスク対応を図るとよい。

Q7：リスクコミュニケーションについて東京証券取引所やゆうちょの事故から考えると、トップの説明内容で気になる部分があった。気を付けるべきことは何であろうか。

A7：菅内閣も説明責任を果たしていない、という批判があるが、わざと説明していない、という説もあるように、日本には無難に目的を果たすためにわざと説明をしないこともあるように見受けられる。しかしながら、多くの場合、トップがよく理解していないように見える。西洋生まれの規格ということもあり、そこを突いている。トップは、現場が抱えているリスクを適宜認識しておくことが大事であろう。

以上

3. Zoom/Teams を使用したライブ配信セミナーのお知らせ

今人気の**オンライン**（Web）セミナーは[こちら]。

【内部監査員コース】

ISO 9001 内部監査員 2 日間コース（QN31）

ISO 14001 内部監査員 2 日間コース（EN31）

【JRCA 登録 CPD コース】

平林良人によるマネジメントシステム活用のヒント（MD02）

ISMS 審査員補【2020 年度-情報セキュリティと暗号】（JD27）

事業プロセスと統合したマネジメントシステム構築の手引き（MD26）

講師派遣型（出張）コースも
オンライン（Web セミナー）で承ります。
Zoom だけでなく **Teams** も対応可能です。

複数の MS 審査員 CPD を満たす JRCA 登録 CPD コース　オンライン（Web）セミナー

NEW!!

事業経営に役立つ内部監査へ－内部監査事務局にできること、なすべきこと－（MD27）
※QMS/EMS/ISMS/FSMS/OHSMS 対応　JRCA 登録 CPD 研修コース

ISO 9001/14001 運用と審査の肝～発想を変える～（QE83）
※QMS/EMS 対応　JRCA 登録 CPD 研修コース

品質/環境活動の充実に～マネジメントシステムの実効性を上げるためのヒント～（MD42）
※QMS/EMS 対応　JRCA 登録 CPD 研修コース

審査員研修コースのオンライン（Web）
セミナーもいよいよ 4 月から始まります。
詳細は弊社ホームページをご確認ください。

お問い合わせ：（株）テクノファ　研修事業部 hinshitsu@technofer.co.jp
弊社ホームページ https://www.technofer.co.jp/ もご参照ください。

お待たせしました。**2021 年度セミナー**
年間スケジュール公開しました！

4. テクノファ動画ポータルからのお知らせ

有料動画配信開始

リモート監査①（基本・実技編）
https://technofer.info/contents/115

リモート監査②（計画・推進編）
https://technofer.info/contents/116

各¥3,300-(税込)
※クレジットカードでの決済が可能です

無料で視聴できる対談コンテンツ

廃プラ輸出規制への対応を考える
～廃プラの判断基準を読み解く～
https://technofer.info/contents/150

「プラスチックの輸出に係るバーゼル法該非判断基準」について、当基準策定の検討委員会に参画された一般社団法人資源プラ協会代表理事 犬飼健太郎氏、また、株式会社テクノファ技術顧問 平田耕一氏を迎え、対象となる「廃プラスチック」の判断基準を読み解く動画です。

その他にも ISO マネジメントシステムや環境法規制、内部監査などに役立つ動画を 100 本以上掲載しています。ぜひアクセスしてみてください。

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
HP: https://www.technofer.co.jp/

株式会社テクノファ
http://www.technofer.co.jp