審査機関移転のご案内

現状の規格審査に対して、
こんなことでお困りではありませんか？

高すぎる審査費用

簡略化を許さない審査

付加価値のない審査

威圧的な審査

認証機関の移転はいつでもできます。移転に特別な費用は掛かりません。
東京事務所営業部の「審査機関移転見積り担当」まで是非ご相談ください。

すでにISO9001、ISO14001など他の
ISO規格をお持ちのお客様へ

統合審査のご案内

ISO規格認証には「統合審査」という複数の規格を
同時に審査する方法があり、以下のメリットがあります。

◎ 日数・回数・費用の削減
◎ 審査準備・対応の負担軽減
◎ 多彩な切り口で経営に相乗効果を発揮！

統合審査のご相談は、東京事務所営業部の「統合審査見積り担当」までお寄せください。

[ISO/IEC27000シリーズの取得を検討される組織・企業様の例]

会員、加入者向けサービスの提供、向上を図りたい ▶電気・通信・スポーツクラブ・福祉サービス・警護サービス　等	**機密性の高い個人情報を取り扱っている** ▶医療機関・銀行・証券・保険会社　等
顧客の機密情報を取り扱っている ▶コンサルティング・研究機関・会計・法律・特許事務所　等	**各種ITサービスを提供している** ▶情報通信・SNS・ネットゲーム・クラウドサービス　等

インターテックについて

私たちインターテックは世界中で幅広い産業分野の品質を支えるリーディングカンパニーです。審査、検査、試験、トレーニング、アドバイザリー、品質保証、認証業務を通じて、あらゆるお客様の製品やプロセス、資産に付加価値を提供します。また、1,000ヶ所を超える試験所やオフィス、100ヶ国以上で勤務するスタッフ44,000人のネットワークを活かし、グローバルな市場でお客様の成功をサポートします。そして、私たちは世界中の市場でお客様の期待に安全で継続的に、実行力を持って誠実にお応えします。
詳しくは、 www.intertek.com(英文)まで

intertek
Total Quality. Assured.

インターテック・サーティフィケーション株式会社

■ 東京事務所　〒103-0012　東京都中央区日本橋堀留町1-4-2 日本橋ノーススクエア
TEL.03-3669-7408(代表)／03-3669-7435(営業部直通)　FAX.03-3669-7410

■ 大阪事務所　〒532-0003 大阪府大阪市淀川区宮原3-5-24 新大阪第一生命ビル5階
TEL.06-6150-0571／FAX.06-6150-0575

■ URL　https://ba.intertek-jpn.com/

(2021年4月版)

ISO/IEC27001

& ISO/IEC27000 family of standards

Information Security Manegement System

情報セキュリティマネジメントシステム

intertek
Total Quality. Assured.

intertek
Total Quality. Assured.

インターテック・サーティフィケーション株式会社

情報社会におけるリスク・脅威とは？

**情報システムやインターネットは、組織の運営に欠かせないものになる一方で、
以下のようなリスク・脅威にさらされています。**

機密情報の漏えい

組織は顧客情報、技術資料等を含む機密情報を取り扱っていますが、これらの機密情報を適切に管理できない場合、自組織の信用・信頼を失墜し大きな損失が生じる可能性があります。実際に、ウイルスへの感染による機密情報の流出、機密情報の不正持ち出し、記録媒体の紛失など、様々な原因による機密情報の漏えいにつながる事件・事故が発生しています。

情報システムの停止

DoS攻撃、DDoS攻撃をはじめとした攻撃や災害など、様々な理由により、情報システムがダウンしてしまう事例が増えています。ISO/IEC27000シリーズの認証取得を通して、外部からの攻撃や災害発生時のリスクを管理し、情報システムをどのように守るべきなのかを理解することができるようになります。

個人情報の流失

ひとたび個人情報が流出すると損害賠償といった訴訟リスクを抱えると同時に、組織の信用・ブランドイメージは傷つけられ、顧客離れなど今後の事業継続にも影響を与える恐れがあります。また、個人情報保護法やGDPR(EU一般データ保護規則)といった関連法規に基づき損害賠償の責任を負うことになります。

ウイルスへの感染

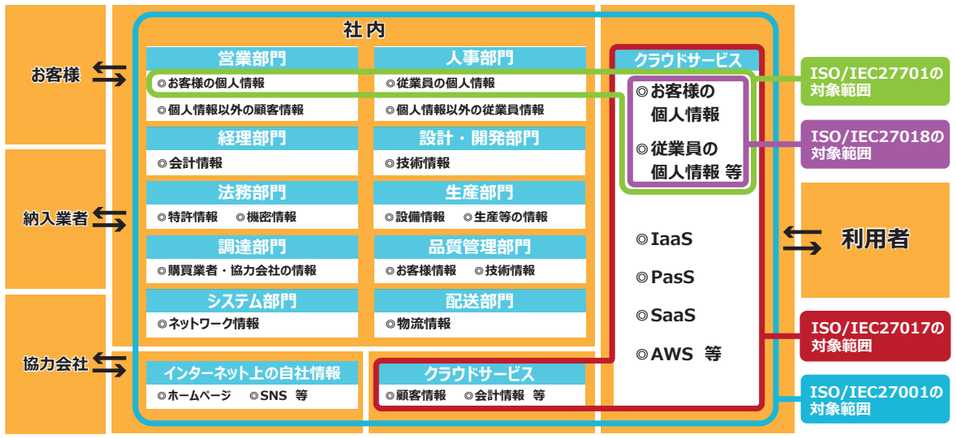
外部から攻撃を仕掛ける最も簡単な方法はウイルスを介したものです。ウイルスなどに影響を受ける組織は、情報資産のアップデート等の管理がうまくいっていない組織です。
ISO/IEC27000シリーズの取得によって、このようなリストの傾向分析、リスク管理、そして実際にどのような対応をすべきかといった体系的な管理方法を構築することができます。

ホームページデータの改ざん

第三者による改ざんなどの事態に陥ってしまうと、組織としての対策不足が露呈し信用を失うことにもつながります。さらに、ウイルスが埋め込まれてしまった場合、ホームページの訪問者に対しても悪影響を及ぼす可能性があります。また外部からのサイバー攻撃は年々高度化・複雑化しており、組織的な攻撃も増えています。ランサムウェア、ソーシャル・エンジニアリング、パスワード盗難など多くの脅威に自組織のホームページ、クラウドサービスなどがさらされています。このような脅威への効果的な対策法を知らない組織が依然多いようです。

**こうしたリスクが組織の規模に関係なく、どのような組織にも存在していることを認識し、リスクを低減するための適切な情報セキュリティ対策を導入する必要があります。
この対策として注目されているのが、情報セキュリティに関する国際基準としての「ISO/IEC27000シリーズ」です。**

日々の業務と ISO/IEC27000シリーズの活動対象範囲(例)



ISO/IEC27000シリーズとは

情報化社会である現在、あらゆる組織にとって情報は資産となっています。しかし、災害やインシデントなどによる情報システムの停止やデータの損失、偽サイトやフィッシングサイトを使用した詐欺行為による個人情報や顧客情報といった機密情報の漏えい、ウイルス感染によるさまざまなリスクの発生など、情報資産は数多くの脅威に常にさらされており、組織ではこのような脅威への対策が急務となってきました。このような背景から2005年に国際規格化されたのがISO/IEC27001(情報セキュリティマネジメントシステム)で、2013年10月には、最新の動向を反映する等のため改訂されました。

通信技術は日々進化し続けて便利になる一方で様々な課題や問題も発生しています。これらに対応するためISO27000シリーズでは様々な規格を制定し、それぞれの固有リスクに対応できるようにしています。

特に個人情報やクラウドに関しては社会的な関心が高まり、ISO/IEC27001をベースにクラウドサービスに関するガイダンスであるISO/IEC27017やISO/IEC 27018が、また、使用されるメディアや環境に関係なく、組織によって取り扱われるすべての個人情報(PII)に焦点をあてたISO/IEC27701が新たに制定されました。

これら「ISO/IEC27000シリーズ」を取得することで、自組織が提供するITサービスやソフトウェア、組織全体のセキュリティ側面などについて定期的なチェックがなされていることを社内外に対して明確にすることができます。

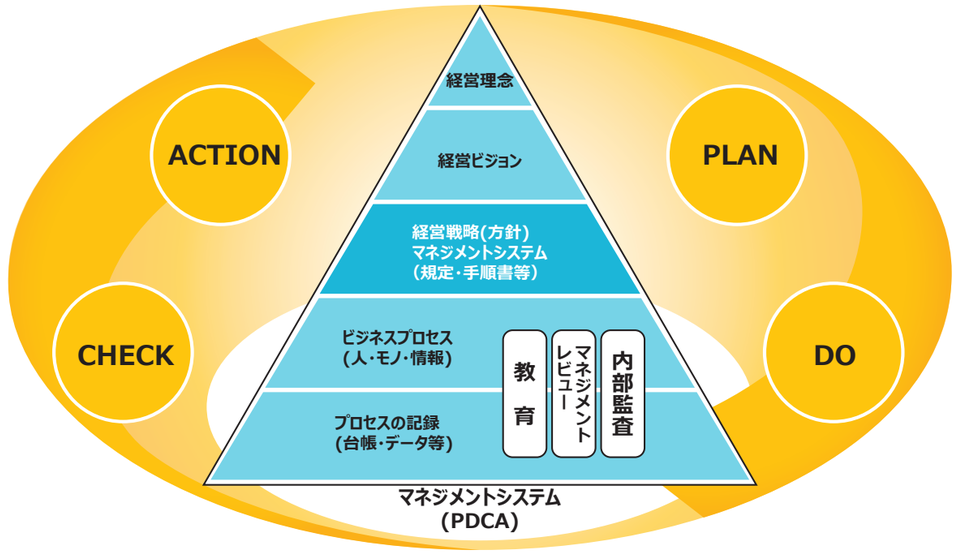
ISO/IEC27000シリーズが選ばれる理由

**ISO/IEC27000シリーズは適切な情報セキュリティ対策についての基準として世界中で認知されており、
この規格の要求事項を効果的に実施することによって組織に多様なメリットをもたらします。**

ISO/IEC27000シリーズ 導入メリット

[1]組織内の情報セキュリティを確保するルールや手順の整備・明確化
[2]組織全体による継続的な情報セキュリティ対策・意識の維持、向上
[3]情報漏えい、業務停止等によるリスク低減・回避による発生損害の抑止効果
[4]取引条件への対応(官公庁の入札対応、取引企業への要請に対応)
[5]認証取得による顧客・取引先からの安心・信頼感の獲得

ISO/IEC27001の PDCAサイクル



ISO/IEC27001 審査・認証の流れ(例)

ISO27001:2013 認証取得
(認証ロゴイメージ)

ISO/IEC27017審査・認証の流れ(例)