

## 製造業様向け情報セキュリティマネジメントシステム

国際規格ISO27001:2005「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」は、IT企業のみならず製造業や建築業、医療関係、その他サービス業など業種を問わず適用することができる。

ISMSを構築・運用しようとする製造業は、企業情報を適切に管理し、情報セキュリティを確保するための体系的なしくみ、コンピュータシステムのセキュリティ対策だけでなく、情報を扱う際の基本的な方針(セキュリティポリシー)や、それに基づいた具体的な計画、計画の実施・運用、一定期間ごとの方針・計画の見直しまで含めた、トータルなリスクマネジメント体系を構築し運用していくことになる。

## 製造業様向け情報セキュリティマネジメントシステムの必要性

- 日本の製造業の各社は、国際競争力を確保するため海外への工場進出の推進、あるいは国内工場における外国人研修生を受入れ、協力会社との分業を行うなど、企業の競争力を左右する企業情報に携わる人が多岐にわたっている。こうした動きは、既に避けることが出来ないものとなっている。こうした状況の中で、超優良企業と呼ばれる自動車関連の企業製造業で、大きな機密情報の漏洩事件があったことは記憶に新しい。これは対岸の火事ではない。
- 先端技術を扱う親会社は、下請け取引をする製造業に対しても大事な技術情報の漏洩などが発生しないように細心の管理を行うようになってきている。そうした親企業との取引を継続していくには自社にもしっかりと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必要がある。
- 大手製造業は知的財産権の保護のため特許戦略などが重要になるが、その下請け中小製造業の場合、製造現場での製造方法や用いる原材料など、文字や文書になっていない現場作業の中に守るべき情報資産が隠れている。
- ひとたび、先端技術情報の漏洩や情報ネットワークシステムに何か問題が発生し、事件・事故の発生となれば、企業の事業継続性にも大きな影響が及ぶことを意味し、日常の工場稼働、事業存続にも大きな影響を受けることを意味している。

## 認証取得までにPDCAサイクルを1回転させる

- Plan - 計画 (ISMSの確立)
  - 全般的な基本方針及び目標に沿った結果を出すための、リスクマネジメント及び情報セキュリティの改善に関連する情報セキュリティ基本方針、目標、プロセス及び手順を確立する。顧客の機密情報、顧客情報、自社の技術的な機密情報を明確にする。
- Do - 実施 (ISMSの導入及び運用)
  - 情報セキュリティ基本方針、管理策、プロセス及び手順を導入し、運用する。入退室管理、図面の管理などを見直し、従業員や協力会社との契約管理などさまざまな管理策を実施していく。
- Check - 点検 (ISMSの監視及び見直し)
  - 情報セキュリティ基本方針、目標及び実際の経験に照らしてプロセスの実施状況を評価し、可能な場合これを測定し、その結果を見直しのために社長に報告する。
- ACT - 処置 (ISMSの維持及び改善)
  - ISMSの継続的な改善を達成するために、内部監査及びマネジメントレビューの結果やその他関連情報に基づいて是正処置及び予防処置を講ずる。

## ISMS付属書Aの詳細管理策とは

詳細管理策は以下のようにA.5からA.15まで11の領域 / 分類 (管理目的: 39個、管理策: 133個) が

ある。適用宣言書でこれらの詳細管理策を採用するか否かを明確に記述する。

- A.5 セキュリティ基本方針情報セキュリティの重要性を伝達など
- A.6 情報セキュリティのための組織契約関連の文言の見直しなど
- A.7 資産の管理ラベル付けのルールを明確にするなど
- A.8 人的資源のセキュリティ従業員の管理（雇用前、雇用中、雇用の終了時の処置）など
- A.9 物理的及び環境的セキュリティ工場の入退室管理ルールの徹底など
- A.10 通信及び運用管理webや電子メールのルールなど
- A.11 アクセス制御機密情報へのアクセス管理など
- A.12 情報システムの取得、開発及び保守生産管理システム、CAD/CAMなど
- A.13 情報セキュリティインシデントの管理情報漏洩など発生時の対応手順の確立など
- A.14 事業継続管理工場が天災や情報ネットワークの破壊で機能しなくなった場合の対応・復旧につ
- A.15 コンプライアンスライセンス管理、特許関連及び輸出入関係のルールなど

これからシステム構築しようとする製造業の推進担当は、事前のチェックとして、次のチェックを試みるとよいでしょう。

- 物理的・環境的側面のチェック（出入口やパーティションなど）
- オフィスセキュリティ面でのセキュリティゾーンのチェック（オフィスレイアウト図）
- ネットワーク環境のチェック（ネットワーク図）
- 情報管理に関するコンプライアンス上のチェック（ソフトウェアライセンスなど）
- 新規システム構築または更新の検討
- 関連する過去のセキュリティ事件・事故
- セキュリティ組織の編成

## システム導入・運用

システム導入運用にあたり社員教育を実施する。初回構築時におけるP D C Aの運用であるD oは、初めての取り組みとなるため、開始時は特に「試行」的な運用として、試行錯誤を繰り返しながらシステム運用を確立していくことになる。そのため、取得期限などを加味しながらも出来る限り長い期間を取って、定められた規則や手続きに従い、各人の役割を確かめながら進めていくことが肝要となる。次にISO27001規格に基づき、運用状況を点検、評価する内部監査を実施する。内部監査において指摘された事項、日々の事件・事故報告、また情報セキュリティに関する利害関係者からの報告事項などをもとに是正処置及び予防処置を実施する。内部監査結果などのインプット情報を収集してマネジメントレビューを実施する。

## 情報セキュリティマネジメントシステム実践のポイント

1. 製造業の現場の知識・経験を持ち、かつISO27001の知識・経験、経営の知識・経験があるコンサルタント
2. その組織にあたりリスク評価を行い、現状に合った対策を実施する。
3. 適切なリスク対策の策定と実践。
4. 啓発・教育・訓練で、従業員意識の維持/向上を図る。
5. すでにISO9001、ISO14001を導入済みの製造業様では統合マネジメントシステム（MS）の構築すること

## ニーズで選べる支援内容

製造業様向け情報セキュリティマネジメントシステムの構築には製造業に携わった実務経験と、ITの知識、マネジメントの知識を持ち合わせたコンサルティングの採用が重要です。タテックス有限会社ではすでに製造業様向け情報セキュリティマネジメントシステムの構築・運用支援コンサルティング実績がございます。ISO取得に必要な工数をお客様のニーズで選べます。お問合わせください。また、既にISMSシステム運用をしているのが、さらに改善したいのだが。。。といった改善のご相談もお気軽に[お問合せ](#)ください。

製造業様向け情報セキュリティマネジメントシステムの[お問合せ](#)、御見積りはタテックスまで！

ISO27001,ISO14001,ISO9001,Pマーク取得に関するお悩み・ご相談、御見積りを無料メール相談でお受けします。お気軽に[お問合せ](#)ください。