

情報セキュリティとは、ISO27001:2005では次のように定義されています。情報セキュリティ（information security）とは情報の機密性、完全性及び可用性を維持すること。さらに、真正性、責任追跡性、否認防止及び信頼性のような特性を維持することを含めてもよい。ここで、機密性（confidentiality）とは、認可されていない個人、エンティティ又はプロセスに対して、情報を使用不可又は非公開にする特性をいう。また、完全性（integrity）とは、資産の正確さ及び完全さを保護する特性をいい、可用性（availability）とは、認可されたエンティティが要求したときに、アクセス及び使用が可能である特性をいう。これらをバランスよく維持することを指します。

## ISO27001とは

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、情報セキュリティ（information security）をマネジメントするシステムの要求事項が書かれた規格です。

## ISMSとは

ISMSとは情報セキュリティマネジメントシステム（Information Security Management System）の略称です。企業などの組織が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のことを指しています。

## ISMS（情報セキュリティマネジメントシステム）の必要性

好むと好まざるに関わらず、企業の活動の奥深くまでコンピュータネットワークシステムが入り込んできている。これは既に避けることが出来ないものとなっている。既にインターネットシステムは、輸送・交通、エネルギー、金融のネットワークとともにそれらを支える基幹の情報ネットワークとしてライフラインとなっている。あらゆる分野、あらゆる立場で「情報セキュリティ」が極めて重要となっている。言い換えれば、ひとたび「情報ネットワークシステム」に何か問題が発生すれば企業の継続性にも大きな影響が及ぶことを意味し、日常生活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。

- 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。

- 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。

## システム構築（ISMSの確立）

ISO27001のシステム構築の始めにISMSの適用範囲を決め、ISMS基本方針を制定する。制定した基本方針に基づいて、リスクマネジメントを始めとした具体的な構築作業に取りかかる。ISO27001認証取得の中核となるリスクマネジメントについては、まずリスクアセスメント手法を決定（Step 1）する。続いて、保護すべき情報資産に対するリスクを識別（Step 2）し、リスクを分析し評価（Step 3）する。さらに、リスク対応についての選択肢を明確にし、評価（Step 4）し、リスク対応に関する管理目的と管理策を選択（Step 5）する。経営陣は残留リスクの承認（Step 6）と、当該ISMSの導入及び運用について許可（Step 7）し、最後に適用宣言書を作成（Step 8）する流れとなる。なお、リスクマネジメント用語の汎用的な定義によれば、リスクマネジメントとは「リスクに関して組織を指揮し管理する調整された活動」としている。この結果を元に、各社の業務運営実態に則した各種規定類の策定を行い、経営者の承認を得る。

## リスクアセスメント4つの手法

リスクアセスメントにはいくつかの手法があり、企業が自社の情報資産やその保護の状況を勘案してどの方法を選択するかを決定する。リスクアセスメントは始めてISMSのシステム構築に取り組む際に最も難しい部分となる。自力で行なうより、信頼と実績のあるプロのコンサルタントを活用することがムリ・ムダのない取り組みとなる。分析手法の例として一般的には次の4つの手法がある。

1. ひとつまたは複数の対策を一律にシステム全体に適用する方法（ベースラインアプローチ）
2. 専門家や経験者の知識に依存して実施する方法（非形式的アプローチ）
3. 情報資産の一つひとつについて詳細な分析を実施する方法（詳細リスク分析）
4. ベースラインアプローチと詳細リスク分析を組み合わせる方法（組み合わせアプローチ）

これらの手法については、ISMSユーザズガイド - リスクマネジメント編「補章2 GMITSにおけるリスク分析の手法」に解説がある。特長を理解して、最適な手法を選択する。

## 情報資産とは

情報資産の例としては、次のようなものがあります。

情報資産（紙媒体）	見積書、契約書など
情報資産（電子媒体）	CD、MO（持ち運び可能な記憶媒体）など
情報資産（システム）	顧客DB（サーバやPC内に格納される電子情報）など
ソフトウェア資産	DTPソフト、文書作成ソフト、表計算ソフトなど
ハードウェア資産	PC筐体、サーバ、ルータなど
サービス	清掃サービス、ペンディングサービス、ASPサービスなど
要員	サーバールームオペレータ、個人情報入力オペレータなど

## ISMS付属書Aの詳細管理策

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](#)
- [A.6 情報セキュリティのための組織](#)
- [A.7 資産の管理](#)
- [A.8 人的資源のセキュリティ](#)
- [A.9 物理的及び環境的セキュリティ](#)
- [A.10 通信及び運用管理](#)
- [A.11 アクセス制御](#)

## [A.12 情報システムの取得、開発及び保守](#)

- [A.13 情報セキュリティインシデントの管理](#)
- [A.14 事業継続管理](#)
- [A.15 コンプライアンス](#)

これからシステム構築をされる組織は事前のチェックとして、次のチェックをして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

- その組織にあったリスク評価を行い、現状に合った対策を実施する。
- 適切なリスク対策の策定と実践。
- 啓発・教育・訓練で、従業員意識の維持/向上を図る。

### 製造業 / 医療情報処理業におけるISO27001・情報セキュリティマネジメントシステム

製造業 / 医療情報処理業におけるISO27001・情報セキュリティ、ISMSは下記をクリックください。

- [製造業様向けISO27001・情報セキュリティマネジメントシステム認証取得支援コンサルティング](#)
- [ISO27001|医療情報処理業のISMS|認証取得コンサルティング|TATECS](#)

#### ニーズで選べる支援内容

実績豊富なISOコンサルタント陣がISO取得に必要な工数をお客様のニーズで選べます。お問い合わせください。また、既にシステム運用をしていて、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い合わせください。

#### ISO27001システム構築で参考となる資料

- JIS Q27001：2006（有料）日本規格協会か書店で購入
- JIS Q27002：2006（有料） ”
- ISMS適合性評価制度の概要（無料）[JIPDEC](#)のホームページで入手
- ISMSユーザーズガイド - リスクマネジメント編（無料）同上
- 外部委託におけるISMS適合性評価制度の活用方法（無料）同上
- ISMS構築事例集（無料）同上

## ISO27001特別レポートを無料公開！

---

実績豊富なISOコンサルタント陣がISO9001、ISO14001、Pマーク取得ノウハウをご提供。ISO担当者だけでなく経営者も必見の情報です。まずは最新の無料レポートをご覧ください。ISO27001,ISO14001,ISO9001,Pマーク取得に関するお悩み・ご相談を無料メール相談でお受けします。専門家のアドバイスを受けたい方、まずはこの無料サービスをご利用下さい。

御見積りは信頼と実績のタテックスまで[お問合せ](#)ください。

お問合せは、[ここをクリック](#) [お問合せ](#)