ISO基礎研修テキスト

～ISO9001, ISO14001,ISO27001の基本～

ISOマネジメント研究所

ISO全般

～ISOを理解する上で必要なこと～

3つの問い

問1：なぜ、会社は存続できるのか？

問2：誰が、会社を支えているのか？

問3：会社が発展するためには何が必要か？

ISOの規格はこんなことをいっている

組織は、この規格に基づいて品質マネジメントシステムを実施することで、次のような便益を得る可能性がある。

a)　製品及びサービスを一貫して提供できる

b) 顧客満足を向上させる機会を増やす

・・・・・

・・・・・

『ISO9001：2015　品質マネジメントシステム−要求事項　序文』

ISOとは？

ISOは、各国独自の規格（たとえば、日本ではJIS規格）とは違い、世界共通の規格です。

ISO：国際標準化機構（本部：ジュネーブ）
(International Organization for Standardization)

- 1947年に設立され、現在は加盟国163カ国あり、国際標準化を推進する非政府組織。公共部門と民間部門の橋渡しを行う役割。
- 規格は任意規格で強制（規制）ではない。

物の規格

- 「写真フィルム感度」「ネジの形状」「クレジットカードの寸法」「タイヤ」「非常燈の出口のマーク」、等

仕組みの規格

- ISO9001「品質マネジメントの国際規格」
- ISO14001「環境マネジメントの国際規格」
- ISO27001「情報セキュリティマネジメントの国際規格」、等

ISOのよくある誤解

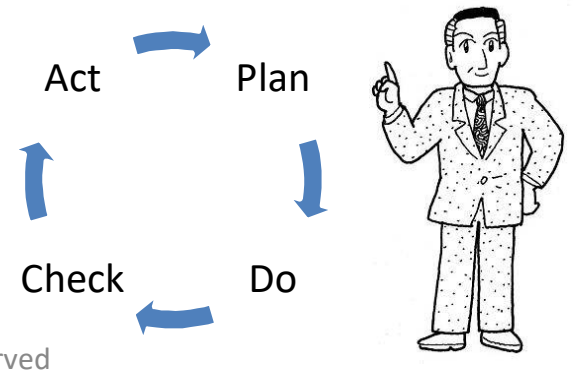
仕様（スペック）規格ではなく

マネジメント規格である

*何をするか*はISOの規格要求事項の中で、規定しているが、*具体的にどうするか* は規定していない。

ISOとは、組織内にPDCAの仕組みを作ること

Plan	目標や計画を作成すること
Do	計画に基づき実行すること
Check	目標や計画に照らして、実行を検証すること
Act(Action)	検証した結果、対策を考え、また、目標や計画につなげていくこと



ISO取得のメリット・デメリット

メリット

・社員の意識向上
・企業PR（第三者評価取得）
・業務管理能力向上
・リスク対応力向上
・業務の標準化・効率化
・目標管理能力向上

・品質/サービスの向上
・顧客の拡大/維持
・不良やクレーム、事故低減
・継続的な教育の実施
・社員の力量アップ
・体制の整備
・目標管理の明確化、等

デメリット

取得費用等お金がかかる。手間が掛かる。うまく運用できなければ社員の士気を損ねる。

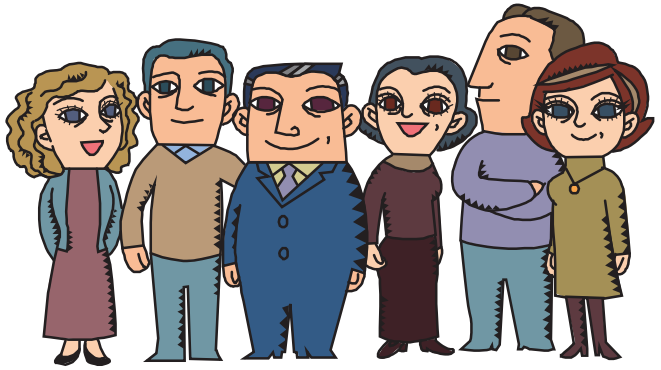
ISO9001とは？

ISO9001の背景

	欧米的なアプローチ	日本的なアプローチ
習慣	契約社会	根回しの社会
重視する立場	***購入者（買う側）の立場***	***供給者（売る側）の立場***
品質保証の考え方	・契約重視 ・供給者（売る側）への立ち入り監査 ・仕組みによる保証 ・トップダウン	・顧客要求先取り ・顧客の満足する製品の開発提供 ・ボトムアップ
手段	・ISO9001 ・TQM	・TQM ・QC

→ ***経済のグローバル化によって、***
欧米的なアプローチがスタンダードになった。

品質マネジメントシステム（QMS）とは？



企業が顧客満足を実現するために行う、組織的な仕組み

ISO9001のポイント

ﾎﾟｲﾝﾄ１：顧客満足の実現を図る

さらなる顧客満足を図るためには、どうしたらよいか、そのための方針や具体的な実行策を、裏付けを持って行うこと。

ﾎﾟｲﾝﾄ２：プロセスアプローチの取組み

望まれる成果を生み出すために、プロセスを明確にし、その相互関係を把握し、運営管理することと併せて、一連のプロセスをシステムとして適用すること。

ﾎﾟｲﾝﾄ３：リスク対応を図る

主に起こり得る問題、不具合を明確化し、対応を図ること。リスクとの関連では、現場において、ヒューマンエラー対策を行うこと。

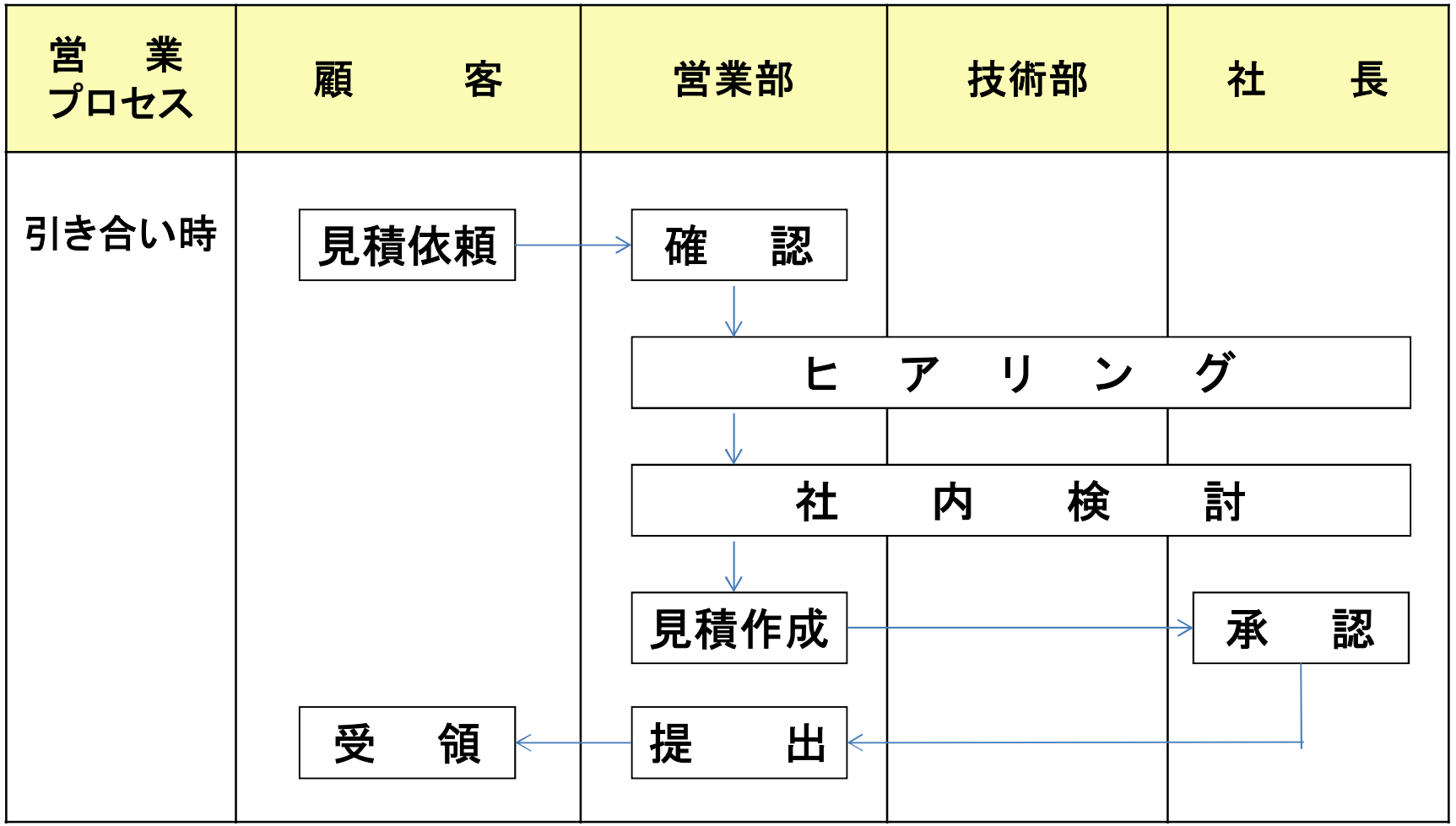
プロセスとは？

インプットを使用して、意図した結果を生み出す、相互に関連する又は相互に作用する一連の活動。

具体的なプロセスの例

分野	事業プロセス	活動プロセス
主要プロセス	営業	・広告宣伝 ・見積り ・受注契約等
	購買	・購買先評価 ・発注 ・受入検査等
支援プロセス	人材開発	・人事 ・教育訓練等
	インフラ	・設備保全計画の立案 ・設備保全実施

例:プロセスを明確化する



品質マネジメントの原則
～ISO9001の考え方のベース～

1．顧客重視
(Customer focus)
・現在、将来の顧客のニーズ・期待を理解
・顧客満足の向上を目指す

2．リーダーシップ
(Leadership)
・組織の目的、方向などを取りまとめ
・目標達成に参画できる環境を提供

3．人々の積極的参加
(Engagement of people)
・すべての階層の人々の参加
・全面的な参画で組織の目的を達成

4．プロセスアプローチ
(Process approach)
・プロセス（過程）を重視かつ保証
・プロセス（過程）のつながりを明確化

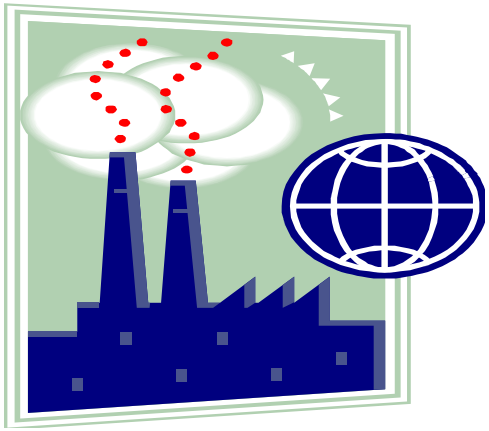
5．改善
(improvement)
・改善には、改革と継続的改善が含まれる
・組織の永遠の目標として推奨

6．客観的事実に基づく意思決定
(Evidence-based decision making)
・データ、情報の分析実施
・意思決定の客観性及び信頼性を高める

7．関係性管理
(Relationships management)
・組織と利害関係者との協働体制作り
・両者の価値創造能力の向上

ISO14001とは？

環境マネジメントシステム（EMS）とは？



企業の経営をリスクマネジメントの面（環境面）からサポートする仕組み

ISO14001が要求する実施事項

1. 場当たり的に、対策をするのではなく、組織の状況を考慮して、重要な環境側面を特定すること（環境法令の適用確認も含む）
2. 組織で特定したリスクや特定した重要な環境側面、順守義務に関する目標を設定し、その対策を計画し、実行すること
3. 実行したら、検証し、問題があれば改善し、次につなげること

ISO14001のポイント

ﾎﾟｲﾝﾄ１：環境側面の特定

会社が関わりを持つ環境の接点を明確にし、環境に大きな影響を与えるものは、何か？ライフサイクルの視点を考慮して、重要な環境側面（著しい環境側面）を特定すること

ﾎﾟｲﾝﾄ２：環境目標の設定

組織で特定したリスクや特定した重要な環境側面、順守義務に関する目標を設定し、その対策を計画し、実行すること。この場合、形骸化しない目標の設定が必要

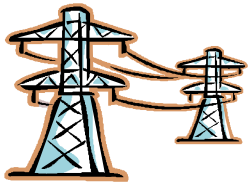
ﾎﾟｲﾝﾄ３：環境法令の順守とその理解

適用する環境法令の順守は、順守義務として重要視されており、社員への周知およびその法令対応は、審査において重視される

環境側面 – インプット・プロセス・アウトプット

インプット　プロセス　アウトプット

原材料の投入



エネルギーの使用

廃棄物

下水・排水

提供する製品もしくはサービスのライフサイクルを考慮することが必要！

具体的な環境影響の特定

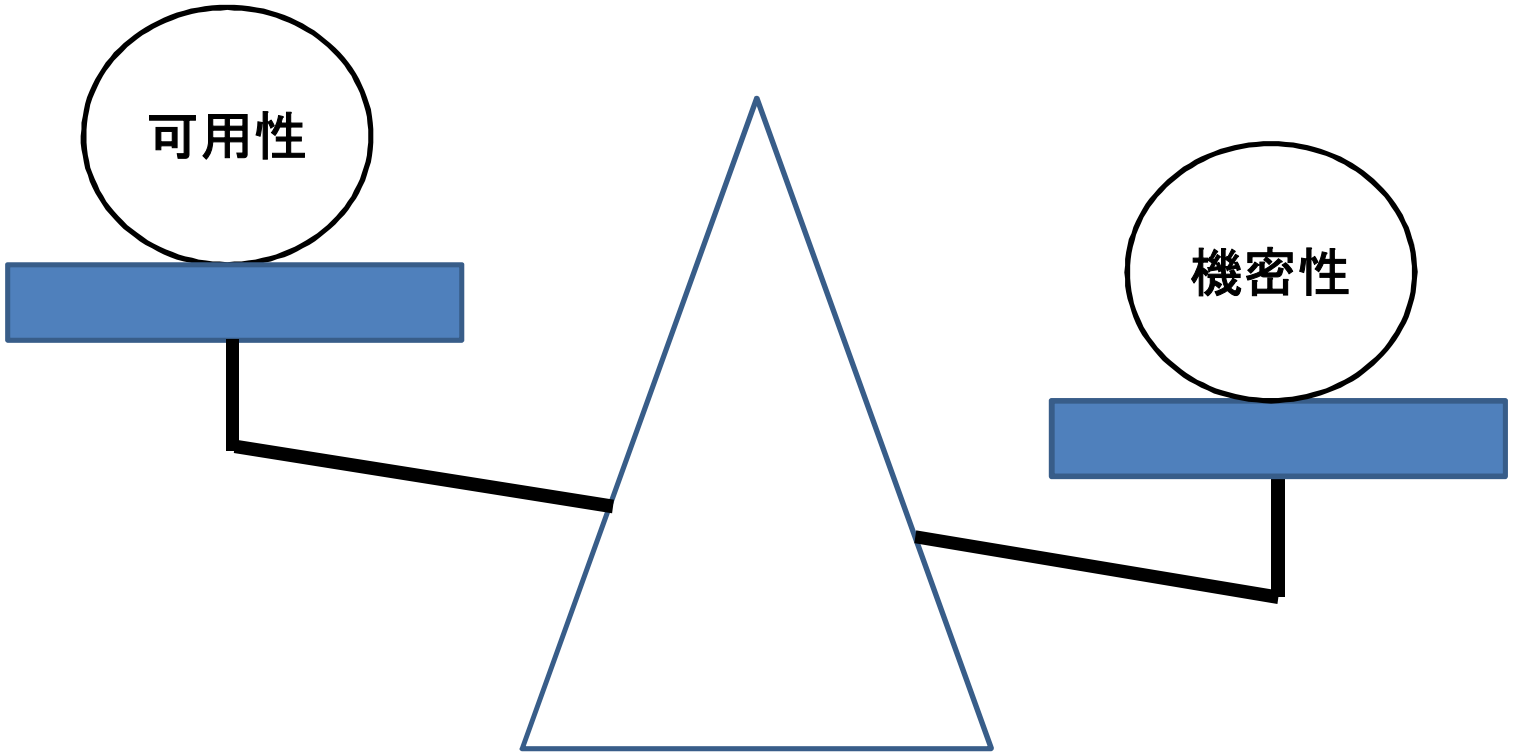
分　類	関連するインプット、アウトプットの例
①大気への放出（大気汚染）	CO2、Nox、フロンなどの排出
②水への排出（水質汚濁）	下水、排水
③土地への排出（土壌汚染）	油などの地下浸透
④原材料及び天然資源の使用（資源枯渇）	石油などの使用
⑤エネルギーの使用	電気、ガスなどの使用
⑥放出エネルギー（騒音・振動）	騒音・振動などの放出
⑦廃棄物（廃棄物負荷）	一般廃棄物、産業廃棄物の排出
⑧悪臭	アンモニア、メチルメルカプタンなどの不快な臭いの原因物資の排出

ISO27001とは？

ISO27001とは？

	Pマーク(JISQ15001)	ISO27001（ISMS）
規格の名称	個人情報保護マネジメントシステム規格	情報セキュリティマネジメントシステム規格
規格の種類	国内規格	国際規格
取得のメリット	顧客、一般利用者、関係者等へのｱﾋﾟｰﾙ	顧客、すべての関係者等へのｱﾋﾟｰﾙ
規格の特長	個人情報保護法の順守をメインに、組織対策としてPDCAの仕組みの構築を要求	組織内の重要な情報資産を認識し、そのﾘｽｸ対策をPDCAの仕組みによって運営管理することを要求
取得企業数 (2016年3月末現在)	約14,000社	約6,000社

機密性と可用性の関係



機密性を重くすれば、可用性が軽くなり、可用性を重くすれば、機密性が軽くなる。状況に応じた取扱いが大事となる。

ISO27001のポイント

ﾎﾟｲﾝﾄ1：組織の状況の確定

場当たり的にセキュリティ対策を行うのではなく、会社にとっての経営課題、業務課題を明確にし、仕組みに関連付け、守るべきものは何か（重要な情報資産は何か）を明確にすること。

ﾎﾟｲﾝﾄ2：リスクアセスメントの実施

組織の状況を考慮した上で、リスクアセスメント（リスク分析）を行い、適切な情報セキュリティのリスク対応を決めること。

ﾎﾟｲﾝﾄ3：リスク対策は、PDCAで取り組む

リスクを低減させるものには、組織的な対策を行い、一連の活動には、PDCAサイクルが適用されていること。

リスク及び機会の決定

１：会社の外部・内部の課題から決定する

たとえば、会社の外部課題としては、社会的な要請として、情報セキュリティへの対応が課題としてある。このリスクとして考えられるのは、外部および内部からの「顧客情報の漏洩」がある。また、会社の内部課題としては、委託先の管理が課題としてあり、これに対応するリスクとしては、「委託先による情報漏洩」がある。

２：利害関係者の要求事項から決定する

主に顧客の要求事項、法令等の要求事項から、リスクを決定するとよい。

情報資産の特定

情報資産の分類	具体的な資産例
紙情報	経営資料、人事資料、業務資料、顧客情報等
電子データ	上記の電子情報
ハードウェア資産	パソコン、サーバー、プリンター、ファクシミリ、ネットワーク機器、電源設備等
ソフトウェア資産	市販ソフト、業務用ソフト、グループウェア等
その他資産（サービス）	通信サービス、一般ユーティリティ（電源、空調等）

資産洗い出しの目的は、適切なセキュリティ対策を決めることで、詳細な資産目録（台帳）を作成することではない！

脅威とぜい弱性とは？

狼が羊を食べる可能性（リスク）

＝「狼と羊が存在すること」と「柵の弱さ」

＝「狼という**脅威**」と「弱い動物という羊（対象の**ぜい弱性**）」と「柵の弱さ（**ぜい弱性**）」

脅威

ぜい弱性

脅威の例

ウイルス感染、不正アクセス、業者からの漏えい、社員の持ち出し、誤操作等

ぜい弱性の例

扉、窓などの物理的保護の欠如、不充分なパスワード管理、社内教育に不足等

具体的なぜい弱性の特定

ぜい弱性の分類	具体的なぜい弱性の例
ハードウェア	不十分な受入れ試験・保守・管理、廃棄時の注意欠如
ソフトウェア	不十分な試験、不十分なアクセス権・パスワード管理、手順書の不備、複雑な利用者インターフェース、公知のソフトウェア欠陥、不要サービスの実行可能
ネットワーク	保護されていない通信回線、送受信の識別・認証の欠如、単一障害点のある構成、不適切なネットワーク管理
組織、要員	次における不備または欠如 教育訓練、利用者管理、情報取扱い手順、インシデント管理、第三者との契約等
サイト	入退室管理の不備、災害対策の不備等

参考：ISMSユーザーガイド-リスクマネジメント編

演　習

演習４：著しい環境側面（定性評価）

作業名 ﾌﾟﾛｾｽ名	機械・ 設備等	ｲﾝﾌﾟｯﾄ	ｱｳﾄﾌﾟｯﾄ	環境 影響	影響 評価	著しい 環境側面登録	今後の 対応
インスタントラーメンを作る	ガスコンロ	都市ガス	ー	エネルギーの使用	コスト削減	●	使用を減らす
		ー	CO2	大気の放出			
		水	ー	天然資源の利用			
		ー	排水	水への排出			
		ー	袋	廃棄物			

演習５：具体的なリスクアセスメント（数値評価）

リスク（トラブル）	資産価値	起こる可能性（脅威）	ぜい弱性	リスク値	リスク対策
パソコンが壊れる	2	2	2	8	データのバックアップ
スマートフォンを紛失する					

リスク値　＝　「資産価値」×（「起こる可能性」＋「ぜい弱性の程度」）

まとめ

ISO9001 のポイント	ISO14001 のポイント	ISO27001 のポイント
1.顧客満足の実現を図る 2.プロセスの明確化 3.リスク対応を図る	1.環境側面の特定（重要な環境側面の特定） 2.環境目標の設定 3.環境法令の順守とその理解	1.組織状況の特定（重要な情報資産の特定） 2.リスクアセスメントの実施およびリスク対応計画策定 3.リスク対策は、PDCAで取り組む