

# ISMS認証取得支援のご提案

**株式会社日本マネジメントシステム**

〒231-0002 横浜市中区海岸通3-9 横浜ビル6F

TEL 045-319-6031 FAX 045-319-6032



## 概要

パソコン、スマートフォン、タブレットなど情報機器のなしでは、仕事が進まない現代社会において情報セキュリティは企業にとって必須の課題と言えます。

サイバーテロ、標的型攻撃など、ニュースや話題となる事象だけでなく、情報セキュリティにおいては、自社の仕組みの構築が重要な要素のひとつといえます。

もちろん、様々なセキュリティ製品を導入し、ネットワークや端末を保護してゆくことは必要なことですが、俯瞰的に何がどの程度重要で、情報セキュリティの観点から、どの情報に対し、どの程度のセキュリティ対策を実施するか？という全体的な戦略がなくては、有効な情報セキュリティ対策になりえません。

高額な製品を購入し、セキュリティ対策を行っている企業を良く見ますが、それはウイルス感染や標的型攻撃などの事象に対する対策であり、俯瞰的な戦略なくして製品を購入することは、もぐらたたき状態と言えます。

まずは、自社がどの様な情報を保有しており、その情報が「機密性」「完全性」「可用性」の観点からどの程度重要で、どの程度のセキュリティ対策を講ずるべきかを検証することが重要です。

そのひとつの指標として、ISMS認証取得を目指されてはいかがでしょうか？



## 弊社 J M S のコンサルティングの特徴

---

1. システム構築、ネットワーク構築の経験者がコンサルタントとして担当
2. IRCA認定研修機関として、内部監査員研修は同等の内容の提供が可能
3. メインコンサルタントとアシスタントコンサルタントの2名以上の体制で担当
4. ドキュメント作成においては、お客様の既存文書、雛形等を考慮した文書化を実施
5. 雛形コンサルの否定（お客様の状況を考慮し、十分なギャップ分析を行った上で、仕組みの構築、規程類の作成を実施）
6. 技術的な情報セキュリティ対策支援の会社として、ISMSにおいても技術的な管理策導入の支援が可能

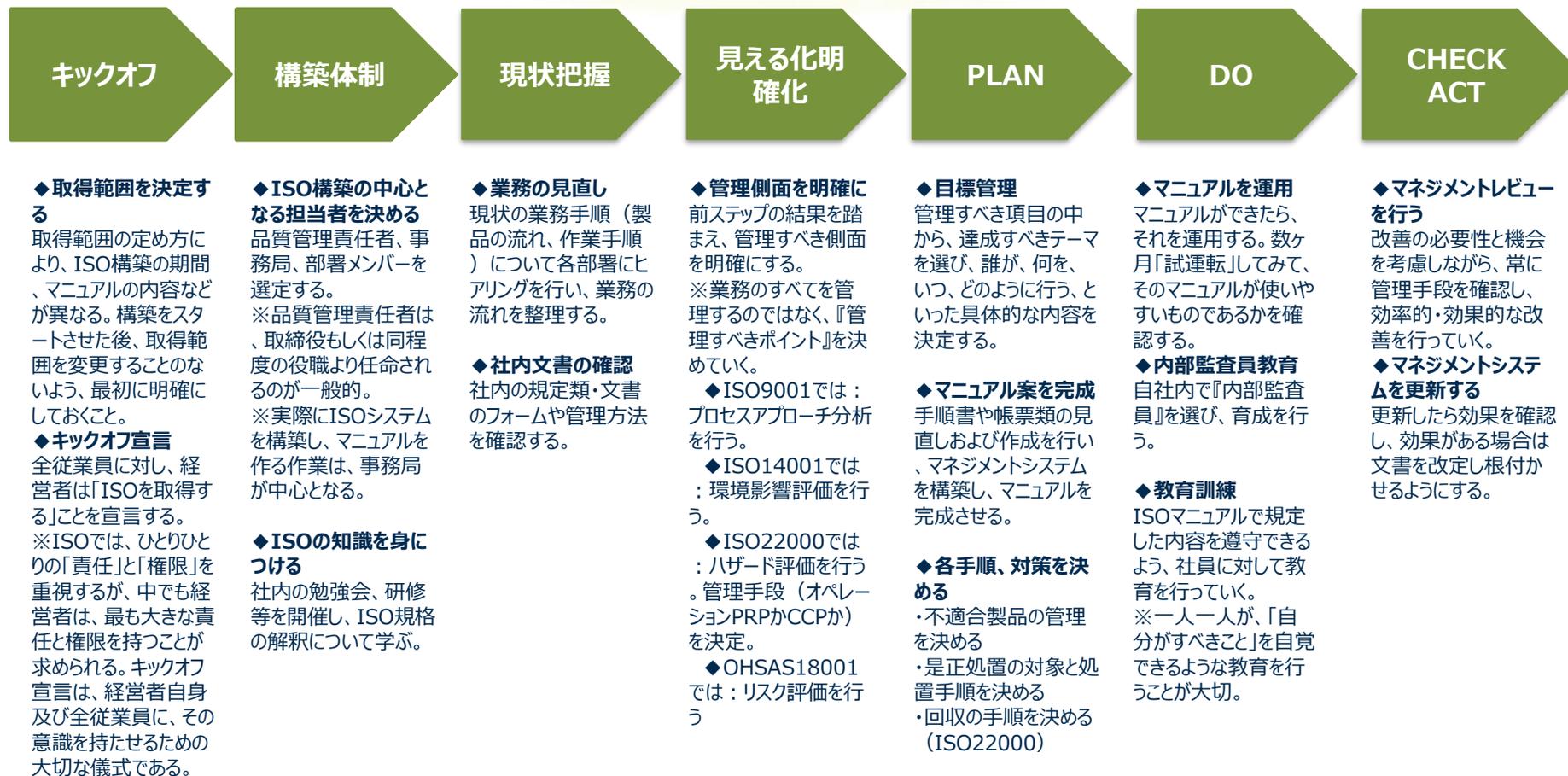


# スケジュール例 (ロードマップ例)

		参加者	1ヶ月目	2ヶ月目	3ヶ月目	4ヶ月目	5ヶ月目	6ヶ月目	7ヶ月目	8ヶ月目	
ISO/IEC 27001	体制・スケジュール・TODOの確認	トップマネジメント 事務局	2								
	経営理念・方針確認	トップマネジメント 事務局									
	適用範囲決定	トップマネジメント 事務局									
	導入教育	一般従業員	1								
	内部監査員教育	内部監査員 事務局			0.5		2				
	内部監査	内部監査員 事務局 一般従業員(必要 なところのみ)						1.5			
	マネジメントレビュー	トップマネジメント 事務局 内部監査員							0.5		
	是正処置	事務局							2		
	情報セキュリティ方針・目標決定	トップマネジメント 事務局			0.5						
	情報の特定(情報資産の洗い出し)	事務局			1		1		1		
	リスクアセスメント				1		1		1		
	リスク対応計画作成				1		1		1		
	文書化	情報セキュリティ方針	事務局			1		1		1	
		ISMSマニュアル				1		1		1	
		適用宣言書				1		1		1	
		リスクアセスメント手順・結果				1		1		1	
		リスク対応計画				1		1		1	
	その他内部文書(最適化含む)			1		1		1			
第一段階審査(準備)	事務局							0.5			
第一段階審査	トップマネジメント 事務局							0.5			
第二段階審査(準備)	事務局							0.5			
第二段階審査	トップマネジメント 事務局							0.5			

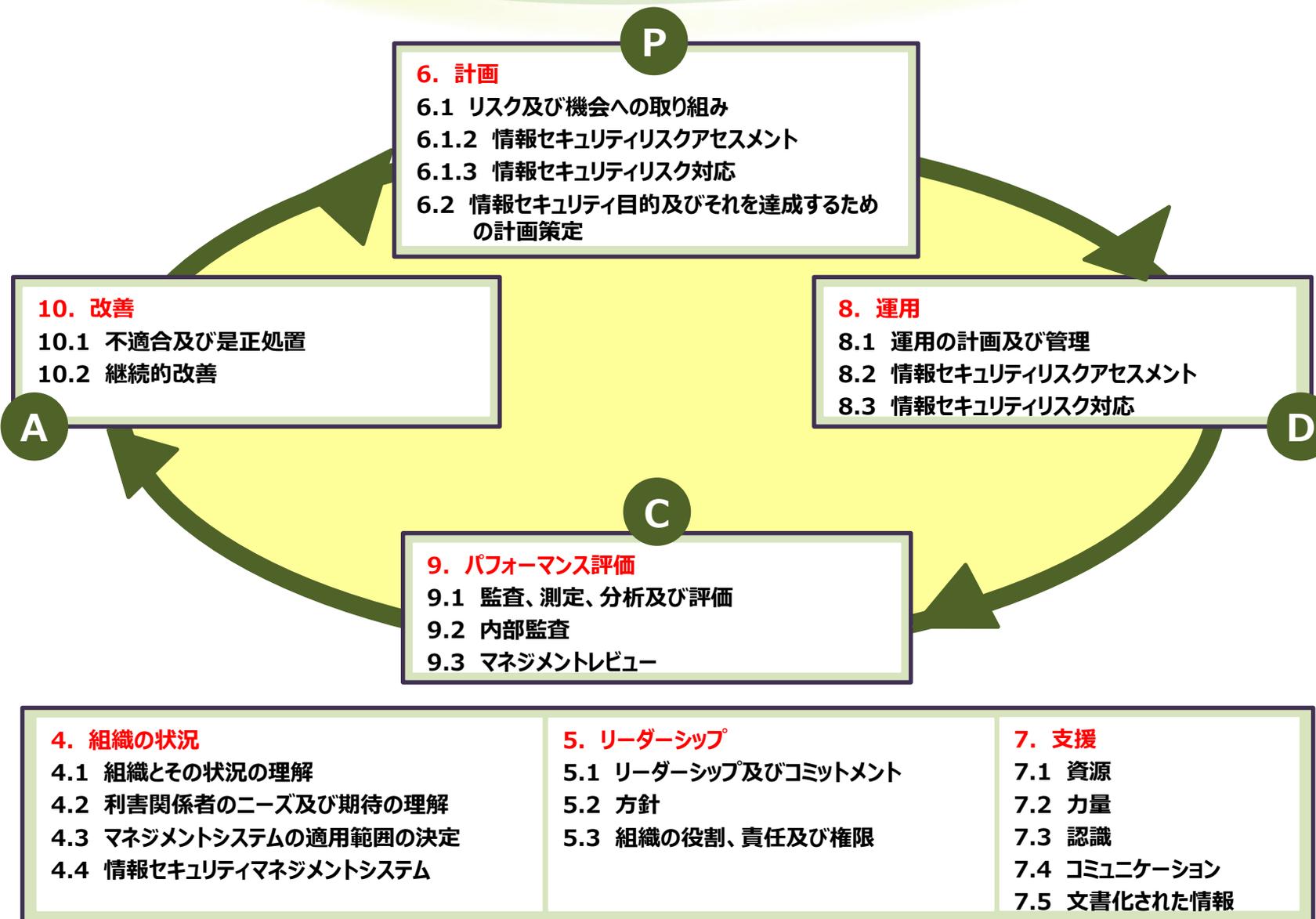


# ISO認証の流れ



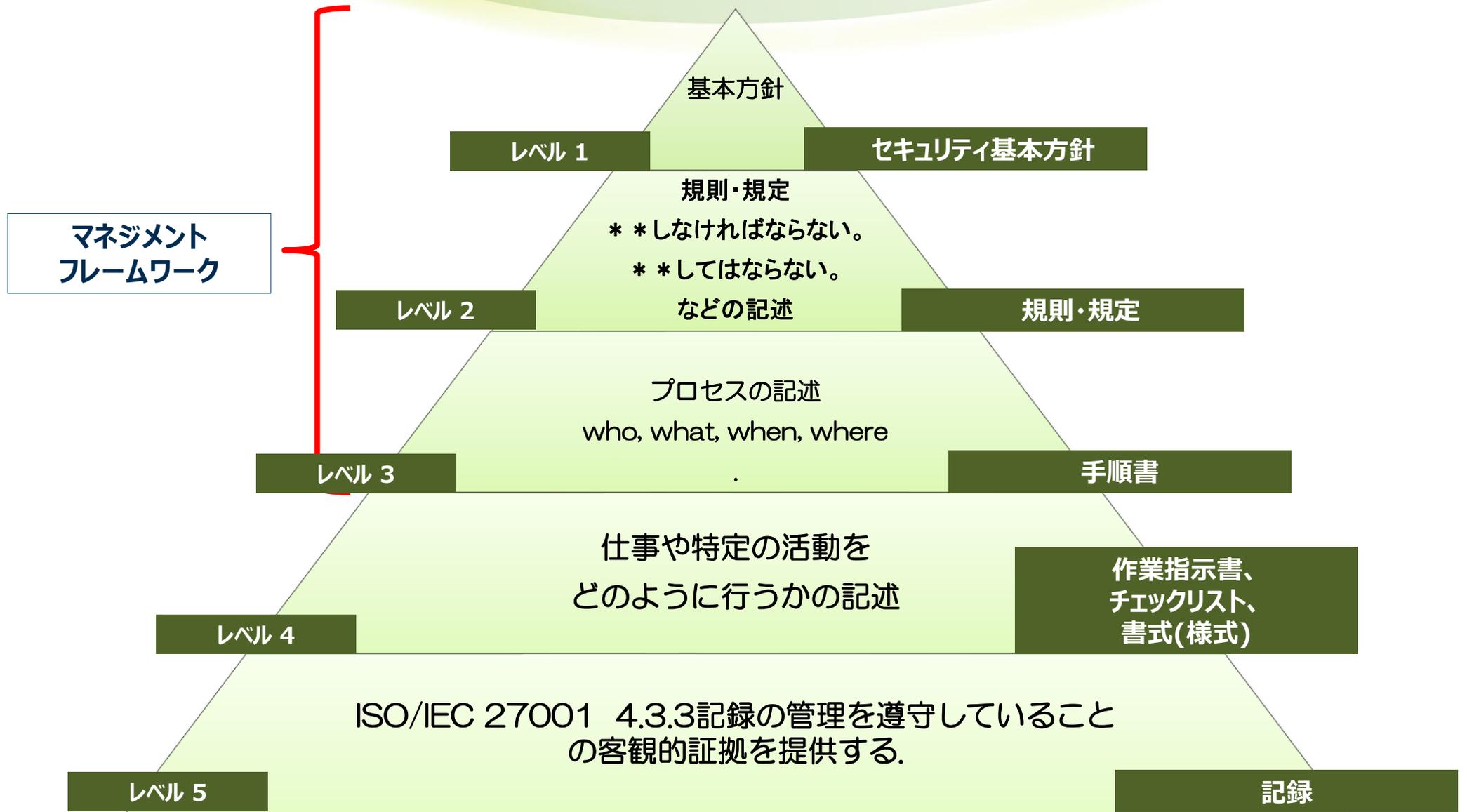


# ISOにおけるPDCAサイクル





# 情報セキュリティ関連文書体系（あるべき姿）



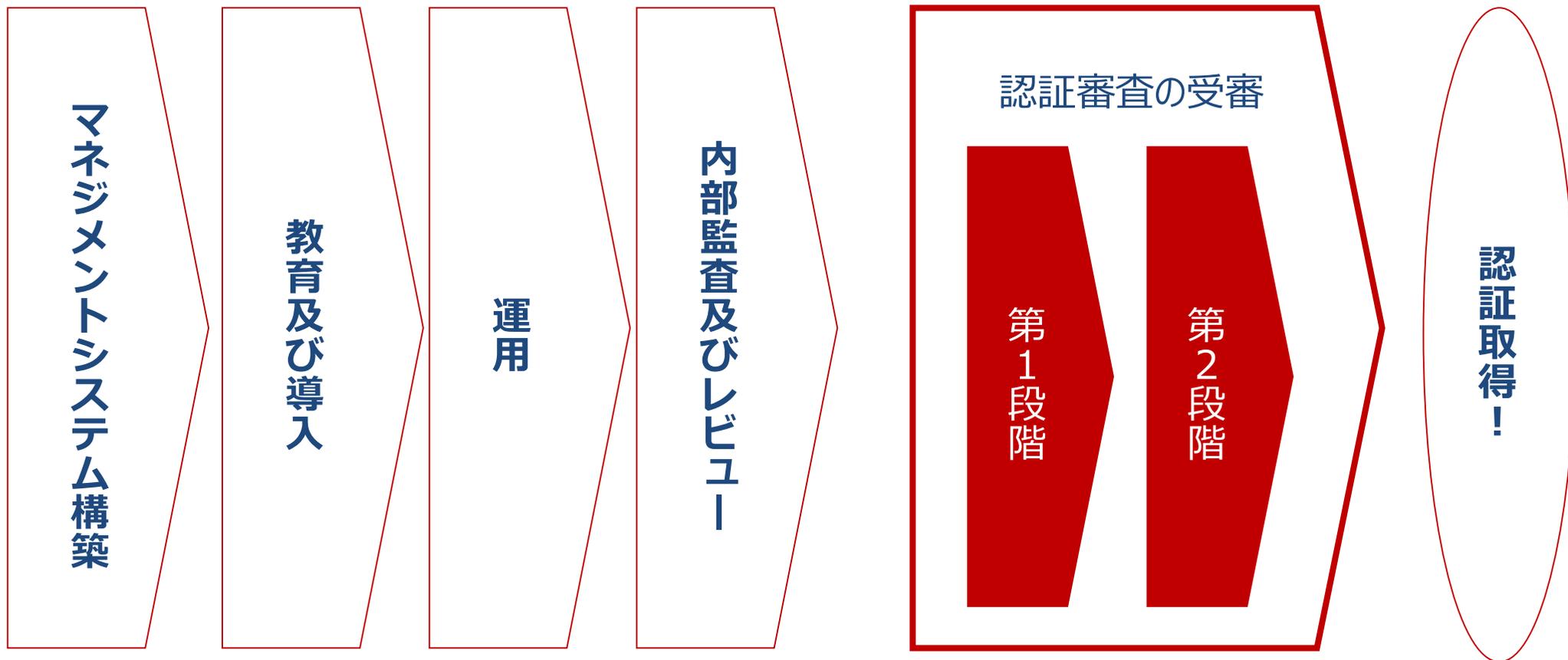


# ISMS構築及び認証のステップ

- 1 適用範囲の決定
- 2 ISMS基本方針の策定
- 3 リスクアセスメントの実施、適用宣言書の作成
- 4 ISMSの文書化
- 5 フレームワークの確立(PDCA)
- 6 セキュリティ対応計画の策定・実施
- 7 導入教育
- 8 内部監査制度の確立
- 9 マネジメントレビュー・是正／改善
- 10 審査 (S T 1・S T 2)



# 認証審査の流れ(初回審査)





# ISMSの認証審査 - 第一段階審査 -

---

- マネジメントシステムが適切に確立されているかについての体制面に関する審査
  - マネジメントシステムのフレームワークを重点に審査（適用範囲、リスクアセスメントなど）
  - 方針、体制、主要な管理手順の確立および実施状況（内部監査の実施状況やマネジメントレビューも含む）の確認
    - 特に「計画すること」や「手順を確立すること」と規定している要求事項を確認
    - 監査計画、セキュリティ対応計画など
  - 個別の運用手順の実施状況は、第二段階で確認
- (但し、業務標準・業務手続等が適切に計画され準備されているかは、第一段階の対象)



# ISMSの認証審査 - 第二段階審査 -

---

- マネジメントシステムの実装状況と運用状況についての審査
- 第一段階で確認された手順が、計画されたとおりに運用されているかを確認
  - **実施状況及び記録を確認**
  - **実装された管理策、実施された教育の結果、実施された是正及び予防処置など**
- 含まれる場合は、第一段階の不適合への確認も実施
- 原則的には、サンプリング方式にて実施

# Japan Management System

---

[www.j-ms.biz](http://www.j-ms.biz)