

講義内容	1 時間 45 分(+50 分)
講義 1 : ISO とは / ISMS とは / 情報セキュリティ基準・規則等の歴史 ISMS 適合性評価制度 / プライバシーマークとの違い	22 分
講義 2 : ISMS の情報セキュリティ / ISMS 規格の構成	14 分
講義 3 : ISO/IEC27001 箇条 4	16 分
講義 4 : ISO/IEC27001 箇条 5	12 分
講義 5 : ISO/IEC27001 箇条 6	32 分
講義 6 : ISO/IEC27001 箇条 7~10	9 分
講義 7 : 参考資料① 附属書 A	36 分
講義 8 : 参考資料② ISMS 認証取得の仕組み	14 分

※ 講義 3~6 は「ISO/IEC27001:2013 要求事項テキスト」  
 講義 7 は「ISO/IEC27001:2013 附属書 A – 管理目的及び管理策テキスト」  
 をご活用ください

## 講義 1 : ISO とは / ISMS とは / 情報セキュリティ基準・規則等の歴史 ISMS 適合性評価制度 / プライバシーマークとの違い

22 分 スライド NO.

ISO とは ?	3
ISO 規格とは ?	6
ISMS とは	7
情報セキュリティ基準・規則等の歴史	8
情報セキュリティに関連する法律、評価制度、監査制度、基準等	10
情報セキュリティ事故事例	11
ISMS 適合性評価制度	12
ISMS 認証取得組織数推移	13
ISMS 適合性評価制度 : ISMS 制度の目的 (2002 年創設期)	14
プライバシーマーク (P マーク) との違い	15
ISMS と P マークのどちらを選べばよいのか	17
参考 : 一般データ保護規制 (GDPR)	18

## ISO 入門セミナー (ISO/IEC27001)

## 講座の概要(目次)

講義	時間	スライド NO.
<b>講義 2 : ISMS の情報セキュリティ / ISMS 規格の構成</b>	<b>14 分</b>	
ISMS の情報セキュリティ		2
ここでちょっとお聞きします : 「機密性」「完全性」「可用性」に関して想定できる事故		3
ISMS 規格の構成		4
ISMS 認証を取得するためのステップ		6
<b>講義 3 : ISO/IEC27001 箇条 4</b>	<b>16 分</b>	
規格要求事項 : 4.組織の状況		2
4.1 組織及びその状況の理解		
4.2 利害関係者のニーズ及び期待の理解		
4.3 情報セキュリティマネジメントシステムの適用範囲の決定		4
適用範囲の見地 事業・組織の境界		6
適用範囲 scope		7
4.4 情報セキュリティマネジメントシステム		8
<b>講義 4 : ISO/IEC27001 箇条 5</b>	<b>12 分</b>	
規格要求事項 : 5.リーダーシップ		2
5.1 リーダーシップ及びコミットメント		
トップマネジメントの悩み		3
トップマネジメントの積極的関与が得られないと・・・		4
情報セキュリティは IT 社会の「転ばぬ先の杖」		5
5.2 方針		6
5.3 組織の役割、責任及び権限		7
<b>講義 5 : ISO/IEC27001 箇条 6</b>	<b>32 分</b>	
規格要求事項 : 6.計画		2
6.1 リスク及び機会への取組み		3
6.1.1 一般		
リスク : 目的に対する不確かさの影響		4
リスクアセスメント及びリスク対応に関する作業		5
6.1.2 情報セキュリティリスクアセスメント		6
リスクアセスメントプロセス		7
情報セキュリティリスクアセスメント		8
リスク特定		
リスク分析		9
リスク評価		10

## ISO 入門セミナー (ISO/IEC27001)

## 講座の概要(目次)

6.1.3 情報セキュリティリスク対応	11
管理策の確認	14
A10 暗号/A13 通信のセキュリティ	15
6.2 情報セキュリティ目的及びそれを達成するための計画策定	17

## 講義 6 : ISO/IEC27001 箇条 7~10

9分

スライド NO.

規格要求事項 : 7.支援	2
7.1 資源	
7.2 力量	
7.3 認識	3
7.4 コミュニケーション	
7.5 文書化した情報	4
7.5.1 一般	
7.5.2 作成及び更新	5
7.5.3 文書化した情報の管理	
規格要求事項 : 8.運用	6
8.1 運用の計画及び管理	
8.2 情報セキュリティリスクアセスメント	
8.3 情報セキュリティリスク対応	
規格要求事項 : 9.パフォーマンス評価	7
9.1 監視、測定、分析及び評価	
9.2 内部監査	
9.3 マネジメントレビュー	
規格要求事項 : 10.改善	8
10.1 不適合及び是正処置	
10.2 継続的改善	

## 参考資料

## 講義 7 : 参考資料① 附属書 A 管理目的及び管理策

36分

スライド NO.

附属書 A 管理目的及び管理策	2
A5 情報セキュリティのための方針群	3
A6 情報セキュリティのための組織	4
A7 人的資源のセキュリティ	5
A8 資産の管理	6
A9 アクセス制御	7
A10 暗号	9
A11 物理的及び環境的セキュリティ	10
A12 運用のセキュリティ	12
A13 通信のセキュリティ	13
A14 システムの取得、開発及び保守	14
A15 供給者関係	15
A16 情報セキュリティインシデント管理	16
A17 情報セキュリティ継続	17
A18 順守	18
ISMS での情報セキュリティのポイント	19
審査員が審査で確認する主なポイント	20

## 講義 8 : 参考資料② ISMS 認証取得の仕組み

14分

スライド NO.

ISMS 認証取得の仕組み	2
ISMS 認証取得のサイクル	3
初回認証審査	4
定期審査の例	5
定期審査の効果	6
認証取得のメリット	7
社内的メリット	8
対外的メリット	8
経営管理上のメリット	9
動機の背景	10