



ISMS

情報セキュリティマネジメントシステム適合性評価制度

ISMS 審査員研修コース基準

JIP-ISAC220-1.1

2006 年 6 月 1 日



財団法人 日本情報処理開発協会

〒105-0011 東京都港区芝公園 3 丁目 5 番 8 号

Tel.03-3432-9386 Fax.03-3432-6200

URL <http://www.isms.jipdec.jp/>

JIPDECの許可なく転載することを禁じます

改 版 履 歴

版数	制定 / 改訂日	改定箇所 (改訂理由)	備考
1.0	2002/4/1	初版	
1.0a	2002/10/1	名称統一：書類審査、審査を文書審査 (Stage1)、実地審査 (Stage2) に統一 誤記訂正： 1.3- b)、1.4.2、1.4.3、1.4.4、2.1-e)、 2.2.8.1.1、2.2.9.1、2.2.9.1-a)、-b)、 -c)、2.2.9.2	
1.1	2006/6/1	用語の統一、表現の見直し：全般 2.1.2、2.2.7：指針追加 2.3.1.1：備考追加 2.3.3：機関立上げ時の条件追加 2.3.5.5.3：採点差異への対応	

目 次

- 1. 適用範囲
 - 1.1 基準の目的
 - 1.2 記述内容
 - 1.3 引用規格
 - 1.4 用語の定義
 - 1.4.1 ISMS 審査員研修
 - 1.4.2 文書審査報告書
 - 1.4.3 実地審査報告書
 - 1.4.4 是正計画
- 2. 研修コースへの要求事項
 - 2.1 般
 - 2.1.1 想定する受講者
 - 2.1.2 ISMS 認証のための関連規格への準拠
 - 2.1.3 専門性の追求
 - 2.1.4 実用性の確保
 - 2.1.5 応用性の確保
 - 2.1.6 受講者の評価
 - 2.2 履修目標
 - 2.2.1 情報セキュリティに関する知識
 - 2.2.2 ISMS 適合性評価制度の知識
 - 2.2.3 ISMS 審査員研修制度の知識
 - 2.2.4 ISMS 審査員登録制度の知識
 - 2.2.5 ISMS 認証のための基準の解釈
 - 2.2.6 ISMS 構築の手順
 - 2.2.7 ISMS 審査の手順
 - 2.2.8 ISMS 審査の着眼点
 - 2.2.8.1 初回審査
 - 2.2.8.1.1 文書審査
 - 2.2.8.1.2 実地審査
 - 2.2.8.2 サーベイランス（維持審査）
 - 2.2.8.3 更新審査
 - 2.2.9 ISMS 審査報告書の書き方

- 2.2.9.1 文書審査報告書
- 2.2.9.2 実地審査報告書
- 2.2.10 審査業務一般に関する知識
 - 2.2.10.1 機密保持義務
 - 2.2.10.2 審査マナー
 - 2.2.10.3 面談技術
 - 2.2.10.4 ドキュメント調査技術
 - 2.2.10.5 報告書作成技術
 - 2.2.10.6 審査チーム
- 2.3 コースの実施要件
 - 2.3.1 コースの流れ
 - 2.3.1.1 研修時間
 - 2.3.1.2 研修日数
 - 2.3.1.3 受講者の出席義務
 - 2.3.1.4 カリキュラム
 - 2.3.1.4.1 実践的な研修
 - 2.3.1.4.2 補助教材の使用
 - 2.3.2 クラス
 - 2.3.3 講師
 - 2.3.4 施設及び設備
 - 2.3.4.1 適切な研修施設及び設備
 - 2.3.4.2 研修施設近隣での滞在
 - 2.3.5 受講者の評価
 - 2.3.5.1 研修機関による評価
 - 2.3.5.2 評価の方法
 - 2.3.5.3 修了試験
 - 2.3.5.3.1 評価の観点
 - 2.3.5.3.2 解答時間
 - 2.3.5.3.3 物品の使用・参照
 - 2.3.5.3.4 解答様式
 - 2.3.5.3.5 問題及び解答用紙の取り扱い
 - 2.3.5.4 研修中の観察評価
 - 2.3.5.4.1 継続した観察評価
 - 2.3.5.4.2 研修中の活動の評価
 - 2.3.5.4.3 成果物の評価
 - 2.3.5.4.4 ISMS 審査員適性の評価
 - 2.3.5.4.5 研修への取組みの評価

- 2.3.5.4.6 観察評価の手法
- 2.3.5.4.7 観察評価の評価点
- 2.3.5.4.8 観察評価の結果通知
- 2.3.5.5 合格判定
 - 2.3.5.5.1 合格基準
 - 2.3.5.5.2 採点の再検
 - 2.3.5.5.3 採点に誤りがあった場合への対策
- 2.3.6 再試験
 - 2.3.6.1 再試験の受験資格
 - 2.3.6.2 再試験の実施
 - 2.3.6.3 再試験の内容
 - 2.3.6.4 再試験の委託
 - 2.3.6.5 再試験の立会い

1. 適用範囲

1.1 基準の目的

本基準は、財団法人日本情報処理開発協会（以下、本協会と呼ぶ）が認定した情報セキュリティマネジメントシステム（以下、ISMS と呼ぶ）審査員研修コース（以下、研修コースと呼ぶ）の内容について、その要求事項等を定めたものである。ISMS 審査員研修を実施する研修機関は、本基準に準拠して研修コースを企画しなければならない。

1.2 記述内容

この基準では、研修機関が研修コースに盛り込むべき以下の内容について規定する。

- a) 履修目標を含む要求事項
- b) 研修コースの内容及び実施条件
- c) 受講生の評価及び修了判定

1.3 引用規格

以下に掲げる基準は、この基準の本文で引用された場合には引用の範囲に限り、この基準の一部となる。

JIP-ISAC200 ISMS 審査員研修機関認定基準

JIP-ISAC100 ISMS 審査登録機関認定基準

JIP-ISAC101(EA-7/03) ISMS 審査登録機関認定基準に関する指針

JIS Q 19011:2003 (ISO 19011:2002) 品質及び/又は環境マネジメントシステム監査のための指針

JIS Q 27001:2006(ISO/IEC 27001:2005) 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

1.4 用語の定義

この規格の目的のためには、上記引用規格に記載の該当する定義を適用するとともに、以下の定義も適用する。

1.4.1 ISMS 審査員研修

ISMS 審査員として必要な知識・ノウハウを習得することを目的とした研修。

1.4.2 文書審査報告書

文書審査 (Stage1) の結果、指摘された不適合等をまとめた報告書。

1.4.3 実地審査報告書

実地審査 (Stage2) の結果、指摘された不適合等をまとめた報告書。

1.4.4 是正計画

文書審査での指摘事項に対し、受審者が作成した是正処置の計画

2. 研修コースへの要求事項

2.1 一般

2.1.1 想定する受講者

研修コースの受講者としては、ISMS 審査業務に現在従事もしくは近い将来従事する予定で、ISMS 審査員補の資格取得を目指している者を想定する。

2.1.2 ISMS 認証のための関連規格への準拠

研修コースで受講者が習得する内容は、JIS Q 27001、JIP-ISAC100、JIP-ISAC101 の該当事項に準拠しなければならない。

2.1.3 専門性の追求

ISMS の一般的な知識の習得にとどまらず、研修コースを修了したものは ISMS 審査の実務を支障なく遂行するに足る能力を身に付けていなければならない。

2.1.4 実用性の確保

研修コースの内容は ISMS 審査の実務に即したもので、審査を遂行する上で、直ちに活用できるものでなければならない。

2.1.5 応用性の確保

研修コースの内容は ISMS 審査で想定されるあらゆる局面に応用できるものでなければならない。

2.1.6 受講者の評価

研修機関は受講中の観察評価及び修了試験を通して受講者の評価を厳密に行わなければならない。

2.2 履修目標

2.2.1 情報セキュリティに関する知識

ISMS の考え方を理解するための前提となる情報セキュリティに関する下記の知識を習得する。

a) 情報の概念と保護の必要性

情報の概念及びその類型を整理し、機密性、完全性、可用性の確保の観点からその保護の必要性を理解する。

b) 情報セキュリティの概念

下記の用語の意味を理解しながら、情報セキュリティの概略を把握する。

情報管理上の脅威、脆弱性、情報セキュリティの基本方針、リスクアセスメント、リスクマネジメント、管理策、事業継続管理、教育・訓練

c) 法律、規範、規格

セキュリティに関連する各種法規

(不正アクセス行為の禁止等に関する法律、個人情報保護に関する法律等)

規範(各種業界ガイドライン、プライバシーマーク制度等)

規格(ISO9000s、ISO14000s、ISO15408、JIS Q 15001等)

2.2.2 ISMS 適合性評価制度の知識

ISMS 適合性評価制度の目的・体系・内容・運用体制・沿革に関する知識を習得する。

2.2.3 ISMS 審査員研修制度の知識

ISMS 審査員研修制度の目的・体系・内容・運用体制に関する知識を習得する。

2.2.4 ISMS 審査員登録制度の知識

ISMS 審査員登録制度の目的・体系・内容・運用体制に関する知識を習得する。

2.2.5 ISMS 認証のための基準の解釈

ISMS 認証のための基準の各項目についてその内容を理解し、実務に即した解釈の手法を身に付ける。

2.2.6 ISMS 構築の手順

審査を受ける事業者が構築する ISMS について、下記のような作成手順を理解し、受講者自身が熟知する業務分野において実際に作成する能力を身に付ける。

- a) ISMS の適用範囲及び境界の決定
- b) ISMS の基本方針の策定
- c) リスクアセスメントの取組方法の策定
- d) リスクの識別、分析及び評価
- e) リスク対応の実行
- f) 管理目的及び管理策の選択
- g) 残留リスクの承認及び ISMS 実施の許可
- h) 適用宣言書の策定

2.2.7 ISMS 審査の手順

ISO/IEC 27001、ISO 19011、JIP-ISAC100、JIP-ISAC101 及び関連規格による ISMS 審査の一連の手順と、それぞれの内容及びその成果物を理解し、審査を実際に遂行する能力を身に付ける。

- a) 審査機関の選定
受審者が審査機関を選定する際の手順・観点を理解する。
- b) 申請書類の受付け
必要となる申請書類の種類、記述されるべき内容、申し込みから受付けまでの手続き等を理解する。
- c) 依頼内容の確認と見積及び契約
受審者からの審査依頼内容の確認の際の手順・観点を理解する。同時に、見積手法及び契約の内容を理解し、実際に見積から契約までの一連の業務を遂行できるようにする。
- d) 審査準備
審査の実施が決定した後、審査登録機関及び受審者が審査に先立ち準備すべき事柄（計画策定、審査チーム編成、チェックリスト策定など）を理解する。
- e) 文書審査
文書審査の目的と流れ、審査の手法、成果物の種類と内容、審査対象の事業者とのコミュニケーションのとり方、実地審査への移行判断基準等を理解する。
- f) 実地審査
実地審査の目的と流れ、審査の手法、成果物の種類と内容、審査対象の事業者とのコミュニケーションのとり方、実地審査及び全審査終了の判断基準等を理解する。
- g) 審査報告
指摘事項の種類と審査報告の内容、報告の手続き、審査対象の事業者とのコミュニケーションのとり方等を理解する。
- h) 是正処置及び是正報告
受審者による是正計画の策定と是正処置の内容、及びその是正報告の受領手続き等を理解する。
- i) 審査結果の判定及び登録文書の発行
是正報告の評価の手法、審査結果判定の基準及び手法、成果物の種類と内容、審査対象の事業者とのコミュニケーションのとり方等を理解する。また、合格した受審者への登録文書の発行手続きを理解する。
- j) サーベイランス（維持審査）
サーベイランスの目的と流れ、審査の手法、成果物の種類と内容、審査対象の事業者とのコミュニケーションのとり方、サーベイランス結果判定基準等を理解する。
- k) 更新審査
更新審査の目的と流れ、審査の手法、成果物の種類と内容、審査対象の事業者とのコミュニケーションのとり方、更新審査結果判定基準等を理解する。

2.2.8 ISMS 審査の着眼点

2.2.8.1 初回審査

2.2.8.1.1 文書審査

文書審査における下記のような活動毎に、一般的に留意すべき点、慎重に審査すべき点を各々理解する。

- a) 適用宣言書の分析
- b) 適用宣言書の内容を裏付けるための関連書類の調査
- c) 実地審査に先駆けて当該事業者の調査

2.2.8.1.2 実地審査

実地審査における下記のような活動毎に、一般的に留意すべき点、慎重に審査すべき点を各々理解する。

- a) 適用宣言書の作成手順の妥当性の確認
- b) 適用宣言書等成果物の内容と整合性の確認
- c) 管理目的及び管理策の有効性の確認
- d) 情報セキュリティ基本方針との適合状況の確認

2.2.8.2 サーベイランス（維持審査）

サーベイランスにおける下記のような活動毎に、一般的に留意すべき点、慎重に審査すべき点を各々理解する。

- a) 初回審査、更新審査又は前回サーベイランス以降の、審査対象の事業所及びそれを取り巻く情報セキュリティ環境の変化の確認
- b) 初回審査、更新審査又は前回サーベイランス以降の、情報セキュリティの基本方針の変更の確認
- c) 初回審査、更新審査又は前回サーベイランス以降の、情報セキュリティ基本方針との適合状況の確認

2.2.8.3 更新審査

更新審査における下記のような活動毎に、一般的に留意すべき点、慎重に審査すべき点を各々理解する。

- a) 初回審査又は前回更新審査以降の、審査対象の事業所及びそれを取り巻く情報セキュリティ環境の変化の確認
- b) 初回審査又は前回更新審査以降の、情報セキュリティの基本方針の変更の確認
- c) 初回審査又は前回更新審査以降の、情報セキュリティ基本方針との適合状況の確認
- d) サーベイランスの実施状況
- e) 更新審査時点の ISMS 適合性の審査

2.2.9 ISMS 審査報告書の書き方

2.2.9.1 文書審査報告書

下記の項目を含む文書審査報告書の記入手法を習得する。

- a) 文書審査での不適合の内容
- b) 文書審査での不適合の程度(重大・軽微の別)
- c) 文書審査での不適合の理由
- d) a)～c)の根拠資料

2.2.9.2 実地審査報告書

下記の項目を含む実地審査報告書の記入手法を習得する。

- a) 発見された不適合の内容
- b) 不適合の程度(重大・軽微の別)
- c) 不適合の理由
- d) a)～c)の根拠資料
- e) 是正処置の内容及び実施状況の評価

2.2.10 審査業務一般に関する知識

2.2.10.1 機密保持義務

審査に関連し、知り得た情報等に関する機密保持義務の存在とその手法について理解する。

2.2.10.2 審査マナー

審査を実施するにあたっては社会的常識を逸脱しないことはもとより、受審者の意図に反して受審者の業務を妨害したり、規則に抵触しないよう格別の配慮が必要であることを理解する。

2.2.10.3 面談技術

審査の各プロセスにおいて発生する面談を有効かつ円滑に進めるための面談技術を習得する。

2.2.10.4 ドキュメント調査技術

審査の各プロセスにおいて発生するドキュメント調査に関して、そのサンプリング、要点整理、関連質問等の技術を習得する。

2.2.10.5 報告書作成技術

審査報告書等の報告書の構成、図式表現、文章表現等を含む作成技術を習得する。

2.2.10.6 審査チーム

審査チームに関して、その意義、編成、役割分担等を理解し、実際にチームとして活動できるようにする。

2.3 コースの実施要件

2.3.1 コースの流れ

2.3.1.1 研修時間

研修コースは、少なくとも40時間の講義及び模擬審査等の実践的訓練で構成されなければならない。この時間には、試験、食事、休憩その他の自由時間は含まれない。但し、以下の有資格者に対する研修コースは、本協会が承認した場合に、カリキュラムの内「2.3.1.4.1 実践的な研修」を除いた研修コース（備考）を提供する事ができる。

・ISO900s、ISO14000sの審査員補、審査員、主任審査員

備考：実践的な研修を簡略化した25時間以上の研修コースを意味し、実践的な研修を排除するものではない。

2.3.1.2 研修日数

本協会の承認がない限り、所定のコース（通常5日間）を連続して実施しなければならない。

2.3.1.3 受講者の出席義務

受講者はコースの全期間出席しなければならない。講師は、出席状況を把握し受講者の観察評価に反映しなければならない。

2.3.1.4 カリキュラム

2.3.1.4.1 実践的な研修

研修カリキュラムには講義形式の他、ケーススタディ及びロールプレイング形式の実践的な研修を15時間以上織り込まなければならない。

2.3.1.4.2 補助教材の使用

ビデオおよびCD-ROM等、受講者にとり受動的な補助教材を講義の代わりに用いる場合は、合計3時間以内とする。

2.3.2 クラス

本協会の承認がない限り1クラスあたりの受講者数は、4人以上20人以下とする。

2.3.3 講師

1クラスあたり最低1人の講師を割り当てなければならない。また1クラスあたりの人数が11人以上の場合は2人の講師を同時に割り当てなければならない。但し、修了試験等に立ち会うだけの場合は1人の講師でもよい。また、各講師は担当するクラスのコースの運営全体の責任を負わなければならない。審査の実技時（本コース基準2.2.7項相当）には、ISMS主任審査員を必須の講師とする事（備考）

備考：研修機関の立ち上げ時（通常1年間位）主任審査員の確保が困難な場合は、所属する研修機関の責任者が、審査実技の講師にふさわしい能力と見識を持っていることを保証することで代用できる。

2.3.4 施設及び設備

2.3.4.1 適切な研修施設及び設備

研修機関は、研修コースを実施するにあたり適切な研修施設を準備しなければならない。研修施設には、受講者数に応じた教室、講師数に応じた控え室が確保される他、快適に研修が実施できるよう空調・照明設備等が整備されていなければならない。また、研修に必要な各種機材が完備していなければならない。

2.3.4.2 研修施設近隣での滞在

研修機関は、研修期間中、研修施設の近隣に滞在するよう受講者を指導しなければならない。また研修施設の選定に際しては、交通の便及び宿泊施設の有無に配慮しなければならない。

2.3.5 受講者の評価

2.3.5.1 研修機関による評価

研修機関は、受講者の理解度及び実行能力を評価し、修了認定を行わなければならない。

2.3.5.2 評価の方法

研修機関は、講師による研修中の観察評価、及び研修の最後に実施される修了試験により受講者を評価しなければならない。また、この評価基準は予め文書で規定しなければならない。

2.3.5.3 修了試験

2.3.5.3.1 評価の観点

本書の履修目標で挙げた各項目の理解度と実施能力を正しく評価する。

2.3.5.3.2 解答時間

修了試験の解答時間は2時間とする。ただし身体に障害がある等の理由から所定時間内に解答を完了することが難しい者については、予め申し入れがあった場合に限り、研修機関の判断により30分を上限として解答時間を延長することができる。

2.3.5.3.3 物品の使用・参照

筆記用具、電卓等研修機関が解答に必要と認めた物品、資料を除き、受講者はテスト中に使用・参照してはならない。ただし、予め申し入れがあった場合に限り、身体に障害がある等の理由による特例を、研修機関の判断により設けることができる。

2.3.5.3.4 解答様式

試験問題は、得点配分の4分の3以上が記述式解答になるよう構成されなければならない。

2.3.5.3.5 問題及び解答用紙の取り扱い

修了試験で使用した試験問題、解答用紙、答案及びこれらの写しは、当該修了試験を実施した研修機関及び本協会以外に公表してはならない。

2.3.5.4 研修中の観察評価

2.3.5.4.1 継続した観察評価

研修機関は、各受講者を継続的に観察し記録した上で、それを元に評価する。

2.3.5.4.2 研修中の活動の評価

各受講者について、質問の的確性、コミュニケーション能力、チーム活動への順応性・貢献度、討議中の発言の貢献度等について評価する。

2.3.5.4.3 成果物の評価

各受講者が作成した成果物の内容の妥当性及び表現の明確性を評価する。

2.3.5.4.4 ISMS 審査員適性の評価

研修期間全般の観察を通じて、各受講者の審査管理能力、チーム指揮能力を評価する。

2.3.5.4.5 研修への取組みの評価

研修への出欠、遅刻・早退の程度、受講マナーの遵守状況等、研修への取組み姿勢を評価する。

2.3.5.4.6 観察評価の手法

講師は研修中に各受講者毎に評価メモをつけ、毎日の研修を終えた後評価を行い、評価点をつける。同じ講義で講師が2名いる場合は、講義担当と観察評価担当とを分担するなど、観察評価にも十分時間を取ることができるよう配慮する。

2.3.5.4.7 観察評価の評価点

評価結果は、「修了の基準に達している」水準をCとした下記5段階で絶対評価する。各段階毎に一定の人数枠を設定して強制的に割り振るような相対評価は行わない。

- A 著しく優れている、B 優れている、C 修了の基準に達している、D 劣っている、E 著しく劣っている

2.3.5.4.8 観察評価の結果通知

観察評価の結果不合格になった場合は、その評価結果を当該受講者に通知しなければならない。

2.3.5.5 合格判定

2.3.5.5.1 合格基準

下記の両方の要件を満たす受講者を修了と認定する。

- a) 修了試験で満点の70%以上を得点している。
 - b) 観察評価の全評価項目の70%以上がA、B、Cの何れかに評価されている。
- ただし観察評価において特定の評価項目だけが著しく劣るため、審査実務の任に堪えないと主任講師が判断した場合は、上記の条件を満たしていても、修了は認められない。

2.3.5.5.2 採点の再検

修了試験の答えは、その採点責任が明確になるように、受講者一人分を一人の講師が全て採点しなければならない。採点の結果が満点の65～75%の場合は、再度採点しなおさなければならない。

2.3.5.5.3 採点に誤りがあった場合への対策

研修機関は、採点に誤りがあった場合や最初の採点と再度採点の結果に差異があった場合は、その内容に応じて適切な対策を取る手続きを定めなければならない。

2.3.6 再試験

2.3.6.1 再試験の受験資格

観察評価には合格したが筆記試験で不合格となった受講者は、コース修了日から1年以内に一度だけ再試験を受験できる。観察評価で不合格となったものは、筆記試験の合否に関わらず再試験を受験することが出来ず、再度研修コースを履修して修了試験を受験しなければならない。

2.3.6.2 再試験の実施

再試験は、通常不合格となった研修機関で実施しなければならない。

2.3.6.3 再試験の内容

再試験の内容は、研修コースの修了試験に準じる。ただし試験問題は修了試験とは異なるものを使用しなければならない。

2.3.6.4 再試験の委託

本協会の承認がある場合は、別の機関に再試験の実施を委託してもよい。

2.3.6.5 再試験の立会い

再試験には、研修機関の定める規程により承認された試験官が立ち会わなければならない。