



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 審査登録機関認定基準

JIP-ISAC100-1.0

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
0.8	2001.5.1	パイロット事業用として0.8版制定	
1.0	2002.3.13	<p>本格事業公開用として1.0版に改版 共通の変更は下記</p> <ul style="list-style-type: none"> ・表紙、目次、改版履歴、文書番号追加 ・本基準表記の規格を基準に変更 ・認証基準 Ver0.8 の Ver0.8 を削除 ・ISMS 規格/基準を ISMS 認証基準に変更 ・項番、備考番号付与方法を一部変更 ・その他誤記訂正、句読点変更、標準表記化等 <p>項目別改定箇所は下記</p> <p>2.2.3.1 : 明示すべきを明示が望ましいに変更</p> <p>3.1.1.2 : c) ~ g) を追加</p> <p>3.5.3 d : 適用宣言書のバージョンの明確化</p>	
1.0a	2002.4.1	本格事業用として1.0版を公開	
1.0b	2003.6.2	<p>JIS Z 9911 JIS Q 19011 に伴う変更 :</p> <p>1.2、2.1.4.3n)、2.1.5.4、2.2.2.2、2.2.2.3</p> <p>ISMS 認証基準 Ver.1.0 Ver.2.0 に伴う変更 :</p> <p>1.2 ISMS100-1.0 ISMS100-2.0</p> <p>1.3 ISO/IEC17799 JIS X 5080</p> <p>誤記訂正 : 1.3</p>	
1.0c	2006.6.1	<p>認証基準 (Ver.2.0) JIS Q 27001 及び JIS X 5080 JIS Q 27002 に伴う変更:1.2</p> <p>ISO/IEC Guide2 ISO/IEC 17000、ISO 8402 ISO 9000 に伴う変更 : 1.2、1.3</p> <p>ISMS 認証基準 ISMS 規格に変更:1.3.2、1.3.3、2.1.1.3、2.1.5.2、3.5.3b)、3.8</p> <p>訳の適正化 : 3.1.1.2b)、3.1.1.2</p>	

目 次

1. 一般
 - 1.1 適用範囲
 - 1.2 引用規格
 - 1.3 用語の定義
2. 審査登録機関に関する一般要求事項
 - 2.1 審査登録機関
 - 2.2 審査登録機関の要員
 - 2.3 審査登録要求事項の変更
 - 2.4 異議申立て、苦情及び紛争
3. 審査登録に関する要求事項
 - 3.1 審査登録の申請
 - 3.2 審査のための準備
 - 3.3 審査
 - 3.4 審査報告
 - 3.5 登録に関する決定
 - 3.6 サーベイランス及び更新審査の手順
 - 3.7 登録証及びロゴの使用
 - 3.8 組織に対する苦情の記録の閲覧

1. 一般

1.1 適用範囲

この基準は、情報セキュリティマネジメントシステム（以下、ISMSという）審査登録業務を行っている第三者機関（以下、審査登録機関という）が、その業務の遂行に関して適格であり信頼できると承認されるために遵守すべき一般要求事項を定めている。

この基準に含まれる要求事項は、ISMS審査登録を行うすべての機関に対する一般要求事項を記述している。

なお、この基準は、JIS Z 9362-1996 (ISO/IEC GUIDE 62)およびEA-7/03を基にしている。

1.2 引用規格

以下に掲げる規格、基準等は、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、この基準の一部をなす。

JIS Q 17000:2005(ISO/IEC 17000:2004) 適合性評価 - 用語及び一般原則

JIS Q 9000:2000(ISO 9000:2000) 品質マネジメントシステム - 基本及び用語

JIS Z 9362-1996(ISO/IEC GUIDE 62:1996) 品質システム審査登録機関に対する一般要求事項
EA-7/03 情報セキュリティマネジメントシステム審査登録機関の認定に関わるEA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

JIS Q 27002:2006(ISO/IEC 17799:2005) 情報技術 - セキュリティ技術 - 情報セキュリティ
マネジメントの実践のための規範

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

1.3 用語の定義

この基準の目的のためには、JIS Q 17000 及び JIS Q 9000 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。

1.3.1 組織

法人化されているか否かにかかわらず、公共又は民間の会社、法人、企業、機関、あるいはそれらの一部又は組み合わせで、独自の機能及び管理を有し、情報のセキュリティ機能を実施する能力をもつもの。

1.3.2 審査登録機関

公表されているISMS規格及び対象のISMSのもとで要求される補足文書を用いて、組織のISMSを審査し登録する第三者機関。

1.3.3 登録文書

組織のISMSが、ISMS規格及び対象のISMSのもとで要求される補足文書に適合していることを示す文書。

1.3.4 審査登録システム

審査の実施から登録文書の発行、及びその後の維持に至る手順と運営管理に関する独自の規則をもつ、審査登録機関の品質システム。

1.3.5 サーベイランス

審査登録された組織のマネジメントシステムが、引き続き維持されていることを定期的に審査すること。

1.3.6 更新審査

登録の有効期限後、登録を更新する際に実施する審査。

2. 審査登録機関に関する一般要求事項

2.1 審査登録機関

2.1.1 一般

2.1.1.1 審査登録機関がその業務を遂行するための方針及び手順は差別的であってはならない。また、それらの運用も差別的に行ってはならない。この基準に特に規定されていない限り、問い合わせ、申請などの申請者による当該機関の利用を妨げたり禁止するためにその手順を用いてはならない。

2.1.1.2 審査登録機関は、すべての申請者がそのサービスを受けられるようにしなければならない。不当な財政的又は他の条件があってはならない。サービスの提供に当たり、申請者の規模を条件にしたり、協会又はグループの会員であることを条件にしてはならない。また、既に登録した組織数によって登録に条件をつけてはならない。

2.1.1.3 申請者のISMSを審査するための基準は、ISMS規格又は申請者が遂行する機能に関連する他の規準文書に示されているものでなければならない。特定の審査登録プログラムにこれらの規準文書を適用することについての説明が求められる場合に提供する内容は、所要の技術能力をもつ適切で公平な委員会等が準備し審査登録機関が公表しなければならない。

2.1.1.4 審査登録機関は、審査登録についての要求事項、審査及び決定を当該登録範囲に特に関係する事項に限定しなければならない。

2.1.2 組織運営機構

審査登録機関の組織運営機構は、その審査登録に信頼を与えるようなものでなければならない。審査登録機関は、特に以下の要件を満たさなければならない。

- a) 公平である。
- b) 登録の授与、維持、拡大、縮小、一時停止及び取消しに関する決定に責任を負う。
- c) 以下の事項のすべてに総括的な責任をもつ管理主体（委員会、グループ又は個人）を定める。
 - 1) この基準に規定された審査及び登録の実施。
 - 2) 当該審査登録機関の運営に関する方針の策定。
 - 3) 登録に関する決定。
 - 4) 方針実施の監督。
 - 5) 当該審査登録機関の財政の監督。
 - 6) 必要に応じて、この管理主体に代わって特定の活動を行う委員会又は個人への権限の委譲。

- d) 法人格をもつ組織であることを示す文書をもつ。
- e) 公平性を確保するための組織運営機構をもち、これを文書化している。これには、当該審査登録機関の運営の公平性を保証する規定を含む。この組織運営機構によって、審査登録システムの内容及び機能に関する方針及び原則の立案に重要なかわりをもつすべての関係者が参加可能となるようにしなければならない。
- f) 登録に関する決定は、当該審査の実施者以外の者が行うようにする。
- g) 審査登録活動についての権利及び責任をもつ。
- h) 審査登録活動から生じる賠償責任等に伴う債務を履行するための適切な準備をしている。
- i) 審査登録システムの運営に必要な財政的安定性及び経営資源をもつ。
- j) 遂行する職務の種類、範囲及び量に応じて、審査登録機能に必要な教育・訓練を受け、かつ、専門的知識・経験をもつ十分な数の要員を、担当する上級の経営管理者のもとに雇用する。
- k) 審査登録システムを運営する能力について信頼を与えるように、この基準の2.1.4 に概要を示す品質システムをもつ。
- l) 組織を審査登録する活動と当該審査登録機関が行う他の活動とを区別する方針及び手順をもつ。
- m) 上級の経営管理者及び職員を含め、審査登録プロセスの結果を左右しかねないような営業上、財政上及びその他の圧力に影響されない。
- n) 審査登録プロセスに直接かわるあらゆる委員会の設置及び運営のための公式な規則及び組織運営機構をもつ。これらの委員会は、登録の決定を左右しかねないような営業上、財政上及びその他の圧力に影響されない。（備考1参照）
- o) 関連機関の活動によって、審査登録の守秘性、客観性又は公平性が影響されないようにする。また、以下の事項を申し出たり提供してはならない。
 - 1) 組織が実施している、登録の対象となるサービス。
 - 2) 登録の取得又は維持のためのコンサルティングサービス。
 - 3) ISMS又は関連するマネジメントシステムの立案、実施又は維持のためのサービス（備考2参照）。
- p) 登録又はその他の関連する事項の取り扱いに関し、組織又はその他の者からの苦情、異議申立て及び紛争を解決するための方針及び手順をもつ。

備考1：ある特定の利害関係者を優先せず利害関係の均衡を考慮して委員を選任するようになっている組織運営機構は、この基準を満足するものとみなせる。

備考2：審査登録のプロセス及び決定における守秘性、客観性、公平性を損なわない限り、直接又は間接的に他の製品、プロセス又はサービスの提供を行ってもよい。

2.1.3 下請負契約

審査登録機関が、審査登録に関連する業務（例えば、審査）を外部の機関又は個人に下請負契約することを決定する場合、機密保持及び利害抵触に関する事項を含む取決めを定めた適切な協定文書を作成しなければならない。審査登録機関は、以下の事項を満たさなければならない。

- a) 下請負契約した業務に対する全責任を負い、登録の授与、維持、拡大、縮小、一時停止又は取消しに関する責任をもつ。
- b) 下請負契約先の機関又は個人が相応の能力を持ち、この基準の該当規定を遵守するようにさせる。また、ISMSの立案、実施又は維持に、直接的であれその雇用者を介してであれ、公平性が損なわれるような形での関与がないようにさせる。
- c) 下請負について申請者又は登録組織の同意を得る。

備考：審査登録機関が、協定締結のうえ他の審査登録機関が行った業務を利用して自身の登録を授与する場合にも、a)及びb)の要求事項を適用する。

2.1.4 品質システム

2.1.4.1 審査登録の品質に執行責任をもつ経営管理者は、品質に対する目標及び品質にかかわる決意表明を含む品質方針を定め、文書化しなければならない。経営管理者は、組織のすべての階層でこの方針が確実に理解され、実施され、維持されるようにしなければならない。

2.1.4.2 審査登録機関は、この基準の該当する条項に従った、また実施する業務の種類、範囲及び量に相応した品質システムを運用しなければならない。この品質システムは文書化し、また、その文書は審査登録機関の職員が使用できるようにしなければならない。審査登録機関は、文書化した品質システムの手順及び指示が効果的に実施されるようにしなければならない。審査登録機関は、最高経営層に直接接触でき、他の責任とはかわりなく以下の事項に対する権限をもつ者を指名しなければならない。

- a) この基準に従って品質システムを確立し、実施し、維持させる。
- b) 審査登録機関の経営管理者に対し、品質システムの見直し及び改善の基礎として、品質システムの実施結果を報告する。

2.1.4.3 品質システムは、品質マニュアル及び関連する品質手順書として文書化しなければならない。また、品質マニュアルには少なくとも以下の事項を含めるか又は引用しなければならない。

- a) 品質方針の表明。

- b) 審査登録機関の法的地位の簡潔な記述。これには、所有者がいる場合はその氏名、また管理運営を行っている者がこれと異なる場合はその氏名を含める。
- c) 審査登録機能の品質に影響を与える、上級の経営管理者及びその他の審査登録要員の氏名、資格、経験及び業務分担。
- d) 上級の経営管理者から発する、権限、責任及び職務分担の系統を示す組織図。この組織図では特に審査に責任をもつ者と登録にかかわる決定に責任をもつ者との関係を示す。
- e) 審査登録機関の組織の記述。これには、2.1.2 c) で定められた管理主体（委員会、グループ又は個人）の詳細、その構成、業務分担及び運営規則を含める。
- f) マネジメント・レビューを実施するための方針及び手順。
- g) 文書管理を含む業務運営の手順。
- h) 品質に関する運営上・機能上の職責及び業務。これによって、各人の責任の範囲を関係者全員に周知させる。
- i) 審査登録機関の要員（審査員を含む）の採用及び教育訓練、並びに要員の業務の監視についての方針及び手順。
- j) 下請負契約者のリスト、及びその能力を評価し、記録し、監視するための手順の詳細。
- k) 不適合の取り扱い手順、及び実施した是正処置の有効性を保証する手順。
- l) 以下の事項を含む審査登録の実施に関する方針及び手順。
 - 1) 登録文書の発行、保留及び取消しの条件。
 - 2) ISMS審査登録に用いる文書の利用及び適用の点検。
 - 3) 組織のISMSの審査及び登録の手順。
 - 4) 登録組織のサーベイランス及び更新審査の手順。
- m) 異議申し立て、苦情及び紛争の取り扱いに関する方針及び手順。
- n) JIS Q 19011 の規定に基づいて内部監査を実施する手順。

2.1.5 登録の授与、維持、拡大、縮小、一時停止及び取消しに関する条件

2.1.5.1 審査登録機関は、登録の授与、維持、拡大及び縮小に関する条件、並びに組織の登録範囲の一部又は全登録の一時停止又は取消しに関する条件を規定しなければならない。また、審査登録機関は、組織がISMSに何らかの変更を行う場合、又は適合性に影響を与える可能性のあるその他の変更を行う場合に、その旨を速やかに当該審査登録機関に通知するよう組織に要求しなければならない。

2.1.5.2 審査登録機関は、組織に対して、適用するISMS規格又はその他の規準文書に適合する、文書化したISMSをもつよう要求しなければならない。

2.1.5.3 審査登録機関は、以下の手順をもっていなければならない。

- a) 登録の授与、維持、取消し、及び該当する場合は登録の一時停止。
- b) 登録範囲の拡大又は縮小。
- c) 組織の活動及び運営に重大な影響を与える変更があった場合（例えば所有者、要員又は設備の変更など）、又は、苦情若しくはその他の情報の分析結果からその組織が当該審査登録機関の要求事項に適合していないことが明らかになった場合の再審査。

2.1.5.4 審査登録機関は、以下の事項について、要請に応じて提示できる手順書をもっていなければならない。

- a) JIS Q 19011 及びその他の関連文書に準拠して行う、組織のISMSの初回審査。
- b) JIS Q 19011 に準拠して定期的実施する組織のISMSのサーベイランス及び更新審査。このサーベイランス及び更新審査は、組織のISMSが該当する要求事項に継続的に適合していること及び組織がすべての不適合に対して適時に是正処置を実施していることを検証し記録するために行う。
- c) 登録についての不正確な言及又は誤解を招くような登録情報の利用などに関する不適合及びこれらに対して組織が実施する適時な是正処置の必要性を明確にし記録すること。

2.1.6 内部監査及びマネジメントレビュー

2.1.6.1 審査登録機関は、自身の品質システムが実施され有効であることを検証するために、計画的かつ体系的な方法ですべての手順について定期的な内部監査を実施しなければならない。審査登録機関は以下の事項を確実に実施しなければならない。

- a) 監査された範囲に責任をもつ要員に対する監査結果の通知。
- b) 適時かつ適切な是正処置の実施。
- c) 監査結果の記録。

2.1.6.2 審査登録機関の執行責任をもつ経営管理者は、当該審査登録機関の品質システムが、この基準の要求事項、品質方針及び品質目標を満足するうえでの適切性及び有効性を継続して確保するに足る定められた間隔で、その品質システムの見直しを行わなければならない。見直しの記録は維持しなければならない。

2.1.7 文書化

2.1.7.1 審査登録機関は、以下の事項を文書化し、定期的に更新し、要請に応じて（出版物、電子媒体又は他の手段を用いて）提示できるようにしなければならない。

- a) 当該審査登録機関の業務実施のよりどころとなる権限についての情報。
- b) 登録の授与、維持、拡大、縮小、一時停止及び取消しの規則及び手順を含む、審査登録システムの説明。

- c) 審査及び登録のプロセスについての情報。
- d) 当該審査登録機関の財政基盤の安定性を確保する手段の記述、並びに申請者及び登録組織が支払うべき費用に関する一般情報。
- e) 申請者及び登録組織の権利及び義務の記述。これには、当該審査登録機関のロゴの使用方法及び授与された登録についての言及方法に関する要求事項又は制約事項を含める。
- f) 苦情、異議申し立て及び紛争の処理手順に関する情報。
- g) 所在地及び授与された登録範囲の記述を含む、登録組織の名簿。

2.1.7.2 審査登録機関は、審査登録機能に関するすべての文書及びデータを管理する手順を確立し維持しなければならない。これらの文書類は、最初の作成、又はその後の訂正若しくは変更に際して、適切に権限を与えられた適格な者が、発行前にその妥当性を検討し承認しなければならない。版及び/又は改訂状態を識別したすべての適切な文書のリストを維持しなければならない。これらすべての文書の配布を管理し、申請者、又は登録組織の活動に関する機能の遂行に必要な場合には当該審査登録機関の要員又は組織が、適切な文書を確実に利用できるようにしなければならない。

2.1.8 記録

2.1.8.1 審査登録機関は、当該審査登録機関の状況に適しかつ法規にも適合する記録の体系を維持しなければならない。記録は、審査登録の手順、特に申請書、審査の報告書及び登録の授与、維持、拡大、縮小、一時停止又は取消しに関する他の文書についての手順が、効果的に実施されていることを実証するものでなければならない。記録は業務プロセスの完全さ及び情報の機密保持が確保できるように識別し、管理し、処分しなければならない。記録は、継続的な信頼が実証できるように、最短でも一審査登録サイクル、又は法律で要求される場合は、その期間は保持しなければならない。

2.1.8.2 審査登録機関は、契約上、法律上又は他の義務で定められた期間にわたって記録を維持するための方針及び手順をもっていなければならない。審査登録機関は、記録の利用に関してこの基準の2.1.9 に沿った方針及び手順をもっていなければならない。

2.1.9 機密保持

2.1.9.1 審査登録機関は、当該審査登録機関の名のもとに活動する委員会及び外部の機関又は個人を含む組織のすべての階層において、審査登録活動の過程において得られた情報の機密を保護するために、該当の法律に従った適切な取決めをもっていなければならない。

2.1.9.2 この基準で特に定められている場合を除き、ある特定の組織に関する情報は、その組織の書面での同意がない限り第三者に開示してはならない。法律で第三者に情報を開示するよう要求されている場合は、法律に従って開示する情報をその組織に通知しなければならない。

2.2 審査登録機関の要員

2.2.1 一般

2.2.1.1 審査登録に携わる審査登録機関の要員は、遂行する職務に関し適格でなければならない。

2.2.1.2 審査登録機関は、審査登録プロセスにかかわる要員各人についての、関連資格、教育訓練及び経験に関する最新情報を保有していなければならない。教育訓練及び経験の記録は常に最新の状態にしておかななければならない。

2.2.1.3 職務及び責任を記述した明確な指示書を要員が利用できるようにしておかななければならない。これらの指示書は最新の状態にしておかななければならない。

2.2.2 審査員及び技術専門家の資格基準

2.2.2.1 審査登録機関は、審査を有効かつ一様に実施できるようにするために、審査能力に関する最低限の基準を定めなければならない。

2.2.2.2 審査員は、該当する国際文書の要求事項を満たさなければならない。ISMSの審査に関しては、該当する審査及び審査員の指針は、JIS Q 19011 に規定されている。

2.2.2.3 技術専門家は、JIS Q 19011 に規定されている審査員に対する要求事項に適合することは要求されていない。その個人的特質についての指針としてJIS Q 19011 の7項を適用できる。

2.2.3 選定手順

2.2.3.1 審査員及び技術専門家の選定全般

審査登録機関は、以下の事項に関する手順をもっていなければならない。

- a) 審査能力、教育訓練、資格及び経験に基づいて、審査員及び必要な場合は、審査に該当する技術分野において特定の能力をもつ技術専門家を選定する（その際、技術専門家はISMS審査員の代わりとしての役割を果たすことができないことを明示することが望ましい）。
- b) 初期に審査員及び技術専門家の審査中の行動を評価し、その後も業務遂行状況を監視

する。

2.2.3.2 個々の審査業務の割当て

ある一つの審査を担当させる審査チームを選定する場合、審査登録機関はその審査チームの技量が担当する審査に対して適切なものとなるようにしなければならない。

審査チームは、以下の事項を満足しなければならない。

- a) 適用される法規制、審査登録の手順及び審査登録の要求事項に精通している。
- b) 該当する審査方法及び審査文書について十分な知識をもっている。
- c) 登録対象となる活動に関する適切な専門的知識をもっている。また、該当する場合は、それらの活動に関連する手順の内容及び情報セキュリティの不具合が生じる可能性についての知識をもっている。(審査員でない技術専門家がこの役割を果たしてもよい。)
- d) 組織が活動、製品又はサービスの情報セキュリティ面を管理する能力に関して、信頼できる審査をするのに十分な程度の理解力をもっている。
- e) 要求された言語で文書及び口頭の両方で効果的に意思疎通ができる。
- f) 審査チームメンバーが不公平又は差別的な行動をとる原因となるようないかなる利害関係もない。例えば、
 - 1) チームメンバー又はメンバーの所属組織が、申請者又は登録組織に対し、審査登録のプロセス及び決定の公正さを損ねるようなコンサルティングサービスを行ったものであってはならない。
 - 2) 審査登録機関の指示書に従って、チームメンバーは、メンバー自身又はメンバーの所属組織と審査される組織との間の、現在の関係、過去の関係及び予定されている関係について、審査に先立って当該審査登録機関に通知しなければならない。

2.2.4 審査要員との契約

審査登録機関は、審査に携わる者(以下、審査要員という。)に対し、当該審査登録機関が規定した規則に従うことを約束する契約書又はその他の文書に署名することを要求しなければならない。この契約書又はその他の文書には、機密保持に関する事、並びに審査される組織との間の営業上及びその他の利害関係並びに過去又は現在の関係に影響されないことが含まれていなければならない。審査登録機関は、下請負契約した審査要員がこの基準に定める審査要員に対するすべての要求事項を満たすようにし、また、そのための方法を文書化しなければならない。

2.2.5 審査要員の記録

2.2.5.1 審査登録機関は、審査要員に関する以下の事項からなる記録を保持し、最新の状態に維持しなければならない。

- a) 氏名及び住所。

- b) 組織における所属及び地位。
- c) 学歴及び専門的資格。
- d) 当該審査登録機関が審査能力をもつ各分野における経験及び教育訓練。
- e) 直近の記録更新日付。
- f) 業績の査定。

2.2.5.2 審査登録機関は、すべての下請負契約機関に対し、その下請負機関の管理下において当該審査登録機関が主管する審査業務に従事する審査要員について、この基準の要求事項を満たす記録を維持するようにさせ、また、これを検証しなければならない。

2.2.6 審査チームのための手順

審査チームには、最新の審査指示書、並びに審査登録についての取決め及び手順に関するすべての関連情報を提供しなければならない。

2.3 審査登録要求事項の変更

審査登録機関は、審査登録の要求事項を変更しようとする場合には、十分な期間において適切な予告をしなければならない。審査登録機関は、変更にかかわる正確な内容及び発効日を決定する前に、利害関係者が表明した見解を考慮しなければならない。審査登録機関は、要求事項の変更に関する決定及びその公表の後に、当該機関が合理的であるとする期間内に登録組織が自らの手順に対して必要な対応を行ったことを、検証しなければならない。

2.4 異議申立て、苦情及び紛争

2.4.1 審査登録機関は、組織又はその他の者から当該審査登録機関に持ち込まれる異議申立て、苦情及び紛争を定められた手順に従って処理しなければならない。

2.4.2 審査登録機関は、以下の事項を実施しなければならない。

- a) 審査登録に関するすべての異議申立て、苦情及び紛争の記録、並びに修正処置の記録。
- b) 適切な是正処置及び予防処置。
- c) 実施した処置の文書化、及びそれら処置の有効性の評価。

3. 審査登録に関する要求事項

3.1 審査登録の申請

3.1.1 手順に関する情報

3.1.1.1 審査登録機関は、審査及び登録の手順の詳細な説明書、審査登録のための要求事項を記述した文書、並びに登録組織の権利及び義務を記述した文書を、2.1.7.1 に規定したとおりに最新状態に維持し、申請者及び登録組織に提供しなければならない。

3.1.1.2 審査登録機関は、組織に対し以下の事項を要求しなければならない。

- a) 審査登録のプログラムにかかわる該当規定に常に適合する。
- b) 審査の実施に必要な準備をすべて行う。この準備には、当該審査登録機関が行う審査、サーベイランス、更新審査及び苦情の解決のために必要な、文書の調査並びにすべての場所への立ち入り、記録（内部監査報告及び情報セキュリティの独立したレビューの報告を含む）の閲覧及び組織側との面接のための用意を含む。
- c) 登録の対象となっている活動についてだけ登録されていることを表明する。
- d) 授与された登録を、当該審査登録機関の評価を損なうような使い方をせず、また、誤解を招く又は認められた範囲を逸脱すると当該審査登録機関が考えるような登録に関する表明を行わない。
- e) どのように決定されようと、登録の一時停止又は取消しを受けたら、登録を引用しているすべての宣伝・広告を中止し、当該審査登録機関の要求どおりに登録文書を返却する。
- f) ISMSが適用規格又は他の基準文書に適合していることを示すためにだけ登録を使用し、当該審査登録機関によってサービスが適格であると承認されたと思わせるように、登録を利用しない。
- g) 登録文書、マーク、報告書及びそれらの一部であっても、誤解を招くような方法では使用しないようにする。
- h) 文書、パンフレット又は宣伝・広告などの媒体で登録について触れる場合には、当該審査登録機関の要求事項に従う。

3.1.1.3 申請された登録範囲が特定のプログラムに関係する場合には、申請者に対して必要な説明をしなければならない。

3.1.1.4 求められた場合には、申請に関する追加情報を申請者に提供しなければならない。

3.1.2 申請

3.1.2.1 審査登録機関は、申請者に対して、必要事項をすべて記入し権限をもった申請者代表が署名した正式な申請書を提出するよう要求しなければならない。申請書又はその

添付書には以下の事項が含まれていなければならない。

- a) 希望する登録範囲の明確な記述。
- b) 審査登録に関する要求事項を遵守し申請者の評価に必要なすべての情報を提供する旨の申請者の同意。

3.1.2.2 申請者は、実地での審査前に少なくとも以下の情報を提供しなければならない。

- a) 申請者の法人概要。すなわち、名称、所在地、法的地位並びに該当する場合は人的資源及び専門的資源。
- b) ISMS及びその対象となる活動にかかわる一般情報。
- c) 登録を希望するシステム並びに適用する規格又はその他の規準文書の記述。
- d) ISMSマニュアルの写し及び要求のある場合には関連文書一式。

申請書類及びISMSマニュアルの検討で得た情報は実地での審査の準備に使用できるが、適切な機密保持を行わなければならない。

3.2 審査のための準備

3.2.1 審査登録機関は、以下の事項を確実にを行うために、審査を始める前に審査登録に関する申請者の要請内容の確認を行い、その記録を維持しなければならない。

- a) 審査登録のための要求事項が、明確に規定され文書化され理解されている。
- b) 審査登録機関と申請者との間に生じる理解の違いはすべて解消されている。
- c) 審査登録機関は、申請登録範囲、申請者の業務実施場所及び特別な要請（例えば申請者の使用言語）に応じて審査登録サービスを実施する能力をもつ。

3.2.2 審査登録機関は、必要な準備作業の管理ができるように、審査活動の計画を作成しなければならない。

3.2.3 審査登録機関は、審査登録機関を代表して、申請者から収集した全資料を評価し審査を実施するのに適格な審査チームを指名しなければならない。審査する範囲の専門家を助言者として審査チームに加えてもよい。

3.2.4 審査登録機関は、審査を実施する審査チームメンバーの氏名を組織に通知しなければならない。この通知には、特定の審査員又は専門家の指名に対して異議申立てをする場合に必要となる情報を付し、また、十分な予告期間をおくこと。

3.2.5 審査登録機関は、審査チームを正式に任命し、そのチームに適切な作業文書を与えなければならない。審査計画及び審査日については組織と合意しなければならない。審査チームが実施すべき業務を明確に定め、組織にも通知しなければならない。この業務

命令は、組織の組織運営機構、方針及び手順を調査し、かつ、これらが登録範囲に関するすべての要求事項を満足していることを確認し、さらに、これらの手順が実施され、組織のISMSに対して信頼を与えるものであることを確認するよう、審査チームに要求するものでなくてはならない。

3.3 審査

審査チームは、審査すると定めた範囲に含まれる組織のISMSを、適用されるすべての審査登録の要求事項を基準として審査しなければならない。

3.4 審査報告

3.4.1 審査登録機関は、自らの必要性に合った報告の手順を採用してよいが、この手順は最小限、以下の事項を确实なものとするものでなければならない。

- a) 審査場所を離れる前に審査チームと組織の経営管理者との間で会議をもち、その会場の場で、審査チームが審査登録の要求事項に対する組織のISMSの適合性に関して書面又は口頭で特に重要と思われる事項を示す。また、審査チームが検出した事項及びその根拠について組織に質問の機会を与える。
- b) 審査チームが、すべての審査登録の要求事項に対する組織のISMSの適合性に関して検出した事項の報告書を当該審査登録機関に提出する。
- c) 審査登録機関は、審査の結果に関する報告書を速やかに組織に送付する。この報告書では、すべての審査登録の要求事項に適合するために是正すべき不適合を特定する。
- d) 審査登録機関は、組織に対し報告書への意見の提出を求め、また、審査時に明らかになった審査登録の要求事項に対する不適合を是正するために実施した処置、又はある一定の期間内に実施を計画している処置について書面による回答を求めなければならない。次に、審査登録機関は全面的又は部分的な再審査が必要かどうか、又は処置に関する書面での回答をサーベイランス中に確認することで十分と認められるかどうかについて、組織に通知しなければならない。
- e) 報告書は、少なくとも以下の事項を含まなければならない。
 - 1) 審査の日付。
 - 2) 報告書に責任をもつ者の氏名。
 - 3) 審査を実施した対象の明記（例えば、施設の名称及び所在地、並びに審査した組織の部門）。
 - 4) 審査した登録範囲又はその登録範囲を示す文書の参照（適用規格又は適用規準文書の参照を含む）。
 - 5) 不適合についての明確な記述を含む、審査登録の要求事項に対する組織のISMSの適合性に関する意見、及び該当する場合には以前の審査結果との有益な比較。
 - 6) 終了時の会議で組織に提示した情報との相違の説明。

- 3.4.2 審査登録機関が正式に承認した最終報告書が3.4.1 c)及びe)で述べた報告書の内容と異なる場合には、前の報告書との差異に関する説明をつけて組織に提出しなければならない。最終報告書を作成する場合には、以下の事項を考慮しなければならない。
- a) 面談した組織側職員の資格、経験及び権限。
 - b) ISMSに対する信頼を与えるために組織が採用している内部の組織及び手順の適切性。
 - c) 明らかになった不適合を是正するために組織がとった処置。これには、該当する場合には、以前の審査で明らかになった不適合についての処置も含む。

3.5 登録に関する決定

- 3.5.1 組織のISMSを登録するか否かの決定は、審査プロセスで収集した情報及び他の関連情報に基づいて、当該審査登録機関が行わなければならない。登録の決定を下す者は、当該審査に参加した者であってはならない。

- 3.5.2 審査登録機関は、登録の授与、維持、拡大、縮小、一時停止又は取消しを行う権限を外部の個人又は機関に委譲してはならない。

- 3.5.3 審査登録機関は、ISMSを登録する各組織に対し、権限を与えられた者が署名した、例えば、書簡又は証明書のような登録文書を交付しなければならない。これらの文書では、以下の事項を記載することによって、組織及び登録の対象となる各情報システムを特定しなければならない。

- a) 名称及び所在地。
- b) 以下の事項を含む、授与された登録範囲。
 - 1) ISMSを審査登録するに当たって、基準としたISMS規格、及び該当する場合はその他の規準文書。
 - 2) 製品、プロセス又はサービスの分類についての組織の活動。
- c) 登録の発効日付及び有効期間。
- d) 適用宣言書のバージョンの明記。
- e) 該当する審査登録機関、認定及びその他のロゴやマーク

- 3.5.4 既に授与した登録に対する登録範囲の変更申請は、当該審査登録機関が処理しなければならない。審査登録機関は、範囲を変更して登録を授与すべきか否かを定めるために、どのような審査手順が適切であるかを決定し、その手順に従って実行しなければならない。

3.6 サーベイランス及び更新審査の手順

3.6.1 審査登録機関は、ISMSを登録した組織が審査登録の要求事項に引き続き適合していることを検証するのに妥当な間隔で、定期的なサーベイランス及び更新審査を実施しなければならない。

備考：定期的なサーベイランスの間隔が1年を超えると、多くの場合、この条項の要求事項を満たすとは考えられない。

3.6.2 サーベイランス及び更新審査の手順は、この基準に規定された組織のISMSの審査に関する手順と整合するものでなければならない。

3.7 登録証及びロゴの使用

3.7.1 審査登録機関は、ISMS登録のマークやロゴの所有権、使用及び表示を適切に管理しなければならない。

3.7.2 審査登録機関がISMSが登録されていることを示すためにシンボル又はロゴを使用する権利を与えたときには、組織は指定されたシンボル又はロゴを、審査登録機関が書面で承諾した方式でのみ使用することができる。登録組織には、このシンボル又はロゴを、製品それ自体に付けたり、製品の適合性を示すと解釈されるような方法で使用させてはならない。

3.7.3 審査登録機関は、宣伝、カタログなどにおける、審査登録システムについての不正確な言及、又は登録証及びロゴの誤解を招くような使用に対して、相応の処置をとらなければならない。

備考：このような処置には、是正処置、登録証の取消し、違反の公表、及び必要に応じて他の法的手段をとることが含まれる。

3.8 組織に対する苦情の記録の閲覧

審査登録機関は、ISMSを登録している各組織に対して、ISMS規格又は他の規準文書の要求事項に従ってすべての苦情及び是正処置を記録し、当該審査登録機関が必要に応じて利用できるようにすることを要求しなければならない。