



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に関する指針

JIP-ISAC101-1.0

2005年4月26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

Email info@isms.jipdec.jp

JIPDECの許可なく転載することを禁じます

1. 目的

この指針は、ISMS 審査登録機関認定基準（JIP-ISAC100）の、ISMS 審査登録機関に対する一般要求事項の条項に適用する指針を示すものであり、財団法人日本情報処理開発協会（以下、本協会という）が EA¹による文書 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する EA 指針²）を日本語化し、ISMS 適合性評価制度（以下、本制度という）に適用できるようにしたものである。

2. 指針の構成

1) この指針は、EA-7/03 原文³（以下、EA-7/03 英語版という）を日本語に翻訳したものを（以下、EA-7/03 日本語版という）を採用し、本制度に適用するために、本協会の指針（以下、JIPDEC 指針という）を追加したものである。

備考：EA-7/03 日本語版は、JIPDEC が本指針に使用するために EA の許可を得て EA-7/03 英語版を翻訳したものであり、必要と思われる部分には注記を追加している。

2) EA-7/03 英語版にある「ISO/IEC Guide 62（ISMS に適用できるよう最小限の修正を加えたもの）」の部分は、本制度では認定基準として「ISMS 審査登録機関認定基準（JIP-ISAC100）」を使用するため、EA-7/03 日本語版には含めていない。

3. JIPDEC 指針

JIP.1 EA-7/03 日本語版に対し、本指針では以下の規格の読み替えを行う。

EA-7/03 日本語版	本指針での読み替え
ISO/IEC Guide 62	JIP-ISAC100
ISO 10011-1～3	JIS Q 19011

JIP.2 指針 G.1.3.2 では、附属書 1 の「経済活動に関する統計的分類基準」に基づいて認定範囲を決める様になっているが、本制度ではこの分類を認定範囲に適用しない。審査登録機関は、ISMS 認証審査において、必要により審査チームに技術専門家を加えて審査可能か否かを判断し、可能な場合のみ審査を行うものとする。審査登録機関は、審査可能か否かを判断するための文書化された手順をもつことが望ましい。

¹ EA : European co-operation for Accreditation

² EA 指針 : EA Guidelines for the Accreditation of Bodies Operating Certification/Registration of Information Security Management Systems

³ 本協会は、EA-7/03 の著作権は EA が保持しており、正本は英語版であることを認めている。

JIP.3 指針 G.2.1.9 の「EA 加盟の認定機関から認定を受けた審査登録機関によって、EA 発行の指針に限定されることが望ましい」の部分は、本制度に適用するために「認定された審査登録機関によって、認定機関から発行された指針に限定されることが望ましい」と読み替える。

JIP.4 「内部セキュリティレビュー」の用語は、組織においてリスク分析に続いて行う見直し (review) 作業のことをいう。この見直しでは、組織はセキュリティの状態と、改善のための計画及び対象 (targets) を定める。この見直しの結果に基づいて内部監査のようなその後の活動を実施することが望ましい。

備考：この説明は EA に確認した結果に基づいている。

JIP.5 指針 IS.4 c) の「5 日間の研修を成功裏に終了していること」の部分は、本制度では「認定された 5 日間又は 3 日間の研修を成功裏に終了していること」と読み替える。

備考：「5 日間の研修」及び「3 日間の研修」は、審査員研修機関の認定された研修コースを意味し、日数を規定するものではない。

JIP.6 指針 IS.9.1 の「審査 (ステージ 1)」及び「審査 (ステージ 2)」は、本制度ではそれぞれ「文書審査 (ステージ 1)」及び「実地審査 (ステージ 2)」と言っているが、文書審査 (ステージ 1) は、文書審査のみに限定するものではない。

JIP.7 指針 IS.14 e) の「更新審査の方法は、審査の方法と同様」の部分は、本制度では「更新審査の方法は、初回審査の方法と同様」と読み替える。

JIP.8 指針 3.3.1 の「審査、又は更新審査」の審査は、初回審査、サーベイランス等を含んでいる。



European
co-operation for
Accreditation

**Publication
Reference**

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
認定に関する
EA 指針

目的

この文書は、欧州認定協力機構（EA: European cooperation for Accreditation）の作業部会によって作成されたものである。この文書の目的は、情報セキュリティマネジメントシステムの分野において、認定機関、認定審査員、及び認定申請の準備を行っている審査登録機関が ISO/IEC Guide 62/EN 45012 を矛盾なく適用できるようにするために説明を提供することである。この文書は、1999 年 11 月に EA 総会で承認されている。

ISO/IEC Guide 62/EN 45012 は正式文書であり、この文書の適用に関して紛争のある場合は、個々の認定機関が裁定を下すことになる。

著者

この文書は、情報通信技術に関する作業部会 EA C5 WG7 によって作成された。

公式言語

この文書は必要に応じて他の言語に翻訳できるが、英語版を正式文書とする。

著作権

この文書の著作権は EA が保有する。この文書を転売目的で複製することを禁ずる。

追加情報

この文書に関して追加情報が必要な場合は、自国の EA 加盟組織に問い合せ下さい。最新情報については、当機関のホームページ <http://www.european-accreditation.org> を参照下さい。

日本語版について

この EA-7/03 日本語版は、EA-7/03 英語版を ISMS 適合性評価制度（以下、本制度という）の指針として使用するために、財団法人日本情報処理開発協会（以下、本協会という）が EA の許可を得て日本語に翻訳したものである。

この中で点線の下線部分は、EA-7/03 英語版にない事項である。

この EA-7/03 日本語版の著作権は本協会が保有する。この文書を本協会の許可なく転載することを禁ずる。

2005 年 4 月 26 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

Email info@isms.jipdec.jp

目 次

はじめに - 情報セキュリティマネジメントシステム (ISMS) 審査登録機関の認定に関する EA 指針について -	4
序文 - ISMS の審査登録について -	5
1. 一般	6
1.1 適用範囲	6
1.2 引用規格	6
1.3 用語の定義	6
2. 審査登録機関に関する一般要求事項	7
2.1 審査登録機関	7
2.2 審査登録機関の要員	13
2.3 審査登録要求事項の変更	17
2.4 異議申立て、苦情及び紛争	17
3. 審査登録に関する要求事項	18
3.1 審査登録の申請	18
3.2 審査のための準備	18
3.3 審査	18
3.4 審査報告	22
3.5 登録に関する決定	22
3.6 サーベイランス及び更新審査の手順	23
3.7 登録証及びロゴの使用	25
3.8 組織に対する苦情の記録の閲覧	26
附属書 1: 認定範囲	27

はじめに - 情報セキュリティマネジメントシステム (ISMS) 審査登録機関の認定に関する EA 指針について -

この文書は、ISO/IEC Guide 62 : 1996 (EN 45012:1998 と同じもの)、ISO/IEC Guide 62 に関する IAF 指針、及び ISMS 審査登録機関に対する EN45012 の適用に関する EA 作成の追加指針という 3 つの主要な文書をもとに作成された。 Guide 62 及び IAF 指針は、情報セキュリティマネジメントシステム (ISMS) に適したものとなるよう必要に応じて修正されている。こうした原文の (最小限の) 修正作業及び ISMS 指針の作成は、当初 UKAS 後援の英国作業部会が実施し、その後情報通信技術に関する EA 作業部会 EA-C5-WG7 に引き継がれた。

この文書の出典は、以下に示す書体によって識別できる。

- ・ISO/IEC Guide 62 (ISMS に適用できるよう最小限の修正を加えたもの)。EA はこの文書の所有権が ISO にあることを認めており、ISO/IEC が最新版を発行した場合にはこの文書を改訂する予定である。

注記:EA-7/03(日本語版)では、この部分は項目のみを記載している。

- ・ISO/IEC Guide 62 に関する IAF 指針 - ISMS に適用できるよう最小限の修正を加えたもの。
- ・特に ISMS についての ISO/IEC Guide 62 に関する EA 指針。

この文書において“ ~なければならない (shall) ”という表現は、ISO/IEC Guide 62 の要求事項を反映した強制規定を示すために使用されている。この文書において“ ~望ましい (should) ”という表現は、要求事項を適用するための指針であるが、審査登録機関において採用することが期待される規定を示すために使用されている。この指針に対し審査登録機関が変更を加えた場合、その変更はすべて特例とする。こうした変更は、審査登録機関が認定機関に対し、ISO/IEC Guide 62 の関連条項及びこの指針の目的に準じたものであることを実証した場合に限り、個別に認められる。

序文 - ISMS の審査登録について -

情報セキュリティマネジメントシステム (ISMS) に関する規格は、組織に対し、最良の実践規範を定めたものである。英国規格 BS 7799 Part 2 及びその他の規準文書は情報セキュリティマネジメント仕様であり、ISMS の審査登録に適している。これらの規格は、現在利用されている情報セキュリティのベストプラクティス (最良の実践方法) から成る、包括的なセキュリティ管理策を提供するものである。また、これらの規格の目的は、組織に対して情報セキュリティのための共通基盤を提供し、組織間での情報共有を可能にすることである。これは、各組織が電子的な相互接続を希望する場合特に重要となる。

組織の情報セキュリティマネジメントシステム (ISMS) の審査登録は、登録を受けた組織が規格又は規準文書に従って情報セキュリティマネジメントシステムを実施しているという信頼を与える一つの手段である。

この文書は、審査登録機関が第三者審査登録システムを一貫した信頼できる方法で確実に運用するために遵守すべき要求事項を規定し、これによって国内外における審査登録システムの受け入れを促進するものである。また、この文書は適切な各国のシステムを国際貿易のために承認する基礎となるべきものである。

この文書は、ISMS を審査し登録する機能を果たす機関 (機関名にこだわらない) が使用するためのものである。この文書では便宜上この機関を総称して「審査登録機関」と呼ぶ。この用語は、この文書が規定する活動を行う別の呼称の機関がこの文書を使用することを妨げるものではない。この文書は、ISMS の審査登録に関連するすべての機関が利用できるべきものである。

ISMS の審査登録は、組織の ISMS の評価に関わるものであって、組織の製品やサービスに関連する情報セキュリティが一定レベルに達していることを意味するものではない。規格又は規準文書及び補足文書 (もしあれば) への適合の証拠は、登録文書の形をとる。ISMS の審査登録は、組織がリスクアセスメントを実施し、事業で必要とされる情報セキュリティに適した管理策を明確にし、実施していることの証ともなる。

ISMS の審査登録はまったくの任意である。審査登録プロセスを経て登録を受けた組織は、自らの情報セキュリティマネジメントに対してよりいっそう信頼を置くことができ、また登録証によって情報を共有する取引先からも信頼を得ることができる。この登録証によって、組織は情報セキュリティ対策の詳細を機密情報として保持する一方で、情報セキュリティマネジメント能力を保有していることを公式に表明することができる。

この文書は、審査登録機関が適格であることを承認する機関が使用するためのものであるが、ここに含まれている多くの条項は第三者監査手順にも役立つであろう。

1. 一般

1.1 適用範囲

1.2 引用規格

1.3 用語の定義

IAF 指針

G.1.3.1. この文書の指針には以下の定義が適用される。

審査： 組織の審査登録に関連するすべての活動。これは、当該組織が登録の授与に必要な所定の規格に定める関連条項の要求事項をすべて満たしているかどうか、及びその要求事項が適切に実施されているかどうかを判定するための活動である。これには、文書審査、実地審査（audit）、審査報告書の作成・検討、及び登録の決定を行うのに十分な情報を得るために必要なその他の関連活動が含まれる。

ロゴ： 識別の形のの一つとして機関が使用するシンボルで、通常は図案化されている。マークがロゴとなることもある。

マーク： 法的に登録された商標、又はその他の保護されたシンボルで、認定機関又は審査登録機関の規則に基づいて発行されるもの。このマークは、機関の運用するシステムが十分に信頼できるものであることが実証されていること、又は関連する製品や個人が所定の規格の要求事項を満たしていることなどを示すものである。

不適合： マネジメントシステムの要求事項のうち、一つ又は複数欠けているか又は実施・維持されていないこと、あるいは組織のセキュリティ基本方針及び目標を達成する ISMS の能力に関して、客観的な証拠に基づいた重大な疑いが生じる状況。

審査登録機関は、自らの裁量で欠陥の分類及び改善領域を定めることができる（例えば重大な不適合、軽微な不適合、観察事項など）。但し、上記の不適合の定義に相当する欠陥がある場合は、指針 G.3.5.2 及び G.3.6.1 に従って対処することが望ましい。

G.1.3.2. 審査登録機関が認定される範囲は、「認定範囲」（附属書 1 を参照）と呼ばれる産業分野・製品分類一覧のうちの一つ又は複数の項目に基づいて示される。

G.1.3.3. 例えば特定の事務所やその所在地等の限定など、他にも認定に対して制限が課せられることもある。

ISMS 指針

IS.1 審査登録機関の認定範囲は審査員の力量と密接に関連しており、これは組織が ISMS を構築及び維持する場合に行うリスク分析の審査を実施する際に特に重要である。審査登録機関は、審査員が ISMS の審査登録を行う産業分野において適格であることを、認定機関に対して実証しなければならない。

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

IAF 指針

- G.2.1.1. ISO/IEC Guide 62 の 2.1.1.3 の「説明が求められる場合」という規定を適用する場合、「これらの規準文書」は認定機関が認めた文書に限定することが望ましい。ISO/IEC Guide 62 の 1.3.1¹⁾及び 1.3.3 の「対象の ISMS のもとで要求される補足文書」は、認定機関が認めたもので、関連規格又はガイドの適用に関する追加指針や補足的指針を提供する文書を意味することが望ましい。指針 G.2.1.9 も参照すること。例外として審査登録機関も補足文書を発行できるが、その場合は ISO/IEC Guide 62 の 2.1.1.3 の要求事項に従うことを条件とする。
- G.2.1.2. ISMS の審査登録は、当該システムが所定の要求事項を満たしているということについて十分に信頼を与えるものでなければならない。組織の ISMS の審査登録では、登録証に明記された範囲において組織が ISMS を効果的に実施し維持していること、及び当該 ISMS に従ってプロセスを運用していることを実証しなければならない。
- G.2.1.3. 指針 G.2.1.2 の「所定の要求事項」は、顧客と組織との間で合意された要求事項を意味する。組織が自ら表明している仕様に従ってサービスを提供している場合、顧客の購入という行為によって「合意された要求事項」とすることもある。また、組織が「法的要求事項」への適合を表明している場合、あるいは組織に「法的要求事項」への適合が義務付けられている場合、「合意された要求事項」にはこうした「法的要求事項」も含まれる。いずれの場合でも、製品やサービスに適用される「法的要求事項」への適合は、たとえそれが契約内容の確認の際に考慮すべき暗黙の契約条件であっても、通常は顧客からの要求事項となる。
- G.2.1.4. 審査登録機関は、申請受理を早めたり遅らせたりするといった目に見えない形での差別をはじめ、いかなる差別も行ってはならない。
- G.2.1.5. ISO/IEC Guide 62 の 2.1.1.2 は、審査登録機関に対し、すべての申請者がそのサービスを利用できるようにすることを要求している。但し、審査登録機関は、審査登録する資格を与えられていない活動領域、又は特定の分類においていかなる組織に対してもサービスを提供しないと決めた活動領域を、その機関の提供するサービスから除いてもよい。例えば、法律の許す範囲で、サービスの提供を特定地域の申請者に限定してもよいし、審査登録機関が認定されている範囲内の技術分野又はその一部で活動している組織に限定してもよい。
- G.2.1.6. 審査登録機関は、ISMS の審査登録のみを提供してもよいし、ISMS の審査登録に関連した製品認証や品質システムの審査登録を提供してもよい。
- G.2.1.7. 審査登録機関が ISMS 規格以外の規準文書を使用して組織の審査登録を行う場合、それらの文書は一般に入手可能なものでなければならない。
- G.2.1.8. ISO/IEC Guide 62 の 2.1.1.3 で使用されている「特定の審査登録プログラム」という用語は、産業分野特有の制度を含むことがある。
- G.2.1.9. ISO/IEC Guide 62 の 2.1.1.3 で言及されている「これらの規準文書」の適用に関する説明の内容は、EA 加盟の認定機関から認定を受けた審査登録機関によって、EA 発行の指針に限定されることが望ましい。指針 G.2.1.1 を参照のこと。

¹⁾ „1.3.2”の誤記と思われる。

2.1.2 組織運営機構

IAF 指針

- G.2.1.10. ISO/IEC Guide 62 の 2.1.2 d)に記載の通り、認定は法人格をもつ機関にのみ授与される。また、認定は宣言された範囲、活動、所在地に限定される。審査登録業務がより大きな組織の一部である法人組織によって遂行される場合は、この親組織の他部門との関係を明確にしなければならず、指針 G.2.1.22 及び G.2.1.23 に記載されている利害抵触のないことを証明することが望ましい。審査登録機関は、親組織の他部門の活動について、自機関に関連する情報を認定機関に提供しなければならない。
- G.2.1.11. 審査登録機関が ISO/IEC Guide 62 の 2.1.2 d)で要求される法人格をもつ組織であることを示すということは、申請する審査登録機関がより大きな親組織の一部である場合には、認定は当該法人全体に対してのみ授与されることを意味する。このような場合、認定機関は、特定の審査の追跡調査及び / 又はその審査登録機関に関する記録の内容の確認のために、当該法人全体の組織運営機構を審査することがある。法人の一部が実際の審査登録機関を構成している場合、独自の機関名称で業務を実施してもよいが、その名称は認定登録証に記載されることが望ましい。
- ISO/IEC Guide 62 の 2.1.2 d)の趣旨から、政府の一部又は政府の部局である審査登録機関については、政府の地位に鑑みて法人格をもつとみなす。このような機関の地位及び組織運営機構は正式に文書化されなければならない、この機関は ISO/IEC Guide 62 の要求事項をすべて満たさなければならない。
- G.2.1.12. 審査登録機関の公平性及び独立性は、以下の三段階で確保されることが望ましい。
- 1) 戦略及び方針
 - 2) 審査登録に関する決定
 - 3) 審査業務
- ISO/IEC Guide 62 の 2.1.2 に対する指針は、この三段階すべてにおいて公平性と独立性を規定することを目的としている。
- G.2.1.13. ISO/IEC Guide 62 の 2.1.2 a)で要求される公平性は、ISO/IEC Guide 62 の 2.1.2 e)で要求されている「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」が参加可能な組織運営機構によってのみ確保できる。
- G.2.1.14. ISO/IEC Guide 62 の 2.1.2 c)の要求事項を満たすために設けられる管理主体は、ISO/IEC Guide 62 の 2.1.2 e)で要求されている組織運営機構と同じである必要はない。
- G.2.1.15. ISO/IEC Guide 62 の 2.1.2 e)への適合により、審査登録機関の所有者の一部が、技術的に客観性のある一貫したサービスの提供を妨げるような営業上の配慮や、その他の配慮を行うことを可能にするあらゆる傾向を阻止する効果が得られる。これが特に必要なのは、審査登録機関の設立資金がある特定の利害関係者によって提供され、それによって株主及び / 又は役員会の意向が大きく左右される場合である。
- G.2.1.16. 従って、ISO/IEC Guide 62 の 2.1.2 e)では、審査登録機関の組織運営機構を文書化し、そのなかに重要な関係者全員の参加規定を盛り込むことが要求されている。通常、これはある種の委員会を通して行うことが望ましい。このようにして設立された組織運営機構について、審査登録機関は文書により規定することが望ましく、またこの機構を変更する際には認定機関に通知することが望ましい。
- G.2.1.17. 審査登録システムに重要な関わりをもつすべての関係者が参加できるか否かは、常に判断の問題である。ここで重要なのは、識別可能な主な利害関係者すべてに参加する機会を提供し、特定の利害関係者を優先せず利害の均衡を図ることである。

ISMS 指針

- IS.2 ISO/IEC Guide 62 の 2.1.2 e) でいう関係者とは、産業界や商業界における顧客及び供給者、監督機関、貿易機関、情報セキュリティマネジメントの専門家及び関連専門家、政府などである。

IAF 指針

- G.2.1.18. ISO/IEC Guide 62 の 2.1.2 c) に規定されている各種の機能について責任を負う管理主体は、ISO/IEC Guide 62 の 2.1.2 e) に記載されている委員会又はこれと同等の組織が適切かつ公平な審査登録を実施できるようにするために、審査登録に関連するすべての重要な決定及び処置の理由や特定業務の責任者の選定をはじめ、必要な情報をすべて当該委員会等に提供することが望ましい。管理主体が当該委員会等の助言を尊重しなかった場合、それがいかなる事項であっても当該委員会等は適切な方策を講じなければならず、これには認定機関へ通知することも含まれる。
- G.2.1.19. 審査登録機関と、申請者又は登録組織がともに政府の一部である場合、これらは両者の運営責任を負う個人又はグループの直接的な監督下でないことが望ましい。審査登録機関は、公平性に関する要求事項を満たすため、こうした事例にどのように対処するかを実証できなければならない。
- G.2.1.20. ISO/IEC Guide 62 の 2.1.2 n) に基づいて登録証を発行又は取り消す決定を委員会が行う場合、特にその委員会の委員の一つ又は複数の登録組織からの代表者が含まれている場合は、審査登録機関の運営手順によって、これらの代表者が決定に重大な影響を及ぼさないようにすることが望ましい。これは、例えば投票権の配分やその他同等の方法を採用することによって保証することができる。
- G.2.1.21. ISO/IEC Guide 62 の 2.1.2 o) では、2 つの異なる要求事項を取り扱っている。一つは、審査登録機関はいかなる場合でも 2.1.2 o) の 1)、2)、3) に規定されたサービスを提供してはならないということである。もう一つは、関連機関が提供するサービスや業務に対して特別な制約はないが、こうしたサービスや業務は、審査登録機関の守秘性、客観性又は公平性に影響を与えてはならないということである。
- G.2.1.22. コンサルティングは、審査対象の ISMS の構築に積極的かつ創造的な方法で参画することとみなされる。これには、例えば以下の事項が含まれる。
- a) マニュアル、ハンドブック、手順書を準備又は作成すること。
 - b) マネジメントシステムに関する事柄についての意思決定プロセスに参画すること。
 - c) 審査登録の対象となるマネジメントシステムの構築及び実施について、具体的な助言を与えること。
- 備考：指針 G.2.1.22 でいうマネジメントシステムには、財政面をはじめそのシステムのあらゆる側面が含まれる。
- G.2.1.23. 審査登録機関が以下の職務を実行しても、それがコンサルティングとみなされたり、利害抵触の可能性があるとみなされることはない。
- a) 審査登録業務。これには、情報連絡会議、計画の打ち合わせ、文書の調査、審査（内部監査や内部のセキュリティレビューではない）、不適合のフォローアップなどを含む。
 - b) 研修コースを準備し、その講師として参加すること。但し、このコースが情報セキュリティマネジメント、関連マネジメントシステム、又は審査業務に関連する場合は、すでに公知で自由に入手できる一般的な情報や助言の提供に留め

ることが望ましい。つまり、指針 G.2.1.22 c)の要求事項に違反するような、企業に具体的な助言を提供しないことが望ましい。

- c) 審査に適用する規格の要求事項について、審査登録機関の解釈の根拠に関する情報を、要請に応じて提供又は公開すること。
- d) 審査を受ける準備が整っているか否かの決定のための確認のみを目的とする審査前の活動。但し、こうした活動によって、指針 G.2.1.22 に違反するような勧告や助言を提供しないことが望ましく、またかかる活動がこの要求事項に違反しないこと、及びその活動が結果的に審査期間の短縮根拠として利用されないことを審査登録機関が確認できることが望ましい。
- e) 認定範囲以外の他の規格や規制に従って、第三者及び第三者審査を実施すること。
- f) 審査やサーベイランスで訪問する際に付加価値を付けること。例えば、具体的な解決方法を勧告することなく、審査中に明らかになった改善の機会を明示すること。

G.2.1.24. 審査登録業務と関連機関によるコンサルティングは、一緒に営業活動しないことが望ましい。書面又は口頭による宣伝活動のための資料や説明は、この二つの活動が連携しているという印象を与えるものでないことが望ましい。審査登録業務の公平性を継続して維持し、またそのように見られるようにするために、いかなる顧客に対しても、この二つのサービス（審査登録業務とコンサルティング）を両方とも利用した場合には、ビジネス上の利益が得られるかのような印象を与えないようにするのは審査登録機関の義務である。

G.2.1.25. 審査登録機関は、特定のコンサルティングや研修サービスを受ければ審査登録が簡素化されたり、容易になったり、又は費用が少なくなるようなことを示唆することは望ましくない。

G.2.1.26. ISO/IEC Guide 62 の 2.1.2 o)でいう関連機関とは、審査登録機関と同じ所有者や役員がいること、契約による取決め、共通の名称、非公式の理解事項、又はその他の手段により関連のある機関、例えば審査結果から利益を受けることになっていたり、あるいは審査結果に影響を及ぼし得る潜在的な能力を有している機関を意味する。

G.2.1.27. 審査登録機関は、審査登録業務を提供する際に利害抵触の可能性の有無を判断するために、このような関連機関との関係を分析し、文書化することが望ましい。また、適切に管理しないと守秘性、客観性又は公平性に影響を及ぼす可能性のある関連機関及び活動を明確にすることが望ましい。

G.2.1.28. 審査登録機関は、実際の利害抵触を排除し、公平性に対するリスクを最小限に抑えるために、どのようにして審査登録業務及びその他の活動を管理しているかを実証しなければならない。その際、審査登録機関内に起因するものであれ、関連機関の活動に起因するものであれ、利害抵触の要因となり得るすべての要素も明確にしなければならない。認定機関は、審査登録機関が審査の際にこうしたプロセスを開示することを期待する。その際、現実的で正当な理由のある限り、対象となる活動について審査登録機関と関連機関の記録を確認するために、審査証跡の追跡調査を実施することがある。こうした審査証跡の範囲を検討する際には、当該審査登録機関の公平な審査登録の実績を考慮することが望ましい。公平性を維持できなかった証拠が発見された場合は、利害抵触の可能性を排除するための管理が再構築されたことを確認するために、関連機関も審査証跡の調査対象に含めることが必要となる場合もある。

G.2.1.29. ISO/IEC Guide 62 の 2.1 及び 2.2.3 の要求事項は、管理職としての業務を含めコンサルティングを行う者について、過去 2 年以内に当該組織（又はその組織の関連会社）に対してコンサルティング活動を行っていた場合には、審査登録プロセスの一部である審査の実施に携わってはならないということを意味している。雇用者が

審査を受ける組織に関係していたり、過去に関係したことがある場合は、審査登録プロセスのいずれの部分に携わる者であっても利害抵触が生じる可能性がある。審査登録機関は、このような状況を把握、評価し、公平性が損なわれないように責任と任務を割当てる義務を負う。

- G.2.1.30. ISO/IEC Guide 62 の 2.1.2 に言及されている上級の経営管理者、職員及び / 又は要員は必ずしも常勤である必要はないが、彼らの他の職務が自らの公平性を損なうようなものであってはならない。
- G.2.1.31. 審査登録機関は、審査を行うすべての下請負契約者や外部審査員に対し、すべてのコンサルティングサービスの営業活動について、指針 G.2.1.24 及び G.2.1.25 で要求されている内容に相当する誓約書の提出を求めることが望ましい。
- G.2.1.32. 審査登録機関は、関連機関、下請負契約者、外部審査員に対し、提出した誓約書に違反しないように活動させる責任がある。また、審査登録機関は、こうした違反が確認された場合には適切な是正処置を実施する責任がある。
- G.2.1.33. 審査登録機関は、審査登録の対象となる組織の ISMS の内部監査や内部セキュリティレビューを実施する機関（個人を含む）と関係のないことが望ましい。
- G.2.1.34. 審査員は、審査期間中及び / 又は最終会議において、審査所見を説明し、また審査に適用する規格の要求事項を明確にしなければならない。但し、審査の一環として指示的な助言やコンサルティングを行ってはならない。
- G.2.1.35. ISO/IEC Guide 62 の 2.1.2 p) に言及されている方針及び手順では、あらゆる紛争及び苦情を、建設的かつ速やかに処理できるようになっていることが望ましい。この手順により容認可能な解決に至らなかった場合、あるいは、提案された手順が苦情申立て者又はその他の関連当事者にとって容認できないものであった場合は、審査登録機関の手順によって異議申立ての手続きが行えるようになっていなければならない。この異議申立ての手順には以下の規定を含めることが望ましい。
- a) 異議申立て者に対しその案件を正式に説明する機会を提供すること。
 - b) 異議申立ての手続きの公平性を確保するために、他の業務から独立した要素又はその他の手段を提供すること。
 - c) 異議申立てに関する所見文書を、決定理由を含めて異議申立て者に提供すること。

審査登録機関は、従うべき異議申立ての手続きや手順があることを、必要に応じ、適切な場で、すべての関係者に周知するようにしなければならない。

2.1.3 下請負契約

IAF 指針

- G.2.1.36. 審査登録機関は、他の機関が実施した審査に基づいて登録証を発行することができる。但し、その場合、ISO/IEC Guide 62 及び認定に関連するその他の文書のすべての関連要求事項、特に ISO/IEC Guide 62 の 2.2 の要求事項を下請負契約先の機関が遵守しなければならないことを、下請負契約先の機関との間で合意しておかなければならない。下請負契約先の機関が実施する審査業務は、審査登録機関自身の審査業務と同等の信頼を与えるものでなければならない。審査報告書の評価及び登録の決定は、他の審査登録機関ではなく、当該審査登録機関自身が行わなければならない。共同で審査を実施する場合は、審査全体が適格な審査員によって十分に実施されたことを、各審査登録機関が確認しなければならない。
- G.2.1.37. 審査登録機関は、指針 G.2.1.36 に従って登録証を発行する場合、下請負契約先の機関がこの文書の関連条項すべてに適合していることを確認できる手順をもってい

なければならない。

2.1.4 品質システム

IAF 指針

- G.2.1.38. ISO/IEC Guide 62 の 2.1.4.3.e) で要求されている「記述」には、委員会、グループの各メンバー又は個人がどの関係者を代表しているかについての記述も含めることが望ましい。

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

IAF 指針

- G.2.1.39. 登録の決定に関して、組織の ISMS の完全な内部監査、マネジメントレビュー及びセキュリティレビューはある一定の間隔で実施されなければならないが、ISO/IEC Guide 62 の 2.1.5 では、この間隔について特に言及していない。この間隔は審査登録機関が定めてもよい。審査登録機関は、この間隔を最低周期とする選択をしたか否かには関係なく、組織のマネジメントレビュー、セキュリティレビュー及び内部監査のプロセスが効果的であることを確認するための評価尺度を確立しなければならない。
- G.2.1.40. 組織のマネジメントレビュー及びセキュリティレビューに関する取り決めが既に実行されていること、それが効果的であること、及び今後も維持されるであろうことを証明する証拠が十分得られるまでは、組織に登録を授与してはならない。

2.1.6 内部監査及びマネジメントレビュー

IAF 指針

- G.2.1.41. 審査登録機関は、品質システムについて、完全な内部監査及びマネジメントレビューをある一定の間隔で実施することが望ましいが、ISO/IEC Guide 62 の 2.1.6 ではこの間隔について特に言及していない。審査登録機関は、品質システムの完全な内部監査とその後のマネジメントレビューを、少なくとも年一回以上実施することが望ましい。認定機関は、内部監査及びマネジメントレビューにおける検出事項や、認定機関に提出された報告書に基づき、ISO/IEC Guide 62 の要求事項への適合の程度に応じて、これより短い間隔を指定することができる。
- G.2.1.42. 内部監査及びマネジメントレビューの記録は、要請に応じて認定機関に提示できるようにしておくことが望ましい。

2.1.7 文書化

IAF 指針

- G.2.1.43. ISO/IEC Guide 62 の 2.1.7.1.d) に記載されている財政基盤の安定性を確保する手段の記述は、審査登録機関が公平性を維持できるか否かを十分に示すものであることが望ましい。

2.1.8 記録

2.1.9 機密保持

IAF 指針

- G.2.1.44. 機密保持に関する要求事項の対象には、審査登録機関が機密を保持すべき情報を閲覧できる者すべてが含まれる。下請負契約先の要員には、特に同僚の従業員や他の雇用主から、こうした情報の機密を保護することを要求しなければならない。
- G.2.1.45. ISO/IEC Guide 62 の 2.1.9.2 の「書面での同意」が適用されるのは機密情報に限られる。

2.2 審査登録機関の要員

2.2.1 一般

IAF 指針

- G.2.2.1. ISO/IEC Guide 62 の 2.1.2 j) は、審査登録機関が認定されている範囲全体（又は業務を遂行する部分）において、ISO 10011 及び該当する分野別の制度の要求事項を満たしている自らの管理下にある資源を用いて、審査を行うことができないことを意味する。
- G.2.2.2. 「自らの管理下にある資源」という表現には、契約に基づき審査登録機関のために業務を遂行する各審査員、又はその他の外部要員を含めることができる。審査登録機関は、正規職員、契約職員、外部機関からの派遣職員を含めたすべての要員の業務を管理し、それについて責任を負う立場になければならず、また特定の分野で用いられる全要員の適格性を管理する包括的な記録を維持しなければならない。
- G.2.2.3. 審査登録機関の管理主体は、個々の審査員が活動している審査登録範囲において要求される業務の遂行に適格であるか否かを判断するための資源、およびこの適格性を確認するための手順をもっていなければならない。審査員の力量は、検証された経歴、特定の研修、概要の説明などによって確立することができる（認定を受けた審査員評価登録機関によって ISMS 審査員として登録されることで、これを証明することができる）。審査登録機関は、業務を遂行するすべての要員と効果的な意思疎通ができることが望ましい。
- G.2.2.4. 審査登録機関は、以下を実施するのに適格な要員を有していなければならない。
- 審査に適切な審査チームとなるよう ISMS 審査員を選定し、その力量を検証する。
 - ISMS 審査員に対する概要の説明を行い、必要な研修の手配をする。
 - 登録の授与、維持、取消し、一時停止、拡大、縮小に関する決定をする。
 - 苦情、異議申立て、及び紛争に関する手順を定め、それを運用する。

ISMS 指針

IS.3 管理能力

IS.3.1 一般

この指針では、審査登録機関が審査登録プロセスを指導し管理する能力に重点が置かれている。ISMS 審査登録の実施に要求される能力において必須の要素は、審査登録機関の要員全体としての能力が、審査対象の活動や関連する情報セキュリティの課題に対して適切となるように要員を選定、供給し、管理することである。

IS.3.2 能力分析と契約内容の確認

審査登録機関は、審査対象組織の ISMS に関連する技術動向や法律の改正に関する知識を得られるようなシステムをもっていなければならない。

審査登録機関は、業務を行うすべての技術分野に関して、情報セキュリティマネジメント能力を分析する有効なシステムをもっていなければならない、またこれを利用可能な状態にしておかなければならない。

審査登録機関は関連契約の内容を確認する能力をもっていなければならない、また各依頼者の契約内容の確認を行う前に、関連する各産業分野の要求事項について能力の分析（確認されたニーズに応じた能力の評価）を行ったことを実証できなければならない。審査登録機関は、特に以下の活動を遂行する能力をもっていることを実証できなければならない。

- a) その産業分野の活動領域において、資産に対する脅威、脆弱性、及び組織に及ぼす影響といった、情報セキュリティに関連する特徴的な事項を識別する。
- b) 組織の活動分野を明確にする。
- c) 組織の活動範囲全体から生じる、資産に対する脅威、脆弱性、及び組織に及ぼす影響といった、情報セキュリティに関連する代表的な事項が上記 a) で識別された事項と対応していることを確認する。
- d) 識別された活動に関連して、並びに資産に対する脅威、脆弱性、及び組織に及ぼす影響といった、情報セキュリティに関する事項に関連して、審査登録を行うために必要とされる能力を明確にする。
- e) 必要な能力を提供できることを確認する。

IS.3.3 審査チームの教育訓練と選定

審査登録機関は、審査チームの教育訓練及び選定に関する基準をもっていなければならない。これは、以下の事項について適切なレベルを確保できるものでなければならない。

- a) ISMS 規格又は規準文書の理解
- b) 情報セキュリティ問題についての理解
- c) リスクアセスメントとリスクマネジメントについての理解
- d) 審査対象となる活動についての専門的知識
- e) ISMS に関連した規制要求事項についての知識
- f) マネジメントシステムの審査能力
- g) マネジメントシステムについての知識

IS.3.4 意思決定プロセスの管理

管理機能には、ISMS 登録の授与、維持、拡大、縮小、一時停止、及び取消しに関する意思決定プロセスを管理する能力をもたせなければならない、そのための適切な手順をもっていなければならない。

2.2.2 審査員及び技術専門家の資格基準

ISMS 指針

IS.4 審査員の力量

ISMS の審査を行うために審査登録機関に採用された者は、ISO 10011-2 に基づく以下の基準を満たすことが望ましい。ISMS 審査のために複数の要員を採用する場合は、指針 IS. 5.3 に従ってこれらの特質を審査チームメンバーに割り振ることが

できる。

- a) 大学レベルの教育（豊富な経験を持ち、専門的な教育・訓練を受けている場合は、大学レベルの教育と同等とみなすことができる）
 - b) 情報技術分野において 4 年以上の常勤による実務経験があること。このうち 2 年以上は情報セキュリティ関連の役割又は職務を担当していたものであること。
 - c) 審査業務と審査のマネジメントに関する 5 日間の研修を成功裏に修了していること。
 - d) 審査員としての責任を負う前に、情報セキュリティの全審査過程を経験しておくことが望ましい。この経験は、文書審査、リスク分析のレビュー、実地審査、審査報告の作成を含む、最低 4 回延べ 20 日間にわたる審査への参加によって得られたものであることが望ましい。
 - e) これらの経験はすべて最近のものであることが望ましい。
 - f) 客観的である、分別がある、洞察力がある、分析力がある、粘り強い、現実的であるなどの個人的特質をもっていること。複雑な業務を広い視野から理解し、大きな組織における個々の部門の役割も理解できることが望ましい。
 - g) 情報セキュリティと審査に関する知識及び技能を維持していること。
- 主任審査員の場合は、上記に加えて以下の要求事項も満たすことが望ましい。
- h) 審査プロセスを管理する知識及び特質をもっていること。
 - i) 少なくとも 3 回の完全な ISMS 審査で、審査チームリーダーとして活動した経験をもっていること。
 - j) 審査プロセスを管理するのに十分な知識と特質があることを実証していること。
 - k) 口頭及び文書の両方で効果的な意思疎通の能力を実証していること。

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

IAF 指針

G.2.2.5. ISO/IEC Guide 62 の 2.2.3.1 b)は、審査登録機関に対し、ISMS の審査員及び技術専門家の行動と業務遂行状況を評価し監視することを要求している。この評価及び監視には、審査員と技術専門家の活動に現地で立ち会うことも含めることが望ましい。

2.2.3.2 個々の審査業務の割当て

IAF 指針

G.2.2.6. ISO/IEC Guide 62 とこの文書の要求事項を満たす審査を行うための適切な資源を確保できるまでは、認定を受けた審査登録機関としての認証登録証を発行できないのは、認定条件の一つである。審査登録機関は、組織の審査実施のために採用された職員が、その活動分野における力量をもっていることを実証する手順をもっていなければならない。審査の管理責任者を特定し、その力量を文書化しておかなければならない。

G.2.2.7. ISO/IEC Guide 62 の 2.2.3.2 f) 2)の「指示書」という用語は、ISO/IEC Guide 62

の 3.2.5 という「業務命令」と同じ意味である。

- G.2.2.8. 審査チームは、審査対象のシステムに関する要求事項をチームメンバーが理解していることを確認できる記録をもっている必要がある。審査チームは、審査業務の遂行に必要な技術分野及び産業分野全般を理解してなければならず、またその分野における経験をもっていなければならない。
- G.2.2.9. 重要な要求事項や特別な手順の要求など特殊な事情がある場合、審査チームの知識等に対して、概要説明、特別研修、技術専門家の参加などによって補うことができる。審査登録機関は、審査員ではない技術専門家を審査チームに加えてもよい。審査登録機関が技術専門家を利用する場合、そのシステムには技術専門家の選定方法、及び選定された専門家の技術的知識を最新の状態にする方法の詳細を定めておかなければならない。審査登録機関は、例えば産業界や専門家協会など外部機関の支援を求めることもできる。
- G.2.2.10. ISO/IEC Guide 62 の 2.1² と 2.2.3.2 の要求事項は、コンサルティングを行ったことのある者の採用に関係している。指針 G.2.1.29 を参照のこと。

ISMS 指針

IS.5 審査チームの力量

- IS.5.1 以下の要求事項は登録審査に適用される。サーベイランス活動については、定期的なサーベイランス活動に関する要求事項のみが適用される。
- IS.5.2 以下の要求事項は、技術専門家を除く審査チームの各メンバーに適用される。
審査チームの全メンバーは、以下のすべての事項について理解しており、また十分な経験があることを実証できなければならない。
- a) ISMS 規格又は規準文書
 - b) マネジメントシステム一般に関する概念
 - c) 様々な情報セキュリティ分野に関連する問題
 - d) リスクアセスメントとリスクマネジメントに関する原則及びプロセス
 - e) 審査原則
- IS.5.3 以下の要求事項は、審査チーム全体に適用される。
- a) 以下の項目それぞれについて、審査チームメンバーの少なくとも 1 名が、審査登録機関の規定する、チームとして責任を持つことに関する基準を満たしていることが望ましい。
 - i) チームの管理
 - ii) 該当する情報セキュリティ分野における法的及び規制要求事項、並びに法的遵守に関する知識
 - iii) 情報セキュリティに関連する脅威の識別
 - iv) 組織の脆弱性の識別及びその影響の把握と、それらに対する軽減策や管理策の理解
 - v) 当該分野の最新技術の知識
 - vi) 情報セキュリティに関するリスクアセスメントの知識

² "2.1"となっているが、"2.1.2.o)"を示している。

- b) 審査チームは、組織の ISMS のセキュリティ事件・事故に関する兆候を追跡し、適切な ISMS の要素を突き止める能力があることが望ましい。
- c) 審査チームのメンバーは 1 名でもよいが、その場合、その個人は上記 a) の基準をすべて満たしていなければならない。

IS.5.4 技術専門家の利用

プロセス、情報セキュリティ問題、及び組織に影響する法令に関して特定の知識を有している技術専門家については、上記の基準をすべて満たしていない場合でも審査チームに加えてもよい。技術専門家は単独で活動しないことが望ましい。

2.2.4 審査要員との契約

2.2.5 審査要員の記録

2.2.6 審査チームのための手順

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

IAF 指針

- G.2.4.1. 苦情は、潜在的な不適合についての情報源である。苦情を受け取った場合、審査登録機関は速やかにその原因を明らかにし、必要に応じて処置を講じなければならない。この原因には、審査登録機関のマネジメントシステム内において、不適合の原因となる可能性のある（又はその傾向のある）要因も含まれる。
- G.2.4.2. 審査登録機関は、上記のような調査を実施して修正 / 是正処置の方法を策定することが望ましい。これには、以下の対策を含むことが望ましい。
 - a) 早急に基準に適合させる。
 - b) 再発を防止する。
 - c) 採用した修正 / 是正処置の有効性を評価する。

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

ISMS 指針

IS.6 要員に関する記録の閲覧

審査登録機関は、組織が機密情報又は取扱いに慎重を要する情報とみなしているために、審査中に審査チームが調査できないのはどのような記録かを、審査実施前にレビューすることが望ましい。審査登録機関は、調査可能な記録で有効な審査が行えるか否かを判断することが望ましい。審査登録機関が有効な審査を行えないと判断した場合は、適切な閲覧を組織が受け入れた場合にのみ、審査を実施できることを組織に通知することが望ましい。

3.1.2 申請

3.2 審査のための準備

ISMS 指針

IS.7 適用宣言書

申請者は適用宣言書を作成し、そのなかで ISMS 規格又は規正文書のどの部分が組織の ISMS に該当し適用されるかを説明しなければならない。適用宣言書は、審査チームに提供される作業文書に含めなければならない。

3.3 審査

IAF 指針

G.3.3.1. 審査登録機関は、審査、又は更新審査に関連するすべての活動を実施するのに十分な時間を審査員に与えなければならない。このように割当てられる時間は、組織の規模、審査するサイトの数、及び審査登録に適用される規格などの要素に基づいていることが望ましい。審査登録機関は、審査、又は更新審査に使用する時間の根拠を具体的に示すことができるように、又はその正当性を示すことができるように準備しておかなければならない。

ISMS 指針

IS.8 登録範囲

組織は、ISMS の適用範囲を定めることが望ましい。審査登録機関の役割の一つは、適切に含めるべき ISMS 活動の要素を、組織が適用範囲から除外していないことを確認する業務に一貫性をもたせることである。

従って、審査登録機関は、組織の情報セキュリティのリスクアセスメントが組織の活動を適切に反映しており、ISMS 規格又は規正文書の規定する活動の境界まで含めていることを確認することが望ましい。また、審査登録機関は、組織の適用宣言書の中にこのことが反映されていることを確認することが望ましい。

ISMS の適用範囲に完全には含まれないサービスや活動とのインターフェースは、審査登録の対象となる ISMS 内で取り扱うことが望ましく、組織の情報セキュリティ

ィのリスクアセスメントに含めることが望ましい。こうした状況の一例には、他の組織と施設を共有するケースがある（例えばコンピュータや通信システムなど）。

IS.8.1 複数のサイト

ISMS の審査登録における複数のサンプリングに関する決定は、品質システムにおける同様の決定より複雑である。複数のサイトを審査する場合に、サンプルに基づいた手法の適用を希望する審査登録機関は、サンプリング計画の作成に際して以下の事項をすべて含む手順を維持する必要がある。

審査登録機関は、サンプリングに基づく初回審査の実施に先立って、採用する方法と手順を認定機関に通知し、これらの方法と手順のなかで、複数のサイトの ISMS 審査を管理するために以下の事項がどのように考慮されているのかを実証できる証拠を提供しなければならない。

審査登録機関の手順では、最初に行う契約内容の確認によって、サイト間の違いを可能な限り明確にできるようになっていることが望ましく、そうすることで、以下の規定に従って適切なサンプリングのレベルを決定できることが望ましい。

単一の ISMS のなかに類似したサイトが複数ある場合は、組織に対しそのすべてを範囲に含む登録証を発行できるが、以下を条件とする。

- a) すべてのサイトが同一の ISMS のもとで運営されていること。この ISMS は、中央で管理・監査されており、かつ中央でマネジメントレビューが行われるものであること。
- b) すべてのサイトが、組織の内部セキュリティレビュー手順に従って監査されていること。
- c) 審査登録機関が、代表し得る数のサイトをサンプリングしていること。その際、以下の要求事項を考慮していること。
 -) 本部及び当該サイトの内部監査の結果
 -) マネジメントレビューの結果
 -) 各サイトの規模の違い
 -) 各サイトの事業目的の違い
 -) ISMS の複雑さ
 -) 各サイトの情報システムの複雑さ
 -) 作業慣行の違い
 -) 実施業務の違い
 -) 重要な情報システム、又は取扱いに慎重を要する情報を処理する情報システムとの間に生じる可能性のある相互作用
 -) 法的要求事項の違い
- d) このサンプルは、一部は上記 c) に基づいて選択し、一部は無作為に選択することが望ましく、結果としてサイト選択のランダムな要素を失うことなく、広範囲にわたり異なるサイトを選択することが望ましい。
- e) 審査登録機関は、登録に先立って、当該 ISMS の範囲のなかで資産に対する重大な脅威、脆弱性、又は影響があると思われるすべてのサイトを審査することが望ましい。
- f) サーベイランス計画は、上記の要求事項に照らして作成することが望ましく、また組織の全サイト、又は適用宣言書に含まれる ISMS の審査登録の範囲内の全サイトを、妥当な期間内で網羅できるものであることが望ましい。

- g) 本部又は単一のサイトで不適合が観察された場合は、審査登録対象の本部及び全サイトに是正処置の手順を適用することが望ましい。

以下の指針 IS.9 に記載する審査では、単一の ISMS がすべてのサイトに適用されていること、及び運用レベルで中央管理が行われていることを確認するために、組織の本部の活動を取り扱うことが望ましい。この審査では、上記の事項をすべて取り扱わなければならない。

IS.9 審査方法

審査登録機関は、組織の ISMS 審査を、当該組織のサイトにおいて少なくとも 2 つの段階に分けて実施することが望ましい。但し、代替的な方法を適用する正当な理由を示すことができる場合はこの限りではない。個別の状況においては、非常に規模の小さい組織のニーズに合うように審査登録プロセスを適応させることが正当な理由となることもある。この指針の目的のため、上記 2 つの段階を「審査（ステージ 1）」及び「審査（ステージ 2）」と呼ぶ。それぞれの主な目的、及び最低限含むべき内容を以下に示す。

審査登録機関は、審査の開始に先立って、申請者が内部のセキュリティレビューの実施を計画していること、及びその計画内容と手順が運用可能でかつその運用可能性を実証できることを、申請者に要求する手順をもっていることが望ましい。

備考：審査については、コンサルティングに関する指針 G.2.1.10～G.2.1.33 も参照のこと。

IS.9.1 審査（ステージ 1）

審査（ステージ 1）では、審査登録機関は、ISMS の設計に関する文書入手することが望ましい。この文書には、少なくとも組織の実施した情報セキュリティに関するリスク分析、適用宣言書、及び ISMS の中核を成す要素を含む。

審査（ステージ 1）の目的は、組織のセキュリティ基本方針及び目標に照らして当該 ISMS を理解し、また特に当該審査に対する組織の準備状況を理解することにより、審査（ステージ 2）計画の焦点を定めることである。

審査（ステージ 1）には文書審査が含まれるが、この審査（ステージ 1）を文書審査のみに限定しないことが望ましい。審査登録機関と組織は、いつどこで文書審査を行うかについて合意しなければならない。いずれの場合でも、文書審査は審査（ステージ 2）の開始までに終了しておくことが望ましい。

審査（ステージ 1）の結果は、報告書にまとめることが望ましい。審査登録機関は、審査（ステージ 2）への移行を決定するため、及び審査（ステージ 2）のための必要な力量を備えた審査チームメンバーを選定するために、審査（ステージ 1）の審査報告書をレビューすることが望ましい。

審査登録機関は、審査（ステージ 2）における詳細な調査で必要となる可能性のある別の種類の情報や記録について組織に通知することが望ましい。

文書審査を含む審査（ステージ 1）を複数メンバーで実施する場合、審査登録機関は、各チームメンバーの活動をどのように調整しているのかを実証できることが望ましい。

IS.9.2 審査（ステージ 2）

この審査（ステージ 2）は、常に組織のサイトで実施する。審査登録機関は、審査（ステージ 1）の審査報告書に記載された検出事項に基づき、審査（ステージ 2）の審査計画を立案する。審査（ステージ 2）の目的は以下の通りである。

- a) 組織が自ら定めた基本方針、目標、及び手順を遵守していることを確認する。

- b) 当該 ISMS が ISMS 規格又は規準文書のすべての要求事項に適合していること、並びに当該 ISMS が組織の基本方針及び目標を実現しつつあることを確認する。

これを実施するために、この審査では当該組織の以下の事項に焦点を当てることが望ましい。

- c) 情報セキュリティに関するリスクのアセスメント、及びその結果に基づく ISMS の設計
- d) 適用宣言書
- e) このプロセスの結果に基づいて設定された目標及び対象
- f) 目標と対象に照らした実施状況の監視、測定、報告、及びレビューの実施
- g) セキュリティレビュー及びマネジメントレビュー
- h) 情報セキュリティ基本方針に対する経営陣の責任
- i) 基本方針、情報セキュリティのリスクアセスメントの結果、目標及び対象、責任、計画、手順、実施状況のデータ、並びにセキュリティレビュー間の関連

IS.10 ISMS 審査の個別の要素

IS.10.1 資産に対する脅威、脆弱性、及び組織に及ぼす影響といった、情報セキュリティに関連する事項の評価、及び重要だと思われる事項の管理：審査登録機関の役割

資産に対する脅威、脆弱性、及び組織に及ぼす影響といった、情報セキュリティに関連する事項を識別、調査、評価するための手順を組織が一貫して確立、維持していることに対して信頼を与えるために、審査登録機関は以下の要素を考慮することが望ましい。

- a) 資産に対する脅威、脆弱性、及び組織に及ぼす影響といった、情報セキュリティに関連する事項の重大性を識別するための基準を策定し、そのための手順を作成するのは組織の責任である。
- b) 審査登録機関は、情報セキュリティに関連する脅威の分析が組織の運営にとって適切かつ妥当であることを実証するよう、組織に求めることが望ましい。
- c) 組織の基本方針、目標及び対象と、手順又はその適用結果との間の矛盾点。

審査登録機関は、重大性の分析に用いられる手順が適切であり正しく実施されているか否かを確認することが望ましい。情報セキュリティに関連する事項で、資産に対する脅威、脆弱性、又は組織に及ぼす影響が重大だと識別されている場合、それらは当該 ISMS 内で管理されていることが望ましい。

IS.10.2 法規制の遵守：審査登録機関の役割

法規制を遵守し、その遵守状況を評価するのは組織の責任である。審査登録機関は、当該 ISMS がこの点において機能していることを確認する手段としてチェックとサンプリングだけに留めることが望ましい。

ISMS の登録を受けた組織は、その活動、製品、及びサービスにおける情報セキュリティ上の影響に関して、該当する規制要求事項にマネジメントシステムを継続的に適合させることが望ましい。審査登録機関は、この要求への適合を実現するシステムが十分に実施されていることを確認する。

審査登録機関は、組織が法規制の遵守状況を評価していること、及び関連規制が遵守されていないことが発見された場合には、是正処置がとられていることを検証することが望ましい。

IS.10.3 ISMS 文書と他のマネジメントシステム文書の統合

ISMS 文書を他のマネジメントシステム（品質、安全衛生、環境など）文書と組み合わせることは容認可能である。但し、他のシステムとのインターフェースも含め、ISMS を明確に識別できることが条件となる。

IS.10.4 マネジメントシステム審査の組み合わせ

ISMS 審査は、他のマネジメントシステム審査と組み合わせることができるが、その場合、その審査が ISMS の審査登録に関する要求事項をすべて満たしていることを実証できることが条件となる。ISMS にとって重要な要素すべてが審査報告書に明確に記載されており、容易に識別できるようになっていることが望ましい。審査を組み合わせることによって、審査の質に悪影響が及ばないようにすることが望ましい。

3.4 審査報告

3.5 登録に関する決定

ISMS 指針

IS.11 登録に関する決定

組織への登録の授与を決定する機関は、通常、審査チームの否定的な勧告を覆すことは望ましくない。そのような状況が生じた場合、審査登録機関は、審査チームの否定的な勧告を覆すという決定の根拠を文書化し、その根拠の正当性を示さなければならない。

IAF 指針

G.3.5.1. 審査登録の過程で収集する情報は、以下の事項に関して十分なものであることが望ましい。

- 1) 審査登録機関が、十分な情報に基づいて登録の決定を行うことができること。
- 2) 例えば、異議申立てがあった場合や、次回に審査を計画する場合などに（別のチームが行う可能性も考慮して）、情報を追跡できること。
- 3) 継続性を確保すること。

ISO/IEC Guide 62 の 3.4.1 e)の報告に関する要求事項に加え、この情報には以下の事項を含めることが望ましい。

- 内部セキュリティレビューの信頼度
- ISMS の実施と有効性に関して、肯定的なものと否定的なものを含めた最も重要な観察事項の要約
- 審査チームが出した結論

ISMS 指針

IS.12 審査チームによる審査登録機関への報告

登録に関する決定の基礎として、審査登録機関はその決定を行うのに十分な情報を盛り込んだ明確な報告書を審査チームに要求する。

- a) 審査登録機関に提出する審査チームの報告書は、審査プロセスの様々な段階で必要となる。既にファイルされている情報と組み合わせ、この報告書に

は、少なくとも以下の情報を含めることが望ましい。

- i) 文書審査の要約を含む審査の詳細
 - ii) 組織の情報セキュリティリスク分析に関する評価の詳細
 - iii) 審査時間の合計、並びに文書審査、リスク分析のレビュー、実地審査、審査報告書の作成に要した時間の内訳
 - iv) 不適合事項の明確な記述
 - v) 審査で使用した調査項目、それらを選択した根拠、及び採用した手法
 - vi) 審査チームによる、審査登録機関への登録に関する勧告
- b) サーベイランス報告書には、特に、以前に指摘された不適合事項の是正に関する情報を含めることが望ましい。また、このサーベイランス報告書は、少なくとも上記 a)の要求事項を全体として含むことが望ましい。

IAF 指針

- G.3.5.2. 指針 G.1.3.1 に定義されている不適合がすべて是正され、審査登録機関がサイト訪問又はその他の適切な検証方法によって是正処置の完了を確認するまでは、登録を授与してはならない。
- G.3.5.3. ISO/IEC Guide 62 の 3.5.3 c)では、登録文書に有効期間を記載することが要求されている。登録の有効期間は、更新審査に関する取決めと整合のとれたものであることが望ましい。

ISMS 指針

IS.13 登録機能に関連する意思決定

審査登録機関のなかで登録の授与 / 取消しを決定する組織又は個人は、審査プロセス及び関連する審査チームの勧告の評価を行うのに十分なレベルの、あらゆる分野における知識と経験をもっていることが望ましい。

3.6 サーベイランス及び更新審査の手順

IAF 指針

- G.3.6.1. 審査登録機関は、審査登録の維持に関する状況及び条件を規定した明確な手順をもっていなければならない。サーベイランス又は更新審査において、指針 G.1.3.1 に定義された不適合が検出された場合、この不適合は審査登録機関の合意した期間内に有効に是正されなければならない。この合意した期間内に是正が行われなかった場合は、審査登録機関は登録の縮小、一時停止、又は取消しを行わなければならない。是正処置実施のために認める期間は、不適合の程度、及び製品又はサービスが所定の要求事項を満たすことの保証に対するリスクの程度に応じたものであることが望ましい。
- G.3.6.2. 審査登録機関が実施するサーベイランスは、審査登録にあたって基準とした規格の要求事項に登録組織が引き続き適合している、という保証を与えるものでなければならない。審査登録機関は、これを達成し得る資源と手順をもっていることが望ましい。
- G.3.6.3. ISO/IEC Guide 62 の 3.6.1 では、審査登録機関に対し、登録され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、サーベイランス及び更新審査を実施することが要求されている。

- G.3.6.4. サーベイランスの目的は、認証された ISMS が引き続き実施されていることを検証し、組織運営の変更を受けて当該 ISMS に加えられた変更の影響を検討し、審査登録の要求事項に引き続き適合していることを確認することである。組織の ISMS のサーベイランスは定期的を実施しなければならず、通常は少なくとも年一回実施することが望ましい。サーベイランス計画には、通常以下の事項を含めることが望ましい。
- システムの維持に必要な要素、すなわち内部監査、内部セキュリティレビュー、マネジメントレビュー、及び予防・是正処置
 - ISMS 規格又は規準文書で要求されている、外部からの情報
 - 文書化されたシステムの変更
 - 変更された領域
 - 審査規格又は規準文書のなかの選択した条項
 - 該当するその他の選択した領域
- G.3.6.5. ISMS の審査登録を受けた組織のシステムに重大な変更があった場合、又はその他登録理由に影響を及ぼすような重大な変更があった場合は、審査登録機関はサーベイランス活動の際に特別な準備をしなければならない。
- G.3.6.6. 更新審査の目的は、組織の ISMS が総合的に ISMS 規格又は規準文書の要求事項に引き続き適合していること、及び ISMS が適切に実施され継続されていることを検証することである。多くの場合、組織の ISMS の定期的な更新審査の間隔が 3 年を超えると、この要求事項を満たすとは考えられない。更新審査では、登録期間における当該システムの過去の実施状況及び現在の維持状況をレビューすることが望ましい。更新審査計画では、このレビュー結果を考慮することが望ましく、またこの計画には少なくとも ISMS 文書の審査及び実地審査を含めることが望ましい（これは定期的なサーベイランスに代えて、又はその審査範囲を拡大したものとして実施してもよい）。更新審査では、少なくとも以下の事項を確認しなければならない。
- ISMS の全要素間における有効な相互作用
 - 運用上の変更を考慮した、ISMS 全体の包括的な有効性
 - ISMS の有効性を維持するとの意志表明
- G.3.6.7. 例外的に更新審査の実施間隔が 3 年を超えた場合、審査登録機関は、ISMS 全体の有効性が定期的に評価されていることを実証することが望ましく、また同程度の信頼性を維持するためにこれを補う頻度でサーベイランスを実施することが望ましい。
- G.3.6.8. 審査登録機関は、審査登録機関に持ち込まれた異議申立て、苦情、紛争の記録をサーベイランス期間中に確認することが望ましい。また、審査登録の要求事項を満たす上での不適合や不備が明らかになった場合は、当該組織が ISMS 及び手順を調査して適切な是正処置をとったことを確認することが望ましい。
- G.3.6.9. サーベイランス報告書には、指針 G.3.5.1 の要求する情報に加え、以前に発見された不適合に対する処置の報告についても記載することが望ましい。

ISMS 指針

IS.14 サーベイランス及び更新審査

審査登録機関が実施するサーベイランスには、少なくとも、年間で以下の事項を含めることが望ましい。

- i) 組織の情報セキュリティ基本方針の目標達成の点からみた ISMS の有効

性

- ii) 該当する情報セキュリティに関する法規制の遵守を、定期的に評価しレビューする手順が機能している状況
- iii) 前回の審査で発見された不適合に対してとった処置

また報告書については、少なくとも ISO/IEC Guide 62 の 3.4.2 に記載の項目を含めることが望ましい。

- a) 審査登録機関は、資産に対する脅威、脆弱性、及び組織に対する影響といった、情報セキュリティに関連する事項に応じてサーベイランス計画を調整でき、かつこのサーベイランス計画の正当性を示せることが望ましい。
- b) 審査登録機関のサーベイランス計画は、審査登録機関自身が作成することが望ましい。その実施日については、登録された組織と合意の上で定めることができる。
- c) サーベイランスは、他のマネジメントシステムの審査と組み合わせて実施することができる。その場合、報告書のなかで、それぞれのマネジメントシステムに関連する側面を明確に示すことが望ましい。
- d) 審査登録機関は、登録証及び報告書の適切な使用を監視しなければならない。
- e) 更新審査の方法は、審査の方法と同様であることが望ましい。

3.7 登録証及びロゴの使用

IAF 指針

- G.3.7.1. 認定を受けた審査登録機関により発行される認証登録証には、審査登録にあたって基準とした規格又はその他の規準文書、登録証を発行した審査登録機関の名称、及び該当する一つ又は複数の認定機関の名称を記載することが望ましい。また、この登録証が審査登録機関の認定範囲内で発行されていることも明記することが望ましい。
- G.3.7.2. 認定を受けた審査登録機関が認定範囲内で発行するすべての登録証には、該当する認定機関のマークを表示することが望ましい。組織が認定マークの付いていない登録証の発行を希望した場合、その登録証が認定を受けた審査登録機関により発行される認証登録証であるとみなされるためには、認定機関の名称と認定登録番号が記載されていないといけない。
- G.3.7.3. 審査登録機関が複数の認定機関から認定を受けている場合、登録証には市場のニーズに適した、少なくとも 1 つの認定マークを表示することが望ましい。
- G.3.7.4. 審査登録機関は、自機関のマークの使用に関する文書化された手順をもっていることが望ましい。また、登録に関する誤った表明や審査登録機関のマークの誤った使用を含めた誤用に関する手順ももっていることが望ましい。
- G.3.7.5. 審査登録機関が正式な認定を受ける前に発行した登録証について認定資格を誤って表明した場合、認定機関は、当該審査登録機関に対してその登録証を取り消すよう求めることができる。
- G.3.7.6. 「登録のマークやロゴ」について定めた ISO/IEC Guide 62 の 3.7.1 の規定、及び「シンボル又はロゴ」について定めた 3.7.2 の規定は、両方ともマーク、ロゴ、及びシンボルに適用される。
- G.3.7.7. 審査登録機関は、異なる適合性審査登録システム（例えば、製品認証やマネジメントシステム認証）を示すのに同じマークを使用しないことが望ましく、複数のマークを用いる場合には、それぞれのマークが示す意味の混同を避けることが望まし

い。

- G.3.7.8. 審査登録機関は、登録された組織が誤解や混乱を招くような方法で審査登録機関のマークを使用するのを防ぐ手順をもっていることが望ましい。

3.8 組織に対する苦情の記録の閲覧

IAF 指針

- G.3.8.1. この条項の対象は、登録された組織に対する苦情のみであり、審査登録機関に対する苦情ではない。
- G.3.8.2. 苦情は、潜在的な不適合についての情報源である。苦情を受け取った組織は、速やかにその原因を明らかにし、必要な場合にはそれを報告することが望ましい。これには、組織の ISMS における不適合の原因となる可能性のある（又はその傾向のある）要因も含まれる。
- G.3.8.3. サーベイランスにおいて、規格の要求事項を満たす上での不適合や不備が明らかになった場合、審査登録機関は、組織が自己のシステム及び手順を調査して適切な是正処置をとったことを確認することが望ましい。
- G.3.8.4. 審査登録機関は、組織がこのような調査を実施して修正 / 是正処置の方法を策定していることを確認することが望ましい。これには、以下の対策を含むことが望ましい。
- 法律で要求されている場合は、管轄当局に通知する。
 - 早急に適合状態に復旧させる。
 - 再発を防止する。
 - セキュリティ事件・事故及びその影響を評価し、軽減する。
 - ISMS の要素を他の関連する箇所にも十分反映させる。
 - 採用した修正 / 是正処置の有効性を評価する。
- G.3.8.5. 修正 / 是正処置の実施は、その有効性が実証され、手順、文書、記録に必要な変更が加えられるまでは、完了したとみなさないことが望ましい。

附属書 1: 認定範囲

認定範囲のリストは、EC 委員会が 1994 年に発行した「経済活動に関する統計的分類基準」(NACE Rev.1) に基づいている (EC 官報第 L083 1993 号)。

分類番号	認定範囲	NACE コード
1	農業、漁業	A, B
2	鉱業、採石業	C
3	食料品、飲料、タバコ	DA
4	織物、繊維製品	DB
5	皮革、皮革製品	DC
6	木材、木製品	DD
7	パルプ、紙、紙製品	DE 21
8	出版業	DE 22.1
9	印刷業	DE 22.2,3
10	コークス及び精製石油製品の製造	DF 23.1,2
11	核燃料	DF 23.3
12	化学薬品、化学製品及び繊維	DG minus 24.4
13	医薬品	DG 24.4
14	ゴム製品、プラスチック製品	DH
15	非金属鉱物製品	DI minus 26.5,6
16	コンクリート、セメント、石灰、石こう他	DI 26.5,6
17	基礎金属、加工金属製品	DJ
18	機械、装置	DK
19	電氣的及び光学的装置	DL
20	造船業	DM 35.1
21	航空宇宙産業	DM 35.3
22	その他輸送装置	DM 34,35.2,4,5
23	他の分類に属さない製造業	DN 36
24	再生業	DN 37
25	電力供給	E 40.1
26	ガス供給	E 40.2
27	給水	E 41,40.3
28	建設	F
29	卸売業、小売業、 並びに自動車、オートバイ、個人所持品及び家財 道具の修理業	G
30	ホテル、レストラン	H
31	輸送、倉庫、通信	I
32	金融、保険、不動産、賃貸	J, K 70, K 71
33	情報技術	K 72
34	エンジニアリング	K 73, 74.2
35	その他サービス	K 74 minus K 74.2
36	公共行政	L
37	教育	M
38	医療及び社会事業	N
39	その他社会的、個人的サービス	O