IAF Mandatory Document

ISO/IEC 27001:2022への移行に関する要求事項

Issue 2

(IAF MD 26:2023)

注:この文書は、IAF Normative Document Transition Requirements for ISO/IEC 27001:2022の内容を変更することなく情報マネジメントシステム認定センター及び公益財団法人 日本適合性認定協会が翻訳したものであるが、原文だけが正式なIAF文書としての位置付けをもつ。原文は、IAFウェブサイト（P.12参照）から入手できる。

2023年4月13日

公益財団法人 日本適合性認定協会

Issued: 15 February 2023 Application Date: 15 February 2023 IAF MD 26:2023, Issue 2

国際認定フォーラム（IAF）は、IAF メンバーによって認定された適合性評価機関 (CAB) が発行する適合性評価結果が全世界で受け入れられるよう、認定機関 (AB) 間における相互承認協定を世界的規模で運用することによって、貿易を推進し、規制当局を支援している。

認定は、認定された適合性評価機関（CAB）が認定の範囲内において業務を行う能力をもつことを保証することによって、事業及びその顧客にとってのリスクを軽減する。IAF メンバーである認定機関（AB）及びそれらに認定された適合性評価機関（CAB）は、適切な国際規格及びその一貫した適用のための IAF 適用文書に適合することが要求される。

IAF国際相互承認協定（MLA）に加盟している認定機関は、認定プログラムの運用に信頼を与えるために、選任された相互評価チームによる定期的な評価を受ける。IAF MLAの構造と範囲は、“IAF PR 4-Structure of IAF MLA and Endorsed Normative Documents”に詳述されている。

IAF MLAの構造は5つのレベルで構成されている。レベル1は全ての認定機関 (AB) に適用される基準、JIS Q 17011を規定している。レベル2の活動と、対応するレベル3の基準文書との組合せをMLAのメインスコープと称し、レベル4（該当する場合）及びレベル5の関連する基準文書の組合せをMLAのサブスコープと称する。

- MLAのメインスコープは、例えば製品認証のような活動と、JIS Q 17065などの関連する基準文書を含む。メインスコープレベルにおける適合性評価機関（CAB）による証明は、同等に信頼できると見なされる。
- MLAのサブスコープは、例えばJIS Q 9001などの適合性評価に関する要求事項と、該当する場合、例えば、ISO TS 22003などのスキーム固有の要求事項を含む。サブスコープレベルにおける適合性評価機関（CAB）による証明は同等と見なされる。

IAF MLAは、市場による適合性評価結果の受入れに必要な信頼性を提供する。IAF MLA加盟認定機関に認定された機関によって、IAF MLAの適用範囲内で発行される証明は、世界中で認知されることができ、それによって国際貿易を推進する。

目次

第2版
作業：IAF技術委員会
承認：IAFメンバー 承認日: 2023年2月3日
発行日：2023年2月15日 適用日: 2023年2月15日
問い合わせ先： Elva Nilsen
IAF Corporate Secretary
電話番号：+1 613 454-8159
Eメール：secretary@iaf.nu

IAF基準文書への序文

この文書で使用されている“should”（望ましい）は、規格の要求事項を満たすことの、認知された手段であることを示す。適合性評価機関（CAB）は、この要求事項を同等の方法で満たすことも、それを認定機関（AB）に対して実証できれば可能である。この文書で使用されている用語“shall”（なければならない）は、関連する規格の要求事項を反映したそれらの規定が強制されることを示す。

ISO/IEC 27001:2022への移行に関する要求事項

1. 序文

基準文書の移行に関する情報を提供するすべての文書は、IAF MLA署名認定機関（AB）及び認定された適合性評価機関（CAB）が従うべき基準文書となり、その適用範囲はこの文書に定義されているとおりである。この文書は、IAF技術委員会において任命されたタスクフォースが、IAF PR 7:2022 *Requirements for Producing IAF Mandatory Documents on Transitions*に従って作成したものである。

この文書は、以下に関する移行の要求事項を提供し、関連する IAF MLA 署名認定機関（AB）及び認定された 適合性評価機関（CAB）に義務付けられる。

基準文書	ISO/IEC 27001:2022
移行前の文書	ISO/IEC 27001:2013
現在の状況（MD発行時点）	IS
移行期間	3年 (36か月)

2. 主な変更点の概要

2.1 背景

関連するISOポリシーに従って、ISO / IEC FDIS 27001：2022は、2022年7月にISO / IEC 27001：2013、ISO/IEC 27001:2013/COR 1:2014、ISO/IEC 27001:2013/COR 2:2015及びISO/IEC 27001:2013:DAmd1の統合を通じて準備された。更に、ISOはISO/IEC FDIS 27001:2022が、ISO/IEC 専門業務用指針第一部及び統合版ISO補足指針2022年版に定義されているマネジメントシステム規格 (MSS) のための調和された構造に整合するよう求めた。FDIS投票の結果に基づき、ISOは2022年10月25日にISO/IEC 27001:2022を発行した。

注記1　ISO/IEC 27002:2013/DAmd1は、ISO/IEC 27002:2022と一致させるために準備され、附属書A及び6.1.3 c)の注記が更新された。DAmdとは、追補原案 (Draft Amendment)の略語である。

注記2　現行の国際規格を変更する追補は、2回を超えて発行してはならない（ISO/IEC専門業務用指針第1部2022、2.10.3項参照）ため、ISO/IEC 27001:2022は、ISO/IEC 27001:2013/DAmd1:2022 の作成後に発行されなければならなかった。

2.2 主な変更点

ISO/IEC 27001:2013と比較すると、ISO/IEC 27001:2022の主な変更点は以下を含むが、これらに限定されない：

1) 附属書Aは、ISO/IEC 27002:2022の情報セキュリティ管理策を参照しており、管理策名称及び管理策に関する情報が含まれている；
2) 6.1.3 c)項の注記は、管理目的を削除し、「管理策」の代わりに「情報セキュリティ管理策」を使用するという、編集上の改訂がされている；
3) 6.1.3 d)項の文言は、潜在的な曖昧さを取り除くために再整理されている。
4) 組織は、利害関係者の関連する要求事項のうち、情報セキュリティマネジメントシステム (ISMS)を通して取り組むものを決定しなければならないと規定する4.2 c)項を新規に追加。

5) 組織がISMSの変更の必要があると決定したとき、その変更は、計画的な方法で行わなければならないと規定する、6.3項 変更の計画策定を新規に追加。

6) 文書化した情報に関する動詞の使い方に一貫性を持たせた。例えば、9.1項、9.2.2項、9.3.3項及び10.2項で「XXXの証拠として、文書化した情報を利用可能な状態にしなければならない。」としている。

7) 8.1項の「外部委託したプロセス」を「外部から提供されるプロセス、製品又はサービス」に変更し、「外部委託」という用語を削除した。

8) 9.2項 内部監査及び9.3項 マネジメントレビューをそれぞれ細分化し、細分箇条名をつけた。

9) 10項 改善の2つの細分箇条の順番を入れ替えた。

10) ISO/IEC 27002及びISO 31000といった、参考文献に記載された関連文書の版を更新した。

11) 例えば、6.2 d)項のような、MSSの上位構造、共通の中核となるテキスト、共通用語及び中核となる定義に対するISO/IEC 27001:2013のいくつかの逸脱が、MSSのための調和された構造との整合性のために改定された。

注記1　上記1)及び2)はISO/IEC 27001:2013/DAmd1 、3)はISO/IEC 27001:2013/COR 2:2015、それ以外の変更はMSSのための調和された構造に関するものである。

注記2　旧版（ISO/IEC 27002:2013）と比較すると、ISO/IEC 27002:2022の情報セキュリティ管理策は14箇条114管理策から4箇条93管理策に減少している。ISO/IEC 27002:2022の管理策は、11管理策が新規、24管理策が既存の管理策からの統合、58管理策が更新である。さらに、管理策構造を見直し、各管理策に「属性」と「目的」を導入し、管理策群に「管理目的」を設定しないこととした。

注記3　ISO/IEC 27001:2013/COR 1:2014は、附属書Aに関連するものであり、ISO/IEC 27001:2013/DAmd1に反映されている。

2.3 影響

ISO/IEC 27001:2022の変更の影響は、以下の理由により新しい附属書 A及び箇条 6.3の導入を含むが、これらに限定されない：

1) ISO/IEC 27001:2013/COR 2:2015は既に発行され、適用されている；
2) 附属書Aは規定である。
3) MSSのための調和された構造は、MSSの上位構造、共通の中核となるテキスト、共通用語及び中核となる定義に対する軽微な改定であり、ほとんどの変更は編集上のものであると考えられる。

ISO/IEC 27001において附属書Aの参照用の管理策群を使用する要求事項は、組織が決定した情報セキュリティ管理策と附属書Aにある管理策との比較プロセス（6.1.3 c））及び適用宣言書（6.1.3 d））の作成である。組織は、必要な情報セキュリティ管理策と附属書Aの管理策とを比較することにより、附属書Aの参照用管理策群にある必要な情報セキュリティ管理策が不用意に見落とされていないことを確認してもよい。

このような比較では、必要な情報セキュリティ管理策が不用意に見落とされていることを発見できない可能性がある。しかし、必要な情報セキュリティ対策が不用意に見落とされていることが判明した場合には、組織は、追加的に必要な情報セキュリティ管理策に対応するようリスク対応計画を更新し、それらの管理策を適用しなければならない。

上記の通り、ISO/IEC 27001:2022がすでにISMSを適用している組織に与える影響は、それほど重大ではない。

3. 移行に係る主な期間

活動	期日
認定機関（AB）	
ABは、遅くとも右記の期日までにISO/IEC 27001:2022に対する認定審査ができるようにする。	ISO/IEC 27001:2022の発行月の末日から6か月 (2023年4月30日)
ABによるISO/IEC 27001:2022に対する初回認定審査は、遅くとも右記の期日までに開始する。	ISO/IEC 27001:2022の発行月の末日から6か月 (2023年4月30日)
ABによる適合性評価機関（CAB）の認定の移行は、右記の期日までに完了する。	ISO/IEC 27001:2022の発行月の末日から12か月 (2023年10月31日)
適合性評価機関（CAB）	
CABによるISO/IEC 27001:2022の初回認証及び再認証は、遅くとも右記の期限までに開始する。	ISO/IEC 27001:2022の発行月の末日から18か月(2024年4月30日)
CABは被認証組織の認証の移行を右記の期日までに完了する。	ISO/IEC 27001:2022の発行月の末日から36か月 (2025年10月31日)

4. 移行プロセスにおける処置

4.1 認定機関（AB）の処置

活動	要否	注記
ABの措置	要	1) ABは，この文書の要求事項を考慮して，ISO/IEC 27001:2022 への移行措置を定めなければならない。 2) 移行措置では、AB及びCABがしなければならないことを扱わなければならない。ABは、移行措置に対応するために、いくつかの個別の文書を作成してもよい。 3) 移行措置では、少なくとも次の事項を考慮しなければならない： • ISO/IEC 27001の変更点及びギャップ分析 • 関連する要員が、ISO/IEC 27001:2022及び移行プロセスに関する力量を備えている。

		注記　審査チームは、全体として、情報セキュリティ技術及び実務に関する知識をもたなければならない（IAF MD 13:2020, 4.2 参照）。周知の通り、ISO/IEC 27002 は、実施の手引きを含む参照用の一般的な情報セキュリティ管理策群を提供している。 • ISO/IEC 27001 の変更により影響を受ける、ABの関連するプロセス及び文書、並びに該当する場合、認定活動を管理するための IT システムが特定されている • 移行審査プログラム • スケジュール、移行審査の方法、期限までに移行が完了しなかった場合の影響など、移行審査プログラムについて、CABに適時に連絡する 4) ABは、できるだけ早い機会に、必要な処置を計画し、開始することが奨励される。
CABの文書のレビュー	不要	
CABの文書に関する技術的レビュー	要	1) ABは、CABが ISO/IEC 27001:2022 に対す る能力をもつか否かを確認するために、技術的文書レビューを実施しなければならない。 2) AB は、CABから提出された次の情報のレビューを通じて、CABの移行措置の適切性、及び該当する場合、その実施の有効性を判断しなければならない。 • ISO/IEC 27001の変更点のギャップ分析 • 移行措置及びその実施の証拠 • 関連する要員の承認 • その他、ABが必要と判断する関連情報
CABの本部事務所での技術的な認定審査（現地又は遠隔審査による）	該当する場合	ABが、CABの文書の技術的なレビューを通じて十分な証拠を得られた場合は、CABの本部事務所の審査を実施する必要はない。CABがその移行措置に適合し、有効に実施していることをABが検証できない場合は、事務所審査が必要である。

CABの審査の立会	不要	
移行のために追加の審査工数が必要になる可能性はあるか？	要	単独の審査で移行確認を行う場合は、CABの移行を確認するために、少なくとも0.5 日の追加の審査日を含まなければならない。
その他	要	1) ABは、移行審査プログラムにおいて、CABが移行を申請するスケジュールを定めてもよい。 2) AB は、移行審査の結果に基づいて、移行を決定しなければならない。 3) ISO/IEC 27001:2022 に関するCABの能力が実証された場合、ABは、認定されたCABの認定情報（例：認定登録証）を更新しなければならない（該当する場合）。 4) 認定されたCABが、箇条3に挙げた関連する期日までに移行審査を成功裏に完了しなかった場合、ISO/IEC 27001:2013 に対する認定の有効期限は、移行期間終了日を超えてはならない。

4.2 適合性評価機関 (CAB)の処置

活動	要否	注記
CABの措置	要	1) CABは，本文書の要求事項及び関連するABの移行措置を考慮して，ISO/IEC 27001:2022 への移行措置を定めなければならない。 2) 移行措置では、CAB及び被認証組織がしなければならない ことを扱わなければならない。CABは、移行措置に対応するために、いくつかの個別の文書を作成してもよい。 3) 移行措置では、少なくとも次の事項を考慮しなければならない。 • ISO/IEC 27001の変更点及びギャップ分析 • 関連する認証プロセス及び文書、並びに該当する場合、認証活動を管理するための IT システムを修正する必要性

		• 関連する要員が ISO/IEC 27001:2022 及び移行プロセスに関する力量を備えている • 審査チームは、全体として、ISO/IEC 27002:2022 に含まれる全ての管理策及びその実施に関する知識をもたなければならない（ISO/IEC 27006:2015, 7.1.2.1.3 b)を参照） • 移行審査プログラム • スケジュール、移行審査の方法、移行期間終了前に移行できなかった場合の影響など、移行プログラムについて被認証組織に適時に連絡する。 4) CABは、できるだけ早い機会に、必要な処置を計画し、開始することが推奨される。
移行審査	要	1) CABは、移行審査を、サーベイランス審査、再認証審査と同時に、又は個別の審査として実施してもよい。 2) 移行審査は、文書レビューだけに依存してはならず、中でも技術的管理策のレビューについては特にそうである。 3) 移行審査には次を含まなければならないが、これらに限定されない。 • ISO/IEC 27001:2022のギャップ分析及び被認証組織のISMSの変更の必要性 • 適用宣言書の更新 • 該当する場合、リスク対応計画の更新 • 被認証組織が選択した、新規又は変更された管理策の実施及び有効性 4) CABが移行審査の目的を確実に達成できる場合は、CABは、移行審査を遠隔で実施してもよい。

移行のための追加の審査工数が必要になる可能性はあるか？	要	1) 移行審査を再認証審査と同時に実施する場合、少なくとも0.5人日を追加しなければならない。 2) 移行審査をサーベイランス審査と同時に、又は単独の審査として実施する場合は、少なくとも1.0人日を追加しなければならない。
その他	要	1) CABは、移行審査プログラムにおいて、被認証組織が移行を申請するスケジュールを定めてもよい。 2) CABは、移行審査の結果に基づいて、移行を決定しなければならない。 3) CABは、被認証組織のISMSがISO/IEC 27001:2022の要求事項を満たしている場合、認証文書を更新しなければならない。 注：移行審査が成功裏に完了した結果として認証文書が更新された場合、現在の認証周期の有効期限は変更されない。 4) 移行期間終了時には、ISO/IEC 27001:2013に基づくすべての認証は、失効または取消しとしなければならない。

4.3 その他

4.3.1 認定の移行決定後の適合性評価機関（CAB）の事務所審査では、CABの移行措置が完全に終了する前の、移行措置の実施状況の検証に焦点を当てなければならない。この事務所審査には、最低限、次を含めなければならない。

- CABの改訂されたプロセス及び手順の実施状況
- 関連する要員が、ISO/IEC 27001:2022の認証活動に関与する前にその力量を実証されている
- 被認証組織のISO/IEC 27001:2022への移行の進捗状況

4.3.2 認定の移行決定後に選択される全ての立会審査は、ISO/IEC 27001:2022に基づかなければならず、ISO/IEC 27001:2022に基づく審査を実施するためのCABの能力に焦点を当てなければならない。

IAF基準文書「ISO/IEC 27001:2022への移行に関する要求事項」の終わり。

追加情報

この文書又は他のIAF文書について追加の情報を必要とする場合、IAFメンバー又は事務局に連絡して下さい。

IAFメンバーの連絡先詳細については、IAFウェブサイト参照。 http://www.iaf.nu.

事務局:

Elva Nilsen
IAF Corporate Secretary
Telephone: +1 (613) 454-8159
Email: secretary@iaf.nu