



情報マネジメントシステム

IMS 認証機関認定に関する推奨事項

一 認証範囲及びその表記に関する基本的な考え方 一

JIP-IMAC121-1.0

2010年2月10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



## 目 次

1. 目的
  2. 発行の背景
  3. 関連文書
  4. 認証範囲の基本的な考え方
    - 4.1 認証範囲
    - 4.2 認証範囲の確認
  5. 認証文書への認証範囲の表記
- 付表 1 認証範囲の好ましい例 (参考)

## 1. 目的

この文書は、マネジメントシステム認証機関(以下、機関という)が認証審査を実施するにあたっての認証範囲及びその表記に関する基本的な考え方を財団法人日本情報処理開発協会 情報マネジメント推進センター (以下、本協会という) の推奨事項として示すことを目的とする。

なお、この文書は、本協会の認定審査及び関連の認定活動における要求事項を示すことを目的とするものではない。

## 2. 発行の背景

マネジメントシステム規格認証制度の信頼性確保のためのガイドラインから抜粋：

組織の一部分を認証する場合は、規格の趣旨を踏まえ重要な組織活動が認証範囲に含まれるよう努めること。また、重要な組織活動が認証範囲から欠落しているにも関わらず、あたかも当該活動あるいは組織全体が認証されているかの誤解を社会に与えないよう、十分な処置を講ずること。

この文書は、これをうけ、認証範囲に関して認証審査時における本協会の具体的な推奨事項を提示するものである。

## 3. 関連文書

マネジメントシステム規格認証制度の信頼性確保のためのガイドライン (経済産業省  
2008年7月29日公表)

JIS Q 17021:2007 (ISO/IEC 17021:2006) 適合性評価—マネジメントシステムの審査  
及び認証を行う機関に対する要求事項

JIS Q 27006:2008 (ISO/IEC 27006:2007) 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の審査及び認証を  
行う機関に対する要求事項

## 4. 認証範囲の基本的な考え方

### 4.1 認証範囲

組織が該当するマネジメントシステム規格を適用して認証を申請する範囲 (以下、申請範囲という) に対して、適用規格の要求事項に対する適合性が証明された場合に授与される又は授与した認証の範囲を認証範囲という。

認証範囲は、適用規格が取り扱う利害関係者に関連する、製品・サービスの一連の業務プロセス全体を含むことが望ましい。

## 4.2 認証範囲の確認

機関は、組織の申請範囲で、そのマネジメントシステムが適用規格の要求事項に適合し、当該規格の意図を実現できるように機能していることを確認するが、申請範囲は組織の判断で設定されるため、機関は、組織のプロセス、製品・サービス、関連サイト、事業部、事業所など、適用規格の取り扱う側面に関連する直接／間接の影響を考慮し、申請範囲の適切性を確認する必要がある。

組織が、その直接的な管理下にある活動範囲のうち、本来認証範囲に含めるべき活動を申請範囲から除外している場合、機関はその正当性を評価し、正当と認められない場合は、認証を与えない。

組織が、適用規格の要求事項への適合に影響を与えるようなプロセスを外部委託している場合などには、機関は、その管理が適切に行われているかを十分に確認する。

また、認証範囲に適用を除外されている規格要求事項がある場合、その要求事項の箇条が明確になっていなければならない。機関は、その適用の除外に正当な理由があり、適切であることを確認する。

認証範囲が、適用規格の意図に沿って適切に設定されるよう十分に配慮し、そのマネジメントシステムが全体として適用規格の要求事項に適合しているといえるかを判断することは、機関の責任である。

付表1に認証範囲の好ましい例を示す。

## 5. 認証文書への認証範囲の表記

認証文書に記載される認証範囲は、認証の利用者及び市場にとって、そのマネジメントシステムが信頼できるものであるかを判断するための重要な情報であり、認証の利用者が認証範囲に含まれる製品やプロセスを正しく理解できるよう、製品・サービス、プロセス、サイトなどに基づき正確かつ明確に表現される必要がある。

認証範囲の表記が、認証の利用者及び市場に誤解を招くものではないことを確実にすることは、機関の責任である。

機関は、認証範囲の表記に当たって、次の事項を留意する。

- a) 認証範囲に含まれる製品・サービス、プロセス、サイトなどに関して、認証の利用者が正確に把握できる程度に詳細な表現をする。
- b) 認証範囲に含まれない製品・サービス、プロセス、サイトなどへの言及、又はそれらが含まれると誤解されるような表現をしない。
- c) 組織の営業的要求に便宜を図るような表現をしない。
- d) 適用規格の要求事項への適合に影響を与えるようなプロセスが外部委託されている場合、外部委託の程度を考慮する。

付表1 認証範囲の好ましい例（参考）

側面	例
製品・サービス	<ul style="list-style-type: none"><li>a) 多種類ある製品・サービスのうち、生産量、売上げ、シェアなどが少ない製品・サービスに限定せず、主力製品・サービスを含む。</li><li>b) 環境汚染などのリスクの高い製品・サービスを含む。</li><li>c) 食品安全に対するリスクの大きい製品を含む。</li></ul>
プロセス	<ul style="list-style-type: none"><li>a) 顧客満足に影響する営業活動（営業機能）などの重要機能を含む。</li><li>b) 「設計・開発」などの重要プロセスを含む。</li><li>c) 環境リスクの高い活動を含む。</li><li>d) リスク値の大きい情報資産を含む。</li><li>e) 情報セキュリティ側面の大きい活動を含む。</li></ul>