JIS Q 27001:2023対応

# ISO/IEC 27001
## 情報セキュリティ マネジメントシステム(ISMS)
# 内部監査の実務と応用
【第2版】

羽田卓郎 [編著]　魚脇雅晴 [著]

日科技連

本書は、ISO 19011、ISO/IEC 27000、ISO/IEC 27001、ISO/IEC 27002、ISO 31000、ISO Guide 73という表記で規格条文を掲載していますが、それぞれJIS Q 19011、JIS Q 27000、JIS Q 27001、JIS Q 27002、JIS Q 31000、JIS Q 0073からの引用です。それぞれの規格の引用は、本書の解説に必要な最小限としています。これらのJIS規格を引用するに当たり、(一財)日本規格協会の標準化推進事業に協賛しています。なお、これらは必要に応じてJIS規格票を参照してください。

# まえがき

本書は、ISO/IEC 27001：2022(JIS Q 27001：2023)に基づく、情報セキュリティマネジメントシステム(Information Security Management System：以下、ISMS と記述)を導入した組織が行う内部監査について、内部監査の国際標準[1)]に準拠した監査の実務を具体的事例を含めて解説するものである。

世の中には、本書で解説する内部監査以外にも、さまざまなタイプの監査があり実践されている。情報セキュリティ関連では、経済産業省が主導するシステム監査や情報セキュリティ監査、及び公認情報システム監査人[2)](CISA)が行う監査など、主に情報セキュリティのリスク対策面の監査制度があるが、情報セキュリティの運用面にかかわるマネジメントシステムを含めた監査は、ISMS の内部監査で行われる。

ISMS の内部監査は、マネジメントシステムで要求される「構築し、実施し、維持し、継続的に改善するための活動」において、ISMS の有効性を高め組織のビジネスに寄与するための重要な機能である。しかし、ISO/IEC 27001：2022(JIS Q 27001：2023)の要求事項には、「内部監査をしなければならない」と書かれているが、「どのように実施すればよいか(How to)」は書かれていない。

本書では、内部監査の実務にそのまま使用できるように、内部監査プロセス(計画、実施、報告など)の一連の流れを具体的に解説し、監査手続に必要な書式もすべて組み込んでいる。さらに、内部監査の原則、体制、手法、技術に関する解説と実際の ISMS 内部監査の事例を紹介することで、これから ISMS の内部監査を学ぶ方、すでに内部監査にかかわっているが更に高いレベルの内部監査を目指したい方、内部監査を管理・監督される責任者を含め、内部監査に

---

1) ISO では、ISO 9001(品質)や ISO 14001(環境)などを含め、すべてのマネジメントシステムに適用するための監査の指針である ISO 19011：2018(JIS Q 19011：2019)(マネジメントシステム監査のための指針)を策定し、内部監査や認証審査に適用している。

2) ISACA(The Information Systems Audit and Control Association：情報システムコントロール協会)が認定する監査人制度のことである。

かかわる幅広い関係者の皆様に活用されることを期待している。

監査手続では、監査品質向上のためにチェックリスト(**3.2 節(1)(d)**及び**第 6 章**を参照)を用いることを前提とし、その作成のために、ISO/IEC 27001 のマネジメントシステムに関する要求事項と、リスク対策の要求事項(管理策)の解説と監査の留意点を解説する。

チェックリストは、ページ数の制限から**第 6 章**で例示による解説をしているが、ISO/IEC 27001 のすべての要求事項(本文の箇条 4 ～ 10 と管理策 5 ～ 8)のチェック項目を提供するため、日科技連出版社のウェブサイトからダウンロードする形式とした。

ダウンロード用 Excel ファイルは、そのまま使用でき編集することが可能であるため、自組織が作成した情報セキュリティの方針、規程、標準、手順などを反映することで、組織の実態に合わせた効率的な監査が実施できる。

なお、ISO/IEC 27001 の要求事項について、詳しく学びたい方は姉妹書の『ISO/IEC 27001 情報セキュリティマネジメントシステム(ISMS)規格要求事項の徹底解説【第 2 版】』及び『ISO/IEC 27001 情報セキュリティマネジメントシステム(ISMS)構築・運用の実践【第 2 版】』(いずれも日科技連出版社)を参照されたい。

また、クラウドサービスを導入している場合は、『ISO/IEC 27017 クラウドセキュリティ管理策と実践の徹底解説』(日科技連出版社)を参照されたい。

2024 年 7 月

編著者　羽田卓郎

# 目　次

## 「内部監査チェックリスト」ダウンロードのご案内

本書で紹介した「内部監査チェックリスト」を日科技連出版社のウェブサイト（https://www.juse-p.co.jp/）からダウンロードできます。トップページ上部のタブ［ダウンロード］をクリックすると、検索画面が表示されるので、書名もしくは ISBN を入力し検索します。

該当する書名をクリックすると、ダウンロードのボタンが表示されます。そのボタンをクリックすると ID とパスワードを要求されるので、下記を入力してください。ID およびパスワードはすべて半角で入力してください。

ID：[redacted]
パスワード：[redacted]

**注意事項**

1. 「内部監査チェックリスト」の著作権は羽田卓郎にあります。本リストを無断で複製・配付等することを禁じます。ただし、本書の購入者が購入者の所属する組織内でのみ使用する場合はこの限りではありません。
2. 著者および出版社のいずれも、本対応表をダウンロードしたことに伴い生じた損害について、責任を負うものではありません。

- 部門間、又は業務分野をまたぐ業務用情報システムの相互接続がある場合、それぞれのシステムの利用者が、許可されていない接続システムにアクセスできないようにするなどの方針及び手順を整備し、適切な安全対策を講じているか。
- 外部との情報転送方法(例：送受信の確認手段、暗号の強度、事故発生時の扱いなど)はお互いに合意しているか。
- 社内外(エレベータ、電車、飲食店など)での口頭による情報交換(会話など)における機密保持について明文化した規定があり周知しているか。
- 物理的媒体の輸送では、情報のラベルに応じた対策(物理的損傷からの保護(梱包)、盗難防止、不正開封、輸送経路の追跡、受領確認など)を規定し実施しているか。
- 電子メールを含めた電子的メッセージ通信に関する安全対策(例：改ざん防止、盗聴防止、誤発信対策、相手先認証など)が定められ、実施しているか。

### ③ アクセス権管理

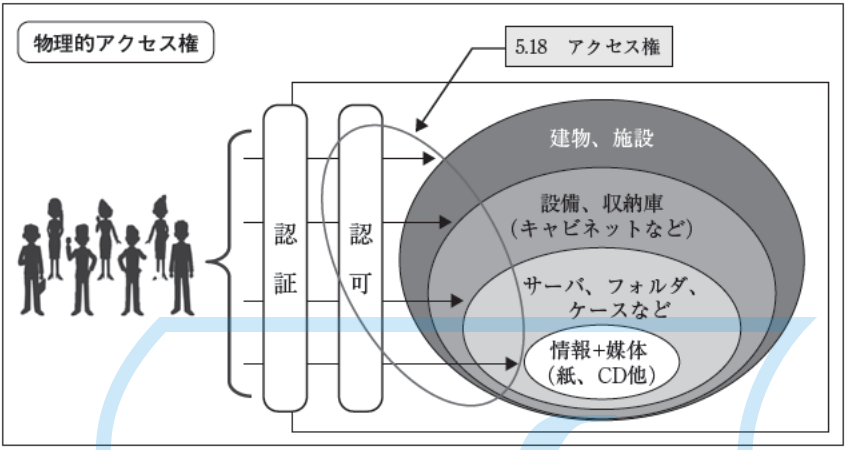
管理策の5.15～5.18は、情報及び情報を扱うための関連資産を保護するために、許可された者が許可された範囲の資産にアクセスできるようにすることを求めている。そのため、「許可された者」を識別するためのID管理、IDをもつ者が本人であることを確認するための認証、認証された者がアクセスできる対象を管理するためのアクセス権を管理する必要がある。

図表2.17及び図表2.18は、アクセス権管理に関連する管理策の適用対象と管理プロセスを物理的アクセスと電子的アクセスのそれぞれについてモデル化したものである。管理策の要求の概略は以下のとおりである。

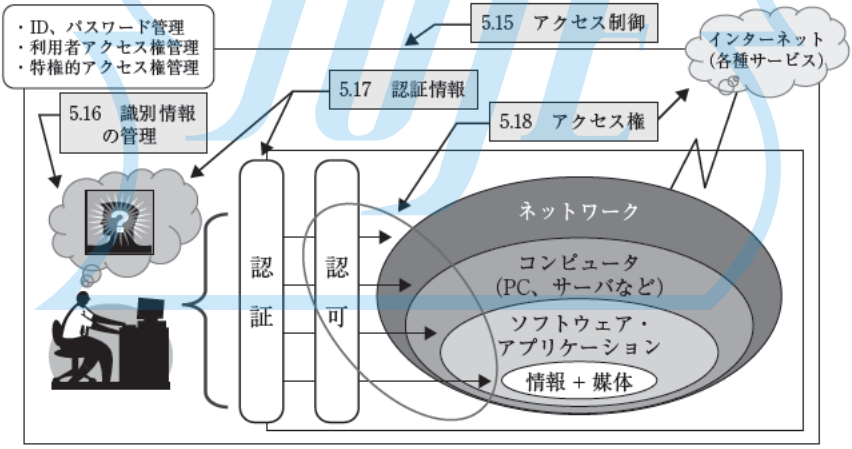
情報及び情報に関連する資産に対するアクセスは、許可のないアクセスや悪意をもったアクセスから保護しなければならない。そのためには、許可されていると主張する者が許可された本人[15]かどうかを確認しなければならない。

図表2.17で示しているように、アクセス許可は、「建物・施設」「設備・収納庫」「サーバ・フォルダ・ケース」「情報・媒体」の各段階で行われることが

図表 2.17　物理的アクセス権の管理策適用イメージ




図表 2.18　電子的アクセス権の管理策適用イメージ




望ましい。

図表 2.18 の電子的アクセス許可も同様に、情報がハードディスクなどの媒体に記録された情報、それを取り扱うためのソフトウェア・アプリケーション

15)「本人」とは、必ずしも「人」を意味しない。情報へのアクセスを許可する相手は、人物、組織、団体、コンピュータプロセス、プログラム、サービスなど、情報システムにアクセス権をもつ任意の主体(エンティティ)である。

図表 6.3　リスク対策（管理策対応）・

| 要求事項（監査基準） | | |
|---|---|---|
| 項目番号 | 項目（管理策） | 確認事項 |
| 5.6 ～ 5.8 | ① 5.6 専門組織との連絡<br>② 5.7 脅威インテリジェンス<br>③ 5.8 プロジェクトマネジメントにおける情報セキュリティ | ① 情報セキュリティに関する情報収集・情報交換などを行う相手専門組織との連絡（情報収集）体制を確立し、ISMS の維持・改善に役立てているか（5.6）。 |
| | | ② 既存の脅威や新たに発生した脅威に関する情報を収集及び分析し、脅威に対する対策を講じることで、その脅威が組織の ISMS に影響を及ぼすリスクを低減するために、情報を収集し、既知のリスクに変化が起きているかを分析し、変化に対応すべきかどうかを決定しているか（5.7）。 |
| | | ③ 組織横断的であったり期間が決められたプロジェクト体制を構築する場合に、アクセス権の設定や役割分担、及びプロジェクト終了時の情報の取扱い等の情報セキュリティにかかわる取決めが行われ、実施されているか（5.8）。<br>情報システムの開発／改訂プロジェクトでは、新しい開発システム又は既存のシステムの改訂に際し、セキュリティ要求事項を分析し、設計仕様として明確にしているか（5.8）。 |
| 5.9 ～ 5.11 | ① 5.9 情報およびその他の関連資産の目録 | ① 重要な情報資産で個別管理の必要な資産に関する目録管理（管理策の運用に必要な情報が管理されていること…例：ソフトウェアライセンス管理ではライセンス数と使用場所／機器／人の情報など）が行なわれているか（5.9）。 |
| | ② 5.10 情報およびその他の関連資産の許容される利用<br>③ 5.11 資産の返却 | ② 資産の使用許可範囲について、物理的な許可範囲（情報資産の閲覧や持ち出しの可否など）と、論理的な許可範囲（データベースのアクセス範囲など）を明確に定めているか（5.10）。 |
| | | ③ 雇用（又は契約）の終了又は変更に伴う資産の返却及び消去の手続が明確になっているか。その際、自宅に持ち帰っている組織の情報や、個人に貸与された PC を異動先に持参する場合の組織の情報の返却及び消去を考慮しているか（5.11）。 |

注）　表の続きはダウンロード用 Excel ファイルを参照（入手方法は目次参照）。

チェックリスト(一部)

| 監査証拠 | 判定 | 確認内容<br>(コメント) |
|---|---|---|
| ※判定＝◎：グッドポイント、○：適合、×：重大な不適合、▲：軽微な不適合、<br>△改善の機会、―：対象外 | | |
| • 情報セキュリティ関連情報収集先一覧<br>• 情報セキュリティ関連情報収集体制<br>• 脅威インテリジェンス分析体制・職務分担表<br>• 脅威インテリジェンス分析報告書<br>• 脅威インテリジェンスリスク対応計画<br>• プロジェクト運営規則<br>• プロジェクト体制・職務分担表<br>• プロジェクト管理記録(議事録など)<br>• システム開発設計仕様書 | | |
| • 資産目録(例：ソフトウェアライセンス管理台帳、PC管理台帳、サーバ管理台帳、文書管理台帳、など)<br>• 社内システム利用規則<br>• その他ヒアリングで確認した監査証拠<br>• 情報資産分類の定義書<br>• 文書等のラベル<br>• 外部記憶媒体管理基準(保管、持出し、処分など) | | |
| • 資産へのアクセス許可定義書(利用者の範囲を明記したものであれば体裁フリーでよい)<br>• 資産の持ち出し規則・手続(ノート PC、USB メモリなどの媒体他)<br>• 社内システム利用規則<br>• 外部記憶媒体管理基準(保管、持出し、処分など) | | |

# 索　引

【さ　行】

【や　行】



【ら　行】

## ■編著者紹介

**羽田　卓郎**（はねだ　たくろう）（執筆担当：第 1 章～第 4 章、第 6 章）

【略歴】

1970 年　昭和石油㈱（現 昭和シェル石油）入社
1990 年　ICT 子会社出向 情報セキュリティ G マネージャー
2002 年　情報セキュリティコンサルティング会社 技術部長兼執行役員
2003 年　リコー・ヒューマン・クリエイツ㈱ リコー情報セキュリティ研究センター副所長
2012 年～ 2018 年 9 月　リコージャパン㈱ ICT 事業本部 ICT 技術本部 コンサルティング推進室 エグゼクティブコンサルタント
2018 年 10 月～現在「羽田情報セキュリティ研究所」を開業し、主にリコージャパン㈱において委託コンサルタントとして活動を継続

【これまでに取得した資格と活動】

ISO/IEC 27001 主任審査員、ISO 9001 審査員補、情報セキュリティアドミニストレータ、ISO 22301（BCMS）審査員補、AMBCI 会員（BCI 日本支部個人会員）、ITIL ファンデーション、ISO/IEC 20000 審査員補、日本 ISMS ユーザーグループ会員、ISO/IEC JTC1/SC27 WG1（情報処理学会 情報規格調査会 27000 シリーズ規格標準化作業グループ）リエゾンメンバー、IRCA 諮問委員、公認マインドマップインストラクター

【その他活動】

ISO/IEC 27001（ISMS）認証取得支援、ISMS 運用・強化支援、ISO/IEC 27001 審査員研修主任講師、ISO 22301（BCMS）認証取得支援、BCP 策定支援、ISMS 及び BCP 関連各種研修講師、ISMS 及び BCP のセミナー・講演多数

【著作】

『個人情報保護法と企業対応』（共著、清文社）
『ISO 22301 で構築する事業継続マネジメントシステム』（共著、日科技連出版社）
『ISO/IEC 27001　情報セキュリティマネジメントシステム（ISMS）規格要求事項の徹底解説【第 2 版】』（共著、日科技連出版社）
『ISO/IEC 27001　情報セキュリティマネジメントシステム（ISMS）構築・運用の実践【第 2 版】』（日科技連出版社）
『ISO/IEC 27017　クラウドセキュリティ管理策と実践の徹底解説』（共著、日科技連出版社）

## ■著者紹介

**魚脇　雅晴**（うおわき まさはる）（執筆担当：第5章）

【略歴】

1977年　日本電信電話㈱（現 NTT）入社

1981年　研究所にて仮想計算機の研究開発に従事

1996年　スーパーキャッシュシステム（電子マネー）のプロジェクトリーダーとしてシステムの設計、構築、運用において不正利用防止・検出・暗号化などのセキュリティ分野に従事

2002年　インターネット上での認証・決済PFのプロジェクトリーダーとして開発、運用に従事するとともに不正利用防止やISMSの認証取得

2007年　金融系プロジェクトのシステム開発のPM業務や運用に従事しながら、セキュリティコンサルティング業務などに従事

2011年　NTTコムソリューションズ㈱ マネジメントソリューション本部（本務）経営企画部企画担当セキュリティマネジメント室（兼務）：オープンソース系の監視ソフトウェアの企画・開発及び全社のセキュリティマネジメントに従事

2021年～現在　NTTコミュニケーションズ㈱　情報セキュリティ部　サイバーセキュリティ部門：サイバーセキュリティを含めた総合的なセキュリティ調査業務に従事

【主な保有資格と公的活動】

- 保有資格：CISSP、ITILファンデーションなど
- 対外活動：現在、JNSA（日本ネットワークセキュリティ協会）の標準化部会の日本ISMSユーザグループのWGリーダー及びインプリメンテーション研究会主査としてISMSの規格要求事項の実装方法（サイバー攻撃やクラウド利用などの最新のリスク対応）をテーマとして活動し、毎年、情報セキュリティマネジメントセミナーとして標準化動向や研究会の成果を情報発信することでISMSの健全な普及、促進活動を継続中。また、これまでにJASA（日本セキュリティ監査協会）でサプライチェーンセキュリティ評価基準の検討やクラウドセキュリティ監査制度の検討WGに参画

# ISO/IEC 27001 情報セキュリティマネジメントシステム(ISMS)内部監査の実務と応用【第2版】

2019年 5月30日　第1版第1刷発行
2021年 4月 5日　第1版第2刷発行
2024年 9月 6日　第2版第1刷発行

編著者　羽田卓郎
著　者　魚脇雅晴

発行人　戸羽節文

検印省略

発行所　株式会社　日科技連出版社
〒151-0051　東京都渋谷区千駄ヶ谷5-15-5
DSビル
電　話　出版　03-5379-1244
営業　03-5379-1238

Printed in Japan　印刷・製本　三秀舎



ISBN 978-4-8171-9785-6
URL　https://www.juse-p.co.jp/