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)
規格要求事項の徹底解説
【第2版】

羽田卓郎・土屋直子・山﨑　哲 [著]

日科技連

本書は、ISO/IEC 27000、ISO/IEC 27001、ISO/IEC 27002、ISO 31000、ISO Guide 73という表記で規格を掲載していますが、それぞれ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、以下の状況を踏まえて、ISMSを構築し、運用する組織の皆様及びISMSをビジネスとしてコンサルティングや教育・研修に携わる皆様に、ISMSの国際規格(ISO/IEC 27001を含むISMSファミリー規格)を担当する標準化委員会(ISO/IEC JTC 1/SC 27/WG 1)の国内委員が直接解説することで、規格を開発・改正した意図を含め正しい規格の解釈を提供する。

ISO/IEC 27001は、「情報セキュリティマネジメントシステム(以降、ISMSという)」の要求事項を規定した国際規格である。本規格は、2005年10月に初めて発行され、8年後の2013年10月に改正第2版発行(JIS Q 27001は2014年、そして今回9年後の2022年10月に改正第3版発行(JIS Q 27001は2023年9月に発行)された。

ISO/IEC 27001：2013(第2版)が発行されてから2022年に改正されるまでの10年間で、日本におけるスマートフォンの世帯保有率が2013年の62.6%に対して2022年は90.1%まで上昇(約1.4倍)、世界のデータセンター市場規模は2013年の1,630億ドルから2023年は2,370億ドル(約1.5倍)に増加すると予測され、世界のパブリッククラウドサービスは2014年の約604億ドルから2019年は2,420億ドル(約4倍)に増加している(総務省「令和5年版情報通信白書」)。また、NICT(国立研究開発法人情報通信研究機構)が発表した日本国内のサイバー攻撃関連通信のパケット数は2013年の約129億件から2022年は5,226億件(約40倍)に増加している(NICTのウェブサイトより)。

このように、情報セキュリティを取り巻く国内外の状況は急速に変化しており、情報セキュリティインシデントの内容も大きく変化しているため、情報セキュリティ対策への要求もまた大きく変化している。

特に、ISO/IEC 27001：2013では十分に考慮されていなかったサイバーセキュリティやクラウドセキュリティなどへの対策が、ISO/IEC 27001：2022では新しい管理策として追加されたり、既存の管理策について要求事項はそのままでも、ガイドライン規格のISO/IEC 27002：2022の手引(ISO/IEC 27001の管

理策を実装するためのガイドラインとなる）には、新しい又は変化した脅威に対する対応策が盛り込まれたりしている。

本書は、ISO/IEC 27001：2022（JIS Q 27001：2023）の要求事項について、国際規格策定の過程を踏まえ、規格に記述された内容だけでは読み取れない解釈を含めて解説することを通し、規格の正しい要求内容が読者に理解され、以下のようなことが可能になることを目指している。

想定している読者は、ISMS の構築・運用にかかわるすべての関係者で、例えば、経営者、代表者、CISO、CIO、ISMS 事務局、ISMS 推進者、ISMS 内部監査員、ISMS コンサルタント、ISMS 審査員、及びこれから ISMS を構築しようとするプロジェクトメンバーである。

本書の執筆で目標としたものは以下のとおりである。

① ISO/IEC 27001：2013 から ISO/IEC 27001：2022 で改正された変更点について、これまで実施してきた ISMS の成果を活用しつつ、変更によるインパクトに適切に対応できる（例えば、リスクの定義、リスク特定）。

② 2013 年以来の新しいビジネス環境やシステム環境の変化に対応し、企業の経営戦略を実現するために、必要かつ有効な ISMS を構築できる（例えば、組織及びその状況の理解、リスク及び機会に対処する活動）。

著者の羽田は、国内の「ISO/IEC JTC 1/SC 27/WG 1」の会議に参加し、国際会議の原案作成にかかわり内容を熟知していると同時に、「日本 ISMS ユーザグループのインプリメンテーション研究会」メンバーとして、ISMS の計画・構築の研究を実践的にリードしている。また、現役の ISMS 構築・運用コンサルタント、JRCA 承認の ISMS 審査員研修主任講師としても活動しており、本書の解説に、その知見を反映している。共著者の土屋は、「ISO/IEC JTC 1/SC 27/WG 1」の委員として、ISO/IEC 27001 や ISO/IEC 27002 及び ISO/IEC 27017 に関する国際会議に参加したうえで、各国との討議を通じ、規格の改正作業に参加してきた。また、羽田と同様に ISMS 構築・運用のコンサルタントとしても活躍している。そのため、本書には、国際会議において討議された規格原案の審議結果や解釈も盛り込んでいる。

2023 年 11 月

羽田卓郎　土屋直子

本書の構成

■ JIS Q 27001：2023 の要求事項の掲載を止めた理由

本書の第 1 版では、JIS Q 27001：2014(JIS 規格票)の要求事項を掲載しながら解説してきたが、第 2 版では、JIS Q 27001：2023 の要求事項を掲載せず、要求事項を要約したうえで解説している。この変更は、JIS Q 27001：2014 の著作権は国にあったものの、JIS Q 27001：2023 の著作権が一般財団法人日本規格協会にあることによる。規格本文および附属書 A を転載するには、日本規格協会に著作権使用料を支払う必要があり、本書の定価が高くなり、読者に多大な負担をかけることを避けるために JIS 規格票の転載を断念した。

JIS 規格票からの転載がなくても理解しやすいように要求事項の要約を掲載しているが、認証取得のために正確な要求内容を確認する場合は日本規格協会の JIS 規格票を参照していただきたい。

■第 1 章から第 11 章の構成について

2022 年の ISO/IEC 27001 の改正は、ISO/IEC のマネジメントシステム規格(MSS)の共通テキスト[1)]の改訂に伴う規格本文の改正、及び ISO/IEC 27002 の改訂に伴う附属書 A の管理策[2)]の差し替えとなっている。

ISO/IEC 27001 の本文(箇条 4 ～ 10)に関する改正による変更は、マネジメントシステム規格(MSS)の共通テキストの改正によるもので、情報セキュリティ固有の要求事項に対する変更は含まれていない。

脚注 1)の ISO/IEC 専門業務用指針共通テキストの改訂は、定期的に行われており最新版は 2022 年に発行されている。今回の変更は、主に要求事項の最

1） ISO/IEC のマネジメント規格作成者に対する指針「ISO/IEC 専門業務用指針第 1 部統合版 ISO 補足指針附属書 SL の Appendix 3(規定)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」で提供している共通テンプレート。

2） ISO/IEC 27001 の附属書 A は、ISO/IEC 27002 の管理策を一覧として反映したものである。

適化であり、規格要求事項に対する変更対応は部分的なものにとどまっている。

今回の改正の大部分は、附属書 A の管理策について、すべての管理策の項番が変更になったほか、管理策の集約と新規管理策の追加、分類の変更、管理目的の廃止、など大きな変更が行われた。また、ISO/IEC 27001 が参照している ISO/IEC 27002 の管理策の目的や手引についても、2013 年以降の社会的、技術的環境の変化を受けて見直しが行われ、2013 年版と 2022 年版では、同じ管理策であっても要求内容に変化が起きていることを認識する必要がある。

本書は、規格が求める要求事項について、そのねらいを明確にし、具体的な事例を含めた解説を通じて理解を助けるために、以下のように構成している。

① 第 1 章は、「情報セキュリティマネジメントシステムの意義と規格開発・改正の仕組み」を、第 2 章は「ISO/IEC 27001 の改正の趣旨と主要な改正点」を解説することで、改正の全体像を示している。

② 第 3 章の「ISO/IEC 27001：2022 の用語及び定義」及び第 4 章の「箇条 4　組織の状況」から第 10 章の「箇条 10　改善」までを解説している。また、改正内容についても ISO/IEC 27001：2013 からの変更点を解説し、ISMS 運用組織が適切に変更対応できるようにしている。

　第 3 章の ISO/IEC 27000 の用語及び定義は、ISO/IEC 27001 の規格要求事項の用語に当てはめた場合に、定義部分も要求事項とみなされるため、ISO/IEC 27001 の用語を定義と置き換えたものが要求事項であることに留意されたい。

　第 11 章は、附属書 A の管理策について、管理策が要求している対策の目的と要求内容の解釈及び実施のための事例紹介を含めた解説を提供し、改正内容についても ISO/IEC 27001：2013 からの主な変更点を解説し、本文と同様に、すでに ISMS を構築し運用している組織が適切に変更対応できるようにしている。

③ 本書の発行時点では、ISO/IEC 27002：2022 の JIS 化は行われていないが、第 11 章では、27000 シリーズの国際規格標準化委員会に参加している著者が ISO/IEC 27002：2022 の手引を要約する形で解説している。

本書は、ISO/IEC 27001：2022(JIS Q 27001：2023)の規格要求事項を徹底解説したものであるが、ISO/IEC 27001 に基づく ISMS を構築・運用するには規格要求事項を理解しただけでは難しいため[3)]、本書の姉妹書で ISMS 構築・

運用者のための『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)と ISMS 内部監査責任者及び監査担当者のための『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】』(日科技連出版社)を併せて購読することをお勧めする。

また、ISMS 認証に加えてクラウドセキュリティの構築と運用及び認証取得を目指す読者には、『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)の購読をお勧めする。

「新旧管理策の対応表」ダウンロードのご案内

新旧管理策の対応表を、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. 新旧管理策の対応表の著作権は著者にあります。本対応表を無断で複製・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。

3) ISO/IEC 27001 の規格要求事項には「しなければならない」ことは書いてあるが「どのようにすればよいか」は書いておらず「組織が自分で考える」ことになっている。

目　次

目　次

6.3　箇条 6.3　変更の計画策定

要求事項の要約

継続的改善の過程で組織の ISMS を変更する場合、変更中及び変更後も意図した結果を達成できるように変更を計画的に行うことが求められている。

(1)　解説

MSS 共通テキスト改訂に基づき箇条 6.3 が追加された。ISMS はプロセス間の相互作用を含んでいるため、その変更は総合的に考える必要があり、変更のきっかけが計画的か非計画的かは別として、変更は計画的に行うべきということである。

組織を取り巻く環境や法令及び規制要求事項、ビジネス戦略や戦術の変更、利害関係者のニーズ及び期待の変化などによって、組織体制や業務プロセス及び取り扱う情報資産の重要性などを変更する場合に ISMS 要求事項への不適合や、情報セキュリティの弱点が発生しないようにしなければならない(箇条 4.1、箇条 4.2、箇条 4.3、箇条 6.1 に関連)。

また、変更を管理する場合、関連するリスクのアセスメントを行い必要な対策を講じるべきである。特に、アクセス権の変化や、役割責任の変化などが、変更前と変更後でどのようにコントロールされるべきかを見直すことが重要である。

組織の変更によって、物理的な変更(拠点や区画の変更)を伴う場合は、物理的なセキュリティの見直しも必要である。

「情報処理設備、情報システム」に対する変更管理に関しては、11.3.4 項(14)の管理策「8.32　変更管理」の解説を参照されたい。

(2)　ISO/IEC 27001：2013/JIS Q 27001：2014との比較

箇条 6.3 は新規の要求事項である。

ISO/IEC 27001：2013 では、規格本文(箇条 4 ～ 10)に変更管理に関する要求はなく、附属書 A の管理策である「A.12.1.2　変更管理」や「A.14.2.2　シ

ステムの変更管理手順」を選択することで「組織、業務プロセス、情報処理設備、情報システム」に対する変更を管理することを要求していた。

しかし、ISO/IEC 27001：2022では、附属書Aの変更管理に関連する管理策(A.12.1.2、A.14.2.2、A.14.2.3、A.14.2.4)が統合され「8.32　変更管理」となったが、変更の対象が「情報処理施設及び情報システム」に限定されたため「組織、業務プロセス」などの変更については、本項によって管理すべきということになる。

蔵記憶装置をもつ ICT 機器の情報の削除方法は 7.10 と 7.14 の解説を参照)。また、媒体や ICT 機器の内蔵記憶装置の情報の消去を外部委託する場合には、作業完了の証拠を入手すべきである。

クラウドサービスの情報削除では、クラウドサービス特有のリスク[59]があるため、重要な情報を扱うシステムをクラウドサービスに移行又は構築する場合は、利用を開始する前に情報削除の手続を確認し容認できるかどうかを判断すべきである(5.23 を参照)。

(b)　主な変更点

8.10 は新規の管理策であるが、7.10(旧 A.8.3.2)記憶媒体と 7.14(旧 A.11.2.7)の装置のセキュリティを保った処分又は再利用と関連している。

しかし、7.10 及び 7.14 は、廃棄又は再利用を前提としているため、ICT 機器や媒体の処分や再利用を伴わない電子的情報削除の要求にも対応できるように独立した管理策となった。

管理策(附属書A)の要約

8.11　データマスキング

【要約】

個人識別可能情報(PII)を含む、取扱いに慎重を要するデータの開示を制限するため、適用される法令を考慮し、関連するトピック固有の方針、並びに事業上の要求事項に従ってデータマスキングを実施することが求められている。

(a)　解説

個人情報保護法における「匿名加工情報」対応を含め、個人情報及びその他の機微な情報の露出を制限するために、アクセス制御に関するトピック固有の方針及びその他のデータ保護に関連する要求事項に従ってデータマスキングを

59)　クラウドサービスでは、組織が利用している仮想ストレージの物理環境を他のテナントと共有しているため、物理的破壊やデータエリア全体の完全消去による情報削除はできない。したがって、仮想ストレージ上のデータ消去及び上書きによるデータ消滅による情報削除となる。

実施しなければならない。

データマスキングは、取扱いに慎重を要するデータの開示を制限することが目的であり、匿名化だけでなく用途に応じて以下のような方法がある。

① アクセス制御：利用者に応じて必要最小限のデータのみ開示するようクエリやマスクを設計する(不必要なデータは見せない)。

② 暗号化：許可された利用者のみにデータを開示するため暗号鍵の提供を制限する。

③ 難読化：データの中の一部の記録を特定の利用者から掩蔽(えんぺい)したい場合に、データの難読化を行う。例えば、組織の情報の一部を難読化し、一般従業員には重要機密を隠蔽した情報を開示し、管理者にはすべての情報を開示するような仕組みとする。必要があれば、難読化されていること自体を難読化(隠蔽)する[60]ことも必要となる。

④ 匿名化：個人情報の統計的情報が必要な場合などで、個人を特定する必要がない場合は、個人を特定できる情報を無関係のデータに置き換えるか削除する。この処理は不可逆的に行う必要がある。

⑤ 仮名化：他の情報と照合しない限り特定の個人を識別することができないように個人情報を加工して得られる個人に関する情報であり、本人を識別するために他の情報と仮名加工情報を照合することは禁じられている。改正個人情報保護法では、仮名加工情報を利用できるのは、同一社内と委託先及びあらかじめ公表している共同利用先に限定している。

⑥ 偽名化：個人を特定できる情報を別名で置き換える又はランダムに入れ替える。ただし、この処理は復元可能な場合が多いため、偽名化のアルゴリズムを保護する必要がある。

⑦ 置換：開示したくないデータの全部又は一部を他の値に変換し元の値を隠蔽する。

(b) 主な変更点

8.11 は新規の管理策である。5.10(旧 A.8.2.3)の情報及びその他の関連資産の

60) 例えば、PII で血液検査の特定の項目や懲戒処分の記録の難読化を無関係の第三者に開示したくない場合に、PII 主体が難読化のさらに難読化を要求する場合がある。

索　引

【ア　行】

【タ　行】

■著者紹介

羽田　卓郎(はねだ　たくろう)

【略歴】

1970 年　昭和石油㈱(現：出光興産㈱)：販売企画
1990 年　シェル・サービス・インターナショナル㈱：情報セキュリティ GM
2002 年　INSI ㈱　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兼コンサルティング部長
2012～2018 年 9 月　リコージャパン㈱　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

【保有資格と活動】

ISO/IEC 27001 主任審査員 & ISMS クラウドセキュリティ審査員、JNSA-日本 ISMS ユーザーグループ研究会、ISO/IEC TMB JTC 1 SC 27 WG 1(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)リエゾンメンバー他

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、2004 年、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)構築・運用の実践【第 2 版】』(日科技連出版社、2024 年刊行予定)、『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】』(共著、日科技連出版社、2024 年刊行予定)、『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)

土屋　直子(つちや　なおこ)

【略歴】

1998 年 4 月　NTT ソフトウェア㈱　入社
2002 年～現在　ISMS などのセキュリティマネジメントコンサルティングに従事
2015 年～現在　ISO/IEC 27017 などのクラウドセキュリティコンサルティングに従事
2017 年 4 月　NTT テクノクロス㈱(合併による新会社発足)
現　在　NTT テクノクロス㈱ セキュアシステム事業部 テックリード

【保有資格と活動】

ISO/IEC JTC 1/SC 27/WG 1 国内委員会委員、情報セキュリティマネジメントシステム JIS 原案作成委員会委員、クラウドセキュリティ規格 JIS 原案作成委員会委員、

JIPDEC ISMS 審査員、JIPDEC ISMS クラウドセキュリティ審査員、JASA 公認情報セキュリティ監査人

標準化貢献賞受賞(情報処理学会 情報規格調査会 2023 年度)、ISMS、ISO/IEC 27017、ISMAP などの認証取得支援、セキュリティマネジメントコンサルティング、SC27 活動を通して、ISO/IEC 27001：2022、ISO/IEC 27002：2022 策定に貢献、JNSA、日本規格協会などの ISO/IEC 27001：2022、ISO/IEC 27002：2022 改訂セミナーの講演多数

【著作】

『ISO/IEC 27017：2015(JIS Q 27017：2016)ISO/IEC 27002 に基づくクラウドサービスのための情報セキュリティ管理策の実践の規範―解説と活用ガイド』(共著、日本規格協会)

山﨑　哲(やまさき　さとる)

【略歴】

1970 年　京都大学理学部卒業後、日本 IBM ㈱入社
2006 年　IBM ビジネスコンサルティングサービス　セキュリティ最高責任者(CSO)
2009 年　工学院大学エクステンションセンター客員教授
2010 ～ 2019 年　ISO/IEC JTC 1/SC 27/WG 1 主査
2011 ～ 2015 年　ISO/IEC 27017(Cloud security control)プロジェクトエディタ
2012 ～ 2017 年　クラウドセキュリティコントロール標準化専門委員会委員長
2015 ～ 2016 年　JIS Q 27017 JIS 原案作成委員会 委員長
2016 ～ 2019 年　工学院大学情報学部客員研究員
現　在　トーストマスターズクラブ　メンバー

【著作】

『ビッグデータ・マネジメント』(共著、エヌ・ティー・エス)、『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』(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】

2014年 5月24日　第1版第1刷発行
2021年12月 7日　第1版第9刷発行
2023年12月31日　第2版第1刷発行

著者　羽田卓郎
土屋直子
山﨑哲

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 978-4-8171-9782-5
URL　https://www.juse-p.co.jp/