

無断使用をお断りします。日科技連出版社

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

無断使用をお断りします。日科技連出版社



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

まえがき iii

第1章	ISMSの内部監査とは	1
1.1	ISMSにおける内部監査と国際標準	2
1.2	監査の用語及び定義(抜粋)&解説	8
第2章	情報セキュリティ内部監査の考慮点	25
2.1	ISMSの内部監査(全般)	26
2.2	ISMSの規格要求事項の考慮点:本文	31
2.3	ISMSの規格要求事項の考慮点:管理策	64
第3章	情報セキュリティ内部監査の実務	121
3.1	ISMS内部監査の実務	122
3.2	ISMS内部監査プログラムと実施手順	133
第4章	組織の内部監査の課題を解決するための監査の体制と 手法及び技術	157
4.1	よくある内部監査の問題点と解決策	158
4.2	内部監査をレベルアップさせる	163
第5章	企業における情報セキュリティ内部監査の実態と 監査事例	179
5.1	ISMS内部監査の実態	180
5.2	ISMS内部監査の事例紹介	182
第6章	内部監査チェックリスト	213
6.1	内部監査チェックリストの作成	214
6.2	監査チェックリストの有効活用の勧め	225
	参考文献	229
	索引	231

「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 :

パスワード :

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

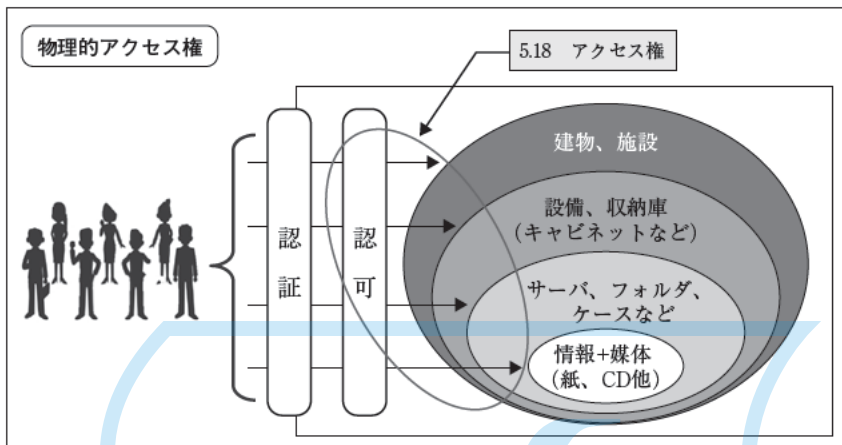
管理策の5.15～5.18は、情報及び情報を扱うための関連資産を保護するために、許可された者が許可された範囲の資産にアクセスできるようにすることを求めている。そのため、「許可された者」を識別するためのID管理、IDをもつ者が本人であることを確認するための認証、認証された者がアクセスできる対象を管理するためのアクセス権を管理する必要がある。

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。

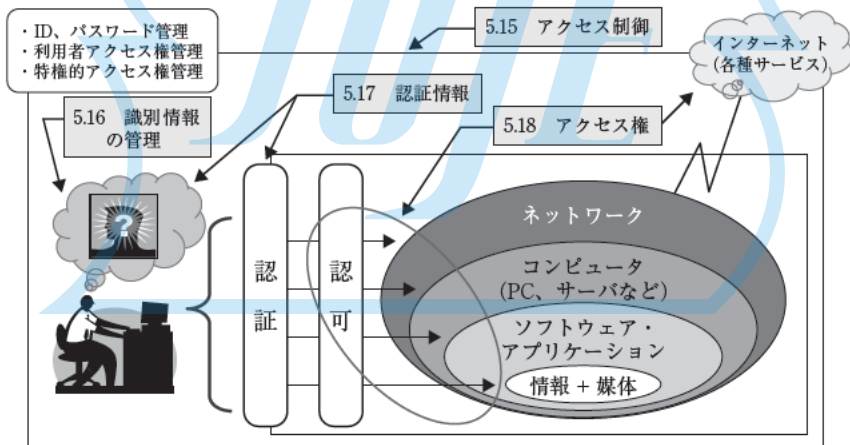
情報及び情報に関連する資産に対するアクセスは、許可のないアクセスや悪意をもったアクセスから保護しなければならない。そのためには、許可されていると主張する者が許可された本人¹⁵⁾かどうかを確認しなければならない。

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 ② 5.7 脅威インテリジェンス 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)。 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 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 (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、 △改善の機会、－：対象外		
<ul style="list-style-type: none"> • 情報セキュリティ関連情報収集先一覧 • 情報セキュリティ関連情報収集体制 • 脅威インテリジェンス分析体制・職務分担表 • 脅威インテリジェンス分析報告書 • 脅威インテリジェンスリスク対応計画 • プロジェクト運営規則 • プロジェクト体制・職務分担表 • プロジェクト管理記録(議事録など) • システム開発設計仕様書 		
<ul style="list-style-type: none"> • 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) • 社内システム利用規則 • その他ヒアリングで確認した監査証拠 • 情報資産分類の定義書 • 文書等のラベル • 外部記憶媒体管理基準(保管、持出し、処分など) 		
<ul style="list-style-type: none"> • 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) • 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) • 社内システム利用規則 • 外部記憶媒体管理基準(保管、持出し、処分など) 		

索引

- 【英数字】**
- 5. 組織的管理策 69
 - 6. 人的管理策 89
 - 7. 物理的管理策 93
 - 8. 技術的管理策 99
 - ISMS 適用範囲の4要素 36
 - ISO 17021-1 : 2018 14
 - ISO 19011 8, 122
 - ISO/IEC 27001 が要求する内部監査
4
 - PREP 法 182
 - に基づく事例の構成 183
- 【あ 行】**
- アクセス権管理 75
 - 委託先との情報セキュリティ管理ルー
ルの締結について 202
 - 委託先の情報セキュリティ管理ルー
ルの順守状況の確認について 204
 - インシデント管理 81
 - インタビューの考慮点 138
 - 運用の計画策定及び管理 57
- 【か 行】**
- 改善の機会 131
 - (例) 155
 - 外部記録媒体の長期保管リスク
186
 - 監査(audit) 9, 123
 - 監査依頼者(audit client) 14
 - 監査員(auditor) 16
 - の力量向上 178
 - 監査基準(audit criteria) 12
 - 監査計画(audit plan) 12
 - の策定 129
 - 監査結論(audit conclusion) 14
 - 監査実施計画(例) 141
 - 監査実施計画書別紙<監査項目一覧表>
142
 - 監査実施計画の策定 140
 - 監査手法 138
 - と技術 160
 - の種類と特徴 139
 - 監査証拠(audit evidence) 13
 - 監査所見(audit findings) 13, 131
 - における改善の機会とストロン
グポイント 173
 - 監査チェックリスト 137
 - の作成 216
 - の種類と考え方 214
 - の有効活用の勧め 225
 - 監査チーム(audit team) 16
 - 会議 145
 - の結成 135
 - 監査手続の流れ 133
 - 監査におけるインタビュー手順(例)
175
 - 監査の基本 123
 - 監査の国際標準(国際規格) 8
 - 監査の実施手順 129
 - 監査の重点項目の決定 174
 - 監査の重点ポイントのイメージ
174

監査の種類	10
監査の手順とその関連	135
監査の歴史	3
監査範囲(audit scope)	11
監査プログラム(audit programme)	
11, 128	
——の作成及び管理	133
——レビュー	156
監査報告における助言	177
監査方針	159
客観的証拠	13
供給者管理	78
業務システム環境とオフィスエリア環境におけるデータの分離(業務システムデータの管理の徹底)について	200
業務遂行部門の監査	145
クラウド環境上のシステム構築リスク	190
継続的改善	62
軽微な不適合	131
コミュニケーション	53
コンプライアンス管理	87
【さ 行】	
事業の中断・障害時の情報セキュリティ管理	83
資源	51
資産管理	72
システム開発・導入・運用の管理	113
システム開発環境と本番環境の分離とデータの隔離(本番データを試験に使用する場合の保護)	198
事前準備	136
実査による確認の必要性の認識	184

実地監査	143
——の基本ステップ	140
重大な不適合	131
終了会議	148
順守(法令、規制及び契約上の要求事項)関連リスク	188
情報アクセスの管理	99
情報資産運用の管理	102
情報セキュリティのリスク対策イメージ	64
情報セキュリティ方針	38
情報セキュリティマネジメントシステムの適用範囲の決定	35
情報セキュリティ目的及びそれを達成するための計画策定	49
情報セキュリティリスクアセスメント	43, 58
情報セキュリティリスク対応	46, 59
初回会議	143
——の議題(例)	143
人的管理	89
推進事務局に対する監査	144
ストロングポイント	131
セキュリティホール(ぜい弱性)への対応	196
是正・予防処置	153
是正処置回答書(例)	149
是正処置回答書作成	148
是正処置要求書(例)	147
是正処置要求書作成	146
是正手順のイメージ	154
組織及びその状況の理解	33
組織管理	69
組織の使命と情報セキュリティの関係	34
組織の状況を把握するための内容(例)	

164	
組織の役割、責任及び権限	39
【た 行】	
チェックリストの有効活用について	210
チェックリストを使った事実確認のプロセス	175
適合(conformity)	19
適正利用の管理	108
特権 ID 管理(共有利用の問題点)	194
トップインタビュー	144
トップマネジメントインタビュー・チェックリスト	214, 216
【な 行】	
内部監査	60
— 員の力量	29
— 基準	128
— 規程・手順書の整備	128
— 計画書(例)	130
— チェックリストダウンロードのご案内	vi
— における 3 つの観点	125
— における効率性の確認	171
— における適合性確認の視点	167
— における適合性確認の視点のモデル	168
— における有効性監査の必要性	160
— における有効性の確認	169
— の運用体制	158
— の抱える問題点	180
— の課題	181
— の基準	125

— の機能と実行体制	7
— の指示と報告の流れ	132
— の体制	28
— の目的	124, 128
— の目的と必要性	2
— プログラム	30
— 報告	150
— 報告書(例)	151
— 報告書別紙〈監査実施項目一覧表〉(例)	154
認識	52

【は 行】

媒体と装置の管理	96
パフォーマンス(performance)	21
— 評価	59
被監査者(auditee)	15
— へのインタビューのテクニックについて	206
被監査組織の事前情報の入手について	208
被監査部門の役割と責任	129
フォローアップ	156
附属書 A の管理策の監査	27
物理的領域の管理	93
不適合(nonconformity)	19
— 及び是正処置	62
— の等級付け	14
プロセス(process)	20
— アプローチ	27
文書化した情報	54
— の管理	56
文書監査	143
【ま 行】	
マネジメントシステム(management system)	16

—・チェックリスト 218
 —・チェックリスト(本文対応)
 215
 —の監査 26
 マネジメントレビュー 61
 目的に対するリスク特定のモデル
 44
 持出し専用 PC に格納した機密情報の
 管理リスク 192
 問題点/改善点を特定するプロセス
 176

【や行】

有効性(effectiveness) 22
 要求事項(requirement) 20

【ら行】

利害関係者のニーズ及び期待の理解
 34
 利害抵触 28
 力量(competence) 19, 52
 リスク(risk) 18
 —アプローチ 163
 —及び機会に対する活動 40
 —対応(risk treatment) 22
 —対策(管理策対応)・チェックリ
 スト 216, 219
 —対策の有効性の考え方 170
 —マップ(例) 45
 リーダーシップ 37

■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(株)(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(株) 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(株)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(株)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(株)(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(株) 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(株) 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

無断使用をお断りします。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)
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

© Takuroh Haneda, Masaharu Uowaki 2019, 2024

ISBN 978-4-8171-9785-6

URL <https://www.juse-p.co.jp/>

本書の全部または一部を無断でコピー、スキャン、デジタル化などの複製をすることは著作権法上での例外を除き禁じられています。本書を代行業者等の第三者に依頼してスキャンやデジタル化することは、たとえ個人や家庭内での利用でも著作権法違反です。