情報セキュリティ：ISO 27001 改訂版

管理策相互比較ガイド

ISO 27001:2013
および
ISO 27001:2022

主な変更点

2022 年 2 月、組織がセキュリティを向上させるために実施できるベストプラクティスの管理策を定めた規格である ISO 27002:2022 が改訂されました。その結果、情報セキュリティマネジメントシステム (ISMS) の要求事項を規定した国際規格である ISO 27001 の改訂版も、2022 年 10 月 25 日に公表されました。

改訂版では ISO 27002:2022 で示されている管理策が採用されており、組織はリスク評価を再検討して、更新または新たなリスク対応を実施すべきかどうかを判断する必要があります。

既存の ISO 27001:2013 認証を取得している組織は、3 年以内に新規格に移行する必要があります。

現在は、
114
ではなく
93
の管理策があります。

合計で
11
の新しい管理策があります。

ISO 27001:2013 の
56 の管理策が
ISO 27001:2022 では
24 の管理策に統合

管理策の
大方は、
規格の解釈および実施方法に影響を与える可能性のある何らかの形のテキスト変更の対象となる

管理策が 4 つの「新しい」テーマに分割された

組織
- 28 統合
- 3 新規

人
- 2 統合
- 0 新規

物理的
- 5 統合
- 1 新規

技術的
- 21 統合
- 7 新規

管理策の相互比較：ISO 27001:2013（附属書 A）と ISO 27001:2022（附属書 A）

ISO 27002:2022 に概説されている管理策は、ISO 27001:2022 附属書 A に含まれる予定であり、これは新規格における最も重要な変更領域を示しています。以下の表は、利用可能なすべての管理策と、それらが以前のバージョンの管理策にどのように対応しているか（示されている新たな管理策と統合を含む）を相互比較したものです。

以前の ISO 27001:2013			新たな ISO 27001:2022		
管理策	**タイトル**		**管理策**	**テーマ（新規）**	**タイトル**
情報セキュリティ方針					
A5.1.1	情報セキュリティに関する方針	→	A.5.1	組織の管理策	情報セキュリティに関する方針
A.5.1.2	情報セキュリティに関する方針のレビュー	→	**A.5.1 に統合**		
情報の整理					
A.6.1.1	情報セキュリティの役割と責任	→	A5.2	組織の管理策	情報セキュリティの役割と責任
A.6.1.2	職務の分離	→	A.5.3	組織の管理策	職務の分離
A.6.1.3	当局との連絡	→	A.5.5	組織の管理策	当局との連絡
A.6.1.4	特別な利害関係者グループに連絡する	→	A.5.6	組織の管理策	特別な利害関係者グループに連絡する
新規			A.5.7	組織の管理策	脅威インテリジェンス
A.6.1.5	プロジェクトマネジメントにおける情報セキュリティ	→	A.5.8	組織の管理策	プロジェクトマネジメントにおける情報セキュリティ
A.6.2.1	モバイル端末方針	→	A.8.1	技術的	ユーザーエンドポイント端末
A.6.2.2	テレワーク	→	A.6.7	人	遠隔勤務

人的資源のセキュリティ					
A.7.1.1	スクリーニング	→	A.6.1	人	スクリーニング
A.7.1.2	雇用条件	→	A.6.2	人	雇用条件
A.7.2.1	マネジメントの責任	→	A.5.4	組織の管理策	マネジメントの責任
A.7.2.2	情報セキュリティ意識、教育研修	→	A.6.3	人	情報セキュリティ意識、教育研修
A.7.2.3	懲戒プロセス	→	A.6.4	人	懲戒プロセス
A.7.3.1	雇用責任の終了または変更	→	A.6.5	人	雇用の終了または変更後の責任
資産マネジメント					
A.8.1.1	資産の在庫管理	→	A.5.9	組織の管理策	情報およびその他の関連資産の在庫管理
A.8.1.2	資産の所有権	→	**A.5.9 に統合**		
A.8.1.3	資産の許容可能な使用	→	A.5.10	組織の管理策	情報およびその他の関連資産の許容可能な利用
A.8.1.4	資産の返還	→	A.5.11	組織の管理策	資産の返還
A.8.2.1	情報の分類	→	A.5.12	組織の管理策	情報の分類
A.8.2.2	情報のラベリング	→	A.5.13	組織の管理策	情報のラベリング
A.8.2.3	資産の取扱い	→	**A.5.10 に統合**		
A.8.3.1	リムーバブルメディアのマネジメント	→	A.7.10	物理的	ストレージメディア
A.8.3.2	メディアの廃棄	→	**A.7.10 に統合**		
A.8.3.3	物理的メディア移管	→	**A.7.10 に統合**		

アクセス制御					
A.9.1.1	アクセス制御方針	→	A.5.15	組織の管理策	アクセス制御
A.9.1.2	ネットワークやネットワークサービスへのアクセス	→	**A.5.15 に統合**		
A.9.2.1	ユーザー登録と登録解除	→	A.5.16	組織の管理策	ID マネジメント
A.9.2.2	ユーザーアクセスプロビジョニング	→	A.5.18	組織の管理策	アクセス権
A.9.2.3	特権アクセス権のマネジメント	→	A.8.2	技術的	特権アクセス権
A.9.2.4	ユーザーの秘密認証情報のマネジメント	→	A.5.17	組織の管理策	認証情報
A.9.2.5	ユーザーアクセス権のレビュー	→	**A.5.18 に統合**		
A.9.2.6	アクセス権の削除または調整	→	**A.5.18 に統合**		
A.9.3.1	秘密認証情報の使用	→	**A.5.17 に統合**		
A.9.4.1	情報アクセス制限	→	A.8.3	技術的	情報アクセス制限
A.9.4.2	安全なログオン手順	→	A.8.5	技術的	安全な認証
A.9.4.3	パスワードマネジメントシステム	→	**A.5.17 に統合**		
A.9.4.4	特権ユーティリティプログラムの使用	→	A.8.18	技術的	特権ユーティリティプログラムの使用
A.9.4.5	プログラムソースコードへのアクセス制御	→	A.8.4	技術的	ソースコードへのアクセス
暗号					
A.10.1.1	暗号制御の使用に関する方針	→	A.8.24	技術的	暗号の使用
A.10.1.2	キーマネジメント	→	**A.10.1 .1 と共に A.8.24 に統合**		

物理的および環境的セキュリティ					
A.11.1.1	物理的なセキュリティ境界	→	A.7.1	物理的	物理的なセキュリティ境界
A.11.1.2	物理的な入室管理策	→	A.7.2	物理的	物理的進入
A.11.1.3	事務所・部屋・施設のセキュリティ確保	→	A.7.3	物理的	事務所・部屋・施設のセキュリティ確保
新規			A.7.4	物理的	物理的セキュリティ監視
A.11.1.4	外部および環境の脅威からの保護	→	A.7.5	物理的	物理的および環境の脅威からの保護
A.11.1.5	安全な領域での作業	→	A.7.6	物理的	安全な領域での作業
A.11.1.6	搬入・積み込み領域	→	**A.11.1 .2 と共に A.7.2 に統合**		
A.11.2.1	機器の設置と保護	→	A.7.8	物理的	機器の設置と保護
A.11.2.2	支援ユーティリティ	→	A.7.11	物理的	支援ユーティリティ
A.11.2.3	ケーブル配線のセキュリティ	→	A.7.12	物理的	ケーブル配線のセキュリティ
A.11.2.4	設備・機器の保全	→	A.7.13	物理的	設備・機器の保全
A.11.2.5	資産の削除	→	**A.7.10 に統合**		
A.11.2.6	施設外の設備と資産のセキュリティ	→	A.7.9	物理的	施設外の資産のセキュリティ
A.11.2.7	機器の安全な廃棄または再利用	→	A.7.14	物理的	機器の安全な廃棄または再利用
A.11.2.8	無人ユーザー設備	→	**A.6.2.1 と共に A.8.1 に統合**		
A.11.2.9	クリアデスクおよびクリアスクリーン方針	→	A.7.7	物理的	クリアデスクとクリアスクリーン

運用セキュリティ				
A.12.1.1	文書化された運用手順	A.5.37	組織の管理策	文書化された運用手順
A.12.1.2	変更マネジメント	A.8.32	技術的	変更マネジメント
A.12.1.3	容量マネジメント	A.8.6	技術的	容量マネジメント
A.12.1.4	開発、テスト、運用環境の分離	A.8.31	技術的	開発環境、試験環境、本番環境の分離
A.12.2.1	マルウェアに対する管理策	A.8.7	技術的	マルウェアからの保護
A.12.3.1	情報バックアップ	A.8.13	技術的	情報バックアップ
A.12.4.1	イベントロギング	A.8.15	技術的	ロギング
A.12.4.2	ログ情報の保護	**A.8.1.5 に統合**		
A.12.4.3	管理者およびオペレーターのログ	**A.8.1.5 に統合**		
新規		A.8.16	技術的	監視活動
A.12.4.4	クロックの同期	A.8.17	技術的	クロックの同期
A.12.5.1	運用システムへのソフトウェアのインストール	A.8.19	技術的	運用システムへのソフトウェアのインストール
A.12.6.1	技術的脆弱性のマネジメント	A.8.8	技術的	技術的脆弱性のマネジメント
新規		A.8.9	技術的	構成マネジメント
新規		A.8.10	技術的	情報の削除
新規		A.8.11	技術的	データマスキング
新規		A.8.12	技術的	データ漏洩防止
A.12.6.2	ソフトウェアインストールの制限	**A.12.5.1 と共に A.8.19 に統合**		
A.12.7.1	情報システム審査の管理策	A.8.34	技術的	審査テスト中の情報システムの保護

コミュニケーションセキュリティ					
A.13.1.1	ネットワーク管理策	→	A.8.20	技術的	ネットワークセキュリティ
A.13.1.2	ネットワークサービスのセキュリティ	→	A.8.21	技術的	ネットワークサービスのセキュリティ
A.13.1.3	ネットワークにおける分離	→	A.8.22	技術的	ネットワークの分離
新規		→	A.8.23	技術的	ウェブフィルタリング
A.13.2.1	情報移管の方針と手順	→	A.5.14	組織の管理策	情報移管
A.13.2.2	情報移管に関する合意	→	**A.5.14 に統合**		
A.13.2.3	電子メッセージング	→	**A.5.14 に統合**		
A.13.2.4	機密保持契約または非開示契約	→	A.6.6	人	機密保持契約または非開示契約
システムの取得、開発、保全					
A.14.1.1	情報セキュリティ要求事項の分析と仕様	→	**A.6.1.5 と共に A.5.8 に統合**		
A.14.1.2	パブリックネットワーク上のアプリケーションサービスのセキュリティ確保	→	A.8.26	技術的	アプリケーションのセキュリティ要求事項
A.14.1.3	アプリケーションサービストランザクションの保護	→	**A.8.26 と統合**		
A.14.2.1	安全な開発方針	→	A.8.2.5	技術的	安全な開発ライフサイクル
A.14.2.2	システム変更管理手順	→	**A.12.1.2 と共に A.8.32 に統合**		
A.14.2.3	運用プラットフォーム変更後のアプリケーションの技術審査	→	**A.12.1.2、A.14.2.2 および A.14.2.4 と共に A.8.32 に統合**		
A.14.2.4	ソフトウェアパッケージへの変更の制限	→	**A.12.1.2、A.14.2.2 および A.14.2.3 と共に A.8.32 に統合**		
A.14.2.5	安全なシステムエンジニアリングの原則	→	A.8.27	技術的	安全なシステムアーキテクチャとエンジニアリング原則
A.14.2.6	安全な開発環境	→	**A.12.1.4 と共に A.8.31 に統合**		
新規		→	A.8.28	技術的	安全なコーディング
A.14.2.7	外部委託開発	→	A.8.30	技術的	外部委託開発
A.14.2.8	システムセキュリティテスト	→	A.8.29	技術的	開発と受け入れにおけるセキュリティテスト
A.14.2.9	システム受け入れテスト	→	**A.14.2 .8 と共に A.8.29 に統合**		
A.14.3.1	試験データの保護	→	A.8.33	技術的	試験情報

サプライヤーとの関係					
A.15.1.1	サプライヤーとの関係に関する情報セキュリティ方針	→	A.5.19	組織の管理策	サプライヤーとの関係における情報セキュリティ
A.15.1.2	サプライヤー契約内におけるセキュリティへの対応	→	A.5.20	組織の管理策	サプライヤー契約内における情報セキュリティへの対応
A.15.1.3	情報通信技術サプライチェーン	→	A.5.21	組織の管理策	情報通信技術（ICT）サプライチェーンにおける情報セキュリティの管理
A.15.2.1	サプライヤーサービスの監視とレビュー	→	A.5.22	組織の管理策	サプライヤーサービスの監視、レビュー、変更マネジメント
A.15.2.2	サプライヤーサービスへの変更の管理	→	**A.15.2 .1 と共に A.5.22 に統合**		
新規			A.5.23	組織の管理策	クラウドサービス使用に関する情報セキュリティ
情報セキュリティインシデントマネジメント					
A.16.1.1	責任と手順	→	A.5.24	組織の管理策	情報セキュリティインシデントマネジメントの計画と準備
A.16.1.2	情報セキュリティイベントの報告書作成	→	A.6.8	人	情報セキュリティイベントの報告書作成
A.16.1.3	情報セキュリティの脆弱性の報告書作成	→	**A.16.1 .2 と共に A.6.8 に統合**		
A.16.1.4	情報セキュリティイベントの審査と決定	→	A.5.25	組織の管理策	情報セキュリティイベントの審査と決定
A.16.1.5	情報セキュリティインシデントへの対応	→	A.5.26	組織の管理策	情報セキュリティインシデントへの対応
A.16.1.6	情報セキュリティインシデントから学ぶ	→	A.5.27	組織の管理策	情報セキュリティインシデントから学ぶ
A.16.1.7	証拠の収集	→	A.5.28	組織の管理策	証拠の収集
事業継続マネジメントにおける情報セキュリティの側面					
A.17.1.1	情報セキュリティ継続の計画	→	A.5.29	組織の管理策	システム中断時の情報セキュリティ
A.17.1.2	情報セキュリティ継続の実施	→	**A.17.1.1、A.17.1.3 と共に A.5.29 に統合**		
A.17.1.3	情報セキュリティ継続の検証、レビュー、評価	→	**A.17.1.1、A.17.1.2 と共に A.5.29 に統合**		
新規			A.5.30	組織の管理策	事業継続に関する ICT の準備状況
A.17.2.1	情報処理施設の可用性	→	A.8.14	技術的	情報処理施設の冗長性

コンプライアンス					
A.18.1.1	適用される法律および契約上の要求事項の識別	→	A.5.31	組織の管理策	法的、法定、規制、契約上の要求事項
A.18.1.2	知的財産権	→	A.5.32	組織の管理策	知的財産権
A.18.1.3	記録の保護	→	A.5.33	組織の管理策	記録の保護
A.18.1.4	個人を特定可能な情報のプライバシーと保護	→	A.5.34	組織の管理策	個人を特定可能な情報（PII）のプライバシーと保護
A.18.1.5	暗号制御の規制	→	**A.18.1.1 と共に A.5.31 に統合**		
情報セキュリティのレビュー					
A.18.2.1	情報セキュリティの独立レビュー	→	A.5.35	組織の管理策	情報セキュリティの独立レビュー
A.18.2.2	セキュリティ方針と規格のコンプライアンス	→	A.5.36	組織の管理策	情報セキュリティに関する方針、規定、規格の遵守
A.18.2.3	技術的コンプライアンスレビュー	→	**A.18.2.2 と共に A.5.36 に統合**		

LRQA の ISO 27001:2022 教育研修および審査サービス

教育研修

ISO 27001:2022 に関する知識を深めるために、様々な学習スタイルで提供される各種コースを経験レベルに合わせて設計しています。

ギャップ分析

移行審査の前に、システムの重要な領域、リスクの高い領域、または脆弱な領域の特定に向けて、専門の審査員が支援するサービスです。

移行審査

ISO 27001:2022 の要求事項に沿って情報セキュリティマネジメントシステムを評価します。特に、附属書 A の管理策と、その管理策がマネジメントシステムに与える影響に重点を置きます。

統合審査

複数のマネジメントシステムを導入している場合、より効率的でコスト効率に優れた、統合審査 / 定期審査プログラムを活用できます。

サイバーセキュリティのあらゆる側面を、クライアントと一緒に取り組む

保証に関する LRQA の深い経験と、受賞歴のあるサイバーセキュリティサービス、脅威主導のインテリジェンスを組み合わせることで、クライアントのビジネスが直面する独自の脅威に対する洞察と防御を提供することができます。今日、明日、また将来のサイバーリスクに先手を打つことが可能になります。

LRQA は世界の主要な国際的規格・スキームに準拠した審査、教育研修、認証サービスを展開するとともに、LRQA のスペシャリストである Nettitude を通じて、幅広い高度なサイバーセキュリティサービスを提供しています。

クライアントのビジネスと協力して、直面している具体的な脅威を特定し、それらを軽減する戦略を構築する支援をします。LRQA がクライアントと協力してシステムを認証し、脆弱性を特定し、ブランド・インテグリティ（整合性）、財務、業務に影響を与えうる攻撃やインシデントの防止を支援します。

情報セキュリティ

LRQA の認証サービスが、ビジネスに不可欠な情報の保護と、国際的に認められたベストプラクティスの実証を支援します。

詳細情報 >

オペレーショナル・レジリエンス

認定、教育研修、ガバナンス、リスク、コンプライアンスのサービスにより、混乱の予防、対応、復旧のために備えます。

詳細情報 >

サイバー脅威からの保護

あらゆる種類のサイバー攻撃に対して第一線の防御と対応を提供するカスタマイズされたソリューションにより、サイバー脅威に先手を打つことができます。

詳細情報 >

YOUR FUTURE. OUR FOCUS.

LRQA について

認証・サイバーセキュリティ・検査・教育研修分野の比類なき専門知識を結集することにより、当社は世界的な認証のリーディングプロバイダーの地位を確保しています。

その伝統は誇るべきものですが、顧客との今後のパートナー関係を構築する上で、本当に重要なのは現在の当社の姿です。揺るぎない価値・リスク管理、軽減における数十年の経験・未来への的確なフォーカスを組み合わせることで、より安心・安全・持続可能なビジネス構築に向けてお客様をいつでも支援します。

独立した審査・認証・教育研修から、リアルタイムの認証技術・データによるサプライチェーン改革まで、当社の革新的なエンドツーエンドのソリューションが、変化の速いリスク環境に積極的に対処できるようお客様をサポートします。つまり、未来の状況を成り行きに任せるのではなく、お客様が自ら構築できるようになるのです。

お問い合わせ

詳細については、https://www.lrqa.com/ja-jp/ をご覧ください。

LRQA リミテッド
〒 220-6010
横浜市西区みなとみらい 2-3-1
クイーンズタワー A10 階