情報セキュリティ：ISO 27001 改訂版

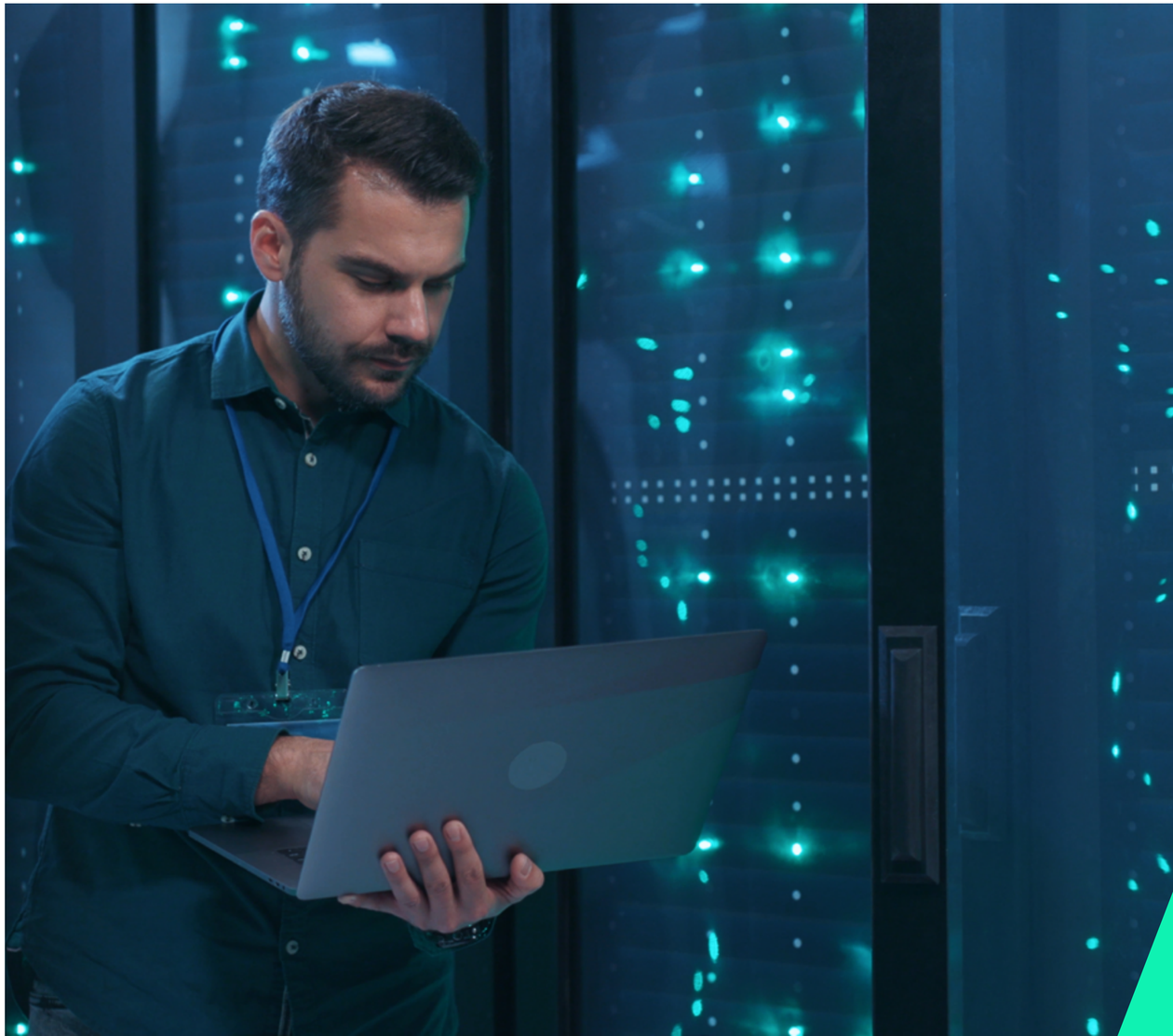
ISO 27001:2022 への移行を成功させるためのガイドライン

序文

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、改訂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。

本資料では、ISO 27001 の認証組織が新規格への移行を成功させるために実施できる 10 の重要なステップについて概説します。



ISO 27001:2022 への移行を成功させるための 10 のステップ

1
変更点を理解する

2
教育研修の必要性を評価する

3
既存の管理策についてギャップ分析を実施する

4
リスク評価を再確認する

5
リスク対応計画（RTP）を改訂する

6
適用宣言書（SoA）を改訂する

7
移行審査の時期を検討する

8
審査を完了し、変更を実施する

9
ISO 27001:2022 認証取得を進める

10
継続的改善に注力する

1. 変更点を理解する

ISO 27001:2022 の附属書 A に新しいセキュリティ管理策の機能が追加されたため、ISO 27002:2022 の理解を深める必要があります。これは、新たな規格の最も重要な改訂部分になります。

ISO 27002:2022 は再構成され、114 ではなく 93 の管理策を備え、以下の 4 つの異なるテーマに分割されています。

- 組織
- 人材
- 物理的
- 技術的

ISO 27002:2022 では、旧バージョンの 53 の管理策が 24 に統合され、11 の新たな管理策が追加されました。また、大半の管理策は、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ことにも留意する必要があります。

2. 教育研修の必要性を評価する

チームメンバーが規格に関する知識を習得し、変更を効果的に実施できるようにするための教育研修プログラムを作成します。

LRQA の ISO 27001 教育研修コースは、近日中に更新され、すべての経験レベルに対応したコースが提供される予定です。

- ISO 27001:2022 規格紹介コース
- ISO 27001:2022 規格導入コース
- ISO 27001:2022 内部監査員コース
- ISO 27001:2022 審査員コンバージョンコース
- ISO 27001:2022 主任審査員コンバージョンコース
- ISO 27001:2022: マネジメントブリーフィング

クライアントとチームメンバーにとって最適な方法に応じて、オンサイト、リモート、または組み合わせた方法で提供することが可能です。

3. 既存の管理策についてギャップ分析を実施する

ISO 27002:2022 に含まれる管理策およびリスク処理を評価するギャップ分析により、ISO 27001:2022 への移行前に対処する必要のある重点分野を特定することができます。

ISO 27002:2022 の附属書 B は、全ての利用可能な管理策の有用な相互比較と、それらが以前のバージョン（ISO 27002:2013）の管理策にどのように対応しているかを収録しているので、手始めに参照することが推奨されます。改訂された規格は管理策を 4 つの主要なテーマ（組織面、人、物理的、技術的）に分類しています。これらの領域に責任を持ち、洞察を提供できる専門家チームを設置することをお勧めします。

LRQA は、専門家の審査員がギャップ分析または事前審査の形で実施するオプションの審査前サービスを提供しています。既存の管理策とより広範な情報セキュリティマネジメントシステム（ISMS）を検討し、注意が必要な領域を識別します。

4. リスク評価を再確認する

リスク評価は、その目的や状況とともに、事業内容やリスクに対する考え方と整合していることを確認し、必要に応じて更新します。情報セキュリティのリスク評価を実施する手順を概説した国際規格である ISO 27005 を参照することもお勧めします。

5. リスク対応計画（RTP）を改訂する

脅威への対応に関する決定を反映するために RTP を改訂し、ISO 27001:2022 の附属書 A に含まれる ISO 27002 の改訂バージョンから適切な管理策を選択する必要があります。

選択した管理策の妥当性と有効性を確認するために、この時点で LRQA にさらなるギャップ分析の実施を依頼することをお勧めします。LRQA の独立した洞察がクライアントの組織の準備状況に確かな自信を与え、LRQA のサイバーセキュリティ専門家である Nettitude が技術的管理策とサービスに関するアドバイスとガイダンスを提供します。

6. 適用宣言書（SoA）を改訂する

管理策や方針の包含や除外に関する証拠と正当性の根拠を反映するために、適用宣言書を改訂することは非常に重要です。また、自社のビジネスが RTP に準拠した管理策を実施しているかどうかを明確化する必要があります。もしそうであれば、自身の活動の有効性を評価するために、堅牢な内部審査プログラムを実施しなければなりません。

7. 移行審査の時期を検討する

この時点までに、実施した変更によって、マネジメントシステム、情報セキュリティ、より広範なサイバーレジリエンスが強化されます。移行審査は、単独で実施することも、他の定期的な訪問審査と並行して実施することも可能です。まずは LRQA までご連絡ください。

既存の ISO 27001:2013 認証を取得している組織は、2025 年 10 月までに ISO 27001:2022 に移行する必要があります。

お気軽にお問い合わせ下さい →

8. 審査を完了し、変更を実施する

審査員は、ISO 27001:2022 の要求事項を満たしているかどうかを判断するために、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 の管理策への変更に焦点を当てます。審査が終了すると、審査報告書が送付されます。審査報告書には、審査員からのフィードバックと、認証を受ける前に対処する必要がある発見事項が記載されています。

9. ISO 27001:2022 認証取得を進める

認証は、国際的に認められたベストプラクティスと継続的改善への取り組みを示すものであり、新しいビジネスの獲得と顧客ニーズへの対応に役立ちます。変化する脅威の状況を反映した管理策とリスク対応を活用することで、情報セキュリティマネジメントシステムが堅牢かつ効果的であることを確信いただけます。

10. 継続的改善に注力する

認証取得後も、情報セキュリティマネジメントシステムを効果的に維持するために、その活動を継続することが重要です。LRQA は、毎年定期審査を実施し、クライアントのシステムの状態に焦点を当て、継続的な改善が行われていることを確認します。

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