情報セキュリティマネジメントシステム

ISO 27001:2022
概要ガイド

LRQA

目次

ISO 27001 とは何か

ISO/IEC 27001 は、情報セキュリティマネジメントシステム（ISMS）の構築、導入、維持、継続的改善のための要求事項を定めた国際規格です。

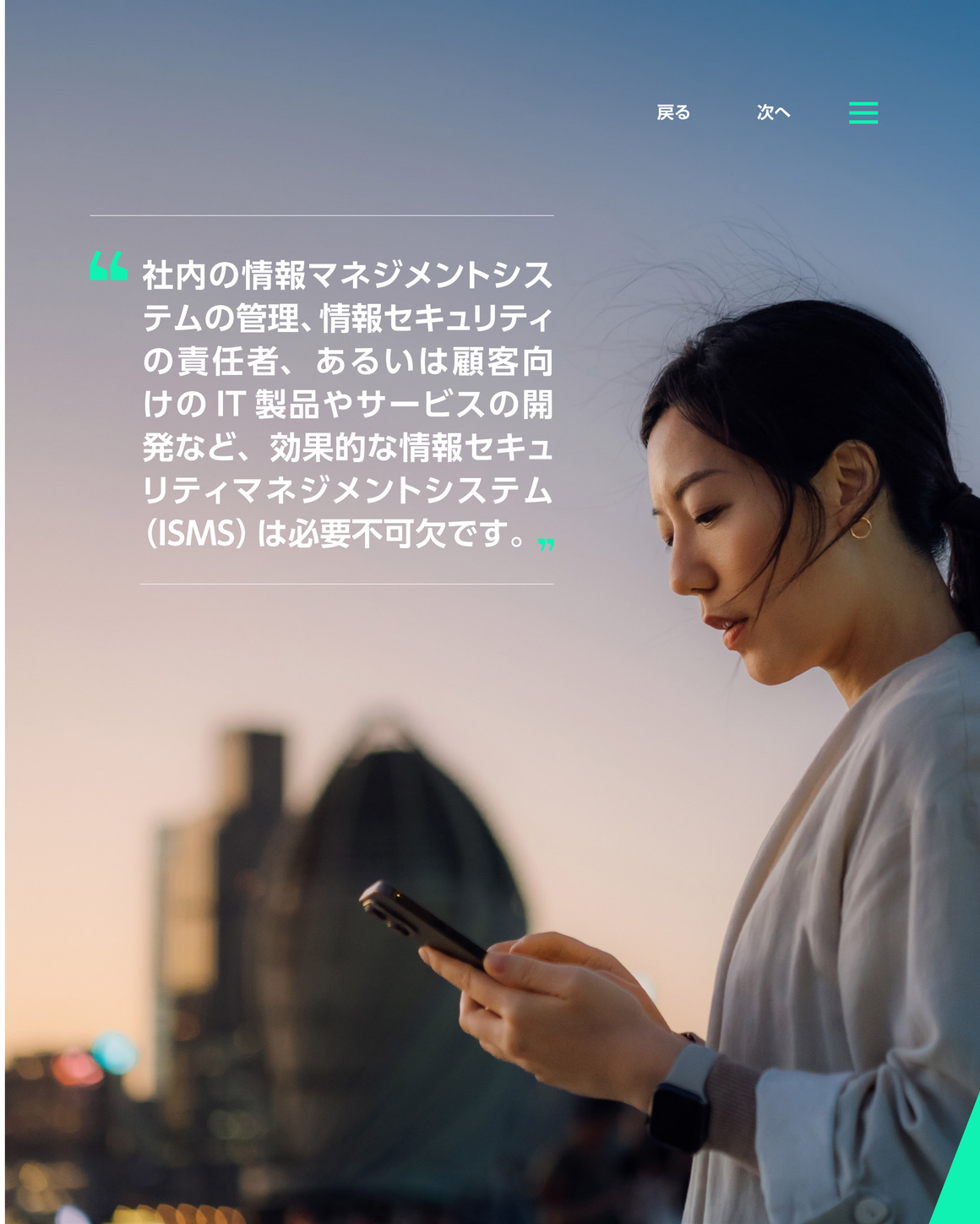
規模やセクターを問わず、どのような組織に対しても、ISO 27001 は包括的な情報とサイバーセキュリティ戦略のための強力な基盤を提供します。この規格では、特定、分析、実行可能な管理策を通じてリスクを軽減し、ビジネス上重要なデータを保護するベストプラクティスとしての ISMS フレームワークを示しています。

社内の情報マネジメントシステムの管理、情報セキュリティの責任者、あるいは顧客向けの IT 製品やサービスの開発など、効果的な情報セキュリティマネジメントシステム（ISMS）は必要不可欠です。ISO 27001 の認証は、ますます複雑化する脅威から組織の情報、そして顧客の情報を守るためのプロセスと管理体制が整っていることを証明するものです。

秘密情報（知的財産や価格情報など）を保護する通常の商業上の必要性に加え、最近では規制やコーポレートガバナンスの分野で、情報の完全性に対してこれまで以上に厳しい要求事項が課されるようになっています。

LRQA によって認証された ISO 27001 情報セキュリティマネジメントシステム（ISMS）は、情報セキュリティマネジメントシステムの適切性と有効性について、独立した公平な見解を提供します。

“社内の情報マネジメントシステムの管理、情報セキュリティの責任者、あるいは顧客向けの IT 製品やサービスの開発など、効果的な情報セキュリティマネジメントシステム（ISMS）は必要不可欠です。”



ISO 27001:2022 の紹介

ISO 27001 が改訂された理由

2022 年 2 月、ISO 27002:2022（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示す規格）が改訂されました。

同時に、2 つの規格を整合させるために ISO 27001 の新しい改訂版が必要になりました。その結果を受けて、ISO 27001:2022 は 2022 年 10 月 25 日に発行されました。既存の ISO 27001 認証取得組織は新しい改訂版に移行するために 3 年間の猶予が与えられます。

変更の内容

ISO 27001 の新しい改訂版は、ISO 27002:2022 によって概説された管理策を特徴としており、これは附属書 A に記載されています。これは ISO 27001:2022 の最も大きな変更点であり、組織はリスクアセスメントを再検討し、更新または新しいリスク処理を実施する必要があるかどうかを判断する必要があります。

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 56 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。規格の 2013 年版と 2022 年版の箇条 0 ～ 10 と比較しても、表面的にはほとんど変化がありません。しかしながら、構造、用語、語順に変更があり、解釈の仕方に影響を与える可能性があります。

管理策は
114 から
93 に

全部で
11 の
新しい管理策

ISO 27001:2013 の
56 の管理策は現在、
ISO 27001:2022 で 24 の
管理策に統合されています

ほとんどの
管理策は、何らかの形でテキストが変更されており、これは規格の解釈と実施方法に影響を与える可能性があります

管理策が 4 つの「新しい」テーマに分割

組織	人	物理的	技術的
- 28 統合	- 2 統合	- 5 統合	- 21 統合
- 3 新規	- 0 新規	- 1 新規	- 7 新規

ISO 27001:2022 の紹介

ISO 27001:2013 で認証された ISMS を持つ組織にはどのような影響がありますか？

既存の認証を受けている組織は、ISO 27001:2022 の発行から 3 年以内に移行を完了する必要があります。つまり、2025 年 10 月 31 日まで移行が可能です。

LRQA の既存のクライアントの皆様には、専門家である審査員が ISO 27001:2022 の要求事項に照らしてシステムをレビューする、専用の移行審査をお申し込みいただけます。

組織はいつ ISO 27001:2022 の認証を受けることができますか？

既存の認証を保持していない場合、ISO 27001:2013 の要求事項に沿って ISMS を導入し、認証を受けることができます。その後、2025 年 10 月 31 日の期限までに移行する必要があります。

ISO 27001:2022 に対する初回認証を求めているクライアントの場合、情報セキュリティ専門家がオンラインまたはオンサイトにて、様々な教育研修および認証サービスを提供しています。LRQA がクライアントと密接に連携し、ビジネス固有の要求事項に合ったプログラムを構築して、認証取得までのあらゆる段階でサポートします。

ISO 27001 の実装

ISO 27001 は、PDCA サイクルとマネジメントシステムのプロセスを用いて、ベストプラクティスと基本原則を実施するための ISMS のフレームワークを提供します。

認識：関係者は、情報システムとネットワークのセキュリティの必要性を認識する必要があります。

責任：全ての関係者は、情報システムとネットワークのセキュリティに関して責任を負います。

対応：関係者は、セキュリティインシデントを防止、検出、対応するために、タイムリーかつ協力的に行動する必要があります。

リスク審査：関係者はリスク審査を行う必要があります。

セキュリティの設計と導入：関係者は、情報システムとネットワークの不可欠な要素としてセキュリティを組み込む必要があります。

セキュリティマネジメント：関係者は、セキュリティマネジメントに対する包括的アプローチを採用する必要があります。

再審査：関係者は、情報システムとネットワークのセキュリティを見直し、再評価する必要があります。

OECD（経済協力開発機構）デジタルセキュリティリスクマネジメントガイドラインより作成

はじめに

組織の現状を問わず、情報セキュリティマネジメントシステム導入の出発点は、マネジメントのコミットメントと支持を得ることです。

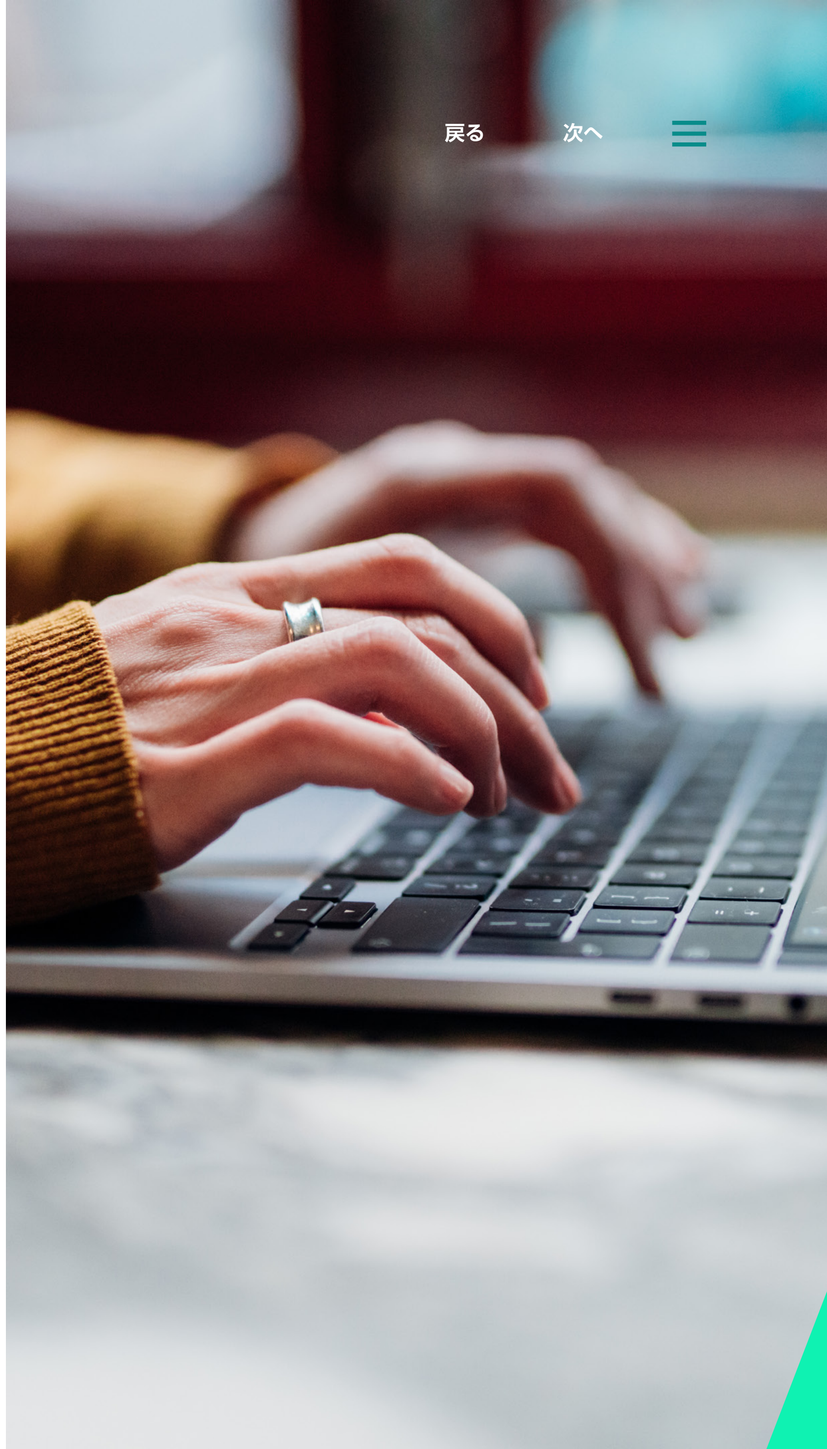
トップマネジメントがモチベーションと方向性を示す必要があります。トップマネジメントは、ISMS の方向性と組織の戦略との互換性を確保し、方針や目的などの重要な側面に責任を持つことに積極的に関与しなければなりません。

成功のための計画

他のプロジェクトと同様に、有意義で現実的な計画を立て、その計画に対するパフォーマンスを測定し、不測の事態が発生した場合に計画を変更する準備ができていれば、成功する可能性は高くなります。

計画では、マネジメントシステムの開発には時間、労力、十分なリソースが必要であることを認識する必要があります。情報セキュリティの全体的な責任はトップマネジメントや、（多くの場合は）IT 部門にあります。とはいえ、情報セキュリティは、人事、セキュリティ、物理的セキュリティ、法令遵守など、IT システムのみにとどまらない広範な影響力を持っています。

ISO 27001 は ISO 9001:2015 と整合性があるため、すでに認証を受けた品質マネジメントシステムを備えている場合は、ISMS の強力な基盤となります。情報セキュリティの問題について他の担当者や講師と話し合うことができる、LRQA 教育研修コースへの参加を強くお勧めします。



ISO 27001 の実装

規格の理解

この規格をよくご理解いただくことが重要であり、これには満たすべき基準の理解も含まれます。このことは、ISMS と関連文書の全体的な構成に影響します。

規格は 2 つの部分に分かれています。

- ISO 27002 は、情報セキュリティに対する特定のリスクを管理するために選択され、実施される可能性のあるセキュリティ管理策について説明する参考文書です。

- ISO 27001 は、ISMS を導入する上で対処する必要がある要求事項を定義する、マネジメントシステムの仕様です。認証機関は、認証審査中に ISO 27001 に沿ってマネジメントシステムを審査します。

この仕様書には、すべてのマネジメントシステムに共通する要素である、方針、リーダーシップ、計画、運用、マネジメントレビュー、および改善が含まれています。また、情報に対するリスクを特定し、適切な管理策とチェックを選択することを特に目的とした箇条も含まれています（附属書 A）。

マネジメントプロセス

ISMS を効果的に実施するためには、マネジメントプロセスが重要です。既に ISO 9001:2015 のマネジメントシステムを運用している組織であれば、その内容は周知の事実と思われます。この場合、最も効率的な方法は、情報セキュリティの要求事項を既存のマネジメントシステムに統合することです。これらのプロセスを初めて実施する場合は、これらの要求事項の全体的な意図を考慮する必要があります。

マネジメントシステムの有効性については、最終的にトップマネジメントが責任を負います。その賛同を得ることが極めて重要であり、ISMS の開発、実施、監視に十分なリソースを配分する必要があります。

- 内部審査は改善の機会を特定し、マネジメントシステムが意図したとおりに運用されているかどうかを検証します。

- トップマネジメントはマネジメントレビューにより、マネジメントシステムがどの程度適切に運用され事業を支えているかを評価し、理解することができます。

適用範囲を定義する

ISMS の論理的・地理的範囲を正確に定義し、ISMS とセキュリティ責任の境界を確認できるようにすることが重要です。適用範囲は、ISMS の対象となる従業員、場所、情報を特定する必要があります。

適用範囲を定義して文書化すると、適用対象となる情報資産を、その価値や所有者と併せて特定することができます。

ISMS 方針

ISMS 方針に関連する要求事項は、ISO 27001:2022（A.5.1）と ISO 27002 の両方で扱われています。ISO 27001 の他の要求事項と附属書 A にこの方針への言及があり、方針に何を含めるべきかを示しています。例えば、ISMS の目標は ISMS 方針と一致していなければなりません。特定の管理目標を達成するために、他の方針が必要となります。

ISO 27001 の実装

リスク審査とリスクマネジメント

リスク審査は、ISMS を構築するための基礎となるものです。セキュリティ管理の実施に焦点を当て、セキュリティ管理が最も必要とされる場所に適用され、費用対効果が高いこと、（また同様に重要なこととして）影響が最も少ない場所には適用されないことを確保します。リスク審査は、「どの程度のセキュリティが必要なのか」という問いへの答えを促してくれます。

リスクマネジメントの重要な考慮事項の 1 つは、リスクを肯定的および否定的に考慮する必要があるということです。リスクとは不確実性が目的に及ぼす影響のことであるため、リスクマネジメントにおいては、これを活用する機会も考慮することが欠かせません。

リスク審査には情報資産の所有者全員が関与します。それがなければ、効果的なリスク審査を行うことはできません。

最初のステップは、リスク審査方法を決定し、文書化することです。CRAMM（CCTA Risk Analysis and Management Method）など、通常はコンピュータベースによる独自の手法が利用できます。

さらに、リスクマネジメントの国際規格である ISO 31000 は、情報システムの複雑さに対処する、より組織固有な方法を開発するために活用できます。

リスク審査プロセスには、情報資産の特定と評価が含まれる場合があります。この評価は金銭的なものだけではなく、風評被害や規制遵守の違反など、他の要因も考慮します。そこには、貴社の状況が重要な影響を与えます。

ISO 27005:2022 は現在、資産ベースに代わる事象ベースのリスク審査オプションも提供しています。このアプローチは、事象と結果の評価を通じてリスクを特定・評価できるという基本的概念を強調するものです。

資産ベースのプロセスでは、資産とその活用に関連する脅威、脆弱性、機会を検討します。最後に、リスクのレベルを決定し、それらのリスクを管理するために実施する管理策を特定する必要があります。

脅威と脆弱性、これらの影響の特定には、セキュリティ環境を考慮する必要があります。例えば、石油化学工場に隣接する工業団地に拠点を置く組織の場合、敷地への物理的なアクセスを拒否される脅威は、都会の小さなオフィス街にある事務所よりも大きいと言えます。

リスク対応

リスク審査では、リスクレベルを特定してから、組織のセキュリティ方針によって決定されたリスクの許容レベルと比較します。許容レベルを超えるリスクを管理するために、以下のような適切な措置を取ります。

- リスクを許容可能なレベルまで低減するため、附属書 A や、セクター固有または国内のベストプラクティスに関連するその他の情報源から選択したセキュリティ管理を実施します。リスクレベルを再計算して、残存リスクが許容レベルを下回っているよう確認しなければなりません。選択された管理策は適用宣言書に記録され、これを附属書 A と比較し、各管理策、ステータス、リスク審査へのトレーサビリティを含めるか除外するかの正当な根拠を含める必要があります。
- 管理者の方針とリスクの許容基準に沿ったリスクの受入れ。措置を講じた後に、残存リスクが許容レベルを超えている場合もあります。その場合、残存リスクもリスク許容プロセスの対象としなければなりません。管理者によるリスク受入れの記録を維持する必要があります。
- セキュリティ環境の変更によるリスクの除去。例えば、データ処理アプリケーションで脆弱性が特定された際の安全なアプリケーションのインストールや、浸水のリスクがある場合の物理的資産の高層階への移動が当てはまります。ここでも、リスク除去活動の後に残存リスクを再計算する必要があります。
- 適切な保険への加入や、物理的資産や業務プロセスの管理を外部委託等をすることでリスクを移転します。リスクを受け入れる組織は、その義務を認識し、義務の引受けに同意しなければなりません。外部委託組織との契約では、適切なセキュリティ要求事項に対処する必要があります。

リスク対応計画では、実行された措置と計画された措置に加え、未実施の措置を完了するための期間を特定することによってリスクを管理します。計画では措置の優先順位を定め、責任と詳細な行動計画を含めなければなりません。

ISO 27001 教育研修および審査サービス

教育研修

様々な経験レベル向けに設計された各種のコースが複数の学習スタイルで提供され、ISO 27001 の知識を構築することができます。

ギャップ分析

移行審査の前に、LRQA の専門審査員の 1 人が、システムの重要 / 高リスク / 脆弱な領域の特定を支援するオプションサービス。

認証・移行審査

ISO 27001:2022 の要求事項に沿って ISMS を評価します。特に、附属書 A の管理策とそれがシステムに与える影響に焦点を当てます。

統合された審査

複数のマネジメントシステムを導入している場合、より効率的で費用対効果の高い、統合された審査・定期審査プログラムを活用することができます。

コースを表示 →

LRQA を選ぶ理由

ローカル & グローバル

クライアントがどこにいても、LRQAがサポートします。世界中に 300 人以上の有能な審査員と 250 人以上の専任のサイバーセキュリティ専門家を擁する LRQA は、グローバルに一貫して卓越性を追求するとともに、ローカルにサービスを提供できます。LRQA の社員は、情報およびサイバーセキュリティのリスク、課題、規格、規制、フレームワークに関する詳細な知識を持つ技術の専門家です。

柔軟な提供

ほとんどの場合、ISO 27001 教育研修および認証サービスは、安全で安心な技術を使用してオンサイトまたはリモートで提供できます。LRQA のリモートサービスを選択すると、オンサイトと同じ高品質のサービスに加えて、柔軟性、迅速な配信、グローバルな専門知識へのアクセスなど複数のメリットを享受できます。

世界初の UKAS 認定機関

LRQA は世界初の UKAS の認定を受け、世界中の様々な規格の認証サービスを提供しています。LRQA は様々なセクターにわたり、各種の具体的な規格やフレームワークの開発に貢献し続けています。

コンプライアンスのその先へ

表彰歴のあるサイバーセキュリティ事業 Nettitude と共に、あらゆる脅威や脆弱性に対して第一線で防御・対応を提供する先進的なサービスにより、高度なサイバー脅威の一歩先を行く支援をします。

NETTITUDE
AN LRQA COMPANY

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、さらに将来のサイバーリスクに先手を打つことができます。

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。

ISO 27001、ISO 27701、
ISO 27017、ISO 27018、
CSA STAR

詳細情報 ›

オペレーショナル・レジリエンス

認証、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。

ISO 22301、ISO 20000-1、
Cyber Essentials 認証

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。

セキュリティ保証テスト、
マネージドセキュリティサービス、
脅威インテリジェンス、
インシデント対応

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