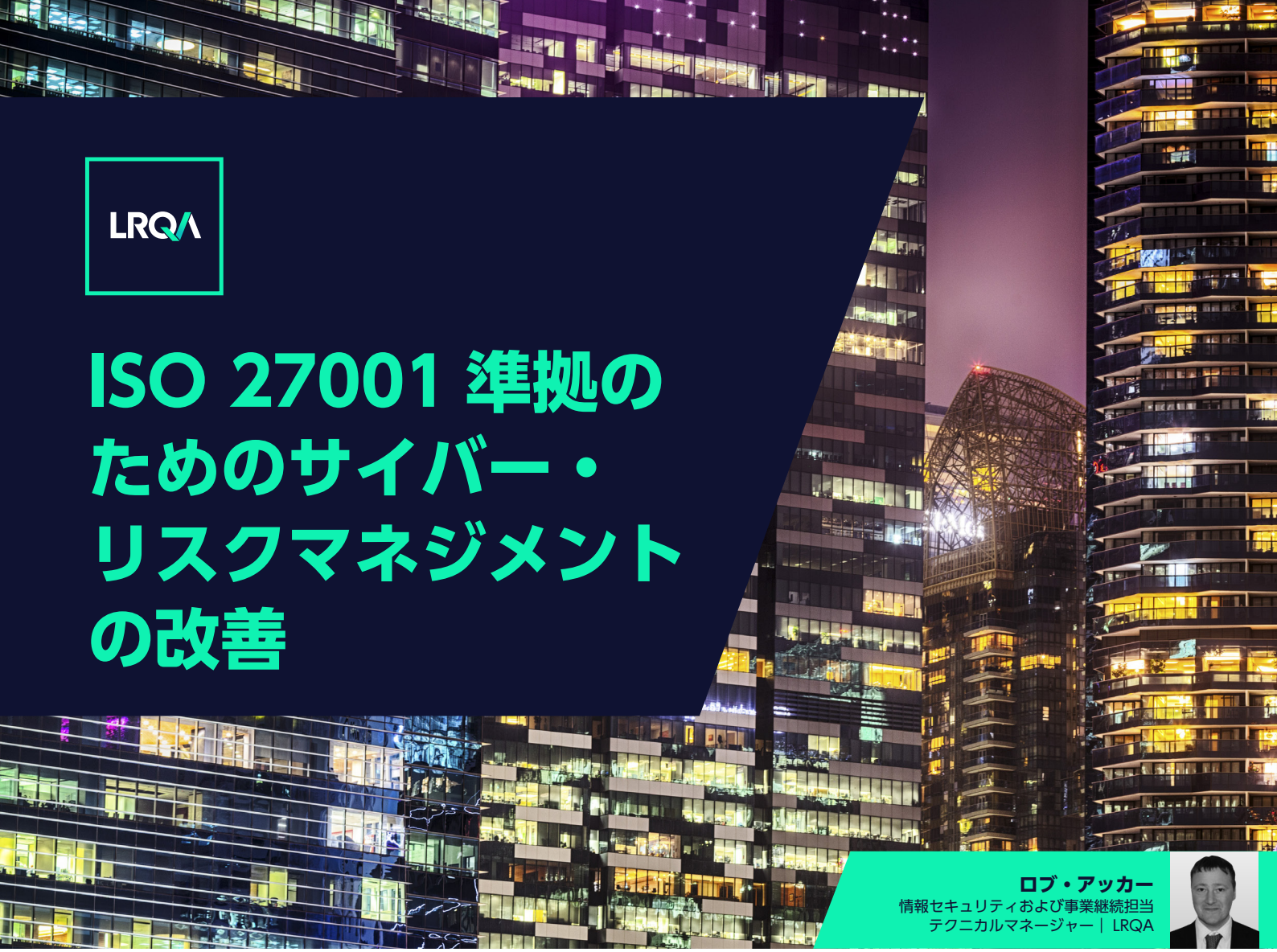


ISO 27001 準拠のためのサイバー・リスクマネジメントの改善

ロブ・アッカー
情報セキュリティおよび事業継続担当
テクニカルマネージャー | LRQA

> サイバー攻撃とデータ漏洩は、企業が高リスクとする上位 5 項目に入り、潜在的な影響という観点でも上位 10 位に入ります。
>
> **ロブ・アッカー**

今日のハイパーコネクテッド（様々なプラットフォームを介した、人々やモノの相互のつながり）な世界では、組織はこれまで以上に高度で破壊的かつ大規模な情報セキュリティの脅威やサイバー攻撃にさらされています。効果的な情報セキュリティ戦略を整備することは、かつてないほどに重要になってきています。

本資料では、LRQA の情報セキュリティおよび事業継続担当テクニカルマネージャーのロブ・アッカーが、情報セキュリティマネジメントシステム（ISMS）がどのようにお役に立つのかに関して説明します。

世界経済フォーラム [1] が作成したグローバルリスク報告書 2018 年版によれば、サイバー攻撃とデータ漏洩は、企業が高リスクとする上位 5 項目に入り、潜在的な影響という観点でも上位 10 位に入ります。

また、サイバー攻撃に対する財務コストも増大しており、サイバー攻撃への対応にかかる年間コストは現在 1,170 万ドルで、前年比で 27.4% 増加しています [2]。

1 世界経済フォーラム、グローバルリスク報告書 2018 年版 http://reports.weforum.org/global-risks-2018/

2 アクセンチュア、2017 年版サイバー犯罪コスト調査 https://www.accenture.com/ t 20170926 T 072837 Z__w __/ us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf

サイバーセキュリティ対策の 10 ステップ

英国政府の情報保証部門である国家サイバーセキュリティセンター（NCSC）は、「サイバーセキュリティ対策の 10 ステップ[3]」をリリースしました。

この指針は、サイバーセキュリティを改善し、最終的には組織内の情報資産を保護する方法についてビジネスリーダーに助言することを目的としています。これらは、組織の規模、場所、セクターに関係なく適用することが可能です。指針の中核となるメッセージとして記載されているのは、企業が効果的な情報リスクマネジメント体制や文化を確立する必要性です。

[3] 出所：NCSC、サイバーセキュリティ対策の 10 ステップ https://www.ncsc.gov.uk/guidance/10-steps-cyber-security

リスクマネジメント体制の構築

法的リスク、規制リスク、財務リスク、運用リスクと同様に、組織の情報とシステムに対するリスクを評価します。これを実装・実施するため、理事会やシニア・マネージャーの支援のもと、組織全体にリスクマネジメント体制を組み込みます。

マルウェア防御

組織全体で関連する規定を策定し、マルウェア対策を確立します。

ネットワークセキュリティ

ネットワークを攻撃から保護します。ネットワークの境界を防御し、不正アクセスや悪意のある内容を排除し、セキュリティ制御のモニターおよび試験を実施します。

ユーザーの教育および意識向上

システムを安全かつ許容範囲内で使用するためのユーザー向けのセキュリティ規定を作成します。これは、サイバーリスクに関する意識向上の維持に役立つ、スタッフの教育・トレーニングも含みます。

安全なコンフィギュレーション

セキュリティパッチを適用し、すべてのシステムの安全なコンフィギュレーションの維持を確保します。システム一覧表を作成し、すべてのデバイスで構築されたベースラインを定義します。

インシデント管理

インシデント対応と災害復旧対応力を確立し、インシデント管理計画を試験します。また、専門的なトレーニングの提供や、不正事象の規制当局への通報も行います。

在宅およびリモートワーキング

リモートワーキング指針を策定し、その遵守に向けてスタッフを教育します。安全なベースラインおよび実装をすべてのデバイスに適用します。転送中および保存中のデータを保護します。

ユーザー権限の管理

効果的なマネジメントプロセスを確立し、特権アカウントの数を制限します。ユーザー権限を制限し、ユーザーの活動を監視し、活動および監査ログへのアクセスを制御します。

リムーバブルメディアの管理

フラッシュメモリーなどのリムーバブルメディアへのすべてのアクセスに対して、管理する指針を作成します。メディアの種類と使用を制限し、企業システムに導入する前に、すべてのメディアでマルウェアをスキャンします。

モニタリング

モニタリング戦略を確立し、支援方針を作成します。すべてのシステムおよびネットワークを継続的に監視します。攻撃と考えられる異常なアクティビティのログを分析します。

リスク選好度の決定 → **サイバーリスクを理事会の優先事項とする** → **支えとなるリスクマネジメント方針の作成**

出所：NCSC、サイバーセキュリティ対策の 10 ステップ https://www.ncsc.gov.uk/guidance/10-steps-cyber-security

ISO 27001 と「サイバーセキュリティ対策の 10 ステップ」の関係

ISO 27001 などの ISMS は、個人データや顧客データ、財務情報など、お客様にとって価値ある資産を識別し、それらを保護することを意図しています。

NCSC が特定した対策と手順は、情報セキュリティマネジメントシステム（ISMS）の対応策と密接に関連しています。ISO 27001 の認証を受けている ISMS は、個人データや顧客データ、財務情報など、お客様にとって価値ある資産を識別し、それらを保護することを意図しています。

NCSC の「サイバーセキュリティ対策の 10 ステップ」で特定された対策と ISO 27001 ISMS 規格との間には密接な整合性が存在します。「サイバーセキュリティ対策の 10 ステップ」は、実践的なアドバイスを提供し、ISMS の確立を目指す企業にとって有用な第一歩となります。そして、トップマネジメントは、管理措置の選択や設計をより選択的に行うために ISO 27001 を使用することが可能です。

当社は、ISO 27001 で強調されている要求事項のいくつかを、「サイバーセキュリティ対策の 10 ステップ」にマッピングする作業を実施しました。これらは 2 ページの表に示されています。

ISO 27001：リスクマネジメントへの体系的なアプローチ

重要な情報資産を保護するための体系的なアプローチは、情報リスク対策において強力な武器となります。

データ保護の侵害、データ損失、不正行為はすべて、サービスの中断、コストの増加、評判への影響を引き起こす可能性のある重大な問題です。

リスク評価は、ISMS 構築の基盤です。セキュリティ・コントロールの導入に焦点を当て、セキュリティ・コントロールが最も必要とされる場所に適用され、費用対効果に優れているよう徹底します。

組織は、リスクアセスメント・プロセスの一環として、リスクを管理するために制定するべき統制や対応戦略を決定する前に、情報資産の特定のみならず、その価値も見出します。ISO 27001 の強みの一つは、組織と均整がとれたシステムの確立を支援することです。直接対応できないリスクは、受け入れることが可能です（その後の継続的なレビューと確認により実施）。対応可能なリスクは、既に適切な統制がとれているか、第三者機関のサービスによる恩恵を受けているものです（例：ISO 27001 の認証データセンターにデータを保有している）。

最も重大な侵害は、人、プロセス、およびテクノロジーが結合する複数のタッチポイントが存在する場所で発生することを、これまでの証拠が示しています。しかし、ISO 27001 に準拠した ISMS を構築するには、組織が包括的なアプローチをとることが必要であり、セキュリティ問題が現在受け入れられているベストプラクティスに従って対処されていることを保証する必要があります。

LRQA のような認定された第三者機関により、マネジメントシステムについて ISO 27001 に照らした外部の評価を取得するプロセスは、システムの妥当性と有効性について独立した公平な見解を組織に与えることができます。

私は、ISMS のテクニカルマネージャーとして、顧客から「審査の準備」についての話を頻繁に聞きます。LRQA がシステムを認証する際には、単に認証を与えるだけではなく、認証プログラムの一環として継続的な関係維持へのコミットメントを求めます。当社では、プログラムのサーベイランスの一つとして、平均的に 6 か月ごとにクライアントを訪問しますが、これはクライアントが定期的に外部の精査の対象となることを意味し、効果的な統制を維持するためのコミットメントを示しています。

しかし、効果的な ISMS は、既知の脅威、さらに重要な未知の脅威に対する保護を提供します。組織が脆弱性に目を向け、各自が導入した統制に自信を持てるかを自問することを求めます。

用心に越したことはない

情報セキュリティシステムが適切に管理および維持されていない場合、組織は重大な財務上および評判上の損失を被るリスクを負います。

深刻なデータセキュリティ脅威のリスクを軽減し、システムの脆弱性が悪用されないようにするための適切な統制を組織が有するよう徹底することは、もはや必須事項と言えるかもしれません。こうした状況は、より厳格な要求事項を設定し、データ漏洩が発生した際に組織により厳しい罰金を科す、EU の一般データ保護規則（GDPR）が公表されてから特に顕著になっています。

「サイバーセキュリティ対策の10 ステップ」と ISO 27001 の要求事項との整合

サイバーセキュリティ対策の10 ステップ	ISO 27001統制／条項	主なポイント
1. 在宅およびリモートワーキング	A.6.2	従業員が自宅、クライアントの事務所または移動中に勤務している場合でも、情報のセキュリティを確保することが重要です。
2. ユーザーの教育および意識向上	A7.2.2	すべての従業員と第三者の委託事業者は、主なリスクおよびインシデントの報告方法を認識しておく必要があります。
3. インシデントマネジメント	A.16	情報セキュリティ事象が発生した後に、インシデントを封じ込め、可能な限り迅速に通常業務に復帰できるようにする組織の能力は非常に重要です。ISO 27001 は、EU の一般データ保護規則（GDPR）への準拠を証明するのに役立ちます。
4. 情報リスクマネジメント体制	6.1 & 8.2	マネジメントはあらゆる組織の方向性を定めます。ISO 27001 では、トップマネジメントに明確な方向性と支援を提示するようことを明示的に求めています。
5. ユーザー権限の管理	A.9.2	ユーザーは情報漏洩の原因となる可能性があるため、役割に基づいてのみアクセスを付与することで、エラーを減らし、ユーザーが適切なセキュリティ慣行を確実に実施することの責任を支援します。
6. リムーバブルメディアの管理	A.8.3.1	メモリスティックやその他のポータブルデバイスの可用性が拡大しているため、組織にとって、これらのリムーバブルメディアの使用を管理する手順の整備は不可欠です。
7. モニタリング	A.12.7, A.12.4	予期せぬアクティビティに注意しておくことは、ビジネスとして理にかなっています。ユーザー・アクティビティの監査ログは、漏洩事象が生じた際に貴重な証拠を提供し、その後の調査に役立ちます。
8. 安全なコンフィギュレーション	A.12.1.2, A.14.2.2, A.14.2.3, A.14.2.4 & 8.1	システムを理解し、システムに対する変更を制御することで、システムの整合性を維持し、適切な保護を確実にします。
9. マルウェア保護	A12.2	システムのパッチ管理および最新状態の維持を確実にすることで、悪意のあるコードやモバイルコードが既知の脆弱性を悪用する可能性を低減できます。
	A13.1	ネットワークにアクセスした人物やネットワークが何に使用されているかを把握し、制御することで、個人やデバイスによる不正アクセスの可能性を軽減します。

LRQA の ISO 27001 の審査および教育・トレーニングサービス

LRQA の幅広い審査および教育・トレーニングサービスは、あらゆる規模組織に適しており、規格を最大限に活用できるよう支援します。

教育・トレーニング

LRQA の幅広い教育・トレーニングサービスは、ISO 27001 認証取得までの全過程において、組織を支援します。LRQA は、ひとり一人の学びは異なることを理解しています。そのため、対面や仮想教室の選択肢から e ラーニングに至るまで、さまざまな形式で教育・トレーニングコースを提供しています。

LRQA の ISO 27001 の教育・トレーニングコースには、以下があります。

- ISO 27001:2013 入門
- ISO 27001:2013 導入
- ISO 27001:2013 内部監査員
- 主任審査員コース
- ISO 27001 の基本ガイド

ギャップ分析

審査員が実施するギャップ分析により、認証取得を可能にするシステムの構築に向け、システムの重要な領域やリスクの高い領域、または弱い領域に焦点を合わせる機会がもたらされます。

さらに既存のマネジメントシステムや手順を、選択した規格の中でどのように利用できるかについても考慮されています。

認証手続き中かどうかに関係なく、対象範囲はお客様が定義できます。

認証

通常はシステム評価と初期審査で構成される 2 段階のプロセスです。期間は組織の規模と種類によって異なります。

維持審査（サーベイランス）

ISMS 認証後、システムの継続的な有効性を確認するために定期審査が実施されます。これにより、ISMS が順調に運用され継続的に改善されていることが、お客様とお客様のトップマネジメントに保証されます。

統合マネジメントシステムの評価

ISMS と既存のマネジメントシステム（品質マネジメントシステムなど）との連携を検討している企業は、評価や査察のプログラムを連携して調整することができます。多くの ISO マネジメントシステム規格は共通の内容となっているため、これは審査時間と費用の全体的な削減につながる可能性があります。

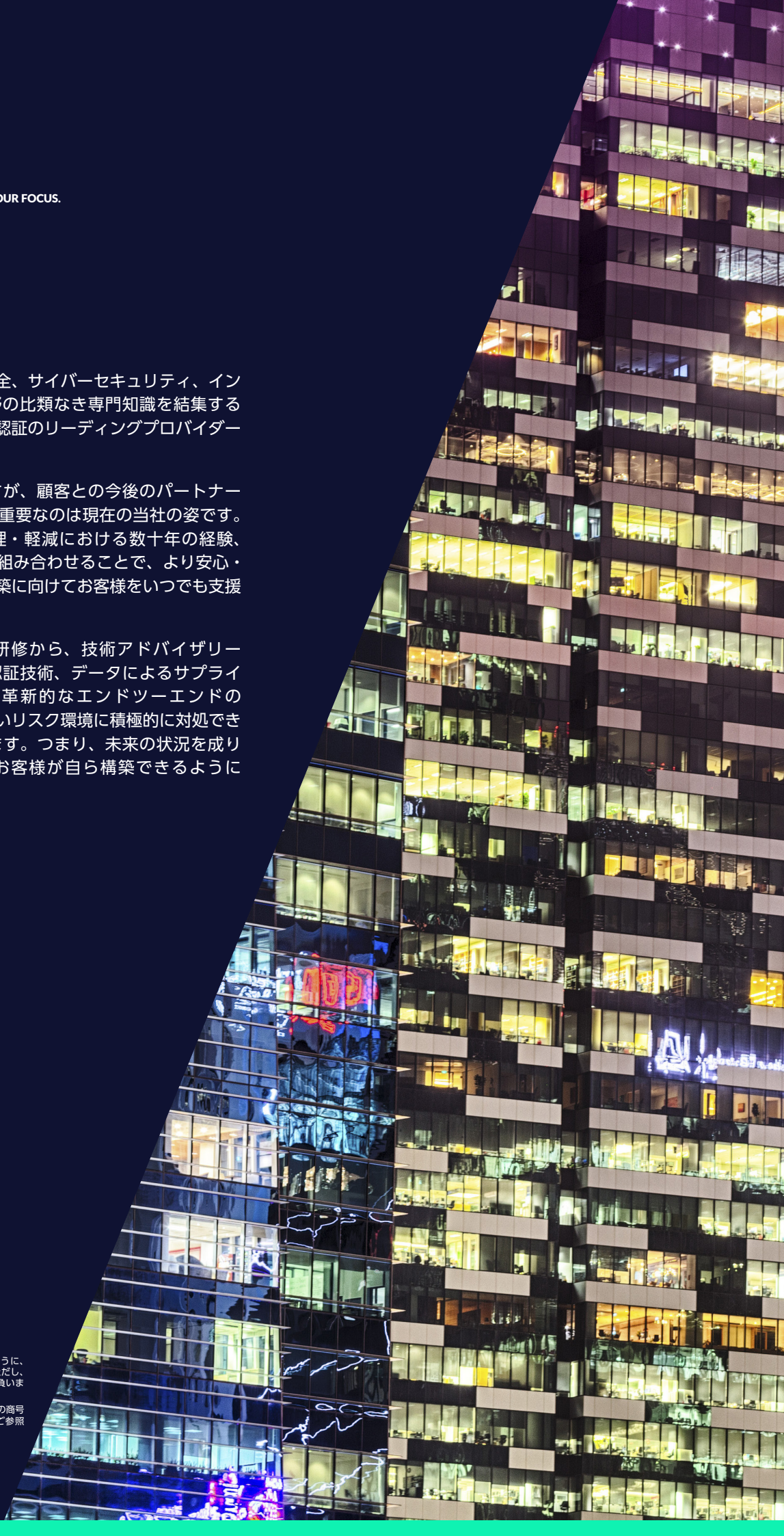
YOUR FUTURE. OUR FOCUS.

LRQA について：

認証、ブランド認証、食品安全、サイバーセキュリティ、インスペクション、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、技術アドバイザリーサービス、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