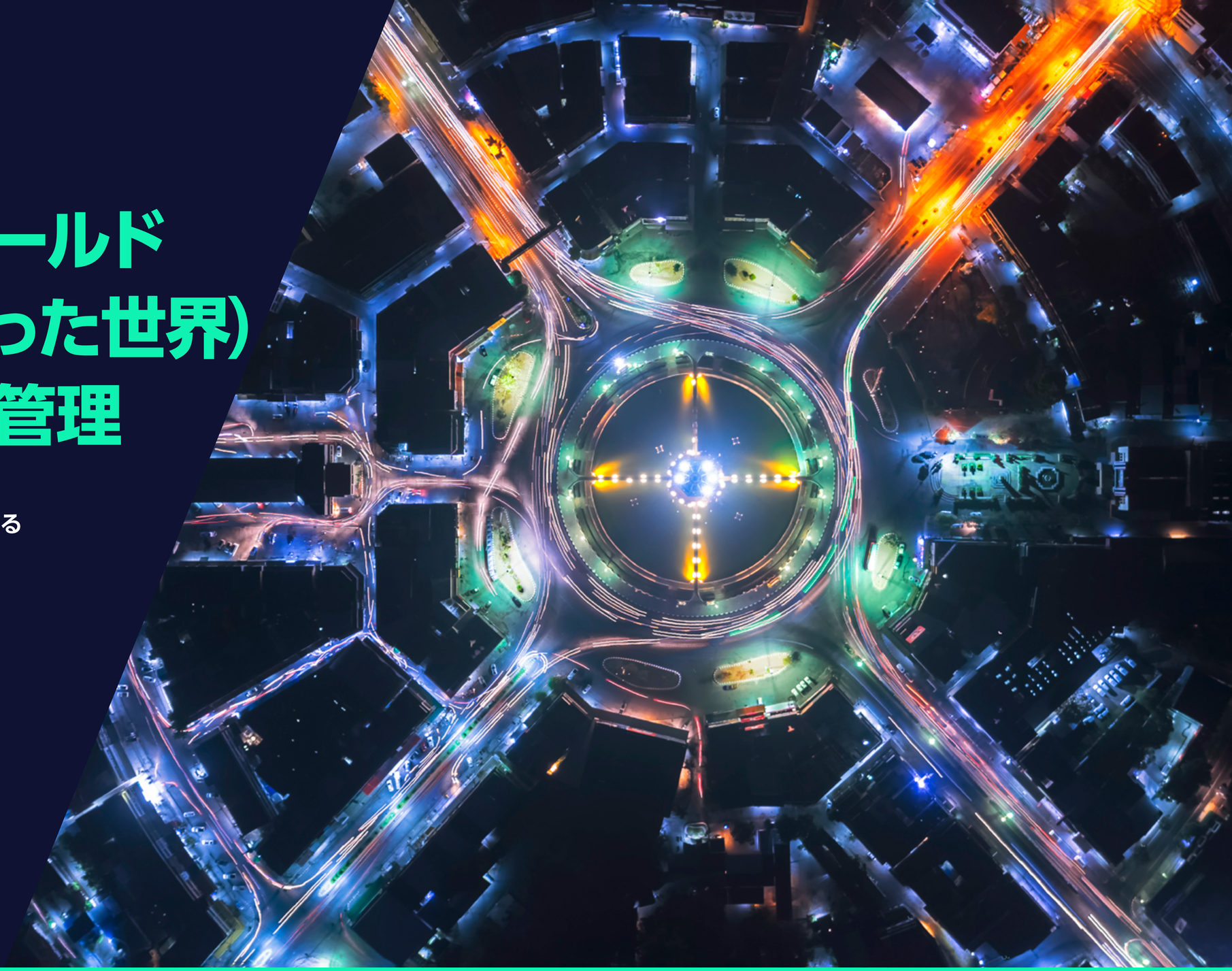
サイバーセキュリティ

コネクテッドワールド（通信でつながった世界）におけるリスク管理

効果的なサイバー保証プログラムを構築する
5 つの方法



序文

ネットワーク化が進む世界では、組織にとって、これまで以上に巧妙で被害の大きいサイバー攻撃から身を守ることがますます難しくなっています。

脅威は進化を続けています。ハッカーは技術を磨き、攻撃手法を調整しています。IoT（モノのインターネット）機器、AI（人工知能）、クラウドコンピューティングなどの革新的技術は、すべての企業にとって高リスクの分野であり、脆弱性をもたらす可能性があります。複雑化するサプライチェーンと変化する規制要件は、組織が対処しなければならない脅威の状況の変化をさらに浮き彫りにしています。

攻撃や情報漏えいの成功が、財務、風評、法律、業務に与える影響はよく知られています。しかし、見出しだけでなく、根本的な原因を探ることで、サイバーリスクマネジメントの真の複雑性に光を当てることができるのです。あらゆる角度からの脅威が存在するため、万能な対策は存在しません。組織は、包括的な対策と広範で堅牢な保証プログラムを実施する前に、独自のリスクプロファイルと脅威の状況をしっかりと理解する必要があります。

ここでは、サイバーセキュリティの第一人者が、あらゆる企業がサイバーセキュリティの確保に向けた実践的なアプローチを確立するための 5 つの重要なステップを解説します。

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

クリス・オークリー
技術サービス担当 ヴァイスプレジデント | Nettitude

アグスティン・レルマ・ガンゴイティ
情報およびサイバーセキュリティ担当 シニア主任審査員 | LRQA

スチュアート・ライト
ガバナンス、リスク、コンプライアンス担当グローバル・ヘッド | Nettitude

1. 顧客固有のリスク属性の理解と対応

成熟したリスクマネジメント慣行を確立しない限り、適切かつ総合的なサイバーセキュリティ戦略と保証プログラムを実施することは不可能です。これには、固有のリスクについて特定、評価、対処するための体系的アプローチが必要です。

脅威環境は進化し続けている

125%

サイバー攻撃の増加、前年比

Accenture、2021年

25+

フィッシング以外にも、さまざまな種類の悪意ある電子メール手法が存在

Microsoft、2021年

3社に1社

過去12カ月間にサイバー犯罪を経験

Norton、2021年

+269%

2020年第1四半期～2021年の間に世界的なフィッシングサイトの数が増加

Statistica、2021年

65%

サイバー攻撃が大幅に増加し、リモートワークの拡大がその原因である組織

Splunk、2022年

74%

リモートワークによって、ハッカーやサイバー犯罪者が従業員につけ込みやすくなったと考える

Norton、2021年

https://www.accenture.com/us-en/blogs/security/triple-digit-increase-cyberattacks
https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report
https://now.symassets.com/content/dam/norton/campaign/NortonReport/2021/2021_NortonLifeLock_Cyber_Safety_Insights_Report_Global_Results.pdf
https://www.statista.com/statistics/266155/number-of-phishing-domain-names-worldwide/
https://www.splunk.com/en_us/pdfs/resources/e-book/state-of-security-2022.pdf
https://now.symassets.com/content/dam/norton/campaign/NortonReport/2021/2021_NortonLifeLock_Cyber_Safety_Insights_Report_Global_Results.pdf

サイバーセキュリティへの取り組みを始めたばかりの場合、またシステムとプロセスを再検討する場合でも、情報セキュリティマネジメントシステムの要件を定義する国際規格の ISO 27001 が、効果的なリスクマネジメントを中核とする優れた出発点を提供します。

ISO 27002:2022 の発行により、ISO 27001:2013 に含まれる管理策のリストに強く必要とされていた更新が実現し、脅威と現在のベストプラクティスの両方に関連する発展を確実に反映しました。ISO 27002 の適用範囲の拡大は、リスクマネジメント措置が広範かつ効果的であることを確保するのに役立ちます。

“ISO 27002の発行は、現在の組織が直面している複雑な脅威環境に即した一連の管理策を導入する重要な節目となるものです。組織は、この包括的な一連の管理策を活用して、特定したリスクへの対処や、潜在的なギャップの発見が可能になります。”

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

ISO 27001に準拠したリスク評価プロセスの5つの必須要素

リスクマネジメントの枠組みを構築する

正式なリスクマネジメント方針、プロセス、登録を含みます。貴社の状況によっては、すでに組織レベルで実施され、トップマネジメントによって承認されている場合もあります。そうでない場合、効果的なリスクマネジメントに関する国際的に認められたベンチマークとガイドラインとして ISO 31000 を利用できます。

情報・サイバーセキュリティのリスクを特定する

内部監査やインシデント分析などの継続的活動が不可欠です。ISO 27002 は、最新の情報セキュリティ、サイバーセキュリティ、プライバシー保護マネジメントについて規定しており、リスク識別におけるギャップを特定するための有用な比較ツールとしても活用できます。

影響と可能性に基づいてリスクを分析する

ビジネスに関連する要因に基づいて、リスクを評価し、対処する際に優先順位を付ける

リスク対応のオプションを選ぶ

所有権とレビューに関する透明性の高いプロセスを使用し、リスクの回避、受け入れ、軽減、移転を行うかどうか決定します。

2. 適切なソリューションの特定

実践的なリスクマネジメントアプローチにより、組織が直面している固有の脅威や課題をより包括的に把握できるようになります。そしてまた、自社のニーズに対応する適切なツールを選択できる道が開かれます。これは効果的な情報・サイバーセキュリティ戦略の基盤となり、ベストプラクティスを実証するカスタマイズされた保証プログラムの開発に必要な洞察を提供してくれるものです。

多くの組織にとって、独立した ISO 27001（ISMS）認証は、自社戦略の広範な基盤となるでしょう。現在では、より多くの組織が、リスク特性に応じた進歩的で統合的なマネジメントシステムのアプローチを採用しています。

ISO 27000 シリーズはこの点を念頭に置いて策定されたものであり、特定の重点分野に関連するガイダンスと管理策を含む一連の拡張機能を備えています。このため実際に、ISO 27001 準拠の ISMS を備えている組織は、その範囲をさらに拡張し、クラウドセキュリティ（ISO 27017、CSA STAR）、クラウドプライバシー（ISO 27018）、サイバーセキュリティ（ISO 27032）、プライバシー情報マネジメント（ISO 27701）に関連する特定の脅威に対処できることになります。これは、幅広い情報セキュリティマネジメントシステム（ISMS）を構築する効果的な方法です。

組織はその後、その他の附属書 SL ベースの規格とのさらなる統合を選択できます。これらは、事業継続性（ISO 22301）や IT サービス管理（ISO 20000-1）などの情報・サイバーセキュリティのベストプラクティス、または労働安全衛生（ISO 45001）や品質（ISO 9001）などその他の重点分野でのサポートも可能になります。その結果、より効果的なシステムが構築され、プロセス、役割、事務管理に関する重複のないアプローチが可能になります。

リスクプロファイルを反映した統合システムの構築

> 多くの組織は、自社のアプローチが目的に適っていることを確保し、サイバー脅威やサイバー攻撃に対する適切な保護、検出、対応、復旧を実現するため、コンプライアンスを超えた取り組みを行う必要があります。

マネジメントシステムを導入し、LRQA のような信頼できる第三者の認証を受けることが、サイバー保証プログラムの基礎を形成します。多くの組織は、自社のアプローチが目的に適っていることを確保し、サイバー脅威やサイバー攻撃に対する適切な保護、検出、対応、復旧を実現するため、コンプライアンスを超えた取り組みを行う必要があります。そのためには、ペネトレーションテスト、インシデントレスポンス、脆弱性スキャンなどの高度なサイバーセキュリティサービスや、場合によってはフルマネージドのセキュリティオペレーションセンター（SOC）サービスも必要です。

LRQA グループの Nettitude で技術サービス担当ヴァイスプレジデントを務めるクリス・オークリーは次のように述べています。

> **情報セキュリティプログラムに、明確かつ測定可能な目標を確実に設定することが重要です。これには、資産とリスクの管理、資産の保護、攻撃の検出、インシデント対応、復旧に関する要求事項を含めることが考えられます。ISO 27001等の国際規格が優れた基盤を提供し、ペネトレーションテスト等の他の保証活動の指針となるでしょう。**

3. トップマネジメントによる責任ある行動で、成功のための計画を立てる

どのようなプロジェクトでも同様ですが、成功には計画と賛同が不可欠です。情報とサイバーセキュリティの全体的な責任はトップマネジメントにあります。しかし、広範な戦略と保証プログラムは、事業のすべての部門・部署に影響を及ぼします。

認証されたマネジメントシステムにとって、トップマネジメントと組織リーダーの関与は必須条件です。審査中にこれが明確に存在しなければ、重大な不適合が発生し、認証取得は難しくなります。適切なシステムを支える真の本質と原動力は、常にトップダウンでもたらされなくてはなりません。

この背景には、情報セキュリティとサイバーセキュリティの戦略、それに続く保証プログラムの目的が、より広範なビジネスの目的と一致するように、リーダーシップがサポートすることが挙げられます。さらに、システムやプログラムが効果的な投資と資源の運用管理に支えられることも重要です。特に、マネジメントシステムの認証やコンプライアンスから、高度な脅威の検知、対応、テストに至るまで、専門的な知識を必要とするサイバー保証活動の複雑な性質を考慮すると、非常に重要な要素になります。

> “情報・サイバーセキュリティの保証に対する360度のアプローチには、リーダーシップが提供できる調整、投資、サポートが必要です。このような考え方が組織全体に浸透すれば、全ての従業員が脅威の防止・特定に自ら役割を果たすという共同責任が推進されます。
>
> サイバーセキュリティのベストプラクティスが企業文化に浸透すると、トレーニングプログラムの導入（および継続的な改善）も容易になります。これにより、組織が抱える最も重大な脆弱性の１つー従業員のリスクを軽減することができます。”

アグスティン・レルマ・ガンゴイティ
情報およびサイバーセキュリティ担当 シニア主任審査員｜LRQA

4. コンプライアンスの十分な証拠を収集する

情報・サイバーセキュリティの観点で、適用される一連の法規制は広範囲にわたっています。関連する法規制を特定するだけでも複雑な作業となり、多くの場合は専門家のサポートが必要です。必須の要求事項は、知的財産の保護からデータの暗号化、労働法に至るまで、さまざまな部署に関連しています。

特に重点を置いている分野の 1 つは、プライバシーと個人を特定できる情報（PII）の保護です。これは、グローバルな規制の観点から見ると、長期的に流動的な状態にあります。EU 一般データ保護規則（GDPR）の導入以降、新たな法律が世界中で制定されており、それぞれに独自の要求事項と定義があります。このため、国際企業にとってコンプライアンスの実証は非常に複雑な作業です。

ISO 27001 のようなマネジメントシステムでは、組織は自らの業務に適用される遵守必須の法規制を特定する必要があります。これには法務、人事、IT、調達など、さまざまな部門からの部署横断的なサポートが必要です。認証取得するため、組織はコンプライアンスが確保されている証拠も提供する必要があります。これは、ISO 27001 に照らした審査の際に、しばしば不適合と繋がってしまう場合があります。

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であるロブ・アッカーは以下のように述べています。“ISO 27001 やその他の関連規格に照らして組織を審査すると、法規制の遵守に関する適切な証拠が整っていないことが明らかになることがあります。これは、情報とサイバーセキュリティに関連する規制の環境がますます複雑化しているという事実が大きいと言えます。”

“マネジメントシステム規格の法的・規制的要件は最も困難なものの一つですが、効果的なフレームワークを確立し、認証を取得するプロセスは、ベストプラクティスを現実のものとし、ビジネスに大きな長期的価値を付加します。”

世界的に、データ保護、電子取引、消費者保護、サイバー犯罪を対象とした法制度を採用する国が増えている[1]

81%
電子商取引法が制定されている国

71%
プライバシー法が制定されている国

80%
サイバー犯罪法が制定されている国

59%
消費者保護法が制定されている国

[1] 国連貿易開発会議グローバル・サイバーロー・トラッカー https://unctad.org/topic/ecommerce-and-digital-economy/ecommerce-law-reform/summary-adoption-e-commerce-legislation-worldwide

5. サプライチェーンの脆弱性に対処する

ビジネスに効果的なサイバーセキュリティ戦略と保証プログラムを導入することと、そのベストプラクティスを広範なサプライチェーンに波及させることは、全く別の課題です。多くの点で、鎖の強さはその環の一番弱い部分で決まるのです。たった一社のサプライヤーの脆弱性が悪用されれば、他のすべての関係者が経済的、評判的、経営的に危険にさらされる可能性があります。

サプライチェーンがますますグローバル化・複雑化するにつれて、より広範なリスク環境も同様に変化します。組織は、単なる安心感だけでなく、サプライヤーがコンプライアンスとリスク管理に関してベストプラクティスを適用しているという信頼と実証を必要としています。これにより、サプライチェーン内で頻繁に発生するより一般的な脅威を一部軽減できます。

まず第一に、組織はビジネスを行う相手と、サイバーリスク管理に関する成熟度や願望を理解する必要があります。サプライヤーの選択をめぐる明確なプロセスとガイダンスが多くの場合重要となり、これには Cyber Essentials や ISO 27001 認証などの必須要件を規定することが含まれると思います。後者には、効果的なシステムとプロセスを企業が備えていることを保証する強固かつ独立した審査が必要です。

サプライチェーンの脆弱性に起因する一般的なリスクと課題

1. **サイバー脅威への不十分な保護と対応**
2. **データ漏洩と法令違反**
3. **製品の整合性の問題**
4. **非効率性**

> **私たちの未来は、サプライチェーンのサイバーセキュリティを積極的に推進し、単純な契約上の要件からエンドツーエンドのサプライチェーン保証プログラムへと移行していくことになります。これにより、脅威環境を反映したさまざまな措置を通じて、セキュリティとレジリエンスが向上します。**
>
> **コラボレーションは今まで以上に重要です。組織はベストプラクティスを共有し、能力を築くための適切なツールをすべてのサプライヤーに備えさせる必要があります。そのメリットは、導入コストをはるかに上回るものです。**

スチュアート・ライト｜ガバナンス、リスク、コンプライアンス担当グローバル・ヘッド｜Nettitude（LRQA グループ傘下）

サイバーセキュリティのあらゆる側面をターゲットに、お客様と一緒に取り組む

LRQAの保証分野での深い経験と、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、お客様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、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、世界の市場から高い評価を得た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。

お客様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がお客様と協力して認証、脆弱性の特定、ブランドの整合性、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 のコンプライアンス・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

認証、教育研修、ガバナンス、リスクとコンプライアンスサービスを提供し、混乱を防止、対応、復旧できるよう準備します。

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で、サイバー脅威の一歩先を行くことができます。

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