サイバーセキュリティ

変化するサイバー環境への対応

ISO 27002の変化とGRC（ガバナンス、リスク、コンプライアンス）の今後を理解する

目次

序文 03

4つの重要なポイント

セクション1　リスクマネジメント 04

セクション2　ISO 27001がGRC（ガバナンス、リスク、コンプライアンス）のベストプラクティスを推進 05

セクション3　ISO認証の重要性と適用宣言書 06

セクション4　ISO 27001の新バージョンが登場 07

LRQAについて 08

序文

進化する環境がリスクの増大をもたらす

世界のリスク環境は急速に変化しています。組織が新しいテクノロジーやデータへの依存を深めるにつれて、サイバー攻撃の件数と巧妙さは高まり続けています。

技術革新に後押しされているこれらの脅威は、多くの場合、組織化された攻撃として企業を標的にします。これは新興企業や既存の大手企業ということは関係ありません。インターネットに接続されたインフラ等の資産がある場合、他の同業者や競合他社と同じように、サイバー攻撃の犠牲者となる可能性があります。

このような長引く脅威が増大し続けていることを受け、ISO 27002 や ISO 27001 などの国際規格には、より多くのマネジメントフレームワークが組み込まれるようになりました。LRQA、Nettitude、Kantar の専門家に、ガバナンスリスク & コンプライアンスの今後と、ISO 27002 規格の変更が、進化するリスク環境をどのように反映しているか尋ねました。

LRQAの専門家

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監査員｜LRQA

ニック・プレスコット
シニアGRCコンサルタント｜Nettitude（LRQAグループ傘下）

ポール・ワッツ
著名なアナリスト、ISFおよび元CISO｜Kantar

> **“このトピックは、脅威の全体像の観点から強調すべき重要なことだと思います。インターネット上で取引を行う企業はすべて最前線でさらされるため、サイバー攻撃は非常に大きなリスクです。”**
>
> ニック・プレスコット
> シニアGRCコンサルタント｜Nettitude

4つの重要なポイント

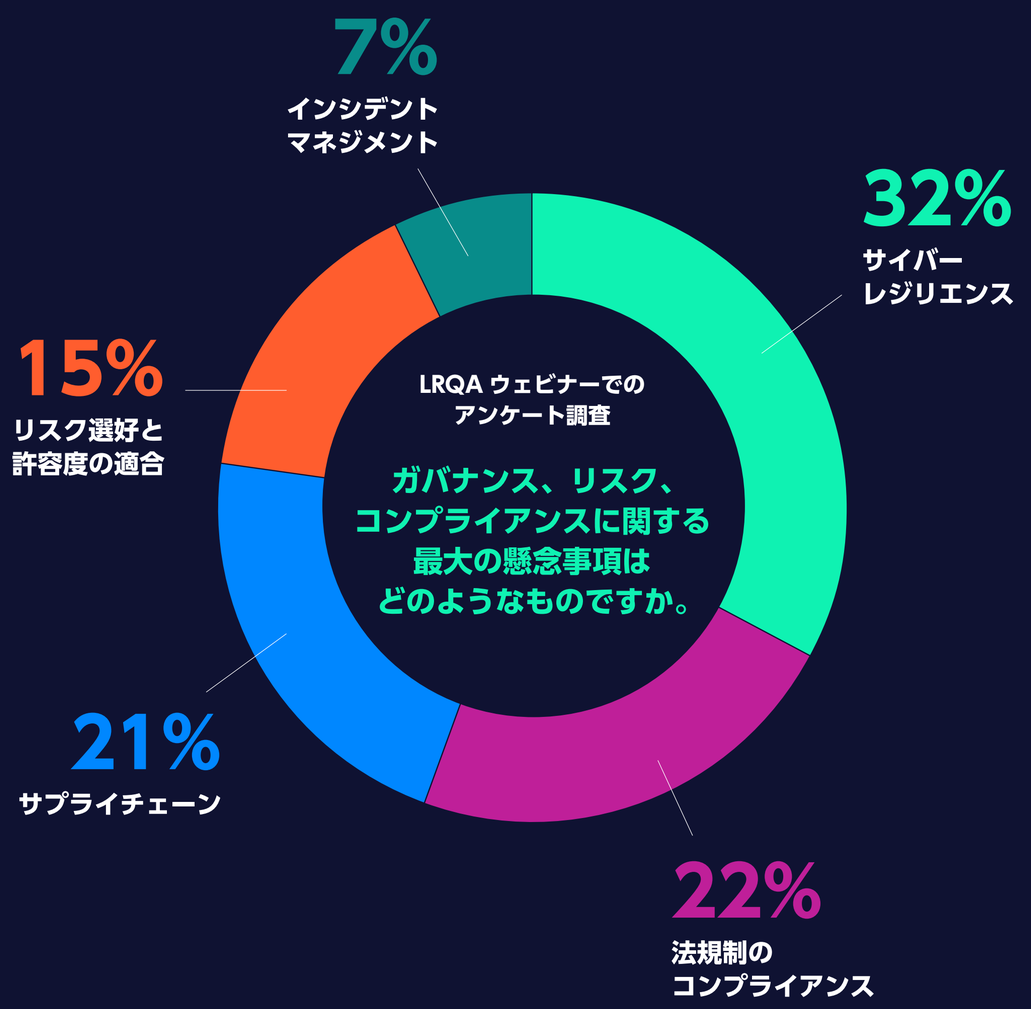
1. リスクマネジメントが GRC（ガバナンス、リスク、コンプライアンス）の中心に

ニック：GRC（ガバナンス、リスク、コンプライアンス）の目的は攻撃が起こらないようにすることであり、リスクマネジメントを中核に据えることで実現することが可能になります。組織は、優れたガバナンス、強力なポリシー、手順、プロセス、テクノロジーパッケージの最適化、更新、保護、そして外部規制のコンプライアンス要件が満たされていることを確認する必要があります。

ポール：テクノロジーは今や、ビジネスの原動力です。そのため、レジリエンスと強力な情報セキュリティ管理の必要性が大幅に高まっています。レジリエンスとは、単なる復旧にとどまらず、新たな姿勢を取れるかということです。パンデミックがあった過去2年間に学んだことがあるとすれば、私たちが新しい技術を導入する速度は、脅威環境がほぼリアルタイムで変化することを意味します。

“コンプライアンスはセキュリティとは異なります。優れたGRC フレームワークとは、適切な統制が整備されていること、これらの統制の成熟度が適切な水準にあること、リスクプロセス内に適切なリスク選好と許容度があるよう確保することです。つまり、リスクと成熟度の間で慎重なバランスを取ることに尽きます。”

ニック・プレスコット
シニアGRCコンサルタント | Nettitude



4つの重要なポイント

2. ISO 27001がGRCのベストプラクティスを推進

ニック：GRC の成熟度を促す一つの方法は、ISO 27001 または ISO 27002 を利用することです。ISO 27001 は戦略的運用を連携させ、ISO27002 は戦術的マネジメントを導入することで、組織の全体的概要を把握し、強固な資産・供給マネジメントのプロセスを確実に実施できるようにします。情報漏えいの約 3 分の 2 がサプライチェーンを通じて起きていることを考えると、その重要性は計り知れません。さらに、これらの国際規格により、強力なセキュリティ運用（物理レイヤーと仮想レイヤーの両方）、事業継続性、スタッフ管理、コンプライアンスなども確保されます。

アグスティン：ビジネス環境の変化や最近の世界的な出来事により、新たな脅威が発生しています。これらのリスクやその他のリスクは、ますます速く進化しているため、組織はより大きな変化をより迅速に取り入れ、データやその他の重要な資産のプライバシーを保護する必要があります。リスクの管理に加えて、多くの規制や契約上の要求事項も管理が必要です。これらの要因が重なって、一貫した GRC マネジメントの枠組みを維持することが非常に困難になっています。当社がソリューションとして、ISO 27001 情報セキュリティマネジメントシステム（ISMS）規格を提案するのはそのためです。この規格は GRC の成熟度と強い関連があり、第 4 章ではガバナンスのシステムと、情報・資産の管理、セキュリティ、プライバシーのための構造について規定しています。

ポール：ISMS（情報セキュリティマネジメントシステム）を構築する場合、まず基盤と構造を構築する必要があります。この構造がなければ、プロセスとコントロールの内容、その適用範囲、測定方法、最適化の方法を定義するのは非常に困難です。ISO 27001 は国際的に認められた規格であり、情報セキュリティマネジメントに対する組織のアプローチの「純資産」に関する保証を提供するものとして認証されています。ISO 27002 は一歩進んでおり、管理策の適用方法について詳細に説明していますが、ISO 27002 に対して直接認証を得ることはできません。ISO 27001 に基づいて認証を受け、ISO 27002 を活用して最適な統制を特定します。

> **“ISO 27001 認証は ISMS の適切な実装を示す証拠であり、GRC 管理のベストプラクティスが行われていることを示します。証明書に含まれている適用宣言書は、この事実を証明する重要な要素になります。”**

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監査員｜LRQA

4つの重要なポイント

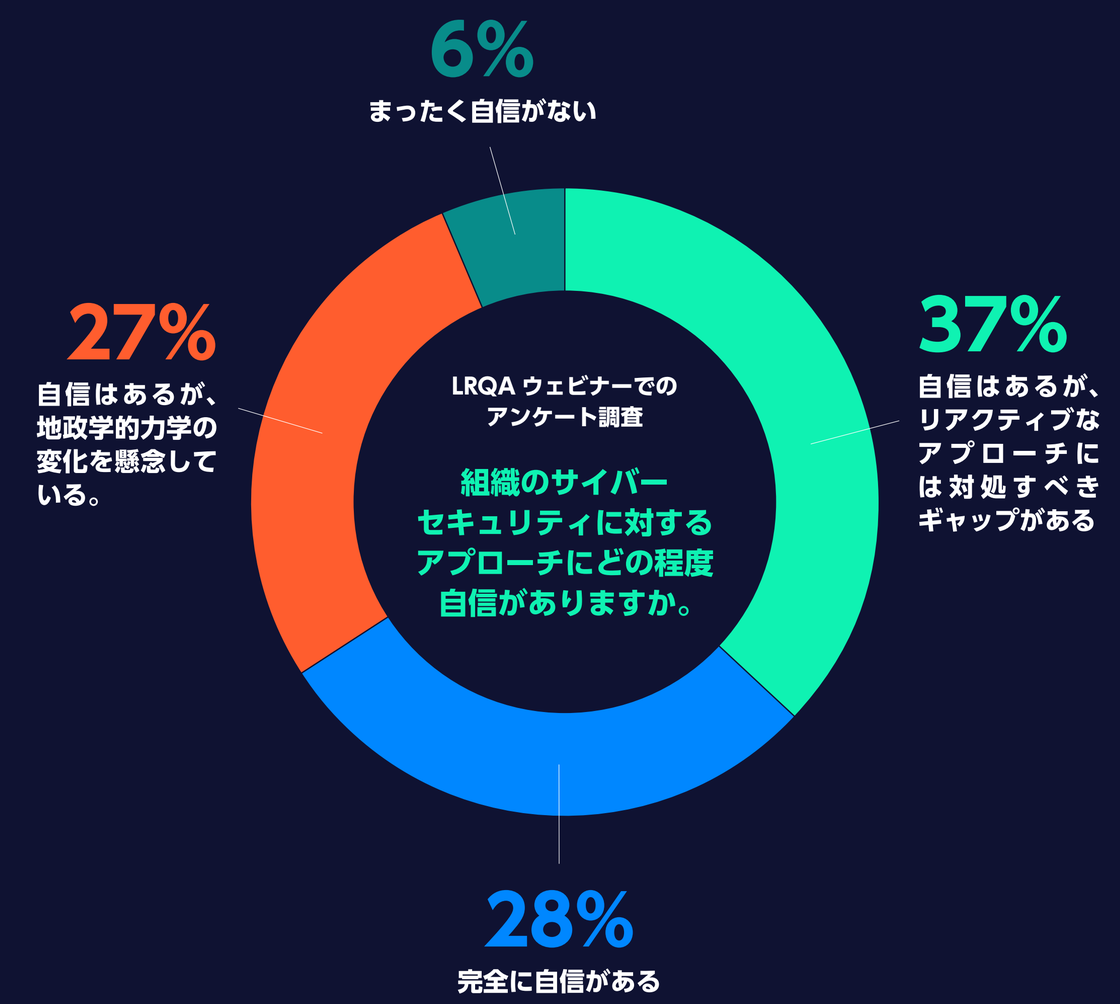
3. ダイナミック（動的）なビジネス環境を反映した新しいISO 27002の管理策

アグスティン：ISO 27002 規格が更新され、GRC に新たな焦点が置かれるようになりました。ISO 27002 は、管理マトリックスとして、リスク、セキュリティ、プライバシーに関する管理の実施と運用に関するガイダンスを組織に提供しています。また、情報セキュリティリスクとコンプライアンスのための統制の実施および運用のベストプラクティスに関する、さまざまな提言も記載しています。

直近の ISO 27002 改訂における最大の変更点は管理策に関するものです。現時点で組織的、人的、物理的、技術的な 4 つの主要な統制グループがあり、93 の個別の管理策（ISO 27002:2013 の 114 から減少）が編成されています。これら管理策のほとんどは 2013 年バージョンからの改訂ですが、ICT の即応性、事業継続性、監視活動などを範囲に含めるために 11 の全く新しい管理策が導入されました。これらの新しい統制は、現代のダイナミックなビジネス環境と、より広範な脅威環境を反映したものです。

“ISO 27002 の 2013 年バージョンを振り返って見ると、非常に多くのカテゴリーがありました。これらは現在、組織、人材、物理、技術の 4 つの分野に統合されており、戦略的な運用のレジリエンスを真に推進するには、4 つの分野のすべてから管理策を実装する必要があります。これは非常に重要なポイントです。”

ポール・ワッツ
著名なアナリスト、ISF および元 CISO | Kantar



4つの重要なポイント

4. ISO 27001の改訂につながる

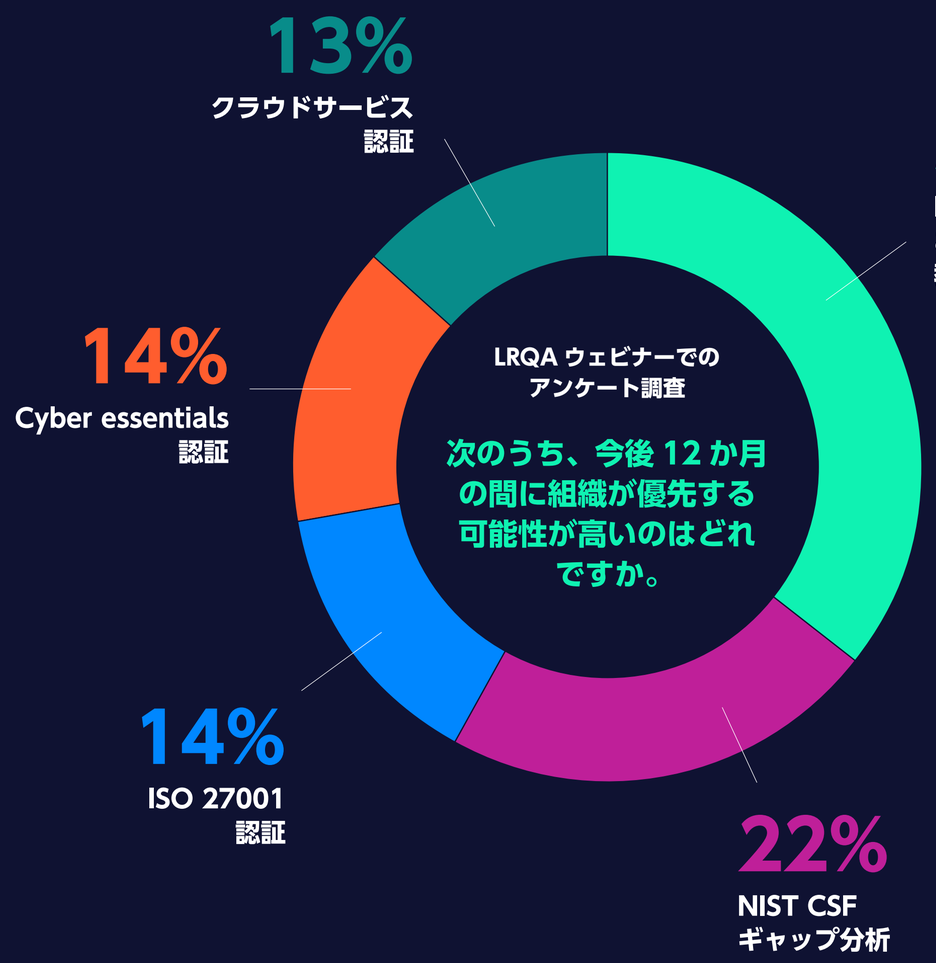
アグスティン：現在顧客から寄せられている最大の質問の 1 つは、「ISO27002 への変更はマネジメントシステムにどのような影響を与えるか」というものです。現在 ISO 27002 が公表されたところですが、これは ISO 27001 の改訂につながるものであり、附属書 A には更新された管理策のリストが反映されます。

今度の変更のほとんどは、ISO 27002 の 6.1.3 項に関するものであることに留意することが重要です。規格の共通の上位構造には大きな変更はないものと思われます。組織が自社の RTP を包括的にレビューし、既存の統制への変更と 11 の新しい統制の両方がどのように適用されたか実証することが期待されています。組織はまた、リスク評価とリスク対応アプローチの反復を新たに形成すべきです。

GRC に関しては、LRQA のような認定された認証機関によって認証された ISO 27001 は、強固な運用リスク管理の信頼性と証拠となります。

“新バージョンの ISO 27002 では、大まかな構造の変更は予定されていません。変更のほとんどは、リスク対応を扱っている第 6 節に反映される予定ですが、修正ではなく明確化を目的としています。”

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監査員｜LRQA



LRQAによる支援

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。

サイバーセキュリティのあらゆる側面を対象にした協力

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