ISO 27001 による リモートワーク環境時 における リスクマネジメント

今日では、ほぼ全ての組織がリモートワークを経験しており、その加速度はさらに高まっています。リモートワークに対して十分な準備をしていた組織にとっても、情報セキュリティの脅威は絶えず変化を続けています。

リモートワークが長期的かつ戦略的な検討事項になるのに伴い、それに関連するリスクマネジメントは、情報と機密データ保護の中核として極めて重要かつ継続的な作業になります。

本レポートでは、LRQA の専門家が、変化する脅威の状況、検討できる主な行動、新たなリスクの軽減における ISO 27001 認証の重要な役割について考察します。

Joyce van Luijn-Bonneveld
主任審査員 - 情報およびサイバーセキュリティ | LRQA

Joyce は経験豊富な IT 審査員で、主に IT インフラストラクチャーを担当するマネージャーです。IT ラインマネージャー、プロジェクト・マネージャー、トレーナーとして約 30 年以上にわたりビジネス界で活躍してきたほか、数年間の経営経験もあります。

Stuart Wright
コンプライアンス・リスクのグローバル・ヘッド | Nettitude

Stuart は IT 業界で 17 年の経歴を有するほか、情報セキュリティ・コンサルティングセクターで 11 年超の経験もあります。小売、地方自治体や中央政府、金融、ヘルスケア等の多様なセクターを担当し、幅広く活躍してきました。

Paul Raines
最高情報セキュリティ責任者 | 国連開発計画（UNDP）

Paul は、情報セキュリティ責任者として、組織の全世界 177 拠点のサイバーセキュリティと障害からの回復計画の管理を統括しています。彼が率いるチームは、国連で ISO 9001、ISO 20000、ISO 27001 認証を受けた唯一かつ初のチームです。

重要なポイント 1

変化する脅威の状況

Stuart: “私たちが目撃してきた脅威の多くは、常に変化し続けています。ご家庭のネットワークや Wi-Fi の利用などは決して新しいものではなく、日頃から使用されているものです。唯一の違いは、リモートワークしている従業員の増加に伴ってリスクが大幅に増加していることです。

仕事に関連した作業のため、従業員が自身のデバイスを使用することを容認している組織は増えてきています。多くの場合、ビジネスを継続ためにそういった状況は必要だからです。そのデバイスを組織として所有していない場合、そのデバイスのセキュリティをコントロールすることはできません。またそのデバイスにパッチが適用されていることや、ウイルス対策、必要な措置がすべて講じられていることを確認することもできません。こうしたコントロールの欠如によってさらに多くのリスクがもたらされています。

これまであまり重要視されていなかったリスクの一つとして、従業員が分断された状態に置かれることや、事務所から離れている場合、通常は行われるはずの報告が行われない可能性が高まるという考えがあります。この中には、懸念事項、従業員が行ったこと、従業員がクリックしたリンク先、その他の様々な事柄が含まれます。何かがいつ間違った方向に進むのかを把握するのが困難なため、迅速に対応できないことを意味しています。”

> “従業員が事務所から離れると、通常なら行われるはずの報告が行われない可能性が高まります。”
>
> **Stuart Wright**
> **コンプライアンス・リスクのグローバル・ヘッド | Nettitude**

> “悪意の有無にかかわらず、友人、家族、訪問者の近くには、安全対策を講じていないデバイスや機密情報が存在している危険性があります。”
>
> **Joyce van Luijn-Bonneveld**
> **上級主任審査員 - 情報およびサイバーセキュリティ | LRQA**

Joyce: “現在、私たちはデジタルに囲まれた時代に生きています。ホテルの部屋を予約する際、また身の回りのアイテムを注文・購入する際も、多くのデータが生成され、そのデータがクラウドに保存されています。その一方で、ハッカーが悪用できる情報が膨大になっていることも事実です。これは、大きな組織だけでなく、リモートワークしている個人にも当てはまります。データ漏洩を防止するために安全方策を導入している大企業でも、サイバー攻撃によってデータに不正アクセスされた事案が数多くあります。

リモートワークが広く普及し、場合によってリモートワークは永続的になる可能性もあるため、潜在的な攻撃者の機会が増大し、多くの事件が発生するおそれもあります。例えば、従業員は自身のデバイスで十分な安全対策を講じていない可能性があります。不正アクセスも重大なリスクになります。悪意の有無にかかわらず、友人、家族、訪問者の近くには、安全対策を講じていないデバイスや機密情報が存在している危険性があります。”

重要なポイント 2

職場を守る意識、行動様式と措置

Joyce: “すべての組織は、長期的なリモートワークを計画しているか否かにかかわらず、リモートワークをしているすべての従業員に対し、リスクと安全確保のためにできる措置について教育していく必要があります。フィッシング攻撃を見つける方法や強いパスワードを作成する方法などがその例です。

組織はリモートワークに対する安全なIT 設備・機器の提供を検討する必要があります。また、従業員が機密文書を自宅に持ち帰ることを禁止するほか、リモートワークに適用される一連のポリシーと要求事項を策定する必要もあります。”

Stuart: “ユーザーは意図的にデータへアクセスできます。ユーザーは仕事をする上で必要なため、多くのデータにアクセスできます。このレベルのアクセスでは、ユーザーには認証情報とアクセス許可を通じて正当にアクセスできる権利が付与されているため、悪意のあるアクセスを検出することは難しくなっています。

犯罪者は盗まれたパスワードを利用することによって、技術的なセキュリティコントロールの多くを回避できることを認識しています。そのため、ユーザー認証情報を重要視し、常に標的としているのです。こういった認証情報があれば、犯罪者は正当なユーザーであるかのように見せかけることができるため、悪意のあるアクセスを検出し、迅速に対応することはさらに難しくなっています。こういった状況は、従業員への教育がこれらの脅威から保護する方法の重要な一部である、という認識を高めるものでもあるのです。”

> “すべての組織は、長期的なリモートワークを計画しているか否かにかかわらず、リモートワークしているすべての従業員に対し、リスクと安全確保のためにできる措置について教育していく必要があります。”
>
> **Joyce van Luijn-Bonneveld**
> **上級主任審査員 - 情報およびサイバーセキュリティ | LRQA**

Joyce: “IT セキュリティとコントロールの欠如は、リモートワークをしている時に見過ごされやすい脅威の一つです。例えば、従業員は自身のデバイスに適切な安全設定を行っていない場合があります。組織はその対応についてまだ検討していないか、または従業員が PC やルーターなどの設備・機器を、一般的なパスワードを変更しないで利用していることが原因となっている可能性もあります。

ある組織では、デバイスにウイルス対策やマルウェア対策を施さず、重要な更新を行っていない場合もあります。また、組織と接続する仮想プライベートネットワーク（VPN）が常に利用できるわけではなく、多要素認証も強制されていないので、従業員の家族や友人など使用権限のない他の者、または悪意を持つ者に機密情報へのアクセスができる状況を与えている可能性があります。

従業員が十分な注意を払っているか、また在宅勤務に伴うリスクに気付いているか検討することが重要です。個人や職場のコンピュータで仕事をする際には、その使用を家族と共有しないようにする必要があります。

不正アクセスが容易なため、一般的な初期設定のパスワードの使用は控える必要があります。自宅のルーターとWi-Fi のパスワードを変更し続け、不正アクセスを防いでいくことが重要です。パスワードは、アマゾンなどのウェブサイトで私的に使用しているものを避け、常に唯一のパスワードを使用する必要があります。従業員は、ロックをせずにコンピュータから離れることや、机の上に置かれた書類や会社の機密データから離れることを防ぐ必要があります。”

重要なポイント 2

職場を守る意識、行動様式と措置

Stuart: “ISO 27001 は、急激な変化に直面する恐れのある新たなリスクを理解するのに役に立ち、それらを軽減することに繋がります。新たなリスクが発生することがないようにするため、適切な水準かつ監督者と承認を得た安全な方法で変更が行われることを確実にするものです。

現在の情勢で ISO 27001 を役立てる方法は多くあります。変更やインシデントのマネジメント、モバイルデバイスとリモートワーク、リスク評価、審査の実施、セキュリティプロセスやセキュリティコントロールのモニタリングなどの領域では特に有効です。

有益な情報セキュリティ・マネジメントシステム（ISMS）はビジネスの目的を支援するものであり、それによって安全な状態を維持することができます。ISMS を導入することで、組織に最も適した方法を確立することが可能になります。近年のパンデミックのような想定外の事象に直面しても、効果的なやり方でリスクを管理することができる方法の一つです。”

> “ISMS を導入することで、組織に最も適した方法を確立することが可能になります。近年のパンデミックのような想定外の事象に直面しても、効果的なやり方でリスクを管理することができる方法の一つです。”
>
> **Stuart Wright**
> **コンプライアンス・アンド・リスクのグローバル・ヘッド | Nettitude**

Joyce: “ISO 27001 は、リモートワークで発生するリスクを軽減するために実際に適用できる包括的な規格になります。

リモートワークに関しては、いくつかのコントロールが注目されています。例えば、A.11 の物理的で環境に配慮したセキュリティコントロールはリモートワークにも適用され、A.17（事業継続性）は具体的にリモートワークの継続性に対処しています。

特に組織の敷地の外で勤務する場合には、リスクを明確に示すとともに、リモートワークに関するガイドラインを作成するため、ISO 27001 セキュリティコントロールの一部と相互比較することができます。ここには、紙の事務処理を減少する方法、指定した場所、組織や個人のデバイスの使用、ネットワークへのアクセスに関するガイダンスが含まれます。また、内部監査と審査を実施することによって、これらのコントロールの有効性を評価することができます。”

> “ISO 27001 は、リモートワークで発生するリスクを軽減するために実際に適用できる包括的な規格になります。”
>
> **Joyce van Luijn-Bonneveld**
> **上級主任審査員 - 情報およびサイバーセキュリティ | LRQA**

重要なポイント 3

ISO 27001 の実践：国連開発計画（UNDP）

Paul: “よく同僚から、現在の役割に伴う課題を意識しながら、24 時間どのように対応しているのかという質問をよく受けます。彼らが実際に聞きたいのは、『サイバー脅威から組織の評判、財務と生産性を保護するためのデューデリジェンス（組織などに要求される実施すべき注意義務および努力）をどのように実証したのか』ということです。

ISO 27001 認証を受けたのは 2011 年のことです。それ以前は、大規模なサイバー攻撃を受けましたが、この重大な事件は広く知れ渡ってしまい、組織にとっては極めて恥ずかしいことでした。

結果的に、金銭的な損失はそれほど大きくなかったですが、世界のメディアに注目され、不正アクセスの結果が報道されたため、組織の評判に関わる問題になりました。その結果、直ちに ISO 27001 認証の取得に着手しました。顧客重視の姿勢を維持する助けになるという理由から ISO 9001 認証のほか、少し遅れて、IT サービスマネジメントを対象にした ISO 20000 認証を追加取得しました。2011 年以降、これら 3 つの認証を取得したことにより、それ以前に経験したことに近い重大なサイバー事件はなくなりました。”

> “よく同僚から、現在の役割に伴う課題を意識しながら、24 時間どのように対応しているのかという質問をよく受けます。彼らが実際に聞きたいのは、『サイバー脅威からこの組織の評判、財務と生産性を保護するためのデューデリジェンス（組織などに要求される実施すべき注意義務および努力）をどのように実証したのか』ということです。”
>
> **Paul Raines**
> **情報セキュリティ責任者｜国連開発計画**

Paul: “これらの ISO 規格に適合しているマネジメントシステムを導入することにより、マネジメント、利害関係者、クライアントから信頼を得ることができます。一つ例えるとすれば、サイバーセキュリティは酸素のようなものということです。酸素が手に入った段階で、それに関して考える必要はなくなりますが、酸素を失ってしまうと、他の事柄を考える余裕は無くなってしまいます。

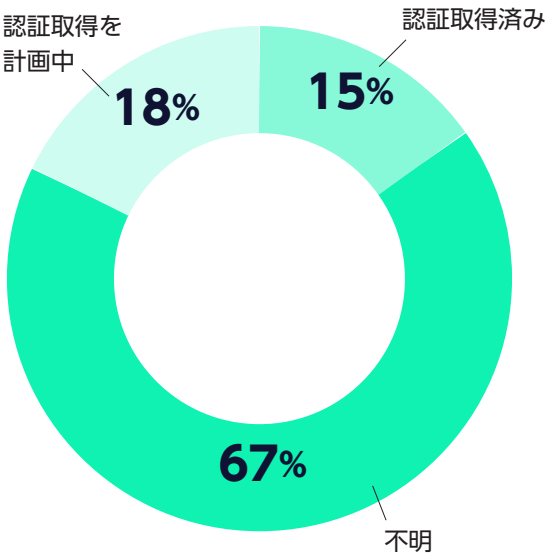
ISO 27001 からもたらされる効果の一つは、プロセスに関して組織に記録が残ることです。例えば、我々の組織では 3 ヵ月毎にマネジメントレビューが行われ、セキュリティコントロールがどの程度有効であるか調べています。

計画とのずれが生じた場合、または特定の種類のインシデント（例えば、フィッシングインシデント）の発生頻度が高まった場合には、その原因を調査すると共に、将来の指標を利用してそれに対処し、それを追跡するための決定を行うことによって、その有効性を見極めています。ISO 27001 にはそのような厳格性が備わっているため、セキュリティ組織の強化につながると見ています。”

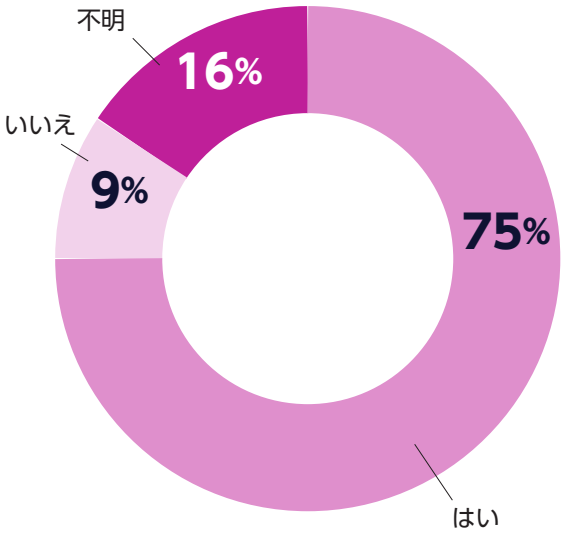
> “サイバーセキュリティは酸素のようなものです。酸素が手に入った段階で、それに関して考える必要はなくなりますが、酸素を失ってしまうと、他の事柄を考える余裕は無くなってしまいます。”
>
> **Paul Raines**
> **情報セキュリティ責任者｜国連開発計画**

業界の見方

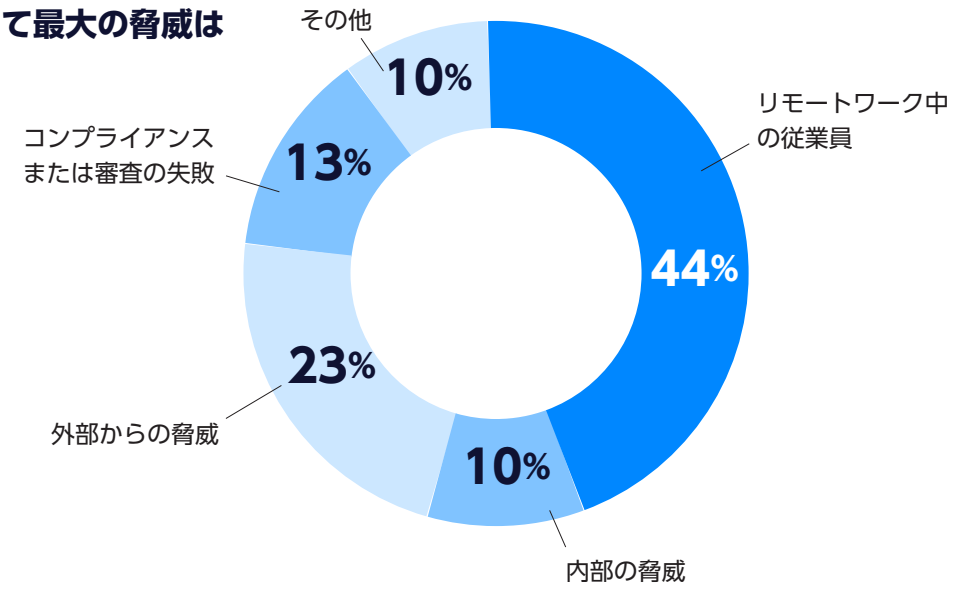
ISO 27001 に関する組織の取り組みはいかがですか？



パンデミックを経験した後、情報セキュリティの脅威は変化しましたか？



組織のビジネスにとって最大の脅威は何ですか？



ISO 27001 審査および教育・トレーニング

LRQA の幅広い審査および教育・トレーニングサービスは、規模や所在地を問わず、あらゆる組織に適しており、規格を最大限に活用できるように支援します。

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。当社は、一人一人の学びが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。

当社の ISO 27001 の教育・トレーニングコースには、以下などがあります。

- ISO 27001 入門
- ISO 27001 導入
- ISO 27001 内部監査員、主任審査員、主任審査員コンバージョン

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。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登録審査で構成される 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。

安全で信頼できるプラットフォームとアプリケーションを通じて遠隔で審査を提供可能です。柔軟性かつ迅速なサービス提供、技術専門家へのアクセス向上など、あらゆるメリットが享受できる、オンサイトと同様かつ高品質の審査サービスを受けることができます。

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。

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

YOUR FUTURE. OUR FOCUS.