kyndryl

規制対応に備えて

グローバルな
サイバールールへの対応

目次

お問い合わせ

追加のガイダンスについては、広報・政策渉外・社会貢献・サステナビリティ・チームチームにお問い合わせください。

- **グローバルポリシー** — Fariba Wells (*fariba.wells@kyndryl.com*)
- **サイバー規制** — Alex Lau (*alex.lau@kyndryl.com*)
- **ソートリーダーシップ** — Chase Purdy (*chase.purdy1@kyndryl.com*)

はじめに

世界最大のマネージド・インフラストラクチャー・サービスのプロバイダーであるキンドリルは、新興テクノロジーと、その技術によって形作る世界的な動向について独自の視点を持っています。

世界、そしてデジタルインフラストラクチャーは、かつてないほど複雑化し、急速に拡大しています。企業のテクノロジーリーダーや政府が厳しいIT環境の舵取りをしようとする中で、堅実な手腕と経験豊富なアドバイザーの必要性がこれまで以上に高まっています。キンドリルでは、この状況を大きな進歩の機会、つまり、お客様が必要とするときに、必要な場所、必要な方法で対応できるチャンスと捉えています。

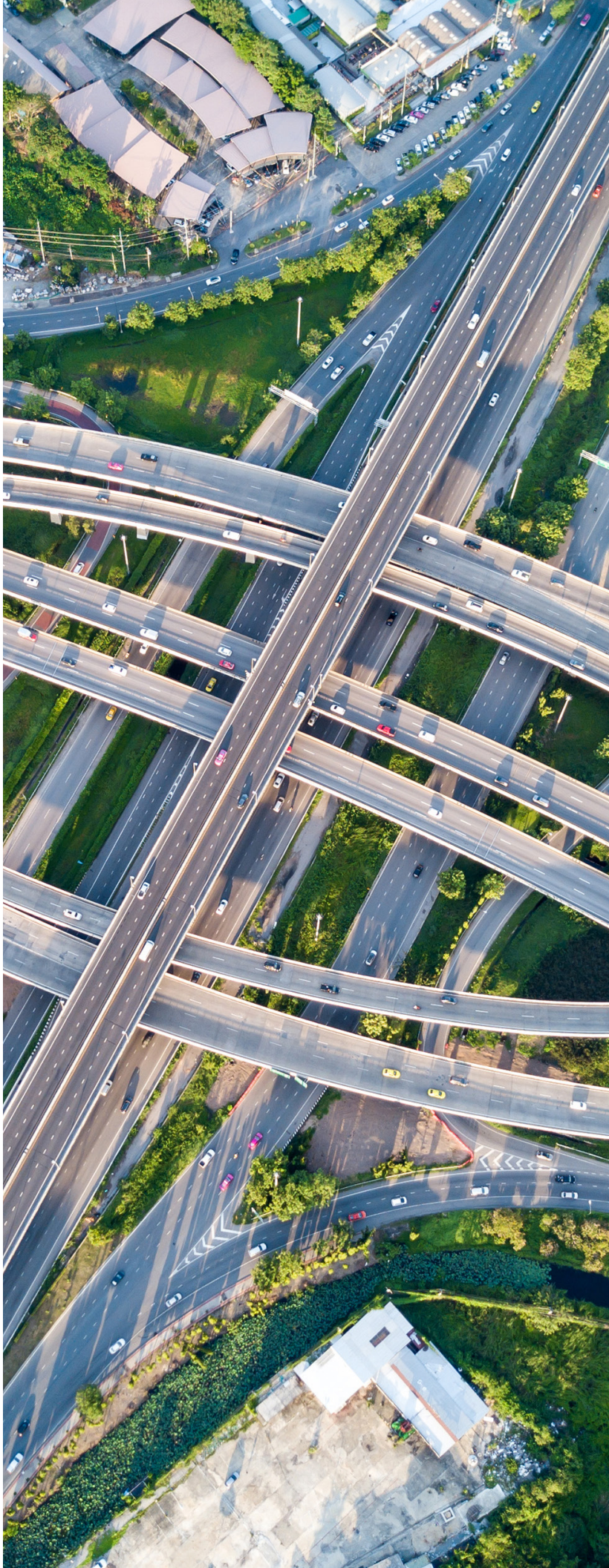
世界経済のデジタル化が進むにつれ、デジタルシステム、サービス、そしてそれらをサポートする重要なサードパーティプロバイダーを標的とするサイバー攻撃、データ侵害、その他の悪意のある活動など、サイバー脅威も増加しています。多くのデジタルサービス、特に金融などの分野のサービスは連携しています。ひとつのサービスプロバイダーで発生したサイバーインシデントが、デジタルエコシステム全体にシステムのリスクをもたらす、つまり連鎖的な影響を及ぼす可能性があります。それを念頭に、各国は規制を通じてこうしたリスクを抑制しようと努めています。

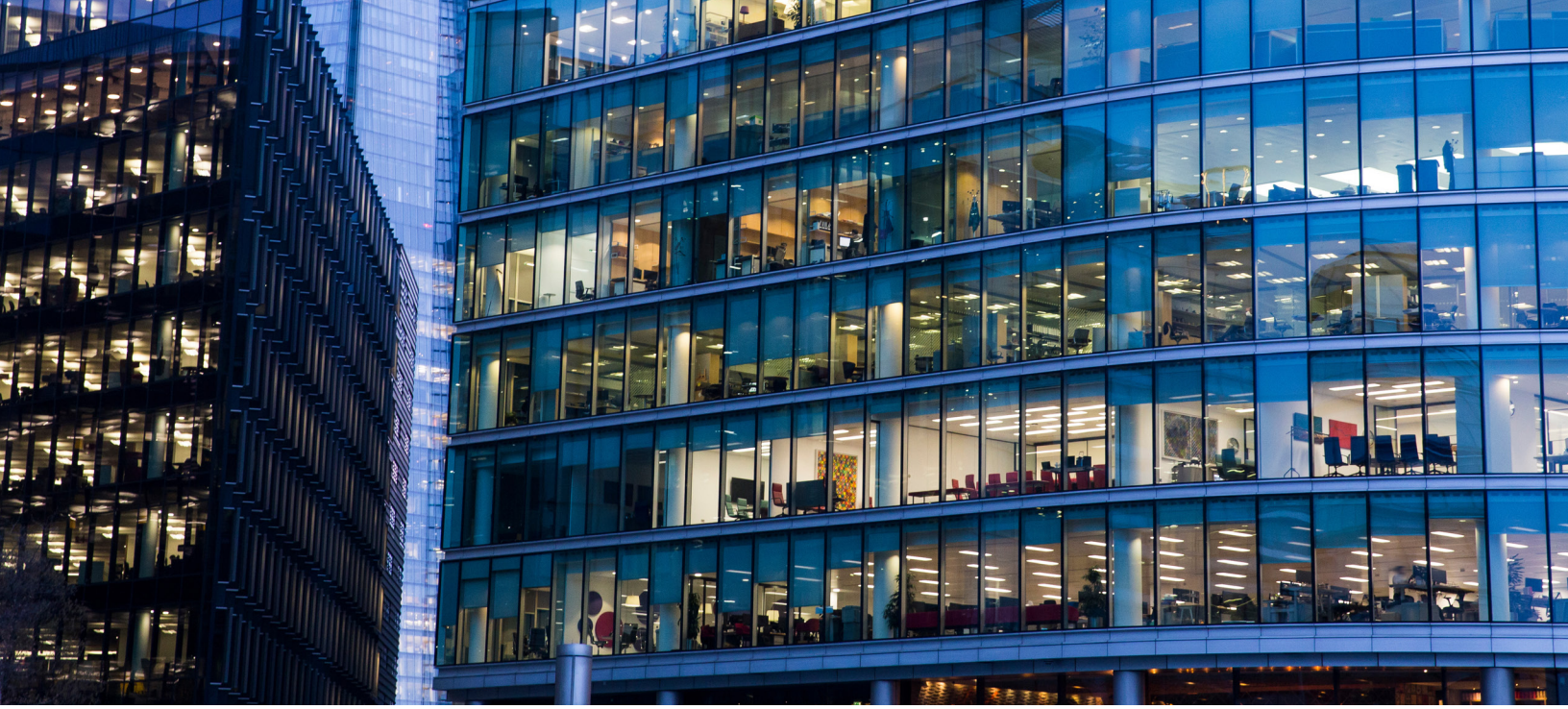
経済のデジタル化に伴い変化する課題やリスクに対処するという共通の目標があるにもかかわらず、世界的に規制の状況は依然として断片化しています。この状況に対応するために、キンドリルは、包括的なビジネス戦略と高い成長目標を維持しながらも新しい規制に準拠しようとしている企業に対して、コンサルティングアプローチを通じた支援の手段として、**サイバー規制への対応整備**のために設計された活動を開始しました。

キンドリルでは、次のことを念頭に置いたサポートを提供しています。

現代のサイバーセキュリティ戦略は、サイバーレジリエンスの考え方を取り入れたものでなければならないこと。サイバー関連のあらゆる出来事を予測、防御、対応、復旧する能力は、一部の攻撃が混乱を引き起こすことがほぼ確実である脅威環境において最も重要だからです。

複雑かつ進化する規制環境への対応に向けたお客様へのサポート。世界的に、各国の政府がガバナンス、リスク、開示に重点を置いた規制によって、高まるリスクに対処しています。これにより、円滑な事業運営を維持し、新しい規制を遵守しようとする企業へのプレッシャーが増しています。





サイバー規制の現状

過去10年間で、あらゆる拠点の企業が急速なデジタルトランスフォーメーションを遂げてきました。このことはサービスデリバリー、運用、顧客エンゲージメントでの革新につながりました。つまり事業成長のための新たな市場と機会を開拓したのです。

しかし、このデジタル環境の拡大は、攻撃者が企業を悪用する機会を増やしてしまうというサイバー脅威の増加にもつながりました。脅威環境の複雑さ、世界中のさまざまな規制コンプライアンス要件に対処することは、困難な課題になるでしょう。

例として、大手金融機関を考えてみましょう。今日の課題は、攻撃者が狙っているのが銀行自体のみならず、銀行にサービスを提供する重要な第三者サービスを悪用する方法が模索されていることです。なぜなら、攻撃者は、これらの組織に侵入する最も簡単かつ最速の方法がサプライチェーンを経由することであることを知っているからです。銀行のマーケティングチームが、プロモーションキャンペーン実施のために外部企業にサービスを委託しているかもしれません。攻撃者が外部の企業を標的にし、マルウェアをそれらの組織を通じて銀行に忍び込み、ランサムウェア攻撃を引き起こすといったことが簡単に起きてしまいます。

このような新たな課題に対応して、一部の政府は企業のセキュリティを強化するために新しい規制の枠組みを採用しています。

71%

サイバーセキュリティ関連インシデントを経験したと報告した回答者の割合。

84%

自分の所属組織が重要な業務を運営するためにIT資産に大きく依存していることに同意または強く同意するとした割合。

50%

攻撃を受けた回答者のうち、業務運営に支障が出たと報告した割合。

出典: キンドリル『*IT*リスク現状レポート』

サイバー規制は、世界経済にとって有益になるものです。規制により、サイバーセキュリティとデータ保護のための標準化された枠組みが確立され、デジタル取引とサービスに対する信頼と自信が育まれます。これらの規制は、企業に強固なセキュリティとレジリエンシー対策を採用し、サイバーリスクを効果的に管理することを義務付けることで、重大な経済的損失や混乱の可能性を軽減する役割を担います。これにより、世界の金融市場とサプライチェーンの安定性とレジリエンスが促進されます。

その多くは常識的に聞こえるかもしれません。ですが、それらの規制が一貫性を欠いてパッチワークのように世界中に存在していたとしたら、新しい規制に準拠しようとするグローバル企業が直面する大きな課題を、無視することはできません。

世界中で事業を展開している大規模な多国籍金融機関に対する新たなサイバー規制の影響をもう一度考えてみましょう。類似するものと異なるものが混在する複数の規制基準に準拠することは、困難で複雑な作業です。また、企業の本社がサイバーポリシーのない国に拠点を置いているからといって、必ずしも企業やその顧客が影響を受けないわけではありません。

サイバー関連規制の取り組み

北米と南米

- 2023年12月 — 米国で、証券取引委員会がサイバーセキュリティのリスク管理、戦略、ガバナンス、インシデントの情報開示を施行
- 2024年上期 — OSFI（金融機関監督官庁）が、第三者リスク管理に関するガイドライン B-10 、テクノロジーとサイバーリスク管理に関するガイドライン B-13を更新し、施行
- 2024年上期 — ブラジルでは、サイバーセキュリティ規制およびサイバーセキュリティ機関法案を導入
- 2024年下期 — OSFIが運用の回復力と運用リスク管理に関する最終的なE-21ガイドラインを公開
- 2025 — カナダでは、規制当局がC-26（重要なサイバーシステム保護法）を施行予定

ヨーロッパ

- 2023年1月 — EU（欧州連合）で、欧州委員会がデジタルオペレーションレジリエンス法（DORA）と改正ネットワークおよび情報セキュリティ指令（NIS2）を制定
- 2024年下期 — EUで、DORAの規制技術基準、NIS2のリスク管理技術的詳細、コネクテッド製品のサイバーレジリエンス法、マネージドセキュリティサービス認証に関するサイバーセキュリティ法の改正、EU全体のサイバー対応の枠組みを構築するためのサイバー連帯法が最終決定されることが予想される
- 2024年10月 — EUで加盟国がNIS2を施行
- 2025年1月 — EUでは、ESA（欧州監督機構）がDORAを施行し、英国では、イングランド銀行、FCA（英国金融行為規制機構）、PRA（健全性監督機構）が金融サービスセクターにおける重要サードパーティの監督を行い、オペレーショナルレジリエンスとテスト要件を施行
- 2025 — 英国では、NIS規制を更新してマネージドサービスプロバイダーを含む新しい法律が制定されると予想されている

アジア

- 2024年上期 — シンガポールでサイバーセキュリティ法の改正の最終案が提出されることが予想される
- 2024年下期 — インドでは、デジタルインド法（サイバー要件を含む）が前進すると期待されており、オーストラリアでも規制当局が重要なインフラに重点を置いて既存の規制を強化する動きが見られる
- 2025 — 日本では、特にインシデント報告に関するサイバー規制の草案をデジタル庁が提出することが見込まれている

今後の予定は未確定

キンドリルの視点

政府や規制当局が新しいサイバーレジリエンス規制についての議論、その採用、施行を開始するにつれて、企業はサイバーセキュリティとレジリエンシーへの支出を優先せざるを得なくなってきています。そのためこの問題は、企業のテクノロジーリーダーや彼らが報告する役員会議の間で最も注目されている議題となっています。

そのため、情報通信技術に関連する混乱や脅威を**予測**し、**防御**し、**対応**し、**復旧**するための視点、専門知識、方向性を提供できるコンサルティングパートナーとの協力が、企業にとって差し迫って必要になっています。このような異なる視点は、これらの複雑な課題に適用する際に非常に貴重です。すべてのソリューションが、箱から取り出してすぐに適用できるわけではありません。

~2,500

セキュリティとレジリエンシーに関する経験を有し、訓練を受けたキンドリルのコンサルタント

7,000+

キンドリルの専門家が保有するセキュリティとレジリエンシーに関する認定資格と認証

568%

9か月間で投資額を回収することができるキンドリルのセキュリティ&レジリエンシーサービスへの投資に対する5年間のROI*

一般的に、政府が企業に求めるサイバー規制の枠組みの中でできることとして関心を持たれている基本的な要素は4つあります。

*出典: 『*The Business Value of Kyndryl Security & Resiliency Services*（キンドリルのセキュリティ&レジリエンシーサービスが提供するビジネス価値）』（*IDC、2023年7月*）

回復する力

規制当局は、企業が情報通信技術（ICT）システムの回復力を確保するための措置を講じることを注視しています。それは、サイバー攻撃、技術的な障害、自然災害などによる混乱を予防し、対応し、迅速に回復するための対策を講じることを意味する場合があります。

重要な論点:

そのステップはどのようなものか

- 定期的なバックアッププロセスの策定、強力なサイバーセキュリティ対策の実装、効果的なインシデント対応計画の策定、潜在的な脅威を継続的に監視するシステムの設定などを意味します。またサイバーセキュリティの現実的な視点として、攻撃が成功してしまうケースがあるものと想定した上で、そのような状況でもデータの整合性を保護し、運用の継続性を維持しながら、そのようなイベント中のダウンタイムを最小限に抑えることを最優先とするというレジリエンスの側面もあります。

透明性へのコミットメント

有害な出来事が実際に発生したケースでは、規制当局による情報開示要求は強くなります。このことが、多くのサイバー規制が企業にインシデント報告の体系的なプロセスを確立するよう求めている理由です。

重要な論点:

報告するべき内容と期限をどのように把握するか

- 通常、規制には報告が必要なインシデントの内容が明確に定義されたガイドラインが定められています。これらには、不正アクセス、データ侵害、システム障害、その他のサイバーセキュリティ関連の出来事などのインシデントが含まれることがあります。また、いつまでに報告する必要があるかという期限が設定されていることもよくあります。事態の詳細を調査する間に過ぎていく時間の中で、さらなる問題が引き起こされる可能性もあります。

どのような内容を報告する必要があるのか

- 第一に、規制当局は一般的に企業がインシデントを報告するための特定のチャネルまたはプラットフォームを確立することを求めています。これは、専用のメールアドレス、オンラインフォーム、安全なポータルなどを通じて行うことができます。第二に、タイムリーな報告です。規制では多くの場合、企業がインシデントを検知した後の特定の期間内にそれを報告することが義務付けられています。これにより、関連する利害関係者（規制当局、顧客、パートナーなど）にインシデントを迅速に通知することができます。

- 共有される情報には、通常、インシデントの性質と範囲、その潜在的な影響、影響を受けたシステムまたはデータ、問題を修正するために行われた取り組みを説明することが含まれます。

備えを怠らない

規制当局がサイバー規制の対象となる企業に対して望んでいるのは、リスクの概況に対する認識を持っていることです。そのためこれらの規則の多くにはリスク評価に関する特定の要件があります。これには、企業のデジタルシステムの運用上のレジリエンスに対する潜在的な脅威と脆弱性を体系的に評価することが含まれます。

重要な論点:

リスク評価には何が含まれるのか

- 従来のリスク評価には、いくつかの重要な要素があります。まず、重要なデジタル資産、システム、プロセスが潜在的に危険にさらされているかどうかをマッピングして理解することから始めます。そこから、企業はそれらの資産のセキュリティとレジリエンスを損なう可能性のある潜在的な脅威や脆弱性がどのようなものかを検討する必要があります。これには、サイバー攻撃、技術的な障害、人為的ミス、さらには自然災害も含まれる可能性があります。

- また、インシデント発生の可能性を減らしインシデント発生時の影響を軽減するための戦略と、実際にインシデントが起きた場合の対応プランを策定しておくことも重要です。また、継続的なモニタリングと見直しの仕組みを確立することも重要です。これは、脅威の状況が進化し続ける中で、各関連部署が必要に応じて戦略を適応させ、見直しするのに役立ちます。

- 一部の規制には、評価することだけでなく対応準備状況をテストすることも含まれています。規制当局が知りたいことは、企業が計画を策定して、それをテストしたこと、そしてそれが機能することです。企業は効果的に対処できることを証明しなければなりません。

- 組織が「何の」目的でリスクを評価する必要があるかを規定するほかに、規制では「どのくらいの頻度」と「誰が」評価を実施するかを明記する必要がある場合もあります。これらはすべて、企業運営全体、自動化基準などに影響する項目です。

防御に目を光らせる

強固なサイバーセキュリティ対策を維持することで、企業はデジタルサイバーレジリエンスを強化できます。デジタルシステムを保護するために、一連の慣行やポリシー、テクノロジを継続的に更新するプロセスが重要です。

重要な論点:

担うべき役割は何か

- この義務を遂行するための具体的な方法は多くあるため、この問いに対する答えは簡単に見失われてしまいます。これには、ユーザー認証手順や暗号化など、機密データへのアクセスを制御するメカニズムの実装が含まれる場合があります。マルウェアの感染やデータ侵害を防ぐためのエンドポイントセキュリティ対策の導入が含まれる場合があります。ネットワークセキュリティのために適切なファイアウォールを設定し、データのライフサイクル（保管、送信、廃棄を含む）を監視することも特に重要です。

- また、ここで重要なのは、企業のシステムやデータにアクセスできるベンダー、サプライヤー、パートナーに関連するサイバーセキュリティリスクを管理するのに役立つ第三者リスク評価です。

関係する企業リーダー

企業内では、ビジネスリーダーと技術リーダーが協力して、世界中で進化する規制基準への対応準備、実施、遵守を行う必要があります。共通の使命を共有しながら、それぞれの役割が問題に対しての独自の専門知識と視点をもたらす立場にあります。

COO

さまざまなサイバー規制への準拠による運用上の影響に関心を寄せています。これには、規制要件を日常業務に組み込むこと、コンプライアンスに関連するコスト、コンプライアンスが業務上のプロセスと効率、全体的な収益に与える影響などが含まれます。

CISO

主に、サイバー規制の技術的およびセキュリティ的側面、法律が企業の情報セキュリティ管理、データ保護ポリシー、サイバーセキュリティツール、サイバー脅威に対する全体的な回復力にどのように影響するかに焦点を当てます。

CTO

革新と技術の進歩をサポートしながら、技術戦略を規制要件に合わせることに重点を置きます。結局のところ、CTOは規制への対応が革新の妨げにならないようにしたいと考えています。

CIO

CIOは、企業の目標をサポートする情報システムの管理を含む、企業全体の情報戦略を監督する責任を負います。本質的に、CIOの関心は、企業のITが規制に準拠しつつ、ビジネス価値を継続的に高めることを保証することにあります。

CRO

進化する規制環境における彼らの主な役割は、変更によりリスク環境がどのような影響を受けるかを評価し、コンプライアンスに関連するあらゆる種類のリスクを特定して軽減することです。これは、リスク戦略をビジネス目標と整合させて価値を保護し、高めることを意味します。

サイバー規制対応の遂行

サイバーレジリエントな戦略を採用し、新しい規制の枠組みと連携するための第一歩は、企業が保護すべきものを明確に定義することです。つまり、ビジネス全体を調べて、**業務、財務、評判、規制の各分野にわたる影響とその意味するところを検討することです。**

インシデント発生時に問うべき質問

- **運用:** このサービスが停止することで、他にどのようなサービスが影響を受けるか。他の重要な組織に影響する可能性があるか。B2Bの顧客とパートナーにどのような影響を与える可能性があるか。
- **財務:** 特定のサービスがダウンしたことによる財務上の損失はどのくらいか。
- **評判:** 顧客ロイヤルティにどのような影響を与えるか。株価に影響するか。サービスのダウンタイムが顧客体験にどの程度影響するか。
- **規制:** サービスの中断によって、規制当局からどの程度の精査が行われ、罰金が科せられる可能性があるか。

脅威や危険を特定し、緩和策を実施するには、重要な資産を支えるビジネスの部分を明確に理解することが重要です。

多くの場合、マネージドサービスやコンサルティングパートナーが、企業の重要なインフラストラクチャーの主要コンポーネントを特定して支援できます。これには、システム、サービス、ネットワーク、人材、情報、その他の重要な要素が含まれます。

Step 1

経験豊富なパートナーと協力して、セキュリティとレジリエンシーのギャップを特定して評価します。規制コンプライアンスの戦略を立てます。

Step 2

新しい規制に準拠し、運用のレジリエンシーを向上させるソリューションを実装します。このアプローチには、ミッションクリティカルなITインフラストラクチャーをモダナイズすることも含まれます。

Step 3

規制対応とレジリエンス戦略を実装し、現状維持のためのプロセスを確立します。

必要なサイバーセキュリティ対策とプロトコルを実装することは、リソースが大量に必要となる可能性があります。場合によっては、テクノロジー、トレーニング、人材への多大な投資が必要になることもあります。従来それほど厳格でないもしくは異なる規制の下で運営してきた企業の場合は、包括的な新しい枠組みに適合するために、既存のシステムとプロセスをモダナイズする必要がある可能性があります。これは、サイバーセキュリティの専門知識が限定的で、新しい規制を解釈する準備が整っていない小規模な組織にとっては特に悩みの種となり、ましてや新たな運用上の課題に取り組むことは困難になります。新たな規制上の期待に応えるためには、協調的な取り組み、戦略的計画、第三者とのパートナーシップが必要となり、コンプライアンスの初期段階は非常に困難と思えるかもしれません。

企業が新しい規制に準拠できるよう支援するために、ITリーダーは次の支援を通じて効果的な対応を図ることができます。

経験豊富な専門家

キンドリルのスタッフは、最も複雑でミッションクリティカルなハイブリッドIT環境の保護と復旧に関して数十年にわたる専門知識を有しており、その専門知識とキンドリルのツールを通じて、主要なプロセスのビジネスへの影響を評価し、リスクと比較するための復旧作業をモデル化するお手伝いをします。また、さまざまなシナリオに定量的および定性的な重要なリスクを割り当てるサポートも提供します。

さらに、私たちは規制機関との連携を通じて、サイバー規制に関する世界的な対話に積極的に影響を与えています。私たちの専門家は、それぞれの視点と運用上の専門知識を共有します。

実績のあるパートナーシップ

最も複雑でミッションクリティカルな、そして規制の多いIT環境とアプリケーションには、多くの場合、モダナイゼーションへの最も包括的なアプローチが必要です。包括的なソリューションを手中に収めることにつながります。これは、ハイパースケーラーとの緊密な提携と、企業のIT資産に関する比類ない洞察と概要を提供するオープン統合プラットフォームであるKyndryl Bridgeなどへのアクセスによって可能になります。

新興テクノロジー

新しいサイバー規制への準拠は、人工知能を含む長期的なトレンドにより進歩した、強力な技術的なツールとソリューションによって支援されます。アドバンストデリバリー環境で導入された場合には、AIはリスク、費用対効果とケイパビリティへの評価を行いながら継続的なモニタリングとスタンダードと管理を更新します。

ツールとしては、企業のサイバーセキュリティのニーズと優先順位に依存せずにサポートするガイド要素、戦略、システム、制御の基盤を提供するように設計できます。これは、脅威からの保護と緩和のほか、脅威のパターンの特定、出現した新しい脅威について企業の技術リーダーへの警告、サイバーインシデント間のパターンの発見などを通じて行われます。

一般的に言えば、企業のサイバー規制対応戦略の一環としてAIが適合する主な領域は次の5つです。

脅威の検出と防止 — AIを活用したサイバーセキュリティシステムは、ネットワークトラフィックを継続的に監視し、異常を検出し、潜在的なセキュリティ脅威をリアルタイムで特定できます。AIは、リスクを事前に特定して軽減することで、企業が堅牢なセキュリティ対策を必要とする規制に準拠できるよう支援します。

コンプライアンス監視の自動化 — AIは、システムとデータリポジトリを自動的にスキャンすることでコンプライアンス監視を合理化し、企業が規制要件を遵守していることを確認できます。セキュリティ管理のギャップや穴を特定すると同時に、潜在的なポリシー違反を追跡し、サードパーティの監査人や規制当局にコンプライアンスを実証するためのレポートを生成できます。

リスク評価と管理 — AIを活用したリスク評価ツールは、膨大な量のデータを分析して潜在的な脆弱性を特定し、サイバーセキュリティ規制のコンプライアンスへの影響を評価できます。重大度と可能性に基づいてリスクに優先順位を付けることで、企業は問題が発生する前に阻止でき、リソース割り当てに関する重要な意思決定を導くことができます。

データ保護とプライバシーコンプライアンス — 機械学習や自然言語処理などのAIテクノロジーは、データ保護とプライバシーコンプライアンスの取り組みを強化するのに役立ちます。機密データの分類、アクセス制御の実施、プライバシー規制への準拠のためのデータ使用の監視、データ侵害の検出に役立ちます。

インシデント対応と修復 — セキュリティインシデントの検出、分析、修復を自動化し、対応時間を短縮し、侵害の影響を最小限に抑える能力は、AIが企業をサイバー規制に準拠させるのに常に役立つ方法です。セキュリティインシデントを迅速に封じ込めて解決することで、企業はコンプライアンスのリスクを軽減し、レポート作成要件をより効果的に満たすことができます。

おわりに

世界中の国々がサイバー規制を採用し実施するにつれて、あらゆる種類の企業が事業運営をコンプライアンスに準拠させ、レジリエンスを高める準備をしなければなりません。その作業は、経験豊富なパートナーを特定して連携することから始まります。それにより、セキュリティとレジリエンスのギャップを評価し、新しい規制に準拠して運用上のレジリエンスを向上させるためのソリューションを実装し、進化し続ける脅威環境を監視して対処するプロセスを確立できます。

新しい規制に先んじるために積極的に取り組む企業は、全体的なセキュリティ体制を改善し、データ侵害やサイバー攻撃の餌食になる可能性を減らすことができます。そうすることで、ステークホルダー間の信頼と評判を向上させ、顧客やパートナーとのより強固な関係が育まれます。さらに、コンプライアンス要件の一歩先を行くことは競争上の優位性にもつながり、サイバーセキュリティとデータ保護への取り組みを示すことにもなります。

総合的に見て、新たなサイバー規制への対応準備は、規制上の必要性に応える取り組みだけに留まらず、企業に数多くの利益と機会をもたらす戦略的な一手にもなるのです。

kyndryl