規制コンプライアンスの解明

セキュリティリーダーと
ITの意思決定者向け

はじめに

規制のフレームワークと基準は、情報技術の管理とデータの保護における課題と要件に対処する必要性から生まれました。これらのフレームワークと基準は時代の流れとともに進化してきただけでなく、テクノロジーの進歩と新たなサイバーセキュリティの脅威によって形作られてきました。フレームワークと基準の開発は、主に次の要因によって推進されてきました。

- **規制機関**は、各組織がサイバーセキュリティの実践に責任を持ち、特定の基準や規制に準拠する必要性を強調しています。
- **高度なサイバー脅威**はより頻繁に発生するようになっており、被害も増大しています。こうした脅威の多くには、かつては国家レベルの支援を受けた脅威のみに備わっていた洗練さが継承されており、現在ではそうした脅威が日和見主義者や「ハクティビスト」（政治的あるいは社会的な主張・目的のためにサイバー攻撃を行う活動家や集団）の手に渡っています。
- **社会や経済の機能に不可欠な重要インフラや必要不可欠なサービス**（医療、エネルギー、金融など）。これには、2022年3月に可決・署名された「重要インフラ向けサイバーインシデント報告法（CIRCA）」などの連邦法が含まれます。
- **異なるセクターや地域でのサイバーセキュリティ実践における**統一性の欠如。一貫性のないアプローチは、セキュリティとコンプライアンスの課題におけるギャップにつながる可能性があります。
- **2021年5月に米国大統領によって可決された**国のサイバーセキュリティの改善に関する大統領令 。

組織がサイバー脅威に対する回復力を保ち、ビジネス継続性を確保して中断から迅速に回復できる能力を維持しなければならないのは明白です。収集および処理される個人データの量が増加するにつれて、こうしたデータをサイバー脅威やデータ侵害から保護する必要性はますます高まっています。 サイバーインシデントは、経済的に重大な影響を及ぼし、経済的損失につながり、経済全体のデジタルサービスに対する信頼を損なうだけでなく、特に医療業界が標的となった場合、場合によっては命にかかわることもあります。

規制コンプライアンスは、組織の回復力を構築するうえで不可欠な要素です。リスクの全容を把握している企業は、コンプライアンスが単なるチェックボックスではなく、全体的なセキュリティ戦略の基本的な部分であることを認識しています。組織は規制を遵守してセキュリティのベストプラクティスを導入することで、ほとんどのサイバーインシデントに耐えて迅速な回復を可能にする態勢を整えることができます。このアプローチによって、危機に直面したときに、迅速な復元のための基盤がすでに整っていることが保証されます。

1.

サイバー攻撃


CYBER SECURITY
Username
Password
Remember me
LOGIN
Forgot password

企業のデジタルインフラストラクチャが攻撃を受けた場合、その影響はデータの損失だけにとどまらず、さらに広範囲に及ぶ可能性があります。ダウンタイムの影響、中核機能の喪失、販売の中断の可能性、組織がどのように認識されているかはすべて、サイバーインシデントの潜在的な結果です。

私たちは、こうした可能性により引き起こされる生活への影響について、常に留意しておく必要があります。特に金融サービス業界（FSI）およびヘルスケア業界（HC）では、請求書や支払い、その他の重要なサービスの中でも特に医療へのアクセスに影響するなど、サイバー脅威は、個人レベルで人生を大きく変えてしまうほどの影響を及ぼす場合があります。こうした懸念やリスクは、組織が業界規制のコンプライアンスに準拠することで自身のセキュリティ体制を改善するための十分な理由となります。

コンプライアンスが重要な理由

コンプライアンスには、組織の業界や地域に適用される法律と規制の遵守が含まれます。コンプライアンスを遵守することで、身代金の支払いによる収益の損失から運用の中断、侵害によるデータの暴露、規制上の罰金、風評被害まで、ビジネスへのさまざまな影響を軽減することができます。コンプライアンス基準は急速に変化しており、今後も変化し続けるでしょう。現在の目標を達成するために今日策定された規制は、将来機能しなくなる可能性があります。新しいフレームワークや規制、そしてそれらの新たな期待事項に遅れずについていくことは、組織を保護するための確実な方法と言えます。

規制とフレームワーク

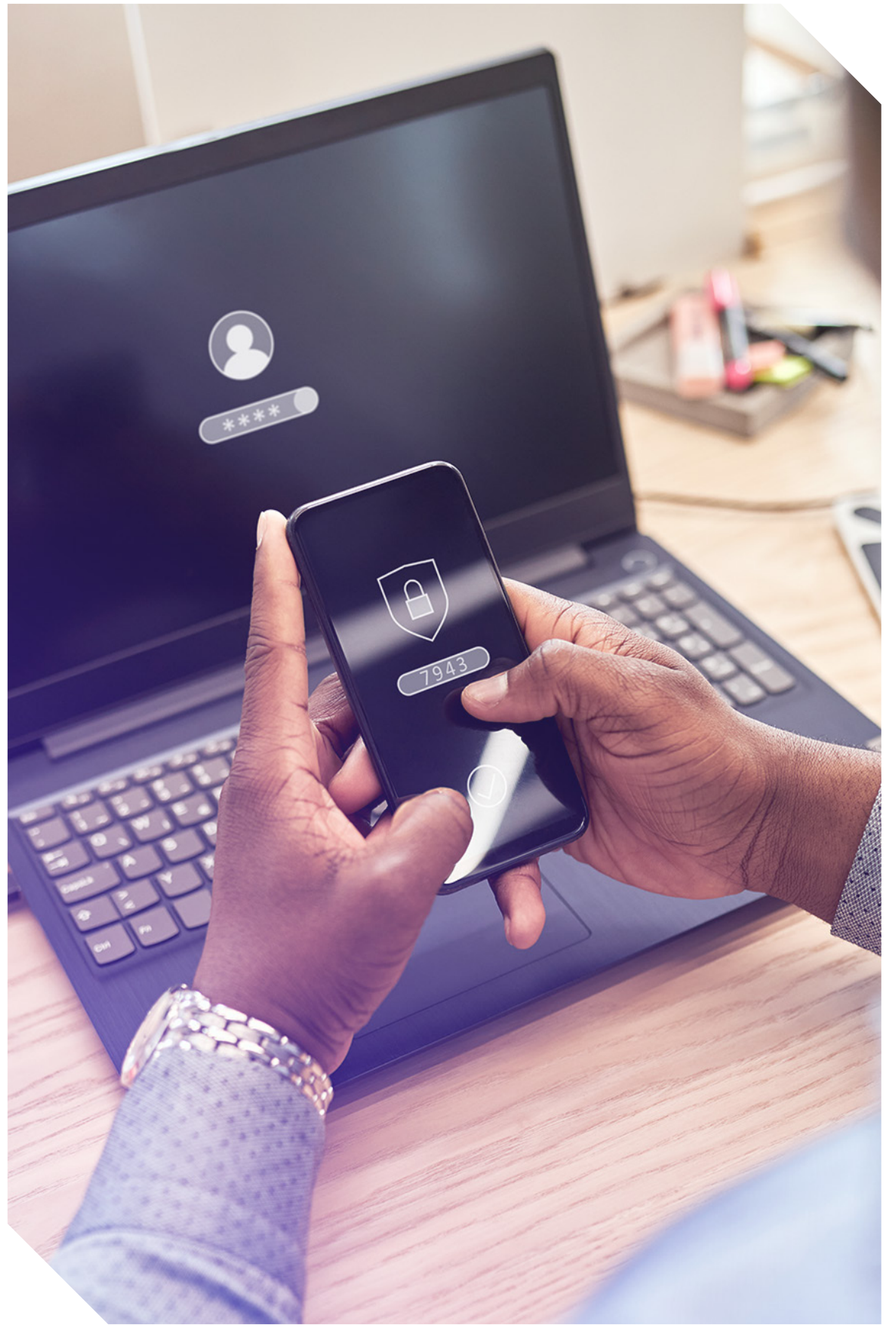
規制とフレームワークの根本的な違いはそれぞれの目的にあります。フレームワークは、組織がサイバーセキュリティ体制を管理および改善するために使用できる一連の構造化されたガイドライン、ベストプラクティス、および標準を提供します。これとは異なり、規制とは、組織全体にサイバーセキュリティ慣行の最低基準を適用するために政府または規制機関によって課される法的要件です。広く使用されている規制には、次のようなものがあります。

- **GDPR**（一般データ保護規則） — データ保護とプライバシーに関する欧州連合の規制。
- **HIPAA**（医療保険の相互運用性と説明責任に関する法律）— 医療情報を保護するための米国の規制。
- **SOX**（Sarbanes-Oxley Act） — 金融慣行およびコーポレートガバナンスに関する 米国の規制。
- **PCI DSS**（ペイメントカード業界データセキュリティ基準）— クレジットカード取引を保護するための基準。
- **FISMA**（連邦情報セキュリティマネジメント法）— 政府の情報を保護するための米国の法律。

このような規制は、フレームワークと連携して機能します。たとえば、フレームワークが規制準拠の基盤を築く一方で、規制はフレームワークの採用を促進します。また、フレームワークは、組織が最低限の規制要件を超え、コンプライアンスと監査を容易にすると同時に、規制によりセクター全体で一貫したベースラインセキュリティを確保するのに役立ちます。広く使用されているフレームワークには、次のようなものがあります。

- **NISTサイバーセキュリティ フレームワーク（CSF）** — サイバーセキュリティ リスクを管理するための包括的なアプローチを提供します。
- **CIS Controls** — サイバー脅威から防御するための一連のベストプラクティス。
- **COBIT** — サイバーセキュリティを含むITの管理目標に重点を置いた、IT管理とガバナンスのためのフレームワークを提供します。

フレームワークはサイバーセキュリティを管理するためのベストプラクティスを提供するもので、規制はセクター全体に対してベースラインのセキュリティを確保するための最低限の基準を適用するものです。



リスク管理とコンプライアンス

リスクベースのアプローチは徹底的なリスク評価から始まります。このプロセスには、セキュリティチーム、IT担当者、法律の専門家、ビジネスリーダーなど、さまざまな利害関係者からの意見を含める必要があります。

たとえば医療機関の場合、電子カルテ（EHR）データの機密性の高さと、患者データの損失やHIPAAに基づく規制上の罰金といった違反による潜在的な結果から、このデータの保護を最優先事項として特定することがあります。EHRセキュリティを優先することで、プロバイダーは、最も重要なリスクを軽減する制御の実装にコンプライアンスの取り組みを集中させることができます。

規制要件が複雑化し続ける中、組織は、コンプライアンスプロセスを合理化し、可視性を高め、継続的な監視と改善を確実にするために、ガバナンス、リスク管理、コンプライアンス（GRC）ツールにますます目を向けています。

コンプライアンスに対するリスクベースのアプローチにより、各組織固有のリスクに合わせてセキュリティの取り組みを調整し、重大な脅威が優先されるようにします。

GRCツールとその利点の概要：

GRCツールは、ポリシーの策定、リスク評価、監査追跡、インシデント対応など、コンプライアンスのさまざまな側面の自動化と管理を支援するよう設計されています。これらのツールには、いくつかの主な利点があります。

- **一元化されたコンプライアンス管理：**GRCツールを使用すると、組織はコンプライアンス活動を単一のプラットフォームに統合できます。
- **コンプライアンスタスクの自動化：**GRCツールは、アクセスログの監視や監査レポートの生成など、日常的なコンプライアンスタスクを自動化することで、貴重な時間を解放します。
- **向上した可視性とレポート機能：**GRCツールによってコンプライアンス状況がリアルタイムで可視化されるため、セキュリティリーダーは進捗状況を追跡してギャップを特定し、規制当局や監査人に対してコンプライアンスを実証することが容易になります。
- **継続的なモニタリングと改善：**GRCツールはコンプライアンス関連のアクティビティの継続的な監視をサポートし、組織が問題を反応的ではなく積極的に特定して対処できるようにします。

2.

コンプライアンス規制の導入が重要である理由

組織が抱えるリスクを理解してそれらを考慮に入れる際のポイントは、欠点を見つけることではありません。むしろ、組織が保護し、前進できるように、事実を見つけることが重要です。経営幹部には組織のサイバー回復力が整っているように見える場合でも、実際はそれとは大きく異なってリスクにさらされているという可能性もあります。

取締役会レベルの関与とコミットメントを確保することが、コンプライアンスを達成するための主な方法です。組織は、リスクを軽減するために、組織全体でコンプライアンスの文化を醸成する必要があります。経営陣は、規制に従ってプロセスとテクノロジーを実装する責任があります。一歩引いて、業界と地域における法律や規制を組織が遵守していることを確認することが重要です。

業界が成長し、変化し続けるにつれて、コンプライアンスと規制の基準がどのようなものになるかも変化します。しかし、組織がコンプライアンスに遅れをとると怠慢になるリスクが生じ、執行役員や取締役が懲罰的措置を受ける可能性があるため、そうした状況は避ける必要があります。停止やランサムウェア攻撃 、金銭的なペナルティや風評被害が生じる可能性があります。しかし、さまざまな規制コンプライアンスに準拠するという点で、組織の成熟度が高まるにつれて、より迅速な回復が可能になる可能性が高まります。

コンプライアンスをグローバルレベルで確保

世界のサイバー関連の法制を見ると、150以上の国々が何らかの形でサイバー関連法を導入しています。たとえば、EUのDORAや英国のNIS/NIS2などがあります。また、日本にはFSAが、中東地域にはNESAおよびDIFCデータ保護法が存在します。世界的に各国はNIST（米国国立標準技術研究所）を参考にすることができます。 米国の人々であれば、ランサムウェアと規制上の罰金というと米国証券取引委員会（SEC）を思い浮かべるでしょう。さまざまな規制オプションが幅広く存在するにもかかわらず、主要なインフラ規制を持つ国は100カ国未満です。これは、多くの国が、これらの重要なインフラ環境に焦点を当てる必要性が非常に現実的であるにもかかわらず、高いレベルでセキュリティに対処していないことを示しています。研究とバイオテクノロジーを含む医療業界を具体的に見てみると、国によってルールが異なることがよくあります。

コンプライアンス規制により、組織はサイバーインシデントに備えることができ、セキュリティ文化を醸成するためには取締役会レベルの関与が不可欠です。

金融サービス業界とヘルスケア業界の違い

米国では、重要インフラ向けサイバーインシデント報告法（CIRCA）により、さまざまな規制に準拠しなければならない16の重要産業が指定されています。重要な産業について考えるとき、人々は通常、ダム、送電網、そしてもちろん医療を思い浮かべます。医療と金融サービスは 世界中の人々の日常生活において重要な役割を果たしています。セキュリティコンプライアンスの欠如が医療機関に及ぼす可能性のある悪影響を見ると、それが人々の生活を脅かすものであることがわかります。

HIPAAは、人々が医療コンプライアンスを考えるときに頭に思い浮かべる主な規制の一つです。HIPAAプライバシー規則は、特定の健康情報の保護に関する国家基準を確立し、HIPAAセキュリティ規則は、電子形式で保持または転送される特定の健康情報を保護するための国家セキュリティ基準を確立します。医療機関が適切に保護されていない場合や、コンプライアンスに準拠していない場合は、ランサムウェア攻撃を受けた際に患者のデータが侵害されるリスクが生じます。

金融業界では、主な規制の一つがGLBA（グラムリーチブライリー法）です。この法律は、ローン、金融または投資アドバイス、保険などの金融商品またはサービスを消費者に提供する金融会社に、情報共有慣行を顧客に説明し、機密データを保護することを義務付けています。金融会社がフレームワークや規制を遵守していない場合は、重大な経済的損失、罰金、経済的安定性への悪影響、風評被害といった潜在的なコストに直面するリスクがあります。

組織は、コンプライアンスを維持し、進化するサイバーセキュリティの脅威に先手を打つために、新しい規制に継続的に適応する必要があります。

3.

ベストプラクティスの推奨事項と導入

コンプライアンスは、1回限りの考慮事項ではありません。法的要件は不変的なものではなく、新たな脅威が出現し、規制が更新されるにつれて経時的に進化します。そのため、すべての重要なフレームワークと規制を常に把握するために、実装すべきベストプラクティスがいくつかあります。

継続的な監視

継続的な監視は、効果的なコンプライアンス管理の重要な要素です。GRCツールは、SIEM（セキュリティ情報およびイベント管理）システムなどの既存のセキュリティインフラストラクチャと統合し、コンプライアンス状況をリアルタイムで追跡することで継続的な監視を促進します。

たとえば、SOXの対象となる金融サービス会社は、GRCツールを使用して金融システムへのアクセスを継続的に監視し、許可された担当者のみが機密性の高い金融データにアクセスできるようにすることができます。組織は、GRCツールをサイバーセキュリティ戦略に統合することでコンプライアンスの取り組みを合理化し、コンプライアンス違反のリスクを軽減して、法的要件と同時にセキュリティ関連の慣行を進化させることができます。

定期的な監査と評価

攻撃を受けた際は、インシデント対応計画の有無ではなく、その計画がうまく機能するかどうかが問題となります。計画が期待どおりに機能することを確認しておく必要があります。これを確実にするための最良の方法の一つはテストを行うことです。組織の計画をテストして、それにパスすることを実証することが、十分なレベルのコンプライアンスの確保につながります。

コンプライアンスに向けた主なステップ

組織がコンプライアンス遵守に向けてどのような規制を実装できるかを検討する際は、全体的なアプローチを保つことが重要です。組織のあらゆる部分が、環境のさまざまな側面に密接に関わっている可能性があるためです。組織のコンプライアンスを確保するうえで、プランニングと事前の考慮が大きな役割を果たします。検討すべき手順には、次のようなものがあります。

- **リスク管理プロセスの開発：**これには、ビジネスに影響を与える可能性のあるすべての潜在的なITリスクの特定と、脆弱性の評価が含まれます。
- **リスクの分析と優先順位付け：**これは、リスク軽減戦略の策定とスタッフのトレーニングを通じて達成できます。
- **インシデント対応計画の策定：**この計画では、環境の可視性と洞察を保ちつつ、リスク移転などについて検討することができます。
- **セキュリティ文化の確立：**これは、関連するすべての利害関係者を巻き込み、適切なテクノロジーを選定して、文書化を忘れないようにすることです。

リスク管理プロセスを開発してリスクに優先順位を付け、コンプライアンスを維持して回復力を強化するためのセキュリティ文化を確立します。

まとめ

今後、規制コンプライアンスはレジリエンス（回復力）に重点が置かれ、組織は新しい規制を予測し、適応性のあるプロアクティブなコンプライアンスプログラムを構築する必要があります。

規制環境は動的なものであり、特に政府や規制機関によるテクノロジーの急速な進歩への対応もあるため、規制変更のペースが減速する可能性は低いと考えられます。このことを念頭に、組織はセキュリティフレームワークを適応させて規制コンプライアンスに継続的に準拠する必要があります。第二の目標としては、セキュリティのベストプラクティスを標準化して、組織が許容できるセキュリティ体制を整えることが挙げられます。

結論として、規制コンプライアンスへの準拠は、継続的な取り組み、適応、コラボレーションを必要とする現在進行形の取り組みです。

単にコンプライアンスを達成するだけでは十分ではなく、組織は進化する脅威や規制に向き合い、コンプライアンスプログラムの維持と強化に努める必要があります。このプロセスではセキュリティリーダーとITの意思決定者が重要な役割を果たし、罰則や罰金を回避するだけでなく、より強力でサイバー回復力のある組織の構築を目的としたコンプライアンス戦略に向けて組織を導きます。組織は、コンプライアンスを組織の業務と文化に統合し、変化に直面しても常に最新情報を入手して俊敏に対応することで、自信を持って複雑な規制環境をうまく乗り切ることができます。