攻めのデジタル活用：CISO Cyber Conciergeで実現する法規制モニタリング支援

PwCコンサルティング合同会社
ディレクター　**上杉 謙二**

はじめに

デジタルトランスフォーメーション（DX）や人工知能（AI）などの最新技術を活用することで、日々の業務を効率化し、労働生産性を向上できます。このような「攻めのデジタル活用」は、業務の品質向上と時間の短縮というメリットをもたらし、企業活動を支える重要な要素になりつつあります。

特に、国内外で増加傾向にあるサイバーセキュリティ関連の法規制やガイドラインのモニタリング業務にデジタル技術を活用すれば、企業は準拠すべき法令をタイムリーに把握し、必要な対応を行うことができます。現在、日本を含む世界各国において、サイバーセキュリティ関連の法令・ガイドラインが急速に増加しています。その数は、2020年と比較して10倍以上に増加しており[※1]、法令違反時には高額な制裁金を科される恐れがあるため、企業は該当する法規制を確実に把握し、法令に準拠する必要があります。

現在、法規制のモニタリングを支援するデジタルサービスが注目されています。企業単独で法令を調査するよりも専門の会社に任せたほうが効率的です。調査する法規制は複数社で重複するため、専門会社がそれらの情報を集約すれば、より深い知見を蓄積しやすくなります。PwCは、デジタルプロダクト「CISO Cyber Concierge」を提供しており、世界各国・地域のセキュリティ関連法規制やガイドライン、サイバー攻撃、情報プライバシーに関する最新情報を提供し、企業が効率的に法規制モニタリングを行えるよう支援しています。

本稿では、サイバーセキュリティ関連の法規制対応における課題を挙げ、どのようにデジタルプロダクトが課題解決に役立つかを紹介します。なお、文中の意見は筆者の私見であり、PwCコンサルティング合同会社および所属部門の正式見解ではないことをお断りします。

※1　PwC「Digital Trust Insights 2025」
https://www.pwc.com/jp/ja/knowledge/thoughtleadership/digital-trust-insights2025.html

1 サイバーセキュリティ関連の法規制対応の課題

多くの国でサイバーセキュリティに関する基本的な法制度が制定されています。例えば、日本のサイバーセキュリティ基本法や欧州連合（EU）のNIS2指令（Network and Information Systems Directive 2）などがあります。それに加えて近年では、重要インフラのセキュリティ、製品セキュリティ、データの越境移転、サイバーインシデントの当局報告などの法規制の整備が各国で進行しており、この傾向は今後も継続すると考えられます。

特に最近は、IoT（Internet of Things）に関する法規制が進んでいます。その背景の1つとして、政府や重要インフラでのIoTの普及が進み、製品セキュリティの基盤となる法規制や認証制度が必要になってきたことが考えられます。製品セキュリティに関する代表的な法規制が、EUのCRA（Cyber Resilience Act）とEUデータ法です。どちらも、多くの企業にとって対応が迫られています。

特にCRAは製品のセキュリティ対策に加え、ぜい弱性対応も必須要件となっています。主要な要件として、セキュリティ設計をはじめとする技術文書の10年間保管、サードパーティコンポーネントのセキュリティ保証、上市後最低5年間のぜい弱性対応、インシデント時の24時間以内の当局報告義務などがあります。

EUデータ法では、IoT機器を使用することから生成されるデータが広く対象となっており、製品利用者はデータへのアクセス、第三者との共有などの権利を有すると定めています。そのため、従来のIoT製品の設計またはビジネスモデルの再考を促す内容になっています。

IT環境が複雑化・多様化するにつれて、新しい脅威が出現し、その脅威に対抗するために法規制が拡充されるという流れが今後も継続すると考えられ、企業の担当者にとっても、世界中で制定されるサイバーセキュリティ関連の法規制への

対応が新たな重要課題となりつつあります。

企業は進出国・地域のサイバーセキュリティ関連の法規制を遵守しなければなりません。そして、それぞれの法規制において、特定時点までに遵守しなければならない義務は何か、遵守計画を作れば足りるものは何か、あるいは努力義務は何かを明確に把握した上で対応する必要があります。しかし、各国・地域の動向を継続的にモニタリングして対応することは、多くの企業にとっては高いハードルになります。

PwCは企業の法規制対応の実態を把握するため、日本企業においてサイバーセキュリティの意思決定や企画に携わる300人にサイバーセキュリティ法規制への対応についてアンケート調査を実施しました。まず、サイバーセキュリティ関連の法規制のモニタリングを行う部門について尋ねました（**図表1**）。

回答からは、以下3点の傾向が確認できました。

1. グローバルのサイバーセキュリティ関連法規制をモニタリングしている部門として、IT部門（30.3%）とセキュリティ部門（20.0%）が多いことがわかりました。これらの部門は法令モニタリングを専門としている部門ではないため、主担当の業務との兼務で法令モニタリングをしていると考えられます。
2. 法規制モニタリングの従来の主担当と想定される法務・コンプライアンス部門（13.9%）において、グローバルのサイバーセキュリティ関連法規制のモニタリング関与度が高くありませんでした。その原因としては、モニタリングリソースの不足、サイバーセキュリティに関するナレッジの不足が考えられます。
3. 外部専門家を使ったモニタリングは3.2%と、ごく少数でした。専門家を活用した体系的な法規制モニタリングではなく、自社リソースでモニタリングを実施しているか、実態としてモニタリングができていない可能性が考えられます。

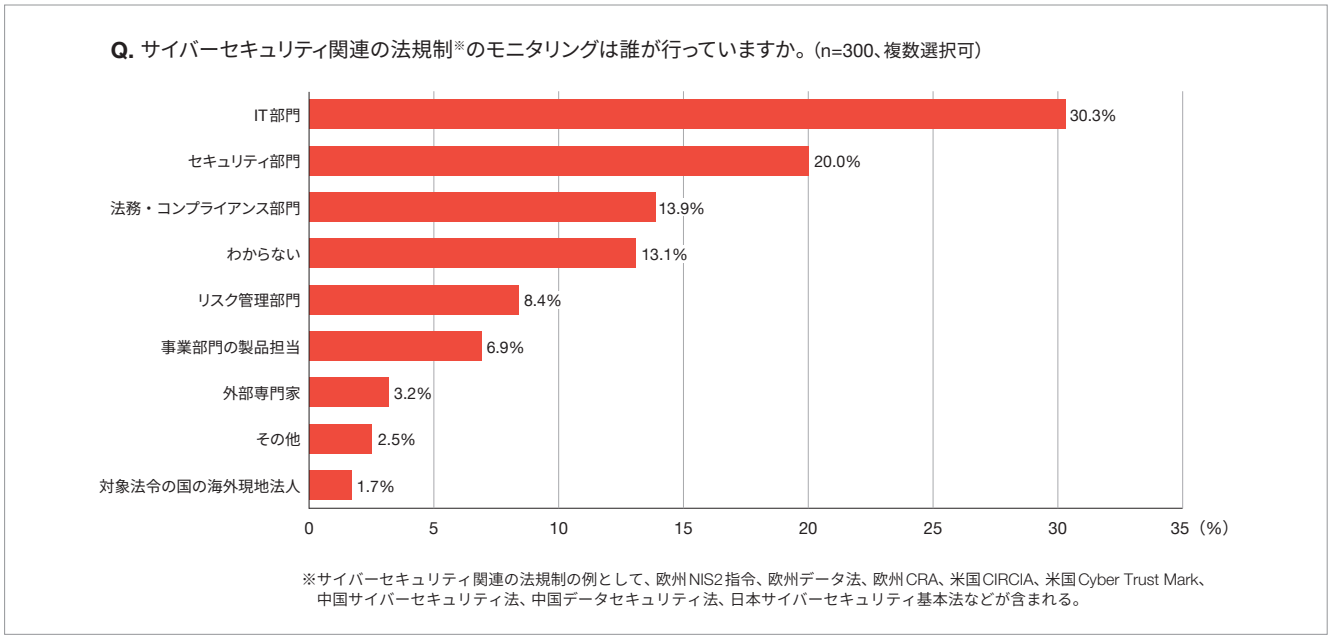
また、サイバーセキュリティ関連の法規制のモニタリングおよび対応を行う上での最大の課題を尋ねました（**図表2**）。

モニタリングにおける最大の難しさとしては、以下の2点が示唆されました。

1. 「法規制対応人材（リソース）不足」（22.7%）が最も大きく、モニタリングできる人材や部門が不足していることを示しています。
2. リソース不足に次いで、「モニタリング対象の法令の自社への影響の解釈」（16.7%）、「モニタリング対象の法令の選定」（14.0%）が高いのは、法規制モニタリングできているとしても、その後の解釈で自社への影響を判断することにも課題があることを示しています。

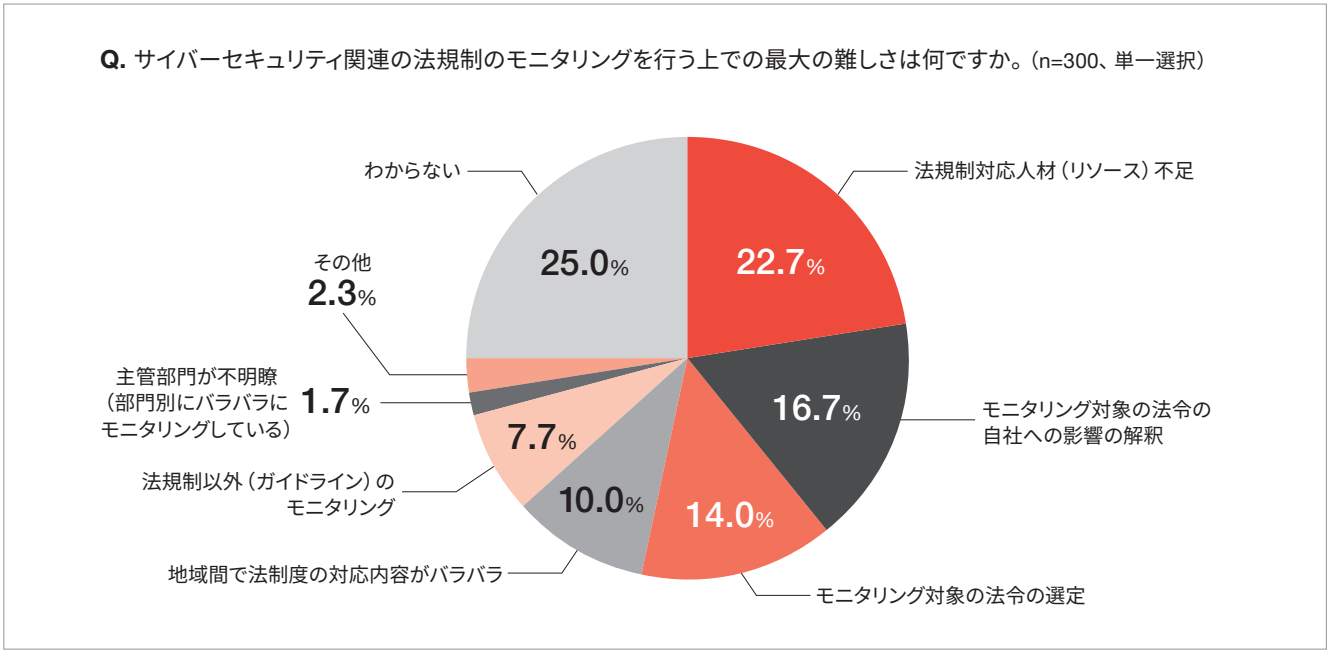
このように「グローバル」「サイバーセキュリティ」「法規制」という複合的スキルが求められる人材を社内で持ち、情報シ

図表1：サイバーセキュリティ関連の法規制に対応している部門



出所：PwC「2025年 CyberIQ調査」 https://www.pwc.com/jp/ja/knowledge/thoughtleadership/2025/assets/pdf/cyber-iq-survey2025.pdf

図表2：サイバーセキュリティ関連の法規制のモニタリングにおける難しさ



出所：PwC「2025年 CyberIQ調査」

ステムや製品をグローバルサイバーセキュリティ法規制に対応させることは、単独の企業で対応するのは非常に困難であることが調査から判明しました。事業を展開している国・地域のサイバーセキュリティ関連の法規制や政策動向に詳しい専門家を活用したモニタリング体制を整え、自社や製品・サービスに対する影響を分析し、専門家のサポートをもとに対応することを推奨します。

2 CISO Cyber Conciergeとは

CISO Cyber Conciergeは、世界各国・地域のセキュリティ関連法規制やガイドラインの最新情報を提供するウェブサービスです（**図表3**）。独自のデータベースには、米欧や中国、東南アジアなどの最新規制動向が更新され、約200本のサイバー関連のインサイトやレポートも随時追加されています。チャット機能を通じて質疑応答が可能で、専門家からの回答内容を閲覧することができます。

サービスは、主に次の6つの機能で構成されています。

① **PwC Knowledge**：サイバーセキュリティや関連ルール、企業の取り組み事例に焦点を当てたインサイトやレポートを提供
② **Global Security Regulation**：デジタル技術に関連する世界の法制動向を網羅
③ **Cyber Incident**：世界各国で発生したサイバー攻撃事例を週次で更新
④ **Vulnerability Report**：デジタル製品のぜい弱性情報をリアルタイムに提供
⑤ **Cyber Intelligence**：サイバー攻撃と地政学的リスクの分析レポートを提供
⑥ **Inquiry List**：質問者からの相談内容と質問への回答を一覧化

サービスの特徴は、サイバーセキュリティやプライバシーに関する相談や調査依頼をウェブブラウザで受け付けることです。これにより、ユーザーは迅速かつ効率的に専門家のアドバイスを受けることができます。また、PwCの過去の実績やグローバルの知見を生かし、月例ミーティングなどを通じて最新のサイバーセキュリティ法規制動向を提供することも可能です。

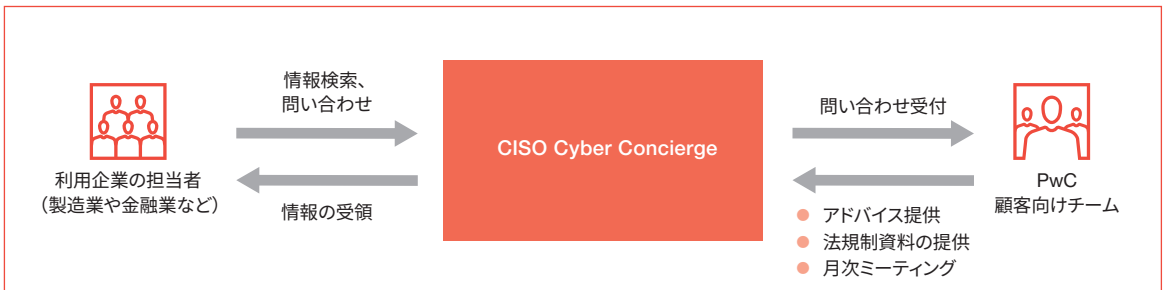
3 CISO Cyber Concierge導入事例

本サービスは、日本の製造業や金融業をはじめとする多くの企業に利用されています。具体的な課題として、本社の情報セキュリティ部門や製品セキュリティ部門が海外のサイ

図表3：CISO Cyber Conciergeの画面イメージ

出所：PwC「CISO Cyber Concierge」

図表4：CISO Cyber Conciergeの利用イメージ



出所：PwC作成

バーセキュリティ法規制の調査を行う際、リソースに限界があると感じている企業が多くありました。そこで、法規制のモニタリングを目的として、PwCのCISO Cyber Concierge を採用しました。導入企業からは、「欧州の動向が目まぐるしく変わる中、最新情報をタイムリーに知ることができた」「自社が準拠すべき法規制に関して、抜け漏れがないか確認できた」といった声が寄せられています。

CISO Cyber Concierge は月額50万円から利用でき、最新の知見や業界動向を常に更新し、サービスの拡充を進めています。また、過去の実績やPwCグローバルネットワークの知見を活用し、サイバーセキュリティやプライバシーの専門家からのアドバイスを提供します（**図表4**）。今後は、デジタル関連の法規制やガイドラインのリアルタイムモニタリングを生成AIによる分析と融合させることで、デジタル分野における法規制対応支援サービスを強化していきます。

4 おわりに

国内外のサイバーセキュリティ法規制の増加に対して、一企業が単独で法令を調査することは容易ではありません。企業は、サイバーセキュリティ関連の法規制や政策動向に詳し

い専門家を活用したモニタリング体制を整え、自社や製品・サービスに対する影響を分析し、専門家のサポートを得て対応することが求められますが、非常に多くのリソースが必要です。

そこで、「攻めのデジタル活用」が必要となります。PwCは、デジタルプロダクト「CISO Cyber Concierge」を提供することで、企業が法規制モニタリングを効率的に行えるよう支援しています。企業は、最新の知見を効率的に収集でき、法令遵守を円滑にできるようになるため、費用対効果を高めることができます。

このように、デジタル技術を活用することで、企業はビジネスの課題を効果的に管理し、持続可能な成長を実現するための基盤を築くことができます。今後、攻めのデジタル活用は、競争力を維持向上するために必須となるでしょう。

上杉 謙二（うえすぎ けんじ）
PwCコンサルティング合同会社　ディレクター
入社以前は、国内通信会社や外資系セキュリティ会社において、セキュリティサービスの製品責任者として製品開発やプリセールス活動に従事。現在、デジタルトラスト部門ナレッジセンターのリーダーとして、グローバルの知見をクライアントなどに提供している。また官公庁や民間企業を対象にしたサイバーセキュリティ戦略立案、サイバー演習、インシデント対応支援、M&A戦略策定に従事している。
メールアドレス：kenji.uesugi@pwc.com