サイバーセキュリティ主要課題2025：エネルギーセクター

「サイバーセキュリティ主要課題2025：エネルギーセクター」における主なポイント

地政学的リスクとサイバー脅威が高まる環境下では、脆弱性管理を単なる技術的な対応にとどめるのではなく、ビジネスの観点に立ち返り、組織への潜在的な影響を踏まえたうえでリスクを判断・優先する「リスクベースのアプローチ」を導入することが重要です。

ITとオペレーショナル・テクノロジー（OT）の融合が進むなか、最高情報セキュリティ責任者（CISO） には、ITとOTの間に長らく存在してきたサイロ型の組織文化を打破し、両チームの緊密な連携を促進することで、持続可能なレジリエンスの構築にむけ、中心的な役割を果たすことが求められています。

CISOには、ITセキュリティ業務を超えて、組織全体のデジタル意識を高めるという「サイバーエバンジェリスト」と、環境変化に柔軟に対応しながら、セキュリティ戦略を継続的に適応・進化させていく「レジリエンスと、俊敏性を備えたセキュリティ・フレームワークの設計者」へと進化することが期待されています。

世界のエネルギー・化学企業におけるセキュリティの在り方は、最高情報セキュリティ責任者（CISO）の役割拡大、スマートデバイスやIoT機器の急増、そしてレジリエントな企業文化やネットワーク環境の構築の必要性など、さまざまな要因を背景に、大きく変貌を遂げています。このように複雑性と相互依存性が増す環境のなかで、多くのCISOは、従業員のデジタル意識をこれまで以上に高めるという新たな課題と機会に直面しています。そして、その実現に向け、CISO自身にも、「サイバーエバンジェリスト（伝道師）」としての役割を果たし、組織のあらゆるレベルで意識を行動へとつなげる働きかけが求められています。

エネルギー・化学セクターにおけるCISOの役割は、もはや従来のITセキュリティ分野にとどまりません。KPMGの調査によれば、「今後3年間でサイバー犯罪およびサイバーセキュリティの脆弱性が組織の成長に影響を及ぼす」と懸念するエネルギー・化学企業のCEOの割合は、約70%に上ることが明らかになっています[1]。こうした状況で、ITとオペレーショナル・テクノロジー（OT）の融合が進むなか、CISOには、経営から生産現場に至るまで、企業全体のテクノロジーエコシステムを包括的に保護するという重い責務が課されています。

このような責任の拡大に伴い、CISOには、サイバーセキュリティが事業に与える影響を経営幹部に的確に伝え、適切な予算を確保するとともに、組織全体にレジリエンス（回復力）の文化を根付かせるといった、新たなスキルセットが求められています。実際に、KPMGの調査によると、技術投資の意思決定プロセスの初期段階からサイバーセキュリティの取組みを実施していると回答したエネルギー・化学企業は59%に上り、CISOが組織の中核として重要な影響力を発揮し、サイバーセキュリティが全社的に浸透しつつあるという前向きな変化が見られます[2]。

ただし、 エネルギー・化学業界の特性が、CISOが直面する課題をさらに複雑化させているのも事実です。エネルギー・化学業界は、欧州のNIS2指令（NIS2）やAI規制法、北米のNERC CIPなど、テクノロジー、サイバーセキュリティやその他サイバー環境に関する複雑かつ厳格な規制の対象となっています。CISOには、これらのコンプライアンス要件を遵守しながら、組織やステークホルダー、さらには社会全体に壊滅的な影響を及ぼしかねない地政学的リスクや増加するサイバー攻撃の脅威にも同時に対処することが求められているのです。

実際、2024年4月には、北米電力信頼度協会（NERC）により、米国の電力網における脆弱なポイントが1日あたり約60ヵ所のペースで増加している旨が報告されています[3]。また欧州では、2023年5月にデンマークの重要インフラが過去最大規模のサイバー攻撃を受け、わずか数日間で22社が被害を被り、一部の企業は、インターネットから完全に遮断された「アイランドモード（孤立運転モード）」への移行を余儀なくされました[4]。

このように地政学的リスクとサイバー脅威が高まる環境下では、CISOには、積極的かつ戦略的な思考・判断が求められます。すなわち、脆弱性管理を単なる技術的な対応にとどめるのではなく、ビジネスの観点に立ち返り、組織への潜在的な影響を踏まえたうえでリスクを判断・優先する「リスクベースのアプローチ」を導入することが重要となります。さらに、CISOは、このような戦略的リーダーシップを発揮するのみならず、ITとOTの間に長らく存在してきたサイロ型の組織文化を打破し、両チームの緊密な連携を促進することで、持続可能なレジリエンスの構築においても中心的な役割を果たすことが求められます。

1.KPMG, エネルギー・化学業界インサイト：KPMGグローバルCEO調査2024
2.KPMG, エネルギー業界インサイト：KPMGグローバルテクノロジーレポート2024
3.Industrial Cyber, Critical infrastructure faces 30 percent surge in cyber attacks, KnowBe4 report highlights, August 28, 2024.
4.SektorCERT, The attack against Danish critical infrastructure, November 2023

CISOが直面するサイバーセキュリティの主要課題

進化し続けるCISOの役割

規制当局による監視の強化と、サイバーセキュリティの戦略的重要性の高まりを背景に、CISOは、説明責任の増大だけでなく、場合によっては個人としての賠償責任リスクにも直面しており、組織における強力なサイバーセキュリティ成果を実現することへのプレッシャーは、これまで以上に高まっています。また、最近では、物理セキュリティや不正対策は最高セキュリティ責任者（CSO）、ボーダーセキュリティやアイデンティティ・アクセス管理（IAM）はITインフラ部門、プライバシーは最高データ責任者（CDO）が担当するなど、セキュリティとプライバシーのさまざまな側面が、他のビジネスリーダーの管轄下に置かれるようになり、従来のCISOの機能は、ますます分散化しつつあるのが実情です。

こうしたなか、CISOには、自身の役割や責任の範囲を明確にし、他の部門のリーダーと連携しながら、「責任を共有する文化」を組織内に根付かせていくことが求められています。経営層からサイバーセキュリティ投資への継続的な支持を得ることは、こうした取組みを推進するうえで、きわめて重要な後押しとなるでしょう。実際に、KPMGの調査によると、エネルギー・化学企業のCEOの72%が、業務や知的財産を守るためにサイバーセキュリティへの投資を増やしたと回答しています[5]。そして、最終的にCISOには、「サイバーセキュリティの唯一の守護者」から、「レジリエンスと俊敏性を備えたセキュリティ・フレームワークの設計者」へと進化することが求められています。

主要課題 1

新たなサイバーセキュリティ秩序のバランス

エネルギー・化学セクターのCISOは、急速に進化するテクノロジーへの対応を進める一方で、気候危機や、それに伴う持続可能性およびESG価値の向上への圧力といった、これまでにない困難な課題に直面しています。さらに、中東やウクライナで続く地政学的な緊張がサプライチェーンに影響を及ぼし、規制面での負担も一段と増しています。実際に、KPMGの調査からも、エネルギー・化学企業のCEOは、サプライチェーンリスクを最大の脅威のひとつとして認識しており[6]、「国家権力構造の変化、経済や貿易の地殻変動、さらに資産・インフラへの多様な脅威」が、企業に深刻な影響を及ぼしているという懸念が示唆されています[7]。このような動的かつ複雑なリスク環境を的確に管理するには、単なる技術的スキルを超えた幅広い能力を持つ、経験豊富なセキュリティリーダーの存在が不可欠です。

主要課題 2

サイバーリスクをビジネスリスクとして捉え直す

CISOには、サイバーリスクを単なる技術的課題ではなくビジネスリスクとして捉えることで、経営幹部と技術チームの間にある意識のギャップを埋めることが期待されています。その実現には、戦略的思考力、交渉力、そして高いリーダーシップといったスキルが求められます。また、業務継続性とデータ・情報保護のバランスという特有の課題を抱えるエネルギー・化学セクターにおいては、経営層や取締役会からの信頼・支持を確保することがきわめて重要です。業務継続性は、定期的なパッチの適用や適切な管理などのサイバー対策を、綿密に計画し、効率的に実行することで高い効果を発揮します。また、セキュリティ投資とその成果とのバランスを明確に提示することで、こうした取組みがセキュリティ対策およびビジネスリスクの軽減にどのように貢献しているかについて、経営層や取締役会の理解を促すことが可能となります。

主要課題 3

規制上の課題

CISOは、サイバーセキュリティプログラムの有効性とレジリエンスを確保する責任を負う一方で、規制当局からの厳格な監視にもさらされています。2023年後半に施行された米国証券取引委員会（SEC）のサイバーセキュリティ開示最終規則などの規制では、取締役会の責任がより明確に問われるようになっており、CISOや経営層に対する規制当局からの圧力が一層強まっています[8]。

主要課題 4

ITとOTが融合する環境における役割分担

ITとOTの融合が進むなかで、これまで明確だった役割の境界は曖昧になりつつあります。こうした状況において、CISOには、テクノロジーと戦略の両面に関する高度な専門知識が求められています。加えて、運用部門とセキュリティ部門の責任やプロセスを明確に切り分け、組織における業務上のギャップを回避することは、安全かつ持続可能なデジタル化戦略を実現するうえできわめて重要です。

5.KPMG, エネルギー・化学業界インサイト：KPMGグローバルCEO調査2024
6.KPMG, エネルギー・化学業界インサイト：KPMGグローバルCEO調査2024
7.KPMG, Top Geopolitical Risks 2025, March 31, 2025.
8.U.S. Securities and Exchange Commission, Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure: A Small Entity Compliance Guide, July 26, 2023.

重要な機会 1

取締役会におけるサイバーセキュリティに関する議論の導入

サイバーセキュリティを取締役会の議論の俎上に挙げることは、CISOにとって、戦略的パートナーとしての地位を確立し、経営目標に対して影響力を持つための重要なステップでしょう。一般的に、CISOが取締役会のメンバーであることは稀ですが、経営幹部への明確かつ直接的な報告ラインを設けることで、取締役会との定期的なコミュニケーションを実現することが可能となります。

重要な機会 2

チームのサイロ化を打破する

CISOは、物理セキュリティ、コンプライアンス、プライバシー、運用といった領域を統合する際に、セキュリティチームと運用チームの連携促進を通じて、リスク管理に対する包括的なアプローチにおける主導的な役割を担うことが可能になります。こうしたチーム間連携は、技術面と運用面のギャップを埋め、ビジネス目標の達成を後押しするとともに、組織のレジリエンスの強化にもつながります。

昨今、多くのエネルギー企業が、AIを活用した予知保全、高度なエネルギー貯蔵ソリューション、スマートグリッドといった先進的なソリューションの導入を検討するなか、エネルギーセクターのCISOには、持続可能なエネルギーへの移行という喫緊の課題と、重要インフラの保護という責務のバランスを取ることが求められています。短期的および長期的な運用の継続性を確保するには、これらの革新的なテクノロジーをレガシーシステムへ段階的に統合していくことが不可欠です。

また、こうしたコグニティブベースのアプリケーションが普及するなか、CISOは、新興テクノロジーの導入をビジネス目標と整合させ、データに基づく洞察を活用してリスクを定量化し、投資判断の妥当性を裏付けたうえで、イノベーションの利点と潜在的なセキュリティリスクを慎重に比較検討することが必要となります。このようなアプローチは、ステークホルダーの理解と支持を得るだけでなく、サイバーセキュリティ・プログラムの持続可能性を確保するうえでも重要な要素となります。

CISOが直面するサイバーセキュリティの主要課題

スマートなエコシステムのためのスマートなセキュリティ

スマートデバイスやモノのインターネット（IoT）の急速な普及により、現代の送配電網は、センサーとソフトウェアが相互接続された広大なネットワークへと進化しています。これに伴い、エネルギー・化学企業のCISOは、デジタルデバイスのセキュリティに対するアプローチを根本的に見直す必要に迫られています。とりわけ、セキュリティ機能が限定的であることの多いスマートセンサーやスマートメーター、さらには送配電網全体が、従来のOTシステムへの潜在的な侵入経路となり得ることから、攻撃対象領域が大幅に拡大するリスクが懸念されています。

こうしたデバイスに対するセキュリティの確保は、もはや10年前の手法では対応できません。CISOには、スマート製品の設計・開発段階から導入・保守に至るまで、ライフサイクル全体を通じてセキュリティを確保する視点を持ちつつ、従来とは大きく異なる新たなアプローチを採ることが求められています。また、セキュリティ戦略を策定するにあたっては、個々のデバイスだけでなく、それらが組み込まれるサプライチェーンや、より広範なエコシステム全体を視野に入れてリスクを捉えることが重要です。

加えて、NIS2、サイバーレジリエンス法（CRA）、AI規制法、ISA/IEC 62443認証といった規制基準の導入により、エネルギー・化学セクターのCISOには、新たな規制要件への対応とともに、それらがもたらす潜在的な影響への対処も求められています。さらに、地政学的な動向や国家とハクティビスト集団の連携といった新たな脅威の台頭により、デジタル製品のセキュリティは引き続き影響を受けており、重要インフラに対する攻撃対象領域の拡大が進んでいます。CISOには、こうした環境変化に柔軟に対応しながら、セキュリティ戦略を継続的に適応・進化させていくことが期待されています。

主要課題 1

データ管理とプライバシー

エネルギー・化学セクターにおけるスマートデバイスは、予知保全やエネルギー最適化などの重要な機能向けに膨大なデータを生成します。しかし、これらのデバイスは、一般的にセキュリティ基準を満たしておらず、認証機能や暗号化機能も不十分であることが多いため、侵害、不正アクセス、データ改ざんのリスクが高まるだけでなく、プライバシーリスクやコンプライアンス上の課題も引き起こします。

主要課題 2

レガシーシステムとスマート製品間の相互運用性と統合

多くのエネルギー・化学企業では、インターネット接続や最新のスマートテクノロジーとの統合を前提としていないレガシーシステムが今もなお稼働を続けています。そのため、これらのシステムにIoTデバイスやスマート製品を後付けで導入すると、セキュリティ上の欠陥が生じる恐れが生じます。また、再生可能エネルギー（再エネ）技術の導入が進むことでシステムの複雑性が増し、サイバーセキュリティ上の脆弱性も高まります。

主要課題 3

安全なライフサイクルとサードパーティ製品

スマートメーターやグリッドセンサーなどのコネクテッドデバイスについては、そのライフサイクル全体を通じたセキュリティとレジリエンスの確保がきわめて重要です。特に、エネルギーセクターは、広範なサプライチェーンに依存しているため、サードパーティ製品に内在する脆弱性が、システム全体に悪影響を及ぼすリスクを増大させています。

重要な機会 1

データ収集と効率性

近年、スマート製品の普及により、業務の効率性、サービス品質、そして信頼性が向上しています。より多くのデータを収集・分析・活用することで、業務全体と顧客の双方にメリットをもたらすことが可能となるでしょう。

重要な機会 2

予測・保守・需要予測

IoTセンサーは、リアルタイムの運用データを分析・活用のもと機器を監視し、問題の早期発見・検知に有効な手段です。ダウンタイムや保守コストの削減に加えて、資産寿命の延長も期待できます。また、需要予測の領域では、こうしたスマートテクノロジーを通じて、消費パターン・傾向を分析し、リソースの割り当て、グリッド管理、再エネの統合を最適化することで、需給バランスの信頼性を高めることが可能となります。

重要な機会 3

規制上の機会

NIS2やCRAといった規制は、より厳格なセキュリティ基準、リスク評価、コンプライアンスを義務付けることでスマートデバイスのサイバーセキュリティを強化するとともに、セキュア・バイ・デザイン（設計段階からのセキュリティ確保）の原則や、サプライチェーン全体の整合性を担保することを目的として導入されています。そのため、スマートグリッドや産業用IoTなど、重要業務を担うデバイスには、安全な通信、パッチの適用、インシデント対応に関して厳格な基準を満たすことが求められます。

エネルギー・化学企業は、効率性、持続可能性、運用信頼性の向上に向けて、分散型エネルギーシステムの実現やピアツーピアのエネルギー取引を促進するブロックチェーンおよびWeb3テクノロジーなど、スマートテクノロジーの導入を積極的に進めています。また、送配電事業者においては、エネルギー供給の最適化と再エネのシームレスな統合を目指し、スマートグリッド技術への戦略的な投資を通じて、高度なセンサー、リアルタイムデータ分析、デマンドレスポンスシステムが導入されています。

さらに、エネルギー効率の高い建物では、スマートセンサー、IoTデバイス、高性能な断熱材を活用することで、エネルギー消費の最小化、化石燃料への依存低減、そして二酸化炭素排出量の削減が進められています。こうした最先端技術の導入は、エネルギー使用の最適な管理を可能にし、送配電網の運用改善・最適化やコスト削減を実現することで、電力企業と需要家の双方にメリットをもたらします。

CISOが直面するサイバーセキュリティの主要課題

企業経営と社会全体のためのレジリエンス・バイ・デザイン

エネルギー・化学企業において重要インフラや資源を管理するCISOは、IoTやOTシステムへの依存が高まるなか、産業制御システムを標的とするサイバー脅威の高度化により、大規模な混乱の発生や人命・機密データの漏洩といった現実的かつ深刻なリスクに直面しています。さらに、こうした複雑な課題に加えて、重要インフラのセキュリティおよびレジリエンスに対する規制当局の監視強化が、CISOの対応・取組みを一層困難なものにしています。

SCADAシステムへの侵入、送配電網への攻撃、パイプラインの停止など、エネルギー・化学セクターが直面するインフラ関連の脅威は、事業継続性に深刻な影響を及ぼします。こうした状況下で運用上のレジリエンスを維持するには、CISOが混乱の未然防止とインシデント発生時の迅速な復旧に重点を置いたサイバーセキュリティ戦略（リアルタイム監視、攻撃対象領域の管理、インシデント対応計画の策定、組織全体にレジリエンス重視の文化を根付かせるための取組みを含む）を導入することが不可欠です。

エネルギー・化学企業には、NIS2やNERC CIPなどの新たな規制の導入や規制環境の変化を背景に、物理インフラとデジタル資産の双方を保護するため、より強固なサイバーセキュリティ対策を講じることが、これまで以上に求められています。こうした環境でエネルギー・化学企業は、レジリエンスを優先することで、脆弱性を最小限に抑え、高度なサイバー脅威に直面しても安定した運用を維持することが可能となります。また、これらの取組みを通じて、CISOは、戦略的な事業推進役としての地位を確立し、組織のレジリエンスを高めるとともに、企業の競争力向上にも貢献することが可能となります。

主要課題 1

デジタル変革のリスク

古いOTシステムをオンラインネットワークに接続してデジタルトランスフォーメーション（DX）を推進する取組みは、不覚にも、安全対策が不十分なレガシーシステムをインターネット経由の脅威にさらす結果を招いています。スマートメーターや洋上風力発電施設、送配電網のリモートセンサーなど、エネルギーシステムへのIoTデバイスの導入が進むことで、攻撃対象となる領域は大幅に拡大しています。実際に、これらのデバイスは、多くの場合セキュリティ対策が不十分で、攻撃者に悪用されやすい脆弱性を抱えているうえ、システム同士が密接に連携・接続されていることから、1つの障害が連鎖的に波及し、インシデントの封じ込めを一層困難にするリスクをはらんでいます。

主要課題 2

再エネインフラの脆弱性

再エネインフラの多くは、遠隔監視を可能とするデジタルインターフェースを備えていることから、サイバーリスクに対して脆弱な側面を抱えています。特に、Wi-Fi対応のIoTデバイスが組み込まれている場合、そのリスクはさらに増大します。

主要課題 3

複雑かつ進化するレジリエンス規制

地域や国際間でサイバーセキュリティ基準が統一されていない現状は、重要インフラを担うエネルギー・化学企業にとって、コンプライアンス対応の複雑化を招いています。とりわけ多国籍企業における規制対応は、国や地域ごとに異なる規制が存在し、なかには内容が矛盾または重複するものもあることから、一層複雑化しています。なお、これらのコンプライアンス違反が発生した場合には、巨額の罰則金、企業評判の毀損、規制当局からの監視強化といった重大なリスクを招くおそれがあります。

重要な機会 1

リアルタイム監視

セキュリティ情報・イベント管理（SIEM）システムや侵入検知・防御システムといった高度な脅威検知ツールの活用に加えて、機械学習（ML）やAIを活用することで、脅威・悪意のある行動をより正確に認識・予測し、IT環境とOT環境の両面においてサイバー脅威を迅速に特定・対応することが可能となります。

重要な機会 2

規制の有効的な取込み

NIS2指令などの規制では、業界間の協力体制の構築やサードパーティ企業に関するリスク管理が求められています。これらの規制は、サプライチェーンリスクの管理を義務付けるもので、主要サプライヤーのサイバーセキュリティ体制を継続的に監視することが不可欠となっています。特に、脅威インテリジェンスの共有や他社・政府機関との連携は、エネルギー企業が新たな脅威に対して先手を打つためにきわめて有効でしょう。また、信頼できるサイバーセキュリティベンダーとの協力体制を構築することで、迅速な対応と的確なインシデント対応支援が期待できます。

重要な機会 3

サイバーセキュリティ意識の向上と危機シミュレーションの普及

近年のサイバーレジリエンス研修では、仮想現実（VR）を活用した没入型の危機シミュレーション、AI駆動型の適応シナリオによるパーソナライズされた学習体験、さらには、ゲーミフィケーションプラットフォームを用いた従業員やオペレーターによるインタラクティブなインシデント対応演習など、最新技術を取り入れた多様なトレーニング手法が次々と導入されています。こうした先進的なトレーニングによって、対応力の向上と組織全体のレジリエンス強化が着実に図られることが期待されます。ただし、重要なインフラを担うエネルギー・化学企業では、こうした新技術の導入に際して、十分なリスク評価と慎重な判断が求められていることも忘れてはなりません。

重要な機会 4

サイバーリスク保険の価値

脅威が拡大するなか、加入するサイバー保険がどのようなリスクや損失（エクスポージャー）を補償対象としているのかを、あらかじめ把握しておくことも必要でしょう。特に、サードパーティ企業のサービス停止に起因する損失を正確に評価したうえで、保険の活用や保険料の見直し、さらには訴訟といった手段を講じることで、その影響を最小限に抑えることが重要となります。

グローバルエネルギー・化学企業における サイバーセキュリティ事例

導入事例

企業が抱えていた課題

あるエネルギー供給事業者では、サイバー攻撃によるIT機能の全面停止に備えた対応力の強化と、事業継続に不可欠なアプリケーションの見直しが喫緊の課題となっていました。こうした状況を受け、同社では、重大なサイバーインシデント発生時に迅速かつ確実な復旧を図るため、初動対応から業務再開に至るまでの手順や段階的対応を体系化した包括的なプレイブックの整備が急務となっていました。さらに、変化の激しい市場環境において的確な意思決定を支えるため、ビジネスプロセスの優先順位を特定・分類するための評価手法（方法論）の導入も強く求められていました。

KPMGによる支援内容

KPMGはまず、世界各地の主要ステークホルダーと連携し、クライアントの既存の復旧プロセスを詳細に把握したうえで、ITシステムの全面停止を想定した実行可能な復旧手順をプレイブックとして策定しました。さらに、事業継続に不可欠なアプリケーションを再評価するためのツールも開発しました。このツールの設計にあたっては、従来の分類基準が陳腐化していた点を踏まえ、BIA（ビジネスインパクト分析）から得られたデータを活用し、各アプリケーションの重要度を客観的に再評価できる仕組みを組み込みました。

企業が得られた成果

この一連の取組みにより、エネルギー供給事業者は、IT機能が全面的に停止するような深刻な事態においても、ダウンタイムや事業損失を最小限に抑えるための明確な対応プロセスを導入することができました。加えて、各ビジネスアプリケーションや業務プロセスの重要度をより的確に把握できるようになり、サイバー脅威への備えと、組織全体のレジリエンス強化にもつながりました。

広範なサプライチェーンと、IT・OTが複雑に連携するシステムを有するエネルギー・化学企業においては、適切な安全対策（ガードレール）を講じないまま新たなテクノロジーを急速に導入すれば、セキュリティ上の脆弱性が拡大し、サイバー攻撃の標的となるリスクが高まります。こうした観点からも、セキュリティは常に経営の最優先事項として位置づけられるべきでしょう。

近年では、エネルギー・化学企業は、こうした課題に対するセキュリティ体制を着実に強化しています。具体的には、AIや機械学習による予知保全や脅威検知、ブロックチェーンを通じた取引の信頼性向上、さらには高性能コンピューティングやIoTを組み込んだリアルタイム監視の取組みが加速されています。また、「セキュア・バイ・デザイン」の原則に基づき、システムの設計段階からセキュリティを組み込むアプローチも広がっています。加えて、クラウドセキュリティの導入やサイバーセキュリティ・ガバナンスの一元管理により、データの安全かつ効率的な運用も進められています。

エネルギー・化学企業における最優先事項

エネルギー・化学セクターのCISOが、リスクを積極的に特定し、重大なサイバーインシデントから迅速に回復する能力を高めるには、以下のような取組みが最優先事項として位置付けられます。

- ✓ 役割・責任・義務・ドメインに関するサイバーセキュリティ・ガバナンスを明確化・強化する
- ✓ IT、セキュリティ（物理およびサイバー）、OT各チーム間のサイロを解消し、脅威の状況、組織環境、サプライチェーンを正確に把握したうえで、緊急時およびインシデント対応機能を統合・調整する
- ✓ サイバーセキュリティをビジネスリスクとして捉え、ITおよびOTにまたがる広範なリスク管理フレームワークを確立する
- ✓ サイバーおよび物理的リスクの双方を考慮した事業継続・災害復旧（BCDR）戦略を導入し、現実的なシナリオに基づいて徹底的にテストおよび演習を行う
- ✓ サードパーティのサービス停止に関連する保険ポリシーを精査し、事業中断保険による補償で財務的影響を軽減できるかどうかを検討・判断する

KPMGによる支援内容

KPMGでは、経験豊富なプロフェッショナルで構成された専門チームが、サイバーセキュリティ分野で信頼できるアドバイザーとして、エネルギー・化学企業のビジネス上の優先事項やリスクプロファイルに応じて、サイバーセキュリティ体制の評価、ITとOTの融合、脆弱性管理、規制対応、インシデント対応など、サイバーセキュリティのあらゆるニーズに対応し、ビジネス価値の向上と競争優位性の確保につながる幅広いサービスを提供しています。

KPMGジャパン
エネルギーセクター

Sector-Japan@jp.kpmg.com

本リーフレットで紹介するサービスは、公認会計士法、独立性規則及び利益相反等の観点から、提供できる企業や提供できる業務の範囲等に一定の制限がかかる場合があります。詳しくは有限責任 あずさ監査法人までお問い合わせください。

本冊子は、KPMGインターナショナルが2025年3月に公表したCybersecurity considerations 2025: Energy and natural resources sectorを、KPMGインターナショナルの許可を得て翻訳したものです。翻訳と英語原文間に齟齬がある場合は、当該英語原文が優先するものとします。