KPMG

サイバーセキュリティ主要課題2025

AI主導のビジネス環境で重要性を増す
サイバーセキュリティの基本原則

目次

序文

デジタル環境は引き続き前例のないペースで進化しており、新たな課題も出現してサイバーセキュリティ施策の緊急性はますます高まっています。今回の「サイバーセキュリティ主要課題」（第6回）では、近い将来、さまざまな組織に降りかかってくるであろう課題に光を当て、組織がどのような戦略的行動をとれるかを8つのポイントに分けて提言しています。

テクノロジーが私たちの仕事や生活と全面的に結び付いている時代にあって、サイバーセキュリティはビジネスの関心事であるだけでなく、社会のあらゆる側面に影響を及ぼす問題となっています。KPMGの調査によると、過去10年間、CEOはサイバーセキュリティを脅威の筆頭に挙げてきました[1]。

AIがほぼすべての業種に導入されたことで、AIのモデルとプロセスのなかに信頼を組み込むという重大な課題が表面化しています。信頼を組み込むためには、堅牢なガバナンスプログラムを確立し、それを通じて最高情報セキュリティ責任者（CISO）がさまざまなビジネスケースを理解し、AIがすでに組織内のどこでどのように使用されているかを判断し、それに起因する脆弱性を突き止めなくてはなりません。

自動車や医療機器から家電製品や各種のモノのインターネット（IoT）関連製品に至るまで、スマート製品が急増したことで、アタックサーフェス（攻撃対象領域）が拡大し続けており、物理的な脅威とデジタルの脅威が過去に例のない形で連動し始めています。ディープフェイクの出現、そして、いまだ規制の網から漏れがちで不安定なデジタル資産（たとえば、暗号通貨）の再流行は、そうした脅威の複雑さを増大させており、警戒と革新的な対抗策が必要になっています。

このような情勢のなかでCISOは、AIテクノロジーに関する自身と配下チームの教育に注力することが強く求められています。その目的は、最も有能なチームを編成することだけでなく、各ユースケースがもたらす固有のリスクを理解することです。優れた人材の獲得と育成の面でCISOは、AIの複雑さと特定困難なリスクを把握する能力を備えたチームを編成するという非常に困難な任務に直面しています。この任務をさらに難しくしているのが、この領域で進行している急速なイノベーションであり、統制困難な「シャドーAI」が業務のあらゆる場面に出現していることです。

一方で、セキュリティチームはサイバー機能の合理化や統合を進めており、多数のソリューションをセキュリティオペレーションセンター（SOC）内で運用する形態から離れ、リーン化された限定的なベストオブブリード（適材適所）ツールスイートへと移行する動きが生じているように見えます。その目的は、複数のソリューションをより効果的かつ経済的に統合すること、そして、そのようなツールのプロバイダーによって提供される新しいAIの能力をより適切に活用することです。

現在のサイバーセキュリティの課題は、従来の技術的なスキルの領域を超えており、リスク管理に対する深い理解をはじめとして、問題解決、批判的思考、コミュニケーションといった多種多様なソフトスキルも包含した分野横断的なアプローチを必要としています。サイバーセキュリティ人材は、従来の技術系以外の経歴からも獲得できます。サイバーセキュリティ担当者に求められるのは、速やかに適応する能力であり、またコンピューターサイエンス、ソフトウェアエンジニアリング、情報テクノロジーといった分野の標準的な学位取得のための教育訓練で授けられる知識を超えた、具体的な知識を習得していく能力です[2]。サイバーセキュリティ担当者が、明確かつ柔軟なコントロールの必要性を見落とすことなく、状況別のリスク評価を優先的に実行することが必要不可欠です。

1 KPMGグローバルCEO調査2024、2024年8月

2 World Economic Forum, Strategic Cybersecurity Talent Framework, April 2024.

サイバーセキュリティは、絶えず進化し続ける動的な課題です。たとえば、量子コンピューティングの台頭があります。量子コンピューティングによって、攻撃者は暗号化ツールを超高速で回避でき、銀行の取引から、ビジネスのデータ、文書、電子メールまで、あらゆるものを危険にさらします。

「スーパーインテリジェント」なAIシステムの可能性もあります。このAIシステムは、察知した危険に対して自己防衛しながら、絶え間なく向上し知識を拡大していきます。さらに、誤情報が（特にディープフェイクによる偽の音声・画像コンテンツを通じて）拡散するスピードも問題となります。こうした現象は、CISOが夜も眠れないほど頭を悩ませている新しい課題の一部に過ぎません。これらをはじめとするさまざまな脅威は、イノベーションと戦略的先見性が緊急に必要とされていることを顕著に示しています。

昨今、地域固有の規制へとシフトしているため、グローバルなセキュリティ業務に困難が生じています。そうした状況に加え、セキュリティ予算の正当化を投資収益率（ROI）だけでなく、リスクの軽減にも基づいて行うという経済的要請も重なることで、CISOは、従来のような財政的保証がない資源の予算化を訴えるという危うい立場に置かれています。

同様に、CISOは複雑さを増す地政学という難題にも直面しています。国家の支援を受けた攻撃の拡大、流動的な規制環境、国家の垣根を越えたデータの流れに対応するため、CISOは、自社のネットワークを効果的に保護するために、膨大な数の込み入った問題を処理していかなければなりません。明らかなのは、新たな脅威において後れを取らないよう、そして規制を遵守するように求める圧力がかつてなく高まっているということです。

重大なインシデントを乗り切ったCISOであれ、小規模な局地戦しか直面していないCISOであれ、今日のCISOの広範な経験は、かつてなく流動化している脅威情勢を完全に理解することの必要性を浮き彫りにしています。

本レポートでは、幅広い分野のKPMGの専門家がサイバーセキュリティの現状を包括的に分析し、CISOにとっての実践的な戦略を8つのサイバーセキュリティ主要課題に沿って提言しています。組織のリーダーがデジタル時代の複雑さを乗り切るために必要とされる知識とツールを身につけられるよう支援し、不確実な未来に立ち向かっていく組織がセキュリティとレジリエンスを実現できるように手助けをすることが、私たちの揺るぎない目標です。

Akhilesh Tuteja
Global Cybersecurity Leader
KPMGインターナショナル

> テクノロジー情勢は急速に進化しており、新しい脅威が毎日のように出現しています。そうした状況で後れを取らないように、企業は、事後の対応ではなく先を見越した積極的な姿勢で、自社のデジタル資産を保護し、コンプライアンスを維持し、イノベーションが安全に発展できる環境を育成しなければなりません。

Bobby Soni
Global Technology Consulting Leader
KPMGインターナショナル

過去5年間を振り返る 2020～2025年

本レポートを作成してきた過去5年間に、絶え間なく進化し続けるサイバーセキュリティ情勢は、組織のリーダーの関心の明確な焦点となりました。重要なテーマの多く、たとえば、レジリエンス、ID（アイデンティティ）・アクセス管理（IAM）、クラウドセキュリティ、人材とスキルのギャップなどは、依然として大きな関心事であり続けています。

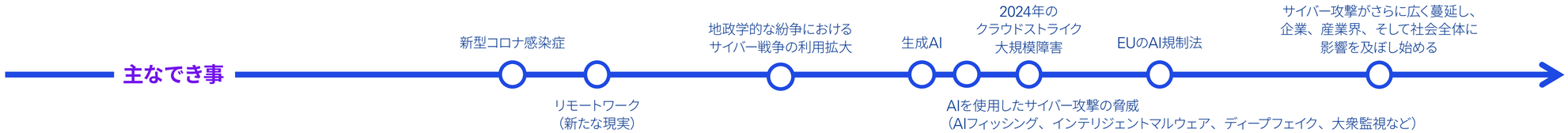
この興味深い中核的なテーマの基本的な土台は変化してきています。つまり、従来のセキュリティ施策から、CISOとそのチームがほぼリアルタイムで対応しなければならない地球規模の多面的なデジタル情勢の優先事項や課題へと変化してきたのです。とりわけ、サイバーセキュリティがどのくらい広範に浸透し、テクノロジーのリスクを超えてより幅広いビジネスへの脅威を包括するように拡大して、産業と社会全体に等しく影響を及ぼすようになってきたかという点が何よりも重要です。

もう少し深く掘り下げてみましょう。

- 新型コロナウイルス感染症（COVID-19）に伴うリモートワークの常態化で、クラウドとAIにおけるセキュリティへの注力がCISOの主要目標となってきました。
- 先進的なテクノロジーが出現するたびに新しい多様なスキルが必要になる状況のなか、人材の確保や常態化したスキルギャップが、長らく重大な懸案となってきました。
- IDは、個別の機能である従来のIAMから、ゼロトラスト戦略の中核的存在へと変化し、デジタルIDを特定したりディープフェイクを見極めたりする手段となりました。
- レジリエンスは全体を通じて必須の目標となり、今後もそうあり続けるでしょう。
- CISOは、特に、サイバー攻撃の脅威が広範囲に及ぶビジネスへの脅威へと姿を変えるなかで、引き続き体制の強化に努めています。そうした脅威は、産業界を混乱させ、社会に危害をもたらす可能性があるためです。

次のページに示した2020～2025年のトレンド分析をみると、当初から調査対象となってきた基本的なセキュリティ基盤の大半が、現在まで引き続き調査の中心的な対象となっています。ただ、新しいテクノロジー、規制の拡大、ますます高度化するツール、脅威情勢の高まりという状況を受け、CISOの役割は規模と責任の両面で増大の一途をたどっています。

トレンド分析：2020～2025年



主なテーマ

	2020年		2025年
戦略とリーダーシップ	• CISOは、信頼される社内アドバイザー兼業務リーダーとなった	• 話題が、コストとスピードから戦略的かつ効果的なセキュリティへと変化した • CISOの予算が、事業部門のリスク低減と徐々に結び付いてきた	• サイバーが組織全体に広く行きわたるにつれ、CISOに結果を出すように求める重圧は増大している • CISOの役割の分散化の進行と責任の増大 — その理由の一部は、規制の拡大である
人材と能力	• セキュリティチームは、戦略を検討する場で重要な発言をする主要な資源へと変貌しつつある	• サイバー部門の存在目的はビジネスの支援であり、阻害ではない — 組織のエンフォーサー（用心棒）からインフルエンサーへと変化 • サイバーが組織の基本構造に組み込まれる	• サイバーのスキルギャップは解消されていない — AIが有望なソリューションを提供してくれる可能性はあるが、人員は新しいスキルに適応してそれを身につける必要がある
テクノロジーとデータ	• 新しいバーチャルインフラストラクチャモデルとコラボレーションツール • クラウドトランスフォーメーションが（COVID-19を背景に）加速したが、セキュリティは後知恵だった • 従来のID認証および管理（IAM）	• 自動化を通じたセキュリティの強化 • 生成AIの急速な進歩がサイバーのユースケースをめぐる熱狂を生み出す • ペリメータレス（境界防御がない）かつデータ中心の世界を保護する • IDをゼロトラストの中心に据える	• サイバーを目的としたAIへの投資は戦略的かつ先見的な性質を増している • 企業規模でのコスト削減、効率化、セキュリティ、イノベーション（特にAIの導入）がプラットフォームの統合の原動力となっている • デジタルIDとディープフェイクの増加
デジタルトラスト	• サイバーおよびプライバシー規制は事業部門の優先課題と責任に重点を置いている — 信頼の重要性	• デジタルトラストは、事業部門から始まって複数のステークホルダー（例：CISO、DPO、CDO、CIOなど）を巻き込んでいく共同責任である	• AIがビジネスと社会のすべての仕組みに浸透するなかで、信頼を組み込む — セキュリティ、プライバシー、安全性、倫理などに注力
レジリエンス	• シナリオからインパクトベースへ — 重大インシデントと規制への注力	• もはや攻撃の阻止だけが問題ではない — 対応と回復への注力	• サイバー攻撃の脅威が技術的なリスクからビジネスや産業に対する脅威へと進化し、社会に危害を及ぼす恐れが生じているなかで、CISOは引き続きレジリエンスの増強を進めている

サイバーセキュリティ主要課題2025：8つのポイント

01

絶えず進化するCISOの役割

CISOとそのチームが何に注力するか、組織の他部門とどのようにかかわるかは流動的です。それは、サイバーセキュリティ機能が組織のなかにより広範に組み込まれ、組織全体で理解が深まるにつれて変化します。

02

人材が持つパワー

デジタル技術の進化とともにビジネスモデルを変革し続ける途上で、多くの組織がワークロードの課題に直面しており、サイバースキルギャップも悪化しています。AIと自動化は助けにはなるが、人材の離職という根本的なリスクが存在しており、対処に苦慮しているケースが多く見受けられます。

03

AIの急速な普及に対する信頼の獲得

AIの存在が定着し、組織内のほぼすべての業務にその活用は広がっているが、サイバーセキュリティとプライバシーの重大な問題がいくつか存在しており、今後のAIの採用と展開に影響を及ぼす可能性があります。

04

AIのサイバーセキュリティへの活用：スピード競争か、安全運転か

AIの採用をめぐる議論では、トレーニングの欠如に始まり、機会の逸失や後れを取る可能性への懸念に至るまで、多くの要因が影響しているように見えます。重要な課題の1つは、AIをサイバーセキュリティとプライバシーの機能に組み込むことのメリットとリスクを比較することです。

05

プラットフォームの統合：可能性を受け入れながら、リスクも認識する

多くのグローバル組織が、使用するテクノロジーの複雑さとコストを減少させようとしています。ツールとサービスを単一（または限られた数）のプラットフォームに統合することでそれを実現しようとする組織は、内在するリスクを見極め、管理していかなければなりません。

06

デジタルIDの重要性

デジタルIDをめぐる取組みが世界で次々と実施されているが、システム間の相互運用性と、ディープフェイクの出現に伴う認証の強化が、依然として課題です。そこでは、規制、リスク選好度、個人データや生体認証データの取扱いに関する世論などが問題となっています。

07

スマートエコシステムのためのスマートセキュリティ

スマートデバイスやスマート製品の世界的な増加によって、セキュリティに対する従来の見方とアプローチが問い直され、変化が生じています。これを受け、多くの規制当局は、そうしたスマート製品が基本的なセキュリティ要件を満たすものであることを保証するための新しい制度の導入を促されています。

08

レジリエンス・バイ・デザイン：企業と社会のためのサイバーセキュリティ

レジリエンスは、CISOのアジェンダの中核となっています。これは、攻撃者がランサムウェアやその他の悪意ある手段を使用して産業界に大規模な混乱を引き起こし、データと人命の両方を危険にさらす可能性を警戒し続けるためです。

主要課題1

絶えず進化するCISOの役割

さまざまな要因の複合によりサイバーセキュリティのあり方が変化しており、CISOの役割も大きな変革に直面しています。規制機関による監視の厳格化、実質的な過誤なく業務を遂行するよう求める圧力、結果責任や個人が負うリスクの増大といった要因すべてが、このような趨勢の変化を促しています。それと同時に、従来のCISOの職務は次第に組織全体にわたって分散化し始めており、この役職の未来とサイバーセキュリティ業務の行方について重要な問題を提起しています。おそらく、CISOの今後の成否は、意思決定の権限を効果的に確立し、新たに出現するテクノロジー（特にAI）の影響を管理し、新しい脅威に適応していく能力に大きく左右されるでしょう。

オペレーティングモデルの進化に伴って高まる期待

CISOの役割は複雑化しています。その主な原因は、規制機関の監視と、サイバーセキュリティの成果向上を組織全体で実現する必要性です。この複雑さは、オペレーティングモデルの変化と外部ベンダーへの依存拡大によってさらに進行します。外部ベンダーが提供するセキュリティコントロールが各組織に固有のニーズと常に一致するとは限りません。特に、複数の国にまたがるグローバルな事業の場合はなおさらです。

CISOは現在、ベンダーの提供するコントロールについて適切に管理・構成することで、それが目的に適い、かつ現地の法規制を遵守したものとなるように取り計らうという課題に直面しています。オペレーティングモデルにこのような変化が生じると、セキュリティ施策の導入実施に対するCISOの直接的な統制力は減少します。そうしたベンダーが提供する組込みのサイバーセキュリティ／プライバシーコントロール機能は、有益であることもありますが、多くの場合、CISOが多様な環境においてリスクを効果的に管理するために必要とされる柔軟性と細分性を欠いています。CISOは、従業員が効率的に働けるように配慮しながら、この増大する複雑さに対処しなければならず、また、さまざまなコントロール機能の運用に対する可視性を組織全体にわたって維持しなければなりません。

> “クラウドベースのソフトウェアベンダーでは、問題がさらに複雑になります。通常、オンかオフかの二値選択であるからです。理想を言えば、CISOは、特定のコントロールを状況や場所に基づいてオンまたはオフに設定したいと考えるでしょう。たとえば、米国ではオンだがドイツではオフである、シンガポールではオンだがスイスではオフである、などです。”
>
> **Paul Spacey**
> Global Chief Information Security Officer
> KPMGインターナショナル

組織内でのサイバーセキュリティの役割と範囲を示す見取り図を作成する

CISOの役割をとりまく組織構造は進化しており、最近の動向としては、テクノロジー情報セキュリティ責任者（TISO）と責任を分担する方向への動きが強まっています（TISOが設けられている場合）。このような役割の分割により、CISOは、リスク管理やより幅広いサイバーセキュリティ戦略に注力することが可能となります。一般に、TISOは組織の技術部門に所属しており、関連するコントロールの導入・実施状況を監視し、日常業務を管理しています。

そのほか、大規模な組織では複数のCISOが存在していることがあり、それぞれがサプライチェーンネットワークやコマーシャルオンラインプレゼンスなど、異なる事業部門を担当しています。このような責任の区分化は、たった1人のCISOが、サイバーセキュリティ情勢全体を効果的に管理しながら、あらゆる分野にわたって詳細な知識を維持するのは難しい、という認識に基づいています。

サイバーセキュリティという領域が拡大し続けるなかで、CISOの責任範囲も拡大しています。CISOは、コントロール、パフォーマンス、リスク、インテリジェンス、ID管理、そして全体的なサイバーハイジーン（ウイルス感染の防止などを目的としたIT環境の衛生管理）など、幅広い側面に関して、「真実の源泉」の役割を果たさなければなりません。CISOは、そのような情報をわかりやすい適切な形で事業部門に提供することで、事業部門が適切な情報に基づいて意思決定を下せるように取り計らう任務を負っています。

CISOは、多くのセキュリティの課題を他のチームに委託することもできます。たとえば、主要リスク指標に関するレポートの発行、リスク評価の実施、侵入テストの実行などです。しかし、それでもCISOはそのような活動に対する監視と認識を維持しなければなりません。CISOにとって困難な課題は、アジリティ、効率性、状況認識を組織全体にわたって確保しながら、この拡大した範囲を効果的に管理することです。

綱わたり的なバランスの維持：リスクが増大するなかでどのように責任と権限のバランスをとるか

規制機関の監視と個人が責任を問われる可能性の増大は、CISOが担う責任と意思決定権限を明確に定義する必要性を浮き彫りにしています。サイバーセキュリティインシデントが発生すると、CISOは、その結果によっては法的および職業的な責任を問われる可能性があり、特に、厳格に規制された業界ではその可能性が高くなります。

組織はこのリスクを低減するため、インシデントの発生時に波及的影響を恐れることなく必要な措置を発動できるようにCISOに権限を付与する、正式なガバナンスプロセスを確立しなければなりません。それには、CISOが、どのような権限が自らに付与され、その行使にどのような制限があるかを明確に理解できるようにすることも含まれます。これにより、CISOは自信を持って迅速に重要な意思決定を下すことが可能となります。

また、CISOが属する指令系統も、サイバーセキュリティのリスクを効果的に管理する能力を大きく左右します。Cレベルの経営幹部、顧問弁護士、および取締役会との直接的なコミュニケーション経路を確保しておくことも重要ですが、その一方で、CISOは、自分自身の技術的な専門知識に基づいて意思決定を下す自律性も持っていなければなりません。

サプライチェーンへの不正侵入などの緊急事態には、CISOは、必要な技術的知識を欠いている上長からの承認を待つことなく、ただちに行動を起こす権限を必要とします。しかし、この自律性は、結果責任に関する明確なコントロールとガードレールとのバランスがとれていなければなりません。これは上級経営幹部と共同で作成する必要があります。CISOは、重大な局面でいったん立ち止まり、想定される結果を検討し、最も効果的な行動方針を見極めることが望ましいでしょう。

> “かつてCISOの仕事の出発点は、組織の重要資産、つまり、重要なデータ、知的財産、営業秘密などを特定して、それらを危険や脅威から守ろうと試みることでした。現在のCISOに本当に求められているのは、事業のセキュリティとレジリエンスに注力することです。”

Wendy Lim
Partner, Cyber, Advisory
KPMGシンガポール

未来に向けてCISOのプレイブックを書き直す

組織が自動化とAIテクノロジーの導入を進めていくなかで、CISOの役割は大きく変化しようとしています。SOCの自動化の拡大は、チームの小規模化や日常業務への注力の縮小という結果をもたらすことが期待できます。サイバーセキュリティに委ねられた任務は膨大であるため、組織は責任を分割する必要があるのです。CISOが、テクノロジーデリバリーチームを効果的に監視し、さまざまなテクノロジーの機能を管理し、コントロールからのシグナルを解釈し、さらにレポート生成、データエンジニアリング、人事、アウトリーチトレーニングの全側面を処理するというのはあまりに大変です。このような過大なワークロードを課されれば、CISOは次第に行き詰まり、最終的に立ち往生してその役割を果たせなくなるでしょう。

このように、CISOには、他の重要な戦略的領域まで注力を拡大することが期待されています。さまざまな業界で生成AIが急速に導入されるなかで、CISOは、AIに関連するリスクを組織が理解して軽減できるように取り計らううえで決定的な役割を果たすことができます。CISOは、より戦略的かつ積極的に動くことで、AIプロジェクトの初期段階から事業部門に働きかけ、潜在的なリスクを説明してその軽減に必要となる段取りの概略を示すことが必要になるでしょう。

要するに、CISOは、企業、従業員、顧客をより効果的に保護するうえでAIがどのように役立つかを見極めながら、AI固有の安全対策に投資し、それをモデルのなかに組み込む必要があります。KPMGの調査でも、グローバルCEOの64%が経済情勢に関係なくAIに投資する考えであることが明らかになっています[3]。

将来的に、CISOは調整しながら、取締役会、事業部門、テクノロジーマネジャーの要望と、時としてそれと相反するサイバーセキュリティ固有のリスクを管理するCISO自身のニーズとのバランスをとって折り合わせていく必要があるでしょう。そのため、CISOは利害関係を調整する有能なステークホルダーマネジャーになり、複雑な関係を処理しながらサイバーセキュリティの優先課題の重要性を効果的に伝達する能力が求められます。

これを容易にする手段として、CISOは、セキュリティ要員を主要な事業部門に組み入れることを検討してもよいでしょう。そうすれば、セキュリティ文化と組織全体の優先課題の連携を強化できるからです。総合的な物の見方を植え付けることで、CISOは、取締役会に価値ある洞察を提供し、サイバーセキュリティが組織の基本構造のなかに組み込まれるように取り計らうことができます。

次に問題となるのが、多くの規制機関が重視しているレジリエンスの目標です。レジリエンスを実現するには、組織がインシデント後に回復させなければならない基幹系のビジネスプロセスとシステムについてマッピングを作成する必要があります。CISOがスイッチを押しさえすれば、事業部門や技術チームがレジリエンスの問題解決に参加してくれるというものではないのです。

組織が責任を分割しようとしている理由はそこにあります。こうした取組みすべてを効率的に進めるには、誰か1人に責任を負わせるわけにはいかないと、企業は気づき始めています。大規模なセキュリティチームが企業全体を常に保護する必要があるのに対し、攻撃者は、防御の甘い1つのベクターを見つけさえすればネットワークにアクセスできてしまいます。

明らかなのは、これは非対称の戦いであり、すべてに適切に対処するためには企業の多数の部門が協力し合わなければならないということです。CISOはそのすべてを監督するのに最適な立場にありますが、すべてを単独で成し遂げることはできません。

> “サイバーセキュリティは、委任された共有機能という側面が強まっています。現在のCISOは企業全体にわたって多くの上級管理職と非常に緊密に連携しているものの、組織の商業的利益を支えながらリスク管理をしていくためには、関係者全員の一層の意思統一を図らなければなりません。”
>
> **Oscar Caballero**
> Partner, Head of Cybersecurity
> KPMGメキシコ

3 KPMGグローバルCEO調査2024、2024年8月

推奨施策

規制の変化に関する情報収集に努め、取締役会と意思疎通し、権限を明確にして個人の法的責任が発生するリスクを軽減してください。

AIによる自動化とクラウドベースのサービスへの移行で生じるCISOの役割の進化に備えてください。

AIのようなディスラプティブテクノロジーの採用に関する議論を主導し、リスクとその軽減策について説明してください。

サイバーセキュリティに注力するチームメンバーを事業部門のなかに組み入れることに加え、セキュリティをDevSecOpsプロセス全体に「バイ・デザイン」で組み込む作業を継続してください。

クラウドベースのサービスやAIサービスのなかで個人データと企業データの境界線が曖昧になってきているため、サードパーティベンダーに対し徹底的なデューデリジェンスを実施して、ベンダーの契約上の義務が明確化され、かつ組織の全体的なデータガバナンスの枠組みに整合したものとなるよう取り計らってください。

> 基本的に、攻撃を受ける可能性を低下させる出発点は、環境を理解することです。知らないものを守ることはできません。CISOは、サイバーセキュリティの対象となる資産全体を把握していなければなりません。たとえば、組織の基幹ビジネスアプリケーションとサービスはどれか、何が外部に公開されているか、どのようなコントロールが設けられているか、どうすればもっと先を見越して対応できるか、セキュリティ体制の現状はどうか、不正行為者が目を付けそうな攻撃ベクターはどこかなど、枚挙にいとまがありません。これらすべては基本です。それを踏まえてはじめて、CISOは、悪いことが起こる可能性を低下する方法について判断できるようになるのです。

Lou Fiorello
Vice President — Security Products
ServiceNow

Learn more

主要課題2

人材が持つパワー

サイバーセキュリティのリーダーが直面している多くの課題のなかでも、従業員のスキルギャップは特に顕著な問題です。サイバーの脅威との戦いで、人的要素は最も重要な要因であり続けています。新しい高度なテクノロジーと急速に進化する脅威は、拡大しつつあるスキルギャップを悪化させる一方です。このような課題を解決し、デジタル資産を守るために、組織はレジリエンスの高いサイバーセキュリティエコシステムの構築に寄与する人材の力を考慮に入れた総合的なアプローチを採用しなければなりません。有望なソリューションとして挙げられるのが、有能な人材に必要なツールを授ける、堅牢なセキュリティ文化を育成する、AIを最適な方法で利用する、人材供給のパイプラインを強化する、といったことです。

サイバーセキュリティのスキルギャップ解消と人材リテンション（離職防止）の取組み

世界経済フォーラムによると、公的機関の半数以上（52%）が、効果的なサイバーレジリエンスプログラムの作成を困難にする最大の課題として資源とスキルの不足を挙げています[4]。経験豊富なサイバー要員の不足とスキルギャップに関する報告が多く確認されており、その離職率は他の職種を8%ポイント近く上回るもので、これによりチームの一貫性を維持するのが困難になっています[5]。現時点では、職業としてのサイバーセキュリティの急成長と専門知識の持続的な必要性が相まって、教育機関が十分な資質を備えた候補者を生み出す能力を超えてしまっています[6]。

技術系と非技術系のスキルセットの断絶の拡大は、特に顕著です。優れた技術的能力が必要不可欠であることに変わりはありませんが、非技術系のスキル、たとえば、効果的なコミュニケーション、問題解決力、適応力、協調性なども、プライバシー、リスク、コンプライアンスの担当者にとってますます重要なものになっています。この断絶を解消するために、業界リーダーには、包括的なトレーニングプログラムを優先的に開発することが求められています。

人材リテンションは、この議論のもう1つの重要部分であり、KPMGのSOC調査では、セキュリティリーダーのほぼ半数（47%）が、優れた従業員を定着させることに「大きな問題」を抱えている、と回答しています[7]。

経験豊富なサイバーセキュリティ要員への需要が供給を上回り続けているなかで、CISOは、多様な人材を引き付けて定着させるための戦略を策定しなければなりません。この戦略には、人事（HR）部門と連携して多世代にわたる労働力の固有のニーズを理解して解決することも含める必要があります。

たとえば、Z世代とミレニアル世代は、労働人口のなかで最も若く急成長している世代であり、特に仕事と生活のバランス、正当な評価、そしてキャリアモビリティに大きな価値を置いています[8]。柔軟な就労形態、明確なキャリアパス、職業能力育成の機会を提供することにより、組織は、サイバーセキュリティの人材にとって魅力的な環境を生み出すことができます。

インクルージョン、ダイバーシティ&エクイティ（IDE）の取組みも、サイバーセキュリティのスキルギャップを解消するうえで重要になるでしょう。女性や多様なグループのサイバーセキュリティへの参加を積極的に支援することで、組織はより幅広い人材プールを活用し、独特な物の見方や創造的なスキルからメリットを引き出すことが可能となります。ただし、ダイバーシティを推進するだけでは十分ではありません。雇用主は、多様なスタッフメンバー、特にニューロダイバーシティ（神経多様性）のスペクトラム上に位置する人々が活躍できるような支持的で包摂的な環境も生み出さなければなりません。

4 World Economic Forum, Strategic Cybersecurity Talent Framework white paper, April 2024.
5 STI Group, The State of US Cybersecurity Employment: Analyzing Growth, Demand, and Retention Challenges, April 5, 2024.
6 KPMG, Matthew Miller, Addressing the Cybersecurity Talent Gap in the SOC, LinkedIn, August 1, 2024.
7 KPMG Cybersecurity Survey, Security Operations Center Leaders Perspective, April 2024.
8 Paychex, Navigating the New Workforce: Engaging Millennials and Gen Z in the Workplace, April 23, 2024.

サイバーセキュリティに不可欠なAIは、セキュリティを弱体化させるものではない

多くの組織は依然としてAI採用の初期段階にありますが、サイバー犯罪者は次第にAIを使って攻撃を高度化してきているため、CISOは、どうすればこのテクノロジーを信頼できる形で安全に自社のサイバーセキュリティ戦略に組み込めるかを探るべきです。先手を打つためには、AIを活用できる領域、たとえば、リアルタイムの脅威検知、より迅速なインシデント対応、プレディクティブモデリングなどに最優先で注力すべきです。

これは人員が不足しているチームの負担を減らすことにも役立ちます。AIは、セキュリティチームにとってスキルギャップの解消を可能にする真の助力者になりつつあります（ほとんどの場合、人間の働き手に取って代わるわけではありません）。実際、KPMGのSOC調査によると、少なくとも10人中6人のセキュリティリーダーが、AIについて、ID・アクセス管理（IAM）、脅威の検知と対応、ペリメーター（境界）監視などを含むすべてのセキュリティ業務の「ゲームチェンジャー」であると考えています[9]。定型的な日常業務をAIによって自動化することで、組織は効率性を大幅に高め、サイバーチームの負担を軽減して、ネットワークの防御に必要不可欠でより複雑かつ戦略的な仕事に注力できるようになります。

人的要素は、AIの導入でも重要な役割を果たすでしょう。CISOは、チームがAIシステムと連携して働くための適切なトレーニングを受けることで、AIの機能、限界、潜在的なバイアスを理解できるように取り計らうべきです。AIは職場の心配の種でもあります。そうした状況では、合意と信頼が物事を前に進めるための鍵となるでしょう。KPMGの調査によると、4分の3以上（78%）の組織が、AIについて多くのユーザーが不可解な「ブラックボックス」であるとみなし続けていることに懸念を表明しています。ほぼ同数（77%）の組織が、AIは業務遂行上の課題を引き起こすと予想しており、それが人員削減を招いたり、倫理的な懸念を引き起こしたりするだろうと考えています[10]。

ただ最終的には、人間の直観、創造性、状況理解力と、AIのスピード、スケーラビリティ、データ分析能力の融合が、よりレジリエンスの高いサイバーセキュリティのエコシステムに貢献するであろうと私たちは考えています。

人間とAIのこうした関係をより深く理解するために、KPMGはマサチューセッツ工科大学（MIT）と協力し、サイバーセキュリティ文化、その課題、そしてAIがどのような影響を及ぼすかを研究してきました[11]。多くの組織は、サイバーセキュリティ文化を醸成する取組みの初期にあり、AIを使用したセキュリティの支援となるとその状況はなおさら顕著ですが、それでも、KPMG-MITの定量的調査の回答者の74%が、サイバーセキュリティを重視する文化を構築することがAIの全社規模での統合を成功させる要となる、という意見に同意しています[12]。

認識から行動へ：積極的なサイバーセキュリティ文化を育成する

強力なサイバーセキュリティ文化が確立されるのは、組織内の全員がサイバーリスクの効果的な管理に積極的に参加したときです。CISOは、従業員はサイバーセキュリティの最弱リンクではなく、むしろ適切に参加しさえすれば従業員こそが最強のサイバー防御能力になることを認識しなければなりません。リスク回避の文化が重視されず、組織全体に組み込まれていない場合、脅威から身を守り、リスクを積極的に見つけ出すという重荷は、もっぱらサイバーセキュリティチームの肩だけにのしかかることになります。これは持続不可能であるだけでなく、潜在的な侵害に対する組織の脆弱性を放置することにもなります。

真のレジリエンスを備えたサイバーセキュリティエコシステムを生み出すために、CISOはセキュリティチームとそれ以外の従業員とのギャップの橋わたしに尽力しなければなりません。

そのためには、チームメンバーと経営幹部の両方に積極的に働きかけて、サイバーセキュリティの重要性について啓発し、組織のデジタル資産の保護を自らの課題として引き受ける能力を育成していく必要があります。

人々の心を動かしてサイバーリスクへの共通理解を生み出していくことで、組織全体がサイバーセキュリティに取り組む姿勢に変革をもたらすことができます。そうすることで、サイバーセキュリティは、どこかの他部門の孤立した業務ではなく、全員の共同責任であるとみなされるようになります。そのためには、CISOが影響力のあるリーダーとなって技術系と非技術系のステークホルダーを結び付ける必要があります。

> サイバーセキュリティは業務の遂行を妨げるものだという通念は払拭すべきであり、問題を安全かつ速やかに解決し、企業内外のステークホルダーとの間に信頼を築くものだというイメージを確立すべきです。

Breah Sandoval
Director, Cybersecurity and Technology Risk
KPMG米国

9 KPMG Cybersecurity Survey, Security Operations Center Leaders Perspective, April 2024.
10 KPMGグローバルCEO調査2024、2024年8月
11 Joint research between KPMG and Cybersecurity at Massachusetts Institute of Technology/Sloan School of Management, September 2024.
12 KPMG, A new age of cybersecurity culture: How to harness AI to promote secure workplace behaviors, December 2024.

よりユーザーフレンドリーで効率的なサイバーセキュリティ環境を生み出すために、CISOは、セキュリティプロセスの評価と改善に際して人間中心の設計アプローチを採用すべきです。これはすなわち、従業員の不満や摩擦を引き起こしているプロセスを見つけ出し、改善の対象とすることを意味します。そうしたペインポイントの多くは、生産性の低下やルール違反のリスクの増大を招きます。そのようなプロセスを注意深く分析することで、CISOは、どのコントロールが重要な資産の保護に必要不可欠であるか、そしてどのコントロールを簡素化、合理化、あるいは除去できるかを判断できます。

このアプローチにより、CISOは、従業員にとってより直感的で仕事の邪魔にならないセキュリティエクスペリエンスを生み出し、ルール遵守と共同責任の文化を強化することが可能となります。これは、サイバーセキュリティに対する肯定的な見方を促し、従業員が能動的な参加者となるよう後押しすることにつながります。サイバーセキュリティと人事（HR）管理を包括するより幅広い観点から、CISOは、従業員のセキュリティに関する知識、態度、行動様式を評価するうえで必須の分野横断的な役割を果たすことができます。その目的は、人的要素によるリスクを生じさせる潜在的な要因を明らかにし、仕事を制約する機能というサイバーセキュリティに対するマイナスイメージを転換して、ビジネスに貢献する中核的な能力という受け止め方に変えることです。

官民連携が職務としてのサイバーセキュリティを支え、キャリアとしてのその地位を高める

現在のスキルギャップを解消することに加えて、政府、学術機関、および企業は連携してサイバーセキュリティを魅力的なキャリア選択肢として奨励すべきです[13]。

この取組みは早い時期から開始すべきであり、高校入学前の若い生徒（特に女子）に働きかけるべきですが、セカンドキャリアに乗り出す人々や家族の介護休暇後で職場に復帰する人々も含めて、幅広い機会があることを紹介すべきです。

政府は、サイバーセキュリティ教育プログラムに投資し、奨学金制度やインターン制度を用意し、産業界と連携して実践的な学習経験を提供することで、この取組みを支援することができます。若い時からサイバーセキュリティの活発なエコシステムに触れてもらい、この重要な分野への関心を呼び起こせば、そこでキャリアを追求したいと考える人を増やすことができます。

早い年齢からの教育と啓発に加えて、政府と産業界のリーダーは、連携してサイバーセキュリティ分野で就労するための多様な経路を開発しなければなりません。

コンピューターサイエンスとその関連分野における従来の大学の学位は依然として有意義であっても、多くの場合、そのような学位は、急速に進化する脅威情勢や雇用主が必要とする特別なスキルに付いていくことができていません。

その対策としては、短期的な認定プログラムや特殊な専門トレーニングコースへの投資が、さまざまな経歴の就労者の速やかなスキルアップや新しいスキルの習得に役立つでしょう。より柔軟で包摂的な人材パイプラインによって、将来の課題に取り組む能力を備えた、よりレジリエンスの高い優秀なサイバーセキュリティの労働力を構築することが可能になります。

> サイバーセキュリティに関する私たちの最大の課題と脆弱性は、もはやコードやシステムに存在するのではなく、また必ずしもデジタル経路に存在するわけでもありません。むしろ、それはそうしたネットワークを毎日のように管理し、探索している人員にあります。そのような人員は、支援やトレーニング、養成を必要としており、これらによって組織のデータとシステムを1日も欠かさず守るために必要なスキルと防御手段を手に入れる必要があるのです。

Dominika Zerbe-Anders
Cyber Human Risk Partner & Solution Owner
KPMGオーストラリア

13 World Economic Forum, Why closing the cyber skills gap requires a collaborative approach, July 23, 2024.

推奨施策

CISOの役割が、もっぱらネットワークの守護者であることから、リスクマネジャー、ロビイスト、そしてインフルエンサーへと拡大していることを認識してください。影響力を行使するスキルを育成して磨き上げることで、サイバーセキュリティの重要性を効果的に伝達し、あらゆる階層と部門にわたって変革を推進できるようにしてください。

サイバーセキュリティの人的要素がセキュリティ侵害の4分の3を占めていることに鑑みて、人的要素への対応に焦点を合わせた人間中心のリスク低減戦略を導入してください[14]。

人間中心のリスクを評価し、定量化し、追跡するためにAIテクノロジーに投資し、より効果的なリスク管理を実現して、進化する脅威情勢において後れを取らないようにしてください。

従来の手法を超えた継続的なトレーニングプログラムを開発して展開し、革新的かつ没入的なテクニックを利用して持続可能な行動変革を従業員の間に生み出してください。

従業員の能力向上を図ってください。そのためには、従業員をサイバーセキュリティの取組みに関与させ、適切な教育を提供し、組織の最も優れたサイバー防御能力としての従業員一人ひとりの役割を正当に評価する文化を生み出していく必要があります。

年1回のサイバーインフルエンサープログラムを設置し、そこでスタッフや経営幹部と定期的に交流することで、サイバーセキュリティに関する意識向上と連携を図ってください[15]。

14 Verizon, Data Breach Investigation Report, 2023.
15 World Economic Forum, Bridging the Cyber Skills Gap, 2024.

Learn more

主要課題3

AIの急速な普及に対する信頼の獲得

組織は、AIがどのように事業活動に価値を付加できるかを模索し続けています。しかし、リーダーはいまだAIの採用に懐疑的であり、特にセキュリティとプライバシーに関してはその傾向が強まります。データの漏洩、不正アクセス、悪用などのリスクは高止まりしています。さらに、一部のAIアルゴリズムがどのようにバイアス、差別、その他の意図しない結果をもたらし得るのかについても明確さが欠如しています。こうした状況のなかで、今後も、AIの開発と展開をめぐる透明性、説明責任、ガバナンスの向上が引き続きCISOの最優先課題となる可能性が高いでしょう。

AIデータの管理が鍵を握る

明らかなのは、データが組織にとってきわめて重要な資産であり、AIシステムの開発と展開の原動力となっていることです。多くの企業が、膨大なデータを思いどおりに管理するための明確なガイドラインとプロセスを確立することに苦慮し続けています。このことは、データのアクセス、使用、分類、そして品質に関する課題も浮き彫りにしています。これらの要素はいずれも、AIシステムがどのように信頼できるインサイトを生成し、妥当な判断を下すかに直接的な影響を及ぼします。データの品質が悪ければ、AIモデルは信頼できない結果を生成する傾向が高まり、望ましくない性能や潜在的に有害な結果につながります。

実際、多くの組織がデータへのアクセス向上に投資していますが、KPMGの調査によると、データ中心の文化の確立とデータ相互運用性の確保に取り組んでいる組織は24%に過ぎません。これは近視眼的な姿勢であり、データを組織のすべての階層で効果的に使用して理解する能力を低下させます[16]。

さらに、組織がAIを取り入れるスピードの速さも、データ管理慣行に巨大な圧力をかけてきました。肯定的な面では、これは、信頼できるAI使用慣行と結び付けた形で優れたデータ管理を実行することの重要性を明らかにしてくれます。多くの場合、データガバナンスに対する従来のアプローチは、手動のプロセスとサイロ化したシステムを必要としています。しかし、そのようなアプローチは不十分であり、AIアプリケーションによって生成されるデータの量、速さ、そして多様性に対応できません。企業は今、変化の速さに付いていくために、よりアジリティの高い自動化されたデータ管理戦略を採用する必要があるのです。

> 企業がAIモデルの生成と訓練に自社のデータと第三者のデータのどちらを使用している場合でも、質の悪いデータはAIモデルの性能を悪化させることがすでに明らかになっています。
>
> **Samantha Gloede**
> Managing Director, US & Global Trusted Leader
> KPMG米国

16 KPMGグローバルテクノロジーレポート2024、2024年9月

このため、組織はデータを静的な資産から動的な資源へと捉え直すという根本的な転換の必要に迫られています。データの質の悪さに起因するリスクを軽減するために、組織は強力な情報ガバナンス慣行を最優先で確立しなければなりません。そのためには、データの収集、保存、管理に関する明確なポリシーと手続きを設定する必要があるほか、堅牢なデータの妥当性検証とクレンジングのプロセスを導入することも必要となります。そうすることで、企業はAIモデルの性能を改善できるだけでなく、透明性の高い責任あるデータ取扱い慣行への真摯な取組みを実証することによってステークホルダーの信頼を築くことも可能となります。

AI採用リスクの地雷原に対処する

AIの採用は幅広いリスクを伴うため、組織は注意深く対処しなければなりません。その例のごく一部を挙げれば、業務、技術、法律、コンプライアンス、人命の安全などに関するリスクがあります。AIシステムによって新たな脆弱性や障害発生点が出現すると、それがビジネスプロセスを混乱させて経済的な損失を招く可能性があります。また、技術的なリスク、たとえば、アルゴリズムのバイアスやデータドリフトは、AIモデルの正確性と信頼性を損なう恐れがあります。CEOの70%が、自組織はサイバーセキュリティに対する投資を、特に業務と知的財産をAI関連の脅威から保護する手段として増額している、と回答しているのはそのためです[17]。

プライバシー規制を遵守しないAIシステム、保護される集団を不当に取り扱うAIシステム、あるいは知的財産権を侵害するAIシステムは、法的リスクやコンプライアンスリスクを招く可能性があります。最も懸念が大きいリスクは人間の安全に対するリスクであり、特に、医療や交通の分野では、AIの障害は人命にかかわる結果をもたらす恐れがあります。

AIに起因するもう1つの重大なリスクは、「忘れられる能力」、すなわち、個人データをモデルから削除する能力が損なわれることです。この能力を維持するためには、モデルを新しいデータセットによって全面的に再訓練する必要がありますが、これは高価で複雑な作業です。

しかし、たとえ個人データが削除され、モデルが再訓練されても、他のデータポイントから学習したパターンと相関関係に基づいて個人に関する推論をかなり正確に行うことが依然として可能なのです。残念ながら、デジタルの世界で本当に忘れられる能力は、ますます実現しにくくなっています。

AIがアクセスしやすいものとなり、多くのさまざまな「スマート」製品に組み込まれるなかで、多くの組織がサードパーティプロバイダーを通じてAI機能を利用しようとしており、予算が限られた中小企業でさえ例外ではありません。これはコスト削減や迅速な導入の助けとなりますが、新しいリスクも発生させます。すなわち、組織は、AIシステムの内部的な仕組みに対して限られた可視性しか得られません。たとえば、モデルがどのようなデータに基づいて訓練されているか、どのようなアルゴリズムを使用しているか、そしてどのようなバイアスが潜在している可能性があるかを、ほとんど知ることができないのです。

「シャドー AI」、すなわち組織内で管理職やセキュリティチームの了解や監視を受けずにAIシステムを使用することは、新たに問題になっているリスクです。シャドーAIは、個々の部門や従業員個人がAIソリューションを自力で展開するときに発生し、多くの場合は、それが適切な点検を受けずに行われています。このリスクの増大は、野放しのAIの脆弱性だけでなく、バイアスのかかった望ましくない出力がビジネスの意思決定に入り込む可能性からも生じるのであり、しかも、そこからどのような影響が生じるかを誰も知ることができません。その結果、適切に管理されていないAIシステムがセキュリティエクスポージャーを発生させ、データプライバシーを毀損する恐れがあります。

こうしたリスクを軽減するために、組織は社内およびサードパーティのAIシステムの調達、展開、監視に関する明確なポリシーと手続きを、先を見越して積極的に策定すべきです。さらに、CISOには、組織がAI使用パターンを特定して分析することでシャドー AIのリスクを低減できるようにする新しいセキュリティツールや機能について幅広く調査することが勧められます。その際、事業部門のリーダーやITチーム、セキュリティ専門家と緊密に連携することが鍵となるでしょう。

> “AIリスクへの対応をCISOやCPOだけに頼り切ることは、さまざまな重要な問題、たとえば、透明性、信頼性、そして潜在的には安全性の問題さえも見過ごすことにつながります。”
>
> **Katie Boswell**
> Managing Director, Cybersecurity and Technology Risk
> KPMG米国

17 KPMGグローバルCEO調査2024、2024年8月

AI関連のリスクに対してボトムアップのアプローチをとる

AIの採用が加速しているにもかかわらず、多くのリーダーは、AIのガバナンスも、予想される複雑な技術的、倫理的、法的な影響も完全に理解しているわけではありません。その結果、多くのリーダーは事後対応的なアプローチをとっています。しかし、AIリスク管理戦略を全体的なビジネス目標やビジネス価値と整合させれば、成功の見込みがはるかに高くなります。

実際、AIシステムに対する信頼を構築して維持するために組織は、AIの判断に対するステークホルダーの利害を最重視しなければなりません。ステークホルダーには顧客、従業員、そして社会全体も含まれます。CISO、データ保護責任者、プライバシー責任者を含む組織のリーダーは、セキュリティとプライバシーをAI開発のライフサイクルのなかに組み込むうえで、きわめて重要な役割を果たす必要があります。

さらに、リーダーはAIのさまざまなビジネスケースに対する可視性を維持することで、AIが組織内のどこでどのように使用されているかを明確に認識していなければなりません。そのような知識は、より幅広いAIセキュリティの枠組みのなかで安全かつ倫理的なデータ管理慣行と適切なコントロールを開発するための指針を提供してくれます。

信頼を強化し、外部リスクを監視する

AI関連のリスクに関しては、単に問題に事後対応するだけでなく、潜在的なリスクに早期から対処しておくという先を見越したアプローチが必要となります。AIセキュリティの枠組みの確立は、はっきりとした目標地点のあるプロジェクトではありません。これは、既存のセキュリティ分野によって支えられた継続的な取組みでなければなりません。たとえば、ID・アクセス管理（IAM）、多要素認証、危機対応・回復計画など、多数の要素を通じて実施しなければならないのです。

要するに、AIシステムの継続的な監視と評価を、組織の平常業務となっているプロセスのなかに織り込むべきなのです。AI環境全体にわたるデータフローをマッピングして理解することにより、組織は潜在的なリスクと脆弱性をより的確に見極めて、対象を絞った戦略を開発できるようになります。

主な外部的な検討課題の1つは、AI関連規制の潜在的な影響です。たとえば、2024年8月に発効したEUのAI規制法です。これはEU域内で営業し、EU域内で使用できるAI製品、サービス、システムを提供するすべての企業に広範な影響を及ぼします。

EUのAI規制法は、おそらく最もよく知られた最も広範囲に及ぶ規則ですが、それでも同法はAIに関する規制機関のガイドラインの世界的な増加という、より広い動向の一部です。全世界の多くの政策決定者が、EUのAI規制法を1つの模範とみなしており、安全性、セキュリティ、プライバシー、ガバナンス、コンプライアンスのほか、公平性、透明性、信頼性などの主題に対する同法の見方に対して一定レベルの整合性を確保しようと努めています。何らかのサービスをEUに提供している企業のCISOは、EUのAI規制法がどのように適用されるかを評価し、これを遵守するための施策を講じる必要があります。

組織はすべての規制の動向を綿密に注視し続け、AIガバナンス慣行を先回りして整合させていくことで、ステークホルダーの信頼を維持し、AIのリスクと課題を緩和しながらその潜在的可能性を実現していかなければなりません。

> 多くの企業は、長い間、データプロジェクトを先送りにしてきました。必ずしもそれに価値を認めていないからです。しかし、そうした企業も、既存のデータをクリーンアップし、適切かつ正確な情報によって大規模言語モデル（LLM）を訓練する必要があることに気づかざるを得なくなってきました。残念ながら、多くのケースで、CISOは必ずしもデータのオーナーではありません。データチームとセキュリティチームの間に橋を架けて、両者の関係を強化するためには、データ分類定義を共有し、共通の行動規則を策定する必要があり、特にAIが関係する場合はそうです。要するに、不良なデータからは誤った判断が導かれるということです。
>
> **Erin Hughes**
> Head of Cybersecurity Advisory — North America
> SAP

推奨施策

CISO、データ保護責任者、プライバシー責任者を含む、さまざまな部門のステークホルダーが分野横断的に集まる場を設け、ポリシーを更新し、AIの導入に伴って生じる潜在的な影響とリスクに対処するための組織規模のアプローチと同調させてください。

規制上の義務を理解し、AIの導入に関連する既存のコンプライアンス要件を見極めてください。明確なAI利用ポリシー、標準、手続きを策定して伝達してください。他の業界リーダー、連邦政府や世界各国の政策立案者と連携し、それら関係者とのオープンな対話を維持してください。

既存のガバナンスプロセスを向上させ、明確なAI利用ポリシー、標準、手続きを伝達してください。これにはAIインテーク（受入れ）プロセスを含めるべきであり、そこでは、一貫したアプローチを通じて、AIリスクを特定し、適切なコントロールを決定し、それに対応するインシデント管理計画を策定することで、潜在的なAI関連の問題の解決を図っていく必要があります。

AI関連のリスクを緩和するために必要なコントロールを見極めてそのオーナーシップを確立し、誰がそうしたコントロールのオーナーとなって、組織の全体的なデータガバナンスの枠組みとの整合性と明確さを維持する責任を担うのかを明確に定めてください。

AIモデルのテストを実行するレッドチーム演習体制を確立し、AIモデルの堅牢性と信頼性を維持することで、不正確な情報や望ましくない情報の生成を防止してください。第1と第2の防御線の間でAIの機能をサポートする役割と責任を定義してください。

Learn more

主要課題4

AIのサイバーセキュリティへの活用：スピード競争か、安全運転か

AIの潜在的なメリットはあらゆる業界のビジネスリーダーを魅了し続けています。CISOにおいてもAIは効率性を高め、業務コストを削減し、リスク管理を向上させる手段として、また特にSOCで見受けられるようなワークロードの急増に対処する手段として注目されています。それでもまだ疑問は残っています。自組織はAIリスクの範囲を完全に理解しているか？堅牢なAI固有のセキュリティ基盤を整えているか？もし、どこから始めるべきかを、あるいはAIが最も有用な領域をどのように見定めるべきかを自分が知らないとしたら、どうなるのか？こうした状況を背景としてCISOは、AIを全社規模で導入したいという願望と、優れたセキュリティ慣行を最優先する必要性との間で慎重にバランスをとっていかなければなりません。

AIを対象とした強力なセキュリティ基盤を構築する

常に流動的なサイバーセキュリティエコシステムのなかで、攻撃者予備軍の先手を取り続けるためには、警戒だけでなくイノベーションも必要となります。すでにAIはSOCの強力なツールとして台頭し、セキュリティ担当者が脅威を検知して対応する方法に変革を引き起こしています。2024年は生成AIの年でしたが、2025年はエージェンティックAI（エージェント型AI）の年です。エージェンティックAIはセキュリティオペレーションを一変させる可能性を秘めており、「ボット」によってこれまでに見られなかった方法で、サイバー攻撃の脅威を先回りして分析し、検知し、対応することが可能になります。

実際、ほぼ4分の3の組織がAIへの投資によりビジネス価値を実現しつつありますが、そのようなメリットを大規模に実現できているのは3分の1に過ぎません[18]。

しかし、AI採用に向こう見ずに飛び込む前に、組織は基本的なサイバーセキュリティ慣行の堅実な基盤を確実に構築しておかなければなりません。これには、効果的なパッチ管理やデバイス暗号化から安全なID・アクセス管理（IAM）に至るまで、あらゆることが含まれます。AIツールの導入に簡単に飛び付いてしまうと、組織をさらに大きなリスクにさらす恐れがあります。

CISOはここで非常に重要な役割を果たします。CISOは、AIを段階的かつ戦略的に導入していくために、組織の現在のサイバーセキュリティ体制を評価し、ギャップや弱点を見つけ出さなければなりません。要は、連携を欠いたちぐはぐな導入を避けるために、投資を緻密な計算に基づいて戦略的に実行すべきだということです[19]。

> 単刀直入に言えば、パッチ管理や権限付与がきちんとできていないのにAIツールを導入しても、まるで無意味だということです。基本を疎かにしてはいけません。

Koos Wolters
Head of Cybersecurity
KPMGオランダ

18, 19 KPMGグローバルテクノロジーレポート2024、2024年9月

人材をめぐる諸問題：AIのスキルギャップを解消する

サイバーセキュリティにおけるAIをめぐる議論は、必然的に人材の話になります。AIを理解するという点だけでなく、サイバーセキュリティの領域でAIを効果的に活用するという点でも、顕著なスキルギャップが存在します。AIテクノロジーの開発ペースは、市場で獲得できるスキルが追い付けないほどの速さになっており、特に生成AIについてはそれが言えます。

従業員のAIスキルを強化することは、この情勢におけるCISOの最重要課題の1つです。今、セキュリティチームが学習に取り組んでいるのは、プロンプトの質の重要性です。AIモデルと対話しながら質問するときに使用するプロンプトの質は、出力の正確性と適切性に大きな影響を与えるからです。ベストプラクティスを確実に理解しておかないと、セキュリティチームは、AIシステムから期待どおりのインサイトや実践的なインテリジェンス（意思決定に役立つ情報）を得ることに苦労するでしょう。

このスキルギャップを解消し、セキュリティチームがAIテクノロジーの急速な進歩に追随できるように取り計らうために、CISOは、チームと自分自身のために、スキルアップとトレーニングの企画に優先的に取り組まなければなりません。そうすることで、CISOは、人材ニーズを正しく見極めて、最適な人材を雇用することが可能となります。そのためには、プロンプトエンジニアリング、データ分析、モデル評価などのAIのコンセプトに焦点を合わせた教育プログラムに投資することも必要となります。

CISOは、継続的学習の文化を育成することによって、セキュリティ担当者が新しいAIの機能を探究し、各自の発見を同僚と共有するように働きかけるべきです。そして、セキュリティ担当者とそのチームが、知的好奇心と知識を高めることで、AIのパワーを活用し、組織のデジタル資産を保護し、サイバーレジリエンスを増大させるように奨励すべきです。

AIの誇大宣伝と現実を見分ける

KPMGの調査によると、サイバーセキュリティにおけるAIをめぐる誇大宣伝が、さまざまな組織に「乗り遅れる不安」（FOMO：fear of missing out）の増大を招いており、特に、経営幹部や取締役会レベルでそれが顕著であることが判明しています。実際、回答者の82%が、競合企業に後れを取らないことを目的として、仮想現実（VR）や拡張現実（AR）のような、AIによって実現されるテクノロジーに投資しようとしていることを認めています[20]。しかし、リーダーは、AIの能力と限界の実態に基づいた意思決定を下す必要があります。AIはサイバーセキュリティに革命を起こす可能性を秘めていますが、現在のSOCにおけるAIの使用はまだ比較的未成熟であり、範囲も限定されています。

CISOは、現実に見合った期待を設定して、AIの本当の潜在的可能性をありのままにシニアマネジメントと取締役会に伝える必要があります。そのためには、現在の限界を明確に示し、AI採用に対して戦略的なアプローチをとることが必要となります。実験の文化を奨励することで、CISOは、組織に固有のニーズや優先課題と一致する適切なユースケースを見つけ出す手助けができます。AIが成熟と進化を続けていくなかで、CISOは常に警戒を緩めずに、AIの能力と限界を見定めていかなければなりません。

> サイバーセキュリティの世界で、私たちは偽陰性（検出漏れ）よりも偽陽性（誤検出）に対して寛容になっています。何か悪いことが起こっているとAIが判定し、手動プロセスを通じて捜査するように、そしてネットワークが不正にアクセスされているかどうかを調べるように促してくれる方が、実際にサイバーセキュリティの問題が発生しているのに、それを知らずに何も対策を発動しないでいるよりも望ましいと思うからです。

Matt Miller
Principal, Cybersecurity Services
KPMG米国

20 KPMGグローバルテクノロジーレポート2024、2024年9月

最も効果が大きいユースケースを見つけ出して投入する

CISOは、最も大きな効果を生み出し、組織の固有のニーズに合致しているAIユースケースの候補を慎重に評価して、優先順位を付けなければなりません。有望な領域の1つは、大量のデータを分析して潜在的な脅威や異常を検出することです。なぜならAIは、膨大な情報を処理してインサイトを引き出すことに秀でているからです。さらに、AIは反復的な手作業を自動化することにも使用できるため、人間のアナリストをそうした作業から解放し、より複雑で戦略的な活動に注力してもらうことができます。AI主導の分析を利用すれば、開発者は小さな脆弱性が大きな問題に発展する前にパッチを適用することも可能となるでしょう。

AIの可能性を探りながら導入のアイデアを提案する権限と能力をチームメンバーに与えることで、CISOは、AIを最も効果的に展開できる領域を発見することができます。現実世界の問題の解決に役立つユースケースを注意深く評価・選定することで、CISOは、AI投資について対象を明確に絞り込み、その効果を高め、組織の全体的なサイバーセキュリティ目標およびビジネス目標と連携させることが容易になるでしょう。

AIを使用したサイバー攻撃に備える

AIテクノロジーを採用してサイバーセキュリティの取組みを拡大・強化する一方で、CISOは、AIを使用した攻撃が引き起こす新たな脅威に応戦する体制も整えなければなりません。

特に懸念が大きい事例の1つはディープフェイクの増加であり、AIアルゴリズムが迅速に、容易に、そして安価にきわめてリアルで本物そっくりの、説得力ある、改ざんされた音声・画像コンテンツを創り出すことができるという現実があります。それどころか、すでにディープフェイクテクノロジーの大衆化が進行して、基本的にどんな脅威行為者でも最小限の労力でこのテクノロジーを入手して攻撃のために使用できる状況になっています。

この意図的に人を騙そうとする技術は、ソーシャルエンジニアリング攻撃や誤情報の拡散にますます広く使用されるようになっているため、サイバーセキュリティチームが本物のコンテンツと詐欺コンテンツとを見分けることは一層困難になっています。

また、コールセンターの音声検出や生体認証におけるAIの使用の増加も、その意図とは裏腹に、ディープフェイクの検知と防御をかえって困難にしています。攻撃者は、その同じテクノロジーを悪用してセキュリティ対策を回避し、システムを不正に操作する可能性があるからです。

そのような進化するリスクと戦うために、CISOは、AIを使用した脅威の最新動向に関する情報収集に努め、それに応じて防御戦略を調整していかなければなりません。そのためには、従業員の教育が必要となるほか、高度なAI主導のセキュリティツール（たとえば、不正操作されている可能性があるコンテンツを検知して警告を出すことを目的としたツール）に投資する必要も生じるでしょう。サイバーセキュリティの効率と効果に及ぼすその影響を最大化するために、CISOは、いかなるAIの導入展開も、明確な役割、責任、状況によって支持されるように取り計らう必要があります。

> 残念ながら、AIに関しては、セキュリティ部門が多くの法的責任を負います。CISOは、すでに難しい立場に置かれていましたが、AIが普及していくスピードが非常に速いため、LLMの大規模な導入に着手しようとする際に、優れたセキュリティとはどのようなものかをめぐって、CISOのストレスのレベルは急激に上昇しています。しかし、効果的な戦略とツールも提供されており、それを利用すれば、この進化する情勢に対処することは可能です。

Terence Jackson
CISM, CDPSE, GRCP
Customer Security Officer
Microsoft Security Solutions

推奨施策

より高度なセキュリティ活動（たとえば、AIの導入や全社規模への拡大など）に取りかかる前に、優れたセキュリティの基礎、すなわち、パッチ管理、データの保護、IAMなどに取り組んでください。

AI利用者の役割と責任に対する明確なビジョンを提供し、AIがどのような状況、どのような取組みで使用されているかに関する透明性を生み出してください。

AIの社内利用や敵対者による使用に伴うリスクに対する従業員と顧客の意識向上を働きかけてください。

セキュリティ担当者のスキルアップを最優先で実施し、必要な技術的スキルを身につけさせることで、担当者が最新のAI動向に立ち後れないように取り計らってください。

SOCのレベル1とレベル2のタスクを対象としたAIのユースケースの評価を継続してください。

AIに対して知的好奇心を持つように、そして実験のアイデアやユースケースの候補を出すように、チームに働きかけてください。

Learn more

主要課題5

プラットフォームの統合：可能性を受け入れながら、リスクも認識する

ますます複雑化するサイバーセキュリティリスクに対応するため、組織はデジタル資産を保護するためのツールやソリューションを次々と導入しています。エンドポイントセキュリティやセキュリティ情報・イベント管理（SIEM）から、脆弱性管理、IoTセキュリティ、拡張検知・対応（XDR）、マネージド検知・対応（MDR）に至るまで、利用可能な機能の選択肢は膨大な数になります。CISOは、このような多種多様なツールの寄せ集めを管理、維持、統合することに苦労しています。さらに悪いことに、データから有用なセキュリティインサイトを得ることよりも、統合作業に多くの時間が費やされています。こうした状況を受け、多くの組織はセキュリティプラットフォームの導入を検討しており、それによる効率性の向上、可視性の改善、セキュリティ環境の制御強化が期待されています。しかし、このようなプラットフォーム統合への広範な移行には、利点と同時に隠れた落とし穴も存在します。

プラットフォーム統合の意義を認識する

大規模な組織は、プラットフォーム統合への移行に特に熱心です。その理由の1つは、共通性を欠く多数の異質なツールが膨大な量のデータとシグナルを生成しており、またそうしたツールがそれぞれセキュリティポリシー全体の異なる側面を執行していることです。この複雑さは、統合化と一貫したセキュリティポリシーの適用を困難にします。異種のソリューションを統合することでサイバーセキュリティツールセットを合理化すれば、リーダーは組織のセキュリティ情勢をより明瞭に、より包括的に見わたすことが可能となります。これは転じて、一貫したセキュリティポリシーの広範な適用を促進するため、潜在的なギャップと脆弱性を減少させることにつながります。

また、プラットフォームの統合はゼロトラストの枠組みという観点からも重要です。根本的に、ゼロトラストは、組織のネットワーク内のあらゆるやり取りの審査を要求します。それには、たとえば、ネットワークへのアクセスに使用されたデバイス、適用された認証手法、要求された具体的なデータなども含まれます。しかし、組織が統一性のない多数のセキュリティツールに依存していると、ゼロトラストモデルの導入は途方もなく困難になります。そこでプラットフォームを統合することで、細分性の高いアクセス制御を適用して、必要な可視性を提供することが可能になります。

> “特定のプラットフォームや規律・分野（たとえば、アイデンティティ）に統合することで、スケールメリット（規模の経済）が得られます。優れたテクノロジーを厳選した環境をセキュリティチームへ提供することで、能力の領域を超えてより効果的に機能する、多才でバランスのとれたセキュリティチームを形成することが可能になります。”

Jim Wilhelm
Principal, Global Microsoft Security Leader
KPMG米国

さらに組織は、IDの管理、データセキュリティ、脅威管理、エンドポイント保護、ネットワーク制御などに関して、規模の経済からメリットを引き出すことができます。統合は大幅なコスト削減を生み出しますが、これはツールが減れば、必要となる保守、トレーニング、サポートも少なくなるからです。また、データソースの統合によって、セキュリティチームはAIのパワーをより適切に活用することも可能になります。

生成AIの機能を使いこなす能力をセキュリティ要員に付与し、SOCやその他の環境で生産性を向上させるためには、セキュリティデータ（ロギングとモニタリング、シグナル、脅威インテリジェンス、認証ポリシー、権限の割当て、ユーザーアカウントデータなど）を理解することが必要不可欠です。この取組みの副産物はデータの統合であり、またAIを利用したサイバープログラムに向けた改革の第一歩を踏み出すことにもつながります。

潜んでいる落とし穴を回避する

プラットフォームの統合は数多くのメリットをもたらしますが、CISOは潜在的なリスクと課題を認識することがきわめて重要です。重大な（しかし定番の）懸念の1つは集中リスクです。すなわち、組織が単一のベンダーやプラットフォームに過剰に依存することの危険性です。「たくさんの卵を1つの籠に入れる」ような1社依存は、クラウド採用の初期以来、CISOが常に警戒してきたリスクであり、特定の製品やプラットフォームに不正侵入経路や脆弱性が潜んでいた場合に、企業はより大きなリスクにさらされます。最近よく話題になるIT関連の社会的混乱でも、このリスクに注目が集まりました。したがってCISOは、合理化されたセキュリティスタックからメリットを引き出すことと、単一障害点（SPOF）の潜在的な影響を軽減することの間で、難しいバランスを維持しなければなりません。

商業的な観点から見たもう1つの課題は、特定ベンダーによるロックインであり、これは今後増える可能性のある問題です。組織が特定の製品やサービスへの依存を深めていくうちに、かつて選択した既存プラットフォームがすでに自社のニーズに合っていないことに気づくかもしれません。そうした場合に、別のベンダーに切り替えようとしても、それは高コストの複雑な取組みになります。切替えによって重大な互換性の問題が生じたり、トレーニングの追加が必要になったりすることもあります。そうしたリスクを軽減するために、CISOは、プラットフォーム統合に対してハイブリッドアプローチを採用することを検討すべきです。

基本的なセキュリティ機能をプラットフォームプロバイダーによって実現し、足りない部分を目的別の専用ソリューションによって補強することで組織は、変化する環境に適応するために必要なレジリエンスと柔軟性を手に入れることができます。そうすることで、CISOは、プラットフォームを基盤とするアプローチの中核的なメリットを活用しながら、単一のベンダーやプラットフォームへの過剰な依存がもたらし得るデメリットを最小限に抑えることができます。

統合の意思決定をCISOが単独で下すことは稀です。むしろ、CISO、CIO、CFO、COO、CDOなどの主要なステークホルダーが関与する共同作業であるのが通例です。すべてのリーダーからさまざまな物の見方が提供されることで、組織の全体的なセキュリティ戦略とビジネス目標に見合ったプラットフォームを選択することが可能になるからです。

人材開発とスキルアップで後れを取らないようにする

プラットフォームの統合を進める時は、人材開発とスキルアップの取組みも同じように進化する必要があります。サイバーセキュリティ担当者は、従来と非常に異なる新しい環境に適応し、そこで能力を発揮できるように準備する必要があります。CISOは、SOCからモニタリング担当者までセキュリティのすべての領域にわたって、継続的な学習と人材開発を最優先しなければなりません。

> “CISOとその組織は人材不足に懸念を抱いています。そうした状況下でサイバーセキュリティを向上させるには、デジタル資産の保護に使用するツールとソリューションの数を減らし、簡素化・統合する必要があります。”

Motoki Sawada
Partner, Technology Risk Services
KPMGジャパン

スキルと知識に適切に投資することで、セキュリティチームは、プラットフォーム統合という機会を最大限に活用するために必要なアジリティと専門知識を確立することができます。業務に使用するツールを絞り込むことで、セキュリティ担当者は、特にインパクトの大きな取組みに時間とエネルギーを傾注してより効果的に脅威に対応することが可能となります。

また、プラットフォーム統合によって、CISOは、人材開発戦略を最大限に活用する絶好の機会が得られます。関係するベンダーの数が減るため、CISOはトレーニングの労力を合理化することができ、チームのスキルアップが容易になって費用効果が高まります。SOCのエンジニアとアナリストも、統合されたツールセットに関するトレーニングを受けることを通じて、より効率的かつ効果的にそれぞれの役割を遂行できるようになります。これは組織の全体的なセキュリティ体制を強化することに役立ちます。人材開発をプラットフォーム統合の目標と整合させることで、CISOは、継続的改善とリスク低減の好循環を生み出すことができます。

変化において後れを取ることなく、ビジネスのスピードでの運用を実現する

組織が成長し、新しい市場や地域に進出するにつれて、サイバーセキュリティチームに対する要求も増大しています。CISOは、ユーザー、デバイス、およびデータポイントの増加と戦わなければなりません。それらはすべてが堅牢な保護とモニタリングを必要とするからです。

その一方で、私たちは、複数のクライアントから、予算が相変わらず制限されており、前年比で微増にとどまっている、という話を聞きました。そうした状況で、サイバーセキュリティ支出を正当化し、経営幹部に対して明確な価値を実証しなければならないという重圧がかつてなく高まっているため、CISOは、絶え間なく、既存の投資からより大きな価値を引き出そうと努める必要に迫られています。そこでの重点は、目に見える具体的な価値と投資収益率（ROI）を生み出すような賢明な戦略的投資を実行することに置かれなければなりません。

さらに、セキュリティはビジネスと同じスピードで運用される必要があります。しかし、ビジネスが成長し、新しいテクノロジーを利用した機能が次々と展開されるなかで、セキュリティツールとの統合に過大なコストをかけることは不可能です。したがって、統合は柔軟性と適応性の高い方法で行わなければなりませんが、プラットフォームアプローチは、長い目で見るとこのプロセスの反復性とアジリティを高めることに役立ちます。セキュリティを組み込む方法が、新しいアプリケーションやテクノロジー資産に高度な認証手法を適用することであっても、シグナルベースのアクセス制御であっても、共通のパターンとプラットフォーム型の統合アプローチは、レジリエンスと採用スピードを高めることに寄与します。

CISOは、プラットフォーム統合への投資が、重大な能力ギャップを解消し、脆弱性とリスクを減少させ、全体的なビジネス目標を後押しすることにどのように役立つかを明確に主張できなければなりません。財務責任と戦略的投資の適切なバランスをとることによって、CISOは、今後の発展に向けて組織を優位に立たせることができます。

> **従来**：サイバーセキュリティ ISVの大半は、多種多様なプラットフォームと連携できると主張していますが、市場はすでに相互運用性と導入効果の達成度はさまざまであり、しかも多くの場合、人件費と保守コストが高くなるということに気づいています。
>
> **新世代**：新しいサイバー ISVの一部は、これまで統一性を欠いていた多様な製品を新しい単一のシームレスなツールへと統合し、しかも機能の拡大とデータアクセス能力の向上を実現しようとしています。これはより効果的なアプローチであり、企業はそのような環境を顧客に合わせてカスタマイズして個々の状況に適合させることが可能となり、データ、スピード、規模、効率性、コスト、機能などの改善に結び付けることができます。
>
> **Philip Bice**
> Global Lead — Service Provider Partnerships
> Google

推奨施策

現在のベンダーを評価し、自社のテクノロジー環境に対するプラットフォームの互換性を判断し、ベンダー選定とパフォーマンス監視に関する明確な基準を確立することで、統合のための強固な基盤を築いてください。

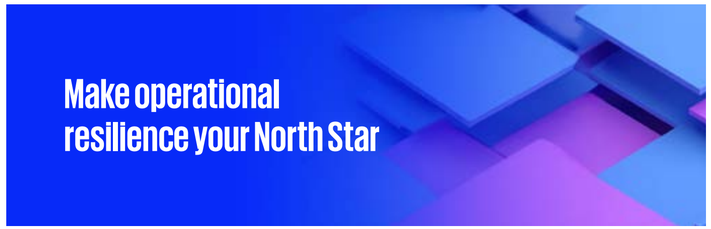
セキュリティチームのトレーニングとスキルアップに投資し、統合されたツールセットを効率的に取り扱えるようにしてください。

統合されたプラットフォームと専門ツールを組み合わせたハイブリッドアプローチがメリットを提供できる領域を明らかにし、両者間の適切なバランスを判断してください。バックアップとリカバリーの手続きを確立してレジリエンスを確保してください。

継続的な監視・監査プロセスを導入して、プラットフォームの性能を維持してください。

完全な統合を実現できない場合があることを認識し、どの領域で専用のツールやプロバイダーが必要となる可能性があるかを明らかにしてください。統合を段階的に進めるアプローチを策定し、まず効果の大きな領域を優先してください。

Learn more



主要課題6

デジタルIDの重要性

デジタルID（アイデンティティ）がよりアジリティと効率性が高いデジタル世界への道を切り開こうとしています。しかし、デジタルIDを不正から守ることはますます困難になっています。その理由は、不適切なシステムやコントロールから、ディープフェイクの増加まで、多岐にわたります。その結果、デジタルIDのベリフィケーション手法のなかに、より高度な新しいセキュリティメカニズムを組み込む緊急の必要性が生じています。しかし、さらに重要なのは、CISOと意思決定者がこの状況をより深く理解し、定着しているプロセスを再考し、しっかりとした原則に根差した革新的なシステムに投資する必要性です。

デジタルID管理の複雑化

突き詰めて言えば、各個人は当人だけに固有の一意のIDを所有しています。しかし、さまざまな場面、たとえば、政府、金融、ライフサイエンスなどの状況ごとに、IDは特定の機能を果たすように、あるいは多様なニーズを満たすように、さまざまな方法で適用されます。したがって、個人のIDは、その本質においては唯一無二であるにもかかわらず、その解釈と検証は組織の状況に応じて変わってくるという事実を理解することが非常に重要なのです。

組織は、個人のIDのインテグリティ（完全性）を維持しようと努めるなかで、次第に高度な認証テクノロジーに目を向け始めており、たとえば、指紋、顔、声、網膜スキャンなどの生体認証の技術によって、セキュリティの強化とプロセスの合理化を図ろうとしています。しかし、そのようなモダリティ（生体認証に使用される生物学的特徴）が発生させるリスクの影響は、一般的なデータ侵害の範囲をはるかに超えてしまう恐れがあります。たとえば、もしそのような一意のIDが漏洩した場合、個人は、なりすましや悪用の可能性に持続的にさらされ、しかもそれを容易には是正できないという事態に直面します。なぜなら、生体測定上の特徴は生まれながらの永続的なものであり、別のものと置き換えることが本質的に不可能であるからです。もう1つの懸念は、生体認証データの収集と処理が、生体認証システム内でデータディスクリミネーション（収集したデータに基づいて特定の属性を持つ人や集団を差別的に取り扱うこと）やバイアスを引き起こす可能性があることです。したがって、データコード化慣行のダイバーシティと正確性を維持し、公正性と信頼性の高い本人識別を保証することが、かつてなく重要になっています。

ディープフェイクはもう1つの非常に手ごわい難題です。なぜなら、ディープフェイクは現実と改ざんの線引きをますます不明瞭にするからです。最新のAIテクノロジーがより強力に、より幅広いアクセスが可能に、そして安価になるにつれて、個人情報（特に声と顔）はますます改ざんと乱用の被害に遭いやすくなっています。ディープフェイクは、なりすましや誤情報の拡散という点で重大な脅威をもたらす一方で、コンテンツクリエイターやコンテンツ利用者の双方にとって機会にもなります。

認証手法の向上は、コンテンツクリエイターの間で説明責任、倫理基準、透明性を高めることに役立つでしょう。その結果として意識向上が生じれば、利用者の側で真偽を識別する能力の向上につながります。認証機能の強化に投資することは、デジタル情報の公正性を守り、私たちが利用するコンテンツへの信頼を回復することに寄与するでしょう。

組織にとって懸念が高まっているもう1つの領域は、マシンID（機械のアイデンティティ）の急増です。特に、人間以外の特権サービスアカウントが、機密データへのアクセス権限を持って特定のアプリケーションを実行するケースに関して、懸念が拡大しています。モノのインターネット（IoT）の急速な普及に伴って、マシンIDは組織にとって管理が難しい大きな課題になり始めています。CISOがチームの意識の大半を人間によるアクセスに向けさせているのは当然であるとしても、その一方で、人間以外のネットワークユーザーについても記録を保持し、それらユーザーが攻撃を受けて不正アクセスされた可能性があるか、もし受けた場合はいつそれが起こったのかも監視しなければなりません。

なぜ企業は将来を見据えたデジタルID戦略を必要とするのか

商業的観点から見ると、B2BでもB2Cでも、デジタルIDの管理は、組織と個人（組織のそのネットワークにアクセスする個人）との間に信頼を築くことを軸として実行されます。企業は、ユーザーに自分自身の個人情報をコントロールする手段と情報の使途に関する透明性を提供することで、顧客ベースのなかに信頼とロイヤリティを育てることができます。この信頼を築く基盤となるのは、個人が自分の必要とする資源にアクセスできるという保証であり、アクセス権限が不要になった時点で迅速に無効化されるという確信であり、そして、システム内で実行されるすべての活動がログに記録されて完全に追跡可能であるという確実性です。

この信頼を維持するためには、プロビジョニングと継続的運用からアクセスのデプロビジョニングに至るまでのID・アクセス管理（IAM）のライフサイクル全体に対する先を見越したアプローチが必要となります。これは特に重要であり、その理由は、長年にわたって勤務している従業員には非常に多くのシステムに対するアクセス権限が集積して、大きな権力が与えられてしまうことがあるからです。そのような特権の蓄積に起因するリスクを軽減するために、CISOとそのチームは、サイバーセキュリティの2つの主要原則であるLeast Privilege（最小権限：特定の情報や権限を必要最小限の人間に必要最小限の時間に限って付与する）とNeed to Know（知る必要性：知る必要がある者に対してのみ情報を与え、知る必要のない者には与えない）を厳守しなければなりません。

個人が特定の業務に必要不可欠なシステムにしかアクセスできないように取り計らうことで、組織は、不正行為者が強力な管理者アカウントを不正使用して機密データへのアクセスを得る危険性を大幅に低減することができます。

従業員のIDと消費者のIDの境界がますます見分けにくくなるなかで、組織は、包括的なアプローチを採用しなければなりません。従業員に対しては、堅牢なデジタルIDの枠組みによって、機密情報へのアクセスが、明確に定義された役割と責任に基づいて付与されるように取り計らうことができます。そのためには、確固としたオンボーディングとオフボーディングのプロセスを導入すること、そしてアクセス制御の定期的な審査と更新を実施することが必要となります。

また、効果的なデジタルID戦略は効率性とユーザーエクスペリエンスを大幅に高めることもできます。合理化されたプロセスは、反復的な事務作業（たとえば、税の申告、保険金請求、病院での受診などに伴うフォームへの入力）を行う必要性を最小限にまで減らすことができます。これによって、従業員と顧客の双方にとって煩わしい作業や待ち時間が減少します。組織が成長とイノベーションの促進を目的にデジタルテクノロジーへの依存を高めていくなかで、強力なデジタルIDの枠組みこそが全体的なビジネス戦略の基礎となります。確固とした透明性の高いユーザー中心のデジタルIDソリューションに投資することで、企業は今後の発展に向けて優位に立つことができます。

> 組織はセキュリティの人的な側面に重点を置く傾向があります。なぜなら、それは具体的で目に見えるからです。マシンIDとその使途を検証したり、そのIDがシステム内でいつ作成されたかを確認したりすることの方がはるかに困難です。

Anubha Sinha
Partner, Digital Trust & Identity
KPMGオーストラリア

政府は信頼されるデジタルIDエコシステムをどのように実現できるか

デジタルIDは依然として、確固とした効率的なベリフィケーションプロセスをさまざまな政府サービスや取引において可能にするための非常に重要なタッチポイントです。世界の政府とグローバル企業は、個人のIDとビジネス関連のIDを対象とする、より優れたソリューションを積極的に探し求めています。たとえば、オーストラリア政府は先ごろ、“Trust Exchange”という名称の包括的なデジタルIDプログラムを導入しました。これは、身元認証が必要となるさまざまな領域（たとえば、政府、福祉、金融、就労など）のIDを統合したデジタルウォレットを特徴としています[21]。

Trust Exchangeは、複数のサービス間でのデジタルIDベリフィケーションを促進することで、そこで共有されている個人情報のコントロールを国民に付与しつつ、組織間の信頼の向上を図ろうとしています。エストニアはもう1つの例であり、国民一人ひとりにデジタルIDを発行します。このIDは出生時に発行され、一生涯にわたって有効です。国民は、自分のIDがいつどこで認証されたかに関して完全な透明性が得られるため、プライバシーに関する懸念の払拭に役立ちます[22]。

このような有望な展開とは裏腹に、グローバルなシステム同士の相互運用性がまだ課題として残っています。その理由は、個人情報や生体認証データの取扱いに関する規制、リスク選好度、そして世論が異なっているからです。信頼性の高いIDのやり取りに関するグローバルな合意に関しては、有志の国による連合が出現する見込みもあります。たとえば、共通の信頼できるIDの枠組みを開発するためのEUの相互運用可能な枠組みなどです。しかし、すべての国が同じ価値を重視しているわけではありません。特に、プライバシーに関してはそうであり、それが短期的な相互運用性の範囲を狭めてしまう可能性があります。

CISOはどのようにデジタルID戦略の導入を先導できるか

デジタルID戦略の策定にあたって、CISOは、政府、規制機関、そして企業の間を取り持つ役目を果たすことができます。セキュリティ環境が複雑化して、ID管理プロセスの大半はCISOの直接的なコントロールが及ばなくなっていますが、そうした状況のなかでも、CISOは、積極的かつ協調的な考え方を身につけ、ステークホルダーにトップダウンで働きかけながら意識啓発を図り、必要な変革を推進していかなければなりません。

セキュリティのリーダーに求められているのは、ユーザーのニーズと期待に応えること、中核的なセキュリティ原則を確実に遵守すること、そしてAIやディープフェイクのような新たに出現するテクノロジーがもたらし得る影響について情報収集し続けることです。さらに、CISOは、デジタルIDに関する議論を取締役会レベルで上程することで、経営幹部がその重要性を理解して必要な支援を提供するように取り計らわなければなりません。

デジタルIDをサイバーセキュリティにおける新しいペリメーター（境界防御）として重視し、セキュリティの文化を組織全体で育成することにより、CISOは、効果的なデジタルID管理の基盤を築くことができます。

> 透明性は、デジタルIDの世界における信頼の基盤です。個人情報がどのように収集され、使用されているかをオープンに共有すれば、プライバシーに関する懸念を軽減できるはずであり、ユーザーは十分な情報を得たうえで自分のオンラインプレゼンスに関する選択を行うことが可能になるだろうと、私は考えています。プロセスの透明性が高まるほど、そのシステムに対する人々の信頼も増大するでしょう。

Imraan Bashir
Partner and National Public Sector Cyber Leader
KPMGカナダ

21 Australia Department of Social Services, Trust exchange drives secure digital services, August 13, 2024.
22 e-Estonia, Solutions and services: e-Identity, 2024.

推奨施策

中核的なセキュリティの基本原則、たとえばデータの最小化や不要データのタイムリーな削除などを遵守することで、最高水準のデータ保護を維持してください。

すべてのステークホルダーにトップダウンで働きかけることで、意識啓発を図り、持続可能なデジタルID・アクセス管理をめぐるニーズに対処してください。

他の事業部門との間に強力な関係と信頼を築くことで、効率的な協力と連携をID管理プロセスの領域で実現してください。

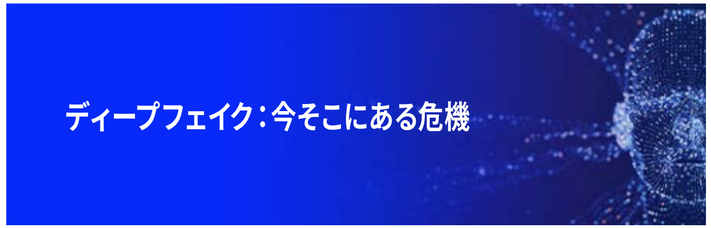
デジタルIDをサイバーセキュリティにおける新しいペリメーター（境界防御）として重視し、デジタルIDが組織の資産とステークホルダーの保護に果たす役割を十分に理解してください。

AIとディープフェイクがデジタルIDに及ぼし得る影響について、幅広い情報の入手に努め、新たに出現する脅威と脆弱性に積極的に対処してください。

セキュリティを維持しながらIDの取扱いを合理化してください。クレデンシャルの発行と利用を簡素化し、パスワードを減らすなどによって、ユーザーエクスペリエンスの向上を図ってください。

> “ディープフェイクテクノロジーの進歩につれてIDの不正使用や詐欺のリスクが増大しており、デジタルIDを確実に保護することが新たな脅威から消費者と組織の双方を守るために必要不可欠になっています。”
>
> **Nancy Chase**
> Global and Canadian National Leader, Risk Services
> KPMGインターナショナル

Learn more



主要課題7

スマートエコシステムのためのスマートセキュリティ

テクノロジーの進歩とともに、スマートデバイスとIoT製品が爆発的に増加し、私たちの身の回りの世界とのかかわり方は大きく変化してきました。家電製品やウェアラブル機器から産業用機器や自動車に至るまで、コネクテッドデバイスの激増は、サイバーセキュリティ担当者が防御すべき新たな脆弱性を生じさせており、企業と消費者の双方に影響を及ぼしています。リスクの多くはまだ完全に姿を現してはいません。ネットワークに接続されたデバイスによってアクセスされる組織のデータを保護することは、業界全体とインフラストラクチャのインテグリティ、安全性、およびセキュリティを維持するために必要不可欠になっていくでしょう。ほんの10年前に使用されていた従来の手法ではもう十分ではありません。ネットワークに接続されたコネクテッドな資産を、そのライフサイクル全体を通じて、また組織のエコシステム全体にわたって、安全に保護するための効果的な戦略を開発することが急務なのです。

スマート製品の保護におけるCISOの役割

工業生産、エネルギー、防衛をはじめとする幾多の業界の組織が効率性の向上と競争優位性の獲得を目指すなかで、消費者は、便利さ、アクセスの容易さ、そしてパーソナライズされた体験を求めています。このような状況を背景として、私たちは、相互接続されたスマートデバイスの急増を予想しており、それがグローバル経済のほぼあらゆる部門、特に、医療、交通運輸、製造、小売業界を変革するだろうと考えています。

そうした製品が、私たちが「Smart-X」テクノロジーと呼んでいるものを原動力として、ますます企業のバックエンドシステムやデータベースと接続されるようになるにつれ、CISOはセキュリティに対してより製品中心のアプローチを取り入れる必要が生じるでしょう。CISOは、組織のプロセスと製品固有のプロセスに深く関与することで、セキュア設計の段階からデバイスの廃止に至るまでのスマートデバイスのライフサイクル全体を通じてセキュリティが組み込まれるように取り計らう必要があります[23]。KPMGの調査によると、72%の組織がサイバーチームをテクノロジー関連のプロジェクトに最初から参加させることでセキュリティ・バイ・デザインの原則を取り入れています[24]。

初期の設計・開発の段階に始まり、継続的な保守・更新に至るまで、CISOは、さまざまなチームと緊密に連携しなければなりません。たとえば、エンジニアリング、開発、製品サポートと連携して、コネクテッドデバイス特有のセキュリティ課題に対処する必要があります。

このようなテクノロジーの拡大は、新しいリスクと脆弱性をもたらします。さらに、この新たな現実によって、サイバーセキュリティはより幅広い社会にとってはるかに身近な問題となっています。つまり、何らかの異常が生じた場合、それはビジネスの問題だけでは済まなくなっているのです。セキュリティ侵害の影響は、ちょっとした不都合から、公共の安全、治安、プライバシーへの大規模な脅威までさまざまです。したがって、Smart-Xテクノロジーのセキュリティを維持することは、単に個々の事業体の保護に欠かせないだけでなく、さまざまな社会部門やインフラストラクチャ全体のインテグリティ、安全性、セキュリティを守るためにも必要不可欠なのです。

> “CISOは、スマート製品を取り巻くサプライチェーンが極度に複雑であることを認識しなければなりません。セキュリティに関しては、そうした外部のベンダーとプロセスをエンドツーエンドで綿密に管理する必要があります。あらゆる側面が相互に結び付いているからです。”
>
> **Marko Vogel**
> Partner, Cybersecurity
> KPMGドイツ

23 KPMG, Smart-X: A holistic approach to cybersecurity for smart devices, January 2024.
24 KPMGグローバルテクノロジーレポート2024、2024年9月

自動車とテクノロジーの出合い

昔から存在した機器が著しい変化を遂げて現在ではスマートデバイスに分類されるようになった一例は、自動車です。近年、自動車は単なる機械的な装置から複雑なコネクテッドデバイスへと進化を遂げました。現代の自動車は、たくさんのセンサー、プロセッサー、ソフトウェアシステムを装備しており、自動運転、リアルタイムのナビゲーション、OTA（over the air：無線）アップデートなどが可能になっています。さらに、OEM（相手先商標製品製造業者）が追加機能をサービス方式（as a service）で提供するようになってきており、高度な車両機能をサービスベースで利用する方式への移行がはっきりと見て取れます。

明らかなのは、私たちの自動車とのかかわり方がコネクテッドビークルによって根本的に変化していることです。しかし、ますます進行する機能の高度化は、サイバーセキュリティ担当者に新しい課題も突き付けています。自動車がソフトウェアとネットワーク接続への依存度を高めるにつれて、自動車も、他のコネクテッドデバイスを苦しめているのと同じようなサイバーの脅威（ハッキング、データ侵害、マルウェアへの感染など）に対して脆弱になっているのです。スマートビークルは、企業のバックエンドシステムやデータベースに直接アクセスする機能を備えているため、企業の延長としての役割も果たします。そのことが、組織の機密データをハッカー予備軍にさらけ出すという新たなリスクを生み出しています。

消費者の観点から見ると、電子化された自律的なコネクテッドビークルが広く普及するにつれて、サイバー攻撃の脅威は著しく高まります。今日の自動車は、数百万行ものコードを使用して多くの高度な機能を実行しており、不正アクセスやハッキングに対して脆弱な状態に置かれています。この部門を担当するCISOは、適切なサイバーセキュリティのプロトコルと手続きを導入・実用化するためのツールと戦略を調査して採用しなければなりません[25]。

スマートメディカルデバイスの「健康診断」

同様に、スマートメディカルデバイスが急激に増加し、サイバー攻撃者がその脆弱性に気づくにつれて、医療機器に対するサイバー攻撃の頻度と重大性も高まっています。医療機器は脅威アクターの格好の標的なのです。急速なイノベーションにもかかわらず、古い医療機器が依然として数多く使用されており、その多くは十分に保護されていなかったり、適切に管理されていなかったりするためです。

不正アクセスを受けた医療機器は、機密性の高い患者情報を権限のない人物に漏洩したり、接続されているテクノロジーに不具合を引き起こしたり、患者に害を与えたり、潜在的には病院の活動を停止させる恐れがあります。ここで必要なのは、機器メーカーや医療サービス提供機関からセキュリティチームまでを含むすべてのステークホルダーが意思疎通を図り、互いに協力しながら、サイバーリスクとその関連の脅威を積極的に特定し、軽減策と是正策を計画し、患者の安全と安心を継続的に確保していくことです。

サイバーセキュリティの基準と慣行が継続的に進化するなかで、機器メーカーは、そしてその延長上でCISOも、そのような医療機器が最新の勧告と要件を遵守するように取り計らうという非常に負担の大きな課題に直面しています。

IoTと産業用IoT（IIoT）のセキュリティを取り巻く規制情勢の変化

IoTとIIoTのセキュリティを取り巻く規制情勢も変化しています。コネクテッドデバイスのプライバシーとセキュリティをめぐる懸念の増大に対処するための新しい規制もいくつか登場しています。

EUサイバーレジリエンス法（CRA：Cyber Resilience Act）は、2024年に発効した画期的なEUの規制であり、コネクテッドハードウェア／ソフトウェア製品の製造業者を規制するものです。CRAは、「消費者と企業が、現在、どの製品が高いサイバーセキュリティを備えているかを判断しようとするとき、また製品をセキュリティの高い方法で設定しようとするときに直面している課題を解決しようとする」ものです。EU域内外のすべての製造業者と供給業者は、EU域内で販売および使用される製品に関して、CRAを遵守することが義務付けられます。多くのグローバル組織がEU域内に製造や流通の拠点を設けたりサプライチェーン関係を築いたりしていることを考えると、この規制は重要です。

英国では、製品セキュリティおよび通信インフラストラクチャ法（PSTI法：Product Security and Telecommunication Infrastructure Act）が、接続可能なテクノロジー製品を使用する消費者の保護を目的とした基準を制定しています。PSTI法は製造業者に、事前にロードされた単純なパスワードの禁止、セキュリティアップデートを提供する最短期間に関する透明性の提供、適合証明書（statement of compliance）の提供など、セキュリティ・バイ・デザインの原則を重視することを義務付けています[26]。

PSTI法は、他の地域にとって、スマート製品に関するセキュリティ規制を検討するときの前例となっています。IoTおよびIIoTデバイスの急速な増加に伴い、組織は、特に欧州において、ますます複雑化するセキュリティ規制や指令の網に対処していかなければなりません。この環境を効果的に乗り切るために、企業は、あらゆる規制をさまざまな法的管轄区域にわたって網羅的に考慮する形で、セキュリティに対する統一的なアプローチを開発しなければなりません。そのために、CISOは、法務部門やコンプライアンスチームを含む、さまざまなステークホルダーと緊密に連携する必要があります。

オーストラリアでも、類似の法律が2024年に発効しました。これは、スマートデバイスの製造業者と供給業者に対して、関連するセキュリティ基準を遵守するように求める法律です[27]。

25 KPMG International, Cybersecure Vehicles: Growing number of connected vehicles warrants better cybersecurity measures, 2024.
26 Center for Cybersecurity Policy and Law, The UK PSTI Act Comes into Effect, April 29, 2024.
27 Australian Government, Department of Home Affairs, Cyber Security Act, November 29, 2024.

スマート製品の長期化したライフサイクルを管理する

スマート製品のライフサイクルの長期化は、CISOとそのチームにとって特別なセキュリティ上の課題となります。製品寿命が比較的短いことの多い従来のデバイスとは異なり、スマート製品は、たとえば自動車のように、何十年も使用され続けることがあります。そうしたデバイスの基盤となるアーキテクチャは、新しいテクノロジー、規制要件、セキュリティへの脅威の進化に適応するための定期的なアップデートやアップグレードに対応できるように設計されていなければなりません。

この流動的な状況のなかで、CISOは、製品開発チームと緊密に連携して、セキュリティの課題をスマート製品の長期的なロードマップに組み入れなければなりません。現時点で実行すべきことの1つは、今後数十年の間にセキュリティ事情に影響を及ぼす可能性がある技術の進歩（たとえば、量子コンピューティング）の見通しを調査することでしょう。

パッチやアップデートを簡単に適用できた従来のITシステムとは異なり、スマート製品に組み込まれているソフトウェアでは、接続能力の制約やリアルタイムでパッチを適用する機能の欠如などが原因でアップデートに困難が伴うことが少なくありません。したがって、CISOは、製品ライフサイクル全体を通じてソフトウェアアップデートを管理するための確固とした戦略を必要としています。さらに、CISOは、定期的なソフトウェアアップデートの重要性についてエンドユーザーを啓発し、明確な指針を提供するように努めなければなりません。

スマート製品を取り巻くサプライチェーンは、自動車や医療機器だけでなくすべての製品について、複雑さを増大させるもう1つの要因です。数え切れないほど多くのコンポーネントがさまざまなサプライヤーから供給されているため、各スマート製品を構成しているソフトウェアモジュールを理解することが必要不可欠です。CISOは、潜在的な脆弱性を把握することによって、サプライチェーンのインテグリティとセキュリティの維持に努める必要があります。それには、詳細なソフトウェア部品表（SBOM）を維持・管理することも含まれます。これにより、製造業者は、たとえデバイスがエンドユーザーまで展開された後でも、重大な脆弱性を速やかに検知して対処することが可能となります。

スマート製品のセキュリティに対して包括的なアプローチを取り、それをSmart-Xのライフサイクルのあらゆる側面に組み入れることは、機密情報や資産を保護するために重要であるばかりでなく、消費者やステークホルダーの信頼を維持するためにも必要不可欠です。

先進テクノロジーがSmart-Xのセキュリティに及ぼす影響を見極める

AIやその他の先進テクノロジー、たとえば、自動化、ロボティクス、5G、エッジコンピューティングなどは、CISOがスマート製品のセキュリティを維持するうえで、機会にも課題にもなります。DevSecOpsの原則を活用し、AIの能力を開発の初期段階からスマート製品のなかに組み込むことで、組織は、製品ライフサイクル全体を通じて役に立つ、より堅牢で適応力の高いセキュリティの枠組みを生み出すことができます。

しかし、新たな複雑さとリスクも生じています。そのようなテクノロジーがさらに高度化し、スマート製品の機能のなかに深く組み込まれるようになると、セキュリティ侵害や誤動作が及ぼし得る影響はさらに拡大します。CISOは、AIやその他の先進テクノロジーがどのようにスマートデバイスと作用し合っているかについて理解を深めるように努めるべきであり、それによって悪意の行為者につけ込まれそうなパターンや潜在的な脆弱性を特定しなければなりません。このためには、製品開発チームとの密接な協力関係および継続的なテストと評価への注力を通じて、テクノロジーが進歩してもセキュリティ施策が引き続き有効であるように取り計らう必要があります。

AIは、セキュリティへの脅威を検知して軽減する方法を大きく変革する可能性を秘めており、セキュリティチームは先手を打って潜在的な脆弱性を予測し、その対策を講じることが可能になります。結局のところ、CISOは、先進テクノロジーの利点をスマートデバイスに取り入れることと、堅牢性と適応力の高いセキュリティの枠組みを維持することを、適切なバランスで両立させなければならないのです。

> “セキュリティに対する調和のとれた見方こそが第一に優先されるべきことです。それが欠けていると、組織はビジネスを効率的に遂行して成果を上げることができなくなります。なぜなら、当然のこととして、今では非常にたくさんのセキュリティ要件が契約のなかに盛り込まれているからです。”
>
> **Jayne Goble**
> Partner, Cybersecurity
> KPMG英国

推奨施策

セキュア設計から廃止に至るまでの、Smart-Xデバイスのライフサイクル全体を網羅するセキュリティの枠組み（IoTデバイスとIIoTデバイスに固有の戦略を盛り込んだ枠組み）を導入してください。

さまざまなネットワーク接続プロトコルや標準（Bluetooth、Ethernet、5G/6G）への投資を奨励し、接続能力とセキュリティを最大化してください。

早期保証メカニズムを確立し、詳細なソフトウェア部品表（SBOM）を維持することで、迅速な検知とデバイスのリコールを可能にし、重大な脆弱性を管理してください。

物理的な安全性に関する潜在的な問題に取り組み、透明性の高いセキュリティ慣行、第三者監査、規制要件へのコンプライアンスを通じて顧客の信頼を醸成してください。

スマートデバイスの具体的な使用環境に合わせて調整されたセキュリティ計画を策定して実施してください。全体的なデバイスの信頼性とデバイスに対する顧客の信用を高めるうえで、セキュリティと信頼感が重要であることを認識してください。

Learn more

主要課題8

レジリエンス・バイ・デザイン：企業と社会のためのサイバーセキュリティ

レジリエンスは、組織と社会の焦点となっています。特に、基幹インフラストラクチャや、情報テクノロジー（IT）と制御・運用テクノロジー（OT）の関係においてそれが言えます。レジリエンスへの取組みとしては、アタックサーフェス（攻撃対象領域）を管理することで攻撃を受ける可能性を減少させること、そしてインシデントを迅速に特定して対応しながら、インシデントが及ぼす影響を最小限に抑えて速やかに業務を回復させることなどがあります。この問題は、CISOのアジェンダの中心になっています。なぜなら、攻撃者がランサムウェアやその他の悪意ある手段を使用して産業界に大規模な混乱を引き起こし、データと人命の両方を危険にさらす可能性が、依然として警戒レベルにあるからです。レジリエンスを効果的に組み込むために、CISOは、脅威情勢、組織の資産のあり方の変化、政府の役割、そして規制などいくつかの要素を考慮する必要があります。

包括的な資産管理を通じてサイバーレジリエンスを強化する

効果的な資産管理は、サイバーレジリエンスの基盤であり続けています。組織が何を保有しているかを知らなければ、守る必要があるものを守るのは不可能であるということを、CISOは認識しなければなりません。それには、単に組織のデータセンターの内部で日常の業務プロセスを維持している資産だけでなく、企業のIT部門の外部にあって、工場を稼働させたり、公共交通機関を制御したり、エネルギーグリッドの送電を維持したりしている基幹系システムやエンドポイントも含まれます。このような資産を監視する体制がなければ、たとえばERP（企業資源計画）のようなシステムを特定して、それを危険にさらすような脅威を見つけ出すことは、単なる推測ゲームになってしまい、組織の脆弱性は改善されません。

基幹インフラストラクチャに対するサイバー攻撃が継続・拡大する可能性は高く、その動機は金銭的な利益から地政学的問題やテロ行為まで、多岐にわたっています。そのような攻撃の影響は計り知れないものがあり、社会に甚大な損害を与える恐れがあります。サイバー犯罪の財務的な被害額も急増しており、2023年第1四半期から2024年第1四半期までのデータ侵害1件当たりの世界平均コストはほぼ500万ドルに達し、前年比で10%の増加となっています[28]。

> 2025年にもなって、相も変わらず、どのようにして組織の重要資産をしかるべく発見し、理解し、分類し、最終的に保護すべきかをめぐる議論が続いているなんて、まったく驚くほかはありません。

Jason Haward-Grau
Global Cyber Recovery Services Leader
KPMG米国

28 IBM, Cost of a Data Breach Report 2024, July 2024. Research conducted between March 2023 and February 2024.

この課題に対処するために、組織は、次第にエンドポイント検知・対応（EDR）や拡張検知・対応（XDR）といったソリューションに目を向け始めています。EDRは、ラップトップ、デスクトップ、モバイルデバイスなどのエンドポイントを監視して保護することに重点を置いていますが、XDRは、複数のセキュリティツールとシステムからのデータを統合して、組織のセキュリティ体制をより包括的に見わたす手段を提供します。EDRとXDRの採用は拡大してきましたが、まだ広く普及するには至っていません。このようなソリューションは、それ自体が特効薬のような解決策なのではなく、組織が整備すべきより幅広いセキュリティコントロールの枠組みの重要なコンポーネントであるとみなすべきものです。このようなソリューションは、資産を効果的に管理し、可視性を獲得し、異常と脅威を迅速に検知し、インシデントに効果的に対応することに役立ちます。

拡大するエコシステムとサードパーティとの関係から生じるリスクを乗り切る

組織がソフトウェアとサービスをますますサードパーティプロバイダーに頼るようになるにつれて、サプライチェーンのなかに弱いリンクが生じるリスクが高まっています。また、エコシステムが拡大すると、アタックサーフェス（攻撃対象領域）も拡大します。なぜなら、サードパーティとの関係が増えるたびに攻撃者の侵入ポイントの候補が増えるからです。ハッカーは多くの場合、ネットワークにアクセスする手段を獲得するために、最も抵抗の少ない侵入経路を探しており、それは保護されていないプリンターといった非常に単純なデバイスであることもあり得ます。

外部プロバイダーのセキュリティにたった1つでも脆弱性があるとシステム全体が危険にさらされ、そこから攻撃を受ければ、ことによると基幹システムが応答しなくなり、アクセスもできなくなる「死のブルースクリーン」（BSoD：Blue Screen of Death）のような壊滅的な事態を招く恐れがあります。したがって、CISOは、パートナー企業、ベンダー、サプライヤーなどのセキュリティ体制を調査してその不備に対処することで、そのようなリスクを効果的に管理することがきわめて重要なのです。

このような課題に対処し、新たに制定された規制、たとえば、EUのDORA（デジタルオペレーショナルレジリエンス法）、NIS2指令（改正ネットワークおよび情報セキュリティ指令）、およびCRA（サイバーレジリエンス法）を確実に遵守するために、組織は、サードパーティのセキュリティに対してより積極的なアプローチを採用し始めています。こうした取組みは、オペレーショナルレジリエンスを正式に規定しようとするものであり、DORAは金融機関のレジリエンスに焦点を合わせています。DORAの目標はレジリエンスに関する枠組みを提供することです。たとえば、攻撃による業務の混乱にどのように備えるか、そうした業務の混乱が生じた時に何を実行すべきか、どのように報告すべきかなどです[29]。

明確な期待事項を最初から設定し、ソフトウェアとハードウェアの両方のサプライチェーンに透明性と説明責任を要求することで、組織は、幅広いサプライチェーン攻撃からより効果的に身を守ることができます。CRAがベンダーに対して慣例的なハードウェア部品表（HBOM）に加えてソフトウェア部品表（SBOM）も提供するように求めていることは注目に値します。これは、ベンダーの製品やサービスのなかで使用されているライブラリーやコンポーネントを包括的に理解できるようにすることを目的としています[30]。

最新の物理的および仮想的な脅威に対抗するために包括的なセキュリティアプローチを取り入れる

サイバー攻撃に関して言えば、物理的な世界と仮想的な世界は、もはや以前ほど明確に区別できなくなっています。両者を切り離すことは不可能です。これはすなわち、物理的なセキュリティ侵害がどのように仮想的な脆弱性を引き起こし得るかに加えて、サイバーの脅威が物理的な資産とオペレーションに及ぼす潜在的な影響も考慮しなければならないことを意味します。CISOは、チームの注力先を、常時監視体制から、ディープフェイクが入り込みそうな侵入ポイントの積極的な検出へと切り替える必要があります。

あらゆる領域の脅威から身を守るためには、セキュリティに対して物理と仮想の両方の領域を考慮する包括的なアプローチを取ることが必要不可欠です。これには、リモート勤務のためのVPNトンネルを守ることや、所有者が企業であるか従業員であるかに関係なく、すべての機器を適切に管理・保護することも含まれます。

また組織は、サイバー攻撃が現実世界における被害を引き起こし得るという現実にも備えなければなりません。基幹インフラストラクチャに対する攻撃が成功すると、非常に広範にわたる社会の混乱、経済的損害、そして人命の犠牲さえ発生しかねません。物理世界と仮想世界が相互に結び付いていることを認識することで、組織は、そのようなタイプのインシデントへの防備と対応能力を向上させることができます。

> 毎日のように、国から国へのサイバー攻撃、そしてその反撃のニュースを耳にします。現代の戦争では、対戦国間のほぼすべての物理的攻撃は、同じように破壊的でありながら目に見えないサイバー攻撃と表裏一体となっており、強固なサイバー防御の緊急の必要性を浮き彫りにしています。

Merril Cherian
Partner
KPMGインド

29 KPMG, Rise to the challenge of DORA compliance, 2024.
30 Manifest Cyber, SBOMs Take Center Stage in the EU's Cyber Resilience Act, March 6, 2024.

政府がサイバーセキュリティで果たす役割の進化

基幹インフラストラクチャに対するサイバー攻撃の影響が増大するにつれて、社会に重大な危害をもたらす攻撃から企業を守ることにおいて政府が果たす役割はますます重要になっています。組織はもっぱら政府だけに保護を頼ることはできませんが、政府が組織のサイバーセキュリティの取組みを支援するために講じることのできる施策は、規制による解決策以外にも存在しています。

たとえば、政府は組織間の情報共有の促進や大規模なサイバー攻撃から企業を守り、その全体的なレジリエンス態勢を強化することを目的とした規制の起草などの面で、決定的な役割を果たすことができます。米国の情報共有・分析センター（ISAC）のような団体は、さまざまな業界にわたって知見を周知させるために活動しています。こうしたタイプの取組みを推進および支援することにより、政府はこれまで組織がサイバー攻撃についてオープンに議論するのを妨げていた障壁を取り除くことに貢献できます。

政府がサイバー犯罪組織に標的を定めて積極的に攻撃することは無理であるとしても、犯罪組織の資金源に照準を合わせ、その攻撃遂行能力を削ぐことによって、特定の集団を解体に追い込むことは可能です。しかし、そうした集団の多くは捜査の手が及びにくい国で活動しています。

推奨施策

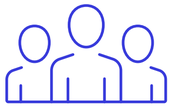
- 進化する規制情勢に常に気を配り、積極的なロビー活動を実施して、全体的なレジリエンスを増大させるコントロールの法制化を支援するように政府に強く働きかけてください。
- リアルタイムの組織レジリエンスを強化するために、積極的なセキュリティ施策を導入してください。たとえば、ユーザーの行動を分析し、異常を見つけ出すなどです。
- サイバー攻撃を受けている間もオペレーションを維持するために、重要な資産と戦略を明示するレジリエンス計画を策定してください。
- サイバーセキュリティ対応計画の定期的な検査と演習を実施することで、重大な攻撃への備えをリーダーに促し、組織全体の準備態勢を向上させてください。
- サードパーティのセキュリティギャップを評価し、組織のサイバーセキュリティ基盤を強化する機会として規制を活用してください。
- 継続的な学習と進歩を重視し、最新の脅威、脆弱性、およびサイバーセキュリティのベストプラクティスについて情報収集に努めてください。
- インシデント発生後には徹底的な事後レビューを実施し、根本原因を究明し、是正計画を策定し、サイバーセキュリティ防御体制を強化してください。

Learn more

2025年のサイバー戦略

CISOとその他のさまざまな事業部門は、特に組織が今後1年間にわたってAI機能などに戦略的に投資していく状況のなかで、どのような施策を実行すれば、セキュリティが企業目標の真の達成手段としての役割を果たせるように後押しできるでしょうか?以下に、世界的な複雑性が高まるなかでビジネスを守り、成長させようと試みるCISOが検討すべき推奨施策のリストを示します。

人材



- AIによる自動化とクラウドベースのサービスへの移行で生じるCISOの役割の進化に備えてください。
- CISOの役割が、もっぱらネットワークの守護者であることから、リスクマネジャー、ロビイスト、そしてインフルエンサーへと拡大していることを認識してください。影響力を行使するスキルを育成して磨き上げることで、サイバーセキュリティの重要性を効果的に伝達し、あらゆる階層と部門にわたって変革を推進できるようにしてください。
- 従来の手法を超えた継続的なトレーニングプログラムを開発して展開し、革新的かつ没入的なテクニックを利用して持続可能な行動変革を従業員の間に生み出してください。
- AI関連のリスクを緩和するために必要なコントロールを見極めてそのオーナーシップを確立し、誰がそうしたコントロールのオーナーとなって、組織の全体的なデータガバナンスの枠組みとの整合性と明確さを維持する責任を担うのかを明確に定めてください。
- AIの社内利用や敵対者による使用に伴うリスクに対する従業員と顧客の意識向上を働きかけてください。
- AI利用者の役割と責任に対する明確なビジョンを提供し、AIがどのような状況、どのような取組みで使用されているかに関する透明性を生み出してください。
- セキュリティ担当者のスキルアップを最優先で実施し、必要な技術的スキルを身につけさせることで、担当者が最新のAI動向に立ち後れないように取り計らってください。
- セキュリティチームのトレーニングとスキルアップに投資し、統合されたツールセットを効率的に取り扱えるようにしてください。

プロセス

- サイバーセキュリティに注力するチームメンバーを事業部門のなかに組み入れることに加え、セキュリティをDevSecOpsプロセス全体に「バイ・デザイン」で組み込む作業を継続してください。
- サイバーセキュリティの人的要素がセキュリティ侵害の4分の3を占めていることに鑑みて、人的要素への対応に焦点を合わせた人間中心のリスク低減戦略を導入してください。
- AIモデルのテストを実行するレッドチーム演習体制を確立し、AIモデルの堅牢性と信頼性を維持することで、不正確な情報や望ましくない情報の生成を防止してください。第1と第2の防御線の間でAIの機能をサポートする役割と責任を定義してください。
- セキュリティを維持しながらIDの取扱いを合理化してください。クレデンシャルの発行と利用を簡素化し、パスワードを減らすなどによって、ユーザーエクスペリエンスの向上を図ってください。
- セキュア設計から廃止に至るまでの、Smart-Xデバイスのライフサイクル全体を網羅するセキュリティの枠組み（IoTデバイスとIIoTデバイスに固有の戦略を盛り込んだ枠組み）を導入してください。
- サイバーセキュリティ対応計画の定期的な検査と演習を実施することで、重大な攻撃への備えをリーダーに促し、組織全体の準備態勢を向上させてください。
- インシデント発生後には徹底的な事後レビューを実施し、根本原因を究明し、是正計画を策定し、サイバーセキュリティ防御体制を強化してください。

2025年のサイバー戦略

データとテクノロジー

- AIのようなディスラプティブテクノロジーの採用に関する議論を主導し、リスクとその軽減策について説明してください。
- クラウドベースのサービスやAIサービスのなかで個人データと企業データの境界線が曖昧になってきているため、サードパーティベンダーに対し徹底的なデューデリジェンスを実施して、ベンダーの契約上の義務が明確化され、かつ組織の全体的なデータガバナンスの枠組みに整合したものとなるよう、取り計らってください。
- より高度なセキュリティ活動（たとえば、AIの導入や全社規模への拡大など）に取りかかる前に、優れたセキュリティの基礎、すなわち、パッチ管理、データの保護、IAMなどに取り組んでください。
- SOCのレベル1とレベル2のタスクを対象としたAIのユースケースの評価とそれへの投資を継続してください。人間中心のリスクを評価し、定量化し、追跡するためにAIテクノロジーに投資し、より効果的なリスク管理を実現して、進化する脅威情勢において後れを取らないようにしてください。
- 統合されたプラットフォームと専門ツールを組み合わせたハイブリッドアプローチがメリットを提供できる領域を明らかにし、両者間の適切なバランスを判断してください。バックアップとリカバリーの手続きを確立してレジリエンスを確保してください。
- 中核的なセキュリティの基本原則、たとえば、データの最小化や不要データのタイムリーな削除などを遵守することで、最高水準のデータ保護を維持してください。
- AIとディープフェイクがデジタルIDに及ぼし得る影響について、幅広い情報の入手に努め、新たに出現する脅威と脆弱性に積極的に対処してください。

規制

- 規制の変化に関する情報収集に努め、取締役会と意思疎通し、権限を明確にしてCISO個人の法的責任が発生するリスクを軽減してください。
- サードパーティのセキュリティギャップを評価し、組織のサイバーセキュリティ基盤を強化する機会として規制を活用してください。
- 進化する規制情勢に常に気を配り、積極的なロビー活動を実施して、企業と社会の全体的なレジリエンスを増大させるコントロールの法制化を支援するように政府に強く働きかけてください。
- 規制上の義務を理解し、AIの導入に関連する既存のコンプライアンス要件を見極めてください。明確なAI利用ポリシー、標準、手続きを策定して伝達してください。他の業界リーダー、連邦政府や世界各国の政策立案者と連携し、それら関係者とのオープンな対話を維持してください。
- 物理的な安全性に関する潜在的な問題に取り組み、透明性の高いセキュリティ慣行、第三者監査、規制要件へのコンプライアンスを通じて顧客の信頼を醸成してください。
- スマートデバイスに関する早期保証メカニズムを規制要件に即して確立し詳細なソフトウェア部品表（SBOM）を維持することで、迅速な検知とデバイスのリコールを可能にし、重大な脆弱性を管理してください。

KPMGによる支援

KPMGは、役員室からデータセンターまで、幅広い領域で網羅的に経験を積み重ねています。KPMGは、顧客企業のサイバーセキュリティの状況を評価し、それをビジネスの優先課題とすり合わせることに加えて、高度なデジタルソリューションの開発、実装、継続的なリスクの監視、サイバーインシデントへの効果的な対応に向け、支援することが可能です。KPMGは、顧客企業がサイバーセキュリティを強化する道筋のどの段階にあっても、その目標の達成に向けて支援します。

新しい市場への参入、製品やサービスの立ち上げ、新しい方法での顧客とのコミュニケーションなど、KPMGは、安全で信頼できるテクノロジーによって、顧客企業が未来を予測したうえで、より効率的に前進できるよう支援することができます。それは、技術的な経験、豊富なビジネス知識、そしてステークホルダーの信頼を守り、築くための支援に情熱を注ぐクリエイティブな専門家という強みを兼ね備えているからです。

KPMG. Make the Difference.

執筆者

Akhilesh Tuteja
Global Cyber Security Leader
KPMG インターナショナル
Partner, KPMGインド

Kyle Kappel
Cyber Security Services
Network Leader
Principal, KPMG米国

Dani Michaux
EMA Cyber Security Leader
Partner, KPMGアイルランド

Matt O’Keefe
ASPAC Cyber Security Leader
Partner, KPMGオーストラリア

Prasanna Govindankutty
Americas Cyber Security Leader
Principal, KPMG米国

KPMGの「サイバーセキュリティ主要課題」チーム（グローバル）：

John Hodson
Samar Iqbal
Billy Lawrence
Leonidas Lykos
Michael Thayer

執筆協力

Imraan Bashir
KPMG カナダ

Katie Boswell
KPMG 米国

Oscar Caballero
KPMG メキシコ

Nancy Chase
KPMG インターナショナル

Merril Cherian
KPMG インド

Samantha Gloede
KPMG インターナショナル

Jayne Goble
KPMG 英国

Jason Haward-Grau
KPMG 米国

Matthew Miller
KPMG 米国

Wendy Lim
KPMG シンガポール

Breah Sandoval
KPMG 米国

Motoki Sawada
KPMG ジャパン

Anubha Sinha
KPMG オーストラリア

Bobby Soni
KPMG インターナショナル

Paul Spacey
KPMG インターナショナル

Marko Vogel
KPMG ドイツ

Jim Wilhelm
KPMG 米国

Koos Wolters
KPMG オランダ

Dominika Zerbe-Anders
KPMG オーストラリア

提携協力

Philip Bice
Global Lead — Service Provider Partnerships
Google

Lou Fiorello
Vice President — Security Products
ServiceNow

Erin Hughes
Head of Cybersecurity Advisory — North America
SAP

Terence Jackson
CISM, CDPSE, GRCP
Customer Security Officer
Microsoft Security Solutions

お問合せ先

KPMGコンサルティング株式会社

T : 03-3548-5111
E : kc@jp.kpmg.com

kpmg.com/jp/kc

本レポートで紹介するサービスは、公認会計士法、独立性規則およ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KPMGコンサルティング株式会社までお問い合わせください。

Designed by Evalueserve.

Publication name: Cybersecurity considerations 2025

Publication number: 139845-G

Publication date: March 2025