KPMG

サイバーセキュリティ主要課題2024

序文

2024年、最高経営責任者（CEO）など組織のリーダーの前途には取り組むべき課題が山積しています。直面している課題は多種多様です。たとえば、1）持続的な成長を達成する、2）先進テクノロジーの影響とリスクを見極め対処する、3）人材の獲得と定着を図る、といったことですが、これらはごく一部にすぎません。最高情報セキュリティ責任者（CISO）に関して言えば、窮地に陥った人々の救援に駆けつける騎兵隊のリーダーという従来の位置付けが後退し、むしろ、「ビジネス上の重要責務に積極的に関与する共同管理者」と見なされつつあります。

本レポートでは、CISOとそのチームが2024年に優先的に取り組むべき8つの主要課題について、世界中のKPMGのサイバーセキュリティ専門家が分野横断的な観点から分析しています。CISOとそのチームはこういった主要課題への取組みを通じ、サイバーインシデントの影響の軽減とサイバーリスク全般へのエクスポージャーの低減を図ることで、組織のビジネス成長を支えることが可能になるでしょう。

世界中の企業がサイバーセキュリティの課題に数多く直面しており、レジリエンスの構築と組込み、規制当局の指令の遵守、全体的なリスクの低減などを実現するためのセキュリティコントロールの導入を迫られています。人工知能（AI）が戦略的ツールとして急速に台頭してきたことで、この問題がリストの上位へと急上昇してきました。AIの民主化、つまり、AIを利用した先端テクノロジーのソリューションなどに誰もがクラウド経由で広くアクセスできるようになった現在の状況は、新たな価値創造の可能性を切り開くと同時に、重大な潜在的リスクを露呈しています。AIは、組織にとって真のゲームチェンジャーになりつつあり、それはセキュリティチームにとっても同様です。

こういった脅威情勢の変化を受け、組織とそのCISOは、より現実的な観点からセキュリティを捉えることが求められています。過去のいかなる時代よりも、データセキュリティやプライバシーと、より広範なビジネス目標とを適切なバランスで両立させなければなりません。

サイバーセキュリティの観点から見ると、社会、経済、政治、規制の動向によってもたらされる影響が、従来よりも全世界で一貫した形で現れるようになっています。その背景には、世界中のあらゆるものが極度に接続された状態（コネクテッド）になっていることがあります。ビジネスのエコシステムが「コネクテッド」になっていることの影響が最も顕著であるのは、グローバルサプライチェーンです。どのような実用的な観点から見ても、隔絶した地域というものは、今や事実上、世界中のどこにも存在しなくなりました。

ただ、地域ごとの細かい相違は残っており、その一例は、企業が遵守しなければならない地域固有の規制要件の存在です。たとえば、一部の市場は個人データの保護により注意深く配慮する一方、責任あるAI、基幹インフラ、サプライチェーンなどに関する新しい規則を制定している地域もあります。

サイバーセキュリティの分野でも、コンプライアンス全般に注目する姿勢が世界的に生じており、多様化するさまざまな報告要件だけでなく、規制によって課される負荷全体に改めて注意が向けられています。その結果、企業は、国境をまたぐ規制要件や制度を幅広く遵守するための仕組みにプライバシーとセキュリティを組み込むことを重視するようになりました。

特に、責任あるAIシステムの構築と管理、顧客のプライバシーの保護、基幹インフラ、サプライチェーン、スマート製品、レジリエンスなどに関するガイドラインの施行が問題になる場面で、こうした動きに注目が集まっています。

一方、経済の不確実性が高まるなかで、今後は、サイバーセキュリティ予算をより客観的に正当化する必要が出てくる可能性があります。多くのCISOは、(縮小とは言わないまでも)横ばい程度の予算を模索していますが、その背景には、資金の一部が組織全体のイノベーション、特に、AIと自動化のソリューションに転用されている現実があります。この注目すべき動向ゆえに、セキュリティチームは、テクノロジーへ投資することへの正当化と予算の最適化に取り組むこと、要するに、より少ない資金からより多くの成果を生み出すことを求められています。

経済的な逆風が予算を圧迫する一方、「サイバーセキュリティはすでに十分なレベルにまで成熟したのだからそろそろ投資を切り詰めてもよいのでは」という見方も拡大しています。さらに、セキュリティ業務は他のIT予算やトランスフォーメーション予算のなかに組み込まれる傾向にあり、中央の予算枠から外されつつあります。セキュリティ技術をクラウドサービスとして提供するSECaaS (Security as a Service) というアプローチへの移行も進んでおり、その結果、セキュリティコストが企業の包括的な営業経費のなかに組み込まれるという、これまで見たこともないような動きが生じています。

このような状況のなか、KPMGはサイバーリスク定量化 (CRQ：cyber risk quantification) のプロセスを精緻化することをCISOに対して提言します。CRQは、数学モデリングの使用により、測定可能な変数を通じてリスクを示すものとして、サイバーセキュリティリスクの影響を財務的な観点から説明する際に役立ちます[1]。リスクをCRQという観点から見ることで、投資収益率 (ROI) と投資の優先順位を、経営層と取締役会に対して効果的に実証できるようになります。それによって、組織はテクノロジーと財務の両面から脅威を理解できるようになるでしょう。

基本的に、本レポートがさまざまな角度から検討しているテーマは、おそらく企業内の経営層全員にとっての根幹的な願望、すなわち、組織のレジリエンス (回復力) を維持することだと思われます。本当に重要なのは「データの漏洩やネットワークへの侵入が発生した際、いかに迅速に平常業務を再開できるか」であり、「いかに顧客への影響を最小限に抑えることができるか」ということです。

つまり、最近提案されている多くの規制、特に基幹インフラ部門を対象とした規制に見られるレジリエンス課題の象徴です。多くの場合、現在の規制の重点は、対応と回復、顧客の被害を軽減することに置かれています。これらはセキュリティに対する新たな視点であり、従来の観点とは異なります。

サイバーセキュリティは、絶えず進化する継続的な取組みとして認識しなければなりません。サイバーインシデントを「不可避であっても対処可能なもの」として受け入れる姿勢が組織のなかで広まるほど、組織が準備とレジリエンスの適切なバランスをとる可能性が高まるでしょう。

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

1 Forrester, The Cyber Risk Quantification Landscape, Q4 2022, November 29, 2022.

*本レポートはKPMGインターナショナルが2024年1月に発行した「Cybersecurity considerations2024」を翻訳したものです。

サイバーセキュリティ主要課題2024：8つのポイント

01

顧客の期待に応え、信頼を高める

サイバーの脅威とデータプライバシーの懸念が高まるなか、CISOは組織内の幅広いステークホルダーとの緊密な連携に努めることで、インシデントが発生した場合にも業務を速やかに立て直し、信頼を維持できるようにすべきです。

02

サイバーセキュリティとプライバシーを恒久的に組み込む

セキュリティを組織全体に組み込む仕事は、オペレーショナルエクセレンスを推進する活動の1つであると見なすべきです。

03

グローバルな境界線を越えて活動する

今、組織が検討すべき中心的な課題は、複雑化するグローバルなビジネス環境を、いかに最も効果的に乗り切ってレジリエンスと事業継続性を維持できるかです。

04

サプライチェーンのセキュリティを最新化する

たとえ、多くの困難や競合し合う優先課題があったとしても、サードパーティのエコシステムを安全に守ることをビジネスの障害とするのではなく、むしろ、ビジネスの推進要因とするべきです。

05

AIの潜在的可能性を解き放つ

セキュリティとプライバシー保護を担当するリーダーは、AIを軸にしたビジネス目標を支援するとともに、ゲームチェンジャーとなるこのテクノロジーを効果的に、かつ、責任を持って活用する方法を見つけ出すべきです。

06

自動化でセキュリティを大幅に強化する

オペレーティングモデルのデジタル化に後れを取らずに対応するため、セキュリティチームはプロセスを自動化し、アップグレードする必要があります。

07

ID管理の主体を組織から個人へと移行する

ビジネスモデルの拡大を背景に、組織は、IDを個別的な課題としてではなく、大局的な観点で扱うことが不可欠になっています。

08

サイバーセキュリティを組織のレジリエンスと整合する

組織は、レジリエントなセキュリティという文化を組織全体にわたって幅広く醸成し、それを共通認識としてすべてのステークホルダーに浸透させる方法を見つけ出すべきです。

主要課題1

顧客の期待に応え、信頼を高める

消費者、従業員、サプライヤーなど、あらゆるステークホルダーが、成長と利益の追求を企業に期待しています。同時に社会的に責任ある経営を企業に求める声もますます高まっています。そうしたなか組織は、セキュリティやプライバシーと、環境・社会・ガバナンス（ESG）要因との結び付きを強化すべきです。この結び付きは、ビジネスエコシステム全体で重視されるようになっており、特に、ESG格付けサービスは、組織を評価・比較する際、この点を重視するようになっています。

信頼を高めることは、サイバーに関連する課題の上位に置かれるべきです。それは特に、さまざまな動画や音声のファイルを使用して制作されているディープフェイクとの関連からも言えることです。ディープフェイクは、プライバシーやさらには民主主義に対しても深刻な脅威となる可能性があります。

Mika Laaksonen
Partner
Global Cyber Security ESG Leader
KPMG フィンランド

ESGの重要性 — セキュリティとプライバシーの大局的な位置付け

KPMGグローバルCEO調査2023によると、CEOの69%がESGを価値創出の手段としてビジネスに組み込んでおり、50%が今後3～5年でESGの取組みから大きなリターンが得られると見込んでいます。

これまで、ESG課題の「環境」の要素が最も大きな注目を集めてきましたが、それに比べて、サイバーセキュリティやプライバシーのような「ガバナンス」の要素はまだ十分に展開されていません。サイバーの脅威とデータプライバシーの懸念が高まるなか、CISOはESG担当部門と緊密に連携することで、インシデントが発生した場合に、業務のレジリエンスの維持、および事業継続計画の発動ができるよう、準備しておく必要があります。

サイバーセキュリティとプライバシーの主要課題を社会的責任がある活動のなかに組み込むことで顧客データを保護できれば、たとえ大規模なセキュリティ侵害が発生した時でも、社会的な評判と顧客の信頼を維持できる可能性が高まります。

個人情報をさまざまな官民のサービスプロバイダーに委ねている消費者は、自身のデータが保護されること、データを提供した本来の用途から外れた目的で使用されないことを求めています。

それと同時に、ビジネス目標を追求しながらも、企業は社会的責任を果たす行動をすべきであるという期待も存在します。たとえば、カーボンフットプリントの削減、地域社会の支援、労務方針の改善、職場のダイバーシティと公平性の実現など、非常に多様な要望が存在します。

サイバーセキュリティとプライバシーという個別テーマや、ESGに取り組むことは、すでに企業全体の優先課題となっており、ひいてはCISOの重要任務となっています。地域や業界ごとにさまざまに異なる規制が存在していますが、そうした規制のガイドラインによって信頼を築く必要があるのです。規制の存在はコンプライアンスの観点から重要であるだけでなく、期待の醸成という点でも注目に値します。なぜなら、BtoBの顧客とBtoCの消費者が企業に対して抱く個々の期待は、さまざまな規則によって直接の影響を受けるからです。

個人消費者は、仮にプロバイダーが示す個人データやプライバシーの扱い、侵害発生時の対応に不満があれば、別の製品やサービスを購入することができます。実際、消費者の82%は、ブランドの価値観が自身の価値観と一致していることを望んでおり、75%は「価値観が相入れないブランドとは縁を切る」と回答しています[2]。大半の消費者は、もし選べるのであれば、ESG基準を遵守することでセキュリティ、プライバシー、サステナビリティを重視している企業を好むのです。

これが特に該当するのはBtoBの領域であり、法人顧客は、自社の機密データと知的財産が安全に保護されることを重視します。多くの業界にはサイバーセキュリティに関する規制要件があり、これらの規制を遵守する組織は利害関係者から好まれています[3]。多くのBtoB企業にとって、そうしたコンプライアンスの姿勢は「あれば好都合」という程度のものではありません。規制上の義務は、規制されている業界内の企業をはじめ、直接にサプライヤーにも及ぶものであり、ブランドに重大なサイバーインシデントが発生するとサプライヤーは連鎖的に信用の失墜を被ることになるからです。

実際、約3分の2の消費者が、サステナブルな製品により多く支出する傾向がありますが、これに対して、小売り企業の経営層の3分の2は、消費者が実際に追加費用を支払うか、懐疑的にみています[4]。消費者がセキュリティ、プライバシー、社会的責任に対して追加で出費することを厭わないとしても、差し当たり、そのようなESGの取組みはゲームの賭け金のようなもので、事業を営むためのコストです。ただ、そうした取組みは、遠からず最終的な損益となって現れてくる可能性が高いでしょう。

未公開株式投資やベンチャーキャピタルがかかわっているケースでは、そうした企業が投資を判断する時に倫理というレンズを通して見ているかどうかに注目すべきです。今では投資会社の多くが、適切なレベルのサイバーセキュリティとプライバシー管理の保証を求めています。結局のところ投資会社は、サイバーインシデントによって投資先の企業が被る可能性のあるブランドへのダメージを心配しているのです。

> **サイバーセキュリティは、AIとデータの倫理に関しても、次第に大きな役割を担うようになっています。AIのアルゴリズムを訓練するために使用されるデータが正確であるか、破損・汚損されていないか、偏見がないかを判定することは非常に困難であり、不可能に近いかもしれませんが、努力に見合うだけの意義は十分にあります。**

Caroline Rivett
Partner
Global Cyber Security Life Sciences Leader
KPMG英国

2 Google Cloud, "New research shows consumers more interested in brands' values than ever," April 27, 2022.
3 KPMG、「ESGにおけるサイバーセキュリティとは」、2023年
4 First Insight/Wharton School of the University of Pennsylvania, "The Sustainability Disconnect Between Consumers and Retail Executives," January 2022.

サイバーセキュリティをESG課題に積極的に組み込むことの社会的メリット

ESGをめぐる対話の範囲は、さらに拡大させる必要があります。多くの組織では、サイバーセキュリティとプライバシーについてESGとの関連で語ることがまだ一般的ではありません。

現在、データ保護に関連して、組織、従業員、消費者の間の社会的契約（どのような制度や規則にどこまで自発的に合意しているか）をめぐる深刻な問題が存在します。信頼を高めることは、サイバーに関連する課題の上位に置かれるべきです。特に、さまざまな動画や音声のファイルを使用して制作されているディープフェイクとの関連からも言えることです（ディープフェイク：特定の個人の特徴を表現している画像、動画、または音声を、他の個人の顔や声にすり替え・改変して、その人が実際には行っていない言動をしているように見せかけること）。

ディープフェイクと闘うのが困難な理由は、多くの場合、その動画や音声の真偽の解釈が、視聴者側の判断に委ねられているためです。組織は、常に警戒を怠らず、そのようなデータを見つけ次第削除するよう警戒しなければならず、また、この問題について、より広く一般社会を啓発する活動に参加すべきです。サイバーセキュリティは、AIとデータの倫理に関しても、次第に大きな役割を担うようになっています。AIのアルゴリズムを訓練するために使用されるデータが正確であるか、破損・汚損されていないか、偏見がないかを判定することは非常に困難であり、不可能に近いかもしれませんが、努力に見合うだけの意義は十分にあります。

プライバシーとサイバーセキュリティは、言論の自由を守ること、今日の激増するデジタルコミュニケーションチャネルを安全に保護することでも非常に重要な役割を果たします。プライバシーの統制は、個人情報を同意も通知もなく詐取・悪用する行為を規制するうえでも重要です。こうした対策は、組織に対する一般社会の信頼を維持するために必要不可欠です。

脱炭素化とCO_2削減プログラムの多くは、デジタルテクノロジーと自動化されたシステムに依存しており、それらを利用してエネルギーの生産、配給、消費を監視・管理しています。こうしたツールは非常に効率的ですが、その一方で、意図していなかったサイバーセキュリティ上の脆弱性を生み出す恐れもあり、高度なデータ保護が必要です。サイバーセキュリティを戦略的に組み込むことは、脅威を軽減し、データ侵害のリスクを低減し、規制コンプライアンスを確立することに役立ちます。

最後に、サイバーセキュリティとプライバシーのいずれにも、社会的責任という重要な次元が存在し、その責任を果たすために、組織は顧客と連携して、顧客のサイバーセキュリティ意識が向上するよう支援すべきです。銀行はそうした支援を日常的に実施しており、同様の支援を行う小売り事業者もますます増えています。サプライチェーンやエコシステムのセキュリティとも結び付いているため、ベンダーエコシステムのセキュリティ向上を図ることも非常に重要です。

企業にサイバーインシデントが起きているのか、たとえ適切に対処されていても世間は気にするのか

建前としては、おそらく、自身が使用している製品やサービスを扱っている企業がデータ侵害を受けるのは望ましくない、と言う人が大半でしょう。ただ、そのように考える人々が追加費用の支払いを望まず、タッチポイントは迅速かつフリクションレスであってほしいと考えているのです。大半の人々は何か悪いことが現実に起こるまで気にかけることはなく、セキュリティの取組みは見えないところで行われることを望んでいると思われます。

この問題の重要な要素の1つは、顧客に対し、サイバーセキュリティは組織の最優先の責務で、問答無用で実行すべき正義であることを実証することです。組織は、顧客や消費者がサイバーセキュリティ意識の重要性を理解し、関心を持てるようなトレーニングを提供するべきです。そして、セキュリティの取組みは「TODOリスト」の単なる1項目ではなく、組織の存続に必要不可欠だということを明確に示すべきです。

組織外の人々をトレーニングすることは、それ自体、ESGの取組みを継続する方法の1つです。たとえば、政府と産業界の取組みであるサイバーセキュリティ啓発月間は、両者の連携を通じ、従業員や消費者がサイバーセキュリティの基礎知識を理解し、リスクを回避する施策です。

100%完璧なセキュリティというものは存在しません。どのような予防措置を講じてもインシデントは発生します。サイバーインシデントが発生したら、その事象を開示する必要があるかどうかを迅速に判断してください。開示する場合は、情報をどこまで伝える準備ができているか整理してください[5]。何よりも重要なのは、隠し事をせず、正直であることです。適切なコミュニケーションは、組織に対する顧客の信頼を、インシデントの発生前を上回るレベルにまで高めることが可能なのです。

5 KPMG インターナショナル、「サイバー攻撃への警戒とレジリエンスを両立するには」、2023年

推奨施策

組織内のESGチームがサイバーセキュリティを重要な責務の1つであると見なしているか、見極めてください。そうでない場合は、サイバーセキュリティがESGの3つの領域すべてにとって、なぜ重要かを認識してもらえるように働きかけてください。

現実的であることを心掛けてください。効果的なサイバーセキュリティを実現するためにビジネスパートナーに仕事の進め方を変えさせることは困難です。むしろ、組織全体で対話のあり方を見直し、他の部門を啓発し、既存業務のなかにセキュリティを浸透させるように促すほうが現実的です。

サイバーセキュリティ全般とESG、特にプライバシーに関する全世界の規制について知見を深めることで適切に遵守し、報告義務を果たしてください。ますます増加する規制とそれらが自社のサイバーセキュリティの取組みに及ぼす影響を追跡し、常に把握しておくようにしてください。

Learn more

ESGにおけるサイバーセキュリティ

ESGとサイバーセキュリティの統合的なアプローチから企業が得られるメリットや安全性について考察

KPMG global tech report: ESG

How businesses can use technology as an opportunity to tackle their ESG ambitions.

Road to readiness

KPMG ESG Assurance Maturity Index 2023.

主要課題2

サイバーセキュリティとプライバシーを恒久的に組み込む

セキュリティは、CISOからチーム全体に至るまで、それぞれの役割を大きく変えようとしています。サイバーセキュリティをビジネスプロセスの中核に組み込む「エンベデッドセキュリティ」を目指す動きが進行しているためです。この現実は、CISOの役職にサイバーセキュリティを集中化する従来の形から、連合型のモデルへの移行、つまり、CISOがオーケストラの指揮者のような役割を果たしつつ、枠組みを確立し、リスクを評価し、実行支援を提供するというモデルへの移行に反映されています。フロントオフィスからバックオフィスまで、セキュリティは組織内のあらゆる職務と切り離すことはできず、今では多くのリーダーが、セキュリティをそれぞれの多様なビジネス文化やプロセスのなかに組み入れることの意義を認識しています。

変化するビジネスモデルとテクノロジーから影響を受けるセキュリティ

ウィジェットの開発やサービスの提供など、業務内容を問わず、オペレーティングモデルは一段とクラウドベースになり、他のさまざまな先進テクノロジーと連携して使用することで、拡張性の増大、コストの削減、収益の創出、利幅の拡大が図られています。

自動車業界は、ビジネスモデルのトランスフォーメーションの良い事例です。今や自動車は車輪の上に載った巨大なタブレットになりました。電気自動車はもちろん、ガソリン車にも非常に多くのテクノロジーが追加された結果、自動車は一般の消費者が購入できる最も高度な製品になったと言えるでしょう。

テクノロジーの負の側面としては、アタックサーフェス（攻撃対象領域）の拡大、潜在的脆弱性の発生、エコシステムの複雑化があり、CISOはこのような問題と向き合わなければなりません。同時に、サイバーセキュリティのコストは急激に高騰しており、組織はそういった課題解決を支援するサービスをいかに提供するか、より良い戦略を検討する必要に迫られています。

このような新しい世界で、数百人の人員をセキュリティのために動員することはできません。セキュリティチームはスリムな体制でなければならず、個々の事業部門に組み込まれたセキュリティチームであればなおさらです。組織は、人員とテクノロジーの最適な組合せを見つけ、AIや機械学習などを利用し、人が効率的に処理できない領域をカバーしなければなりません。

数千ものアプリケーションに対してタイムリーに解決策を提示することは人には不可能です。組織は、アプリケーション開発プロセスへのセキュリティの組込みをどこから開始するかを決定のうえ、継続的な監視へと移行し、潜在的な攻撃と脆弱性の影響を理解する必要があります。

皮肉なのは、この過程で従来のCISOは不要になることです。リスクを管理するためには、全社規模で文化を変革し、セキュリティを組織の標準的な業務手順の一部として受け入れることが必要です。この際、CISOがパッチをインストールしたり、オペレーションを管理したりすることはありません。セキュリティチームは、どこで、どのようにして、所定のセキュリティタスクをビジネスに組み込むかを判断し、それらのタスクが適切に実行されるよう監視すべきです。

ここで問題となってくるのが、セキュリティを顧客に近づける「インソーシング（内製化）」か、それとも、組織の内部に存在しない専門スキルを効率的に活用するアウトソーシング（外部委託）かという点です。多くの組織は、コアコンピテンシーとしてのセキュリティという考え方に苦しんでおり、特に、膨大な量の新しいテクノロジーを習得しようとする際、その苦労は大きくなります。

ビジネスリーダーとの連携でセキュリティを効果的に組み込む

「シフトレフト」（より早い段階でセキュリティを組み込む開発方式）については多くのことが語られていますが、セキュリティを早期に組み込む重要性を認識する一方、組織はエンドツーエンド（概念設計から構築まで）、そして、連続的な監視も含めて網羅的に考慮しながら、継続的な要件としてセキュリティに取り組まなければなりません。そのような過程全体を通じて、セキュリティの筆頭要素は可視性です。

セキュリティ担当者の役割は航空管制官に似ており、「滑走路」から常に障害物を除去しておく必要があります。CISOは、飛行機の往来のような「トラフィック」が維持されるように、つまり、アプリケーションが効率的かつ安全に出入りできるよう、対応しなければなりません。セキュリティが製品やサービスのリリースを妨げることは避けるべきですが、その一方、事業部門が採用しているプロセスを早期に可視化する必要があります。

セキュリティをより幅広いビジネスに組み込むことは、オペレーショナルエクセレンスを推進する活動の1つと見なすべきです。セキュリティチームは、どのようなメリットが期待できるかを説明・実証することで、全社内のエンベデッドセキュリティ担当者の気持ちがそのビジョンに向かうように機運を醸成すべきです。そのためには、まず、セキュリティ・バイ・デザインのアプローチを組み込むための適切なガードレール（安全性やガバナンスのための基準や規則）を確立し、そのうえで適切なツールとテンプレートを開発環境のなかに組み込む必要があります。

CISOとそのチームは、事業部門に組み込まれたセキュリティ人材と同様、オペレーショナルエクセレンスと共同責任に対して包括的なアプローチを採用すべきです。これはすなわち、人、プロセス、テクノロジー、規制要件に平等に配慮することを意味します。リスク管理、インシデント管理、ガバナンスとコンプライアンス、テクノロジーソリューション、従業員のトレーニングと意識啓発に重点的に取り組むことで、組織は持続可能なセキュリティ文化を醸成できます。

“2009～2014年頃には、セキュリティ担当者の「80/20の法則」と言えば、80%が技術的スキル、20%がソフトスキルのことを指しました。CISOは、単なるサポートスタッフと見られるのを避けたいのであれば、新しくなった80/20の法則に順応しなければなりません。この法則のもとでは、コミュニケーション、信頼の構築、問題解決といった任務が、セキュリティオペレーションセンターを効率的に運営することと同様に必要不可欠です。”

Brian Geffert
Principal
Cyber Security Services
KPMG米国

こうした施策が今、特に適切な理由は、組織が米国証券取引委員会（SEC）の新たなサイバーセキュリティ規則[6]やEUの改正ネットワークおよび情報セキュリティ指令（NIS2）への準備を進めているためです。このEUの指令は、加盟国に対し、基幹ビジネスをサイバーの脅威から保護するための法令を2024年10月までに施行するよう要求しています[7]。

CISOが存在感を維持するには何を実行する必要があるか

大半のCISOは、セキュリティの意味をデータ、アプリケーション、およびアタックサーフェス全般を中心として理解していますが、CISOが自らの存在意義を真に際立たせることができるのは、人材、予算、組織横断的な政治力に関してと言えるでしょう。セキュリティをビジネスに組み込むには組織のなかでどのように動くべきかを理解しつつ、事業部門に対するパートナーの役割も維持できるCISOは、最大の成功を収める可能性があります。セキュリティチームは、事業部門が計画している新しい取組みによって露呈する可能性がある新たな脅威のベクトルについて把握しておく必要があります。

CISOは、特殊なサイバーセキュリティの専門用語ではなく、パートナーである事業部門が理解できる用語を使うように心掛けるべきです。たとえば、ゼロデイ脆弱性、持続的標的型攻撃（APT）、あるいはセキュリティのオーケストレーション・自動化・対応（SOAR）戦略について語ってはなりません。そのような用語は、セキュリティ人材を除くほとんどの社員にとって何の意味もないからです。そうではなく、たとえば、「この計画が順調に進まない場合、皆さんの部門はA市場やB市場から締め出されてしまいます。この製品ラインを無事に保護することができなければ、消費者はこの製品を使用しなくなるため、皆さんの部門は十分な収益を上げられなくなります」といった表現を使うのです。

セキュリティチームは、脅しの戦術を使う必要はありません。むしろ、新しいビジネスの実現やリスクの低減を基準とした新たな視点を提示することが求められています。CISOは、セキュリティチームの提供する指針と戦略的ビジョンが組織にとって最も利益になるということを全社員に信じてもらう必要があります。CISOにとって最も役立つ財産は信頼なのです。

新たな必須スキルとコンピテンシー

セキュリティ担当者は、ソフトスキルを向上させなければなりません。たとえば、交渉力、時間管理、聞く力、人脈作りといった対人関係のスキルです。2009～2014年頃には、セキュリティ担当者の「80/20の法則」と言えば、80%が技術的スキル、20%がソフトスキルのことを指しました。

現在、この法則は逆転していると言えるでしょう。今、CISOに求められることは、経営層と連携しながら、全社員が理解できるストーリーを伝え、アイデアを明快に提示することによって、ビジネス全体の行動に影響を及ぼすことです。それができなければ、成功はとてもおぼつかないです。

ソフトスキルに加え、セキュリティリーダーは、CRQ手法を活用してリスクエクスポージャー全般をより効果的に管理することも検討すべきです。これにより、どの領域でサイバーセキュリティ投資の優先順位を上げるべきかだけでなく、財務的なリスクについても、より的確に伝達して明快に説明することが可能になるでしょう。

セキュリティチームは、リスクに応じた対策を講じるように働きかける際、その話をする相手が技術系の社員ではないことをしっかりと認識していなければなりません。CISOは単なるサポートスタッフと見られるのを避けたいのであれば、新しくなった「80/20の法則」に順応しなければなりません。この法則のもとでは、コミュニケーション、信頼の構築、問題解決のような任務が、セキュリティオペレーションセンターを効率的に運営することと同様に必要不可欠です。

6 Securities and Exchange Commission（SEC）, “SEC Adopts rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies,” July 26, 2023.

7 European Parliament, “The NIS2 Directive: A high common level of cybersecurity in the EU,” August 2, 2023.

推奨施策

何がビジネスに大きな支障をきたす可能性があるか、業務やカスタマーエクスペリエンスに影響を及ぼさずにリスクを管理するには何を実行すべきか、新しい視点を取締役会にもたらしてください。

セキュリティチームは、どのような場合に、どのようにして、特定のセキュリティタスクを事業部門に組み入れるべきか、または、アウトソーシングによってそうしたタスクを監視し、適切に実施されるように取り計らうべきかを判断する必要があります。

サイバーセキュリティチームを1つの事業部門のように運営してください。これは、組織の他の部門のセキュリティに関する活動を統制する権限をある程度放棄しなければならないことを意味します。

Learn more

KPMGグローバルCEO調査2023

世界の企業経営者約1,300人に対する、
経済の見通しやビジネスの展望等に関する調査

KPMGグローバルテクノロジーレポート2023

不確実な時代を自信を持って乗り越え、
価値を実現するには

Future of IT これからのIT戦略

クラウドとAIの時代において、企業ITを進化し、
組織を成長させる戦略とは

主要課題3

グローバルな境界線を越えて活動する

グローバル企業は、サイバーセキュリティとプライバシーに関する規制環境が複雑化するなかで事業を展開しています。絡み合う国家の利害が多種多様な規制要件をもたらしています。たとえば、情報の主権、サプライチェーンのセキュリティ、インシデントの報告、プライバシーに関する要件です。企業は、世界のボーダーレス化に合わせ規制当局への報告を手直しする必要がある一方、現地の要件に見合うよう変更できる形でセキュリティコントロールを維持することも求められます。組織は、変化する地政学リスクと多様化する制裁要件に迅速に対応できるように体制を整えることが不可欠です。

セキュリティ担当者にとっての大きな問題は、規制当局の要請に適切に応え続けるように取り計らいつつ、事業開拓のコストとそこから得られるビジネス価値の間で適切なバランスを維持することです。

Orson Lucas
Principal
Cyber Security Services
KPMG米国

グローバル企業を取り巻く状況：サイバーセキュリティとプライバシーの目標は共通だが、実践では異なる

長年の間に、世界の規制情勢は断片化が大きく進行しました。一部の市場は、過去数年にわたって規制の強化を優先してきましたが、多くの市場はそうではありませんでした。その結果、組織は、今後の進路を自ら判断する必要に迫られています。すなわち、市場ごとの条件に基づき強化されたガバナンス、プロセス、規制を状況に応じて導入するのか、または、新たな先進的規制を「来るべき世界の先触れ」と解し、積極的な、完成度の高い、自動化されたプライバシーおよびセキュリティプログラムに投資するかです。一部の組織は後者を選択していますが、多くの組織は予算や資源、その他のやむを得ないビジネス上の優先課題を理由に、前者を選択しています。

こうした情勢はゆっくりと進行しています。欧州、中国、米国などの市場が基本的な方向性を決め、その他の多くの市場がその後を追っています。セキュリティ、プライバシー、AIの領域では、一定のパターンと原則が生まれつつあります。このことは、先進的な組織にとって、原則に基づくアプローチを中心にローカルともグローバルとも連携する機会となり、機密情報の積極的な保護と管理に向かう契機をもたらします。理想的には、これが単一のグローバルなプライバシー／セキュリティプログラムに、特定の市場における規制や地域の慣行の微妙な違いを反映させたものとして出現すると良いでしょう。ただ、依然として若干の課題が存在しており、完全にグローバル化した組織がこのビジョンを実現するためには、そうした課題を乗り切る必要があります。

たとえば、データを現地仕様にすることと転送に関する課題に対処するには、社内および、サードパーティ（ビジネスパートナーやサプライチェーンパートナー）間のデータインベントリやデータの流れ・移動を確実に理解することが必要です。複数の経路が存在することも多々ありますが、いずれの経路についても、効率的でコスト効果に優れ、規制に即した慣行を確立するには、緻密な計画と明確な意図が求められます。

ビジネスという視点から考えると、組織が事業活動を拡大するには、該当する管轄や拠点の所在地がどこであろうと、今後もグローバルな顧客や企業と取引し、グローバルに市場を開拓し続ける必要があるでしょう。セキュリティ担当者にとっての重要な課題は、規制当局の要請に適切に応え続けるように取り計らいつつ、事業開拓のコストとそこから得られるビジネス価値の間で適切なバランスを維持することです。これは微妙なバランスで、CISO、最高プライバシー責任者（CPO）、およびそのチームにとっては難題となります。

グローバル企業は変化・拡大する規制要件を遵守するという課題に直面している

組織は、規則が絶え間なく変化・拡大しているという認識に基づき、規制という課題を注意深く乗り越えていくべきです。

顧客管理ツールやマーケティングテクノロジー（MarTech）ツールが成熟するにつれ、組織は、データがもたらす洞察やROIを通じ、データから価値を生み出し始めています。

世界の多くの管轄地域で、規制当局はターゲットを絞ったプライバシー規則を制定してきました。そのため、CISO、最高マーケティング責任者（CMO）、最高データ責任者（CDO）、CPOは、現行および計画中の規制要件を包括的に調査し、遵守するための確固とした防衛線を設けることが不可欠になってきました。規制がもたらす影響という点では、現在、多くの国や地域が、プライバシー保護違反に対し、営業免許の停止は言うまでもなく、厳しい金銭的な罰則も科しています。

プライバシー保護のサイロ状態は急速に解消しつつあります。規制当局の取組みが前進するにつれ、データの売買、同意と選好の管理、データ倫理、AIの責任ある使用といった分野への注力により、ステークホルダーやビジネス部門を隔てるサイロは解体しつつあります。それに伴い、取締役会と経営層は、規制コンプライアンスと消費者の信頼の双方に重点を置いた目標ベースの視点を持ち始めています。特に先進的な組織は、消費者との関係の構築・維持・変革に努め、消費者からの信頼を差別化要因にしています。

> **サイバー犯罪の目的と戦術が悪質化・高度化している今日の世界では、顧客も企業も規制当局も、従来に比べてより包括的なアプローチに従い、データ管理と情報保護に取り組むべきです。**

Henry Shek
Partner
Cyber Security Services
KPMG中国

地政学上の力学の変化が、対応のスピードと適応能力に影響を及ぼす

現在の環境において、多数の地域で事業を展開するには困難が伴います。ある1つの市場で使用していたツールやテクノロジーが他の市場では使用できないことがあるからです。たとえば、中国のある地域では、一部の企業が特定の主要ツールにアクセスできないことや、中国市場でツールを提供するベンダーの判断によって利用が制限されることがあります。これは、サプライチェーンとオペレーショナルレジリエンスの両方の問題であり、組織の生産性に重大な影響を及ぼす可能性があります。

組織が調査しなければならない中心的な課題は、どうすれば複雑化するグローバルなビジネス環境を効果的に乗り切り、レジリエンスと事業継続性を維持できるかです。プライバシーとデータの課題への対処を試みる場合、厳しい制裁制度を導入している管轄地域で組織が営業する際は、速やかに最低限の成熟度レベルに到達する明確なガバナンス計画が不可欠です。

実際、中国の規制はEUとは異なるアプローチを採用しており、世界の他地域の規制とも異なっています。また、範囲、個人データの定義、収集の制限、責任の原則、基本的な法的枠組みのいずれにも相違があります。確固とした原則に基づいたビジョン、戦略、ガバナンス、戦術が存在しない限り、組織はイノベーションを図るか、脱落のリスクを冒すかという困難な選択に追い込まれていくでしょう。

ビジネスの政治問題化とそれがセキュリティに及ぼす影響も、留意すべきもう1つの力学です。たとえば、米国では一部の企業がなんらかの形で政治的に偏向しており、それは経営層の価値観に基づくこともありますが、多くの場合、顧客への対応にこの偏向が反映されています。このような動向は、ロシアでの営業やロシアとの取引を継続している企業が制裁を受けるなど、ロシアによるウクライナ侵攻で広く知られるようになりました。

セキュリティとITの観点から見ると、セグメンテーションやマイクロセグメンテーションという考え方には学ぶべきものがあります。これは、企業が、きめ細かなポリシー制御によってデータセンターやクラウド環境下のワークロードを管理し、水平移動による脅威の拡散を制限できる仕組みです。包括的なネットワークを擁する組織は、互いに接続されたセグメントを作成しながらファイアウォールで分離することが可能です。セグメンテーションモデルを導入している企業は、地域ごとの営業を必要に応じて速やかに遮断する能力に優れています。

グローバル企業は、国家の司法権を多様な観点から見るべきです。たとえば、欧州域外のEU市民にサービスを提供することはEUの一般データ保護規則（GDPR）要件を発動させます。概して企業は、自社の業務がどこを拠点としているか、誰に（すなわち、どのサプライヤーに）ビジネスの遂行を依存しているか、どの市場で製品とサービスを提供しているか、どこで法人化しているかを明確にしておく必要があります。そのような4つの主権概念の間の相互作用から生じる複雑な規制環境に最も効果的に対処する方法は、政策に基づいた柔軟な経営原則を採用することです。

考慮すべきもう1つの課題は冗長性の確保です。たとえば、コールセンター業務全体をある管轄地域のなかで遂行している企業を考えてみてください。なんらかの理由でこの管轄が制限区域になると、その国内のビジネスすべてを停止する必要が出てきます。特定地域におけるビジネスを一時的に撤退させる必要が生じた場合に備えて一定レベルのビジネス機能やセキュリティに冗長性を持たせておき、それを利用して地政学的な困難の拡大に対処できれば、非常事態にあっても事業が広範な制約を受けるリスクを軽減することができます。

結局のところ、CISOとセキュリティチームは、常にレジリエンスと万が一への備えという視点で物事を見るべきです。これは、企業が次の非常事態よりも一歩先行し続けることに役立つでしょう。そうすれば、非常時にも「緊急脱出」の意思決定を速やかに自信を持って下すことができ、急場しのぎのサイバーセキュリティ戦略を立てる必要もなくなります。

推奨施策

グローバルな規制情勢を常に把握し、特に適用を受ける規則を管轄地域ごとの詳細なレベルで理解してください。

組織のなかで、どこに基幹データ（構造化データと非構造化データ）が置かれているか、それがどこでサードパーティと共有されているかを認識してください。

グローバルサプライチェーン全体にわたって透明性を高め、信頼を醸成してください。サードパーティ、フォースパーティ、フィフスパーティのサプライヤー関係者を単に取引や契約の関係者としてではなく、自社のエコシステムの延長として扱ってください。

Learn more

Privacy risk study 2023

Staying on top of the evolving privacy risk challenges.

The hostile limelight

The future of cyber in geopolitics.

Global Economic Outlook

KPMG International Global Economic Outlook — H2 2023.

主要課題4

サプライチェーンのセキュリティを最新化する

サードパーティやサプライチェーンのセキュリティに対する多くの組織における現行のアプローチは、現在の相互依存性が高く複雑なパートナー組織のエコシステムの実態に見合っていません。従来モデルは、サードパーティは単発的な取引関係としてサービスを提供するという想定で構築されていましたが、この見方はアプリケーションプログラミングインターフェース（API）とプロセスがSaaS（Software-as-a-Service）への依存によって連結されている、今日の入り組んだネットワーク構造を反映していません。今、推奨される方法は、絶えず変化するサプライヤーのリスクプロファイルを継続的に監視、管理することに焦点を合わせた、より戦略的なサプライヤー関係を確立すること、つまり、オペレーショナルレジリエンスを強化することです。

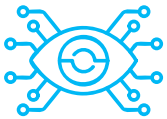
たとえ多くの困難や競合し合う優先課題があったとしても、サードパーティのエコシステムを安全に守ることをビジネスの障害とするのではなく、むしろビジネスの推進要因とするべきです。ただ、そのための最短の方法はなく、それゆえに、最新化（モダナイゼーション）が急務として浮上しています。どうすれば、それをより速く、より効率的に、最小限の資源で、品質を損なわず、実行できるでしょうか。目に見える違いを生み出すことができるのは、リスクベースの考え方を、優れた自動化に牽引されたデータ主導のアプローチと組み合せることです。

Mitushi Pitti
Managing Director
Cyber Security Services
KPMG米国

従来のセキュリティモデルを動揺させるサプライチェーン環境の進化

従来のサードパーティのセキュリティモデルは、特定時点での評価を中心としていました。それに対し、継続的な監視によって、サプライヤーのソフトウェアコンポーネントを絶えず総点検し続ければ、CISOがそのようなプロバイダーのセキュリティ構造をより的確に理解し、潜在的なリスクを特定することに役立ちます。この動向を念頭に置いて、CISOはリスクエクスポージャーをリアルタイムで「コンテナ化」するためのより現代的な基準を策定すべきです。

この体制を実現するために、CISOとそのチームは3つの主要な課題を解決する必要があります。



可視性

長年にわたる問題の1つは、ベンダー集団全体を網羅するための組織能力の欠如でした。大規模な組織は、数千ものサプライヤーを擁していることもあり、多くの場合、従来の手法ではそうしたサプライヤーの活動を正確に評価することができません。物理的なエンドポイントの評価をすべて行うためには、大勢のセキュリティ人材が必要となり、人事的に不可能です。数千万ドルのコストが発生するため、ロジスティクスの面だけでなく、予算面でも非現実的です。

拡張性

幅広いベンダー集団のリスクプロファイルを理解する能力に加え、その規模を拡大する能力まで確保できれば、組織は変化し続ける環境がもたらす課題に後れを取らずに対応することが可能です。サードパーティの環境自体が絶えず流動する脅威ベクトルであり、新しいテクノロジーやプロセスから、既定のセキュリティプロトコルをベンダーが明確に守っていない可能性に至るまで、さまざまなリスクが潜んでいます。

サードパーティパートナーのリスクプロファイルの変化

従来の取引モデルは、どのように関係が変化し、それがどのように新たな脆弱性を生み出す可能性があるかを追跡するためのメカニズムを備えていませんでした。その結果、組織はベンダーとの関係を効率的に機能させながらすべてのコンプライアンス要件を確実に遵守させるために、ベンダーの成熟度に応じて対策を強化（月次レビューを制度化）したり、緩和（四半期に1回のレビューで自主性を高度化）したりする必要が生じています。

テクノロジーが変化するペースの速さと、顧客の要求がますますエスカレートしている現実に直面して、組織は常に先進性を維持しようと努めています。当然ながら、サードパーティやフォースパーティのサプライヤーも、さらにはサイバー犯罪者も、同じ方向に動いています。

たとえば、多くのベンダーが、AIの導入でプロセスを改善し、作業をより速く完了させようとしています。実際、AIは確かに魅力的でパワフルな一方、データインテグリティ、統計的な妥当性、モデルの精度をめぐる疑問に始まり、透明性や信頼性の問題に至るまで、さまざまな新しい潜在的なリスクをもたらします。AIによる人の思考のシミュレーションは、組織レベルで安全に責任ある方法で使用しなければならず、サードパーティパートナーに使用させる場合も同様です。そのようなリスクをサプライチェーン全体に当てはめて考えれば、CISOとそのチームが監視すべき新たな脅威の様相が明らかになります。

たとえ多くの困難や競合し合う優先課題があったとしても、サードパーティのエコシステムを安全に守ることをビジネスの障害とするのではなく、むしろビジネスの推進要因とするべきです。ただ、そのための最短の方法はなく、それゆえに、最新化（モダナイゼーション）が急務として浮上しています。どうすれば、それをより速く、より効率的に、最小限の資源で、品質を損なわず、実行できるでしょうか。目に見える違いを生み出すことができるのは、リスクベースの考え方を、優れた自動化に牽引されたデータ主導のアプローチと組み合せることです。

政府の役割

厳しい規制を受けている組織が、規制環境に後れを取らずに付いて行く一方、同じ規制の制約を受けていないサプライヤーと協働しなければならない場合、組織はサプライヤーが適切なセキュリティコントロールを採用して規制遵守に協力するように促す方法を見出さなければなりません。これは、組織が現在進行形で直面している課題です。そうした組織は、サードパーティがセキュリティ全般の改善に取り組むように働きかけるうえで、どのような分野の規制が効果的であるかを知りたいと考えています。

サイバーセキュリティをめぐる米国証券取引委員会（SEC）の規則には、サードパーティに関する規定が盛り込まれています。規制当局は、サードパーティの問題がすべての組織にとって最優先すべき懸案の1つで、増大しつつある課題であることを認識しています。規制当局からの軽いひと押しだけでも、やや認識の甘い未熟なベンダーを説得し、セキュリティ演習へのより積極的な参加を促し、サイバーセキュリティへの構えを強化することに役立つでしょう。

同様に、EUの改正ネットワークおよび情報セキュリティ指令（NIS2）も「組織はサードパーティによってもたらされるリスクを積極的に管理すべき」と強調しています。サードパーティの情報通信テクノロジープロバイダーによってもたらされるリスクの効果的な監視を促進するデジタルオペレーショナルレジリエンス法（DORA）も、サプライチェーンのセキュリティをより的確に掌握・管理することに注意を向けています。

規制当局はDORAを通じて、広範なサプライヤーエコシステムの全体的なレジリエンスを強化するうえで、どのサードパーティを重要な存在であると見なすべきかを見極めようとしています。そのようなサードパーティは、直接の規制は受けないとしてもシステム上は重要であると見なされるため、規制の対象となっている企業は、自社に課されている要件をそのサードパーティにも転嫁することになるでしょう。

コラボレーションと情報共有：まだ初期段階だが、価値ある戦略

実際問題として、企業とサプライヤー間の情報共有はまだ数年は先のことになりそうですが、ベストプラクティスを強化し、最終的にはサプライチェーン上の関係性を向上させる可能性があります。

不正行為者がもたらす脅威が急激に増加している状況で、さまざまな業界、特に基幹インフラ業界の組織は、脅威やリスクに関する知識の共有を、組織内、および市場・サプライヤー・パートナーとの間で大幅に拡大しなければなりません。

> **AIは、データインテグリティ、統計的な妥当性、モデルの精度をめぐる疑問に始まり、透明性や信頼性の問題に至るまで、さまざまな新しい潜在的なリスクをもたらします。AIによる人の思考のシミュレーションは、組織レベルで安全に責任ある方法で使用しなければならず、サードパーティパートナーに使用させる場合も同様です。そのようなリスクをサプライチェーン全体に当てはめて考えれば、CISOとそのチームが監視すべき新たな脅威の様相が明らかになります。**
>
> **Elizabeth Huthman**
> Director
> Cyber Security Services
> KPMG英国

組織はサイロ思考を打破するべく、ステークホルダー（調達、法務、事業部門、リスク、サードパーティ）がお互いにコミュニケーションとコラボレーションを図るように促す必要があります。

コラボレーションと情報共有もベンダー集中リスクを管理することにつながります。これは、サードパーティ、フォースパーティ、フィフスパーティへと拡大するサプライチェーンにとって大きな課題です。多数の組織が同じサプライヤーに依存する形になっている場合、機密性を維持しつつも互いに協力し合うことで、サードパーティがエコシステム全体のなかでセキュリティ上の脆弱性にならないようにすることが重要となります。

多くの組織は、こういった形のコラボレーションに参加することに消極的です。この現実を踏まえ、欧州ネットワーク・情報セキュリティ機関（ENISA）は、情報共有・分析センター（ISAC）と米国国土安全保障省（DHS）のサイバーセキュリティ・社会基盤安全保障庁（CISA）とを介し、脅威と脆弱性に関する情報を収集し速やかに発信することを目的とした集中型の行動計画を先導しています。

これは、単にベンダーが顧客や企業の機密データにアクセスできるかどうかの問題ではありません。一例として、特定のサプライヤーがオペレーショナルレジリエンスを維持するために必要不可欠な存在（組織が製品を組み立てて流通する能力に影響を及ぼす）にもかかわらず、そのサプライヤーがセキュリティ上は十分に成熟していないという状況を考えてみましょう。そのベンダーのセキュリティレベルを向上させるための施策を講じるか、もしくは、別のパートナーに切り換えるという難しい決断を下すことが必要になるかもしれません。

リスク意識とセキュリティに根差した企業文化を確立することで、いかなる個人やプロセスも、セキュリティ上の脆弱性やビジネスの減速の要因とは見なされなくなります。さらに、そのような意識はサードパーティの協力企業も含め、企業のあらゆる側面に拡散していくでしょう。

推奨施策

多様なサービスを提供するさまざまなサプライヤーを一律に扱うのではなく、リスクベースのアプローチを採用し、サードパーティがたどるプロセスを評価してください。

優れた自動化を活用して、変化するサプライヤーのリスクプロファイルの可視性を向上させ、持続可能で拡張性の高い先見的なサードパーティのセキュリティ計画を策定してください。

組織内でも、信頼できるサードパーティとの間でも、知識のクラウドソーシングと情報共有を推進してください。

Learn more

Staying ahead of cyber risk in the supply chain

With complex global supplier networks and more pathways for threat actors to find a way in, understanding and preventing cyber risk must be a priority.

Supply chain trends 2024: The digital shake-up

With digital opportunities sweeping the supply chain landscape, readiness and line of sight will be paramount to success.

The future of supply chain

ESGからロボット、メタバースに至るまで、サプライチェーンのリーダーが備えるべき新たな課題について考察

主要課題5

AIの潜在的可能性を解き放つ

慎重に計画して実行すれば、AIは、いつ、誰が、どのように仕事をするかを大きく変革するでしょう。現在は、生成AIが話題の中心になっていますが、ロボティクスから機械学習までAIの他の多くの分野もビジネスを変革し続けています。このようなテクノロジーに固有のセキュリティ、プライバシー、倫理に対する影響を正確に評価することは難しいため、組織はAIの導入時に、リスク管理とガバナンスの両方を提供する枠組みを確立しようとしています。

データは、セキュリティ全般、特にプライバシーの根幹をなす要素です。産業界は全世界の政府機関に対し、共同歩調をとるよう求めています。なぜなら現在のように、一部の国が他国よりも規制が厳しいという一貫性のない法制度では、イノベーションの意欲が削がれるためです。市場は、そのようなイノベーションのニーズを効果的な規制のガイダンスやガードレールと適切なバランスで両立させる必要があります。

Sylvia Klasovec Kingsmill
Global Privacy Solutions Lead
KPMG インターナショナル
Partner
KPMGカナダ

AIの現在の進路

どうすれば責任、透明性、誠実さ（インテグリティ）を持ってAIを統制し導入できるかをめぐり、幅広く倫理的な論争が起こっています。ビジネスの成果に対する懸念と、信頼を（狭義では従業員と顧客に対し広義では社会全体に対し）醸成する必要性がこの論争に火をつけました。この議論に応えるように、AI分野の規制が急速に増加しています。セキュリティとプライバシーが開発の最初の段階から組み込まれるようにするには、官民が連携して、進行中のイノベーションや開発に支援を提供する実用的なソリューションを提案しなければなりません。

市場には、イノベーションに対する不安が存在しています。原因としては、警戒心をあおるような報道、規制当局によるガードレールの欠如、AIに対する統一されたグローバルアプローチの欠如などがあります。一方、イノベーションの起爆剤としてのAIの可能性に対する熱狂も存在しています。

AIモデルとアルゴリズムをいかに管理、導入し、法令で規制すべきかについては、地域レベルのアプローチでさえ先行きが見通せない状況です。国や地域ごとに進捗状況も異なっています。組織は、規制の方向性に留意しつつ、信頼の確立と維持に不可欠な基本的要素を注視し続けるべきです。これは将来的に、AIに関する規制の遵守を図るために必要な作業を最小化することに大きく寄与するでしょう。

各組織がAIで実現している重要な成果を前進させることを推奨していますが、一方、組織はそれに伴う複雑な問題と、それぞれのAIモデルのリスクを効果的に回避する方法について徹底的に理解する必要があります。市場が発展するにつれ、AI開発に関する有意義なガイドラインを制定するだけの時間的余裕を世界の規制当局と立法機関に与えることが重要になります。EUのAI規制法案はその代表例で、この画期的な法案は、GDPRがプライバシーに関して実現してきたことをAIにも適用することを意図しており、この分野で素晴らしい、かつ責任ある成果を生み出す助けとなるでしょう。

立法の欠如はAIの発展を妨げる明らかな減速要因ですが、プラスの材料は、既存のプライバシー法制に規定されている類似の原則が、新しいAIアルゴリズムにも適応できることです。通知、同意、説明可能性、透明性、危害のリスクといったプライバシー要因は、すべて既存の法律のなかで成文化されています。

市場での競争力を維持するためにCISOは、CDOやデータ保護責任者と連携し、AIを軸にしたビジネス目標を支援するとともに、ゲームチェンジャーとなるこのテクノロジーを効果的に、かつ、責任を持って活用する方法を見つけ出す必要があります。同時に、以前からほとんど監視なしで運用されてきたプロセスを十分なガバナンスと統制によって管理しなくてはなりません。このような利用促進とガバナンスの適切な組合せこそが、AIの導入を成功させる鍵となるでしょう。

AIによるイノベーションとセキュリティ／プライバシーの懸念との折合いをつけるための主要課題

AIの導入を促進するために、組織は自社のアプローチを方向付けるきわめて重要な選択を行わなければなりません。たとえば、社内独自のモデルを作成するか、それともサードパーティに依存するかといった選択です。どちらかの選択肢がより不確実性が少ないように思えるかもしれませんが、実際はいずれも固有のリスクを伴っており、組織はそれを認識し、効果的に管理しなければならないことに変わりはありません。

組織は自信を持って技術革新とその展開を進めるため、透明性、説明責任、公正性、プライバシー、セキュリティを中心とした安全対策について自己啓発を行わなければなりません。たとえば、AIの導入や対策で先行している大規模なテクノロジー企業や管轄地域に、責任ある開発をめぐる指針を仰ぐことが可能でしょう。

プライバシーとセキュリティの観点から見ると、多くの組織は否応なしに対策を強いられている面があります。多くの事業部門が全力でAIへと突き進むなか、CISOとCPOはその動きに追随しつつ、必要な対策の確実な導入を図らなければなりません。ブランドとそのビジネス目標を達成する能力にとって、そのようなAIソリューションに対する信頼を導入当初から確立して維持することが必要不可欠なのです。

> **CISOをはじめとする経営層とそのチームは、AIを軸にしたビジネス目標を支援するとともに、ゲームチェンジャーとなるこのテクノロジーを効果的に、かつ、責任を持って活用する方法を見つけ出す必要があります。同時に、以前からほとんど監視なしで運用されてきたプロセスを十分なガバナンスと統制によって管理しなくてはなりません。このような利用促進とガバナンスの適切な組合せこそが、AIの導入を成功させる鍵となるでしょう。**

Katie Boswell
Managing Director
Cyber Security Services
KPMG米国

そのためには、部門横断的な協力が、特に資金的な観点から必要となります。ただ、イノベーションの機会を最大限追求するには、組織はセキュリティ、プライバシー、データサイエンス、法務を一体化した総合的な戦略について合意形成する必要があります。EUのAI規制法案を契機として、米国政府は2023年10月にAIの安全性・セキュリティ・信頼性に関する要件を包括的に定めた大統領令を発令し、共同責務に本格的に取り組む決意を明確に示しました。この大統領令は、AIに関連する安全性とセキュリティ、プライバシー、公平性と公民権、イノベーションと市場競争について成文化しています[8]。

迅速なAIイノベーションと確固たるプライバシー／セキュリティ施策の導入を適切なバランスで両立する

データは、セキュリティ全般、特にプライバシーの根幹をなす要素です。産業界は全世界の政府機関に対し、共同歩調をとるよう求めています。なぜなら現在のように、一部の国が他国よりも規制が厳しいという一貫性のない法制度では、イノベーションの意欲が削がれるためです。市場は、そのようなイノベーションのニーズを効果的な規制のガイダンスやガードレールと適切なバランスで両立させる必要があります。

これは、テクノロジーの変革であるだけでなく、文化的な発想の転換でもあるため、チェンジマネジメントが主要な成功要因の1つとなります。プライバシー／セキュリティ・バイ・デザインという考え方をAIやその他の先進テクノロジーと結び付けるためには、その管理を担当する技術者がテクノロジーだけでなく、プライバシー／セキュリティファーストの発想を推進しなければなりません。組織がプライバシーとセキュリティを最初の段階から考慮しておけば、そうした要素はオペレーティングモデルの元来の構成要素になるでしょう。

世の中がイノベーションのニーズに応えるためにAIを導入するという方向に進み続けるならば、ゆくゆくはAIの導入も、クラウドと同様、一般的な出来事になっていくでしょう。

クラウドへの移行が途方もなく画期的な試みだった時代は、それほど昔のことではありません。現在、クラウドは日常的なビジネス慣行になり、結果としてセキュリティのいかなる側面にも存在しています。AIも同じような進路をたどり、「AIセキュリティ」という概念も消滅するでしょう。なぜなら、それはセキュリティ全体の一部となるからです。

8 Whitehouse.gov, Briefing Room, Presidential Actions, “Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence,” October 30, 2023.

推奨施策

AIの枠組みを現在の基準と整合し、確固としたAIガバナンスを構築してください。そのためには、組織内のさまざまなビジネスリーダーの優先課題をすり合わせ、AIの成功に対して既得権を持つ関係者から部門横断的な支援を得る必要があります。

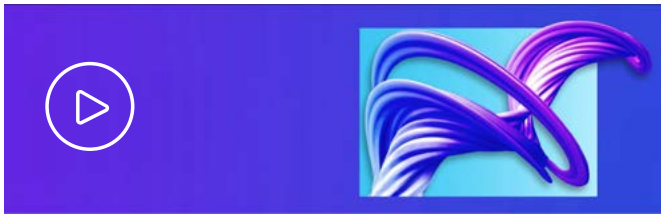
社内で開発するか外部に委託するかにかかわらず、AIアルゴリズムの目的を明確に定義および文書化するために、トレーニングにはビジネス目標に即した適切なデータと安全なコンテキストが使用されるよう取り計らってください。

EUのAI規制法案の規定、AIの安全性・セキュリティ・信頼性に関する米バイデン政権の大統領令の規定に精通してください。

Learn more

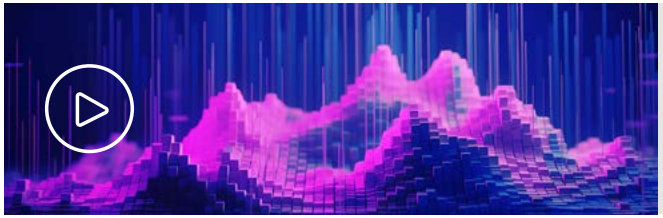
AI時代のプライバシー

プライバシーでAIの信頼を築くには



生成AIモデル：ビジネスにおけるリスクおよび潜在的なリターン

ChatGPT、DALL・E2、Bard等の生成AIモデルの出現が、組織に与える影響や機会、リスクについて考察



KPMG generative AI survey report: Cybersecurity

An exclusive KPMG survey examines four areas where this remarkable technology shows great promise.

主要課題6

自動化でセキュリティを大幅に強化する

企業はシステムをクラウドに移行し、保護を必要とするデータ量は急激に増加し、多くの人々がリモートで働きながら自己所有の機器で企業ネットワークにアクセスするようになっています。その結果、サイバー攻撃のアタックサーフェスが拡大し、多くのアラート、誤検出、トリアージが必要な場面が発生するようになり、それを管理するCISOは多忙を極めています。セキュリティオペレーションセンターには多くのノイズが存在するため、その膨大な量を処理するには、集中管理のためのダッシュボード画面やそれを操作する人員が十分ではありません。CISOは、次から次へと発生する脅威を検知する際、何かを見落としているという不安からどうすれば逃れることができるのでしょうか。CISOは対応が必要な兆候を収集し、関連性を調べ、経営層に報告する必要があり、かつ、それを迅速にやり遂げなければなりません。それを可能にする唯一の方法は自動化を使用することです。

多数の監視ツールから報告されるセキュリティ脆弱性が急増しているため、検出した問題を相関させることで真の脅威となる問題を突き止めることが急務となっています。そうすることで、CISOとガバナンスチームは、組織全体のリスクを包括的に見渡すことが可能となり、どこに専門スキルを備えた人員をより多く投入する必要があるかを明確に理解できるようになります。自動化によって、セキュリティチームは何を優先すべきかを知ることができるのです。

Pratiksha Doshi
Partner
Cyber Security Services
KPMGインド

なぜ今、セキュリティを自動化するのか？

デジタルの課題は急速に増大しています。同時に、多くの組織がコアビジネスとは無関係に、自社をテクノロジー企業と見なし始めています。その理由は、新しいデジタルテクノロジーの爆発的な増加で多くの企業がテクノロジーの採用と習得を強いられているからです。たとえば金融機関は、今では顧客とのやり取りという点でほぼ完全にデジタル化され、多くの医療サービス提供機関は、遠隔医療、AIを利用した医療機器、ブロックチェーンに基づく記録を利用しています。

オペレーティングモデルがデジタル化されるにつれ、後れを取らずに対応するために、セキュリティチームはプロセスを自動化してアップグレードする必要があります。実際、標的型の攻撃者も新しいテクノロジーを使用しており、ほとんど週ごとに攻撃の手口を高度化させているように見えます。さらに、攻撃者は単にアクセスを試みているだけでなく、AIも使用し侵入先で詐欺を働こうとしています。サイバー犯罪者は、他人の顔、声、所作を模倣するように改ざんしたディープフェイクを使用してコールセンターに接触し、より自然に見える方法でフィッシング詐欺を遂行しようとしています。

CISOは、膨大な言葉の洪水のなかから正真正銘のインシデントを迅速に探し当てるために、攻撃者と同レベルの高度な先進的知識を持っていなければなりませんが、それを実行する最も効率的な方法は、セキュリティオペレーションセンターに自動化とAIを導入することです。単純なセキュリティ機能（たとえば、ログ管理、脅威スキャン、アクセス制御など）を自動化することにより、セキュリティチームは、より短い時間で、機動的かつ効率的に対応することが可能となります。

さまざまな業界の多数の組織が、セキュリティ機能の自動化を成功させており、重要ではあってもルーティーン化した反復作業を自動化することで、人的資源を確保しています。以前は高度な訓練を受けた専門人材が実行していた作業、たとえば脆弱性のスキャン、ログ分析、コンプライアンスなどが、今では標準化され自動で実行できるようになっています。

自動化が大局的なセキュリティ情勢を変革する

セキュリティの自動化は、あらゆるサイバーセキュリティ業務で必須のツールになりつつあり、その筆頭が予防です。定期的に実行される手続きや更新を自動化することは、企業や国家主権の防御のレジリエンスと信頼性を維持するうえで重要な役割を果たし、組織化された悪質な不正行為者が大規模化して攻撃を加速させる動きに対抗する助けとなり得ます。また、自動化はサードパーティのエコシステムを保護することにも役立ち、ベンダーとサプライヤーのエコシステムのなかに存在する脆弱性を見極め、それを洗い出します。

検知および対応という面で自動化が特に有用なのは、CISOが一定のレベルのセルフサービス型セキュリティ機能を作成する時です。そうした機能は、評価結果に基づきネットワークを改善するうえで有用なものとなり得ます。これにより、それまで必要だった労働力が大きく減少します。さらに、特定のIPアドレスがすでにブラックリスト化されていれば、人が介入する必要もなく、チケット分析を自動化することができます。

不正行為者は、自動化を使用して攻撃を拡大し、そのスピードも増大させます。自動化された攻撃を防ぐ最も効果的な方法は、検知と対応を自動化することです。侵害が発生すると、自動化された監視プロセスがセキュリティインシデントをほぼリアルタイムで突き止め、アクセスポリシーの規則を変更したり、疑わしい機器やユーザーを隔離したりすることで、修復処理を開始します。

CISO とセキュリティ組織は、デジタルフォレンジックの証拠収集や、セキュリティ対策が所定の機能を果たしているかの検証を目的として自動化を導入しています。これは第一、第二、第三の防衛線のためのリスク管理とガバナンスを合理化してくれます。

Angela Leggett
Managing Director
Cyber Security Services
KPMG米国

デジタルフォレンジックの証拠収集や、セキュリティ対策が所定の機能を果たしているかどうかの検証を目的として自動化を導入しているセキュリティ組織もあります。これは第一、第二、第三の防衛線のためのリスク管理とガバナンスを合理化してくれます。

規制コンプライアンスは、自動化の価値を示すもう1つの代表例です。たとえば、2023年7月、SECは上場企業を対象としたサイバーセキュリティリスク管理、戦略、ガバナンス、およびインシデントに関する情報開示規則を採用しました。この規則のもとでは、重大なセキュリティインシデントを4営業日以内に報告することが義務付けられています。この要件を遵守するためには、企業はインシデントを検知し、その重大さを評価したうえで報告書を提出しなければなりません。この規則で義務付けられたForm 6-Kによる文書を自動的に作成して提出するワークフローを確立することは、コンプライアンスの取組みをサポートする方法として特に有用です[9]。

9 SEC.gov, SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies, July 26, 2023.

さらに、グローバル企業にとって、この規則はForm 6-Kの提出をはるかに超えた負担となります。広範な規制上の情報開示要件を、さまざまなフォーマットで所定の期限内に（時には何時間以内という単位で）満たさなければならないためです。このプロセスを自動化するかどうかが、規制の遵守と違反という正反対の結果を生む可能性があります。

自動化はセキュリティチームと事業部門に人材とスキルの観点から影響を及ぼす

自動化によってセキュリティプロセスが補強されるため、CISOは人の介入する効果が最も大きい場所に優先的に人員を配置することが可能となります。多数の監視ツールから報告されるセキュリティ脆弱性が急増しているため、検出した問題を相関させることで真の脅威となる問題を突き止めることが急務となっています。そうすることで、CISOとガバナンスチームは、組織全体のリスクを包括的に見渡すことが可能となり、どこに専門スキルを備えた人員をより多く投入する必要があるかを明確に理解できるようになります。自動化によって、セキュリティチームは何を優先すべきかを知ることができるのです。

今後、セキュリティチームの仕事の内容が変化していくことは明らかです。人は、より戦略的な問題に注力するようになり、脅威アセスメント、意識啓発トレーニング、事業部門との調整などに従事する一方、AIや予兆分析エンジンによって実行できるような反復的なタスクは実行しなくなるでしょう。

新たな任務は新たなスキルセットを必要とするでしょう。たとえば、CISOとそのチームは、大規模言語モデル（LLM）の動作、およびトレーニングやプログラミングの方法について学び始めなければなりません。クラウド、モノのインターネット（IoT）、AIなどと結び付いた形でセキュリティのさまざまな概念について認識を深め、それに習熟する必要もあります。

推奨施策

自動化に関するセキュリティチームの最初のビジョンと戦略を策定してください。短期的および長期的なセキュリティ目標を検討し、それらが組織の優先的なビジネス課題とどのように整合するかを確認し、そうした共通目標を達成するにはどのような保護対策が必要かを判断してください。

組織がどのデータに一元的にアクセス可能であるかを明らかにするとともに、3つの防衛線すべてにわたって効率性を高めることを目的として、自動化された継続的なセキュリティ対策の監視計画を策定してください。

どのツールを自社開発し、どのツールを外部から調達すべきかを判断してください。サプライチェーンのパートナーが組織間の信頼を強化するためにどのように自動化を進めているかを理解し、そこから得た知識を必要に応じて活用してください。

Learn more

Empowering security

Security orchestration and automated response to help secure the future.

Building trust in cloud environments

2023 KPMG Cloud Transformation Survey

Mastering a multi-cloud environment

The evolution of cloud capabilities.

主要課題7

ID管理の主体を組織から個人へと移行する

消費者とかかわる組織は、消費者にそれぞれ固有のID（アイデンティティ／識別情報）を割り当てており、ユーザー名とパスワードが組織ごとに変わるだけでなく、認証方法も組織によって異なっています。サイバーセキュリティの観点から見ると、このようなIDモデルは変化し始めています。ほとんどのID・アクセス管理（IAM）モデルは、元々、単一の組織のためのデジタルIDとユーザーアクセスを管理する目的で開発されました。現在、その多くは基本構想のレベルから見直され始めており、連合型のプライベート／パブリック／ハイブリッドクラウドのコンピューティング環境に適したレベルのレジリエンスを組み込む方向に変化しています。これにより、個人が（顧客としても従業員としても）新しい機関や団体とやり取りをするたび、毎回のように、手間のかかる身分証明の手続きを求められることはなくなるはずです。

従来型のIDモデルに連合型のアプローチを採用する

現在の環境で、やり取りする相手の正体に確信を持てるかどうかは、セキュリティリーダーにとって最大の懸念ですが、これはまさに動く標的そのものです。過去10～20年間、大半の組織は独自のID管理プログラムを設計・実装しました。そこでセキュリティ担当者が考えたことは、「自組織が実装すれば、完全にコントロールできる」というものでした。確かに、望んでいた統制力は得られたかもしれませんが、このアプローチから生み出される視点は非常に孤立していたため、管理すべき固有のIDがどんどん増えていくという事態が生じました。顧客の立場からすると、関係を持つ企業ごとにIDが必要となり、いつの間にか数十から数百ものIDを抱える結果になったのです。

現在、企業・消費者間（BtoC）取引のセキュリティと企業間（BtoB）取引のセキュリティの線引きは著しく曖昧になっています。一般にBtoBユーザーはBtoCユーザーと比べてネットワークリソースへのアクセス強度が高いという事実を別とすれば、どちらも外部ユーザーであることに変わりなく、ID管理アプローチという点では、組織はおおむね両者を混合して取り扱っています。

ビジネスモデルの拡大を背景に、今では、IDを別個に切り離すのではなく、包括的な観点から扱うことが組織にとって必要不可欠になっています。これは、サプライヤーと最終顧客が、毎回、複雑な身分証明手続きを強いられることなく、複数の組織と機動的にやり取りできるIDモデルに移行するように促す重要な原動力です。

デジタルIDは、消費者が自身のデータを自由に管理でき、同一人物が消費者としても従業員としても使用できるポータビリティ（可搬性）を備えているべきです。近年、多くの卓越したテクノロジーとソーシャルメディア事業者によって提供されるサイバーセキュリティの保証レベルが向上し、同じIDがデジタルコマースのエコシステム全体にわたって活用されるようになってきました。このようなIDに対する信頼感が高まるにつれ、

“IDに付随する保証レベルが上昇するにつれ、連合型のIDモデル、つまり、複数の異なるドメインにわたって安全に活用できる、より少数の、重複のないデジタルIDへと移行する動きが生じ始めています。”

Marko Vogel
Partner
Cyber Security Services
KPMGドイツ

連合型のIDモデル、つまり、複数の異なるドメインにわたって安全に活用できる、より少数の、重複のないデジタルIDへと移行する動きが生じ始めています。

保証レベルの高いデジタルIDが理想のモデルへと進化することで、企業は、収集・保管・処理するPII（個人を特定できる情報）を減らすことができるでしょう。これは、消費者にとって非常に望ましい結果です。

ID管理におけるブロックチェーンの価値についても、言及すべきでしょう。分散型台帳システムが効果的な連合型IDモデルの開発に使用されるようになってきました。セキュリティインフラストラクチャをブロックチェーン技術と統合すると、可視性、検証可能な同意、暗号化、および監査証跡を通じて、信頼が得られます。これにより組織は、データに関する権利の管理とアクセス制御を、集中管理型のサードパーティではなく、操作主体に移譲するという方法でプライバシーと詐欺の問題に対処できます。

デジタルIDが提供する保証のレベルが高くなるほど、ポータビリティは高まります。IDが持ち運べるようになれば、消費者がログインする回数（デジタルIDの数）の減少が期待できます。最終的には、IDにポータビリティを持たせるだけでなく、デジタルウォレットの普及を踏まえ、一貫した改ざん防止機能と本人証明機能を組み込む必要も出てきます。2026年には、デジタルウォレットの利用人口が、2022年の34億人から50%以上も増加し、全世界で50億人を超えると予想されています[10]。そこで注目すべきなのが、生物学的、身体的、行動学的な識別要素を使用したバイオメトリクス（生体認証技術）です。

関連する検討課題は、すべてのIDシステムにとって最大の弱点の1つであるパスワードを組織は捨てることができるか、もし可能なら、それはいつなのか、ということです。安全で確実なID確認のため、パスワードモデルから決別し、多要素認証（機器、位置、生体認証、行動特性など）の使用を、特にビジネスエコシステムの規模で拡大することには多くのメリットがあるように思われます。パスワードは実際に消滅するのでしょうか。何年もかかるとしても、社会はその方向に進んでいるように見えます。

ディープフェイクはIDをめぐる状況を大きく変化させている

ディープフェイクがもたらす脅威はきわめて深刻で、それに伴って生じる財務、社会的評価、サービスへの影響も重大です。CISOは、そうした状況に後れを取らないよう、セキュリティのイノベーションを急がなければなりません。

テクノロジーが驚異的なペースで進化するなか、ディープフェイクに関する懸念が、1999年頃にフィッシングに関連して生じていた懸念をはるかに超えるスピードで拡大しています。最新のテクノロジーを利用できる野心的なサイバー犯罪者は、大手企業、公的機関、主権国家など、より儲けが大きい標的に照準を合わせています。加えて、そうした組織の多くは、サイバー攻撃の脅威から身を守るための備えが不十分です。

鍵となる問題は、ディープフェイクのテクノロジーを習得するには何が必要か、ということです。生体認証を一貫して無効にできるような音声や動画のディープフェイクを作成するためには何が必要なのでしょうか？

コスト面だけを見ても、攻撃者は今後、一段と腕を磨く必要があり、現時点では容易に利用できません。ただ、このテクノロジーが幅広く利用できるようになれば、コストも下がることが見込まれるため、今後、不正行為者がディープフェイクを詐欺行為の戦術に使用することは容易になるでしょう。

ディープフェイクに関する主な懸念の1つは、検知に必要な資金です。適切なコンピューティングパワー、フォレンジックアルゴリズム、監査プロセスを維持することから、そうしたツールを使用するために必要な人材まで、多額の費用がかかるからです。CISOには、経営層レベルの意思決定者との対話を開始し、新たに出現する脅威に予算が見合うように取り計らい、ソフトウェアの更新をリリース直後に必ずインストールさせることでテクノロジーを最新に維持することが推奨されます[11]。

> **保証レベルの高いデジタルIDが理想のモデルへと進化することで、企業は、収集・保管・処理するPIIを減らすことができるでしょう。これは、消費者にとって非常に望ましい結果です。**

Jim Wilhelm
Principal
Cyber Security Services
KPMG米国

10 Juniper Research, Digital Wallets: Market Forecasts, Key Opportunities and Vendor Analysis 2022–2026. August 2022

11 KPMG米国, “Deepfakes: Real threat,” 2023.

パスワードは実際に消滅するのでしょうか。何年もかかるとしても、社会はその方向に進んでいるように見えます。

Danny Flint
Partner
Cyber Security Services
KPMGオーストラリア

新たなIDエコシステムにおける政府の役割

政府と企業部門は、IDの問題で結束しつつあるように見えます。たとえば、ある国の政府は、信頼できるデジタルIDの条件を定めたTrusted Digital Identity Framework（TDIF）の導入を進めています。この制度では、IDサービスプロバイダーがTDIFの適格性認定を獲得し、維持するために満たさなければならない最小限の要件を指定しています。この認定を受けたプロバイダーは、自社の顧客にデジタル行政サービスへのアクセスを許可することができます。

その最終的な目標は、アクセスのしやすさ、安全性、プライバシーを備えたデジタルIDの導入を後押しするユーザーフレンドリーなプラットフォームを維持することです。重要なのは、個人が複数のIDサービスプロバイダーを利用し、個人用と仕事用のデジタルIDを、個別でも両者を一体化した形でも保持できるようになることです。

TDIFによって各個人は、どのデジタルIDを、どの用途と有効期間で使用するかを選択し、そのIDに関する保証を得ることが可能となります。これは、コスト効果が非常に悪いため、政府単独では実現できません。それだけでなく、現在の状況では、おそらく政府機関よりも企業の方が多くの信頼を得ているでしょう。

一部の国では、規制活動が主として領土ごとに別々に実施されており、状況の断片化が進行しています。これは氷山の一角にすぎません。なぜなら、デジタルIDは、クレデンシャルの承認をめぐる新たな検討課題を露呈するためです。人々は、普段から仕事のために領土の境界線を越えて移動しています。そうした人々のデジタルクレデンシャルは、領土境界線の向こう側の当局者によって承認されるでしょうか。官民連携という面について考えた際、もし個人が政府の発行したデジタルクレデンシャルだけでなく、金融機関と結び付いているデジタルIDも持っている場合、その人は、さまざまな状況でどちらのIDを使用するでしょうか。

さらに、政府発行のデジタルIDを提示する場合、紐付けられているすべての情報を開示する義務を負うべきなのでしょうか。確かにそのなかには、金融機関、医療機関、あるいは法執行機関の職員や当局者が知りたい（または知る必要がある）詳細情報も含まれているでしょう。そうだとしても、自身に関してどの情報を開示するかについての全面的な決定権は本人にあるべきです。たとえば、市民権上の地位、学位、職業資格や営業免許などを開示するかどうかの自己決定権を本人が持っているべきですが、基本的な個人データについても、その提供を強いられるべきではありません。

セキュリティ担当者にとってもう1つの重大な問題は、誰がリスクを負うかです。もし誰かのデジタルIDの改ざんや、詐欺目的での使用が発生した場合、発行者と所有者のどちらが責任を負うのでしょうか。デジタルIDの使用目的に応じて、厳格でありながらも運用しやすい規制を企業側に課すべきです。複数のデジタルIDのプロバイダーが高いセキュリティを維持しながら協業できるようにするには、この問題に関する規制と広く受容される基準が存在しなければなりません。

GDPRの基本理念の1つは、組織が特定の限定された状況で特定の限定的な取引に個人データを使用することに対し、データ所有者の同意が必要ということです。

企業がPIIを別の目的に使用したり、販売したりする際は、あらためて同意を取得しなければなりません。この基本的な要請は世界共通の基準になるべきです。

同様に、EUデジタルアイデンティティ（EUDI：EU Digital Identity）は、EUの市民と居住者を対象とした個人用のデジタルウォレットで、これによって自身の身分証明や一定程度の個人情報の確認ができるようになります。このデジタルIDは、EU全域の公共・民間サービスにオンラインとオフラインの両方で使用できるようになる見込みです[12]。

IDをめぐる世界の規制当局の姿勢は、一貫性を欠いています。また、市場は絶え間なく発生するデータ侵害に対し、感覚が麻痺してきています。個人顧客も法人顧客も、どの機密データを開示するか、どこでそれを開示するかについてより一層警戒しなければなりません。CISOとそのチームは、ID管理に関するポリシーと戦略を策定する際、データの責任ある使用と統制を求める顧客の要請を重要な要素として留意する必要があります。

12 European Commission, “Digital Identity for all Europeans,” 2021.

推奨施策

IDに対するアプローチを柔軟に維持して規制環境の進化に適応できるようにするとともに、新たに出現する先進テクノロジーを、現在想定されている2～4年程度のスケジュールを大幅に前倒ししてセキュリティプロセスに組み込めるようなアーキテクチャを構築してください。

連合型のIDエコシステムを推進するために、よりアジャイル（機動的）で相互運用性の高いIDシステムのあり方を探求してください。

進化するIDエコシステムにおいて、IDやクレデンシャルの発行者、リライングパーティ（RP）、デジタルウォレットプロバイダーとして、またはその3つの立場すべてにおいて、自組織が現在および将来、担うべき役割について検討してください。

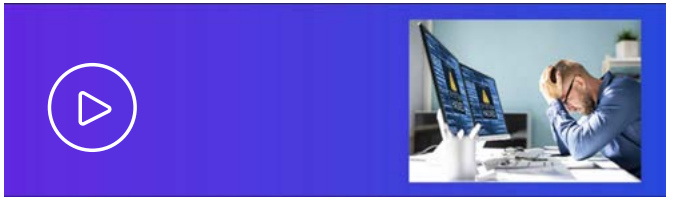
Learn more

Deepfakes rewrite the cybersecurity playbook

Fakes aren’t just for April Fool’s anymore. They’re coming to a boardroom near you, with the potential to destabilize your businesses.

ディープフェイク：今そこにある危機

生成AIにより作成される偽コンテンツが企業にもたらす脅威に立ち向かうには



How Identity and Access Management can enhance resilience and DORA compliance

With new EU regulations demanding vigilance around security, a robust identity and access framework is a vital tool in the kit.

主要課題8

サイバーセキュリティを組織のレジリエンスと整合する

サイバーインシデントの発生時、組織は数日や週単位ではなく、分・時間単位での対応を迫られます。現在の変化の激しい環境で、レジリエンスは、エネルギー、通信、交通などの基幹インフラ業界の組織にとっての共通テーマとなっており、経営層は予防的対策に失敗した場合の事業回復に高い比重を置き始めています。レジリエンスはサイバーセキュリティとシームレスに整合すべきで、保護、検知、迅速な対応と回復に重点を置く必要があります。サイバーレジリエンスは、事業経営能力を維持し、顧客の信頼を守り、将来の攻撃の影響を軽減するために不可欠です。サイバーセキュリティとレジリエンスが連動すれば、組織がリスクを管理する助けとなるでしょう。

レジリエンスとは、インシデントの発生時、速やかに、包括的に、事業への影響を抑えながら対処できる体制を整えることです。二度とインシデントが起こらないようにするという意味ではありません。CISOは、外部的な脅威を左右することはできませんが、組織が準備体制を整えられるよう指揮することは可能です。

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

インシデントの発生後は、信頼を立て直すことが最も重要

データ侵害やランサムウェア攻撃が発生した際、信頼は真っ先に影響を受けます。そして、信頼こそが企業の財産そのものです。組織がどれほど適切に準備を整え、どれだけ速やかに対応して回復できるかは、顧客と（上場企業の場合は）投資家の信頼を取り戻せるかどうかを決定付ける鍵となります。

組織がそのような重要なステークホルダーの信頼を獲得するという決意を固めた時、それがオペレーショナルレジリエンスへの道に踏み出す確固とした第一歩となります。信頼の再構築が迅速な技術的回復を意味する場合もありますが、サービスを提供する別の方法を見つけ出すことが重要な場合もあります。いずれにしても、被害や影響を受けるステークホルダーを明らかにして迅速にニーズに対処し、混乱を最小限に抑えることが重要です。

今、あらゆる地域の規制当局が、レジリエンスと信頼をより重視する姿勢を強めています。たとえば、2021年に英国の金融行動監督機構（FCA）が採用した規則は、英国の金融サービス業界における重要なビジネスサービスが、たとえ業務の混乱が発生しても十分なレジリエンスを持って業務を遂行できるように取り計らうことを意図したものです。この規則は、金融機関に対し、設計当初からレジリエンスを組み込む「レジリエンス・バイ・デザイン」のアプローチを採用していることを実証するように要求しています。この枠組みは、サイバーインシデントの結果として「消費者へ広範な損害を与え、市場の健全性を脅かすリスク（wide-reaching harm to consumers and risk to market integrity）」を避けるという理念に基づいています[13]。

> **組織の全体的な事前対策の主要な柱として、サイバーレジリエンスの状態を継続的に評価し、優先順位付けの演習を経験することは、最終目的にも当面のニーズにも適うようなサイバーセキュリティ計画を維持するために必要不可欠です。これにより、対応と回復のロードマップがもたらされます。**

Jason Haward-Grau
Global Cyber Recovery Services Leader
KPMG インターナショナル
Principal
KPMG米国

ミッションクリティカルな基幹業務への注力：事前計画で最も重要なものに焦点を合わせる

あらゆる組織は、仕事の内容やその進め方においてそれぞれ独自の存在ですが、セキュリティの観点から見ると共通性があります。すなわち、サイバーインシデントが発生する前に、想定シナリオに基づいた系統的な机上演習を実施し、それによって、人、プロセス、テクノロジーの整合を図っておくことは、あらゆる組織にとってメリットがあります。

シナリオ策定は、単にチェックボックスに印を付けることではありません。このような演習は、組織がランサムウェア攻撃のような重大な破壊活動にどう対処するかについて、戦略的な選択肢を明らかにしてくれます。さまざまな対応策を連携し顧客や取引先への影響を考えることで、経営層レベルでも最終的にはリスク軽減の準備が整ったと実感でき、確信が生まれます。また、どのビジネスプロセスが真に重要で、可能な限り早急にオンラインに復帰させる必要があるかを事前に見極めておくことも非常に重要です。

サイバーレジリエンスは、サイバーインシデントに適応してそれを乗り越える能力であり、事業継続性、つまり、インシデントの発生時にも事業を続けるために従うべき手順とは異なります。レジリエンスは戦略的であり、事業継続性はプロセス指向です。その意味で、レジリエンスの演習は、多数の事業部門がパニック状態になる可能性が高いインシデントの渦中ではなく、回復の状況に先立つ段階を想定して実施するほうが、はるかにスムーズに進むでしょう。

組織の全体的な事前対策の主要な柱として、サイバーレジリエンスの状態を継続的に評価し、優先順位付けの演習を経験することは、最終目的にも当面のニーズにも適うようなサイバーセキュリティ計画を維持するために必要不可欠です。これにより、対応と回復のロードマップがもたらされます。

先進的で執拗な脅威アクターは、日々さまざまな攻撃ベクトルを斬新な方法で活用しています。CISOは、このような攻撃側の進化という現実を考慮しなければなりません。徹底的な検討を経た書面によるレジリエンス計画を、具体的な行動に踏み切るためのたたき台として作成しておくことは、攻撃の最中にブレーンストーミングを行うよりも、はるかに効果的です。

変化し続ける脅威情勢のさなかで現状に満足することを避ける

組織の基本的なセキュリティは改善しています。同時に、ビジネスとサプライチェーンの状況も進化しており、IT、ソフトウェア、その他サービスのサプライヤーのネットワークへの依存度が増大するとともに、AI、Web3.0、スマート製品などの先進テクノロジーを実験的に採用する組織も増えています。

それに対応し、組織や国家に支援された攻撃者も一匹狼の攻撃者も、ますます高度化しており、新たな攻撃ベクトルを探索してID乗っ取りやディープフェイクを通じて現実を巧妙にねじ曲げています。今日の攻撃は、サプライチェーンへのセキュリティ侵害や二重または三重の恐喝ランサムウェアを含むように変化しており、その背後には複雑な「サービスとしての犯罪」（CaaS：Crime-as-a-Service）エコシステムに支えられています[14]。

13 Financial Conduct Authority, Policy Statement PS21/3, “Building operational resilience,” March 2021.
14 KPMG インターナショナル、「サイバー攻撃への警戒とレジリエンスを両立するには」、2023年

最も重要な点は、組織はレジリエンスに対して動的なアプローチに従う必要があるということです。現状に満足することは許されません。なぜなら、脅威が日々変化しているだけでなく、不正行為者が内部プロセスとサプライチェーンの両方をかく乱する方法も変化しているからです。

組織は、改善と適応を継続する必要があります。レジリエンスとは、インシデントの発生時、速やかに、包括的に、事業への影響を抑えながら対処できる体制を整えることです。二度とインシデントが起こらないようにするという意味ではありません。CISOは、外部的な脅威を左右することはできませんが、組織が準備体制を整えられるよう指揮することは可能です。

時間、人、予算への投資は、インシデントの回避だけに向けられるべきではなく、むしろ、長期的なレジリエンス体制を築くこと、そして、それをサイバーセキュリティ計画全体に必須の構成要素（エンベデッドコンポーネント）にすることに向けられるべきです。

組織と不正行為者の間で、終わりのない戦いが繰り広げられており、不正行為者のほうが絶えずより速く進化し、イノベーションを遂げています。なぜなら、攻撃側はそのことだけを考えていればよいからです。CISOも、組織のセキュリティ動向を理解し適切に管理すれば、脆弱性を見つけ出してそこにつけ込む攻撃者の能力を少しずつ弱体化していくことができます。

組織が今日の進化する不安定なサイバーセキュリティ環境に直面するなかで、レジリエンスを1回限りの、あるいは断続的なプロジェクトと見なすべきではありません。レジリエンスは適応力を備えた戦略であるべきで、組織のサイバーセキュリティの課題を補完し、顧客の利益を守り、ビジネスの目標と連動し、長期的な価値の実現に貢献する役割を果たすべきです。

推奨施策

もし再度の攻撃が来週、来月、来年に到来した場合、どうすればより適切かつ迅速に対応できるかを分析し、たとえば、支払いの迅速な処理、流動性の確保、コミュニケーションの改善、対応スピードの向上といった「クイックウィン」を見つけ出してください。

組織全体で行動と文化の足並みを揃え、組織にとって、データ、サービス、インフラストラクチャなどの点で真に重要なものを明らかにし優先順位を付けてください。

プランとプレイブックを定期的に更新し、脅威情勢の進展やITとサプライチェーンに対する依存度の変化との整合を図ってください。

Learn more

サイバー攻撃への警戒とレジリエンスを両立するには

いかにサイバー攻撃から回復し、効果的に再構築するか

Cyber and digital operational resilience

Targeting strategic resilience.

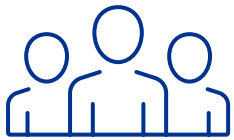
Mid-market: a holistic approach to boost cyber resilience

A more connected world has increased risk and expectation. In response, the mid-market can implement holistic cyber security strategies.

2024年のサイバー戦略

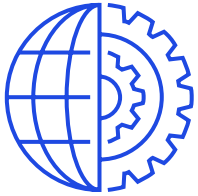
セキュリティを組織の根幹とするために、CISOと組織内のさまざまな事業部門は、今後1年間どのように行動できるでしょうか。以下に、サイバーインシデントからの回復を迅速化し、従業員、顧客、パートナーが被る影響を軽減し、セキュリティ計画によってリスクを低減しながら事業目標の達成を支援する取組みの一環として、CISOが検討すべき推奨施策のリストを示します。

人材



- 組織内のESGチームがサイバーセキュリティを重要な責務の1つであると見なしているか、見極めてください。そうでない場合は、サイバーセキュリティがESGの3つの領域すべてにとって、なぜ重要かを認識してもらえるように働きかけてください。
- 何がビジネスに大きな支障をきたす可能性があるか、業務やカスタマーエクスペリエンスに影響を及ぼさずにリスクを管理するには何を実行すべきか、新しい観点を取締役会にもたらしてください。
- 組織全体で行動と文化の足並みを揃え、組織にとって、データ、サービス、インフラストラクチャなどの点で真に重要なものを明らかにし優先順位を付けてください。
- どのような場合に、どのようにして、特定のセキュリティタスクを事業部門に組み入れるべきか、またはアウトソーシングによってそうしたタスクを監視し、適切に実施されるように取り計らうべきかを判断する必要があります。
- 現実的であることを心掛けてください。効果的なサイバーセキュリティを実現するためにビジネスパートナーに仕事の進め方を変えさせることは困難です。むしろ、組織全体で対話のあり方を見直し、他の部門を啓発し、既存業務のなかにセキュリティを浸透させるように促すほうが現実的です。

プロセス

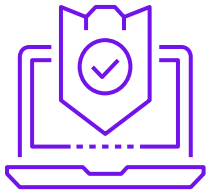


- サイバーセキュリティチームを1つの事業部門のように運営してください。これは、組織の他の部門のセキュリティに関する活動を統制する権限をある程度放棄しなければならないことを意味します。
- 自動化に関するセキュリティチームの最初のビジョンと戦略を策定してください。短期的および長期的なセキュリティ目標を検討し、それらが組織の優先的なビジネス課題とどのように整合するかを確認し、そうした共通目標を達成するにはどのような保護対策が必要かを判断してください。
- グローバルサプライチェーン全体にわたって透明性を高め、信頼を醸成してください。サードパーティ、フォースパーティ、フィフスパーティのサプライヤー関係者を単に取引や契約の関係者としてではなく、自社のエコシステムの延長として扱ってください。
- プランとプレイブックを定期的に更新し、脅威情勢の進展やITとサプライチェーンに対する依存度の変化との整合を図ってください。
- 多様なサービスを提供するさまざまなサプライヤーを一律に扱うのではなく、リスクベースのアプローチを採用し、サードパーティがたどるプロセスを評価してください。
- 組織内でも、信頼できるサードパーティとの間でも、知識のクラウドソーシングと情報共有を推進してください。
- もし再度の攻撃が来週、来月、来年に到来した場合、どうすればより適切かつ迅速に対応できるかを分析し、たとえば、支払いの迅速な処理、流動性の確保、コミュニケーションの改善、対応のスピードの向上といった「クイックウィン」を見つけ出してください。

データ／テクノロジー

- 組織がどのデータに一元的にアクセス可能であるかを明らかにするとともに、3つの防衛線すべてにわたって効率性を高めることを目的として、自動化された継続的なセキュリティ対策の監視計画を策定してください。
- 組織のなかで、どこに基幹データ（構造化データと非構造化データ）が置かれているか、それがどこでサードパーティと共有されているかを認識してください。
- 社内で開発するか外部に委託するかにかかわらず、AIアルゴリズムの目的を明確に定義および文書化するために、トレーニングにはビジネス目標に即した適切なデータと安全なコンテキストが使用されるよう取り計らってください。
- 優れた自動化を活用して、変化するサプライヤーのリスクプロファイルの可視性を向上させ、持続可能で拡張性の高い先見的なサードパーティのセキュリティ計画を策定してください。
- どのツールを自社開発し、どのツールを外部から調達すべきかを判断してください。サプライチェーンのパートナーが組織間の信頼を強化するためにどのように自動化を進めているかを理解し、そこから得た知識を必要に応じて活用してください。
- 連合型のIDエコシステムを推進するために、よりアジャイル（機動的）で相互運用性の高いIDシステムのあり方を探求してください。
- 進化するIDエコシステムにおいて、IDやクレデンシャルの発行者、リライングパーティ（RP）、デジタルウォレットプロバイダーとして、またはその3つの立場すべてにおいて、自組織が現在および将来、担うべき役割について検討してください。

規制



- サイバーセキュリティ全般とESG、特にプライバシーに関する全世界の規制について知見を深めることで適切に遵守し、報告義務を果たしてください。ますます増加する規制とそれらが自社のサイバーセキュリティの取組みに及ぼす影響を追跡し、常に把握しておくようにしてください。
- AIの枠組みを現在の基準と整合し、確固としたAIガバナンスを構築してください。そのためには、組織内のさまざまなビジネスリーダーの優先課題をすり合わせ、AIの成功に対して既得権を持つ関係者から部門横断的な支援を得る必要があります。
- EUのAI規制法案の規定、AIの安全性・セキュリティ・信頼性に関する米バイデン政権の大統領令の規定に精通してください。
- グローバルな規制情勢を常に把握し、特に適用を受ける規則を管轄地域ごとの詳細なレベルで理解してください。
- IDに対するアプローチを柔軟に維持して規制環境の進化に適応できるようにするとともに、新たに出現する先進テクノロジーを、現在想定されている2～4年程度のスケジュールを大幅に前倒ししてセキュリティプロセスに組み込めるようなアーキテクチャを構築してください。

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。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、技術的な経験と豊富なビジネス知識を有し、ステークホルダーの信頼を守り、築くこと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
Billy Lawrence
Leonidas Lykos
Michael Thayer
Jessica Booth

執筆協力

Katie Boswell
KPMG米国

Pratiksha Doshi
KPMGインド

Danny Flint
KPMGオーストラリア

Brian Geffert
KPMG米国

Jason Haward-Grau
KPMG米国

Elizabeth Huthman
KPMG英国

Sylvia Klasovec Kingsmill
KPMGカナダ

Mika Laaksonen
KPMGフィンランド

Angela Leggett
KPMG米国

Orson Lucas
KPMG米国

Dani Michaux
KPMGアイルランド

Mitushi Pitti
KPMG米国

Caroline Rivett
KPMG英国

Henry Shek
KPMG中国

Akhilesh Tuteja
KPMGインド

Marko Vogel
KPMGドイツ

Jim Wilhelm
KPMG米国

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 2024 | Publication number: 139117-G | Publication date: January 2024