KPMG

強制者から インフルエンサーへ

時代に合わせたセキュリティチームの再構築

Contents

エグゼクティブサマリー

デジタルトランスフォーメーション（DX）の実現に向けて―進化するサイバーセキュリティの役割

ブレーキは車を減速させるものだと思っている人が多いのは驚くべきことだ――。元レーシングドライバーのマリオ・アンドレッティ氏の有名な言葉です。「ブレーキは車を安全に速く走らせるためのもの」という言葉は、現在のサイバーセキュリティの役割―組織がDXの恩恵を最大限に享受しつつ多くのリスクを管理できるようにする―ということを見事に表しています。

新型コロナウイルス感染症（COVID-19）は、デジタル化の機会とサイバーセキュリティの脅威の両方を拡大させました。企業は従業員同士の連携やリモートワークの浸透、デジタルカスタマーエクスペリエンスの向上などにおいて目覚ましい進歩を遂げましたが、同時に、物理的な境界線がもはや存在しないことが明確になりました。さらに、第三者への依存度が高まり、IoT（Internet of Things）などのデバイスが普及したことで、サイバーセキュリティの脅威が飛躍的に高まっています。市場への迅速な参入が不可欠な経済環境において、サイバーセキュリティチームは、実用的なセキュリティ文化を構築し、デザイン思考による安全性の定着を支援することで、信頼と回復力を高める責任を負うようになりました。

そのためには、自らをイネーブラー（実現者）、ファシリテーター（促進者）と認識し、顧客、従業員、社会全体からサイバー関連の信頼を得られるようなサービスやブランドの提供を支援しなければなりません。

本レポートは、セキュリティチームが直面する主要な課題に対処するための一助としていただくことを目的に、幅広い業種・地域における主要企業のCISO（最高情報セキュリティ責任者）へのインタビュー結果を、世界各地のKPMGのサイバーセキュリティ専門家が考察したものです。ご協力いただいたすべての方々に感謝申し上げます。

Fred Rica
Principal, Cyber Security
KPMG米国

CISOが取り組むべき7つのアクション

1. C-suiteの一員として行動する

CISOはC-suite（経営幹部）のように発言し、コンセンサスを築き、現実主義を示し、政治力を駆使することで、リーダーがサイバーセキュリティの戦略的な意味を理解できるようにしなければなりません。また、CISOは会社の顔として信頼と信用を築くため、公人としての役割を果たすことが求められています。

2. 視野を広げる

CISOの責任は、データの保護、破壊的な事象への対処、サードパーティの管理、規制遵守への対応、サイバー金融犯罪への対応など、多岐にわたります。そのために、CIO（最高情報責任者）をはじめ、CRO（最高リスク責任者）、CDO（最高データ責任者）など、ほかの役職者と強固な協力関係を築く必要があります。

3. 組織のDNAにサイバーセキュリティを組み込む

CISOはほかの役職者と協力し、サイバーセキュリティを組織のDNAに組み込むべく、洗練されたコミュニケーターでなくてはなりません。セキュリティをガバナンスや管理プロセス、従業員教育、意識に組み込むほか、企業と個人のインセンティブを適切に組み合わせることが必要です。

4. 未来のサイバーセキュリティチームの組成

CISOは外部から人材を獲得して新しいパートナーシップを築き、型破りで多様な人材を育成し、未来に向けたサイバーセキュリティチームを組成する必要があるでしょう。将来的には、サイバー面の役割がはるかに小さくなる代わりに、戦略的かつガバナンスの役割を担い、サイバーセキュリティが真にビジネスに組み込まれるようになるかもしれません。

5.「期待の星」として自動化を受け入れる

自動化によって手作業を減らし、スキル不足を解消することで効率性を高め、増大するコンプライアンス要件に対してより一貫性と再現性をもって対応することができるようになります。自動化は、セキュリティ強化やユーザーエクスペリエンスの向上、大規模なサイバーインシデントへの対応時間の短縮にもつながります。

6. さらなる混乱に備える

私たちは「極度に相互接続された世界」に近づいています。その世界ではIoTと5Gネットワークによって、大幅な効率性の向上や新たなビジネスモデルの構築が可能となります。同時に、組織を新たな攻撃対象にさらし、プライバシーに対する懸念を高めることになり、ゼロトラストなど新たなセキュリティモデルへの移行が求められています。

7. サイバーセキュリティエコシステムの強化

企業は今や、データやサービスを共有することでつながれた、サプライヤーとパートナーの複雑なエコシステム（生態系）の一部となっています。従来の契約や賠償責任モデルは、急速に進化するサプライチェーンの脅威には適さないと思われ、すべての組織と個人に安全をもたらす新しいパートナーシップのアプローチが求められています。

C-suiteの一員として行動する

ビジネスとサイバーセキュリティの
目的の合致でより大きな影響力を

サイバーセキュリティは、今や取締役会での議論の中心となっています。世界のCEOを対象に調査した「KPMG 2021 CEO Outlook Pulse Survey」では、サイバーリスクが組織的な脅威のトップに挙げられ、データセキュリティがほかのすべてのテクノロジー投資に比べ優先されていることが分かりました。

上級管理職や社外取締役は、データ損失、ランサムウェア、詐欺などのインシデントが業務を停止させ、収益や評判を低下させることの影響を十分に認識していますが、同時にジレンマにも直面しています。ビジネスのデジタル化を急速に進めたいと考える反面、設計段階でセキュリティを考慮せずスピード重視で進めると、リスクが生じることを認識し始めているのです。

企業のデジタル技術への依存度が高まるにつれ、あらゆるビジネス上の意思決定にサイバーセキュリティの要素が加わるようになりました。CISOの優先事項は、ファイアウォールやID管理から、ブランドの信頼性、製品の安全性、回復力のあるオペレーション、堅牢なサプライチェーンなどの主要な戦略的課題へと変化しています。

多くのCISOがCEOの直属になってきていますが、彼らはそのような高い職位の仕事を果たす準備ができているのでしょうか？ CISOは、自らがC-suite（経営幹部）の一員となるに値すると認識し、問題解決に焦点を当て、イノベーション、成長、収益にかかわるビジネスイネーブラー（実現者）になることを目指す必要があります。

広範なビジネスリスクと機会の文脈で考える

▶ 取り組むべき課題

CISOはC-suiteの役割にステップアップするため、新しいスキルと考え方を身につけ、セキュリティとコンプライアンスを単体で考えるのではなく、より広範なビジネス上のリスクと機会に焦点を当てなければなりません。

ビジネスに貢献し、収益を上げるために

現在の企業は、市場に迅速に参入する必要がありますが、当然のことながら、サイバーセキュリティの脆弱性を持つ製品やサービスをリリースすることは避けなければなりません。CISOがブレーキをかけるべき局面は必ずありますが、新製品開発の初期段階から関与することで「セキュリティバイデザイン」を導入し、最終的に企業がより速く、より安全に、デジタルの信頼性を維持していくためのイネーブラーとしての役割を果たすことができます。

共通のリスク観

リスクアドバイザーであるCISOは、取締役会において技術的な詳細は避け、サイバー脅威の状況と顧客、成長、収益、コスト、ブランドに対する関連リスクを明確に説明すべきです。サイバーリスクとオペレーショナルリスクの共通言語を使い、取締役会の共感を得ることで、サイバーセキュリティのリスクに関する建設的な議論を進められ、そのリスクに対応する必要性を強調することができます。

強制するのではなく、影響を与える

取締役会レベルでの影響力は、多くの場合、複数の利害関係者との間で築かれた非公式なものとなります。そこでCISOは、企業内での影響力を高めるために、財務、マーケティング、オペレーションなどの会議に出席し、ビジネスリスクについて学び、サイバーセキュリティの脅威について伝えることで、信頼を得る必要があります。

> “リスクの全体像を明確に示せる強力なCISOが必要です。そのために、組織への真の理解と、サイバー環境に対する技術的な見識が求められます。取締役会での議論は、CISOがリスクを管理し、より良い方向に動いているという確信を与えるためのものです。”

Lisa Heneghan
Chief Digital Officer
KPMG英国

リスク軽減のための投資

Palo Alto Networks社のヨーロッパ・中東・アフリカ担当副社長兼CISOのGreg Day氏は次のように述べています。「収益への脅威という観点から問題の範囲を定量化し特定できなければ、リソースを確保することは困難です。そこで、私は取締役会にゴールド、シルバー、ブロンズの3つのソリューションを提示するようにしています。ゴールドは、リスクを最も低減できますがより大きな投資が必要になるソリューションです。このようにすれば、取締役会はトレードオフの観点で判断を下すことができます。」

また、CISOはサイバーチームの内外から興味深い展望やリスクに対する知見を持った魅力的な人物を取締役会に招き入れることで、サイバーセキュリティの重要性を明確にできます。新しいC-suiteの世界では、Greg Day氏が言うように、CISOの影響力が重要です。「莫大な予算と巨大なチームを有するCISOが優れたCISOなのではありません。ビジネスに権限を与え、前進し、成功させられることこそが、優れたCISOの責務なのです。」

グレーゾーンでの仕事

▸KPMGからの示唆

CISOの役割が高まることは、サイバーセキュリティにかかわるすべての人にとって有利となりますが、CISOは役割拡大に値するポストだと自ら示さなければなりません。CISOはリスクを軽減し、ビジネスの成果を向上させるために、サイバーセキュリティがすべての意思決定にどのように関係するのかを取締役会や経営層に明確に説明する必要があります。サイバーセキュリティを企業戦略へ統合するには、より包括的にビジネスにアプローチすることが不可欠であり、技術的な「快適空間（コンフォートゾーン）」から抜け出し、分かりやすく説明する役割を担うことが求められます。また、CISOは法規制への対応に追われるのではなく、セキュリティに関する議論をリードし、法規制への対応を予測することのメリットを認識する必要があります。

企業内政治のグレーゾーンでの仕事は、技術畑出身の多くのCISOにとって特に困難です。どの企業もいつかはハッキングの被害にあうという前提で、「インシデントが企業にどのような損害を与えるか」「サイバーセキュリティへの投資がどの程度リスクを減らし、回復を早めることができるか」を説明しなければなりません。CISOは、犯罪者や悪意ある攻撃者の手口について、独自の視点と知見を持っています。成熟した組織のほとんどは、確立されたリスクマネジメント体制を敷いており、この体制にサイバーセキュリティを組み込むことを目指すべきです。

期待値コントロールも難しい問題です。営業やマーケティングの担当者は新たな製品やサービスの迅速な立上げと強化を求め、オペレーションは24時間365日稼働する必要があり、顧客はデータが安全であることを期待しています。CISOは、CIOやシステムのDevOps（開発担当者と運用担当者が連携して開発する手法）チームと協力することで、次の4つを支援することができます。

- 他者の活躍
- サイバーセキュリティを組み込んだ、自動化の活用推進
- 新たな収益源の確立
- 組織の信頼性向上

> クラウド化の真のメリットは、コスト削減ではなく、市場投入、イノベーション、規模拡大のスピード向上などです。ゆえに、我々はビジネスをより速く、安全で確実に、責任を持って進められるように支援しなければなりません。”

Gary Harbison氏
VP and Global CISO
Bayer

> 取締役会でのサイバーセキュリティ担当者の役割は、セキュリティリスクへの不安を払拭することではなく、出席者すべてのリスクに対する理解度や能力を高め、議論の質を高めることです。”

Martin Tyley
Partner and Head of UK Cyber Security
KPMG英国

視野を広げる

公式・非公式を問わず
重責を担うにはオープンマインドと
大局的な視点が必要

現在の組織は、複雑に絡み合うサードパーティや個人に加え、何千ものIoTデバイスで構成されており、データやシステムへのアクセスの度合いはさまざまです。リモートワークはこの状態に拍車をかけました。従業員は地理的に分散した自宅で働くため、企業内の快適なセキュリティ環境とはまったく異なります。

世界のどこかにいる悪意のある攻撃者が、何千キロも離れた工場や港を停止させたり、グローバルな銀行の顧客向けウェブサイトをダウンさせたりといった脅威に対応しなければなりません。Axiata社のグループ・チーフ・リスク兼コンプライアンス・オフィサーであるAbid Adam氏は「大規模な通信会社が数時間ダウンした場合、自社だけではなく、国家や社会全体が脅威にさらされ、弱体化する可能性があります。そのため、セキュリティバイデザインを導入し、より広範な回復力を実現する必要があります」と強調しています。

CISOの責任はデジタルやオペレーションの回復力にまで拡大しています。データは今や物理的な資産よりも価値があると言っても過言ではありません。データへの依存度がこれまで以上に高まることで、CISOはこの貴重なリソースを守るためにさらなるプレッシャーを感じています。

一方、プライバシー規制は、欧州の一般データ保護規則（GDPR）などにより、個人情報の取扱いに関する要件が地域をまたいで設定されたことで、国境を越えて義務化され、複雑な網目状に拡大しています。情報漏えいに対し、CISOはCDO（最高データ責任者）やCPO（最高プライバシー責任者）と連携し、コンプライアンス違反のリスクを管理する必要があります。

レジリエンスについても同様のことが言えます。欧州で提案されている「Digital Operational Resilience Act（DORA）」は、金融サービス企業に対し、深刻なオペレーション上の混乱に直面した際、回復力のあるオペレーションを維持する能力があると示すことを義務付けるものです。

サイバーセキュリティチームは、データと回復力の問題に焦点を当てるべきです。プライバシーの原則とセキュリティの文化を根付かせれば、現在も将来においてもコンプライアンスの義務を果たすことができます。

新しいスキルとネットワークの開発

▶ 取り組むべき課題

CISOはその役割範囲が広がるにつれ、公式・非公式を問わず、データやレジリエンスの担当役員とどのように連携するか、新たな責任にどのように適応するかを検討しなければなりません。

> パンデミックで明らかになったようにレジリエンスは大きなテーマです。CISOとサイバーセキュリティチームは、一貫性がある包括的な戦略の一部として組織がサイバーインシデントに対応し回復できるよう、インシデント対応計画の策定や事業継続に積極的に関与すべきです。

Hartaj Nijjar
Partner and Cyber Security Leader
KPMGカナダ

> レジリエンスとは、障害が発生した場合にビジネスにどのような影響があるのか、そのような事態に備えてどのような計画を立てるべきかを話し合うことです。どれだけ投資をすれば、どの程度ビジネスの停止を回避できるのかなど、興味深い議論になるでしょう。

Tammy Klotz氏
CISO
Covanta

デジタルレジリエンスの定着

CISO、CRO（最高リスク責任者）、CSO（最高セキュリティ責任者）の役割が似通ってきています。サイバーセキュリティが成熟するにつれ、CIOのプロセスに組み込まれる技術的なセキュリティ管理が増加し、多くのCISOが従来のCIOへの報告ラインとは異なる、より戦略的な役割を担うようになってきました。

KPMGが話を聞いたなかには「CRO（最高レジリエンス責任者）」という新たな役割を担っている人もいました。これは、あらゆるタイプの攻撃や破壊に対する組織の回復力を全体的に見て判断する新しい役職です。事業継続、災害復旧など多様な分野をまとめるもので、ITと物理的なセキュリティに加え、インシデントや危機管理も含まれます。しかし、この役割まで担うことは行きすぎで、サイバーセキュリティに注力できなくなると考える人もいます。

CISOとCRO（最高レジリエンス責任者）を兼任することは、1人の人間には負担が大きすぎます。Vodafone社のグローバルサイバーセキュリティ・ディレクターであるEmma Smith氏は、このアプローチに同意し次のように述べています。「セキュリティ、プライバシー、レジリエンスの対象となるリスク領域は多岐にわたります。これらの機能を組織的に分離し、戦略的に連携させ、真のコラボレーションを実践することでビジネス上のメリットが得られると考えています。」

データを保護する

すべてのビジネスがデータビジネスになるにつれ、個人データの活用とプライバシー保護の限界について議論が続いています。企業は、情報を自由に収集し第三者と共有することで、データを最大限に活用したいと考えていますが、プライバシーに係る規制を遵守する必要があります。

Maersk社では、CISOはCDOと密接に連携しています。CPOまたはDPO（データ保護責任者）が規制遵守を支援しつつ、CDOがデータの基準を設定し、CISOはデータを保証するためのツールを構築しています。

詐欺と金融犯罪への対策

CISOはサイバー犯罪者の心理や彼らが採用する戦術について独自の洞察力を持ち、また、国のサイバーセキュリティ法執行機関との独自の接点や関係を持つことができます。このようなスキルと洞察力は、不正行為防止チームと密接に連携しつつ、不正行為に対抗するために不可欠です。

> 問題を解決するには、発生前と発生後の2つのポイントがありますが、私の仕事は発生前に解決することです。また、最悪の事態を想定して、その影響も評価しています。我々は常に最悪のリスクに備えて努力しており、こういった出来事が起こると想定し、SWIFTが可能な限りの回復力を備えている組織だと示すことを目指しています。

Karel De Kneef氏
Chief Security Officer
SWIFT

広い視野と協調性

▶ KPMGからの示唆

忙しい業務の合間に、多くのCISOがCDO、CRO、CTO（最高技術責任者）、CIOなどとの協力関係を強化しています。ただ、これらの関係をより効果的なものとしたうえで部門を越えた議論とするためには、責任の所在を明確にし、重複を避けるための明確なガバナンス構造を採用して、すべての関係者が互いの強みやビジネスの成功に向けた独自の貢献を認識する意欲を持つことが必要です。

より広範な役割を果たすためには、サイバーインシデントがビジネスに与える影響の全体像を把握するための視野の広さが必要です。CISOは保護や検知にとどまらず、いかにして危機の後にビジネスを迅速に再開させるかを理解し、CEOが顧客、サプライヤー、規制当局との信頼関係を維持できるよう支援する役職になりつつあります。

CRO（最高レジリエンス責任者）の役割を担うか否かにかかわらず、自らの誠実さやプロフェッショナリズムを保ちつつ、現実的でビジネス志向のアプローチを採用する必要があります。多くの企業は膨大な量の新規データやレガシーデータを保有しています。このようなデータを利用して成長を促進すると同時に、データの安全性とプライバシーを維持するためには、CISO、CDO、CTO、CDPO（最高データプライバシー責任者）が幅広くコラボレーションすることが求められます。

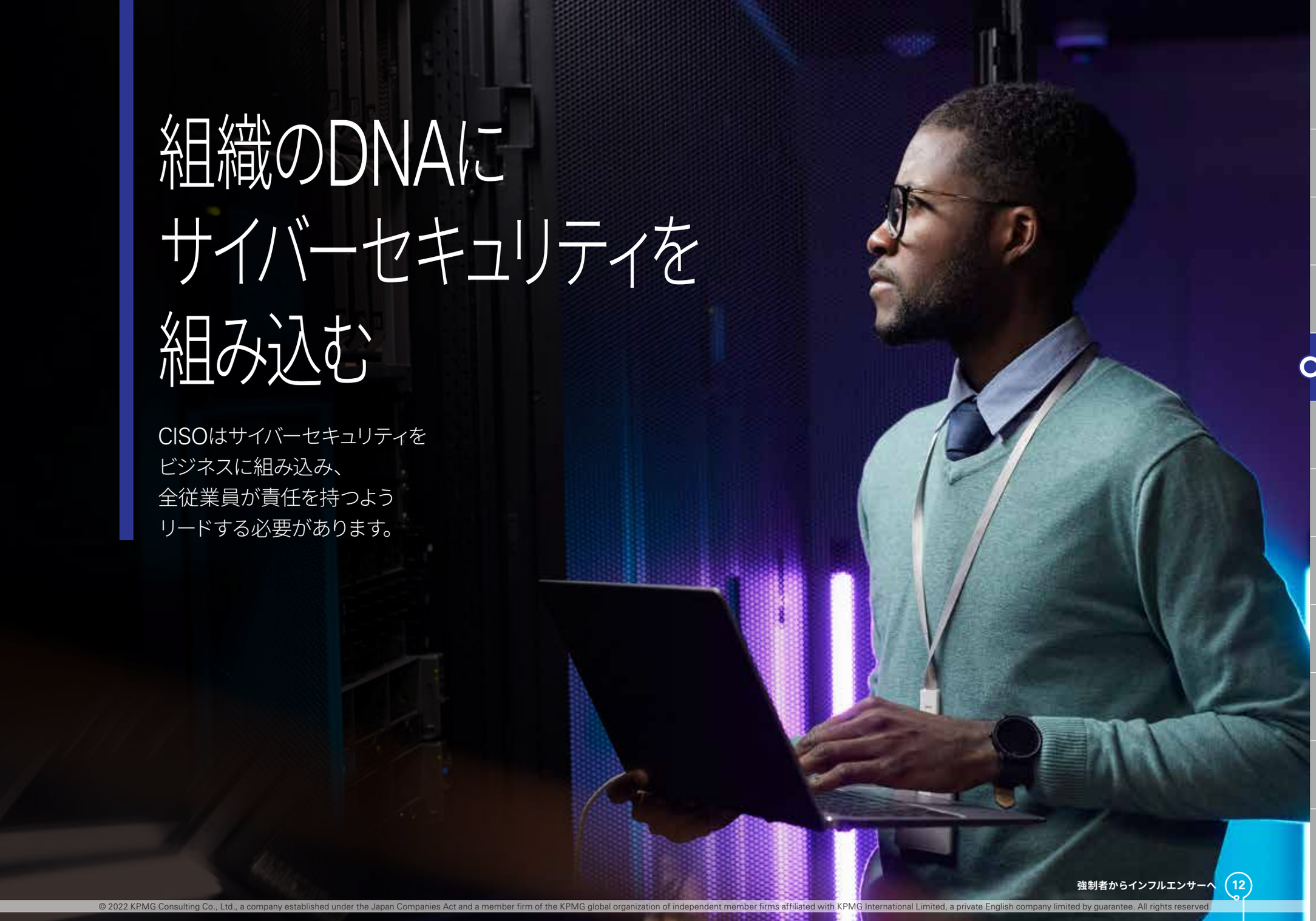
規制がますます細分化され、国境を越えて発生したデータや国民から得たデータの使用に関して、異なる管轄区域で厳しい規則が適用されています。グローバル企業において、CISOは規制遵守の自動化、各国の要件に合わせた管理および報告の合理化を支援するうえで重要な役割を担っています。規制当局による監督技術の利用も増加することが予想されます。

> 産業は破壊されつつあり、CISOは変化するエコシステムを把握しなければなりません。たとえば、通信業界ではかつて、電話回線の不正利用が懸念されていましたが、現在ではオンラインの銀行アプリによるデジタル詐欺が懸念されています。サイバーセキュリティの専門家は、データやレジリエンスなどの新しい課題に適応し、ビジネス全体のリスクを高いレベルで認識する必要があります。

Leandro Antonio
Cyber Security and Privacy Leader and Partner
KPMGブラジル

組織のDNAにサイバーセキュリティを組み込む

CISOはサイバーセキュリティをビジネスに組み込み、全従業員が責任を持つようリードする必要があります。



インシデントの直後にサイバーセキュリティの予算が増えたという話をよく聞きます。本来、セキュリティはインシデントに迫られて初めて実行されるものではなく、製品設計から顧客サービス、サプライチェーン、生産に至るまで、組織のあらゆる部分に浸透していなければなりません。

サイバーセキュリティは企業戦略に不可欠な信頼を築くための重要な要素で、決して後回しにしてはなりません。これはDevOpsにおいても同じで、開発者は市場投入までのスピードにインセンティブを求められる傾向があります。

建設や石油・ガスなどの業界では、安全は当たり前の要素になっています。すべての事業には安全重視の文化が根付いており、責任ある行動を奨励・評価し、報酬を与え、公表することで、従業員が本能的にインシデントを回避できるようになっています。CISOも同様の道をたどるべきです。

サイバーセキュリティチームは、インフルエンサーという新しく難しい役割に慣れる必要があるかもしれません。また、CISOは、全従業員が企業のセキュリティへの取組みを積極的に推進するような倫理観を醸成することを最も優先すべきです。

変革の担い手

▶ 取り組むべき課題

サイバーセキュリティを組織のDNAに組み込むには、開発チームに見られる文化の違いを尊重しつつ、CISOとサイバーセキュリティチームがエバンジェリスト（伝道者）となって、セキュリティプロセスを自然に身につけ、行動を変えていくことが求められます。

トップダウンによる改革

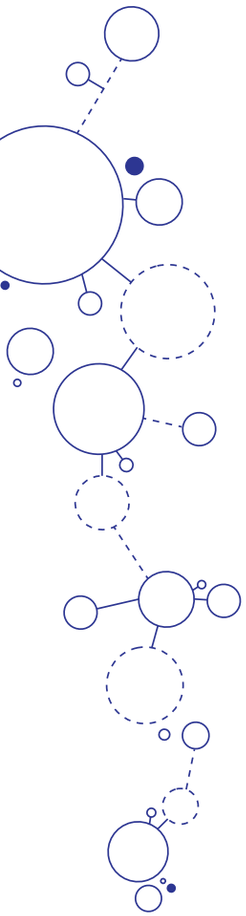
CISOは取締役会レベルでの強固な関係の構築に時間をかけるとともに、サイバーセキュリティがいかにビジネスに役立つかを浸透させていかなければなりません。取締役会と経営層がセキュリティの重要性を理解すれば、CISOはより強力な立場に立つことができます。経営層のサポートがあることを事前に知っていれば、メッセージをより幅広い層に伝えることもできるでしょう。

セキュリティ文化の醸成

CISOは目に見える形で行動すること、各個人がサイバーセキュリティの習慣を実践するための知識と力を与えることで、影響力を発揮することができます。これは従業員だけでなく、請負業者、サプライヤー、パートナーなど、データを扱うすべてのサードパーティに対しても当てはまります。Covanta社のCISOであるTammy Klotz氏が述べているように、重要なステークホルダーと一対一の関係を築くことは何よりも大切です。「CISOの仕事は関係者としっかりとした会話をすることです。最も重要なことを確実に理解していると示すため、保護すべきビジネスオペレーションを把握することに時間を費やすべきです。私がこの仕事に就いた1年目は、まず人間関係を築くことに専念しました。施設を訪れ、自らの手を汚すことなく、オペレーションテクノロジー（OT）のセキュリティを行うことはできません。」

> もし、製品のコンセプト検討の一環としてサイバーセキュリティを検討していないのであれば、もはや手遅れと言えます。

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



DevOps（開発担当者と運用担当者が連携して開発する手法）からDevSecOps（セキュリティを考慮したDevOps）へ

開発チームは作業の遅延や管理費が増えることを懸念して、依然としてサイバーセキュリティへの取組みに消極的になりがちです。一部の企業では、CISOがサイバーセキュリティの専門家の時間をDevOpsチームに惜しみなく提供し、標準的なアプローチを使用して製品開発プロセスにセキュリティを統合する作業をさせています。そうすることで、CISOは開発パイプラインにセキュリティ対策がどのように組み込まれているかを示すことができる「開発エバンジェリスト」を生み出します。

サイバースキルの提供

Vodafone社は、製品やサービスの設計・開発にDevSecOpsモデルを採用しています。セキュリティリーダーを任命するとともに、トレーニングやツール、再利用可能なコードを提供することで、開発チームを強化したいと考えています。

American Express社も同様の理念を持っています。エンタープライズITリスク・情報セキュリティ担当エグゼクティブ・バイスプレジデントのMichael Papay氏は、「私たちは情報セキュリティとリスクに関する問題を認識し迅速に対処するために、専門的なリソースを各機能分野に配置しています。これらの人材はビジネス上の課題を理解し、最も効果的に対応するためにセキュリティの視点を活用します」と語っています。

ゲーミフィケーション

特にDevOpsチームの製品開発者に対して、サイバーセキュリティの重要性を理解し、興味を持ってもらうための効果的な方法として、ゲーミフィケーションがあります。これにより、開発者は日常業務のなかにセキュリティを組み込むことができ、市場への迅速な投入という最終的な成果を得られます。また、「Capture The Flag（情報セキュリティのスキルを競い合うセキュリティコンテスト）」のようなイベントは、DevOpsチームのスキルアップと緊密な関係の構築に役立ちます。

OTセキュリティの弱点

コンピュータがユビキタスになった今、セキュリティはサーバやラップトップだけのものではありません。今日の生産環境は、ソフトウェア、ハードウェア、IoTに大きく依存しています。しかし、OTを管理する文化は、エンジニアリングの考え方、可用性と安全性へのこだわり、時間の活用における厳格なアプローチなどの点で大きく異なっている可能性があります。

エンジニアの頭脳を持ったつもりで彼らの目的を理解し、信頼を獲得し、脅威が現実のものであることを示すことが重要です。そうすることで、時代遅れのシステム、複雑なベンダー構造、24時間365日利用可能にする必要性など、今日の現実を反映した実用的なソリューションを開発することができます。

共通の利益のためのインセンティブ

「頭脳のコラボレーション」と呼ぶアプローチを採用した企業の1つであるAxiata社のAbid Adam氏は次のように述べています。「私たちは、異なる事業会社が適切に連携し、一貫性を保つためのインセンティブを設定しました。KPI（重要業績評価指標）と報酬を再構築し、従業員全員が自らの力を発揮できるようにしたのです。他の事業会社の問題を解決し、自社のビジネスにも貢献するようなソリューションを考え出すことも求めました。」

> 私たちの役割は、セキュリティ意識から行動管理へとシフトしています。これは、フィッシング演習やゲーミフィケーションなどの手法を用いて行動を変え、どこにいても情報セキュリティの重要性を理解できるような、より良い「デジタル市民」を育成することを意味しています。

Jim Nelms氏
CISO
LabCorp

OTリスクの分離

世界各地に多くの研究・製造拠点を持つGSK社は複数年にわたり、企業としてリスクを認識するためのプログラムに取り組んでいます。OTのアップグレードは各拠点が責任を持って行いますが、攻撃を受けた場合の対応は本社のサイバーセキュリティ組織が一括して担っています。

仲介人、統合者、取りまとめ役としてのCISO

▸KPMGからの示唆

ヒトはしばしば「サイバーセキュリティの最も脆弱な要素」と指摘されますが、十分な教育やサポートを得て、自身の行動が顧客、業務、知的財産、売上などにどのような影響を与えるかを理解することができれば、サイバーセキュリティにとって重要な役割を果たすことができるでしょう。CISOは「サイバーセキュリティマーケティング最高責任者」のような役割を果たすことで、真のセキュリティ文化を醸成し、組織のミッションや価値観に沿った効果的なサイバーブランドを構築することができます。

サイバー脅威は繊細かつ洗練されているうえ、常に進化しています。そのため、セキュリティを組織文化に組み込み、従業員がハッカーや犯罪者を警戒し、見分けられるように、社会的認知理論に基づいた学習テクニックが必要です。特に、詐欺や金融犯罪に対処する際や、カスタマージャーニーにかかわるすべての人が高度につながり関与する場合、この学習テクニックによって顧客のデータとお金を守ることができます。

自宅とオフィスのハイブリッドワークの世界では、複数の脅威が発生します。多くの場合、気づかないうちに家族が同じネットワークを使用していますが、すべての従業員が、自宅を職場の延長として扱い、「家庭のCISO」になるよう指導されるべきです。組織だけでなく、自身や家族を守るために従業員を教育することが必要であり、また従業員の年齢層を認識することも重要です。データセキュリティやプライバシーに対する考え方は、年齢層によって大きく異なり、サイバーセキュリティに関するメッセージにも影響を与えます。

セキュリティを導入する方法は1つではありません。「ハブ&スポーク・モデル」を好む人もいます。セキュリティ業務を担う小規模なコアセキュリティチームと、ビジネスラインに組み込まれたセキュリティ専門家を持つモデルです。この構造において、サイバーセキュリティ機能は、ブローカー（仲介人）やインテグレーター（統合者）、オーケストレーター（取りまとめ役）となります。このことは、これまで机上の作業に慣れ親しんできた技術者にとって大きな飛躍となります。自動化によって作業が容易になり、忙しい従業員の手から日々の手動チェックを取り除くことができます。

> 組織のデジタル化が急速に進むなか、デジタル改革の際にセキュリティについて考えてもらえるよう、私たちはソリューションや製品を開発するすべてのプロセスにセキュリティを組み込む必要があります。

Leah Gregorio
Managing Director, Cyber Security
KPMG米国

未来のサイバーセキュリティチームの組成

アウトソース、ギグワーカー、
自動化で飛躍的に高まる能力

サイバーセキュリティは、クラウドセキュリティ、OTセキュリティ、データサイエンスと解析、セキュリティアーキテクチャとエンジニアリング、攻撃シミュレーションなど、幅広い分野で決定的なスキル不足に直面しています。また、IT分野でも同様の能力を持つ人材への需要が高く、給与の上昇を招いているため、人材獲得競争はさらに厳しいものとなっています。

Forrester社の調査によると、CISOの平均在職期間は、英国では2年半強、米国では4年強と推定されています[1]。多くのCISOは、自身の市場価値や（特に規制上の義務による）要求の高まりがストレスや「燃え尽き」につながることをよく理解しています。多忙なCISOのもう1つの課題は、自身とそのチームが「サイバーエバンジェリスト（サイバーの伝道者）」となり、人間関係を築き、行動に影響を与えるために必要なソフトスキルを身につけることです。それに向け、サイバーセキュリティを専門化し、資格やキャリアパスを明確にしようという動きがあります。

さらに先を展望すると、レジリエンスストラテジスト、サイバーリスクモデラー、オーケストレーションマネジャー、ビヘイビアアナリスト、AIエシシストなど、今はまだ存在しないような新しい役割が生まれてくるでしょう。アウトソーシングやサードパーティとのパートナーシップの急増に伴い、ベンダー管理の重要性が増しています。特にクラウドベースのサービスでは、サイバーチームがセキュリティに対する責任を共有する必要があるため、おそらくエコシステムのセキュリティを構築する人材（エコシステムセキュリティアーキテクト）も必要になるでしょう。

1 UK CISO Career Paths, Forrester Research, Inc., March 24, 2021.

> 人材面での課題を解決するためにグローバルのリソースを共有して活用することで、将来的にサイバーセキュリティは、多くの下請け業者やギグワーカーと少数のコアチームで運営されます。しかし、私たちは関係者が信頼できる人材であることを知る必要があります。私は信頼できる（社内外の）人々の周りに、一種の「信頼の輪」が作られる世界を想像しています。

Fred Rica
Principal, Cyber Security
KPMG米国

> 人を率いるリーダー、マネジャーとしての私の役割は、メンタルヘルスとウェルビーイングに一層注力することです。サイバーセキュリティの専門家は、あらゆるインシデントを防止または阻止することを期待されていますが、それが不可能であることは誰もが知っていることであり、過剰な要求です。CISOにインシデント発生時に予想することを尋ねると、おそらく「自分はクビになる」と答えるでしょう。これは不健全なことであり、変えなければなりません。

Darren Kane氏
Chief Security Officer
NBN Co, Australia

未来のサイバーセキュリティチームを組成していくにあたり、CISOは既存の能力と新しい能力の両方に着目しなければなりません。また、新たな脅威に対応するためには、変化する需要に合わせてチーム内のスキルバランスを見直す必要があります。

サイバー・スキル・ギャップの解消

▶ 取り組むべき課題

KPMGのインタビューに応じたCISOは、雇用、再教育、アウトソーシングなど、スキル不足を解消するための革新的なアイデアを持っていました。

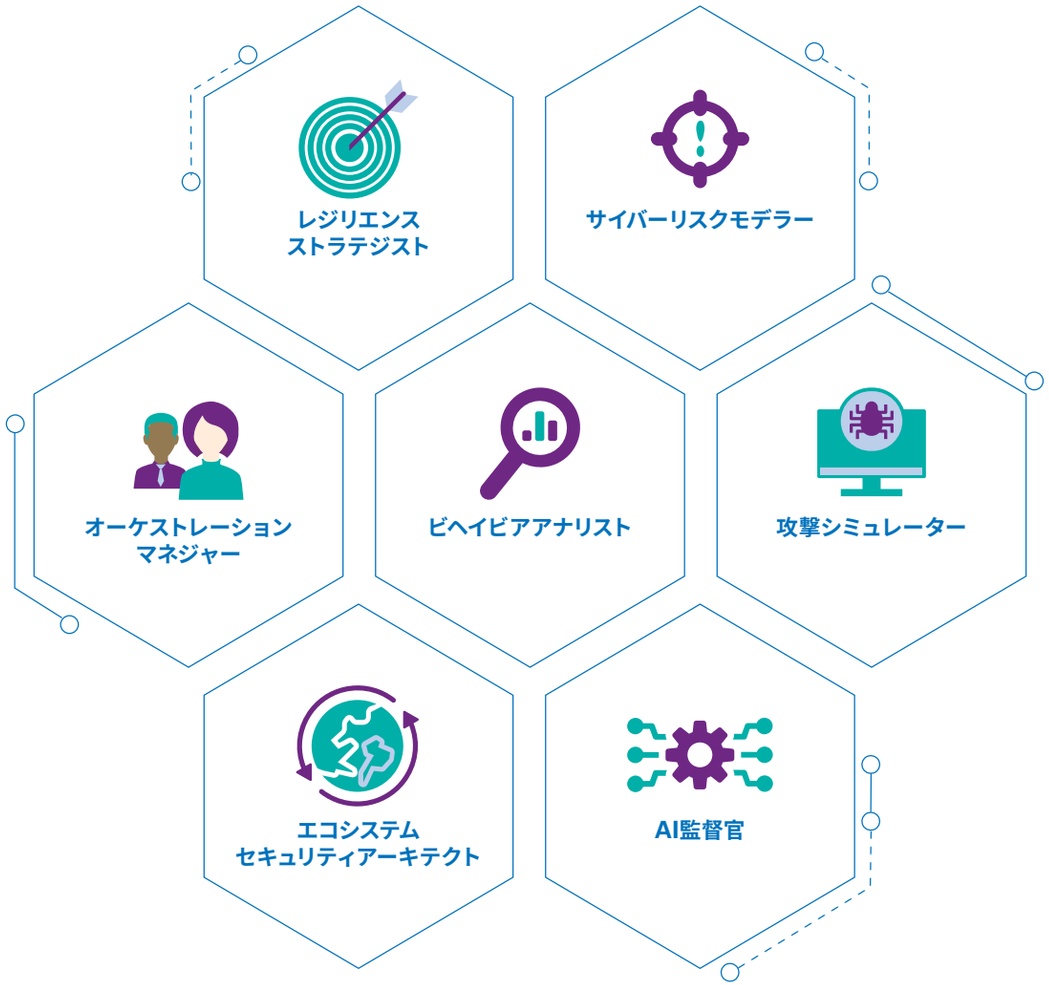
自動化ツールの活用

HP社のCISOであるJoanna Burkey氏が認めているように、自動化はサイバーチームにおいて重要な役割を果たすでしょう。「サイバー業界には深い構造的課題があります。技術革新の速度にスキル面で追いつけていない。また、十分な人材の採用や離職をゼロに食い止めることもできない。そういった意味でも、技術革新のペースについていくためには、自動化が不可欠です。」

ペースを維持する

チケット管理システムとワークフローを橋渡しするような付加価値の低い業務には自動化が不可欠です。Vodafone社のEmma Smith氏は「自動化は効率を高め、アナリストの関心を引き付けます。根本的な原因を突き止めることは、継続的な改善のために重要です。それによって同じ課題に対応し続けることはなくなります」と述べています。

未来のサイバーセキュリティの役職



深い技術力の再興

Vodafone社のEmma Smith氏が指摘するように、サイバーセキュリティのゼネラリストを求める傾向は弱まり、強い技術力を持つ人材への新たな需要と評価が高まっています。「テクニカルな専門知識、エンジニアや技術力を持つ従業員への報酬、キャリアパス構築のための新しいモデルの構築などは、私たちの戦略の基本となるものです。今や組織は、サイバーセキュリティチームにおけるリーダーシップと技術力の両方の重要性を認識していると考えられます。」

リスキリング

既存のサイバーセキュリティ人材を再教育するには、コストも時間もかかります。GSK社のSVP兼CISOであるMatthew McCormack氏は「再教育には課題があります。たとえばバイクの整備士が一晩でテスラの整備士にはなれません」と語っています。オンプレミスから、モバイル、IoT、ビッグデータへのシフトに対応するために既存のセキュリティチームのスキルを向上させるには2〜3年かかると思われます。

サイバーの専門家以外に目を向ける

CISOは、データ分析、リスク管理、クラウドなど、需要のあるスキルセットを持つ人材を中核的な技術分野として受け入れ、これらの人材を総合的なサイバー専門家に育成することができます。最初からサイバーのプロフェッショナルである必要はありません。それよりも重要なのは、ビジネスを理解していること、学ぶ意欲があることです。このような動きは、サイバーセキュリティにおける多様性の欠如を克服し、新しいスキル、経歴、視点、意見を奨励することにつながります。

2020年のKPMG英国とNational Cyber Security Centre UKの論文「Decrypting Diversity」によると、サイバーセキュリティにおけるダイバーシティとインクルージョンについて調査した結果、キャリアの壁を感じている人のうち、32%が「男女差別」が原因と回答し、22%が「人種、民族、社会的背景、地域による差別」を挙げています。

> “スキルの差よりも、多様性の差が大きいのです。多様なスキル、経歴、視点、意見を持つチームが、より良い答えを得られるでしょう。”

Leon Chang氏
Head of Cyber Defence Group
IHiS

人材プールを広げるためのコラボレーション

大学やカレッジとパートナーシップを結び、若い才能に投資することは、個人の育成と忠誠心の醸成という2つのメリットがあります。YPF社のCISOであるBrian O'Durnin氏は「失業率が高く、恵まれない人々が多い地域に、実習制度や大学への入学資格を提供することで、職業全般に貢献できると考えています。もし当社で働くことにならなかったとしても、私たちはサイバーセキュリティのエコシステムに貢献し、世界を少しでも安全にすることができるでしょう」と述べています。

アウトソーシング

アウトソーシング化の流れはさらに加速すると思われます。リモートワークの増加に伴い、賃金が比較的安いエリアでCISOを探すケースもあるでしょう。ギグ・エコノミーも拡大する可能性が高く、サイバーセキュリティの専門家は、場所や時間に縛られない柔軟性の高い働き方を求めています。この傾向は、COVID-19を契機としたリモートワークへの移行によってさらに強まりました。

「実行者」から「実現者」へ

▶ KPMGからの示唆

21世紀のダイナミックな労働力を形成するために、正社員、派遣社員、契約社員などを組み合わせ、組織内外から必要なスキルを持った人材を調達します。

CISOが業務の一部を外部に委託するケースが増えてきています。アウトソーシングの対象となるのは、拡張や縮小が容易な専門業者、変革支援や戦略的アドバイスを提供するプロフェッショナルサービス、ニッチなサービスプロバイダーや請負業者などです。また、企業がクラウドへの移行を進めていくなかで、CISOがクラウドサービスプロバイダーに期待するセキュリティ活動の範囲は広がっています。

トランザクション業務の大部分が自動化されたことで、サイバー人材は「実行者」から「実現者」へと移行し、新製品の開発、オペレーションの生産性と回復力、そしてより大規模で戦略的なサイバー関連活動に注力しています。しかし、このヒトと機械のパートナーシップを正しく理解するには時間がかかります。

CISOにとって重要な問題は、「組織がセキュリティを管理し、戦略的な方向性を定め、十分なリスク情報に基づいた選択を行い、インシデントや危機を管理するために、どのようなスキルを社内に保持する必要があるか」ということです。その先にあるのは、複雑な調達戦略と外部委託・共同委託先との関係です。責任共有モデルへの移行の一環として、セキュリティ運用に必要な規模と専門的なスキルの向上が求められています。また、CISOとサイバーセキュリティチームの役割と能力に対する規制当局の期待が高まっていることも影響を与えるでしょう。

周辺産業の人材をサイバーセキュリティに引き込むことは重要ですが、サイバー実務者が逆方向に進むのを促すことも有効です。そうすれば、キャリアの可能性が広がるだけでなく、サイバーセキュリティの価値を広く知ってもらうことができます。ほかの機能にもサイバーセキュリティを導入し、従業員一人ひとりの思考により深く浸透させ、自然に身につくようにしています。たとえば、クラウドエンジニアリングチームとレガシーITチームは、人を入れ替えることで、前者にはより厳格なセキュリティが、後者にはスピードが加わります。このような交配は、ダイバーシティ&インクルージョン（多様性）やニューロダイバーシティ（神経多様性）にも影響を与え、創造性の面で大きなメリットをもたらします。サイバー業界は、一度退職した親世代、レイトキャリア、定年退職者など、スキルベースを向上させることができる新しい人材をもっと受け入れるべきでしょう。

> 「サイバーセキュリティの専門家にとっての朗報は、その重要性と注目度が高まっていることです。求められる役割はコラボレーションツールやトランスフォーメーションなど幅広い課題を包含しており、スキルを拡大してより豊かなキャリアを築くチャンスになっています。」
>
> **Lisa Heneghan**
> Chief Digital Officer
> KPMG英国

「期待の星」として自動化を受け入れる

多大な効率性と従業員による
付加価値をもたらす自動化

自動化はサイバーセキュリティ業界にとって大きな可能性を秘めています。世界的な研究グループであるResearch for Marketsによると、世界のセキュリティ、オーケストレーション、自動化、レスポンス市場は、2025年までに約190億米ドルの規模になると言われています[2]。

これまで人の介在を必要としていた作業を自動化することで、作業負荷の軽減、効率化、一貫性の向上、対応の迅速化を実現し、セキュリティ担当者の包括的な意思決定を支援することができます。データ量が増加し続けるなか、自動化はサイバーセキュリティチームにとって必須の取組みとなっています。侵入検知システムの監視、従業員やサードパーティのオンボーディング、インシデントへの対応、コンプライアンスのチェックなどに対する自動化が不可欠です。自動化によって、エラーを減らし、顧客に安心感を与え、サイバー専門家を作業負荷から解放します。

自動化の大きな可能性を実現するために

▶ 取り組むべき課題

自動化は、CISOとサイバーセキュリティチームの有効性に大きなプラスの影響を与えます。

タレントギャップの克服

ほかの職種と同様、自動化によってサイバーセキュリティの専門家の作業負荷はさまざまな形で軽減されますが、Bayer社のCISOであるGary Harbison氏は次のように説明しています。「自動化は、手作業を減らすための大きなチャンスです。インシデントが発生すると自動でデータが収集されるため、エンジニアはデータを評価し、リスクを見極めるといった分析業務に専念できます。専門知識や価値を高めることに重点を置くことで、サイバーの仕事はより興味深いものとなり、より多くの人材を惹きつけられるでしょう。」

ほかにも便利なツールとして、セキュリティに関する問い合わせのためのチャットボックスがあり、特にサードパーティのセキュリティ管理に役立ちます。迅速な回答を得ることは、従業員やユーザーの体験を向上させるほか、ベストプラクティスを広めることでサイバーセキュリティを向上させることができます。また、新入社員の受入れも効率化され、システムやリソースへの適切なレベルのアクセスを自動的に提供することができ、貴重な人材を解放することができます。

サイバーセキュリティを組織に組み込む

サイバーセキュリティの専門家と開発者の関係は難しいものがあります。前者は脆弱性を減らすこと、後者は技術革新と市場への迅速な製品投入を目的としています。HP社のJoanna Burkey氏は、自動化によって、目的を見失わずサイバーセキュリティを組織に組み込むことができると感じています。「私たちは、現場がどのように仕事をしているかを理解し、杓子定規にならないようにしなければなりません。開発コミュニティは一般的に統一されたものではないため、自動化を用いることで、開発者がセキュリティを確保しつつツールを組み込むことを推進するのに役立ちます。」

総合的なサイバーセキュリティの強化

自動化によって、ヒューマンエラーを削減するとともに、新たな脅威に対するレーダーの役割としてリスクの発生源を把握することができます。これにより、機密性の高い個人情報やプライベートデータを保護することが可能となります。また、SOAR（Security Orchestration, Automation, and Response：セキュリティのオーケストレーションと自動化によるレスポンス）やチケット管理システムと連携することで、実際に起こった、あるいは潜在的なインシデントへの

> SecOps（セキュリティ運用）の役割は、ほぼ完全に自動化されるはずです。サイバーセキュリティチームは、SecOpsを設計し、結果と例外を管理すべきですが、これらについても自動化し、繰り返し作業できるようにします。
>
> **Matt O'Keefe**
> Asia Pacific Region Cyber Security Leader and Partner
> KPMGオーストラリア

2 Security, Orchestration, Automation, & Response Market Research Report, Research for Markets (360iResearch), 2021.

迅速な対応につながります。攻撃者の自動化もますます進んでおり、サイバーセキュリティチームはこのような脅威に対抗するために、同じペースでデータの収集と分析を行う必要があります。

オペレーション技術に自動化を導入する際には、安全性が最重要となります。世界の複数の港を運営する世界的な大手総合海運会社であるMaersk社でCISOを務めるAndy Powell氏は、そのアプローチを次のように説明します。「私たちは、ある港の桟橋で自動化を慎重に開始し、サイバー攻撃による被害を最小限に抑えられることを証明しなければなりませんでした。そして、これが達成されたことで、自動化の安全性に関するテンプレートを構築し、ほかのオペレーションにも拡大することができました。」

意思決定の強化

Axiata社はデータ分析を強化するために自動化へ投資しており、最終的には意思決定の多くを自動化することを目指しています。Abid Adam氏は次のように説明しています。「自らが革新しなければ、革新的な企業になることはできません。自動化、デジタル化を進めるために、データガバナンスモデルに取り組み、データの収集・分析方法を改善し、分析モデルを構築することをチームに課しています。」

規制当局を満足させる

グローバル企業は、複数の国や地域で異なる規制への対応に直面しており、規制上の要求は大きな課題となっています。このようなプライバシーの状況を管理するには、迅速で効率的なデータ収集が必要であり、自動化は継続的な管理のモニタリングにおいてますます重要な役割を果たしています。

サイバーチームの再構築

▸ KPMGからの示唆

黎明期の技術をどのように活用するのがベストなのかを思案するなか、自動化の急速な進展は低いレベルから始まっています。その潜在能力は非常に大きく、さらに成長を続けています。日々変化する規制環境や拡大し複雑化し続けるエコシステムにおいてセキュリティチームへの要求が増えるにつれ、自動化を活用することの重要性は増しています。

①SOARとチケット管理システムとの連携、②従来の顧客サービス業務を代替するボット、③リソースへのアクセスの自動設定および解除といった低レベルのアクティビティがあります。このような従来のサイバーセキュリティ機能のなかで最も労働集約的な3つの分野においても、自動化を活用することができます。

セキュリティの自動化を活用することで、サイバーチーム全体の将来像を検討することができます。一貫した基準とのギャップを特定して報告することが容易になり、CISOは投資の再配分を行うことができます。

複雑な規制環境では、自動化によって「1回のテストで、多くの要件に応じる」というアプローチが可能になり、レポーティングが自動処理され、規制当局へも迅速に通知することができます。

しかし、セキュリティとDevOpsの統合には現在のところ明確なガイドラインがないため、サイバーセキュリティチームは少し後れをとっています。クラウドには一貫した方法でコントロールを組み込む機能がありますが、CISOとサイバーセキュリティチームは、どのように自動化するか、どのようなツールが必要かを正確に把握しなければなりません。

> 自動化された環境において、私たちは手動では監視しないため、行動がトリガーとなる必要があります。つまり、インサイダーの脅威を回避するために、社内および顧客やサプライヤーの行動分析にさらに投資する必要があります。”

Sharon Barber氏
CISO
Lloyds Bank

自動化によって、システムをより複雑にしないことが重要です。計画が不十分で複数のテクノロジーが統合されていないために、取組みが失敗することがよくあります。CISOは、C-suiteの役割を活かしてCTOと連携し、組織全体のデジタルオートメーション戦略に積極的に参加して、共有機能を最大限に活用する必要があります。

プライバシーは、企業にとってビジネスおよび規制上の大きな課題となっています。KPMGインターナショナルが2021年に発表したレポート「Privacy technology : What's next?」は「プライバシー自動化の技術とは、データの管理や保護、プライバシープログラム管理の効率化や費用対効果の向上など、さまざまな側面における補完技術を紡ぎ合わせるもの」としています。

興味深い動きの1つとして、「権利行使のサービスプロバイダー」と呼ばれるものがあります。同サービスでは、アクセス権の自動化、デジタルフットプリントの削減、検索エンジンなどからの個人データの削除、オンライン上の電子メールIDのマスキングなどを行うことができます。

セキュリティを自動化することは、サイバーチーム全体の未来を形作ることにつながります。この分野の専門家が正しく行動すれば、セキュリティに関連する従来のプロセス重視の役割の多くはアルゴリズムと機械学習にとって代わられるでしょう。ただ、人間が不必要になるわけではなく、より不確実な事態についての決定を下し、戦略的なアドバイスやサポートを提供する役割を担うことになります。

> コンプライアンスは、金融サービスやエネルギー・公益事業などの業界では特に、サイバーセキュリティチームにとって大きな負担となっています。すべての要件に対して評価を行うのではなく、簡素化して自動化することで、一度のテストで多くの要件への適合性を見極めることができます。テストの自動化を、継続的に検討しましょう。そうすることでデータが充実し、より深い相関関係や分析を推進することができます。

Leah Gregorio
Managing Director, Cyber Security
KPMG米国

さらなる混乱に備える

めまぐるしく変化する世界に、
技術的、戦略的に対応するには

CISOはサイバーセキュリティに（おおむねポジティブな）影響を与える可能性がある、さらなる技術革新に備えています。

人工知能（AI）には幅広い可能性があります。基本的なロボティックプロセスオートメーション（RPA）の上に構築するものから、高度な機械学習や分析まで、ますます大規模なデータセットをカバーし、相互作用する人や企業の中核となるプロセスとのかかわりが、より頻繁になっています。

現在の「高度につながった世界」では、従来の境界線が取り払われ、複数の関係者が世界のどこからでも組織のデータやシステムにアクセスできるようになっています。さらに、5G、エッジコンピューティング、何百万ものIoTデバイスが加わって、サイバーセキュリティは格段に複雑になりました。このような状況においては、ネットワーク内外の誰も自動的には信頼せず、重要なリソースにアクセスする前に自らのIDとアクセス権を証明する必要があるといったゼロトラストやSASE（セキュアアクセスサービスエッジ）のコンセプトは、将来のセキュリティモデルの基礎となるかもしれません。

この先にある課題

▸取り組むべき課題

AIの安全性確保

私たちは、予測可能な決められた方法でコンピュータが動作し、固定されたアルゴリズムとコードでセキュリティを確認することに慣れています。一方、機械学習の増加は、次のような新たな疑問を投げかけています。どのようにアルゴリズムが学習され、どういったバイアスが導入されたか？　パラメーター内で動作していることを確認するために、どのように動作を監視することができるのか？敵対するAI技術によってどのように操作され、結果はどうなるのか？――。これらは新しい未熟な分野であり、データサイエンス、セキュリティ、倫理のスキルを融合させることが必要です。

データ国家主義への対応

データの民主化はすべての国境を取り除くことを意味していたはずでしたが、データの収益化の価値が高まるにつれ、国家主義への回帰が予想されるようになりました。GSK社のMatthew McCormack氏は次のように説明しています。「今後は国民のプライバシーを守るために各国がガードを強め、国家的な垣根が出現することになるでしょう。このような状況では、データの活用に関する最新の厳格な規則に準じなければならないセキュリティの活動は一段と難しくなり、企業は自由なグローバルネットワークに背を向け、国ごとの『城』を再構築するようになるかもしれません。」

ゼロトラストの導入

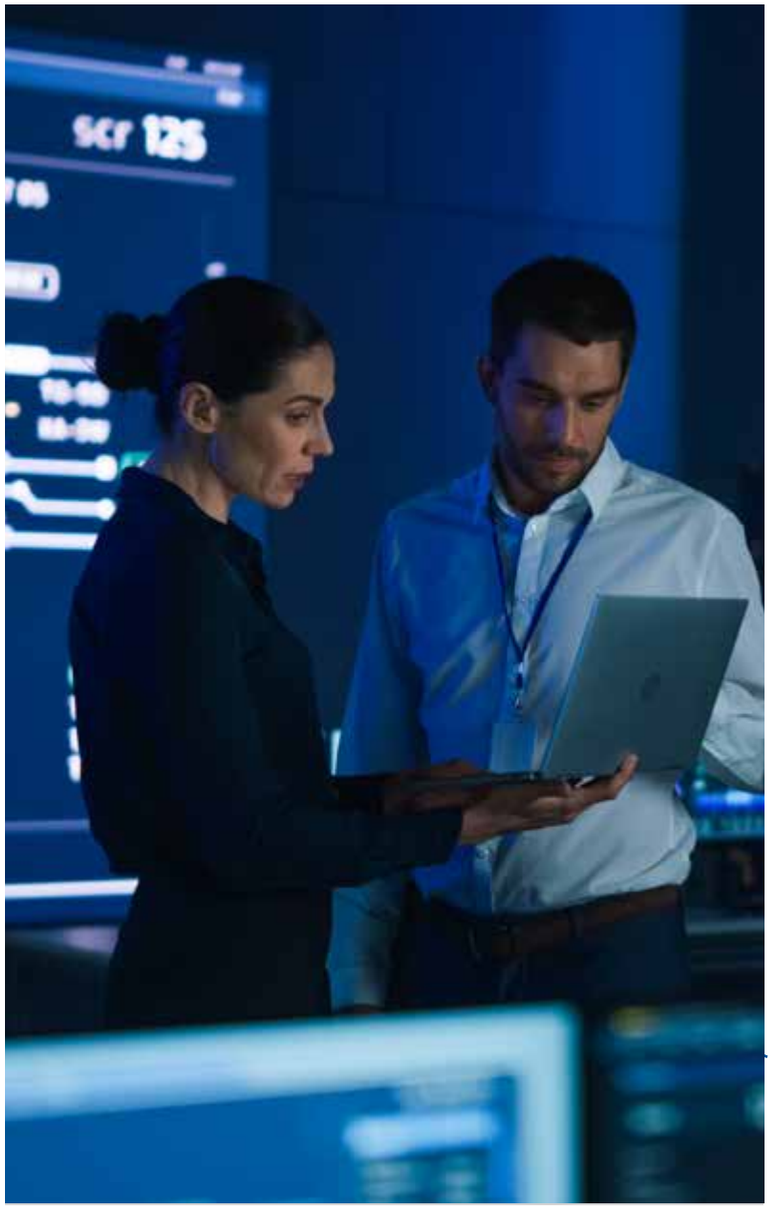
ゼロトラストとは、強力なID管理、高度な分析、デバイスインベントリを用いて、自身のデータがどこにあるかを把握し、そのデータへのアクセスをコントロールすることです。組織は通常とは異なる行動をより適切に検知し、許可されていないアプリケーション、サーバ、アカウントとの通信を防ぐことができます。

CTOやCISOとして25年以上の経験を持ち、IAM（IDアクセス管理）市場とテクノロジーのスペシャリストであるDarran Rolls氏によると、「よりスマートなクラウドと、より愚かなエンドポイント。つまり、エンドポイントはより賢く統合されたクラウドサービスを利用できるようにするために、ブラウザーセッションを提供するだけ」ということになります。このような世界では、組織はネットワークアクセスの可視性を高めることが求められます。

ゼロトラストやSASEは、セキュリティチームのためだけでなく、チームのためのコード作成や、インフラの開発をする人たちにも適用されるべきです。

> 社内外の攻撃から自社を防御する能力はもはや当たり前と見なされていますが、今日でも革新的な差別化要因のように語られることも少なくありません。勝者はAIや高度な機械学習、サイバーツールを採用して脅威アクター（攻撃主体）に対応するだけでなく、サイバー空間での戦いに積極的に挑んでいます。

Steve Bates
Global Leader
CIO Center of Excellence
KPMG米国



忘れてはならないのは「ゼロトラストは技術ではなくアイデアである」ということです。あまりにも多くの企業が、ゼロトラストを有限のプロジェクトとして捉えていますが、それは正しくなく、実際は始まりも終わりもない継続的な哲学です。”

Greg Day氏
VP and CISO, EMEA
Palo Alto Networks

データこそが未来

▶ KPMGからの示唆

今や、データの保護はエンドポイントの保護よりも重要であり、企業は多くの個人や組織がさまざまなチャネルを介してデータにアクセスすることを受け入れなければなりません。ゼロトラストとSASEは、網状に複雑に絡まった権利を管理するのに役立ちます。

一方、大手クラウド事業者は、この新しいエコシステムを実現するため、分散管理されたIAMモデルに裏付けられた、安全なコラボレーションの環境を一段と確立しています。

個人情報保護規制が進展してデータ主体の権利が明確になる一方で、国家は国境の内外を問わず国民のデータを管理する権利を主張しているため、データの扱いに関するポリシーはさらに複雑になるでしょう。これにより、メタデータの正確さと、それに基づいた高度なポリシールールを適用することでアクセスを制御することが重要となります。これらのアクセスルールは、機械学習システムと相互に作用し、ベースデータをいかに解釈するかを管理します。これにより、CDOの役割が拡大するとともに、組織内の情報ガバナンスの拡大の一環として、機械学習を高度に監督することが求められます。

サイバーセキュリティエコシステムの強化

サイバー攻撃に対応するための協力関係

CISOは、サプライヤー、アウトソースプロバイダー、請負業者、ビジネスパートナーなど、データにアクセスする第三者が増えたことによる複雑さと脅威を痛感しています。

何百、何千もの企業を調査し、厳しい契約を結んで監視することは理論的には素晴らしいですが、実際には非常に困難であると言わざるを得ません。アイデアは豊富にあるものの、サイバーセキュリティの専門家はこの難問に対する包括的な解決策を持ち合わせておらず、すべてのCISOがサードパーティの信頼性と継続的なセキュリティを確認する方法を模索しています。

さらなる信頼を目指して

▶ 取り組むべき課題

複数の関係者にまたがるデータを保護するという課題に直面しているCISOには、いくつかの選択肢があります。

サプライチェーンの引き締め

契約締結前のデューデリジェンスに関する明確なガイドラインに基づく契約とコンプライアンスは当然のことながら、要求されるサイバーセキュリティ基準を満たすことができない懸念がある場合には、サードパーティのアクセスを厳重に管理し、制限することが求められます。

機械学習を構築し、自動化されたリスク評価を確立することで、問題の規模を管理することができます。1,000社以上のベンダー評価を控えている多くの企業では、自動化がおおいに期待されています。

> 仮想化やデジタル化が進むにつれ、CISOの役割は企業中心のものから、社会全体の取組みであることを認識するようになります。この課題に直面しているのは自社だけではないため、外部にも目を向け、違反や攻撃の試みを規制機関に報告するとともに、コミュニティの強化を支援する必要があります。”

Prasad Jayaraman
Americas Region Cyber Security Leader and Principal
KPMG米国

> 強固なセキュリティ基盤を提供できるオペレーション、SecOps、セキュリティバイデザインで構成された堅牢なプラットフォームを構築するまでは、第三者のデータを扱う外向きの構築はできません。歩けるようになる前に走ってはいけません。そうでなければ、基本的な脆弱性につけ込まれてしまいます。”

Andy Powell氏
CISO
Maersk

業界内のコラボレーション

CISOが単独でこの問題を解決できないことは広く認識されており、その点をPalo Alto Networks社のGreg Day氏が強調しています。「私たちは、単なる傾向分析だけでなく、重大なサイバー脅威をより多く共有しながら国際的なレベルで調整し、データの共有を可能にする業界コミュニティを構築する必要があります。」

さまざまなステークホルダーとの協力

▸ KPMGからの示唆

現在のサプライチェーンやアウトソーシング環境を特徴づける複雑なネットワークに内在する脅威には、すぐに解決できるような策はありません。金融サービスなど、多くの共通の課題に対して業界全体で取り組むことによる効果が見られます。情報や知識を共有したり、他社から学んだり、共同戦線を張るなどの協力は多くの関係者に利益がもたらされます。Munich Re社のグループCISOであるPhilipp Südmeyer氏は「個人的な関係が重要です。相手をよく知り信頼できる関係を築くことで、より深い話をすることができます」と語っています。これは規制当局との関係にも応用でき、ともにチームとして動くことで、サイバーセキュリティの問題を積極的に対処し、コミュニティを守ることができます。

たとえば英国では、ACD（アクティブサイバーディフェンス）プログラムの目的として「大多数のサイバー攻撃による甚大な被害から英国の人々を守る」ことを掲げています。この概念は、ますます攻撃的で洗練された脅威から身を守るための、より広範なエコシステムに適用することができます。

協力関係の新時代

従来のサードパーティのセキュリティは、信頼性を錯覚させるものでした。契約にセキュリティを組み込んでも保証は限定的であり、定期的な評価ではサードパーティのリスクをリアルタイムに把握することはできません。また、4次、5次、6次のプロバイダーまで入れると、手に負えなくなることもあります。

社内の問題に対処するだけでなく、CISOは一段と広いエコシステムの安全性を確保する役割を果たすことにも目を向けなければなりません。

> 仮想化・デジタル化が進むにつれ、CISOの役割は企業中心的なものから脱却し、単独では果たせないことを認識するようになっています。社会全体における脅威インテリジェンスは、規制上の課題を解決するだけでなく、コミュニティをより強固なものにします。

Prasad Jayaraman
Americas Region Cyber Security Leader and Principal
KPMG米国

次のステップへ

CISOは、進化するサイバー脅威に対応するために、公式・非公式に多くの責任をバランスよく果たす必要があります。つまりこれは、セキュリティ意識を醸成し、同業の関係者との重要な関係を築くため、強制者からインフルエンサーへとシフトすることを意味します。絶対的な世界から、結果の確実性が低くリスクの回避と抑制が主な目的である世界へと移行していくなかで、白か黒かではなく「グレー」で対処する方法を学ぶことが重要です。

本レポートで紹介されている7つのアクションに対応するにあたり、CISOは次のステップを考慮する必要があります。

1. 顧客、収益、コスト、ROI（投資利益率）の観点から考え、C-suiteのように発言する。
2. インシデント発生後に素早く通常の状態に戻せるよう、オペレーショナルレジリエンスに重点を置く。
3. 組織内のネットワークを構築することに時間を費やす。さまざまな部門と連携し、運営方法を学び、安全を確保することが可能である、という信頼を得る。
4. 恒久的な役割や構造ではなく、ビジネスの要望に合わせてセキュリティチームを組成することを考える。正社員、契約社員やギグワーカーなど、従業員の最適な比率を検討する。
5. 自動化によってもたらされる効率性や、より高度な作業に集中できるようになった従業員による付加価値を考慮して、自動化のビジネスケースを構築する。
6. ゼロトラストを単発のプログラムではなく継続的な哲学として捉え、自社のビジネスにおけるゼロトラストの意味を考える。
7. 既存の業界団体への参加やカジュアルなグループの形成など、同業の関係者とつながる方法を見つける。

> “CISOはよりビジネスパーソンになってきています。つまり、製品が予定通りに出荷されなかった場合のビジネスへの影響を考え、ビジネスリスクとセキュリティリスクのバランスを取るようになってきています。”
>
> **Walter Risi**
> Global IoT Cyber Security Leader and Partner
> KPMGアルゼンチン

KPMGによる支援

KPMGは、進化する脅威に直面しても回復力のある、信頼できるデジタル世界の構築を支援します。そして、リスクを多面的に捉え、組織全体にセキュリティを浸透させることで将来を予測し、迅速な行動と安全で信頼できるテクノロジーによって、企業の優位性を確立します。

また、企業におけるサイバーセキュリティ対策の実施レベルにかかわらず、役員室からデータセンターに至るまで、一連の流れを通して専門知識を有しています。企業のサイバーセキュリティを評価し、ビジネス・プロフェッショナルに合わせて調整するだけでなく、先進的なソリューションの開発、その導入支援、継続的なリスクの監視に関するアドバイス、サイバーインシデントへの効果的な対応をサポートします。

さらに、技術的な専門知識とビジネスに関する深い知識、クリエイティブな専門家を兼ね備えており、企業のビジネスを守り、構築することに情熱を持って取り組んでいます。KPMGは、企業が可能性の限界に挑戦するために、信頼できるデジタルの世界を創造できるよう支援します。

謝辞

本レポートの作成にあたり、時間と知見を惜しみなく提供してくださった世界中のサイバーセキュリティのリーダーの方々に心より感謝申し上げます。

Abid Adam
Group Chief Risk and Compliance Officer, Axiata

Sharon Barber
CISO, Lloyds Banking Group

Joanna Burkey
CISO, HP

Leon Chang
CRO, IHiS

Greg Day
CSO, Palo Alto Networks

Karel De Kneef
CSO, SWIFT

Gary Harbison
CISO, Bayer

Darren Kane
CISO, NBN Co, Australia

Tammy Klotz
CISO, Covanta

Matthew McCormack
CISO, GSK

Jim Nelms
CISO, LabCorp

Brian O'Durnin
CISO, YPF

Michael Papay
CISO, AMEX

Andy Powell
CISO, Maersk

Darran Rolls
IAM Market and Technology Specialist 25+ years experience as a CTO, CISO

Emma Smith
Global Cyber Security Director, Vodafone

Philipp Südmeyer
Group CISO, Munich RE

分析・執筆協力

Leandro Antonio
KPMGブラジル

Steve Bates
KPMG米国

Jonathon Dambrot
KPMG米国

David Ferbrache
KPMGインターナショナル

Rommel Garcia
KPMGメキシコ

Leah Gregorio
KPMG米国

Lisa Heneghan
KPMG英国

Prasad Jayaraman
KPMG米国

Billy Lawrence
KPMGインターナショナル

Dani Michaux
KPMGアイルランド

Hartaj Nijjar
KPMGカナダ

Matt O'Keefe
KPMGオーストラリア

Daryl Pereira
KPMGシンガポール

Guillaume Rablat
KPMGフランス

Fred Rica
KPMG米国

Walter Risi
KPMGアルゼンチン

Kathy Robins
KPMGオーストラリア

Martin Tyley
KPMG英国

Tim Wood
KPMGローワーガルフ

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

home.kpmg/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。

home.kpmg/jp/socialmedia

本冊子は、KPMGインターナショナルが2021年7月に発行した「From enforcer to influencer - Shaping tomorrow's security team.」を、KPMGインターナショナルの許可を得て翻訳したものです。翻訳と英語原文間に齟齬がある場合は、当該英語原文が優先するものとします。

Publication name: From enforcer to influencer | Publication number: 137595-G | Publication date: July 2021