KPMG

サイバーセキュリティの主要検討課題2020

巧妙化するサイバー攻撃に、
今、必要な対抗策

ビジネスの世界は変化し続けており、第4次産業革命も進行中です。データは現在、企業の生命線となっています。デジタルエコノミーの潜在能力の活用、新しいカスタマーエクスペリエンス（顧客経験）の創出、サービスの変革、そして効率化とコスト削減の推進に、データは必要不可欠です。新しいビジネスモデル、新しいテクノロジー、新しいパートナーシップの融合により未来が作られていくのです。

変化する世界の中には、荒稼ぎを目論むサイバー犯罪者や、違法行為に手を染めている集団もあり、こうした存在によって繰り広げられるサイバー攻撃が、新たな脅威となっています。その中で企業は、競争優位性をどのように守るべきかを改めて検討し、サイバーセキュリティの構築と維持を目的とした新しい仕組みを導入する必要に迫られています。

サイバーセキュリティの専門家は、デジタル化が進むビジネスの心臓部（クラウンジュエル）を、サイバー攻撃から守り抜く必要があります。そのためには、サイバー犯罪者の先手を取り、思考と行動の両面でサイバーセキュリティ対策のスピードを高めていくことが不可欠です。

また、これらの課題に積極的な姿勢で果敢に取り組むことのできる協調性をもった人材を企業全体から集める必要があります。CISO（最高情報セキュリティ責任者）単独ですべてを背負うことはできないため、新しいパートナーシップ（組織横断的な対応チーム）が必要となります。テクノロジーは脅威ではなく、機会です。そして今、サイバーセキュリティはビジネスの主要な成功要因として成長の原動力になろうとしています。

本レポートでは、サイバーセキュリティに関する6つの項目を取り上げています。これらは、2020年以降KPMGがセキュリティの問題に取り組むための指針となっています。以下では、企業が今後直面するであろう課題を解決するうえで役立つKPMGの知見を項目ごとに紹介します。

事業戦略との整合性の確保

デジタルトラストと消費者の認証

進化するセキュリティチーム

新たな規制の波

クラウド変革とレジリエンス

セキュリティ機能の自動化

> **サイバー攻撃に対するレジリエンスを継続的に維持するためには、サイバー戦略をインシデント対応計画、事業継続計画、ならびに災害復旧計画と整合させる必要があります。また、フロントオフィスからバックオフィスまで、企業全体で取り組むことが重要です。**
>
> **Akhilesh Tuteja**
> Global Cyber Security
> Co-Leader
> KPMGインターナショナル

> **セキュリティ運用（SecOps）チームは、重要なタスクを可能な限り自動化する必要があります。多種多様な業務（たとえば、アクセスや不正のアラート、データプライバシーやリスク軽減に至るまで）を自動化することで、効率化とコスト削減の両方を実現することが可能です。**
>
> **Tony Buffomante**
> Global Cyber Security
> Co-Leader
> KPMGインターナショナル

事業戦略との整合性の確保

多くの企業は、サイバーセキュリティの管理体制の構築や人員の確保に膨大な費用を投じてきました。昨今、コスト削減が求められる企業も多く、セキュリティコストには大きな関心が向けられています。その注目度は、サイバーセキュリティそのものに対する関心にも劣らないかもしれません。コスト削減の努力や、ビジネスとサイバーセキュリティの課題に対する取組みの一環として、企業はサイバーセキュリティ機能の自動化に着手しており、デジタル化されたサイバーリスク管理プロセスを導入することで、企業全体の経営や営業戦略に結び付けようとしています。

KPMGの現状認識

KPMGは、企業のリスクモデルを再検証する中で、リスクシナリオの洗い出しにおいて事業部門の主体性が欠如していることを発見しました。本来、この洗い出しは事業部門が主体となり、セキュリティチームと協調しながら実施するべきですが、実際にこれを実現できている企業は多くありません。

リスクシナリオの洗い出しを効果的に進めるためには、セキュリティ施策による効果をより正確にビジネスリーダーに伝える仕組みが不可欠となります。これにより、リスクシナリオの実効性は飛躍的に高まるといえます。ただし、多くの企業はこれらのノウハウがないため、事業戦略とセキュリティ施策との整合性が未だに確保されていません。

サイバーセキュリティの世界では、最悪の事態を想定した計画を作成することが通常ですが、実際に発生するインシデントは、世間を驚かせたり、事業を揺るがしたりするまでには及ばないことがほとんどです。そうした観点から、多くの企業はスリーラインディフェンスにおける第2線だけでなく、業務執行ラインの第1線や、監査主導の第3線の中にも、セキュリティの視点を組み込もうと努めているように見受けられます。

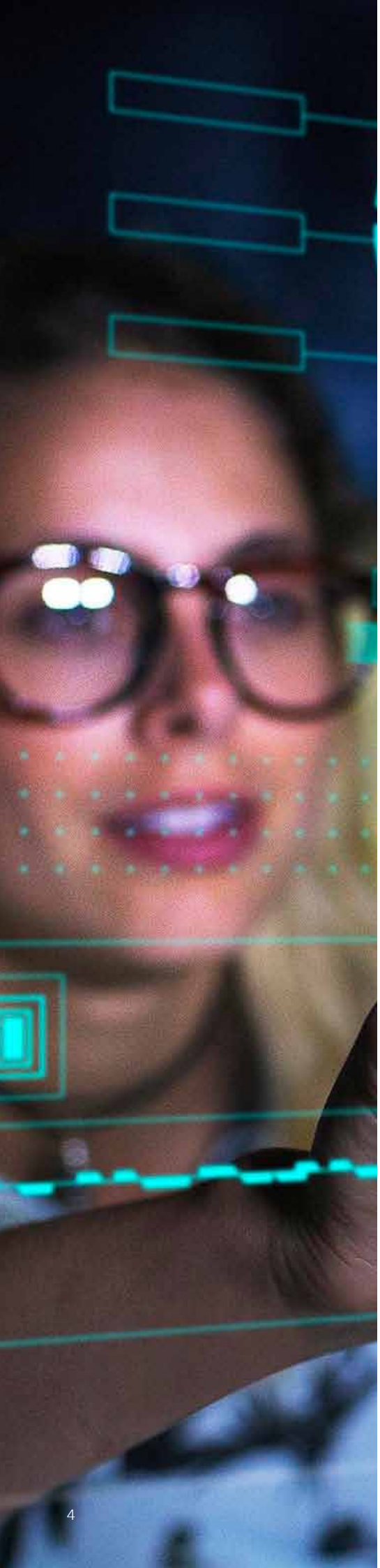
大規模な企業では、過去10～15年にわたってサイバーセキュリティ対策に膨大な資金を投じてきましたが、現在は、セキュリティ管理を自動化するというアプローチを通じてコストを低減すること、および適切な人材を適切な役割に就けることに焦点を合わせた新しい仕組みを構築する必要があると考えています。

各国の多くの企業（特に大手銀行）では、幅広いサイバーセキュリティ機能を集約したシェアードサービスセンターの設立を進めています。それは、すべてを自社で対応するとなると費用対効果が低くなり、また業者に対応を委託すれば保護すべきものを把握できず実効的なサイバーセキュリティ対策にならないことがあるためです。

John Hermans
Partner
KPMGオランダ

私たちは、リスクという観点から企業全体を分析する必要があります。まず、ITリスクを調査し、それからビジネスリスクの観点で分析します。そうすることで、トップからボトムへの一貫した視点が得られます。どこに潜在的な脆弱性が存在するのか、その脆弱性が攻撃された場合にどのような影響が生じるのかを理解するため、セキュリティチームには、ビジネスの優先課題にかかる深い知見が必要です。

Ben Krutzen
Partner
KPMGオランダ



KPMGが推奨する行動指針

サイバーセキュリティのどの分野に投資するべきかを、俯瞰的に検討しなければなりません。どのリスクシナリオに対処する必要があるのか、そのシナリオにはどのような対策が適切なのかを検討します。デジタル化を推進している企業では、サイバーセキュリティとリスク管理プロセスの自動化を進めていく必要があります。

セキュリティポリシーとセキュリティ対策がビジネスの中で有効に機能していれば、多くのインシデントはごく簡単に検知することが可能です。重要なことは、サイバーセキュリティをスリーラインディフェンスにおける3つの防衛線で、個別に運用するのではなく一体化して運用することです。

さらに、サイバーセキュリティ対策を現場まで巻き込む全社的な優先課題とすることが重要です。セキュリティチームが他の部門と継続的にコミュニケーションを取ることで、企業における戦略策定と事業計画の両面においてビジネスとセキュリティを結びつけていくことが求められます。

また、このような取組みに向けて、DevOpsチーム（開発担当と運用担当が密接に協力する体制）に、セキュリティバイデザインやプライバシーバイデザインなどのセキュリティを組み入れることを意図したアプローチを導入することも重要です。

最終的にKPMGが期待しているのは、サイバーセキュリティの専門家がITだけをリードする職務という立ち位置から脱却することです。そのためには、セキュリティチームが、ビジネスを深く理解し、リードできるようになる必要があります。そうならない限り、ビジネスとサイバーの共生は成立しません。

デジタルトラストと消費者の認証

若い世代の顧客は、銀行をはじめとする金融機関のオンライン取引や、通信販売などのオンラインサービスを日常的に使用しています。実店舗が徐々に姿を消しつつある中で、優れたカスタマーエクスペリエンスを提供する新進企業が市場シェアを拡大しており、従来の大企業やグローバル企業はこれを脅威と認識しています。

KPMGの現状認識

顧客は、取引が最も簡単かつ安全であると感じられるサービスを利用します。

オンラインサービスは、「手間」を減らすことが、より優れたカスタマーエクスペリエンスの提供につながります。たとえば、「パスワード忘れ」の対応として、顧客のモバイル端末にPIN（認証コード）が送付され、それを入力すればパスワードを再設定できるという仕組みは、まさに「手間」の軽減といえます。

簡単かつ安全なオンライン環境を提供するために、多くの企業は機械学習ベースのアプローチを取り入れ、顧客の一般的および固有の特徴や行動パターンを把握しようとしています。固有の特徴として、たとえば、指紋や声紋をはじめとする身体の様々なバイオメトリック（生体的）な特徴が挙げられます。また、特に金融機関では、顧客の行動パターンを把握するために、顧客が普段利用している取引のタイミング、ログイン方法、取引タイプ、送金や引出の金額等の解析を行っています。こうした要素を集約することで、各顧客における固有の行動パターンを把握することが可能になります。

オンラインサービスの提供に際しては、簡潔かつ効率的に利用できることに加えて、安全性に関する信頼感を顧客に与えることが重要です。オンラインサービス利用時の「手間」が多いほど、顧客が他社のサービスに乗り換えてしまう可能性が高まります。そのため企業は、顧客が望む結果を得るために「手間」がかからずに利用できるサービスを提供する必要がある一方で、商品またはサービスの提供者としてそのサービス全体を安全なものにする責任を負っています。

企業は、どのようにデータを収集するのか、また、データに対してどのようなリスクを想定したセキュリティ対策を適用するのか再検討する必要があります。機械学習用に構造化／非構造化データやバイナリデータをひとまとめに格納する「データレイク」という考えは新しくありませんが、そのデータの「湖」からどのデータを「釣り上げる」のか、どのように安全を保持するか、そしてデータへのアクセスを最適な関係者だけに許可するにはどうすればよいかといった問題は、いずれも重要な検討項目です。

Charlie Jacco
Principal
KPMG米国

近年、特に米国では、セキュリティフュージョンセンターに注目が集まっています。その目的は、集約したデータからセキュリティ上のインシデントを検出し、より無駄のない即応性の高いプロセスを実現することで、絶えず変化する脅威に適応し、悪意ある行為者より一歩先行し続けるように努めることです。

Alex Anisie
Director
KPMG米国

KPMGが推奨する行動指針

業種を問わず企業は、データ、認証、そして不正対応の各チームを連携させる必要があります。規制の要求事項を理解し、取り扱うデータの内容、所有者、入手元、格納先、活用方法などについて把握したうえで、セキュリティ管理体制を構築することが重要です。

体制に続いて、顧客の認証がより容易になるようにプロセスを見直すため、認証プロセスを改善させる必要があります。また、顧客が日常的に行う取引は、できるだけ簡単で手間がかからないようにする一方で、非定型的な取引では要件を少し厳しくして、通常の手順に一手順を加えることで、セキュリティを強化します。

最優先すべき点は、データの安全性や利用方法に関する顧客の懸念を理解し、それに対処することです。将来的には、データの大半がクラウド内に保管されることが想定されるため、データを暗号化して保護する方法を検討しなければなりません。データの安全性は、テクノロジーを用いて確保することが可能ですが、この問題への対処には、顧客に対する企業としての姿勢が問われます。そのため、顧客が抱えている懸念や課題を認識し、より快適なユーザーエクスペリエンスを提供していくことが求められるのです。

また、データの評価方法を見直すことも必要です。多種多様なデータに対して膨大なルールを適用するという従来のアプローチだけでは、サイバー攻撃を十分に防ぐことはできません。従来の方法ではデータやルールの増加に伴い偽陽性の検出が増加する一方、シナリオ外の攻撃パターンが見落とされ、不正行為者に攻撃する隙を与えてしまうことが考えられます。このような方法から脱却するためには、機械学習アルゴリズムを活用した効率的なデータ解析によって顧客の行動パターンを把握し、異常検知プロセスに組み込むといった対応が不可欠です。

そして、予防・発見・対応のプロセス全体にわたって、人とテクノロジーの相互関係に留意しなければなりません。ここで重要なことは、内部だけではなく外部からの影響、すなわち第三者によって引き起こされる問題も考慮することです。これは、結局のところ過去の教訓に学ぶという話になります。たとえば、認証プロセスについて、少し時間をかけて過去のインシデントを検証し、それに基づいた対策やストレステストの検査項目を追加することで、プロセスの改善に寄与することができます。

進化するセキュリティチーム

ここ数年間で、取締役会レベルでサイバーセキュリティの検討をする企業が増加しています。その結果、現在、多くの取締役がサイバーセキュリティの重要性を認識しています。セキュリティの専門家に求められているのは、セキュリティの知見をビジネスの視点で整理し、事業に対してどのような影響を与えるのかについて、取締役と同じ目線で説明する能力です。

KPMGの現状認識

多くの企業のセキュリティチームは、依然としてセキュリティの専門家、業務の従事者、そしてコンプライアンスの専門家で構成されています。しかし、本来セキュリティチームには、戦略的かつ先見的なビジネス感覚を有する人材が求められます。さらに、これからのセキュリティチームは、サイバーセキュリティの知見をもとにビジネスにインパクトを与えるチームへ変革を遂げていくことが必要です。

CISOとその配下となるセキュリティチームは、刻々と変化するビジネス環境への適応を求められています。彼らは、事業戦略を討議する中で、的確な情報を発信し、事業部門からの信頼を獲得し続ける必要があります。さらに、企業における業務上の優先課題を伝える際には、具体的かつ明確なイメージが伝わるように情報を発信するべきです。また、事業部門のリーダーと連携し、セキュリティチームの知見を可能な限り速やかに会社のセキュリティ施策に組み込むことや、時間とコストの両面から効率的な方法を判断していくことも重要です。

そのためセキュリティチームには、セキュリティに関する知識のみならず、ビジネスへの理解や、サイバーリスクを全社的な課題と捉えて、わかりやすく表現する能力なども求められています。

KPMGが推奨する行動指針

セキュリティチームには、俯瞰的な視点を持ってビジネスの多様な観点の意見を取り入れることが不可欠です。進化しつづけるビジネスモデルの中で企業が真に対応すべき課題を把握するために、事業部門のリーダーとも頻繁にコミュニケーションを取る必要があるのです。

デジタルトランスフォーメーションを推進している企業のセキュリティチームは、事業部門と、戦略的観点から深くコミュニケーションを取る必要があり、業務、デジタル、およびセキュリティを結び付ける接点としての役割を果たしていくことが求められています。ここで重要なことは、事業部門とセキュリティチームが共通の目標を掲げることです。

セキュリティチームは、事業部門がクラウド上にどのようなデータを格納しようとしているか把握することも重要です。開発環境と本番環境の双方に対して、必要となるデータを把握したうえで、セキュリティ施策を立案しなければなりません。

また、広報部門や営業部門などのカスタマーエクスペリエンスを所管する部門と緊密にコミュニケーションを取り、マーケティング戦略を検討することも必要です。万一、サイバーインシデントが発生した場合に、迅速かつ的確な対応をできるようにあらかじめ準備しておくことが、顧客との信頼関係の維持につながります。

さらに、自社のセキュリティ対策の自動化に取り組むことも求められています。人工知能（AI）が対応可能な対策と、人間による思考や判断が必要になる対策を切り分けることで、少なくとも50%の自動化を目指すことが必要です。

そして、サイバーセキュリティを企業におけるESG（環境・社会・ガバナンス）の重点施策として掲げるように働きかけ、サイバーセキュリティ戦略に対する包括的な展望と多種多様なインシデントに対応する方法の明示化も重要です。

新しい世界がこれまでとは異なるという現実を受け入れなければなりません。現状に満足せず、固定観念を持つことはやめるべきです。「それ以外の方法なんて存在しない」と思考を停止せず、謙虚な態度で「そもそも企業として何をしようとしているのか？」と自身に問うべきです。そして、利用可能なテクノロジーを評価して、今のビジネス環境に最も適した最善のプランを考案することが重要です。

Dani Michaux
Partner
KPMGアイルランド

CISOは、企業にとって欠かすことのできない存在になりました。デジタル化の推進、データの利活用、グローバルでの優先課題への対応という三つ巴の環境の中で、ビジネスとの整合性と戦略意識を備えたCISOは、あらゆる企業に必要不可欠な存在です。CISOとその配下のセキュリティチームは、今後ますます成長を遂げる企業を守り、その能力を高めてくれるでしょう。

Rik Parker
Principal
KPMG米国

新たな規制の波

テクノロジーリスクについて検討するとき、その当事者はIT部門です。しかし、サイバーリスクの当事者は、IT部門ではありません。サイバーセキュリティ関連の規制は、事業部門の優先課題と責務を重視する傾向が見受けられ、より組織横断的な対応が求められるようになってきています。たとえば、顧客指向の営業活動（信頼関係の構築等）、ミドルオフィスやバックオフィスにおける運営業務の改善、および取締役会主導のコーポレートガバナンス機能の強化などが該当します。つまり、スリーラインディフェンスの第1線である業務執行部門が、サイバーリスク対応の当事者になる必要があるということです。

KPMGの現状認識

KPMGでは、2020年以降も引き続き、さまざまなテーマに対して各監督官庁による規制が増加すると予測しています。特にアジアでは、実際に「サイバー」という用語が使用されているサイバーセキュリティ関連の新しい規制が制定されています。以前は、この分野の規制にIT部門を含意する「テクノロジー」という言葉が使われていましたが、正確な表現が使われるようになったことは称賛すべき変化です。

非常に多くの国が、EUの一般データ保護規則（GDPR）の要求事項を遵守するための規制を発令したり、自国固有のプライバシー保護法を制定したりしています。これを受けて、新たに主体的にデータを管理する部門を創設する動きが、特にグローバルの大企業において見られます。そのような企業では、データアナリティクスだけでなく、企業内におけるデータの格納先や所有者、データの利用方法、そしておそらく最も重要なこととして、データに対するアクセス権限を管理しています。

また企業は、さらなる投資の必要性を感じ始めています。単にツール整備やプロセス開発といったテクノロジーへの投資だけでなく、サイバー関連の人材不足という観点での投資も必要になりつつあります。サイバー経営やリスク戦略からシステムの構築や保守に至るまで、多くの分野で人材が不足しているのです。残念なことに、IT部門に所属するテクノロジーの専門家だけでは、サイバーセキュリティの規制に対処することはできません。そのため、IT部門による提言は内容が不十分なことが多く、また意図は適切であっても、経営陣や取締役会に正しく理解されずに、結果として不適切な形で導入されてしまうということが、多くの企業で発生しています。

私は、いわゆるレッドチーム演習や倫理的ハッキングといった多層化された攻撃シミュレーションに注目しています。SecOpsチームが多種多様な攻撃を検知できたり、あるいはそれをテストしたり、また検出された場合の対応計画や対応手順のストレステストを行ったりすることは、非常に重要です。サイバーセキュリティの規制に対処するチームは、このような対応を次々と業務に組み込んでいます。

Ton Diemont
Director
KPMGサウジアラビア

サイバー規制が焦点を合わせている分野は、基盤となる運用テクノロジー、委託先や外部サービスを利用したデータの処理、そしてレジリエンスです。レジリエンスとは、企業がサイバー攻撃を検出し、そこから復旧する全体的な能力を意味します。私はこれら3つを「トリロジー」（3点セット）と呼んでいます。

Daryl Pereira
Partner
KPMGシンガポール

KPMGが推奨する行動指針

スリーラインディフェンスモデルに関して、KPMGが推奨しているのは、サイバーセキュリティの責務とCISOの役割を第1線に組み込むとともに、それらの職務を業績評価指標と結び付けることです。CISOの役割は第1線の中核となり、サイバーセキュリティ戦略とそのビジョンを統括するものであるべきです。そして、SecOpsチームに対して、定常的な監視業務やツールの構成を、サイバーセキュリティ戦略やビジョンと整合させるように働きかける必要があります。

第2線では、テクノロジーのリスク管理として、設計の品質と、レジリエンスにかかるポリシーおよび基準をサポートし、その結果を経営陣と取締役会に報告することが求められます。第3線では、最初の2つの防衛線での業務を点検、評価します。これにより、法令遵守を含む企業のサイバーセキュリティ対策を企業全体に拡大することにつながります。

また、サイバーセキュリティ対策の設計、実施状況、そして実効性の点で法令遵守がなされていることを継続的に検査する仕組みを導入し、改善の必要な領域を明らかにすることが非常に重要です。さらに、業務に関するサイバーレジリエンスを全体的なアーキテクチャとプロセスに組み込むことで、テクノロジーとOT（制御・運用技術）両方のセキュリティを強化します。

サイバー関連規制遵守の監督役としては、テクノロジーの専門家ではない人材の登用を推奨します。具体的には、事業部門が対策の意図を正しく理解し適切に実行できるように、事業部門の言葉でコミュニケーションを取ることができる人物が望まれます。また、監督役は、企業の経営モデルに関して幅広い考え方を持っている必要があります。そのため、企業全体のリスクを把握している最高リスク責任者（CRO）、最高財務責任者（CFO）、あるいはCEO代理などが理想的な候補です。監督役は、全社規模でサイバーセキュリティを推進する支援者となり、最高執行責任者（COO）やCISOと緊密に連携していくことになります。

そして、十分な時間を割いて、内部統制や社内ポリシーから、各国・地域の規制に至るまでのあらゆる要求事項の管理を、単一の統合管理フレームワークに集約する必要があります。そのフレームワークで企業内のガバナンス、リスク、コンプライアンス、およびそれらのテスト手順の実効性向上を図ることが求められます。プライバシー、レジリエンス、およびセキュリティ規制によって課されるさまざまな対策との間にシナジー（相乗効果）が隠れていないか探ってみると、意外な可能性を発見して驚くかもしれません。

各企業は、システムやテクノロジーではなく、ビジネスに着目するべきです。何が市場で競争優位を生み出すのかをピンポイントで明らかにする必要があります。それは知的財産であったり、サプライチェーンであったり、あるいは価格設定かもしれません。それが何であれ、サイバーセキュリティの観点からすると、それこそが守るべきもの（クラウンジュエル）なのです。

クラウド変革とレジリエンス

多くの企業が取り組むべき課題の1つは、クラウドの成熟度と有効性について、CISOおよびセキュリティチームと事業部門の認識を共通化することです。事業部門が、「今後はクラウド化を推進したい」と言っている中で、セキュリティチームが、本来の要求とは合致しないプロセスやツールを開発しているといったことがしばしば見受けられますが、この状況を変革する必要があります。

KPMGの現状認識

従来IT部門は、ITインフラの整備に対する責任を担っており、クラウドという概念が出現するまでは、主に現場という地上の課題を解決することに注力していました。特に、ITインフラとその関連資産を管理することは常に大変なことで、ITインフラの脆弱性スキャンを担当するセキュリティチームが、最新の脅威リストの影響範囲を特定できず、どのシステムをスキャンすればよいのか判断できないことが少なくありません。あらゆるものが、より迅速になるクラウドにおいて、セキュリティ機能をITインフラの整備計画の早い段階で組み込むことは、現在、多くの企業が取り組むべき課題となっています。

クラウドに関して、多くの企業のセキュリティチームは、スキルの点でも人材の点でも、事業部門を支援する準備ができていません。クラウドでは、情報の保護が最優先の課題です。KPMGの調査では、データをクラウド内に保管する現在の方法は、必ずしもレジリエンスが高いとは言えないということが明らかになっています。これは、単に複数の可用性（アベイラビリティ）ゾーンを設ければよいという話ではなく、大規模なセキュリティ侵害が発生したときに重要な資産を復旧する能力があるかという問題でもあります。

また、多くの企業では、セキュリティ分野全体について、2つの陣営が両極端の立場で活動しているように見受けられます。一方は、セキュリティアーキテクチャに20年以上も取り組んできた保守的な実務家で、クラウドの中で生きることに完全には適応できていません。もう一方は、最新のテクノロジーに精通している最先端のセキュリティに関する専門家で、セキュリティを設計レベルから大規模に組み込むことで、クラウドの考え方の普及と実現に努めています。このように分断された陣営に対して、セキュリティに関する共通の理解を持たせることが最も重要な課題の1つです。

セキュリティチームは、場合によっては既存の成果を破壊することさえ許されるということに気づく必要があります。そこから何かを学んで、その知識を生産的に活用すればよいのですが、多くの企業は、このような考え方を推し進めることができません。しかし、実験と学習の文化こそが、今日の急速に進化する市場の中で、企業から必要とされるサイバー人材を惹き付ける要素です。クラウドによって、すばやく何かを作っては壊し、また作り直していくことで、徐々に成果を積み上げていくことが可能になったのです。

Caleb Queern
Director
KPMG米国

私たちの見るところでは、コンピューターサイエンスの出身でコード作成プロセスも少し勉強してきたというセキュリティアーキテクトがますます増えています。こうした人材は、自ら主導権を握り、新しいクラウドツールを使用して、セキュリティを設計段階からサポートできるようにする必要があると考えています。つまり、クラウドとセキュリティの橋渡しが始まり、クラウドセキュリティの専門家としての役割が出現し始めているのです。しかし、そうした人材はまだ非常に少数であり、極めて稀な存在です。

Katherine Robins
Partner
KPMGオーストラリア

セキュリティチームの行動指針

学習する企業へと変革する ― クラウドに精通した人材を惹き付けるものは、報酬ではなく「文化」です。有望な候補者は、「昔ながらの、過度にリスクを嫌悪する動きの鈍い企業には入りたくない」と考えています。変化と実験をいとわない企業としての文化を醸成することで、優秀なクラウドに精通した人材にアプローチすることができます。

小さく考え、すばやく行動する ― 迅速に作り、迅速に壊し、これらから学んだことに基づいて再び作るというメッセージを発信することが必要です。また、段階的に手順を踏むことが成功の秘訣です。たとえば、新しいセキュリティ対策に関しても、少しずつ実施していくことで、ビジネスのスピードダウンを避けることができます。

シフトレフトを実施する ― 顧客とユーザーの両方に最大の価値を提供する取組みの一環として、「シフトレフト」を実施します。ソフトウェアの開発プロセスの、可能な限り早い段階で、セキュリティ評価を実施する必要があります。これには、コードによるインフラの構成管理（Infrastructure as Code、IaC）を含みます。シフトレフトの実施には、開発者がセキュリティチームを介さずに必要なセキュリティ対策を実装できるようになることが求められますが、これはクラウドによって容易に実現が可能です。

基本的なコードを理解する ― コードを読み書きする能力があると、DevOpsチームとコミュニケーションを取り、セキュリティの専門家による関与が必要となる機会を正しく検知することができます。セキュリティの専門家に求められる役割は、設計書をレビューするという従来のものから変わってきており、コードを読み書きする能力がますます求められるようになってきています。

理解しようと努める ― 企業全体とコミュニケーションを取り、業務改革、事業継続、および情報保護の理解に努める必要があります。その方法は、企業内部で開発しているソリューションと決定的に違うわけではありませんが、クラウド上で複数の地域の重要なデータを保持しているときは少し異なります。「理解しようと努める」ことをセキュリティチームの文化に組み込むことは、運用視点で考えた場合に「ノイズ」を除去することに役立ち、より大きなセキュリティの優先課題に集中することが可能になります。

CISOが支出の削減とセキュリティチームの効率化を目指すためには、不要になったデータの自動削除が全社戦略の柱になるはずです。同様に、CISOは、クラウドやセキュリティ、イベント管理をけん引するサービス提供者と連携することで、SecOpsチームの作業、不正の判定、およびセキュリティ対策を自動化することについても検討するべきです。

Anthony Gawron
Director
KPMG米国

企業は、デジタル環境における顧客行動を分析するためのテクノロジーに投資しています。その目的は、認証の観点から顧客の身元を確認するためだけでなく、デジタル環境が顧客行動に対して、どのように作用するかを知るためです。そのような企業は、過去10年間その種の活動が極めて効果的だったという過去の事例に倣っているのです。

Ronald Plesco
Principal
KPMG米国

セキュリティ機能の自動化

企業では、ID認証から、脅威の検出、そして対処まで、セキュリティ対策を自動化することを目的としたデータの集約が推進されているように見受けられます。金融サービス、eコマース／小売、テクノロジー、メディアおよび通信、そして自動車などの非常に幅広い顧客情報が、多くのセクターによって収集、分析されています。これらの情報は、これまで極めて分断された環境で保持されるのが普通でしたが、企業はそれらの情報が宝の山であることに気づき始めています。情報を適切に整理し効率的に利用することができれば、抽出や分析により様々な付加価値を生み出すことができるのです。

KPMGの現状認識

企業は、ごく最近まで完全に手作業で行われていた業務を、分断されていた情報の一元化によって自動化しようとしています。

情報の一元化による自動化に伴い、オンラインサービスの本人確認機能を強化できるだけではなく、どの端末、コンピューターがウイルスに感染しているか、最近フィッシングメールを受け取ったか、アクセス権限のないネットワークに侵入しようとしたかといった、さらに踏み込んだ情報も入手できるようになります。

セキュリティの専門家は、外部サービスと自社開発ソリューションの組み合わせで、サイバーセキュリティ対策を可能な限り自動化することを目指しています。また、セキュリティ戦略が、企業価値の創造やカスタマーエクスペリエンスに関する目標と整合するように働きかけています。企業は、クラウドサービスを活用して、スリーラインディフェンスの第1線と第2線を自動化することにより、企業全体の脅威に対してより的確に、人間が介在することなく対応できるようにすることを目指しています。それと同時に、すでに実施しているセキュリティ対策が、実際に期待どおりの役割を果たしているか評価しようとしています。

KPMGが推奨する行動指針

データ管理部門の担当者に相応の権限を付与しているということについて、常に注意する必要があります。そのことを肝に銘じたうえで、踏み出すべき最初のステップは、重要なデータをさまざまな外部サービスから中央のアクセスしやすい場所に集約することです（現在、非常に多くの企業が外部サービスに重要なデータを保持しています）。

また、企業におけるデータ管理ポリシーの策定を推奨します。これによって、データの整形方針、適切なラベル付け、保有するデータの種類、データの移転先や利用方法などに関する企業内の理解の共通化を図ることが可能になります。

データ管理の対応が遅れている企業は、AIや機械学習の利用を開始する準備が整っていないと考えられます。そのような企業にとって重要なことは、対策を講じたい課題（たとえば、不正検出、カスタマーエクスペリエンスの向上、業務効率の改善など）に優先順位を付けることです。また、適切なツール、テクノロジー、および高度な分析機能をどのように準備しておけば、データが利用可能になった時点でそのデータを活用することができるかを判断することです。

KPMGによる支援

KPMGは、ビジネスがサイバーリスクによって制約を受けてはならないということを理解しています。また、サイバーセキュリティの本質は、リスクの完全な排除ではなく、リスクの管理であると認識しています。

KPMGは、サイバーセキュリティへの取組みがどの段階まで進んでいるかにかかわらず、侵入テストやプライバシー戦略、アクセス管理や企業風土の変革といったあらゆる局面において、企業が目指す目的地に向けての支援を提供します。この目的地とは、サイバー攻撃やセキュリティインシデントから壊滅的な打撃を受けることなく、事業継続のできる環境を構築することです。KPMGは、顧客と緊密に連携することで、戦略とガバナンス、企業変革、サイバーディフェンス、そしてサイバーセキュリティ対策への取組みの支援をします。そして、単にソリューションを提言するだけではなく、その導入と遂行までを一貫してサポートします。

お問い合わせ先

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

home.kpmg/jp/socialmedia

Designed by Evalueserve.

Publication name: All hands on deck: Key cyber security considerations for 2020

Publication number: 136862-G

Publication date: March 2020