KPMG

ライフサイエンス・エコシステムにおけるセキュリティ

拡大するサプライチェーンの
セキュリティ確保のための新たな方向性

KPMG International

home.kpmg/cybersecurity

目次

はじめに

ヘルスケア業界とライフサイエンス業界は、的確な治療と専門的ケアを確実に提供するために、研究者、臨床試験の専門家、医療提供者、製造業者、規制当局、そして患者を結び付ける関係者のネットワークを構築しています。

ネットワークでつながる関係者間で機密性の高い医療情報やデータを共有することで、より良質かつ迅速で個々の患者に合わせた治療やケアが可能となります。また、リモートアクセスやモバイルアクセス、5Gネットワークのような新興テクノロジーによりバリューチェーン全体の接続性が加速しており、テクノロジープロバイダーはライフサイエンス企業の事業やパートナーシップを構成する不可欠な要素となりつつあります。

しかし、このネットワークがシームレスかつ高度になるにつれ、サイバーセキュリティの脅威が急増しています。2020年、ランサムウェアの標的となることが最も多かったのは、ヘルスケア業界でした[1]。多額の損失につながる破壊的なランサムウェア攻撃は脆弱なサードパーティ・サプライヤーによって拡散されることが多く、複雑なエコシステムのセキュリティを確保することが急務であると警鐘を鳴らしています。

「KPMGグローバルCEO調査2021」によると、新型コロナウイルスの世界的な感染拡大以降、サプライチェーンリスクおよびサイバーセキュリティリスクが増加しており、今後3年間の成長に対する主要な脅威となっています。ライフサイエンス業界も例外ではなく、現在、業界が世界各地でコロナワクチン接種プログラムを支援するという役割を果たすなか、サプライチェーンリスクはさらに大きな影響をもたらします。

業界の複雑化およびリスクによる課題の増大に加え、ライフサイエンス企業は、これまでは1次請けサプライヤーの管理にのみ注意を払っていましたが、今日では2次請け、3次請け、そして4次請けサプライヤーまでもが存在する、広大で新たなリスクが伴う世界に直面しています。こうした新たな当事者にはクラウドサービス、ITプロバイダー、パートナー、アライアンスなどがあり、エコシステムが拡大しています。

イノベーションと新たな脅威がいずれも急速に進展するなか、サードパーティ評価に対する従来のアプローチは、もはや目的に適合しなくなっています。現在の業界を構成するものは、従来の明確な境界を持つ「城」ではなく、「都市国家」の様相を呈しており、その拡大したエコシステムでは、当事者たちがデータセキュリティを確保するための共通のアプローチの確立に向けて力を合わせています。

サードパーティリスク管理、モニタリングおよびイノベーションは新しい課題ではありませんが、新たなリスクが交錯するなか、組織にとって今日の新しいエコシステムにおける自らの役割を正確に理解し、自組織のデータ共有機能を把握して脆弱性を識別することが不可欠になっています。将来における競争優位性と繁栄を目指す組織は、業界内の連携を強化するとともに、クラウドサービスへの依存度が高まるなか、セキュリティ評価とリアルタイムのモニタリング機能を活用し、データ管理を改善していく必要があります。

現実にデジタルトランスフォーメーション（DX）の範囲は広がり、その進行は加速しています。デジタル時代におけるエコシステムの機能およびセキュリティを強化する新たな方法が利用可能になったことにより、成功と失敗の差が浮き彫りになっていくと考えられます。

本稿では、世界中のクライアントを支援しているKPMGのサイバー専門家の協力を受け、ライフサイエンス業界における現在の課題と新たなソリューションを検討します。リスクの軽減・信頼の構築・プライバシーの向上・継続的なイノベーションの推進・コンプライアンス管理を実現する高いセキュリティを備えた最新のエコシステムを導入するにあたり、このソリューションが役立つことを祈っています。サイバーセキュリティに関する脅威とリスクは増加の一途にあるため、一刻の猶予もありません。

Caroline Rivett
Global Cyber Security
Life Sciences Leader
and Associate Partner
KPMG英国

1 2021 Ransomware Threat Report, Unit 42 Palo Alto Networks, 2021.

オープンイノベーションに潜む脅威をシャットアウト

デジタルテクノロジーを活用した新しいオープンイノベーション・モデルが急速に普及するなかで、今日のビジネスを支えるサードパーティ・エコシステムを的確に把握し、効果的に管理することは、かつてないほど困難になっています。

KPMGの専門家は、重要な市販ソフトウェアやオープンソース・ソフトウェアにバックドア（認識外の不正アクセス経路）が書き込まれている事例を確認しています。バックドアが組み込まれると、悪意のある者によってマルウェアが仕込まれるおそれが生じます。これらのバックドアは、攻撃者によって起動されるまで休眠状態となっていることがあります。マルウェア検出に用いられる特徴を変化させて検出を回避する「ポリモーフィック型マルウェア」は、セキュリティや管理ツールの瑕疵によって持ち込まれることが多く、きわめて堅牢なセキュリティ環境であっても瞬く間に弱体化させてしまう可能性があります。

この課題も加えると、従来のサードパーティリスク管理では、規模および複雑性が増大した今日のサプライチェーンを明確に把握することは非常に困難になっています。

従来

これまでサプライヤー関連のインシデントでは、組織は外部のセキュリティモニタリング・ツールを使用して侵害の兆候を特定し、対応していました。その過程で、自社のデータが安全であるか懸念を持つ顧客による問い合わせが殺到することがあり、多くの場合、被害を受けた企業はこの安全性を説明するプロセスに忙殺され、影響範囲の特定や顧客への案内を迅速に行うことができなくなっていました。

現在

このような脅威に対処するため、サードパーティ・セキュリティの技術が開発されています。セキュリティ評価およびモニタリングを行う企業は、人工知能や機械学習の活用により、異常な動作をモニタリングする支援を開始しています。これらのツールを使うことで、どのような潜在的リスクがあるかについて、1人のアナリストが広範囲に把握することができます。

さらに、米国国立標準技術局（NIST）が中心となり、セキュリティコントロール・データの送受信、標準化および自動化の強化を目指してOpen Security Controls Assessment Language（OSCAL）などの機能が開発されています。この枠組みは、当初は米国政府を支援するために創出されたものですが、現在では、重要な評価データの可視性および生成頻度を高めるため、商業的に利用されています。

ケーススタディ | リスクの可視性の向上がもたらす力の解放

KPMG米国は最近、金融業界に属するクライアントの協力を受け、サードパーティ・セキュリティ評価について特定の一時点に対する評価から、より積極的なリスクベースのアプローチに移行するための最適な方法を検討しました。この概念実証では、クライアントとサードパーティとの間でほぼリアルタイムでセキュリティコントロール・データの収集が行われるように設定するとともに、OSCALを標準化した上で、サービスレベル契約（SLA）に準拠しているかどうかも確認しました。このモデルでは、リスクの可視性の向上によってリスクに対するクライアントの理解がどのように深まるか、そして問題の発生時に自動的に対応するにはどうすればよいかが明らかになりました。

新たなエコシステムにおけるセキュリティリスクの管理

今日の企業には膨大な量の機密情報と知的財産があふれており、それらがエコシステム内を移動しています。当然のことながら、サプライチェーンリスクを評価する上では、サプライチェーン内を移動するデータの流れを理解することが重要であると考えられてきました。しかし、今日のエコシステムでは、こうしたデータフローがますます複雑かつ不透明になっています。テクノロジーが急速に進歩するなか、ビジネスデータに対する脅威および脆弱性は種類・件数ともに増加しており、なかでもサードパーティでのインシデントが増加しています。

エコシステムのリスクを識別することは困難ですが、組織に対する潜在的な脅威を把握するために重要でもあります。そのためには、次の点を明確にすることが重要です。

エコシステムにおける組織の位置付け

リスク管理プロセスの第一歩は、組織がエコシステム内のどこに位置しているかを理解することです。組織の内部環境と外部環境を理解するとともに、ミッションクリティカルな情報資産は何か、それらはどこにあり、システム内をどのように移動しているかを特定する必要があります。これにより、すべての重要な情報の保護にしっかりと狙いを定めたリスクベースのアプローチが可能になります。

データ共有

このモデルにおける脅威とリスクの範囲は大きく、1社のサプライヤーが上流または下流の顧客に影響を及ぼした場合、サービスの途絶、データ完全性の喪失、またはデータ損失につながる可能性があります。このようなデータ・サプライチェーンにおける依存関係により、エコシステムにおけるすべてのパートナーとの接続性、データ共有、および関係性を積極的に把握することが必要となっています。これには、企業とサプライヤーとの間のデータ共有のレベルを継続的に把握することが含まれます。例えば、スマート・エコシステムのステークホルダーは現在、2次請けサプライヤーやリスクの集中についてさらに踏み込んだ議論を進めています。

クラウドのセキュリティ

コロナ禍による破壊的な影響への対応としてクラウドサービスへの移行が飛躍的に加速しましたが、内部および外部における潜在的な脅威の可能性を高めています。特に、主要なクラウドプロバイダーのセキュリティアーキテクチャについて得られる保証が限られているにもかかわらず、クラウドサービスが侵害された場合のデータ損失や漏洩に対しては利用者企業が責任を負っている点にも留意が必要です。

クラウドサービスの利用によってリスクが変化したため、企業は保証を受ける方法や自社のリスク選好を再評価する方法について工夫を強いられています。メガクラウドプロバイダーの急増を考慮すると、クラウドにおけるセキュリティリスクの課題は、規制当局のみが対処できる課題なのかもしれません。

リスクの交錯

サイバーリスクおよびデータリスクにとどまらずエコシステムにおけるリスクについて、組織は複数の異なる種類のリスクの交錯について、より詳細な検討を行っています。高度なアナリティクスや機械学習モデルを用いることで、そのような潜在的なリスクシナリオが特定され、重大な潜在的課題が明らかになりつつあります。リスクモデル、エコシステム内のデータへのより容易なアクセス、そしてテクノロジーの改善がサードパーティ・セキュリティに具備されることで、リスクの可視性が高まり、サイバーリスクに対応した意思決定能力も強化されるでしょう。

サードパーティの先まで拡大するサプライヤーリスク

直接取引するベンダー以外のどこにデータが共有されているかの把握に組織が苦心しているなか、規制当局および顧客では、2次請けサプライヤーリスクの議論が盛んになっています。データ・サプライチェーンによって、顧客データにかかる懸念は、3次請け、4次請け、そしてさらにその先のサプライヤーにも及んでいます。KPMGの報告書、「サードパーティリスク管理の展望2020」では、調査対象企業の72%が「2次請けサプライヤーの評価方法を早急に改善する必要がある」と回答したことが指摘されています。

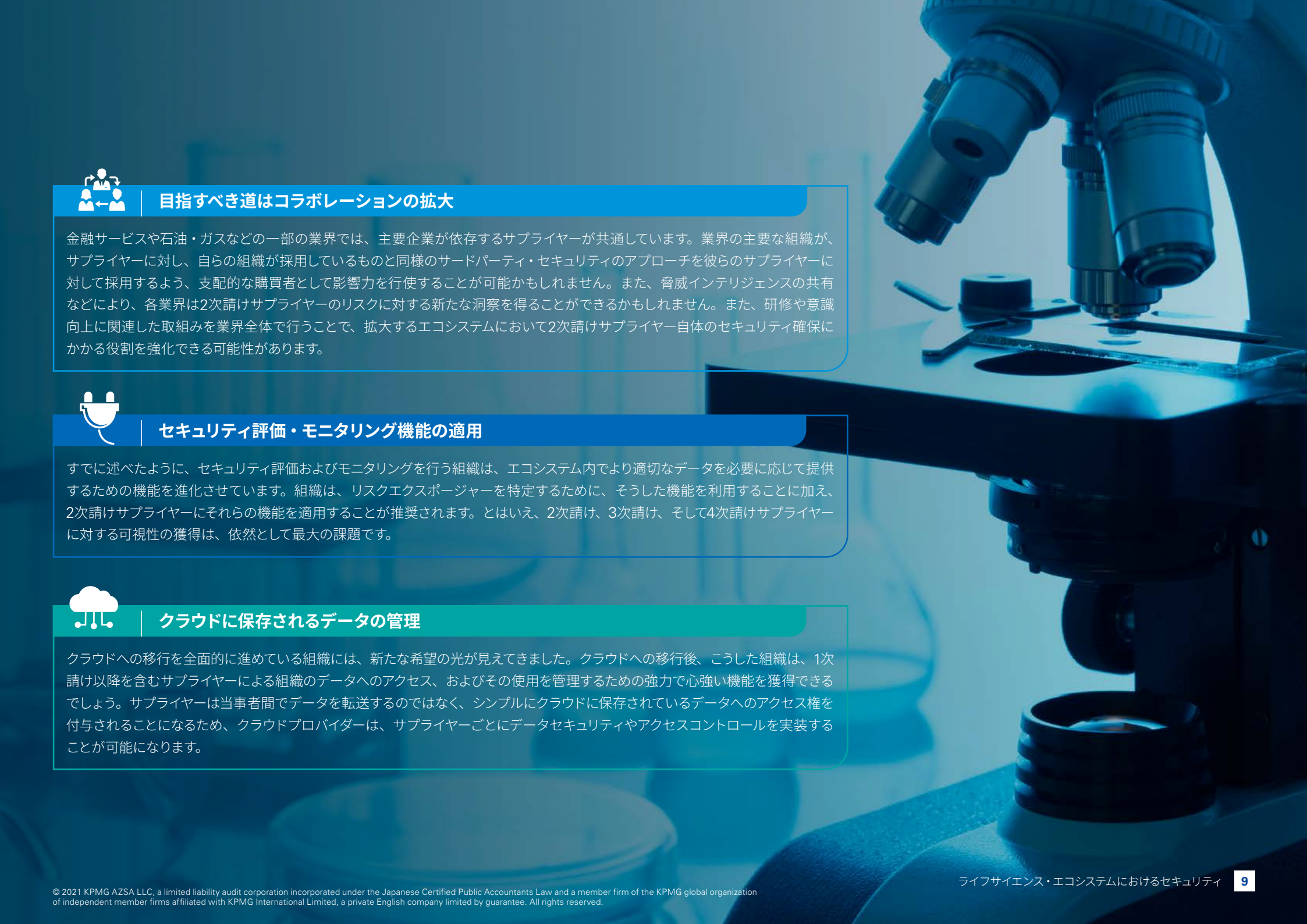
課題は監督官庁、可視性および実行可能性であり、課題のさらなる複雑化は、すべての業界のビジネスリーダーにとっての関心事となっています。さらに、クラウドベースのエコシステムにおいてサプライヤーの集中化が進んでいますが、そうしたサプライヤーに完全に依存していることで、サービス停止に陥った場合の影響について懸念が持ち上がっています。

現状では、ほとんどの業界は、拡大するサプライヤーの全体像を把握して課題に対する一貫した解決策を定めるには至っていません。この問題について規制当局と業界、あるいは、業界内で議論しているという事実自体が、効果的な新しいアプローチへの期待を抱かせます。答えはまだ出ていませんが、それには、以下のような業界全体でのイニシアティブを組み合わせたものが含まれると考えられます。

規制上の監視に関する新しい考え方

金融業界の規制当局は2次請けサプライヤーリスクについてレビューを行っていますが、主な課題は、2次請け以降のサプライヤーの多くが中小企業であることです。中小企業に規制を課すことは、それらの企業が現在顧客に求められているようなイノベーションを行うことの妨げとなる可能性があります。

しかし、この考え方について変化の兆候が表れています。欧州委員会は最近、ネットワークおよび情報セキュリティに関する指令の改正案（NIS2指令）において、デジタルインフラ（ドメインネットワークシステム、トップレベルドメイン、クラウドサービス、検索エンジン、ソーシャルメディア）に対して、サイバーセキュリティ要件およびインシデント報告要件への準拠を求める要求事項を含めることを提案しました。デジタルインフラのプロバイダーは、これまでサプライチェーン・セキュリティに対するアプローチの対象外であった2次請け以降のサプライヤーの大半を占めています。



目指すべき道はコラボレーションの拡大

金融サービスや石油・ガスなどの一部の業界では、主要企業が依存するサプライヤーが共通しています。業界の主要な組織が、サプライヤーに対し、自らの組織が採用しているものと同様のサードパーティ・セキュリティのアプローチを彼らのサプライヤーに対して採用するよう、支配的な購買者として影響力を行使することが可能かもしれません。また、脅威インテリジェンスの共有などにより、各業界は2次請けサプライヤーのリスクに対する新たな洞察を得ることができるかもしれません。また、研修や意識向上に関連した取組みを業界全体で行うことで、拡大するエコシステムにおいて2次請けサプライヤー自体のセキュリティ確保にかかる役割を強化できる可能性があります。

セキュリティ評価・モニタリング機能の適用

すでに述べたように、セキュリティ評価およびモニタリングを行う組織は、エコシステム内でより適切なデータを必要に応じて提供するための機能を進化させています。組織は、リスクエクスポージャーを特定するために、そうした機能を利用することに加え、2次請けサプライヤーにそれらの機能を適用することが推奨されます。とはいえ、2次請け、3次請け、そして4次請けサプライヤーに対する可視性の獲得は、依然として最大の課題です。

クラウドに保存されるデータの管理

クラウドへの移行を全面的に進めている組織には、新たな希望の光が見えてきました。クラウドへの移行後、こうした組織は、1次請け以降を含むサプライヤーによる組織のデータへのアクセス、およびその使用を管理するための強力で心強い機能を獲得できるでしょう。サプライヤーは当事者間でデータを転送するのではなく、シンプルにクラウドに保存されているデータへのアクセス権を付与されることになるため、クラウドプロバイダーは、サプライヤーごとにデータセキュリティやアクセスコントロールを実装することが可能になります。

より緊密なコラボレーションとつながりの構築

ニューノーマルのなかでイノベーションとコラボレーションを行うには、データおよびサプライヤーのエコシステムへの統合をより簡単に、大きな混乱を招くことなく行えることが必要です。現代の経済におけるイノベーションはデータドリブンであり、その中心にあるのがオープンアーキテクチャおよびオープンAPI（アプリケーション・プログラマブル・インターフェイス）です。APIは、組織を1次請けサプライヤーおよびより幅広いエコシステムに結び付ける架け橋の役割を果たしており、ビジネスの未来のために不可欠なものとなっています。

オープンバンキング

オープンバンキングの時代において、APIは銀行と顧客の間により強固でよりダイナミックなつながりを構築するのに役立っているほか、欧州ではいわゆるチャレンジャーバンクに市場を開放しました。市場競争の激化に伴い、APIは今や、イノベーションを迅速に実施して顧客の要求に応えるために非常に重要となっています。サプライヤーおよび他社とのコラボレーションによるイノベーションや、データ共有を奨励する目的でAPIを導入している銀行もあります。一部の銀行は、新しいオンラインバンキングのコンセプト、顧客データ、クレジットカード、支払い、口座などについてフィンテックを含むさまざまなステークホルダーとのコラボレーションを実現するため、APIマーケットプレイスを開発しました。

このような現状の疑問に対処し、API統合を行う際の主要なセキュリティ課題を特定するため、オープンソース・ソフトウェアコミュニティであるOpen Web Application Security Project（OWASP）は、APIセキュリティ・プロジェクトを公開しています。このプロジェクトは、セキュリティに対する責任を担うリーダーが潜在的なセキュリティ課題に対処する方法を理解する一助となっています。

オープンAPIのインフラが普及するにつれ、サプライチェーンの垂直統合が強力に推進され、エコシステムのセキュリティガバナンスに関して重要な考慮事項が生じることが考えられます。組織のデータ環境は今、2次請け、3次請けサプライヤーと外側に拡張していく可能性があります。そのため、以下のような問いを検討する必要があります。

01 組織は今後、サプライチェーン内を流れる顧客データの動きをどのように把握するか

02 将来のデータフロー図はどのようなものになるか

03 エアギャップの役割を果たすサードパーティAPIの層が顧客との間に介在する可能性があるなか、企業はどのようにして不正防止やマーケティングを目的とした顧客行動のモニタリングを行うか

データセキュリティとプライバシーについてより賢明な選択を

エコシステムによって消費者データが大幅に増大し、アクセスも容易となったことから、プライバシーに関する重大な課題が新たに発生しています。コロナ禍の発生を受けてプライバシー、セキュリティ、および倫理に関する規制上の監視が強化されるなかで、組織のデータ環境を把握することの重要性が注目を集めています。プライバシーの分野においてこの動きが最も顕著に見られるのは、データ主体の権利の領域です。

欧州連合の一般データ保護規則（GDPR）、米国カリフォルニア州の消費者プライバシー法（CCPA）、ブラジルの個人情報保護法（LGPD）など世界各地で新たな規制が導入されることで、消費者や従業員は、企業が収集または購入したデータに対し、より大きな可視性、透明性および管理を要求する法的権利を獲得しています。また、欧州司法裁判所による最近のシュレムスII判決は、EU・米国間の個人データの移転に大きな影響をもたらすことが考えられます。

プライバシー擁護派であろうとなかろうと、消費者は、利用する企業やサービスについてよりよい選択をすることが可能になりつつあります。企業の立場から、このような権利を適時かつ正確に充足させることは、特に大規模に行う場合、きわめて困難なことは明らかです。この困難さをもたらしている主な要因は、以下の2つです。

きわめて困難な性質

さまざまなサプライヤーやステークホルダーを擁する大規模かつ複雑なエコシステムの全体にわたって個人データを管理・保護するためのプログラムおよびシステムを積極的に構築・維持することは、非常に困難です。多くの業界において、個人データの可視性の向上やデータ主体の権利に関する要求の充足については、限られた進歩しか見られていません。しかし、プライバシーおよびデータ保護に関する規制が世界各地で次々と導入されている今こそ、困難に敢えて挑み、業界最高のデータ管理・保護プログラムを構築する理想的な時期かもしれません。

企業文化と方針

企業文化上の規範は、方針によって強制されているものもありますが、問題を悪化させただけでした。例えばデータ保持の慣行です。データストレージが安価となった今でさえ、多くの企業は依然として、ビジネス記録を永久的に保持することをビジネスの状況に関係なく従業員に推奨または要求しています。法的証拠開示に関する懸念はさておき、このアプローチによって生成されるデータ量では、データ主体の権利への対応がほぼ不可能なインベントリを作成することになります。

エコシステム全体におけるデータの流れ、データの利用への依拠について理解し、エコシステム全体で顧客のプライバシーを保護するための枠組みが不可欠になりつつあります。これには、参加者間のさまざまなレベルでの協力に加え、下流におけるより厳格な実施も必要となるでしょう。

規制当局が進歩を促す好機の到来

サードパーティリスク管理およびセキュリティに関する規制は急速に進展しており、新たな規制が地域および国のレベルで次々と施行されています。これには米国カリフォルニア州の消費者プライバシー法（CCPA）、欧州連合の一般データ保護規則（GDPR）、オーストラリアの健全性基準「CPS 234情報セキュリティ」などがありますが、これらはすべて、サードパーティリスク管理について指針を示し、明確化することを目的としています。

規制当局の役割の1つは、市場の課題に戦略的な視点を適用することです。コロナ禍により、組織、業界、および国家は、サイバー攻撃にさらされるなか、グローバルな市場エコシステムの相互接続性、テクノロジーへの依存、そしてレジリエンスについて根本的な前提を問い直すことを余儀なくされました。コロナ禍によって特に明らかになったのは、政府や規制当局が、業界のエコシステムにおける単一障害点を特定する方法や、壊滅的なサイバー攻撃に対する業界のレジリエンスを高める方法について、一歩下がって全体的な視野を持つことが必要であるということでした。

業界レベルでの取組みが成功への鍵

最も効果的なアプローチを知るには、重要な業界からのインプットが不可欠です。このような行動を促進するための主な施策として、政府に代わって大規模な介入を行うこと、すなわち、サイバー犯罪、不正行為および組織的犯罪の脅威となるグループを対象としたエコシステム全体にわたる防御モデルを推進する取組みに参画することが挙げられます。例えば、現在4年目を迎えている英国の国立サイバーセキュリティセンターによる進行中の防御プログラムでは、防御に関するさまざまなサービスを英国の公共部門にとどまらず提供しています。

サイバーに関するサードパーティ評価に関する規制が時代とともに進み、市場のエコシステム全体にとって生産的かつ有益であり、ひいては規制による保護の対象者からも支持されることを確実にするには、業界からのインプットが鍵となります。サイバーに関するサードパーティ評価に対する現在のアプローチは、ニューノーマルにもはや適合していません。この先10年間は規制当局にとって、レジリエンスと敏捷性という新奇な組合せをガバナンスに組み込み、真の効率性向上を推進する機会です。

エコシステムの進化に向けた協力

評価範囲をより適切に定め、より継続性のあるデータを提供し、サービスを適切に機能させるために不可欠な統制をモニタリングすることを可能にする方法を検討する必要があります。しかし、KPMGの報告書、「サードパーティリスク管理の展望2020」によると、要求される評価の実施に必要なデータすべてを自組織が持っていると考えている組織はわずか26%にとどまりました。また、回答者の37%が、サードパーティのデータを組織内で共有する際、互換性のないシステムなどの技術的障壁が主な障害となっていると述べています。

最新テクノロジーの役割

新しいサードパーティリスク評価モデルには、社内およびベンダーのシステムからデータを取り込み、それらを処理し、学習する最新のテクノロジーが必要です。エコシステムにおいてセキュリティの可視性、修復性、およびレジリエンスがオープンイノベーションのモデル自体のなかに組み込まれるようになるまでは、これらの課題の解決に向けて迅速に対応することは容易ではないでしょう。しかし幸いなことに、統制に対する継続的なモニタリング、脅威インテリジェンス、および機械学習におけるイノベーションにより、企業がこれらの課題に対処するための新たな扉が開かれています。

法令上の枠組みの改善

この新しいエコシステムに基づくサイバー環境では、法令上の枠組みを改善し、可視性の低下や責任の増大につながることの多い監督官庁の考慮事項を減らすことが必要になると考えられます。いくつかの国では政府により、サイバー導入のスピードおよび可視性を妨げている縦割り型組織の解体が開始されています。機械による読取り、共有性、そしてリスクベースのモデルを評価に組み込むことも、効果を上げつつあります。

組織はセキュリティ上の目的を達成するため、これらのモデルのいくつかを商業的に検証し、相互運用性、責任の軽減、および規制上のハードルを低くすることを支援するよりよいエコシステムの枠組みを実現する必要があります。

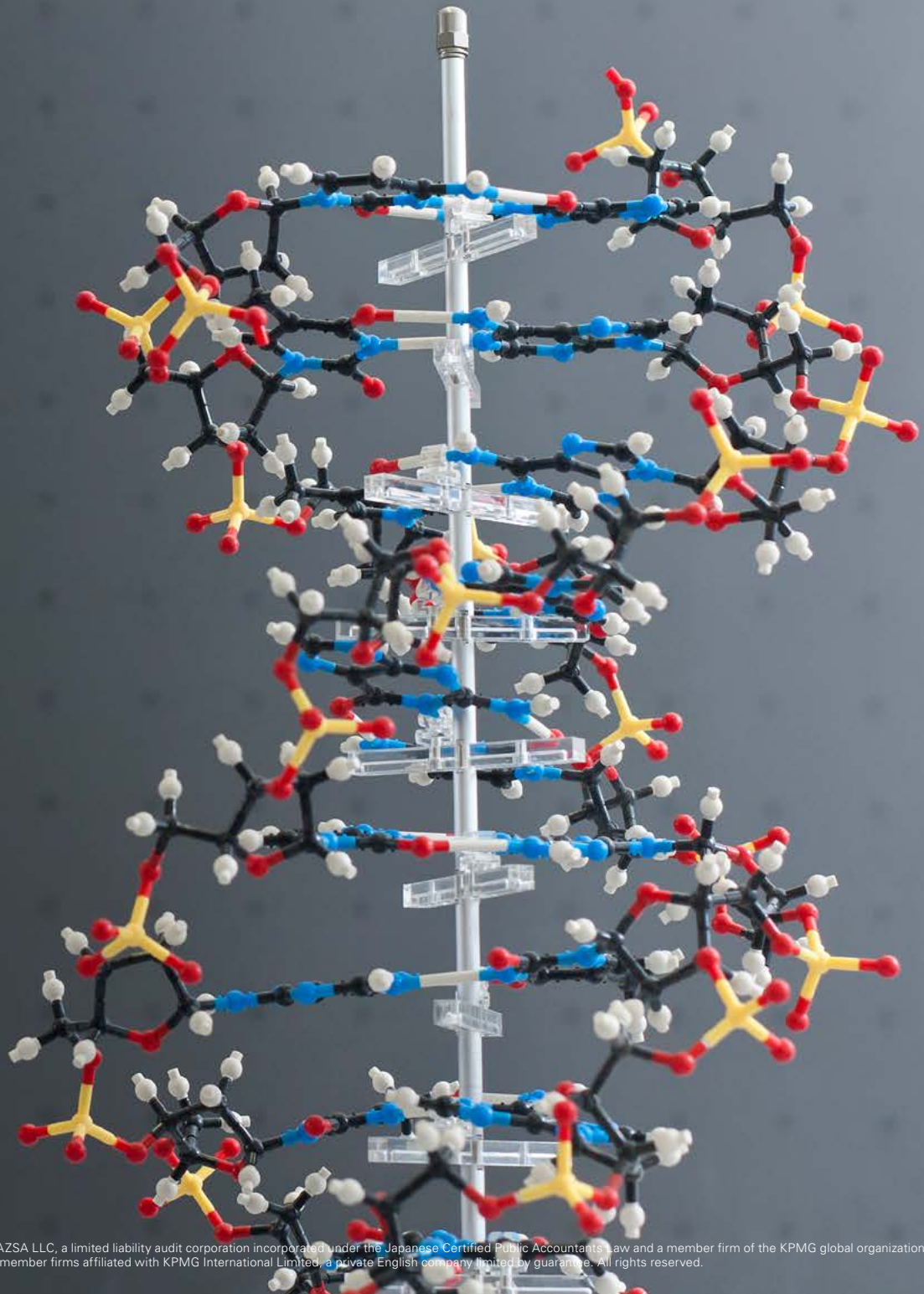
力を合わせ、リスク管理、規制、プライバシー、レジリエンス、およびテクノロジーの枠組みを構築することにより、エコシステムを継続的に進化させ、リスクを低減することができます。ニューノーマルにおいて、切望されるイノベーションおよび進歩をビジネスのスピードに合わせて進めることが可能となることが期待されます。

KPMGが提供可能な支援

KPMGでは、サイバーセキュリティの専門家で構成されるグローバルな組織が、リスクに関する分野横断的な知見を提供しています。私たちは、組織全体のセキュリティ確保を支援し、それにより、組織が明日を予測して迅速に行動し、セキュアで信頼できるテクノロジーをもって優位を獲得することを可能にします。

組織がサイバーセキュリティ・ジャーニーのどこに位置するかは問いません。KPMGは、取締役会からデータセンターまでを網羅する幅広い専門知識を有しています。サイバーセキュリティを評価して組織の優先事項への適合を図るだけでなく、高度なソリューションの開発と実装、リスクの継続的なモニタリング、サイバーインシデントへの効果的な対応を支援します。

KPMGは、深い技術的専門知識、ビジネスに関する強力な洞察力、そしてサードパーティとの関係におけるセキュリティ確保とサードパーティ・セキュリティ投資の価値の実現を支援するクリエイティブな専門家というほかにはない組合せを提供し、組織が確信を持ってビジネスを成長させることを可能にします。可能性の限界を超えることができるよう、信頼できるデジタルワールドをともに構築していきましょう。



Our authors

Jonathan Dambrot
Global Third Party Security Leader
KPMG in the US

Caroline Rivett
Global Cyber Security Life Sciences Leader
KPMG in the UK

Rangana Guha
Director, Cyber Security Services
KPMG in the US

Orson Lucas
Principal, Cyber Security Services
KPMG in the US

Jackie Hennessey
Director, Cyber Security Services
KPMG in Ireland

Sebastiaan Pronk
Manager, Cyber Security Services
KPMG in the UK

Pratiksha Doshi
Director, Cyber Security Services
KPMG in India

David Ferbrache
Global Head of Cyber Futures
KPMG

Contacts

栗原 純一
KPMGジャパン
ライフサイエンスセクター統轄パートナー
KPMGコンサルティング パートナー

宮原 潤
KPMGジャパン
ライフサイエンスセクター
KPMGコンサルティング ディレクター

KPMGジャパン
セクター統轄室
Sector-Japan@jp.kpmg.com

ライフサイエンスセクター
home.kpmg/jp/life-sciences

home.kpmg/jp/socialmedia

Designed by Evalueserve.
Publication name: Securing the life sciences ecosystem
Publication number: 137397-G
Publication date: September 2021