KPMG

サイバーセキュリティ主要課題2023

序文

新型コロナウイルス感染症（COVID-19）の拡大を背景に、デジタル化が急速に進み、それに伴い、さまざまな課題が顕在化しました。世界経済やサプライチェーンの混乱を経験し、企業はデジタルインフラへの依存を見直す必要性を認識し始めました。

人工知能（AI）、ブロックチェーン、生体認証、極度に接続された（ハイパーコネクテッドな）システム、バーチャルリアリティなど、画期的なテクノロジーが未来を形作っていくことが予想されています。これらのテクノロジーは、セキュリティ、プライバシー、倫理面で新たな課題を提起し、デジタルに依存した社会に対する信頼に根本的な疑問を投げかける可能性があります。ただ、このようなテクノロジーはグローバルな商取引に必要で、信頼を損なうなど手遅れになる前に、イノベーションを進める過程で問題に対処する必要があります。

システム上重要と考えられてきた業種にも変化が訪れています。従来、公益事業、電気通信、金融サービスなどに焦点が当てられてきましたが、現在では、官民パートナーシップ、企業間のエコシステム連携、情報インフラが複雑に絡み合っています。金融市場に目を向けると、金融機関、市場インフラ、データプロバイダー、マネージドサービスプロバイダーなどの重要な存在が、ハイパーコネクテッドな社会で極度に接続し合う状況になっています。相互接続と依存の度合いが高まるにつれ、これらのインフラを攻撃し、悪用しようとする人の関心も惹いてしまうわけです。

このような変化に伴い、サイバーセキュリティに関する規制の強化が世界的に進められ、規制にかかわる負担が増大し、さまざまな報告要件が多様化することへの懸念が、組織の間で高まっています。企業は、脅威の変化や国境を越えた規制要件に対応する必要性から、プライバシー保護とセキュリティを事業運営に組み込むことに一段と重点を置くようになりました。

サイバーセキュリティは、すべてのビジネスライン、機能、製品、およびサービスにおいて不可欠であるべきです。組織は、サイバーセキュリティがデジタル企業全体に浸透し、戦略、開発、運営に全面的に織り込まれることを目指さなければなりません。

KPMGインターナショナルのChief Global Digital OfficerであるLisa Heneghanは、次のように語っています。

「企業はサイバーセキュリティについて、組織全体を貫く『金の糸』、つまり扇の要のような存在として考える必要があります。サイバーセキュリティをビジネスの中枢に据え、デジタルトラスト（デジタル技術の活用への信頼）を構築するための基盤として利用するべきです。最高情報セキュリティ責任者（CISO）とそのチームは、単独で行動するのではなく、組織全体の責任で実行していかなければなりませんが、それは簡単なことではありません。まず、サイバーセキュリティが自身とどのように関係しているかを理解する必要があり、次に、セキュリティを既存の業務プロセスにどのように統合するかを考えなければなりません。あらゆる業務プロセスの変遷を考慮したセキュリティ管理を設計することで、責任ある安全な行動を促すことができます。それは、ビジネスに多大な利益をもたらすことにつながるでしょう。」

CISOは、「デジタルディスラプション」に対する企業のレジリエンスをめぐる幅広い対話の活性化と形成に大きな役割を果たすと思われます。こういった貢献は、企業が保護すべき資産とデジタルサービスの進化する性質をよりよく理解することを促進し、信頼基盤の構築を推進するでしょう。

本レポートでは、デジタルトラストが競争優位になり得ることを取締役会や上級管理職に示すため、広範なビジネス関係者、特にCISOが今後1年間にとるべき行動について考察しています。

具体的な人材、プロセス、データ／技術、規制に関する推奨事項については、22ページを参照してください。

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

*本レポートはKPMGインターナショナルが2023年2月に発行した「Cybersecurity considerations 2023」を翻訳したものです。

サイバーセキュリティ主要課題2023：8つのポイント

01

デジタルトラスト：責任の共有

組織は、従業員、顧客、サプライヤー、パートナーの利益を守ることを十分に検討しているか？

02

「縁の下の力持ち」のセキュリティが安全な行動を促す

セキュリティチームは、セキュリティをどのようにビジネスプロセス、アジャイル開発プログラム、異なるオペレーティングモデルと効果的に統合するか？

03

データ中心の未来を守る

セキュリティの境界がなくなってしまった今、組織はエコシステムのあらゆる側面を保護するゼロトラストアプローチに、どのように現実的かつ実用的に移行することができるか？

04

新しいパートナーシップとモデル

アウトソーシングやマネージドサービスが急激に成長する環境において、組織はどのようにセキュリティ、プライバシー、レジリエンスを重視していくか？

05

自動化への信頼

ロボティックプロセスオートメーション（RPA）、機械学習（ML）、その他のAIを、効果的に、賢明かつ安全に導入・管理するために、組織は何をすればよいか？

06

スマートな世界を守る

企業がスマートでハイパーコネクテッドな製品重視の考え方にシフトしていくなかで、セキュリティとプライバシーのチームにはどのような影響があるか？

07

俊敏な敵に対抗する

変化し続ける脅威や、攻撃者の高度な戦術に、セキュリティチームはどのように対応すればよいか？

08

必要に応じたレジリエンス

復旧対応だけではなく、復旧のための積極的な計画がなぜ必要か？

主要課題1

デジタルトラスト：責任の共有

プライバシー、セキュリティ、倫理に関する議論が活発化するにつれ、規制や世論に後押しされる形で、取締役会の議題としてデジタルトラストが取り上げられるようになりました。デジタルトラストは、デジタル技術を駆使したビジネスを将来の成功へと導き、サイバーセキュリティとプライバシーは、デジタルトラストを構築するための重要な基盤です。CISOは、取締役会と経営幹部がステークホルダーの信頼を構築・維持し、競争優位性を確立することを支援できるよう準備しておく必要があります。これらの実現には、すべてのステークホルダーが一丸となって取り組まなければなりません。

グローバル化は、世界をボーダレスにし、相互に結びつけています。このことは、パンデミックによって引き起こされたグローバルサプライチェーンの混乱によって、明確に証明されました。B2B、B2Cを問わず、顧客と永続的な関係を築くためには、組織はデジタルトラストを確立し、維持する必要があります。

デジタルトラストは、組織のあらゆる側面にかかわる幅広い分野を網羅しており、本質的に企業戦略と結びついています。これは、デジタルトラストが競争優位性を生み出すことができるからだけでなく、幅広い産業と社会にとって、デジタルトラスト自体が単に正しいものであるからです。

John Anyanwu
Partner, Cyber Security Services
KPMGナイジェリア

価値と信頼

信頼は成功のカギであり、それは単なる評判の問題ではありません。信頼を高めることで、競争優位性が生まれ、収益に貢献することができるのです。

3分の1以上の組織が、「信頼の向上が収益性の向上につながる」と回答しています。

65%の回答者が、一方で「情報セキュリティは、長期的な戦略というより、コンプライアンス面での必要性による」と回答しています。

65%の回答者が、「情報セキュリティはビジネスを実現するものというより、むしろリスク低減のための活動として捉えられている」と回答しています。

49%の回答者が、「取締役会は、情報セキュリティについて競争優位性を得るための手段ではなく、必要なコストとみなしている」と回答しています。

出典：KPMGサイバートラストインサイト2022

*本レポートにおける各種調査レポートからの引用データについては、素データからの引用もあるため、元のレポートに掲載されていない場合があります。

企業は関心を持ち始めている

デジタルトラストのメリットを認識するシニアリーダーの数は増加しており、37%の回答者が信頼性の向上による最たる商業的メリットとして収益性の向上を挙げています[1]。

デジタルトラストは幅広い分野を網羅しています。サイバーセキュリティは信頼性、安全性、プライバシー、透明性といった課題と密接に関連し、広範囲にわたって主要な役割を担っています。これらの課題は、提供する製品やサービス、使用する技術、データの収集と利用の仕方、顧客、従業員、サプライヤー、その他すべての第三者（サードパーティ）パートナーやステークホルダーの利益といった、企業のビジネスの進め方や価値の追求に影響を及ぼします。

一方65%の回答者は、「情報セキュリティはビジネスを実現するものというより、むしろリスク低減のための活動として捉えられている」と回答しています[2]。

多くの組織が依然としてサイバーセキュリティを主にコストとして捉え、将来への投資とは必ずしも考えていませんが、これは間違っていると言わざるを得ません。CISOは、デジタルトラストの概念を受け入れ、セキュリティがビジネスの推進役として、組織のデジタル成長目標をいかに安全にサポートするかを示す必要があります。

CISOは、組織がデジタルトラストを構築するうえで重要な役割を担っていますが、単独でそれを行うことはできません。CISOは、他の重要な社内外のステークホルダーに対して、デジタルトラストの潮流におけるそれぞれの役割を認識させるために十分な時間を費やす必要があります。CISOは経営幹部や取締役会に対して、デジタルトラストの重要性と、デジタル技術の信頼性を高めるためのビジネス戦略について説明しなければなりません。

消費者にとってのデジタルトラストとは

一般的な消費者は、企業のデータ保護プログラムの詳細には関心を示さないかもしれませんが、情報漏えいを知った瞬間、どのような措置が取られるか、誠意ある対応をしてくれるかを知りたがるものです。組織はインシデントに対し、迅速に、かつ透明性を重視しながら対応することで、信頼を再構築することができます。

現代の消費者は、情報漏えいが起こり得ることを理解しています。企業が納得のいく価格帯で確かな製品とサービスを提供し、情報漏えいが起きたとしても、サイバーインシデントへの対応と復旧に関する詳細な説明があり、安心感を得られるのであれば、大半の顧客は少しずつ戻ってくるでしょう。

“透明性は、対象者によって異なる意味を持ちます。消費者は、インシデントが発生した時に透明性を求めるため、組織は、一緒に仕事をするサプライヤーやパートナーがどのように情報を保護しているかを事前に知っておく必要があります。なぜなら、組織は顧客に対してより重い義務を負っており、情報保護の面で信頼を提供できることを確認しておく必要があるからです。”

Henry Shek
Partner, Cyber Security Services
KPMG中国

1 KPMGサイバートラストインサイト2022
2 同上

効果的なデジタルトラスト戦略

デジタルトラストの概念を企業戦略、製品開発、企業全体の市場プレゼンス、法人・小売顧客との関係に組み込むことが極めて重要です。さまざまなステークホルダーに関係するデジタルトラストの意味について広く考えることは、サイバーセキュリティやデジタルトラストの確立と維持に貢献するその他の分野の重要性を強調し、分野横断的な全体的アプローチを奨励するのに役立ちます。

CISOは、取締役会および経営幹部に対し、サイバーセキュリティがデジタルトラストに不可欠な構成要素である理由を明確に説明し続ける必要があります。

簡単に言えば、自社の製品やサービス、事業の運営や保護方法について、すべてのステークホルダーの信頼を確立できている企業は、商業的にも企業イメージ的にもプラスの影響を受ける可能性が高い、ということです。

Annemarie Zielstra
Partner, Cyber Security Services
KPMGオランダ

CISOは、信頼できるパートナーやサプライヤーを選定するための支援をすべきです。そのためには、情報保護に関する透明性や、適切な復旧・対応能力を証明するための適格な基準を設けることが不可欠です。

デジタルトラストを構成する要素に関して、規制に関連する義務が増大することは間違いなく、規制当局が企業に求める透明性と説明責任のレベルを上げることが予想されます。多様化し、複雑化する規制の状況に対応するための、原則に基づいた全体的なアプローチをとることは組織に利益をもたらし、コンプライアンス主導のサイロ化したアプローチよりも、コストを低減することができます。

組織のリーダーがこうした説明を受け入れ実践すれば、組織の他のメンバーも同じように実践するはずです。つまり、企業の年次報告書で、この潮流について具体的に紹介し、デジタルトラストに関する企業哲学と戦略を詳細に説明することが必要です。KPMGサイバートラストインサイト2022によると、34%の回答者が、サイバーセキュリティとプライバシー保護の透明性向上に関する報告要件を満たすことができるかを懸念していますが、KPMGの専門家は、企業自ら積極的に取り組むことを提唱しています[3]。

Learn more

KPMGサイバートラストインサイト2022
サイバーセキュリティとプライバシー保護による信頼の構築

デジタルトラストに向けた協業
信頼がかつてなく重要な理由とは

デジタルの信頼不足の解消
テクノロジーの進化に伴い重要性が増す「デジタルトラスト」について、取組みや課題を考察

3　KPMGサイバートラストインサイト2022

主要課題2

「縁の下の力持ち」のセキュリティが安全な行動を促す

従業員が自信を持って仕事をし、生産的な選択を下し、組織を守る役割を果たすような形でセキュリティをビジネスに組み込むことはCISOの重要な目標ですが、捉えどころがないのも事実です。

人とビジネス両方の視点でセキュリティを考慮することによって、CISOのマインドセットを変えることができるでしょう。

重要なポイントは、いつどこでセキュリティが最も重要になるか、どこにセキュリティ対策を追加すればビジネスにプラスの影響を与えるかについて気を配ることでしょう。絶対的なセキュリティは存在しません。CISOが常にすべてを守ろうとしても、侵入を防御するためのセキュリティ対策を回避する方法をみつけられると、何も守れなくなる危険性があります。CISOは、特定のビジネスプロセスの重要性と関連するリスクプロファイルに見合った、正当なセキュリティの管理領域について現実的に考慮する必要があります。

結局のところ、強制ではなく自発的なセキュリティコントロールは、従業員にとってプラスであり、従業員こそが最大のファイアウォールとなるのです。

Julia Spain
Partner, Cyber Security Services
KPMG英国

CISOへの信頼

CISOが重要な任務を遂行する能力について、組織は大きな信頼と強い確信を抱いています。

約80%の回答者が、「CISOは企業内の重要なデータの所在を正確に認識できる」と確信しています。

4分の3の回答者が、「CISOは自社の最重要データを特定できる」と確信しています。

78%の回答者が、「CISOは自社の機密データがどの程度サードパーティにあり、適切に保護されているかを知っている」と確信しています。

出典：KPMGサイバートラストインサイト2022

企業は、セキュリティを二項対立で考えることから脱却する必要があります。今日の環境では、セキュリティは常に変化しており、「安全」または「安全ではない」という概念は一過性のものにすぎません。その代わりに、CISOは従業員と経営幹部への知識の提供と、従業員が使うことを前提にしたシンプルで直感的にわかりやすいセキュリティプロセスの設計、および従業員のセキュリティに対する意識向上を通じて、組織的なIQを高めていくよう働きかける必要があります。

顧客体験は、セキュリティにも適用される

悪意ある行為を検知し、迅速に対処する手段を持ちつつ、責任ある従業員のための現実的なプロセスの構築に注力することが極めて重要です。つまり、サイバーセキュリティを単なる規制上の必須事項として考えるのではなく、幅広いビジネスニーズを踏まえた企業全体の優先事項に沿ったサイバーセキュリティの計画と顧客体験、使いやすさを考慮することが重要です。

テクノロジーの進歩は、その助けとなります。防御的なAI、機械学習（ML）、チャットボットから、クラウド暗号化、ブロックチェーン、拡張検知・対応アプリケーションまで、すべてが重要な要素です。また、一貫したITガバナンスのもと、デジタルコミュニケーションに適切な注意を払うような、よりセキュリティ意識の高い従業員を育成することも重要です。CISOは、従業員が直感的に正しく行動できるようにするにはどうすればよいかを考え、それを支援するセキュリティ管理を設計する必要があります。

テクノロジーだけでは問題を解決できません。サイバーセキュリティには莫大な資金が投下され、何千ものサイバーセキュリティ企業が対応ツールを提供していますが、企業はいまだに脆弱なままです。なぜでしょうか？　それは、悪質な攻撃者が同じツールにアクセスしているからです。

Prasad Jayaraman
Principal, Cyber Security Services
KPMG米国

サイバーセキュリティは、常に進化し続ける取組みのため、新しいツールや制御の機能を後から搭載・交換できる機会は多くありますが、組織が人的要素を考慮し、最初からそれらを組み込んでおくことを推奨します。主要な変革の取組みには多くの要素がありますが、そのうちの1つはセキュリティであるべきです。DevSecOps、運用技術、調達など、幅広いプロセス中心の戦略にセキュリティを組み込むことは、従業員に安全な行動をとるよう促し、人的ファイアウォールとして機能させる、有効かつ自発的な方法となり得ます。

CISOは、技術だけでなく、人的な側面にも目を向けなければなりません。教育やトレーニングから基本的な認識に至るまで、組織全体で強固なセキュリティ文化を構築することが重要です。

Eddie Toh
Partner, Cyber Security Services
KPMGシンガポール

セキュリティチームは、組織が顧客体験を向上させる方法から多くを学ぶことができます。内部セキュリティ管理は、使いやすいものでなければ、従業員がこれらのプロセスを回避する可能性があります。顧客体験の専門家をセキュリティ管理の設計に加えることを検討してください。

内部ユーザーは、セキュリティプロセスを自分事として捉えるべきです。各個人に判断を求め、背景を説明させ、私生活とキャリアにおける慎重で安全な行動の価値について類似点を引き出すことで、“楽しみながら学んでもらう（edutaining）”のです。そうすれば、セキュリティに関する文脈で自分の役割を果たすことができ、セキュリティの最も弱い部分（weakest link）としてみなされることもないでしょう。

Learn more

人的ファイアウォール
ヒューマンリスクの克服

Synthetic identity fraud
A $6 billion problem.

Want better cybersecurity? Don't check that box
The greatest threat to your organization's security might not be ransomware or phishing attacks — it might be your tendency to do this.

主要課題3

データ中心の未来を守る

この10年でビジネスの運用モデルが根本的に変化しました。より流動的で、データが重視され、社内外のパートナーやサービスプロバイダーとつながるエコシステムになったことは、驚くべきことではありません。

このような分散コンピューティングの世界において、CISOとセキュリティチームは、潜在的な機能停止や侵害の影響を軽減するために、ゼロトラスト、SASE（Secure Access Service Edge）、サイバーセキュリティメッシュモデルなどのさまざまなアプローチを採用する必要があります。

今や、従業員、顧客、サプライヤー、その他のサードパーティを、シームレスにリモートで安全につながるようにすることが、ビジネス上の明確な必要条件になっています。それに伴うセキュリティ上の課題は、境界のない環境において、組織がもはやすべてのユーザーとデバイスを信頼することができなくなっていることです。

境界のないビジネスのためのゼロトラスト

ゼロトラストアプローチは、機能停止や侵害が発生した際の影響を縮小し限定することで、インシデントをより適切に管理・抑制するのに役立ちます。

相互接続されたデジタルの世界では、従来の境界型セキュリティのアプローチは時代遅れになっています。CISOは、公共および民間のインフラと分散したユーザーエコシステムにまたがる、より広範な攻撃対象領域を保護しなければなりません。つまりCISOは、どこからでも、どのデバイスでも、信頼できる方法でセキュリティを提供することで、ビジネスの継続を可能にするよう努める必要があります。

Natasha Passley
Partner, Cyber Security Services
KPMGオーストラリア

データセキュリティはステークホルダーの重要な課題

境界のない環境では、データの保護、使用、共有の方法に関する懸念が、組織のデータ使用・管理能力に対するステークホルダーの信頼を損なう主な要因となります。

28%の回答者が、組織のデータ使用・管理能力に対するステークホルダーの信頼を損なう主な要因として、「ガバナンスの仕組みに対する信頼感の欠如」を挙げています。

32%の回答者が、「特定のサービスにデータが必要な理由や、データを共有・提供することの利点が明確でないこと」を主な要因として挙げています。

36%の回答者が、「データ保護方法に関する懸念」を主な要因として挙げています。

35%の回答者が、「データの使用・共有方法に関する懸念」を主な要因として挙げています。

出典：KPMGサイバートラストインサイト2022

ゼロトラストを基盤とするSASEとサイバーセキュリティメッシュモデルには、「セキュリティ全体をどのように組織化し、分散させ、ネットワーク上で整合させるか」という点で共通の原則があります。ただ、おそらく最も重要なのは、クラウド中心の考え方を採用する組織が増えるなか、セキュリティメカニズムをデータに近づけることが不可欠となっていることです。

境界のない現代のビジネス環境を包括するものとして、ゼロトラストはフレームワークであり、セキュリティとIDアクセスの設計と有効化を、時間をかけてどのように変える必要があるかについて考える手段です。ゼロトラストは、SASEモデルと総合的かつ分析的なサイバーセキュリティメッシュアーキテクチャのもとでサービスの収束を助けます。

ID（アイデンティティ）の新しいモデル

分散型のID・アクセス管理は、CISOの中核的な責任であり、ネットワークトラフィックの機能です。南北（ユーザーからリソースへ）のトラフィック概念は、すべてIDに関するものですが、東西（環境内での横移動）のトラフィック概念は、セグメンテーションなどの制御に関するものです。

データとIDの関連性は疑う余地もありません。境界のない環境では、IDとデータガバナンスに明確に焦点を当てることなしに、ゼロトラスト、SASE、サイバーセキュリティメッシュは存在しないのです。

CISOにとってゼロトラストの課題は、デバイスとユーザーの認証とその信頼性です。この課題を解決するには、CISOがID検証の観点からセキュリティについて考える必要があり、組織内のユーザーや、ユーザーがやり取りする多くのサードパーティの最小権限アクセスに焦点を当てる必要があります。

ゼロトラストを実践する

ゼロトラストは、すべてのシナリオ、すべてのユーザー、およびすべてのエンドポイントに関連して定義されるべきであり、組織の基礎的なセキュリティプログラムと基本原則の重要な柱を表します。CISOは、ゼロトラストモデルとメッセージを体系化するだけでなく、ポリシーの制定、基準の設定、ソフトウェアソリューションの設計、さまざまなテクノロジーリーダーやビジネスリーダーを含む組織全体のセキュリティ協議会の結成においても重要な役割を果たす必要があります。

もう1つの課題は、資金調達と予算編成です。取締役会や他の組織のリーダーが、ゼロトラストへの投資は単なる新しい技術の1つではなく、安全で境界のない未来を支えるための新しい考え方であることを理解できるよう、CISOはゼロトラストの枠組みを説明できなければなりません。

オンプレミスとオフプレミスの中間点を探ることは、特にクラウドネイティブ技術では困難です。多くの組織が複数のプロセスをクラウドに移行しようと考えていますが、大抵の場合、高度な技術が必須要件となり、レガシーインフラストラクチャをSASE仕様に完全に適合させることができません。

大規模で複雑な組織におけるCISOは、オンプレミスとオフプレミスのエコシステムにまたがるセキュリティ体制を管理するという課題を抱えており、このようなデュアル環境で運用していると、短期的に運用コストが高くなる可能性があります。クラウドの全面的な導入を試みる企業は、クラウドに導入するシステムについても、オンプレミスのゼロトラスト原則と同じように検討することが求められます。また、運用モデルの変更の影響も考慮する必要があります。たとえば、クラウド提供者との適切に管理された責任共有モデルは、安全なクラウドアーキテクチャを確保するうえでカギとなり得ます。

> **現在のギグエコノミーの世界では、IDエコシステムが急速に拡大しています。そのため、組織はIDという共通項を通じてのみ、人と機械を正確に監視することができます。**

Deepak Mathur
Principal,Cyber Security Services
KPMG米国

Learn more

The convergent future of identity

What's next for identity access management.

何も仮定しない、すべてを検証する

なぜゼロトラストが進むべき道なのか

Safeguard your digital environments from all angles

Five steps to beginning the zero trust journey.

主要課題4

新しいパートナーシップとモデル

セキュリティチームが組織のITシステムのセキュリティにのみ焦点を当てていた時代は終わりました。CISOは、いつブレーキを踏むべきか、いつサイバーセキュリティ対策のアウトソーシングを進めるべきか、現在および将来にわたって、どのようなスキルを社内に残すべきかを判断する必要があります。セキュリティは一段とビジネスの優先事項となり、組織とサービスプロバイダーの間で責任を共有するモデルを通じて実現されるようになりました。

現在のCISOは、運用技術や製品セキュリティから複雑なサプライチェーンのエコシステムに至るまで、組織全体のビジネス戦略をサポートしています。サプライチェーンやカスタマーサービスから、組織設計や情報セキュリティにわたって、さまざまな連携先とのコラボレーションによってイノベーションが向上することを認識する組織は一段と増えています。

組織が競争優位に立つためには、顧客がどこにいても、納得のいく価格帯で提供されるイノベーションの組み合わせが必要なのです。

一方、人材やスキルの不足から、堅固なセキュリティを大規模に実装することに苦労している組織もあり、そういった組織では、アウトソーシングやマネージドサービス、クラウドへの意向を検討しています。

多くの組織が特定のビジネスプロセスをサードパーティベンダーにアウトソーシングしていますが、データセキュリティとID・アクセス管理、またそれらに関連する管理は、引き続き社内の責任です。

Markus Limbach
Partner, Cyber Security Services
KPMGドイツ

信頼できるコミュニティ

極度に接続された（ハイパーコネクテッド）なエコシステムで成功するためには、外部とのパートナーシップが不可欠ですが、現実的な壁が立ちはだかり、コラボレーションを阻んでいます。

79%の回答者が、「サプライヤーや顧客企業との建設的なコラボレーションが不可欠」と回答しているにもかかわらず、
それを実践していると回答したのは
49%にすぎません。

60%の回答者が、「サプライチェーンの脆弱性によって攻撃される可能性がある」と認めています。

78%の回答者が、「CISOはサプライチェーン全体でデータを保護できている」と確信しています。

出典：KPMGサイバートラストインサイト2022

何を社内に保持すべきかを知る

セキュリティを完全にはアウトソースできないため、適切な人材とスキルが社内にも必要です。内部スタッフとサードパーティが効率的に運用できるよう、再現可能な管理と測定のフレームワークを設定するには、専門知識が不可欠となります。重要なポイントは、セキュリティの観点から何を社内に保持すべきかを理解し、その分野の人材にとって最も効果的な調達戦略を特定することです。

クラウドを例にとると、CISOは複数のペルソナ（ブローカー、オーケストレーター、インテグレーター）を具現化し、必要なスタッフとサードパーティのスキルを調整し、リスク、ガバナンス、レポート作成を戦略的に管理する必要があります。組織はすべてをアウトソーシングすることはできません。準備と計画はアウトソーシングできるかもしれませんが、理想的には、ビジネス環境とセキュリティ環境、およびサイバーインシデントの潜在的かつ広範な影響について理解している社内の誰かが、組織的な役割分担と品質管理を行う必要があります。

クラウドエコシステムにおけるサイバー制御の設計は、従来のセキュリティエンジニアリングのスキルとは異なるスキルセットです。組織全体、アプリケーションプログラミングインターフェース（API）、およびさまざまなテクノロジーをビジネス同様のスピードで管理するには、多くの組織に欠けている高度な能力が必要です。これは特にCISOに求められています。

Matt O'Keefe
Partner, Cyber Security Services
KPMGオーストラリア

適切なスキルの組み合わせをみつける

CISOが社内外の責任を理解し、さまざまなモデルや分野の間のグレーゾーンを舵取りし、それらの複雑さを適切に管理することは非常に重要ですが、簡単なことではありません。

外部のセキュリティプロバイダーと連携するには、技術的なスキルではなく、管理およびガバナンスに重点を置いた独自のスキルセットが必要です。アウトソーシングされる作業の量にかかわらず、組織は社内のセキュリティに関する確かな知識と能力を保持する必要があります。実施された制御とKPI（重要業績評価指標）の報告が適切に管理されていることを保証するために、当事者間の対話が明確かつ定期的になされることも不可欠です。システムテストの際は、明確なインシデント対応プロセスに同意し、関連するシミュレーションを実行することが重要です。

CISOは、自社のスキルベースを定期的に評価し、賢明で協力的なクラウド／マネージドセキュリティサービスである、と理解してもらう必要があります。そのためには、将来のビジネスにおいて必要となる基盤構造について理解し、最適なサポートを提供するためのセキュリティ機能を決定しなければなりません。キーワードは「未来」にあり、組織の今のセキュリティニーズのみに目を向けるのではなく、3～5年先を見据えましょう。

Learn more

サードパーティリスク管理の展望2022

KPMGが実施した、組織のTPRMに関する調査の結果

Evolving vendor, operational and strategic risks

Third party risk management.

Third party and cloud: Regulatory challenges

Companies are forming more frequent and complex relationships with third parties, introducing new or elevated risks.

主要課題5

自動化への信頼

技術革新と新技術の活用をめぐる競争のなか、セキュリティ、プライバシー、データ保護、倫理に対して高まる懸念は、注目を集めながらも、しばしば無視されたり、忘れられたりしています。このような怠慢を放置しておくと、特に新しいAI利用におけるプライバシー規制が目前に迫っている今、組織の可能性を妨害することにつながりかねません。

歴史的にみると、AIはデータサイエンスの実験の積み重ねであり、製品化されるプロジェクトの割合は比較的少ないものでした。今、応用的な現実世界の機械学習（ML）の時代が幕を開け、今後は、より多くのプロジェクトが稼働すると期待できます。数々の試行錯誤がありましたが、そこからの学びは最終的にレコメンデーション機能、意思決定支援ツール、高度なシミュレーション、ニューラルネットワークという形で大きな成功につながり、多くの組織で何億ドルもの価値を引き出すことができるかもしれません。

日常的で反復的な作業を自動化することで、従業員は複雑かつ注意が必要で、繊細な思考が求められる戦略に集中できるようになり、時間の節約と効率化が実現します。そのため、AIは多くの産業で活用されています。銀行関連では、ボットが顧客にとって最適な商品やサービスの決定を支援し、保険会社では、申込者の信用度を自動で評価するための利用が検討されています。

企業が機械学習（ML）の利用についてどのように考えているかを知ることは、セキュリティチームにとって非常に重要です。この理解があれば、セキュリティチームは使用するシステムを検討し、適切な入力データを特定して、AIシステムを使用する際の敵対的リスクに対処することができます。

Michael Gomez
Principal, Cyber Security Services
KPMG米国

AI/MLの課題

ビッグデータ解析のためのAI/MLソリューションの導入に関する倫理、セキュリティ、プライバシーへの影響について、社会全体およびビジネス上の懸念が高まっています。

78%の回答者が、「AI/MLの導入は、サイバーセキュリティの課題をもたらす」と回答しています。

4人に3人の回答者が、「AI/MLの導入は、基本的な倫理の課題をもたらす」と回答しています。

76%の回答者が、「AI/MLを導入した場合、AI/MLシステムのトレーニング方法とその性能の監視に関する追加のセーフガードを導入する必要がある」と回答しています。

76%の回答者が、「AI/MLの導入には、その技術をどのように利用しているか、より透明性のある伝え方が必要」と回答しています。

出典：KPMGサイバートラストインサイト2022

信頼と信用を築くAIモデル

組織はAIを適切に活用し、最も生産性の高いアウトプットを得ているのでしょうか。保険会社のユースケースでは、申込者のうち特定の地域に住んでいる人をアルゴリズムで判断している場合があります。裕福でない地域に住んでいる人と、上流階級の地域に住んでいる人とでは、評価が異なります。その結果、申込者の住所によって保険料に差が生じることになるのです。AIの偏見は差別とみなすことができ、抑制する必要があります。

従来、アプリケーションは平等に動作するように開発、およびテストされており、インプット、アウトプットの関係が変わることは想定されていませんでした。エンドユーザーは、アプリケーションの使い勝手がよいかどうか、開発元との取引を継続したいかどうかを判断しました。

MLやAIのツールは、学習し、進化するように設計されています。そしてその進化は、組織がこれらのシステムについてどう考えるべきか、どのように訓練されてきたのか、どのような目的に適合してきたのかといった、大規模な変革を示しています。

人々はAIに対して複雑な感情を抱いており、多くの組織には、AIを理解する専門家がいないだけでなく、セキュリティを確保する方法もありません。

DevOps志向の組織は、開発ライフサイクルを短縮し、継続的デリバリーを保証する役割を担い始めています。そして、組織が機械駆動の環境にセキュリティを導入しなければ、人々がその環境を信用できなくなるかもしれません。KPMGサイバートラストインサイト2022によると、76%の回答者が、「AI/MLを導入した場合、AI/MLシステムのトレーニング方法とその性能の監視に関する追加のセーフガードを導入する必要がある」と考えています[4]。

AIは強力ですが、もし不注意に偏見や差別的な自動意思決定がなされれば、個人を傷つける可能性があります。

Sylvia Klasovec Kingsmill
Partner, Privacy
KPMGカナダ

AIとデータプライバシー

AIについては、セキュリティチームが顧客データをより詳細に分析できるようにするなど、プライバシーに関する多くの基本原則を強化していますが、組織は特定の規制におけるデータ最小化要件と比較して、収集するデータ量のバランスを考慮する必要があります。同様に、AIが既存の偏見を組み込む可能性があることを考えると、アウトプットには透明性がなければなりません。

規制当局、政府、産業界は協力すべきです。AI規制は単なるプライバシーの問題ではありません。データサイエンティストはプライバシーの専門家と協力して、（AIを）安全で信頼性が高くプライバシーに配慮したテクノロジーとするために、どのような要件を組み込むべきかを判断する必要があります。そして、政府は業界を鼓舞し、イノベーションに予算を割くよう促すために、包括的なデジタルアジェンダを設定する必要があります。

さまざまな国の政府機関がAIを競争の手段として活用する一方で、規制当局は侵入的でリスクの高いアプリケーションのAI機能を制限しようとし始めています。

AI活用に関する原則がG20で採択されたことを受けて、AIのリスク管理と規制に大きな進展がありました。シンガポールはAIセキュリティ基準をいち早く策定し、米国国立標準技術研究所（NIST）はAIリスク管理フレームワークを公表しており、EUもAI関連の法制化に向けて動いています。この分野の規制は、最終的にはGDPR（EU一般データ保護規則）がプライバシーに与えたのと同じくらい大きな影響を及ぼすことが予想されます。多くの企業は準備をする必要があります。

4　KPMGサイバートラストインサイト2022

Learn more

私のAIは安全ですか？

人工知能がビジネスに及ぼすサイバーリスクとは

Trust in artificial intelligence: Global insights 2023

Global survey exploring people's trust in AI and benefits and risks for business and society.

The path to transparency — and trust

Corporate data responsibility survey.

主要課題6

スマートな世界を守る

ほぼすべての産業において、組織はネットワークに対応したサービスの開発と、それを支えるデバイスの管理に重点を置くという、プロダクトマインドセットにシフトしています。CISOとそのチームは、組織が製品のセキュリティも重要であることを認識しているため、エンジニアリング、開発、製品サポートチームとの議論にも参加するようになってきています。

スマートプロダクトに焦点を当てた現在の環境では、いくつかの新たなツール／技術が重要な役割を果たしています。

5G：スピード、ハイパーコネクティビティ、レイテンシーの低減を提供します。

量子コンピュータ：処理と計算にかかる時間を大幅に削減します。

トラストアーキテクチャ：接続されたデバイス間での、データとIDの安全性と信頼性確保を支援します。

ソフトウェア2.0：AIで迅速に書かれたコードによって煩雑さを軽減しつつ、開発スピードを数ヵ月から数週間に短縮できます。

応用人工知能（AI）：スマートプロダクトの発展的なラッパーとしてのAIの実世界における基礎アプリケーションです。

技術革新のスピードは衰えることがなく、規制当局やセキュリティチームはしばしばキャッチアップを迫られます。CISOは、次の規制の波を待つのでも、規制だけに頼るのでもなく、製品ライフサイクルやサプライチェーンを通じてセキュリティ管理を実施するために、積極的かつ現実的なアプローチをとるべきです。

これは並大抵のことではなく、CISOが事業において他の部門といかにうまく連携できるかが成功のカギとなります。

Walter Risi
Partner, Cyber Security Services
KPMGアルゼンチン

CEOの見解

サイバーセキュリティの課題に関する経験が増えることで、CEOは自分たちがどの程度十分に備えられているか、もしくは備えられていないかを明確に把握できるようになりました。

24%のCEOが、「サイバー攻撃への備えが不十分である」と認識しており、2021年調査の13%と比較し増えています。

56%のCEOが、「サイバー攻撃に対し備えている」と回答しています。

4分の3のCEOが、「ランサムウェア攻撃に対抗する手段を計画している」と回答しています。

4人に3人のCEOが、「パートナーエコシステムとサプライチェーンを守ることは、組織のサイバー防御を構築するのと同じくらい重要である」と回答しています。

出典：KPMG 2022 CEO Outlook

スマートデバイスには、デフォルトパスワードの脆弱性、暗号化の不備、ソフトウェアアップデートの遅れ、マルウェア、DoS（サービス拒否）対策の欠如など、多くのリスクが存在します。CISOは、これらのデバイスのセキュリティはCIA（confidentiality：機密性、integrity：完全性、availability：可用性）の3要素に基づくだけではないことを認識する必要があります。ハイパーコネクテッドで具体的な現実世界のシステムが関係するため、安全性も重要な考慮事項となっています。サイバーの専門家は、これらのリスクをCIAS（機密性、完全性、可用性、安全性）のフレームワークに当てはめる必要があります。なぜなら、大規模な標的型攻撃が発生する可能性が高いためです。

エコシステム、製品、デバイス、センサーの世界に移行し、それらが高度なサイバー攻撃の標的になることが増えるなかで、規制当局は、組織が製品のライフサイクル全体でセキュリティをどのように組み込むかについて、監視を強化しています。

スマート製品のライフサイクルにセキュリティを組み込むには、関連するサイバー上の脆弱性を事前に監視、特定および対処するなど、多くの課題があります。CISOの主な課題の1つは、品質管理部門と協力して、製品設計および出荷前検査プロセスにセキュリティを組み込むことです。

澤田 智輝
Partner, Technology Risk Services
KPMGジャパン

極度に接続された世界にCIASのフレームワークを適用する

CISOは、ライフサイクルにまたがる4つの主要な領域（デザインの実装からリリースまでの製品開発、拡大するサプライチェーンの管理、メンテナンスと継続的なソフトウェアアップデート、他の企業や個人の消費者であるエンドユーザー）からスマートデバイス関連のリスクを検討する必要があり、それぞれの領域には、DevSecOpsに関連する特定の優先事項があります。この4つの領域は、CISOがセキュリティプランをどのように編成し、製品が可能な限り安全であるとの確信を得るための判断材料となります。CISOがビジネスの全領域を見渡せるようにすることが不可欠になっています。

CISOは組織全体と協力して、サイバーセキュリティがリスク管理の優先事項となるように働きかける必要があります。また、セキュリティについて、単にデバイス内で適用できる技術的な処理の観点から考えるのは、あまりにも狭いアプローチであり、サプライチェーンや顧客サービスといった分野へのより広い影響を考慮することも重要です。

Jayne Goble
Director, Cyber Security Services
KPMG英国

スマートデバイスに組み込まれたソフトウェアは、接続性や、使用中にパッチを適用できないなどのさまざまな要因により、更新が困難といった複雑さが増しています。つまり、早期保証の仕組みを組み込む必要があり、さらに、デバイスが使用された後に重大な脆弱性が発見された場合に、企業がデバイスを検出し、最終的に回収することができるように、ソフトウェアの部品表（SBOM）をきちんと整理しておく必要があるという、さらなる課題を製造者に突きつけています。

サイバーセキュリティは市場の差別化要因となっています。当たり前のことかもしれませんが、組織のサイバーセキュリティプログラム、特にデバイス制御は常に進化しており、決して固定的ではなく、デバイスのライフサイクルを考慮して管理されていることを、現在および将来の顧客、そして幅広い市場に知ってもらうことが重要です。世界中の規制当局が、これらのシステムのセキュリティと要求される最低基準について、関心を高めていくことを期待します。

Learn more

制御システムサイバーセキュリティ年次報告書 2022

A pathway to cyber resilience
Assessing and bracing against cyber vulnerabilities in industrial sectors.

Accelerating OT security for rapid risk reduction
Securing operational technology environments as they become increasingly digitized and connected.

主要課題7

俊敏な敵に対抗する

最初の侵入からランサムウェアを発動させるまでの時間が短くなっているほか、国家が支援する悪質な攻撃者が、自動化されたツールでシステムに侵入することが増えています。インシデントが発生した場合に備え、セキュリティ関連のオペレーションを最適化し、優先すべきサービスを迅速に復旧できるような仕組みを構築することで、顧客企業、顧客、パートナーへの影響を軽減する必要があります。

サイバー攻撃者は、悪用と破壊という2つの明白な動機を持っています。悪用とは、諜報活動や不正行為を目的としてデータを盗んだり操作したりすることであり、破壊とは、脅迫や政治的利益を得ることを目的としていますが、これらの手口は実にさまざまです。

国家が支援する攻撃者のなかには、石油パイプライン、電気設備、金融システムなどの重要インフラを狙う者がいて、その目的は、政治的・経済的な影響を与えることで損害や混乱をもたらし、攻撃者やそのスポンサーが利益を得ることです。彼らは、他人の不幸を収益化することを意図しています。

サイバーセキュリティインシデントの成功確率は大幅に上昇し、その結果、近年ではランサムウェア攻撃が拡大しています。セキュリティの専門家がサイバー攻撃への対策を強化しない限り、この傾向は続くでしょう。

攻撃者が（システム等に）アクセスしてくることを受け入れなければなりません。重要なのは、滞留時間を短縮することであり、攻撃者の存在と行動を数時間、数日、数週間、数ヵ月以内に検出できるかどうかです。

Charlie Jacco
Principal, Cyber Security Services
KPMG米国

サイバーセキュリティチームが苦戦中

サイバーセキュリティチームは、進化する脅威への対応に迫られており、人材不足がセキュリティ対策に支障をきたすことも少なくありません。

半数以上の回答者が、「サイバーセキュリティ対策のスケジュールに遅れが生じていること」を認めています。

半数以上の回答者が、「組織化された外部の犯罪集団や内部の脅威、サプライチェーンの欠陥などによるさまざまなサイバー脅威に関して、対抗できる“自信がある”または“非常に自信がある”」と回答しています。

59%の回答者が、「調達やサプライチェーンで、攻撃者が脆弱性を悪用していることを認めていますが、自組織の防御が十分かどうか」はわかっていません。

第1位 キーとなるスキルの欠如（40%）がサイバーセキュリティに関する目標の達成を妨げる最大の課題です。

出典：KPMGグローバルテクノロジーレポート2022

さらに悪いことに、（リモートワークと出社を組み合わせた）ハイブリッド勤務は攻撃対象となる領域を拡大し、潜在的な脆弱性を抱えたエンドポイントの数が増加することを意味します。さらに、企業内のシャドーITには、ビジネスアプリケーションやサービスとしてのソフトウェアが含まれることが多いにもかかわらず、潜在的なリスクに対するCISOや最高情報責任者（CIO）の理解が不足しがちなことも課題を大きくしています。

セキュリティ運用戦略を厳格に

時間は重要です。いかに早く攻撃者を発見できるか、封じ込められるか、サービスを復旧できるか、いかにして情報漏えいを最小限に抑えるか。「どのように攻撃者が侵入してきたのか」ではなく、「どういった情報を得たのか、（漏洩したのは）重要なプロジェクトの情報だったのか、脅される原因になるような情報だったのか」が重要です。

攻撃者が初期侵入から実行（システムの破壊に成功するなど）までに要する時間は短くなっています。今や、攻撃者が企業全体にランサムウェアを展開する場合、数日未満ですむかもしれません。また、攻撃者の創造性が高まっており、AIに攻撃を策定させたり、全体を編成させたりといったことも可能になっています。これは、CISOとそのチームが侵入を検知し、迅速かつ果断な封じ込めに至るまでの時間がほとんどないことを意味します。

現在のセキュリティオペレーションセンター（SOC）は三角形の構造から成り立っています。上部には小規模ながら脅威に対応する専門性の高いチーム、中央にはレベル2のさまざまな調査員、下部には膨大な量のアラートのトリアージを行うレベル1のアナリストが配置されています。

この三角形を逆転させる必要があります。レベル1の数を減らし、レベル2と大惨事になりかねない脅威を探す人数を増やさなければなりません。現在の攻撃の量と頻度に対応するための方法の1つが、レベル1を自動化することです。

SOCを効果的に運用するには、より高度なテクノロジーを活用し、関連データをまとめ、アラートを管理する利用可能なツールを信頼するとともに、人間のアナリスト、高度な機械学習（ML）、ロボティックプロセスオートメーション（RPA）を適切に連携することが不可欠です。それにより、潜在的な攻撃の分析に、より大きなビジネスコンテキストを提供する新しいデータソースを取り込み、サイバーセキュリティ業務と物理セキュリティ、不正行為の防止、インサイダー脅威管理との融合を模索できます。

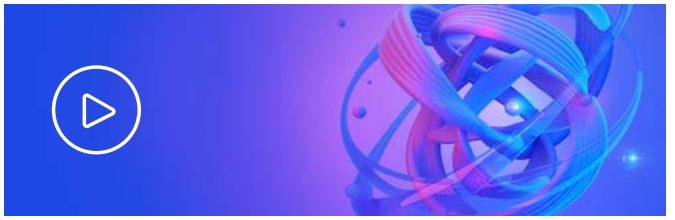
そのレベルの信頼を得るのは、大半のセキュリティ組織にとって困難です。CISOとセキュリティチームがAIを活用してトリアージを行い、ファイアウォールおよびSIEM（セキュリティ情報とイベント管理システム）を見渡し、さまざまな脅威の情報源と脆弱性スキャンツールを評価できると仮定しましょう。それがSOCの向かう先ですが、まだそこに至ってはいません。

サイバーに関する技術的専門知識の活用と維持

人材の減少と定着が最も重要な課題です。多くの組織は、SOC要員の長期的なキャリアパスとモデルを作成するための支援を必要としています。チームはシステムを監視するのに精いっぱいで、人材育成（訓練）よりも、実際に起きている問題の対応に多くの人員をあたらせています。

訓練が優先されない状況が続くと、社員は行きづまりを感じ、最終的には転職してしまいます。また、攻撃者は絶えずテクニックや戦術を進化させていますが、CISOは、そういった攻撃者に追いつくためのリソースを持ち合わせていないのです。

Learn more

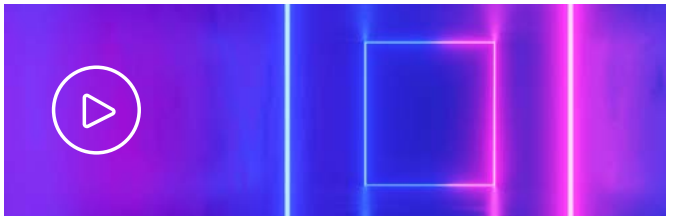


KPMGグローバルテクノロジーレポート2022

世界中のテクノロジーリーダーに対する調査からみえる、デジタルトランスフォーメーションの進捗と、デジタル成熟度をさらに高めるための取組み

ランサムウェア攻撃への備え

現在のリスク、予想される脅威への準備



アメリカ大陸で発生している3つの脅威：KPMG Fraud Outlook

アメリカ大陸における不正行為、コンプライアンス違反、サイバー攻撃に関する2022年の展望

主要課題8

必要に応じたレジリエンス

どんなセキュリティシステムにも欠陥があり、程度の差こそあれ、企業はおそらく複数回のインシデントに見舞われることは避けられないでしょう。規制当局は、実際に起こり得る可能性が高いシナリオに注目し、企業、特にエネルギー、金融、ヘルスケアなど戦略的に重要な業界に対し、復旧のためのレジリエンスを確保するよう求めています。

おそらく最も顕著な問題は、サイバーインシデントの影響と復旧にかかる時間が長期化する可能性があることを、組織が往々にして認識していないことでしょう。サイバーインシデントは通常、72時間や96時間で終わるものではありません。最悪の場合、大規模な事業の中断を想定しなければなりません。多くの場合、シニアリーダーは、企業全体の技術的なつながりや、従業員やサプライヤーへの支払い、顧客や投資家とのコミュニケーションなど、事業運営上の依存関係を十分に理解していません。

CISOは、危機が起こってからではなく、明確かつ柔軟なレジリエンス戦略を事前に適切に設定できるよう、早い段階からビジネスに関与しておくことが重要です。

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

規制の見通し

産業界では、透明性と監視への需要が高まっています。多くの企業は、ますます複雑化するグローバルな規制環境への対応に懸念を抱いています。

36%の回答者が、「デジタルサービスプロバイダーに業務を委託する際、既存または新規のサイバーセキュリティに関する規制に準拠しているかどうか」を懸念しています。

31%の回答者が、「英国やEU、米国で規制強化の対象となっている、重要インフラに関する要求が高まっていること」を懸念しています。

28%の回答者が、「主要システムのレジリエンスに関連する既存または新規の規制」について懸念しています。

26%の回答者が、「インシデント報告義務の厳格化」を懸念しています。

出典：KPMGサイバートラストインサイト2022

また多くの企業は、レジリエンスを高めるためにプロアクティブに何をすべきか、まだ真剣に検討していません。バックアッププランがあり、十分なセキュリティ管理がなされていると思い込んでいるのです。ただ、特定のシナリオに対応した計画がなく、業務が停止してしまったらどうなるでしょうか。財務や評判に深刻な影響を及ぼすほか、心理的なインパクトもあるでしょう。

CISOは、攻撃者の性質と動機について、経営幹部や取締役会と継続的に話し合う必要があります。大半の組織は、自分たちが現実に直面していることを理解するのに依然として苦労しています。

有事でも平時でも積極的な連携が重要

激しい攻撃を受ける混乱期において、CISOの重要な責務は、事業を継続するために必要な知見を社内に提供することです。CISOは日々の技術的な詳細から離れ、迅速な復旧に向けどのように対応するかについて、組織一丸となって積極的かつ戦略的に話し合う必要があります。

CISOの仕事の大部分は、コミュニケーターとして、サイバー攻撃がビジネスに与える潜在的な影響とサイバーセキュリティを最優先することの価値を企業全体に明示することです。さらに、レジリエンスを構成する対応と復旧もCISOの重要な職務ですが、これを遂行するには、CEO、最高財務責任者（CFO）、および最高法務責任者からなる小規模な「危機管理委員会」を通じた連携が必要です。

多くの企業はサイバーインシデントが自社で起こると思っていないため、「危機管理委員会」のような重要なグループが正式に存在していません。また、万が一の場合も、事業継続計画（大半は数年前のもので、時代遅れのユースケースに沿ったもの）があれば十分と考えています。しかし、実際はそうではありません。

最低限のビジネスが可能な状態まで復旧する

制御がうまくいかないからといって、単に優れたセキュリティを構築すればよいといった話ではありません。復旧のために必要なことを明確にする必要があります。企業のリーダーは、目先のことに目を向けがちですが、渦中にいると、それ以上考えられないためです。有事において、CISOは理性の代弁者となり、最低限のビジネスプロセス、つまり、従業員に給与を支払い、業務を再開できるようにすることについて現実的に話さなければなりません。

最低限実行可能なビジネスプロセスに戻るのに時間がかかるほど、事業が存続の危機に陥る可能性は高くなります。悪質な攻撃者は、企業のスケジュールに合わせて動くわけではありません。彼らは金銭的な動機から、より速く進化します。これが、CISOが直面する課題です。

サイバーインシデントの潜在的な軌道を理解したうえで、体制を整える必要があります。リソースを結集するための計画と明確なアプローチを持つことが、60日間の悪夢となるか30日間の悪夢となるかの違いとなります。

Jason Haward-Grau
Principal
Cyber Security Services
KPMG米国

レジリエンスにおける規制の役割

レジリエンスに関して言えば、規制は土台とみることもできれば、天井と捉えることもできます。ほとんどの組織は、規制を遵守しなければならないものとみなし、必要最低限のみ対応しようとしています。一方、規制により、頻繁に新しいアクションや異なるアクションを起こさなければならないため、ビジネスの基礎とみなすこともできます。

規制は、組織のレジリエンス向上に重要な役割を果たしますが、多くの場合、調整または連携が必要です。このことは、規制の対象が企業のサプライチェーンに拡大するにつれ、CISOが直面する主要な課題の1つです。もはや、組織全体に関してのみ心配すればよいという状況ではありません。

CISOは「サプライヤーなどの重要なパートナーが関連規制に準拠しているか」や、「自社が欧州サイバーレジリエンス法に準拠しているかが顧客や投資家に分かりやすいか」など、多方面への影響を考慮しなければいけません。

レジリエンスは最終的には組織全体の問題であり、サイバーセキュリティは、事業継続訓練や復旧能力と合わせて重要な要素です。CISOは、組織が破壊的なサイバーインシデントへの対応を計画する際に、重要な役割を果たすことができます。サイバーインシデントの性質、規模、対応は、典型的なシステム障害や著作権侵害などのインシデントと異なる場合があります。多くのCISOは、組織がこのようなシナリオとその結果にますます注目するようになるにつれ、より広範なレジリエンスを担当することになるかもしれません。

Learn more

The day after

Recovery, resistance and resilience after an industrial cyberattack.

From continuity to resilience

The growing dependence on electricity makes it more critical to build a proactive, resilient organization to help ensure continuity of service.

Incident readiness: A playbook for your worst day

Being prepared for a cyber incident can minimize critical power and utility infrastructure disruption.

2023年のサイバー戦略

セキュリティを組織の要とするために、CISOを中心とするチームは、今後どのような行動をとることができるでしょうか。
以下は、サイバーインシデントが従業員、顧客、パートナーに与える影響を軽減し、セキュリティ計画が事業目標を円滑に実現し、迅速にインシデントから復旧するため、CISOが検討すべき具体的なステップのリストです。

人材

- 従業員に正しい行動を促し、「人的ファイアウォール」として機能させるため、興味深く、魅力的で（時には楽しい）強固なサイバーセキュリティ文化を構築する。
- クラウドやサードパーティの活用を含め、境界のない組織を管理するために必要なスキルミックスを備えたセキュリティチームを構築する。
- 広範かつ明確にコミュニケーションを図る。他の組織のリーダーに、自社が抱えている問題点や、自動化されたプロセスがどのように役立つかを聞く。
- 学際的かつ文化横断的なアプローチをとる。社内の各事業の専門家、セキュリティの専門家、データサイエンティスト、プライバシー保護に精通した弁護士、社外の政策や業界の専門家からなる「セキュリティエコシステム」を構築する。
- 対等な立場で、組織内の相談相手、アドバイザーとして活動する。

プロセス

- 脅威シナリオと攻撃経路を理解したうえで、サイバーリスク管理に向けた一貫したアプローチを構築し、攻撃対象領域の縮小や管理体制の改善の優先順位付けに役立てる。
- 一貫したユーザーエクスペリエンスを特徴とする、目的に合ったセキュリティプロセスに重点を置く。
- 厳格なID管理を確立し、IDガバナンスとサービスを成熟させる。
- レガシー環境をセグメント化して、攻撃対象領域を限定し、侵入を阻止する。
- 組織の最も重要なワークフローに焦点を当てたプロアクティブな復旧計画を立て、コミュニケーション体制を整え、頻繁にストレステストを実施する。

データ／技術

- セキュリティ機能の自動化が避けられないことを受け入れる。SOAR（Security Orchestration, Automation and Response：セキュリティオーケストレーションと自動化・対応）、拡張検知・対応（XDR）システムに、ロボティックプロセスなどの最新ツールを信頼する。
- クラウドプロバイダーと連携し、製品やサービスの設定方法を幅広く可視化することで、意図しない脆弱性を回避する。
- AIシステムの導入に関連する進化したリスクなど、新たなテクノロジーの導入を検討する際には、サイバーセキュリティとプライバシーの問題を事前に考慮する。
- 重要なデータをどのように処理・管理し、重要なビジネスプロセスをどのようにサポートするかについて、的確に役割を分担する。
- スピード、スケーラビリティ、信頼の観点から、クラウドにおけるサービスとしてのIDへの移行を早急に行う必要がある。

規制

- 規制の動向とドライバーの変化、およびそれらが企業の将来の技術戦略、製品開発、業務にどのような意味を持つかを認識しておく。
- AIや自動化に対する規制の影響を考慮しつつ、これらの領域で実現できること、できないことの明確なコンセプトを確立し、世間の関心や期待の変化を敏感に察知する。
- コンプライアンスの監視と報告の自動化を検討し、プライバシーとセキュリティに関する規制の動向を把握する。
- セキュリティとプライバシーのコンプライアンス戦略を自社の広範なビジネス戦略と整合し、組織全体のステークホルダーが認識を合わせるようにする。
- デジタルトラストとそれを戦略的思考の中心に据える方法について、より根本的な質問を自ら問うよう、心がける。

KPMGによる支援

KPMGは役員室からデータセンターまで、幅広い領域で貴重な経験を重ねています。KPMGは、顧客企業のサイバーセキュリティを評価し、ビジネスの優先順位に合わせるだけでなく、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。

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、迅速に行動し、優位に立てるよう、支援することができます。それは、技術的な経験、豊富なビジネス知識、そしてステークホルダーの信頼を守り、築くための支援に情熱を注ぐクリエイティブな専門家という、他に類をみないコラボレーションを生み出すことができるからです。

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

Prasad Jayaraman
Americas Cyber Security Leader
Principal
KPMG米国

「サイバーセキュリティ主要課題」チーム（グローバル）

Jessica Booth
David Ferbrache
John Hodson
Billy Lawrence
Leonidas Lykos
Michael Thayer

執筆協力

John Anyanwu
Partner, KPMGナイジェリア

Jonathan Dambrot
Principal, KPMG米国

David Ferbrache
Head of Cyber Innovation
KPMGインターナショナル

Jayne Goble
Director, KPMG英国

Jason Haward-Grau
Principal, KPMG米国

Lisa Henegan
Global Chief Digital Officer
KPMG英国

Charles Jacco
Partner, KPMG米国

Prasad Jayaraman
Principal, KPMG米国

Sylvia Klasovec Kingsmill
Partner, KPMGカナダ

Markus Limbach
Partner, KPMG米国

Deepak Mathur
Principal, KPMG米国

Dani Michaux
Partner, KPMGアイルランド

Matt O'Keefe
Partner, KPMGオーストラリア

Natasha Passley
Partner, KPMGオーストラリア

Walter Risi
Partner, KPMGアルゼンチン

澤田 智輝
Partner, KPMGジャパン

Henry Shek
Partner, KPMG中国

Julia Spain
Partner, KPMG英国

Eddie Toh
Partner, KPMGシンガポール

Akhilesh Tuteja
Partner, KPMGインド

Annemarie Zielstra
Partner, KPMGオランダ

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。

kpmg.com/jp/socialmedia

Designed by Evalueserve | Publication name: Cybersecurity considerations 2023 | Publication number: 138614-G | Publication date: February 2023