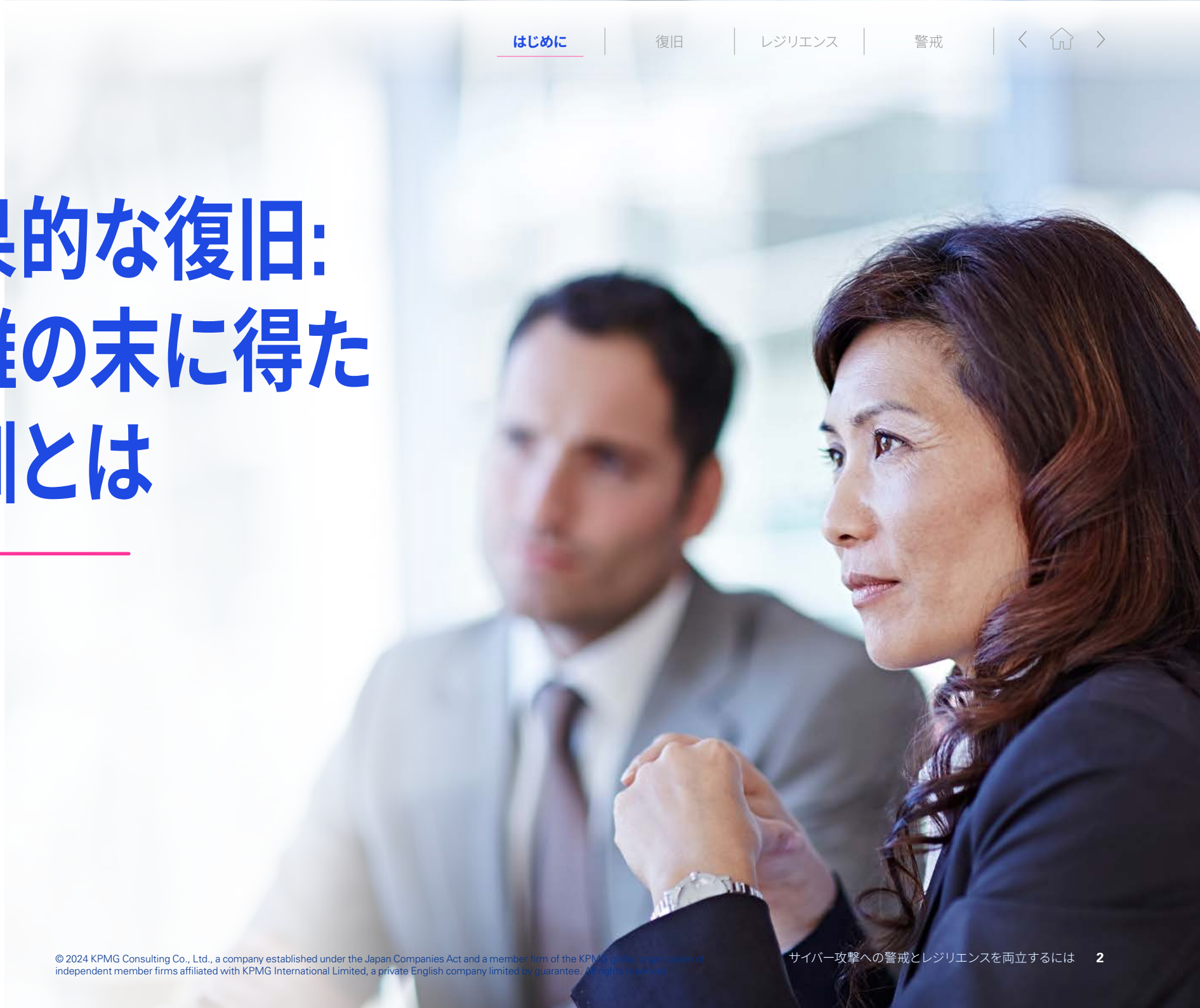
KPMG

サイバー攻撃への警戒とレジリエンスを両立するには

効果的な復旧: 苦難の末に得た教訓とは



サイバーセキュリティの攻撃手法は絶えず変化しています。かつて有効だった防御手段は今や十分ではなく、サイバー攻撃で得た資金によりさらに巧妙な手段で攻撃してくる犯罪集団にも、巨額な資金をサイバー攻撃のための能力開発につぎこむ国家にも太刀打ちすることは困難です。

悪意のある集団も国家も、確立された手法を使用しつつ、先進テクノロジーも利用して新たな攻撃経路を開拓しようと試みています。新たな犯罪者たちは、優位性を得るために人工知能（AI）も活用しています。KPMGグローバルCEO調査2023によると、82%のCEOが「生成AIはサイバー攻撃を検知するのに役立つ半面、サイバー犯罪者に新たな攻撃戦略を与える両刃の剣だ」という見方に同意しています[1]。

依然として予防に高い優先度が置かれる一方、経営層は、最善の防御態勢を敷いてもサイバー攻撃を防ぐことはできず、結果的に知的財産や機密データが盗まれ、それが恐喝や詐欺につながっていくことを認めています。また、同調査において、74%のCEOが、「サイバー犯罪と不十分なサイバーセキュリティは企業の業績に悪影響を及ぼす要因である」と考えています[2]。被害を最小限に抑え、業務を効果的に立て直してレジリエンスを高める手段として、迅速な検知、対処、そして復旧の重要性はかつてないほど高まっています。

油断は、レジリエンスの最大の敵の1つです。サイバーインシデント対応という白熱した闘いが一段落し、日常が戻ってくると、急を要する仕事や運営上の問題へと注意が移っていき、以前のような気の緩みが生じるのは無理もないことです。そうした瞬間を突いて再びインシデントが起きても、同じミスを繰り返したことで顧客や株主に愛想を尽かされても、驚くことではありません。

サイバーレジリエンスは、企業の経営能力を維持し、顧客の信頼を守り、攻撃を受けた場合の被害を縮小させるために必要不可欠な能力です。KPMGグローバルテクノロジーレポート2023によると、71%の組織が、「テクノロジー導入時に信頼、セキュリティ、プライバシー、レジリエンスを積極的に組み入れたい」と考えています[3]。世界的にみても、規制当局はサイバーレジリエンスを重視する姿勢を一段と強めています。たとえば、EUのデジタルオペレーショナルレジリエンス法（DORA）や、改正されたネットワーク・情報システムの安全に関する指令（NIS指令）、あるいは最近制定された米国証券取引委員会（SEC）によるサイバー規制などです。

組織は、インシデントの発生前、発生時、発生後におけるセキュリティ侵害への対応能力に関し、透明性を高めることを余儀なくされています。金融サービスをはじめ、セキュリティが不可欠なセクターでは、規制当局から一定の期間内にサービスを復旧することが求められますが、他のセクターでは、インシデントに起因する被害から顧客や取引先を保護することに重点が置かれます。2023年7月、SECはサイバーセキュリティのリスク管理、戦略、ガバナンス、およびインシデントに関する情報開示を強化するよう企業に求める最終規則を発表しました[4]。

セキュリティ侵害発生後の目標は、単に組織を立て直すことだけではありません。発生前より組織の防御を強化し、攻撃に対する脆弱性を軽減させ、セキュリティとレジリエンスを高めることも含まれます。

本レポートでは、KPMGが苦難の末に得た教訓として、組織がサイバー脅威に自信を持って積極的に対処し、サイバーインシデントから復旧し、防御を強化した状態で再起するのに役立つ情報を紹介します。

ビジネスチャンスとして認識され始めたセキュリティ

74%のCEOが、「サイバー犯罪と不十分なサイバーセキュリティは企業の業績に悪影響を及ぼす要因である」と考えています。

71%の組織が、「テクノロジー導入時に信頼、セキュリティ、プライバシー、レジリエンスを積極的に組み入れたい」と考えています。

82%のCEOが、「生成AIはサイバー攻撃を検知するのに役立つ半面、サイバー犯罪者に新たな攻撃戦略を与える両刃の剣だ」という見方に同意しています。

1 KPMGグローバルCEO調査2023、KPMGインターナショナル、2023年
2 同上
3 KPMGグローバルテクノロジーレポート2023、KPMGインターナショナル、2023年
4 Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Release No. 33-11216; 34-97989; File No. S7-09-22,（September 5, 2023）.

サイバー攻撃から復旧し警戒心を維持するための主なステップ

各ステップをクリックすると詳しい内容に移動します。

インシデント対応の渦中：

復旧

01 何が重要かを定義する

02 最も重要なことに集中する

03 誰が何をするかを明確に

04 コミュニケーション

05 立ち止まってじっくり考える

06 適応力をつける

07 危機が去ったことを的確に判断する

最悪の状況が過ぎた後：

レジリエンス

01 起こったことを正直に認める

02 レジリエンスを構築する

03 クリーンアップを実施する

04 組織全体で取り組む

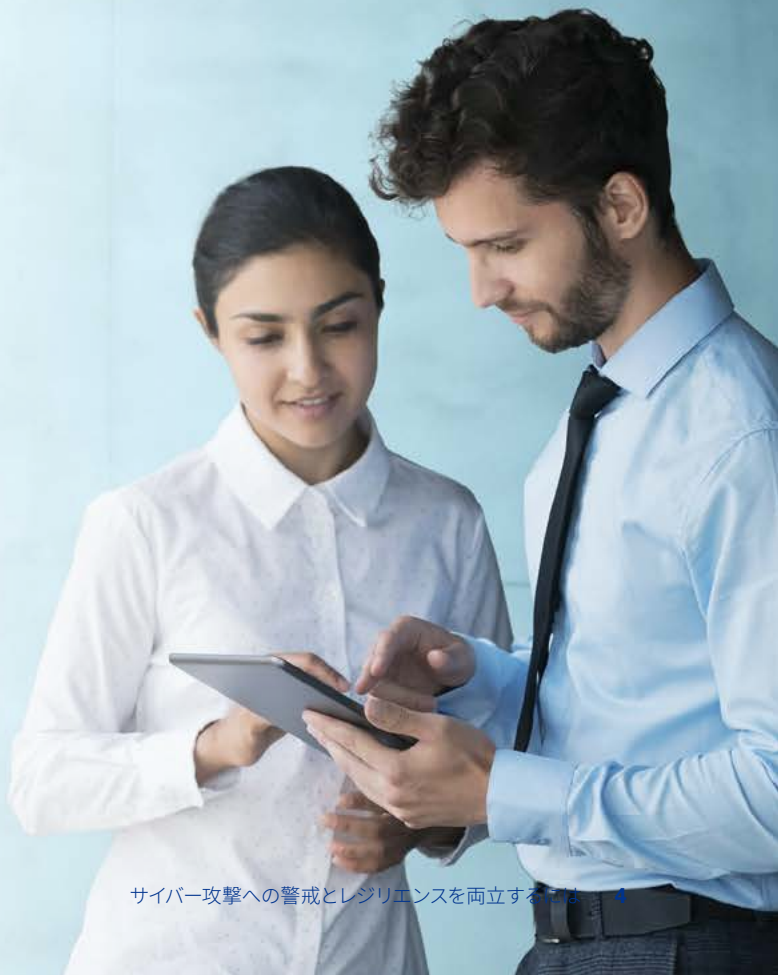
05 サプライチェーンを理解する

06 専門家を頼る

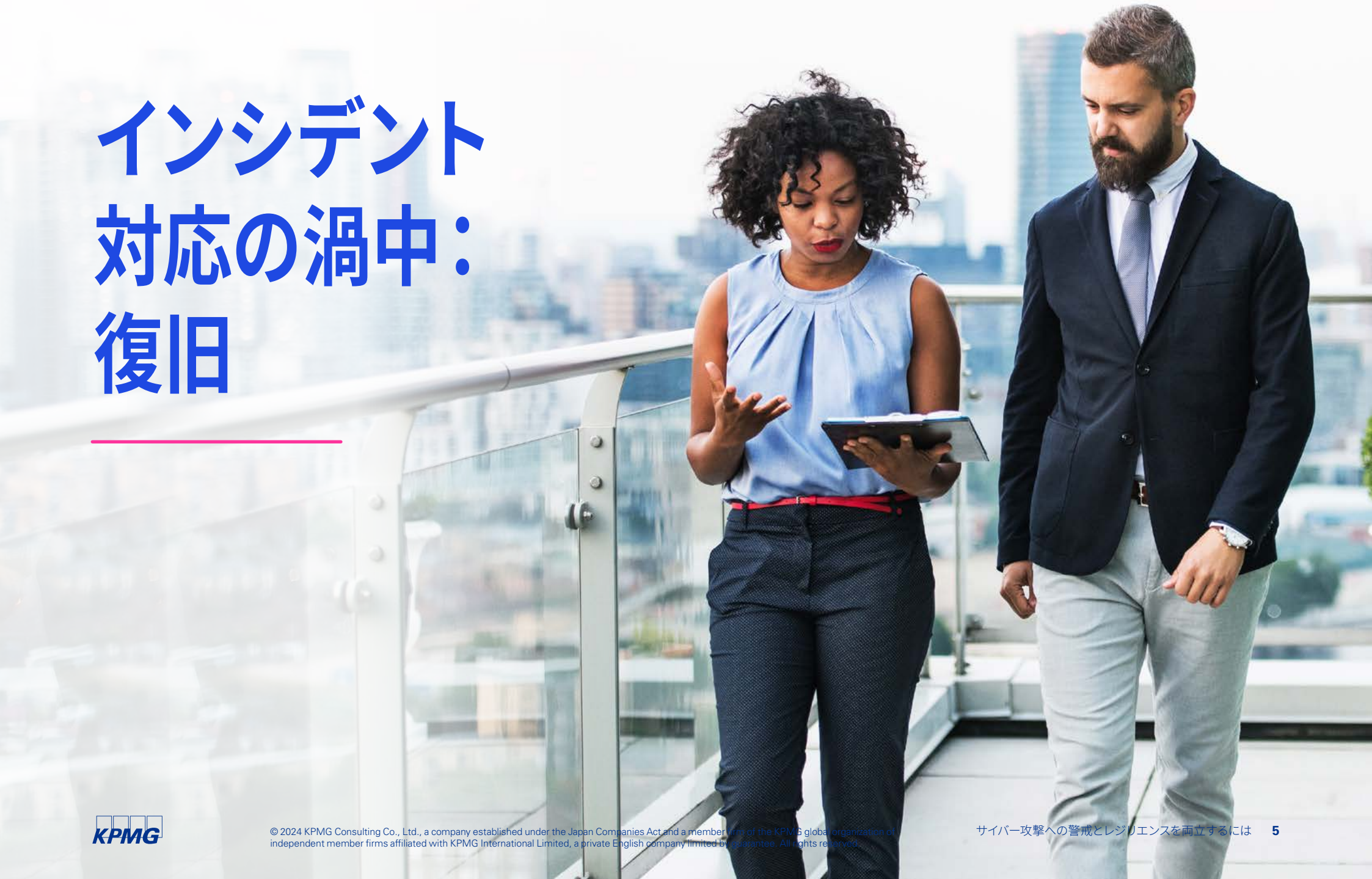
07 世界は常に変化している

何よりも重要なのは：

警戒を怠らないこと



インシデント対応の渦中：復旧



01 何が重要かを定義する

危険なのは、経営層がセキュリティ侵害の影響を過小評価し、技術的な問題として扱うことです。初期の段階で、経営会議で事の重大性、および、近い将来に何が起こり得るかを説明することで、どの程度対応に時間がかかり、不確実な要素があるかについて現実的な見通しを示すことができます。外部のアドバイザーから、経験に基づく本質的な洞察を得ることも可能です。重要な業務が脅威にさらされている（従業員、サプライヤーなどへの支払いができなくなるなど）ことをCEOとCFO（最高財務責任者）が認識すれば、行く手に待ち受けている厳しい現実も受け入れたうえで、より踏み込んだ形でリーダーとしての役割を担おうとするでしょう。

02 最も重要なことに集中する

セキュリティ侵害直後の緊迫した状況では、すべてを迅速に修正したい欲望にかられるのも無理はないことですが、そのような衝動は抑えなければなりません。リーダーは、どのビジネスプロセスとシステムが業務復旧のために最も重要かを明らかにし、そうした重要事項が最優先に緊急対応されるようにすべきです。

たとえば、人的資源への依存度が高い建設業界では、支払いが滞れば誰も現場に来てくれなくなるため、請負労働者への支払いが最も重要です。一方、病院に勤務する医師や医療従事者は、患者のデータと医療機器の継続的な稼働を重視するでしょう。世界規模のメーカーであれば、最大の収益を生み出している生産施設に集中し、流動資金を維持しようとするはずです。また、安全の維持が至上命令である業種もあります。このような多様な経営判断が、技術的なインフラを立て直すという現実と並び、常に重要となるのです。

> **“セキュリティ侵害を受けたある企業は、従業員の記録を失ったため給与を支払えなくなりました。これは、ビジネス全体を危うくする事態です。その点に気づいた同社は、給与の詳細データをバックアップから取り出し復元と復旧に注力しました。”**

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

03 誰が何をするかを明確に

大きなストレスがかかる困難な状況にあって、仕事を人に任せられず、自ら舵を取ろうとする経営層もいます。CEOは何事にも采配を振るう癖が付いているものですが、こういった危機的な状況ではむしろ、事態の収拾に必要な裁量をCISO（最高情報セキュリティ責任者）やCIO（最高情報責任者）に与えるべきです。

CEOの役割は、業務復旧に向けた戦略の責任を負い、そうした戦略がビジネスニーズを最も重視する形で実行されるよう進めることです。組織の対外的な代表者としてステークホルダーとのコミュニケーションを維持し、企業の事業存続能力に対する顧客、規制当局、株主、一般市民の信頼を保つという、きわめて重要な役割も担っています。

CEOの補佐役は、通常、技術的な復旧の責務（ITベンダーの管理も含む）を担うCOO（最高執行責任者）が務め、他のビジネス部門のリーダーはビジネスへの影響を把握し、それを軽減する責任を負います。

インシデントの渦中では、主要な人員に激務を強いることになるでしょう。長時間労働が当たり前になり、その結果、多くの従業員が「燃え尽き症候群」に陥る危険が生じます。したがって、休憩時間を確保するために十分な要員を配置し、人員を適切に交代させることが必須となります。これには、リテーナー型の契約に基づいて第三者やベンダーの支援を受けることも含まれますが、そのような契約には、前述のような復旧の優先順位を反映させた明確なサービスレベル合意書（SLA）を付随させる必要があります。

> **“さまざまなチームがどのように関与し合うかを理解してください。インシデント対応チーム、危機管理チーム、事業継続チーム、障害復旧チーム、コミュニケーション（広報）チームなど、各チーム同士の接点を明確にしなければなりません。そうした接点を計画書や枠組みのなかに組み込み、誰もが自身に託された務めを明確に理解して、各自の能力を発揮できるようにすることが重要です。”**

Campbell Logie-Smith
Director, Business Resilience Services Leader
KPMGオーストラリア

04 コミュニケーション

第一に、インシデントを開示する必要があるかを判断し、開示が必要な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。情報開示が法的に義務付けられていることもあります。

外部のステークホルダーが何らかの形で影響を受ける場合は、最低限、サービスが一時的に影響を受けることを説明し、社外の弁護士の助言を受けながら法的な義務に対応しなければなりません。社内では、危機管理チーム（経営層、人事、広報、法務から成るチーム）と、現場で捜査を実施してセキュリティ侵害対応の活動を遂行するテクノロジーチームとの間で、整然かつ堅固な状況で、協力と情報共有が行われるよう、取り計らうべきです。

セキュリティ侵害の報告に関する規制や、契約上の要求事項に注意してください。そうした義務は侵害の程度によって変わってきますが、一般的に、何が起きたか、重要な業務にどのような影響があるかを開示するまでの期限が定められています。規制当局と緊密に協議し、規制当局が知る必要があることを、適時に開示すべきです。報告が早すぎて情報が多くなること、反対に遅すぎて少なくなることも避けなければなりません。

> **“私の経験では「インシデントに関連する情報を開示する用意がある」と責任者が積極的に公言することが得策で、バランスのとれた形で情報を開示することが重要です。そうしないと何が起きているか誰にもわからず、それぞれが独自の結論を引き出してしまう恐れがあり、個々の勝手な推測を許してしまうと、状況をコントロールできなくなります。”**

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

05 立ち止まってじっくり考える

インシデントの渦中では、即座に行動しないとすべてが終わってしまうように思えるかもしれませんが、焦らずに状況が明らかになるのを待つほうが、より適切な判断を下せる可能性が高くなります。「戦況」を把握することは復旧への闘いにおける鍵であり、そのためには、さまざまな知見を活用し処理する時間が必要です。戦略的に空白時間を作り出すことで、細部にとらわれ大局を見誤るのを避けることができます。非常にストレスの高い状況では、経営層は、「不快を快とする」気構えで、大規模なサイバーインシデント時の、不確実な要素を受け入れていくことが必要となります。

根拠がない想定は避けてください。経営層は技術者やその他の専門家に（できれば24時間以内での）調査を要請し、侵害とその影響の実態をより明確に把握すべきです。

たとえば、単にシステムをシャットダウンしただけでは、攻撃者の意図を見つけ出すことも、環境内のどこに移動したのかを追跡することもできずに終わる可能性があります。実態把握の調査が特に重要なのは、サイバー諜報活動の場合です。なぜなら、工作員は長期的な戦略に従って高度な隠密行動をとる傾向があるからです。これに対し、「スマッシュ・アンド・グラブ」型のランサムウェア攻撃では、攻撃者は最大限の利益を得るために、容赦のない強引な戦術を使ってきます。

「どのような場合に攻撃者をシステムから隔離し、封じ込め、排除すべきか」「どのような場合に攻撃者を泳がせて監視し、その活動をより的確に理解すべきか」の判断が微妙な差異によって決まることもあります。専門家のアドバイスを求め、脅威インテリジェンスを活用することが賢明ですが、これには場合により犯罪者集団と接触してその意図を探り出すことも含まれます。完璧なアプローチは存在せず、業界が違えば判断も大きく異なってきます。たとえば、医療のような人命にかかわる分野では、サービスの停止はデータセキュリティの問題をはるかに超える重大な事態を招きます。

> **“脅威アクターに立ち向かう時は活動の痕跡をたどり、今どこにいるのか、何を改ざんしたか、何を盗み出したかを見つけ出し、環境を徹底的に捜索して、同じ攻撃者の再侵入を許すようなバックドアが仕掛けられていないことを確認すべきです。”**

Matt Dri
Partner, Cyber Response and Forensic Technology
KPMGオーストラリア

06 適応力をつける

テストと演習は有用なトレーニングであり、経験値の蓄積による自信を生み出します。ただ、何をもってしても、サイバー攻撃に対する備えを万全にすることはできません。生じた事態によって方向性の変更を受け入れ、事前に立てた戦略から大きく逸脱することも想定すべきです。

複数の優先課題の対立が生じることも受け入れ、不確実性に対処する覚悟を持つ必要があります。多くの場合、被害が生じている組織は、サイバー危機の「火消し」に忙殺されるあまり「木を見て森を見ず」の状態に陥ります。サイバーインシデントに対応し、ダメージを受けた環境を立ち直らせた経験を持つ外部の専門家は、さまざまな復旧経路の良い点と悪い点を明らかにし、実現可能性、複雑さ、所要時間に関する助言を提供してくれます。

復旧と存続のために必要となる「実用上、最小限のプロセス」がどのようなものかを理解し、インシデント発生後の変更点とともに把握していれば、業務を復旧させる可能性を高めることができるでしょう。

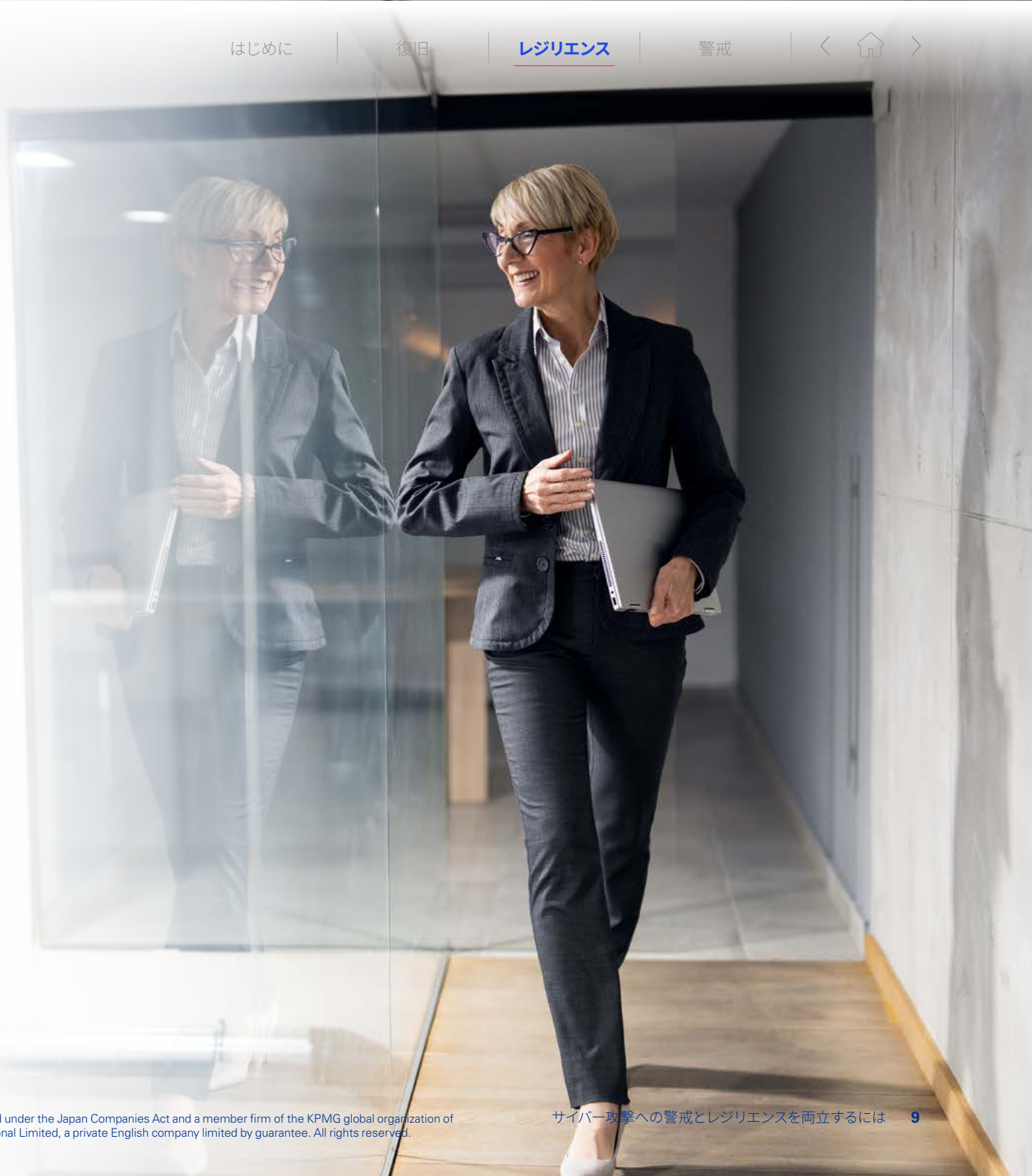
07 危機が去ったことを的確に判断する

ビジネスの復旧状況を監視するための評価指標と報告方法を確立し、そうした手段を利用して、平常業務への復帰がどの程度速やかに進んでいるかを、システムやサービスの可用性、顧客の問合せや苦情、メディアからの関心度といった観点を含めて追跡してください。読みやすく信頼できるデータは、経営層に「唯一の真実」を提示して最新の進捗状況を知らせるのに役立ちます。

危機から抜け出す時点では、すでにフォレンジック（犯罪捜査における分析、鑑識、証拠収集）がほぼ終了し、リスクが軽減されていなければなりませんが、その後も一定期間にわたって「ハイパーケア（システム稼働後のアフターケア）」活動を継続できるように準備しておく必要があります。これは、最初の襲撃で検知できなかった別の攻撃ベクトル（不正アクセスの手段）を通じて、2度目の攻撃が生じるのを避けるためです。

「対応」段階から次の段階へ移行しようとする際は、速やかに、慎重に進めてください。セキュリティ侵害の突破口となるすべての弱点が一掃され、攻撃者の再襲撃が困難になったという確信を得る必要があるからです。そこから焦点は「復旧」へと移り、より効果的な立て直しを通じて、組織のセキュリティ、レジリエンス、堅牢性を高める作業へと進むことになります。

最悪の状況が過ぎた後：レジリエンス



01 起こったことを正直に認める

包括的なインシデント事後レビュー（PIR）ではどのように攻撃が起きたかを分析し、その根本原因（多要素認証の欠如やフィッシングへの意識の低さなど）を究明します。また、組織がそのインシデントにどのように対処したか、今後どのように改善できるかも正直に評価すべきです。PIRの目的は責任を問うことではなく、反省し、改善することです。

PIRを適切に実行するには独立性を確保し、異論を唱えることをいとわず、ビジネスの側面とセキュリティに関する技術的な教訓の両方に目を向ける必要があります。リスク管理、危機管理、サプライヤーエンゲージメント、コミュニケーション、スキル、文化と意識、そして、サイバーセキュリティにかかわる問題を明らかにすることが肝要です。大きな危機に完璧に対処できる組織は存在しませんが、何事も改善することは可能です。

02 レジリエンスを構築する

レジリエンスを高めるために企業が大規模な取組みに乗り出す場合、インフラが古いと何年もかかることがあり、その間に別のセキュリティ侵害に見舞われる可能性もあります。

もちろん、そうした改善に向けた取組みは必要ですが、一方で、レジリエンスを生み出すために数週間以内にどのような緊急対策を講じられるかを考えるべきです。具体的には、「もし来月また攻撃を受けるとしたら、もっと適切に対応するために何ができるだろうか」と問うことは、「クイックウィン（早期に実現される小さな成果）」を生み出す可能性が高いでしょう。たとえば、「危機の渦中にサプライヤーや従業員への支払いを迅速化する方法は存在するか」「流動資金を維持することは可能か」「コミュニケーション能力を向上させることは可能か」「次の危機の到来時に応戦態勢をより速やかに立ち上げることは可能か」といったことです。

03 クリーンアップを実施する

大規模なサイバーインシデントから、意外な、かつ望ましい成果が生じることがあります。そのようなインシデントが起こると、特定のアプリケーションやレガシーシステムが組織にとって本当に必要か、という問題に注意が向けられるからです。多くの場合、その答えは「ノー」であり、そこからIT資産のクリーンアップ（大掃除）が始まります。

組織が必要性の低い大量のデータを保持している場合には、取捨選択の好機となります。数十年も稼働してきたファイルサーバーには、膨大な量の構造化されていないデータが保管されていますが、そうしたデータはセキュリティ侵害に成功した脅威アクターにとって、比較的容易に収集できる対象となる可能性があります。本当に必要なものだけを保存しておくことで、脅威を大幅に減少させることができるのです。

04 組織全体で取り組む

デジタル化の進行によって、さまざまな事業部門間の線引きや、安全、保護、サイバーセキュリティ、倫理などの職務領域間の境界線があいまいになってきました。エンタープライズIT（情報技術）、オペレーショナルテクノロジー（運用・制御技術）、製品のセキュリティの境界は、すでに崩れ始めています。あらゆるものが接続された世界では、組織はレジリエンスに関して単一の次元に集中するのではなく、総合的な視点を持つべきです。

保護されていないノートパソコンのような単純なものでも、データ窃盗から、詐欺、製造システムのハッキング、基幹制御システムの不正操作や改ざんまで、あらゆる種類の攻撃ベクトルになる可能性があります。サイバーレジリエンスを実現するためには、組織規模のアプローチを通じ、事業体ごとにまったく異なる文化を横断する形で適正な行動様式を推進すること、そして、データ、サービス、インフラなど、組織にとって本当に重要な問題に焦点を合わせることが必要となります。

> **“今日のサイバー侵害では、中核的な業務機能や事業拠点に属さない場所で、ユーザー IDへの不正アクセスが生じることが多くなっています。これらのユーザー IDは、拡大するサプライチェーン内の他の信頼できる組織またはサプライヤーに属していることが多くあります。こういった、見たところまったく害のなさそうな入口を通って組織のはるか深くにまで攻撃者が潜入する可能性があり、施設の稼働停止や長期にわたる情報漏洩、さらには環境被害まで引き起こすこともあり得るのです。”**

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

05 サプライチェーンを理解する

現代のサプライチェーンの複雑さと、クラウドを通じてサービスを提供するXaaS（Everythig-as-a-Service：あらゆるもののサービス化）の成長によって、組織はより多くのサードパーティに依存するようになっています。そうしたサードパーティのサイバー侵害に対処する能力を見極めること、法的な責任が生じる可能性がどこにあるかを理解することが不可欠です。難しい問題の1つに、サービスベースの契約は利益率が低いため、サプライヤーにはサイバーセキュリティのスキルを育成するための資源が乏しいことがあります。

サイバー侵害が生じた場合のサプライヤーの責任と法的義務を明確化してください。可能な場合には、それを契約のなかに盛り込んでください。ただ、サプライヤーは当然ながら、自らが負う可能性がある法的責任を限定したいと考えるでしょう。サイバーインシデントが財政的損害をもたらす可能性が高いことを踏まえると、すべての関係者が契約上の義務を理解し、あらゆる規制要件を明確にするために、専門家による法務支援が必要になるかもしれません。

サービスや顧客に対する義務を果たさなかった理由としてサプライヤーの失敗を挙げる組織に対し、規制当局は決して寛容ではありません。そして将来的には、さらにハイレベルなサプライヤーの審査を要求してくるでしょう。

“サプライチェーンをより的確に理解し、それを管理するためのガバナンスを導入する必要性は著しく高まっています。取引関係がある組織、特に、重要なITプロバイダーが、サイバー攻撃に対処できるかどうか、サイバーインシデントが発生した場合に通知してくれるかどうかを知っておく必要があるからです。”

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

06 専門家を頼る

サイバーセキュリティはきわめて専門的な分野で、インシデント対応のスキルは特に不足しているため、緊急時には高額なコストを払わないと専門家を確保できないことが少なくありません。セキュリティ侵害が発生した時に有能で経験豊富なチームをすぐに動員できれば、対応のスピードと実効性を著しく向上させることができます。対応と復旧の専門家をリテーナー契約によって確保しておくことで、インシデント発生時に迅速な動員が可能となるほか、事前に信頼関係を築いたうえで適任の専門家を選び、自社の対応能力のトレーニングと演習を支援してもらうこともできます。

07 世界は常に変化している

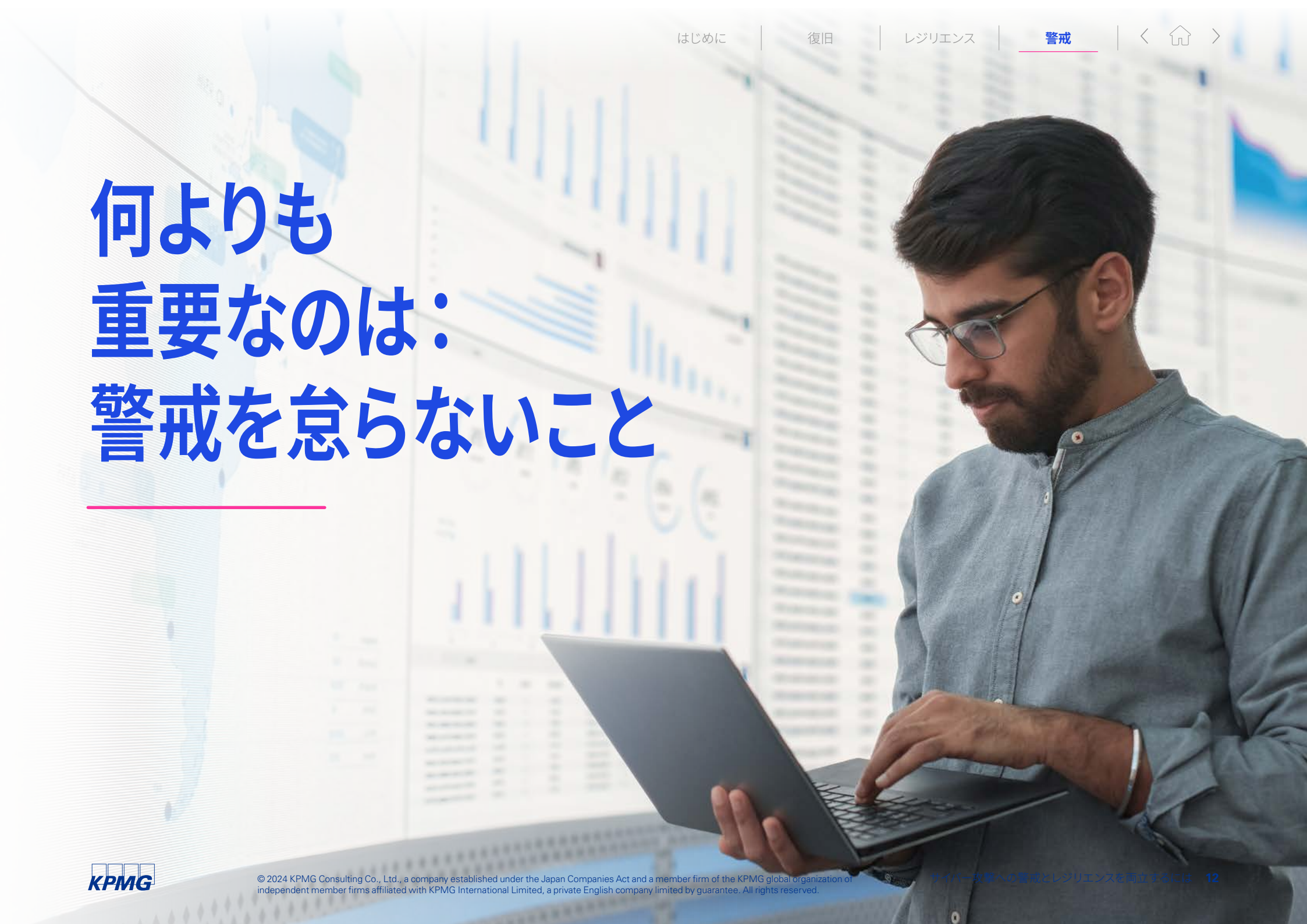
過去のサイバー侵害のパターンに基づいた対策は、攻撃者の戦術が変化して進化を遂げれば不適切になるかもしれません。2018年には、DDoS（分散型サービス妨害）攻撃、スマッシュ・アンド・グラブ攻撃、クリプトワーム型ランサムウェア（WannaCryなど）が一般的であり、主なターゲットはIT資産でした。現在の攻撃は、サプライチェーンへのセキュリティ侵害や二重三重の恐喝へと移行しており、そのすべてが高度なCaaS（Crime-as-a-Service：サービスとしての犯罪）エコシステムに支えられています。また、攻撃者がよりクラウドに精通するようになり、一段と精緻な方法でオンラインバックアップを破壊しようとしているほか、オペレーショナルテクノロジーと産業制御システムへの関心も高まっています。

つまり、対策と戦略を常に精査し、脅威情勢の移り変わりだけでなく、組織の状況やITへの依存性の変化も反映するよう、アップデートしていく必要があります。

“脅威アクターは絶えずテクニックを変化させているため、対策も柔軟に進化させていかなければなりません。そうしなければ、チームが効果的に対応できないという状況に陥る可能性があります。”

Matt Dri
Partner, Cyber Response and Forensic Technology
KPMGオーストラリア

何よりも重要なのは：警戒を怠らないこと



レジリエンスが確立できると、同様のインシデントが再び発生した場合でも以前より整った態勢で臨むことができ、被害の低減が期待できます。外部環境から到来する脅威を制御することはできませんが、それに対処して復旧するための組織の能力をコントロールすることは可能です。セキュリティ侵害やニアミス直後の、レジリエンス向上の機会を見逃さないようにしてください。

組織のなかで必然的に生じる傾向として、過去の事件の記憶が薄れていくにつれて次第に現状でよしとする風潮が生じたり、技術的エコシステム内で「迷走」が始まったり、それがサイバーセキュリティの予算の削減や全般的な気の緩みにつながる可能性があります。そうしたなか、CISO（または最高レジリエンス責任者）は、過去に何が起きたのか、現在他社で何が起きているか、そして将来に何が起こり得るかを取締役会や経営層に説明するという、難しい役割を担っています。

人材という観点から見ると、サイバーレジリエンスに優れた企業文化を生み出すには教育と予備的な訓練が必要です。それによって、全従業員が脅威に対して高い意識を持ち、いざという場合に対応できるようにしておかねばなりませんが、これは思いのほか難しいことです。なぜなら、大規模なサイバー攻撃の深刻さを演習のなかで完全に再現するのは不可能だからです。ですが、理解を深め、経験値を蓄積することには役立つでしょう。

何らかのインシデント対応を先導する人は、相反する優先課題や多岐にわたる不確実な要素に立ち向かう覚悟が必要です。組織にとって本当に重要なことだけに注力する姿勢と、そのような重要な領域を守るために難しい選択をする能力が求められます。

> **“セキュリティ要員とサイバー犯罪者の闘いは際限のない「いたちごっこ」であり、終わりがありません。さらに、犯罪者は絶えず進化しており、革新性では常に私たちよりも一歩先んじています。それでも事前に効果的な話合いを行い、徹底した応戦態勢を敷いておくことで、いざという時に蓄積された経験値が役立つでしょう。”**

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

KPMGの支援

最も優れたサイバーセキュリティ管理体制を導入している組織でさえ、破壊的なサイバー攻撃のリスクと無縁ではありません。KPMGのCyber Resilience Frameworkは、組織が大規模なサイバーインシデントを予防、検知、復旧するのに役立つように設計されています。

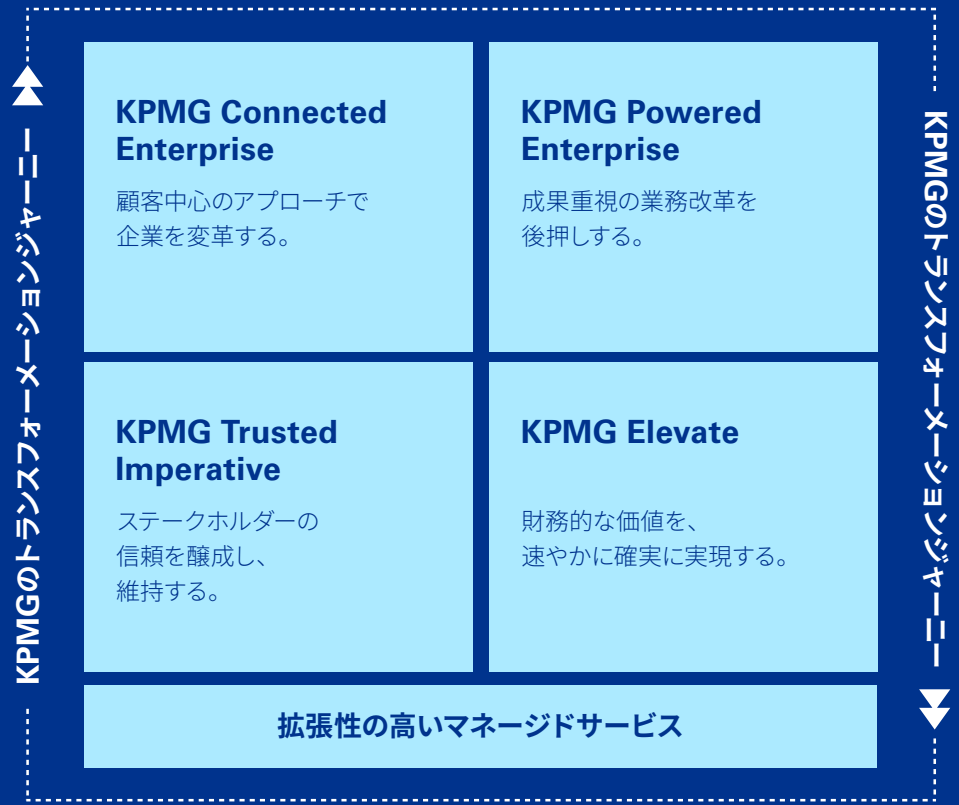
KPMGのCyber Resilience Frameworkは最も重要な標準と規制を網羅しており、先進的なテクノロジーソリューションを開発するKPMGの経験によって補完されています。各フェーズには復旧・耐性・レジリエンス（Recovery・Resistance・Resilience）を組み込んでおり、組織のセキュリティを維持するうえですべての従業員が一定の役割を担うように構成されています。

このフレームワークは、演習、テスト、シミュレーションを通じて組織のレジリエンスを高めるのに役立ちます。また、サイバー攻撃が重要なビジネスサービスに及ぼす影響を可能な限り減少させるのを助け、重要な業務の復旧と継続を可能にします。さらに、インテリジェンスを利用して高度なサイバー攻撃の脅威に速やかに適応する能力も得られます。KPMGのプロフェッショナルはサイバーレジリエンスを組織全体に浸透させることで、多大な損失を招く業務の混乱を回避し、未来への対応力を維持できるように企業を支援します。

詳細については、kpmg.com/jp/cyber-securityをご覧ください。

KPMGは、あらゆる分野のグローバル企業がデジタル経済という新たなビジネスチャンスの時代を迎え入れるための支援をしています。戦略から実行に至るまで、企業のトランスフォーメーションジャーニーの途上でさまざまな差別化を図ることが可能です。企業の現在のビジネスモデルを変革し、将来の競争力、成長、価値を高めるようサポートします。
KPMG. Make the Difference.

デジタルトランスフォーメーションを支援するKPMGのソリューション群



執筆者

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

執筆協力

Matt Dri
Partner, Cyber Response and Forensic Technology
KPMGオーストラリア

Campbell Logie-Smith
Director, Business Resilience Services Leader
KPMGオーストラリア

Alexander Rau
Partner, Cyber Security Services
KPMGカナダ

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

Ali Abedi
Senior Manager, Cyber Security Services
KPMGインターナショナル

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

本冊子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: Maintaining cyber vigilance and staying resilient
Publication number: 139036-G
Publication date: October 2023