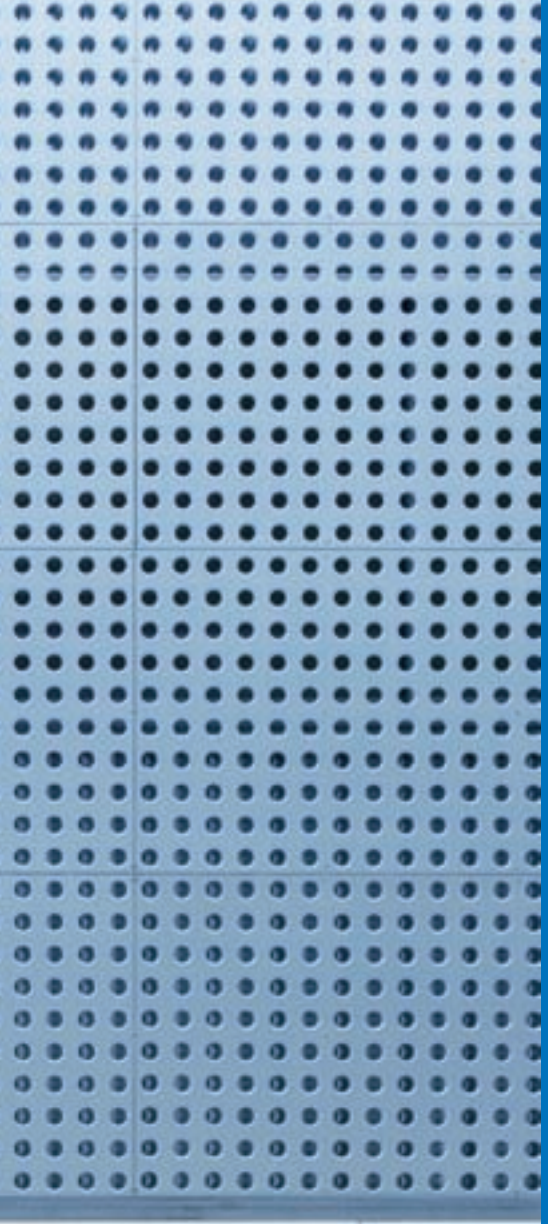
サイバーレスポンスサービス

KPMGサイバーレスポンスサービス

kpmg.com/jp/cyber



目次

サイバーセキュリティの侵害はいつでも発生する可能性があり、組織全体は危険に晒されています。

多くの企業が認識し、経験しているように、サイバー攻撃はもはや「もし」ではなく、「いつ」という問題になっています。昨今の大企業が受けたサイバー攻撃による被害が示すように、今日、企業が直面しているサイバー攻撃は、より洗練され、より高度なステルス性（検知の困難さ）を持ち、そして執拗さを増しています。このような攻撃による情報漏えいは結果として、当局の監視を強め、ビジネスに対してマイナスの影響を与えることになるかもしれません。

知的財産、顧客データ、その他の機密情報が流出すれば、深刻な損害を被り、組織の評判が損なわれる可能性があります。

KPMG は、組織が効果的かつ効率的にサイバーインシデント（セキュリティを脅かす事象）に対応できるよう支援します。インシデントが発生した後、企業は状況や証拠を保全し、法律に基づく法執行による調査を支援するためにインシデント関連のデータを収集する必要があり、そのためにデジタルフォレンジックによる分析と詳細な調査を実施します。KPMG は、組織がサイバー攻撃の脅威を予防・検出し、情報漏えいに効果的に対応するための支援を行うべく、サイバー犯罪調査、デジタルフォレンジック、リスクマネジメントの経験豊富な専門家チームを有しています。

KPMG は、世界中の有力企業が、広範囲にわたり保管する重要なデータを効果的に管理し、進化し続ける脅威と攻撃から保護することを支援します。KPMG は、サイバーセキュリティを一過性のワンタイムプロジェクトではなく、企業が成長過程におけるビジネス目標を達成するための継続的な適応戦略と考えており、プロジェクト全体を通じて長期的なビジネス価値を提供することに重点を置いています。

サイバー攻撃に対する意識が高まっているのは何故か？

2億4千万円

2014年の情報漏えい対応にかかったコストの平均額[1]

監査委員会の25%のみが、有用なサイバーセキュリティに関する情報を継続的に受け取っていると回答[2]

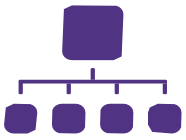
37.5兆〜57.5兆

サイバー犯罪によりグローバル経済に生じる年間コストの概算

サイバーリスクを「パーフェクトストーム（複数のインシデントが連鎖的に起こり、壊滅的な事態）」にまで至らしめる 3 つの傾向

脅威レベルの上昇

組織犯罪やハクティビスト（社会・政治的活動）、企業内部からもたらされる脅威



テクノロジー環境の変化

デジタル取引、技術革新、クラウド、事象のボーダーレス化の急増

コンプライアンスの圧力

サイバーセキュリティの強化を企業に迫る法規制や法的フレームワークの展開

Source: Ponemon Institute, 2014 Cost of Data Breach Study: Australia May, 2014 at www.ponemon.org
Source: KPMG Global Audit Committee Survey
Source: McAfee Cyber Report, Center for Strategic and International Studies

KPMG

KPMGサイバー

データ安全性に関する不安が、新たなビジネスの現実
データのセキュリティの重要性に疑問を挟む余地はありませんが一面的な見方、たとえばサイバー脅威に対して、技術的な防御のみに特化したソリューションに注目するような姿勢は、大局観を欠いており、あなたの組織をより大きなリスクにさらすことになるかもしれません。

KPMGでは、サイバーセキュリティは単に技術的な問題ではなく、企業全体の課題のひとつとして理解しています。

デジタル障壁を越えて：戦略的なアプローチ
今日のサイバーセキュリティの現実は、過去に比べ大きく様変わりしました。情報漏えいを回避することはほとんど不可能に近く、企業はデータ保護とビジネス拡大のためのデータアクセスの利便性という、相矛盾した要求のバランスを取らなくてはなりません。今日の成功が、サイバー攻撃への対応能力と通常業務を継続する能力によって決定されるなら、ビジネス目標を優先順位付けしつつ、重要な情報を守り抜けるよう、戦略をカスタマイズする必要があります。

サイバーセキュリティに対して包括的にアプローチすることは、単にデジタル的な防御策を講じるよりもずっと効果的であり、現実的です。

KPMGは、お客様の個別目標と運用を踏まえた上で、最新の脅威インテリジェンスやリーディングプラクティスから導き出されるカスタムメイドのサイバーセキュリティ戦略を策定します。

- 外部からの脅威
- ビジネスで実施している変化への対応
- 急速なテクノロジーの変化
- 法令順守
- 脅威に対する意識.

予防	改善	検知	対処
お客様のビジネスとコンプライアンスの優先課題に対し、どのように柔軟かつ最適に調和させるかといった理解醸成を支援します。	お客様の情報資産保護の課題を改善するため、適切な組織及びテクノロジーによりサポートされているプログラムやプロセスの構築と向上を支援します。	課題の見える化や、変化するリスクへの理解を醸成することで、お客様のビジネスの発展や技術プログラムの展開を支援し、情報資産保護上の課題解決を進めます。	サイバーインシデントに対する効果的かつ効率的な対応、テクニカル分析、対応活動マネジメントといった支援をします。

お客様のビジネス上の優先順位、コンプライアンス上のニーズへの合致

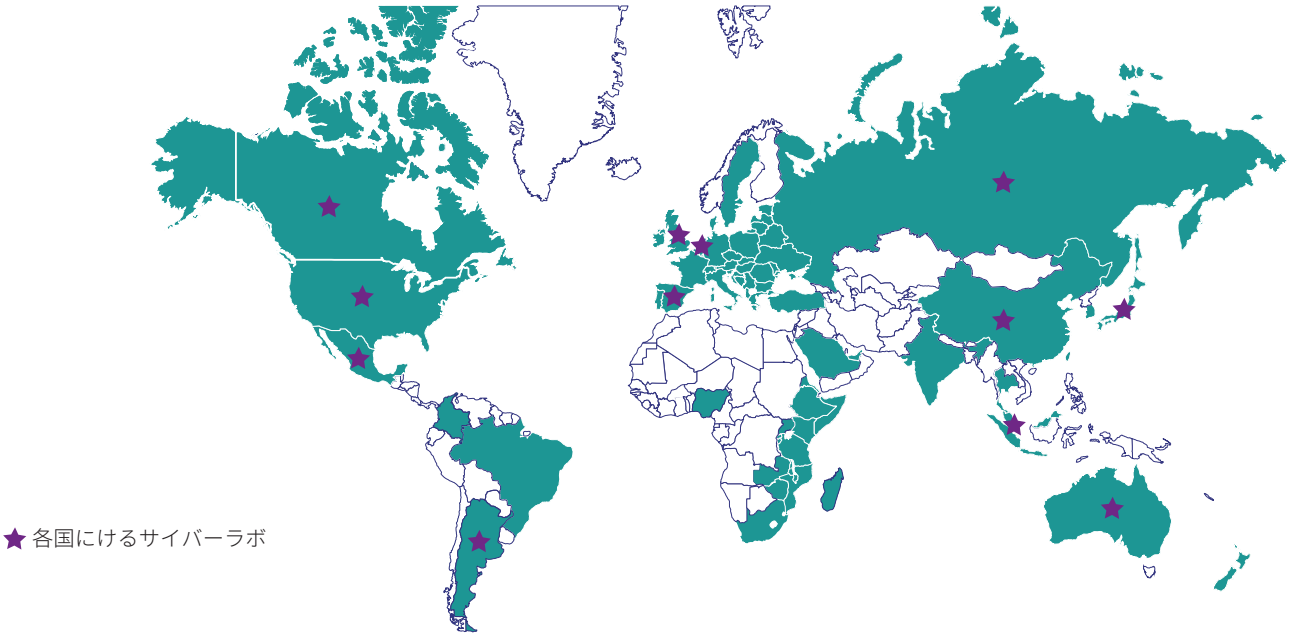
戦略とガバナンス	トランスフォーメーション	サイバーリスク	サイバーレスポンスサービス
脅威は予測不能。政府機関、犯罪集団、ハクティビスト、内部犯行者からの攻撃を受ける企業が増加しています。 トピックはますますビジネス指向になり、取締役とCレベルの会話や行動における関心の焦点になっています。	KPMGの最も成功したプロジェクトのひとつとして、大規模なセキュリティ変革プログラムがあります。 KPMGのお客様は自社のセキュリティ能力を変革・成熟させる必要性を認識していました。すなわち、リスクを軽減し、変化する脅威への適用能力を身に着けることが肝要でした。	サイバー攻撃の検知・対処に求められるタイムフレームは、数週間といった期間です。つまり、一般的な企業が期限内に対処することは、現実的に不可能です。 世の中を騒がしているサイバー攻撃に係る問題は、脅威の予防やリスク・インテリジェンスの改善を要求する契機となります。	高度なサイバー攻撃の進行は、法律上、ビジネス上の大きな影響を及ぼす結果となります。 情報漏えいに関する証拠を安全に保全し、法律や法的手続きに則った調査を支援するにあたり、フォレンジック手法に則したデータの保全・分析が必要となります。

予防	改善	検知	対処
— サイバー成熟度評価 — サイバーセキュリティ戦略とプログラムの策定 — ベンダーのセキュリティリスクと管理	— 認証とアクセス管理 — セキュリティガバナンス、リスクとコンプライアンス — 制御システム（ICS）セキュリティ — セキュリティプログラムの実施	— 侵入テスト／脆弱性評価 — セキュリティ解析 — インシデントレスポンス — 脅威インテリジェンス	— サイバー侵害の検出と詳細なテクニカル分析 — 漏えいデータの調査と軽減 — サイバーインシデント発生後の分析とレポーティング — コンプライアンス報告活動

グローバルな一貫性と各国のサービス提供能力

KPMGは世界中に3,500名を超えるプロフェッショナルと主要国でサイバーラボを有しており、日本、米国、英国、スペイン、オーストラリア、オランダ、ロシア、シンガポール、カナダ、中国、メキシコ、アルゼンチンに設置されています。

— 一貫性のあるグローバルアプローチ、共通メソドロジー
— コンタクト先の一元化と組織力による迅速な対応



★ 各国にけるサイバーラボ

KPMGが選ばれる理由

KPMGのサイバーセキュリティは、世界中のKPMGメンバーファーム内の広範囲な専門家のネットワークを有し、お客様のセキュリティ、プライバシーおよびコントロールの持続性をビジネス対応のプラットフォームに変換することを支援します。そして、全ての重要なビジネス機能の機密性、完全性、可用性を維持します。KPMGのサイバーセキュリティアプローチは、お客様のビジネスの優先事項やコンプライアンスのニーズに戦略的に対応しています。

— 経験豊富な情報セキュリティおよびフォレンジックのパートナーおよびプロフェッショナルが、テクニカルな経験を積み重ね、この専門分野で優良な評価を受けています
— この分野のプロフェッショナルの多くは、サイバーコミュニティのリーダーであり、サイバー犯罪と戦うために日常的に使用されるツールやメソドロジーの開発に貢献しています。
— KPMGは、フォーチュン500やグローバル2000に選ばれている幅広い業界の企業に対し、サイバーセキュリティプログラムを構築、開発、支援しており、豊富な経験を有しています。

KPMGのサイバーセキュリティのアプローチ —予防、改善、検知、対応—はシンプルで効果的であり、最も重要なことはお客様のビジネスニーズに合わせて設計されていることです。

KPMGのサイバー調査専門家は、内部行為者の脅威、情報漏えい、ハクティビズム、高いモチベーションを持つ行為者による標的型攻撃など、様々なサイバー犯罪への対応経験を有しています。KPMGのサービスには、オンデマンドでの悪意あるコードの分析、ホストおよび全社ベースのフォレンジック、ネットワークフォレンジック、脅威インテリジェンスなどが含まれます。

また、KPMGは情報セキュリティのコミュニティーにも深く関わっています。このことにより、アドバイザーとしての役割の一環で、新たな問題に対する知見を迅速に得ることができるのです。実践的なアドバイスとKPMGが提供できるサービスは、他のお客様に提供した様々な規模、範囲、複雑性のあるサービスの経験から成り立っています。

KPMGは、多くの企業の社内チームに対し、優先的なプロバイダーとしてデジタルレスポンスサービスを提供しています。最後になりますが、KPMGは、特定のツールに依存することなく、中立の立場にあります。KPMGは、お客様の類似組織における多くの経験や、価値ある支援を提供できると確信するに足る能力によって、お客様が安心のできるサービスを提供します。

サイバーレスポンスサービス

デジタル調査

ネットワークへの不正侵入－KPMGは、最高峰の技術を有するサイバー犯罪組織によるネットワークへの不正侵入や、内部者が関わるサイバー犯罪などの調査及び対処を専門としています。こうした調査の目的は主に、攻撃者の特定、攻撃および被害範囲の特定、犯行の対象となったデータの特定、脅威の阻止と除去に必要となる施策、ネットワークを保護し、潜在的な侵入行為から回復させるために必要なアプローチを決定することです。

サイバー攻撃による知的財産（IP）の盗難－かつては、知財を窃取するためには、極秘の計画や方策が収納されたキャビネットをくまなく探す必要がありました。デジタル化時代の到来により、企業秘密争奪の場は、ハッキングや外部記憶媒体へと移りました。KPMGのサイバー調査専門家は、知財窃取の一般的な手法を解明するだけでなく、何が、いつ、どのような方法で誰により窃取されたのかを解明することに精通しています。

ボットネットとマルウェアコード－KPMGは、マルウェアコードの構造解析、挙動調査、報告機能、攻撃の痕跡など、自動および手動によるリバースエンジニアリングの経験を有しています。KPMGのインシデントレスポンスチームは、マルウェアを抑制し、根絶するための手がかりを見つけ出し、迅速に感染した環境全体を一掃する能力を有します。

スピアフィッシング－標的型攻撃は、人事部門や財務部門など、重要な情報にアクセスが可能な役員や従業員に狙いを定めています。対象者を騙して重要な情報を漏えいさせるため、あるいは他の活動の遂行、悪意のあるWEBサイトへの誘導や、犯罪組織への不正送金などを目的として、内部情報を利用して巧妙に偽装された電子メールが対象者に送信されます。KPMGの経験豊かなチームは、初期の侵入ポイントや他に被害に遭っている可能性のある人たちを見つけ出すため、偽装電子メールを分析・追跡することができます。

中立かつ裁判所で証言できるサイバー調査専門家－一般的に、技術的な問題に直面した場合には、独立した意見が必要となります。KPMGのサイバー調査専門家は、複雑な技術的課題について説明し、混乱を避けるための客観的な手続きを策定する経験を有しています。我々のチームは、法的なプロセスについて理解し、そこでは、真に公正で偏りの無い意見が必要とされることを熟知しています。

サイバー調査専門家による証言（フォレンジック専門家との協調）－訴訟を抱える依頼人にとって、訴訟における長年の経験を持つ各分野のKPMGの専門家が、総力を結集して行う高度な分析とその報告書は、一考する価値があります。KPMGが擁する豊富な人材の中から、訴訟相手の専門家に対抗するための最適な専門家を選定し、プロフィールを提供します。

人材派遣－KPMGが、お客様のチームの一部として機能します。KPMGから、お客様の監督下でご活用頂くための人材を派遣します。繁忙期の業務支援や大規模なインシデントの対応から、特定の専門知識のご提供にいたるまで、お客様を支援します。

サイバーレスポンス・オンデマンドサービス

KPMGのサイバーレスポンス・オンデマンドサービスは、KPMGの多様なサイバーサービスを1つのパッケージにまとめたカスタムメイドのサービスです。KPMGのオンデマンドサービスは、お客様のリスクを軽減しながらお客様にとっての脅威情報を事前に提供するものであり、長期的なサイバーレスポンス機能の強化にフォーカスしつつ、KPMGのノウハウや専門家のアドバイスを提供します。

お客様で多くの人材を抱えなくとも、KPMGとのオンコール契約により、直接またはリモートで、優秀な人材による迅速な対応を、保証時間内に受けることができます。サービスの一環として、KPMGのサイバーチームは、お客様における潜在的なリスクに備え、お客様の関係者とディスカッションを行う、カスタマイズされたオリエンテーションプロセス（例：2〜3日間のミーティング）を提供します。

このオリエンテーションプロセスは、お客様がKPMGのサイバーレスポンス・オンデマンドサービスを有効に活用し、必要となった際にはKPMGのサイバーチームが効率的に活動できるようにすることを目的としています。オリエンテーションプロセスを通じて得られたお客様のビジネスやインフラに関する知見は、実際にインシデントが発生した際に、詳細な背景情報や初期打合せなしに直ちにインシデント対応プロセスを開始するのに役立ちます。

KPMG

デジタル戦略

サイバー・プリビレッジ・コンサルティング（フォレンジック専門家との協調）ー企業間の紛争は、今日の競争市場においては日常的なものです。KPMGは、随時発見される有意義な情報を保護しながら、お客様の訴訟前の事実調査を定常的に支援します。文書毀損の主張、誰がいつ何を知ったのか、どれぐらい遡ることができるのか等、どのような問題に関しても、KPMGの事実調査チームは、お客様が重要な判断を下すために必要な情報を提供します。

サイバー机上演習ーKPMGは、経営層レベルからインシデント管理チームまでを対象とした机上のデジタルインシデント演習を主催し、ガイドすることができます。このような演習は、お客様のネットワークと業界別にカスタマイズされたデジタルインシデントをシミュレートし、組織の現在の能力をテストします。KPMGは、インシデントの開始から終了までのチームの対応能力を評価することができます。このような演習は、サイバーレスポンスチームにおいて、何ができる状態にあるかを評価し、防御能力の改善の助けとなります。

脅威情報の収集ー現状の外部ネットワークのサイバーセキュリティに対する脅威情報を評価することで、お客様のネットワーク、電子チャネル、および外部ベンダー提供の脅威情報やレッドチームテクニックを活用したコントロールの欠陥や脆弱性を洗い出します。

プロアクティブ・コンサルティングーKPMGのサイバー調査専門家の知識、経験、調査、及び開発スキルを、お客様のサイバーセキュリティに関するニーズに合致するよう、プロジェクトをカスタムメイドするために活用します。一般的なプロジェクトには、インシデントレスポンスに関する組織体制の現状評価、全社でのフォレンジックツールの評価または展開、運用を可能にするための支援またはプロセスの自動化、およびテクノロジー間の統合ポイントの構築等が含まれます。

データの特定と改善ーKPMGは、情報に基づく意思決定が可能となるよう、そして、データが適切に保護されるよう、お客様が業務上不可欠なデータを特定することを支援すると共に、不要となったデータの整理を支援します。

独立第三者的な検証と評価ー調査での発見事項、侵入の範囲、犯罪、不正のスキームや財務報告に関する独立した第三者による検証は、リーディングプラクティスであるだけではなく、状況によっては要求事項である場合もあります。KPMGが独立してテストした追跡記録は、あらゆる調査の正確性と完全性を確かなものとします。

セキュリティ侵害にかかるデューデリジェンスーお客様の買収対象企業が、ハッキングされたことはありませんか？お客様のネットワークに、隠れた問題はありませんか？外部ベンダーの脅威インテリジェンスと内部システムのレビューに基づいた外部及び内部の脅威評価メソドロジーを活用し、KPMGはこうしたリスクの低減を、客観的な立場から支援することができます。

デジタルフォレンジックにかかる規律

デジタル証拠保全ーKPMGは、あらゆる電子メディアに対応した業界最高水準の証拠収集、保全手法を活用します。全ての証拠取得は、証拠保全の一貫性（chain-of-custody）、証拠の真正性、暗号化、証拠の追跡を含むKPMGの証拠取扱手続に則り実施されます。

デジタル証拠の復元ー重要なファイルは多くの場合、削除されていたり喪失したりしています。KPMGのサイバー調査専門家は、暗号化されたファイル、失われたバックアップ、初期化されたハードディスク、ディスクアレイ等、これらに限らず、デジタルデータの特定と復元に関する経験を有しています。

ネットワークフォレンジックーKPMGは、情報収集、侵入検知と対応を目的とした、ネットワークトラフィックのリアルタイム監視と分析の経験を有しています。また、KPMGは、分離されたネットワークセグメントからグローバルエンタープライズ・ネットワークに至るまでの経験を有しています。

ホストとモバイルフォレンジックー何が起きているか説明する必要があるでしょうか？知財の盗難、「誰が言った」「言わない」といった人の問題、不適切なリソースの利用、根本原因の分析やデータ持出インシデント等、あらゆる状況に関して、KPMGのサイバー調査専門家チームは、迅速な事実の把握を支援します。KPMGは、法廷への提出の要件を満たした方法での、コンピュータ機器からのデータ収集において、業界最高水準の調査分析技術を擁しています。

メモリフォレンジックーメモリには、通常、ユーザの行動に加え、マルウェアによって仕込まれた不当なプロセスや疑わしい振る舞いの証拠が含まれます。KPMGのサイバー調査専門家は、稼働システムのメモリのトリアージと分析を成功裏に実施するために不可欠なスキルを備えています。

マルウェアコード解析ーKPMGは、マルウェアコードを静的に構造解析し、その挙動を調査し、報告機能あるいは攻撃の痕跡を報告するための、自動・手動による経験を有しています。

データベースとログ解析ーファイル一個からテラバイトのデータまで、構造化、非構造化のデータ構造を問わず、KPMGのサイバー調査専門家は、データベースのコンテンツ、メタデータ、ログについて、調査の観点からデータ分析技術を適用する、業界最高水準の経験と技術を有しています。

効率的な実施

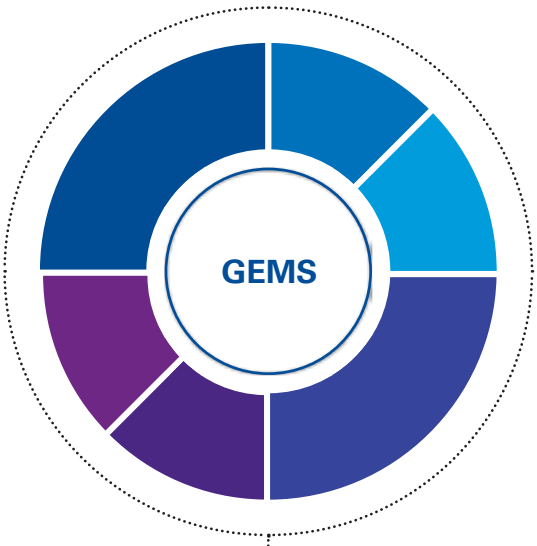
グローバル証拠管理システム（GEMS）
KPMGは、あらゆる状況に適した業界最高水準の証拠収集、保全、分析手法を利用します。証拠取得は全て、KPMGの証拠取扱手続に則り実施され、この手続きには、証拠保全の一貫性（chain-of-custody）、証拠の真正性、暗号化、物理的・論理的な証拠の追跡などが含まれます。

KPMGは、法廷での不利な判決を避けるため、弁護に資する監査証跡を提供するとともに、大量かつ多様なデータセットの取り扱い、予算のコントロール、プロジェクトのスケジュール調整など、効率的な証拠管理の重要性を理解しています。

KPMGは、証拠の追跡をインシデントレスポンスのプロセスに組み込むべきであると考えています。これにより、プロジェクトの全工程を通じて、全てのデータの正確性、効率性、認知が確実なものとなります。

ツールに依存しない
KPMGは、特定のツールに依存することなく、中立の立場にあります。KPMGは、お客様の類似組織における多くの経験や、価値ある支援を提供できると確信するに足る能力によって、お客様が安心のできるサービスを提供します。

KPMGは、あらゆる規模、複雑なインシデントへの対応に、十分に備えています。KPMGのサイバー調査専門家は、デジタルフォレンジック・ラボの能力をお客様の組織に持ち込むことができます。また、これによりお客様はインシデント発生の間、機微な情報を自社外に出す必要がないという点も安心です。



KPMGグローバル証拠管理システム（GEMS）

サイバー調査キット

KPMGデジタルレスポンスサービスのサイバー調査専門家は、カスタムラップトップ、フォレンジックイメージング機器、多くのフォレンジックツールのライセンスはじめとする幅広いツールを使用することができます。しかしながら、これらのツールは、時として様々な企業でのインシデントへの対応、大量のデータ分析、求められる期限によっては、適していないことがあります。

そのためKPMGデジタルレスポンスサービスは、機密データをインシデントの最中に施設から持ち出すことなく分析できる点で、お客様にとって安心です。KPMGには、インシデント時にオンデマンドで利用可能な2種類の対応サービス（ラボとサーバー）があります。

ラボ・バージョンは、ラボにあるサーバーに接続されたネットワークストレージデバイスとで構成されています。これにより、「ウォールーム」環境で働くサイバー調査専門家は証拠の保管を一元化し、処理や分析のためにサーバーのリソースを活用することができます。サイバー調査専門家は、仮想化技術を用いて一つの証拠を並行して共同作業することができ、必要に応じた環境を作成することで、独自のニーズに柔軟に対応します。

このような環境を使用することで、サイバー調査専門家はフォレンジック・ラボに居るかのように、完全に保護・隔離されたネットワークで、徹底的に作業することができます。

KPMG は情報セキュリティコンサルティングのリーダーとして認知されています。

戦略的アドバイス、対象分野の専門知識、柔軟性とコミットメントの提供における強みについてお客様から認められています。

KPMG インターナショナルは、Forrester Research Inc. レポート、Forrester WaveTM：2016 年第 1 四半期において、最高得点を獲得し、情報セキュリティコンサルティングサービスのリーダーに選ばれました。

Forrester の報告書によれば、KPMG は、戦略的アドバイス、専門知識、柔軟性と適応性、コミットメントを強みとして、お客様から認められています。

コンサルティングサービス以外でも、大企業からは、I-4 組織のオーナーシップについて、優れたピアツーピア・ネットワーキングの機会を提供しているとして賞賛されています。

またレポートは、「KPMG は、企業の役員や技術者のセキュリティに関する問題を明確に把握している」と述べています。

出典：Forrester WaveTM：情報セキュリティコンサルティングサービス、2016 年第 1 四半期

“The Forrester Wave ™ is copyrighted by Forrester Research, Inc. Forrester and Forrester Wave ™ are trademarks of Forrester Research, Inc. The Forrester Wave ™ is a graphical representation of Forrester's call on a market and is plotted using a detailed spreadsheet with exposed scores, weightings, and comments. Forrester does not endorse any vendor, product, or service depicted in the Forrester Wave. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change.”

[2] http://www.dell.com/us/business/p/precision-t7610-workstation/fs

KPMGデジタルレスポンダー

KPMGデジタルレスポンダーについて

企業の86%が、サイバーインシデントの検知に時間がかかりすぎると言っています。KPMGは、毎年多くのお客様のサイバーインシデント対応を支援していることから、そのプロセスが難しい課題を抱えていることを認識しています。KPMGデジタルレスポンダー（KPMG Digital Responder: KDR）は、情報セキュリティ、コンプライアンス、フォレンジック、法務に係る費用を削減し、証拠の完全性を維持し、サイバーインシデントへの対応の有効性を高めるのに役立つ洗練されたアプリケーションです。以下はワークフローの例です（図1参照）。

1. KPMGデジタルレスポンダー（KDR）は、稼働中のコンピュータや既存のディスクイメージからフォレンジックに必要な証拠の収集を可能にします。それにより、ハードドライブの完全なコピーを取得する必要がなくなります。同時に、人工知能（AI）を利用してコンピュータシステム上のファイルを静的に分析し、アンチウィルスでは「検出不可能な」マルウェアを識別することもできます。そして、全ての収集データは暗号化されたパッケージに格納されます。
2. その後、暗号化されたパッケージは、セキュアなファイル転送プロトコルまたはオフラインで、KPMGのサイバー調査専門家と技術を含む最先端の研究所（Center of Excellence）であるKPMGフォレンジックオペレーションセンターに転送されます。
3. データはKPMGによって最先端のフォレンジックデータ分析手法を使って、自動処理されます。
4. KPMGサイバー調査専門家は、分析結果をレビューし、新しいインシデントの発見、インシデントの責任者、影響を受けたシステムや人、リスクにさらされている可能性のある人、その他多くの情報を素早く把握することができます。

このプロセス全体を通じて、KPMGは、業界で最先端のデータ収集および保全方法を使用しています。証拠の保全は、当社のグローバル証拠管理システム（GEMS）を使用して、証拠保全の一貫性（chain-of-custody）、証拠の真正性、暗号化、物理的・論理的証拠の追跡を含むデジタル証拠処理手順に従って処理されます。

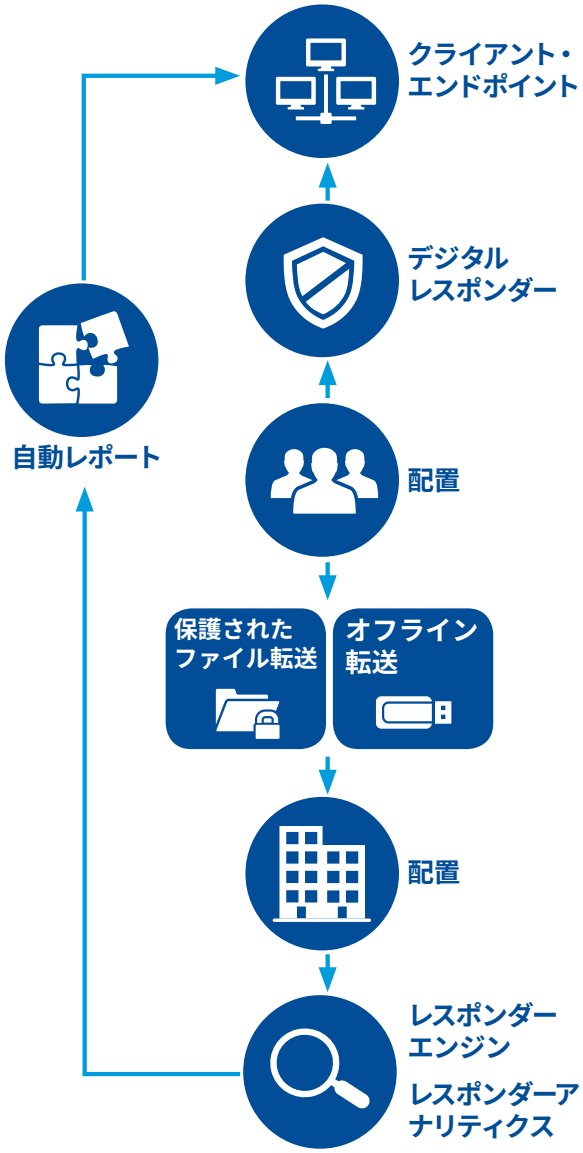


Figure 1 – For illustrative purposes only

KPMG は近年、6 つの戦略的成長イニシアチブの 1 つとしてサイバーセキュリティを挙げています。この戦略的コミットメントを強化するため、当社は R&D や買収に多額の投資をしてサービスの範囲を広げ、深めました。

– Forrester WaveTM：情報セキュリティコンサルティングサービス、2016 年第 1 四半期

[1] Source: 2014 Cost of Data Breach Study: Global Analysis and CERT Insider Threat Center

ソフトウェアの構成

レスポンダー
— ライブおよびディスクを対象としたフォレンジックデータ収集ツール

エンタープライズ・レスポンダー
— コマンドラインF-レスポンス収集ユーティリティ

レスポンダーエンジン
— フォレンジック・アーティファクト処理エンジン

レスポンダーアナリシス
— Webインターフェース、エラスティックサーチ、データ分析・報告のPythonライブラリー

事例1：退職者PCの調査・分析

人事部による最終退職面談に先立ち、ITチームがKPMGデジタルレスポンダーを実行、退職者PCの解析を行うことが可能です。

解析されたデータは暗号化されてKPMGに転送され、リムーバブルデバイス接続記録、インターネット履歴、インストールされた未承認アプリケーション、ファイルの大量削除、直近のユーザーアクティビティなどをはじめとする情報が自動的に分析されます。

これらの分析の結果はレポートにまとめられ、最終退職面談において「なぜ社用ではないリムーバブルドライブに200もの機密ファイルを転送したのですか？」、「なぜ『ファイルを安全に削除する方法』を先週検索したのですか？」「どのような目的で社外のファイル共有Webサービスを使用したのですか？」といった質問をすることが可能となります。

事例2：サイバーインシデントの原因調査

マルウェア感染の調査は、通常、稼働中のコンピュータを対象に行います。

KPMGデジタルレスポンダーを使用すれば、収集されたデータは暗号化されてKPMGに転送され、感染ベクトル、ファイル実行履歴、マルウェア分析情報、感染経路、不正アクセス履歴などをはじめとする情報が自動的に分析されます。また同時に、AIを活用してシステム上のファイルの静的分析を行うことで、従来のウイルススキャンでは「検出不能」なマルウェアを特定することも可能です。

これらの分析の結果はレポートにまとめられ、リスク低減やモニタリング、あるいは他の復旧・再発予防につなげることが可能です。

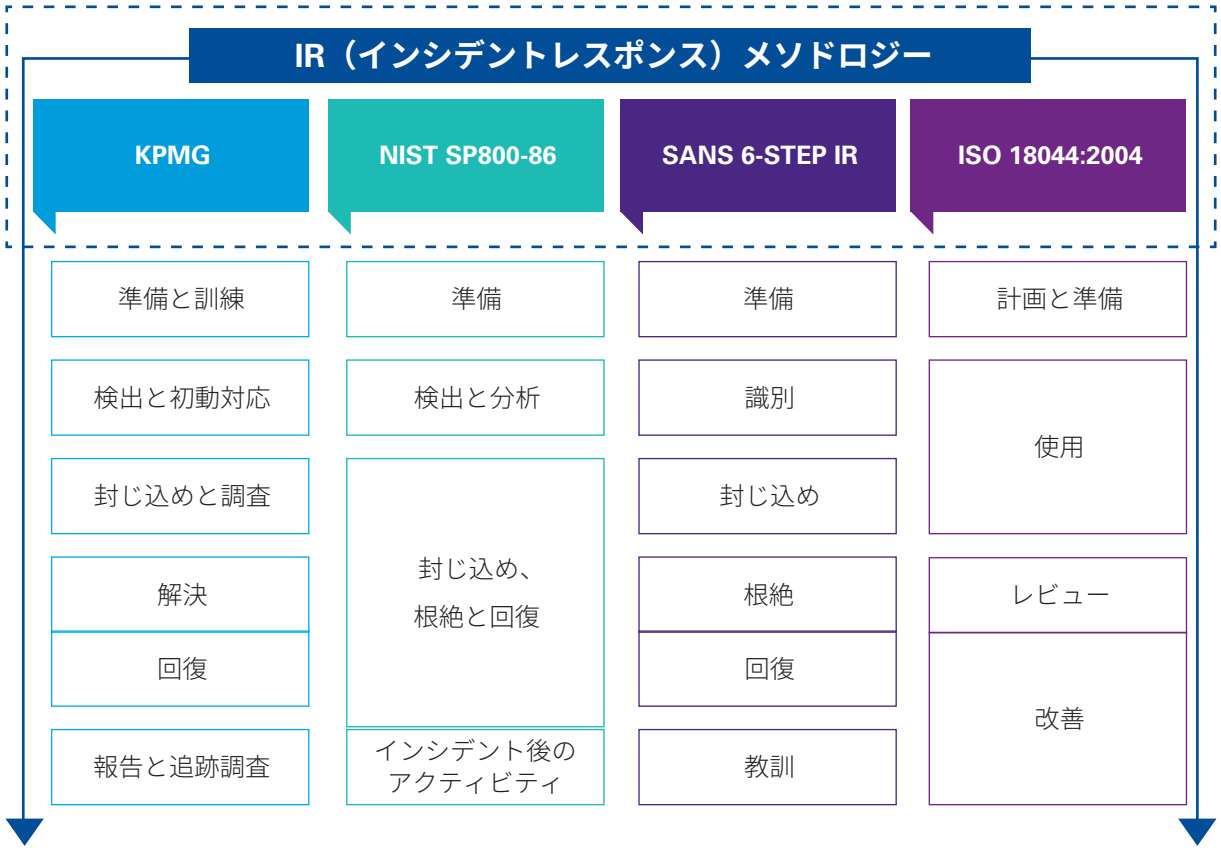
KPMGデジタルレスポンダーの各機能は、クライアントとKPMGのサイバー調査専門家の高いニーズにもとづいて実装されており、高い技術的優位性を有しています。

マルウェアへの初期対応をどのように行うかが、この新たなソリューションを理解する助けとなります。基本的には、ファイルをサンドボックスに転送するだけで、そのファイルが OS に及ぼす影響やファイルシステムの変更履歴、ネットワーク接続履歴などをはじめとする挙動についての分析結果を得ることが出来るのです。KPMG デジタルレスポンダーにより、貴社が求める情報のほぼすべてを効果的に得ることが可能であり、コンピュータシステムおよびフォレンジックに関する初期対応における機密性の高いソリューションとなっています。

– David Nides, Managing Director, KPMG Cyber

メソドロジー

KPMGのインシデントレスポンスのプロセスは、アメリカ国立標準技術研究所の特別刊行物800-86（NIST SP800-86）や国際標準化機構の刊行物18044:2004（ISO 18044:2004）、SAS Instituteにより刊行されたSix-Stepインシデントレスポンスプロセス（SANS 6 Step-IR）等、国際的に公正性・妥当性が認められたフレームワークに沿って作成されています。これらのガイドラインにより、業界のリーディングプラクティスについて、KPMGのフレームワークの網羅性を確認すると同時に、KPMGのインシデントレスポンスプロセスは、実際の現場での経験、実行性へのフォーカス、証拠に関するルール、事後フェーズでの掘り下げたテクニカルなセキュリティテストを通じて、より洗練されたものとなっています。



準備と訓練

インシデント対応に失敗する最も一般的な原因の一つは、適切な準備の欠如です。KPMGは、インシデントが発生した場合に備えた優れた対応の土台を築くために、明確なコミュニケーションライン、方針と手続、活動規則の確立において、お客様の組織を支援することができます。同時に、KPMGのチームは、最新の技術やツール、インシデントレスポンスに関するライセンスを保持しています。

検出と初期対応

このフェーズのトリガーとなるのは、テクニカルなアラート、不正の兆候、あるいは、法執行機関やインタネットサービスプロバイダー等の外部機関からの通報です。KPMGのインシデントレスポンスの専門家は、準備段階に作成された計画の実行を支援します。また、「侵入を受けているのか?」「活動は続いているのか?」「どのような潜在的な被害があるのか?」「注意喚起や報告を行う必要はあるのか?」等といった差し迫った問題への答えも提供します。

封じ込めと調査

このフェーズにおいて、KPMGは、進行中の被害を限定するための施策を試みると同時に、侵入元に関する情報や手口、侵入による影響の特定を支援します。このような取り組みは、通常、調査の実施と脅威の根絶とのバランスをとって実行されます。例えば、対応の施策として、証拠収集のために侵入行為の継続を許容する場合もあれば、被害を最小限に抑えるため、侵入行為を即時に遮断する場合もあります。

回復

このフェーズでは、調査への潜在的な影響を考慮し、あるいは単に他の作業との優先順位付けのために、実施が見送られていた除去作業を行います。この段階では、環境を平常時のオペレーション環境に戻すことに主眼が置かれます。

問題解決

このフェーズでの重要な作業は、脆弱性の評価とペネトレーションテストです。この作業は、戦術的な効果のためにインシデントレスポンスのプロセス全体を通じて発生し得るものですが、このフェーズにおいては、悪意ある活動の根本原因を特定するために徹底的にテストを実施します。このフェーズを通じて、類似事案の再発防止にあたり、技術的な施策あるいは統制環境の整備において、推奨される施策とその優先度を明らかにします。

報告と追跡調査

最終フェーズは、契約に基づく報告を行います。また、個人または集団に対する刑事・民事の訴追に関連した活動の継続的な支援を行う場合もあります。

KPMGの実績
―世界中でお客様を支援

グローバルコンサルティングファームにおけるインシデント対応支援

売上高数十億ドル規模のグローバルコンサルティング企業への不正侵入に対し、KPMGはインシデント対応サービス支援を提供することで、被害の特定、フォレンジック分析、6カ国にまたがる1万9千システムの保全を実施しました。

具体的な作業内容としては、6ヶ月間のネットワークアクティビティのパケットレベルの分析、100を超える異常バイナリについての行動・統計分析を実施しました。この分析により、KPMGは当インシデントが標的型（APT）攻撃であることを特定し、早急にお客様のネットワーク環境への潜入方法や漏えいしたデータを特定し、効果的な改善を行いました。

KPMGは、お客様のグローバルインシデント対応計画策定を支援しました。

米国の大学におけるインシデント対応支援

米国のある大学は、学内で発生していたIT関連の一連の事件の調査のために、KPMGを起用しました。

コアネットワークの分析、選択した従業員のシステム調査を実施したところ、学内ネットワークの感染と、データ漏えいの可能性があること、および上層部の大学関係者の電子メールが不正に盗み見されていたことを確認しました。

KPMGでは、脆弱性診断とリスク評価に基づいて、短期的・長期的な改善を進めるなかで過去から現在にいたる学内ネットワークの侵入が元IT担当者により実施されていた証拠を発見しました。

KPMGは米連邦検事事務所に不正侵入を行っていた者の起訴に必要な証拠を提出し、本件侵入により漏えいした可能性のある個人情報（PII）の識別、および約9万3千人の被害者に対する説明に際しての情報整理をするうえで重要な役割を果たしました。

米国の病院における電子証拠収集

継続中の訴訟における米国政府の調査支援として、KPMGは、米国における大規模な研究教育病院の一つである研究施設の書類のハードコピー及びデジタルメディアの保全を行いました。

研究施設への影響を最小限に抑え、迅速に保全作業を完了するという要求を満たすために、KPMGでは25名のフォレンジック専門家を組成し、108時間で3千9百のデジタルメディア機器からコピーした150テラバイト（TB）の電子データと500箱の書類を保全しました。収集したデジタルメディアは、病院システムの一部とBYODプログラムにおいて使用されており、Macintosh、Windows、Linuxシステム等の異なる仕様や構成が共存していました。

KPMGは、外部弁護士、社内弁護士、IT専門家や医学研究者と連携することで、最小限の業務中断でデータを収集可能な最も効果的な方法を策定し、業界のベストプラクティスに基づいた操作手順に従い必要なデータの保全を実施しました。

KPMGは、お客様の期待を満たすためにカスタマイズされた方法論を策定し、その方法に従い、各管理者、研究所、医療機器、外部メディア、ネットワーク共有、個人共有、電子メールサーバー、およびハードコピー文書から業界最先端の独自のフォレンジック手法を活用しデータ保全を実施しました。

KPMG

グローバルオンライン小売企業におけるインシデント対応支援

グローバルに事業を展開するオンライン小売企業では、VPNの乗っ取りに加え認証情報が窃取されたことにより、ネットワークから大量のユーザアカウント情報が窃取され、史上最大規模の漏えい事件が発生しました。

インシデント発生時は、他のセキュリティベンダーが調査を実施しましたが、お客様はその調査だけに限らずに、デジタル証拠の保全・分析、復旧計画・危機管理の支援、データ分析、およびセキュリティ監視などのより包括的なアプローチが必要であると認識し、KPMGに調査を依頼しました。

KPMGのチームは、お客様のご依頼から4時間以内に目に見える成果を上げ、48時間以内には現場にチームメンバー全員が集結し対応に当たりました。

インシデントの漏えい範囲を調査するため、企業の数万台のコンピュータにセキュリティエージェントを導入し、さらに、米国、英国、アイルランド、ドイツ、インドに分散する100以上のシステムを保全・調査した結果、KPMGのチームは1億人以上の顧客レコードが詐取されていたことを確認しました。

KPMGは、対策本部を支援し、お客様の社外弁護士と連携するなど重要な役割を務めただけでなく、お客様の危機計画・管理のハブとして、インシデント発生期間の24時間サポートを提供しました。また、セキュリティ監視チームと共に分散していた多数のログを収集し、相関分析により攻撃の兆候を特定する機能を開発することでセキュリティ監視（IOC）の高度化を実現しました。さらに対策本部では、経営陣、メディア、及び米国議会への報告書作成を支援しました。

インシデント対応後、KPMGはお客様における更なる態勢改善に向けた取り組みを支援しました。主な取り組みは、監視機能の追加開発、分析能力の向上、認証アクセス管理基盤とプロセスの導入、インシデント対応マニュアルの改訂、パスワードを必要としない次世代認証機能の検討、週次のサイバー脅威レポートと打ち合わせ、およびデジタルフォレンジック・ラボの再構築等であり、これらの実現によりお客様における重要な対策の実施や機能の向上を図りました。

グローバル保険会社におけるインシデント対応支援

KPMGは、FBIよりデータ漏えいの通知を受けたお客様に対し、サイバーセキュリティの調査支援をしました。

限定された情報の中で、まず外部サーバーに接しているお客様のネットワークをスキャンし、24時間の監視体制を構築しました。さらに、主なシステムの脆弱性評価とネットワークログにおける異常分析、外部情報に基づいた調査を実施することで感染したシステムの特定に至りました。

調査においては、VNCの悪用により感染したホストの発見に加えて、本調査とは直接的には関係がないお客様の環境における脆弱性を特定することができました。

KPMGの支援により、お客様のセキュリティ環境は全体的に劇的な改善を実現しました。また入手した証拠が、適切な法的手段を通じて政府に提供されたことで、データ漏えい事件の容疑者は逮捕され、数年の服役と3百万ドルの支払いを命じられました。

グローバルな投資会社―ニューラルエキスパート

2つの投資会社に関する問題において、KPMGがニューラルエキスパートに任命されました。KPMGは、高速金融取引プラットフォームからの「ソースコード」盗難の疑惑を取り巻く両社のデータに関するデジタルフォレンジック分析を依頼されました。KPMGは、9テラバイトのデータを分析して処理し、裁判所が公布した手順に従って両社と結果を共有しました。KPMGは、削除された情報を見つけるために未割り当ての空き領域を広範に分析しました。KPMGは、両社に対し、回収された未割り当てクラスタをレビューするプロセスを開発するよう助言し、協力しました。KPMGはまた、特権IDのログの生成や関連文書の作成など、データのレビューにおいて両社を支援しました。

重要インフラ事業会社の標的型攻撃（APT）調査

標的型攻撃によって社内管理する業務用Webサーバーがマルウェアに感染し、外部からの不正アクセスが行われました。

KPMGは依頼を受け、通信ログとサーバーのフォレンジック分析を実施しました。その結果、行為者は海外拠点のIPアドレスから不正ログインし、ファイル・コマンドを遠隔操作することでWebサーバーのデータ領域をすべて暗号化し機能不全に陥れた事が判明しました。

また、暗号化プロセスをリバースエンジニアし、キャッシュ情報から複合パスワードを抽出し、データ領域の復元に成功しました。

最終的には、短期間のダウンタイムでインシデントから回復することができました。さらにKPMGは継続的な再発防止の支援をしました。

政府機関に対するサイバーインシデント調査

日本の組織をターゲットとして大規模な標的型攻撃が発生し、政府機関でも不正侵入が疑われていました。KPMGは依頼を受け、簡易的なフォレンジックを実施し、不正な通信ログから組織内ネットワーク上に外部からの不正アクセスを確認しました。

そのため、より詳細なフォレンジック調査として、重要機密情報の漏えい痕跡調査、漏えい情報の特定、バックドア等のマルウェア感染有無の確認等の調査と分析を実施しました。

その結果、職員がメールに添付されているファイルを開封した際にPCがウイルスに感染したことが判明しました。このPCが組織内LANに接続されたことで、マルウェアは細分化された複数の個人情報データにアクセスに成功、個人情報を圧縮、転送した痕跡が確認されました。

海外子会社で発生したセキュリティ・インシデント調査

IT技術者が常駐しないお客様の海外子会社から取引先に不正な通信が発生し発覚しました。現地ベンダーとの連携が混乱を招く中、日本と現地のKPMGサイバー調査専門家がヒアリング内容をもとに調査スコープを定め、その後の調査・解析に必要な情報等の現場確保を実施しました。

マルウェア感染が確認され同ネットワーク上のPCすべてのデータ保全を行い被害拡大防止のための救急施策を実施しました。

さらに詳細な本調査へ移行し、原因、手法、漏えいの事実確認を行い、再発防止対策を支援しました。

Contact us

KPMG FAS サイバー緊急ホットライン
T: 03-3548-5550
E: FAS-CyberResponse@jp.kpmg.com

kpmg.com/jp/cyber

www.kpmg.com/jp
kpmg.com/jp/socialmedia