信託セミナー

近年のサイバー被害動向とインシデントへの心構え

KPMG コンサルティング株式会社執行役員／パートナー　薩　摩　貴　人

— 目　次 —

はじめに

私は KPMG コンサルティングにおいて、執行役員／パートナーとして、サイバーセキュリティを担当しています。その中でも主に金融セクターを担当し、金融のサイバーセキュリティに関するビジネスを統括しています。また、サービスとしては、サイバーセキュリティの中でもサイバーレスポンス、つまりインシデントレスポンスや CSIRT（Computer Security Incident Response Team、コンピューター・セキュリティ・インシデント対応チーム）や TLPT（Threat Led Penetration Test、脅威ベースペネトレーションテスト）の支援に携わっています。

1．近年のサイバー被害動向

⑴ KPMG サイバーセキュリティサーベイ2022の結果

まず、近年のサイバー被害動向について説明します。資料４頁は弊社が2022年に実施したサーベイの結果です。なお、本年２月末頃にサイバーセキュリティサーベイ2024を新たに公開する予定ですので、是非ご覧いただければと思います。

2022年当時の情報ではありますが、サイバーインシデントあるいは不正な侵入の痕跡を確認している企業が30％にのぼっています。前回実施時の割合は20％でしたので、サイバーインシデントの被害は着実に増えてきてい

ます。

サイバー攻撃による被害の内訳は、ランサムウェアが１位であり、その他マルウェア感染、DDoS 攻撃など、さまざまな被害が発生しています。これにより実際に発生した被害の内容としては、経済的な損失の発生、自社の業務システムの著しい遅延・中断といったものが多くなっています。また、顧客や取引先の個人情報の漏洩など、個人情報の漏洩も少なからず発生しているということが伺えると思います。

インシデントが発生したという回答があったうちの半数以上、52.8%においては、経済的な損失が発生したということが明らかになっています。経済的な損失の規模については、マジョリティは100万円から1,000万円というところでしたが、1,000万円から１億円、ないしは１億円から10億円という回答もあり、内容と規模によってサイバーインシデントの経済的な損失がかなり大きくなっています。

⑵　ランサムウェア被害の事例

国内組織が公表したランサムウェア被害について説明します。2023年６月から急に国内のランサムの被害が増加しています。業種についてはさまざまですが、一部金融機関も被害の対象になっています。金融機関は今まではあまりランサムウェアの被害が語られてこなかったところですが、いよいよかという状況を感じています。

具体的な被害として、自社がランサムの被害に遭うということだけではなく、委託先やサードパーティがランサムウェアの被害に遭ってしまい、そこに預託していた個人情報あるいは機密の情報が脅かされるということで、委託元が対応に追われたという事案がありました。

これは昨年から大きな論点になってきたと思いますが、特にファイルを共有するサービスなどを利用している場合、ファイル共有のサービスが攻撃を受けて間接的に被害を受ける、言うなれば間接的に脅迫されることで、実際に影響を受けたデータは委託元である自社の資産であるため、間接的な被害であっても直接的に対応しなければならないというケースが多々あります。ランサムウェアを通じてサードパーティリスクが大きく取り沙汰される事案であったと考えています。

また、被害への備えが機能した一方で、復旧作業時に課題が明らかになったケースもあります。ランサムウェアに感染すると、暗号化をしてシステムを止め、それによってビジネスを止めさせることに加えて、窃取した情報を公開するぞと脅かす二重脅迫という被害に遭うことがあります。機密性と可用性の両方を脅かされることへの対応は非常に難しいものですが、可用性の対策としては、バックアップが非常に重要になります。

ただし、バックアップの環境もしっかりと整えておかないと、バックアップ自体が暗号化されてしまい復旧できなくなることもあるため、実環境におけるバックアップの持ち方が、昨今企業において見直しされているところかと思います。

海外の事例では、顧客情報、システムデータ、バックアップデータの全てが暗号化された挙句、脅迫をされた企業が、その脅迫に対して身代金の支払いを拒否したことがありました。支払いを拒否したことによって、全てを失うことになったわけですが、このような対応の背景には、事業が継続できなくなってもやむを得ないといった、非常に大きな意思

決定があったものと思われます。最近は、世界的に協調してランサムウェア被害の身代金を支払わないことによって、犯罪集団の活動を根絶やしにしていくことが求められていますが、そのことを踏まえて身代金を支払わないことを決断した事案として、ビッグニュースになりました。

このように、復旧できないことのリスクがかなり大きくなっていることもあり、ランサムウェアに侵入されないようにすることはもちろん、「サイバーレジリエンス」とも表現される、侵入された後にいかに回復するかということが非常に重要になります。個人情報に関しても、漏洩だけではなく、当然ながら改ざん、滅失についても対策を講じる責任があるので、ランサムウェアの被害に対しては個人情報保護の観点からもしっかりと対応していかなければいけない事象と理解しています。

⑶　ランサムグループの摘発

ランサムグループの摘発については、世界的に協調した動きがあり、ランサム集団に対して断固たる姿勢を堅持することが求められています。金融機関や重要インフラをはじめ、企業においても、実際にランサムウェアの被害に遭って脅迫された場合にどう対応するかということをポリシーとして策定する事例が増えてきています。資料５頁にも記載のとおり、基本的な考え方としては、ランサム被害を撲滅するという世界的な行動を理解し、それに協調して、ランサム集団に対して断固たる姿勢を取っていくということは、持続可能な社会、サステナビリティを実現するために課せられた社会的責務であるとされています。最近、企業にはサステナビリティが求められてきていますが、ランサムウェアへの対策もその一環として認識していただくことが非常に重要であると考えています。本日ご参加の金融機関におかれても、実際に被害に遭った場合に対応できるポリシーがあるか、策定する必要があるかということを是非お考えいただければと思います。

ランサムグループを撲滅するための世界的な活動としては、米国の FBI 等の各国の捜査機関・司法機関が連携して摘発の活動を活発化させています。2022年にはランサムグループの REvil が摘発されて、解体に至りました。2023年１月には、Hive と呼ばれる巨大組織に対して摘発の手が及びました。また2023年10月にも、老舗のランサムグループである RagnarLocker が、国際共同捜査活動によって摘発されました。このように、撲滅のための行動は世界的に行われていますが、各企業においても、これを後押しするために、脅迫されても金銭を支払わないこと、支払わないためには平時に何を準備しておく必要があるかということを是非検討いただきたいと思います。

次に、「ransomwatch（ランサムウォッチ）」と呼ばれるサイトを紹介します。ランサムグループは窃取したデータを公開することについて、窃取された企業等を脅迫する手口を取りますが、「ransomwatch（ランサムウォッチ）」は、ランサムグループが窃取したデータを公開する「リークサイト」をウォッチしているサイトとご理解ください。

例えば、昨日２月１日には14件、１月31日には19件の情報がリークサイトに公開されています。つまり、日本を含む世界中のどこかの企業が、毎日10～20件ほど被害を受け、リークサイトに情報が公開されていることにな

ります。年間にして、3,600件程の組織が被害を受けていると考えると、他人事ではないことが理解できると思います。また、リークサイトに公開されていない被害も考慮すると、年間で5,000件程の被害が発生していると推測できます。このような被害件数の中に自社が含まれないよう未然防止に取り組むこと、発生したときの対応についても準備しておくことが、社会的責務、説明責任という観点からも不可欠です。

2. インシデントへの心構え

⑴ インシデント対応態勢・危機管理態勢の重要性

ここからは、インシデントへの心構えについて説明します。本日ご参加の金融機関においても、資料７頁のとおり、インシデントが発生したときには、インシデント対応態勢として、CSIRT が即時に対応することで被害の拡大を防止し、経営ダメージが生じる段階になれば、危機管理態勢に移行して経営のダメージを最小化して社会的信用を維持することになっていると思います。インシデント対応態勢から危機管理態勢へのフェーズの移行は各社各様で、その成熟度も様々です。インシデントが発生していない、経験がない組織は、フェーズの切替の段階で混乱することがあります。それぞれの役割が異なることを理解し、インシデント対応態勢だけではなく、経営を巻き込んだ危機管理態勢の訓練を実施することが非常に重要です。

⑵ インシデント対応における重要ポイント

資料８頁のとおり、インシデント対応にはプロセスがあります。まずはインシデント発生の可能性があるイベントを検知して、それに対して応急措置をしながら、対応方針を考えます。ここではあまり時間をかけず、迅速に対応方針を決めて必要な情報を至急収集します。

次に、被害拡大を止める封じ込めの作業に移ります。ネットワークの遮断や、ビジネスの停止を検討する必要が生じることもあるので、封じ込めには英断が求められます。封じ込めをした後、問題分析・問題点の除去・修復作業を行います。

続いて、経営への説明、対外的な説明が求められます。当然、当局への説明責任もあるため、証拠を保全して詳細を分析するフォレンジックを行い、実際に何が起こったのかを説明する手続きが必要となります。

その後、回復作業を行います。これは元の状態に戻すということだけでなく、インシデントによって組織の信頼を損なった場合においては、その信頼を回復することもこれに含まれることもあります。その後、再発防止策の策定のために問題分析を行うことが必要になります。

資料８頁には、経営が意識すべき事項も記載していますが、要となるのは迅速に打ち手を徹底していく意思決定と、監督官庁・関係会社とのコミュニケーションです。実際に発生した事象については、適切に情報をコントロールするといったことも必要です。そして関係各所への説明や、その恒久的な対策のための投資の意思決定など、経営が意識しなければならないことがあるため、インシデントレスポンスにおいてどのように対応していくかという基本方針を予め決めておくことは、非常に重要なことです。

⑶ ランサムウェア攻撃発生時の対応

次にランサムウェア攻撃発生時の対応について、資料９頁に基づいて説明します。特にランサムウェアが発生すると、一般的なインシデントレスポンスに比べ、特殊な動きが必要です。ランサムウェアにおいては、脅迫自体が詐称である場合もあるため、脅迫された内容が事実であることをまず確認することが必須です。

脅迫内容は「いつまでにいくら支払え」といった、金銭目的のものが非常に多くなっています。多くの場合､金銭は日本円ではなく、ビットコインなどで支払うことが求められるため、支払い方について考えておくことも事前の対応として考えられますし、支払わないというポリシーを策定している企業もあります。

事実を確認した後、被害範囲を特定し、緊急対策本部を立ち上げて、封じ込めを行うことなどが考えられます。例えば、二重脅迫型のランサムウェアであれば、情報を窃取されて、それを公開するぞと脅かされている被害と、暗号化されてシステムが止まり、それによってビジネスが停止し可用性が脅かされている被害の二つの側面があるため、これらに同時に対応していくことが求められます。したがって、情報漏洩の観点においては、コンプライアンス部門などとの対応協議が必要になります｡システムの復旧の対応においては、システム部門と連携をしながら進めていくということが求められてきます。

続いて、インシデントの発生について、警察への相談・届出を行い、個人情報の漏洩の可能性がある場合には監督官庁あるいは信託協会にいち早く報告することが求められます。身代金の支払い等の対応については、リーガル的な判断が求められてくるので、弁護士等の専門家に相談する必要があります。

また、サイバーインシデント全般にかかわるところですが、保険会社にも相談する必要があります。ただし、ランサムウェアの身代金に対しては、日本のサイバー保険会社は、ランサムウェアによる身代金要求に対し屈しない姿勢をとっており、保険金も支払対象外であることが多い点はご理解いただく必要があります。

加えて、社外公表の検討が必要です。どのタイミングで何を伝えるのかは非常に重要な論点ですが、セオリーとしては、遅滞なくランサムウェアの被害を受けたことを公表するべきかと思います。ランサムウェアであるということをどこまで伝えていくかは、その時々の状況によって判断していくことが重要かと思いますが、リークサイトで公表されてしまうと、あまり情報を出さないで隠ぺいしていると捉えられるおそれがあるため、透明性をもって伝えることも一つの戦略として重要な論点かと考えています。

⑷ 緊急事態における経営判断

緊急事態における経営判断について説明します。資料10頁に記載のとおり、緊急事態における経営判断では、まずは正確な状況把握が必要です。サイバーインシデントは、初期段階では情報量が足りず、雲をつかむような状況ですので、そのような状況下において、推測も含めて事態をどのように判断していくのかということが非常に重要なポイントです。こういった判断力は一朝一夕に身につくものではないため、実際に被害が起こった場合を想定して、訓練をしておくことが重要だと思います。

また、顧客・従業員・関係者の安全・利益確保も必要です。例えば、パスポートの情報などが窃取されていた場合、悪用防止のためにパスポートの切替等の対応も迅速に行う必要があります。どのような情報が漏洩したのか、情報が漏れ出したことによる二次被害として何が考えられるか、そのための対応を取ることも重要です。加えて、身代金の支払いについて、支払わないと決めておくのか、条件次第では支払うこともあり得るのか、リーガルの観点からも検討しておく必要があろうかと思います。

サービスの一時停止・システムの復旧についても、データをバックアップから戻すだけでは十分ではない可能性があるため、BCP等に照らし合わせて対応を考える必要があります。

また、グループ会社、当局、あるいは信託協会への報告と対外広報を行うことも求められます。どのタイミングでどのような情報を公表するのか、初期段階で判断していく必要があります。

⑸　当局等への報告に関する規制等

資料11頁に記載のとおり、金融庁では、不審な動きを把握した場合は速やかに報告することを求めています。また、経済産業省が所管するビジネスをされる社においても、同じく速やかに報告することを求められ、総務省では重大事故発生後、速やかに報告することを求めています。「速やか」の基準ですが、「1時間以内」を目途に判断するとよいかと思います。何かが発生した際には、翌日に報告となると相当遅く、発生後２～３時間で報告することが求められると認識しています。

シンガポール金融管理局（MAS）では、発生から１時間以内に報告することを義務付けています。１時間以内の報告ができるような体制を取っておくことは、レギュレーションとしても非常に高いレベルが求められます。

米国証券取引委員会（SEC）では、最近、レギュレーション改定の報告が公開され、セキュリティインシデントでは４営業日以内の報告が求められることとなりました。

このように、疑わしき事案はまずは関係者に報告することで、協力を求めることが可能になることもあろうかと思います。ご参加の金融機関におかれても、どのタイミングで報告するのか是非ご確認ください。

⑹　犯行グループとの交渉に関する考え方

犯行グループとの交渉についても検討する必要があります。資料12頁に記載のとおり、犯行グループと交渉すること自体は、違法性はないようですが、交渉したやり取りが公開される可能性があること、やり取り自体が脅迫の材料に使用されるおそれもあります。そのため交渉を実施するか否かは慎重に検討する必要があります。

⑺　身代金の支払いに関する考え方

身代金を支払うことも、様々なコンプライアンスリスクをはらみます。資料13頁に記載のとおり、実際に身代金を支払うことは、善管注意義務違反を構成し得る可能性もあるため、情報を収集した上で合理的な判断を下すことが必須です。

具体的には、制裁の対象者に対する支払いにおいては、外国為替及び外国貿易法や、諸外国の規制等の違反に注意する必要があります。当然ながら個人情報が関連するとなれ

ば、個人情報保護法違反、あるいはGDPR（General Data Protection Regulation、EU一般データ保護規則）違反となる可能性があります。また、金融庁などと相談をした上で判断することも有効な手段です。

⑻　インシデント対応と改正個人情報保護法

次に、インシデント対応と改正個人情報保護法の関連について説明します。資料14頁に記載のとおり、改正個人情報保護法の施行により、法人への罰金の上限が１億円に引き上げられました。また、保有個人データの対象が拡大し、要配慮個人情報、財産的被害が発生する情報、故意の不正アクセスなどによる漏洩などは１件であっても報告の対象になります。何かあった場合は、個人情報保護委員会および信託協会に報告してください。

⑼　システム・データ復旧と業務復旧

資料15頁は、インシデント発生から通常業務復旧までのスケジュール例を示したものです。システム・データ復旧と業務復旧については、バックアップが戻せたとして、業務を継続する上で充分なのかどうか、平時の段階でしっかりと確認することが重要です。バックアップには、取得頻度あるいは世代の違いがあるため、バックアップの内容がどこまで安全か確認した上で、バックアップをリストアすることになりますが、その作業時間も考慮すると、バックアップのリストアが完了しても、その時点から見ると相当古い情報になっています。そこから最新の状態に更新するためには、データを遡及させる必要があります。例えば、インシデント発生後、手作業で業務を継続していた場合は、その内容をデータとして取り込むことも必要になり、完全復旧までにかなり時間がかかってしまいます。そのような点も踏まえ、果たして現行システムが耐え得る状態になっているか、RPO（Recovery Point Objective、目標復旧時点）、RTO（Recovery Time Objective、目標復旧時間）、WRT（Work Recovery Time、業務復旧時間）、MTD（Maximum Tolerable Downtime、最大許容停止時間）の観点から是非ご確認ください。

⑽　インシデント対応から得られた教訓

最後にインシデント対応から得られた教訓を資料17頁に沿って説明します。１点目は、攻撃と思われる事象に直面した場合、大抵の人は正常性バイアスが働くということです。正常性バイアスとは、自分にとって都合の悪い情報を無視する、あるいは過小評価してしまう、人間の特性のことを言います。インシデントが発生して痛い思いをした経験のある組織は「これはもう危ない、プロに任せる」といった判断もできるかと思いますが、インシデントの経験のない組織になればなるほど、被害が拡大してその火消しが相当大変になる傾向があります。インシデントの経験のない組織において、インシデントの恐ろしさを理解することは難しいところではありますが、少なくとも正常性バイアスが働きやすいということは認識いただければと思います。

２点目は、サービスを停止させることよりも、サイバー攻撃による被害を放置して拡大させることや、情報を隠ぺいすることの方が、世論は厳しいということです。この点については、現場と経営側の考え方が乖離することがあります。多くの場合、現場はサービスを停止させることは一大事だと考えているところ、経営側はサービスの停止は当然非常に重

いことであるとは認識しつつ、その後のレピュレーションリスクや金融庁等から業務改善命令を出される可能性の方が重要であると考えます。サービスを停止させるにあたっては、経営と現場がコミュニケーションをとり、お互いの認識を共有することが肝心です。

3点目は、サービスを停止させる判断よりも、サービスを再開させる判断のほうがはるかに難しいということです。言い換えればどのような状態であれば、サービスを再開させられるのかがポイントとなるということです。OA環境に被害を受けると、OA環境が安全と言えるようになるまで再開できず、1カ月程度の間、業務を再開できないということも決して珍しくありません。対応としては、代替の環境を準備して再開することや、ディザスターリカバリーのサイトを使ってサービスを継続させるということも考えられますが、その場合、実際にディザスターリカバリーのサイトが使用できるのかどうか等、事前に対応を検討しておく必要があります。

4点目は、何よりも、サイバー攻撃の被害者であるということを主張・顕示するためには、日頃の活動を対外的に説明できる状況にあることが最も重要です。これがおろそかになると、インシデント発生時に、一転して加害者として扱われてしまう場合もあります。

おわりに

本講演をきっかけにして、ご参加の金融機関におえるインシデントレスポンスの手順や訓練を今一度確認いただければと思います。以上で講演を終わらせていただきます。
ご清聴ありがとうございました。

本稿は、令和6年2月2日に開催された信託セミナーにおけるKPMGコンサルティング株式会社執行役員／パートナー　薩摩貴人氏の講演内容をとりまとめたものです。

（さつま・たかと）

〔資料〕

KPMG

一般社団法人 信託協会 御中

近年のサイバー被害動向とインシデントへの心構え

2024年2月2日
KPMGコンサルティング株式会社

近年のサイバー被害動向とインシデントへの心構え

講師紹介

薩摩 貴人

KPMGコンサルティング
執行役員／パートナー
Technology Risk Services

- KPMGコンサルティング株式会社にて、金融サイバーサービスをリード。
- 国内大手SI企業にてUNIX／Linuxエンジニアとしてインターネットデータセンター基盤等大規模システムおよびネットワークの設計・構築に携わった後、セキュリティ専門企業や監査法人系コンサルティング会社にて、一貫して情報セキュリティに関するアドバイザリー業務に従事。
- 近年は、政府機関や金融機関等重要インフラ事業者へのセキュリティ対策やCSIRT、インシデントレスポンス、脅威ベースペネトレーションテスト等を多数支援。マネジメントとテクノロジーの両面からサイバーセキュリティに関するさまざまなアドバイザリー業務を支援している。
- 資格・外部活動等
  - 公認情報システムセキュリティプロフェッショナル（CISSP）
  - 公認情報システム監査人（CISA）
  - 電気通信主任技術者（一種伝送）
  - FISC コンティンジェンシープラン改定部会委員（2005）
  - 東京都教育委員会情報セキュリティ委員会外部委員（2016、2017）
  - 金融財政事情（2019年7月8日発売号）
    「サイバー攻撃への初動対応を強化するTLPTの必要性」他多数

KPMG

01

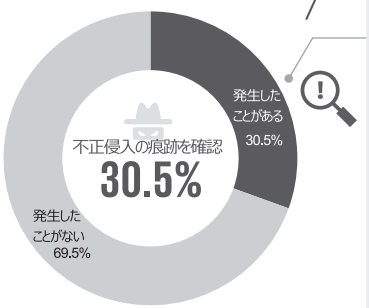
近年のサイバー被害動向

近年のサイバー被害動向

KPMGサイバーセキュリティサーベイ2022より

サイバーインシデントや不正な侵入の痕跡

30.5%がサイバーインシデントや不正な侵入の痕跡を確認している



（n=285）

サイバー攻撃による被害

26.4%でランサムウェアによる実被害が発生している

ランサムウェア	26.4%
マルウェア	25.3%
ウェブサイトの改ざん	20.7%
ウェブサービスへの不正ログインや情報窃取	20.7%
フィッシング詐欺	19.5%
DDoS（サービス妨害）攻撃	19.5%
標的型攻撃	18.4%
不正送金などを指示するビジネスメール詐欺	17.2%
ソーシャルエンジニアリング	17.2%
クラウドサービスに対する攻撃	17.2%
内部不正による情報漏洩	16.1%
IoTデバイスに対する攻撃	13.8%
その他	8.0%

（複数選択可 ／n=87）

近年のサイバー被害動向

ランサムグループの摘発

ランサムウェア被害を撲滅するための世界的な行動に同調し、ランサム集団に対して断固たる姿勢を堅持することは、持続可能な社会の実現に貢献する社会的な責務である。

- 2022年1月、ランサムグループ「REvil」に属するとされる8人の容疑者が起訴された。
- 2023年1月、ランサムグループ「Hive」の暗号化を解除する復号キーを米国司法省が取得したことで、身代金として請求されたのべ1億3,000万ドル（約170億円）の支払いが阻止された。
- 2023年10月、ランサムグループ「RagnarLocker」が国際共同捜査活動によって摘発された。

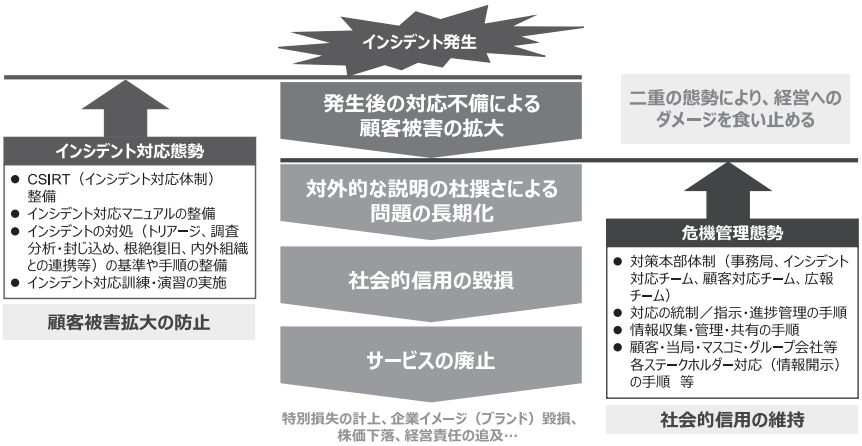
02

インシデントへの心構え

インシデントへの心構え

インシデント対応態勢・危機管理態勢の重要性

昨今のインシデントは被害が拡大し危機的状況に陥るまでのスピードが極めて速く、「被害を最小化」することを目的とした**インシデント対応態勢**と、「経営へのダメージを最小化」する**危機管理態勢**が重要となります。



インシデントへの心構え

インシデント対応における重要ポイント

ベストプラクティスとして定義されるインシデント対応プロセスに沿った組織的な行動が有事において求められる。
インシデント対応においては経営の適切な関与が必要。

インシデント対応プロセス	作業内容	経営が意識すべき事項
イベント検知	インシデント発生の可能性があるイベント（検知情報）を入手する。	・正確な状況把握に努める ・関係する役員を招集 ・インパクト、対応方法、報告に関して迅速に議論 ・打ち手の意思決定
応急措置	被害を最小化するため、運用手順で定められた対応を実施する。	
対応方針の決定	初動対応で把握された事象、被害状況、対象となるIT環境の構成等を基に侵入経路や攻撃手法等の可能性を検討し、今後の対応方針、およびフォレンジック調査の必要性を決定する。	
封じ込め・除去	攻撃の侵入経路および手法等に応じた、被害の封じ込めおよび除去を実行する。	・ビジネス影響の把握に努める ・監督官庁とのコミュニケーション ・関係会社とのコミュニケーション ・現場に対する適切な指示 ・情報のコントロール ・説明責任を果たす
証拠保全	攻撃を受けた機器、侵入経路となった機器、および侵入痕跡の特定に資するログ等のデータ保全を実施する。	
詳細分析（フォレンジック）	被害箇所、被害内容、攻撃の侵入経路、および手法等について保全したログ等を基に調査・分析し、調査報告書を作成する。	
回復	被害箇所を元の状態に復帰させる。	・関係各所に対する説明 ・レピュテーションの回復に努める ・恒久対策のための投資を意思決定
再発防止策の策定	被害発生の原因を分析し、再発を防止するための方策を検討する。	

インシデントへの心構え

ランサムウェア攻撃発生時の対応

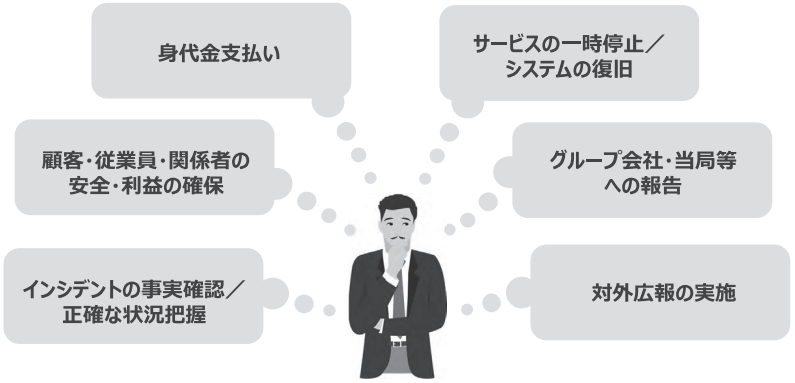
	タスク	アクション	関係組織例
検知・事実確認	兆候（脅迫）	被害部門からの情報収集 ランサムウェアの感染有無確認	JPCERT/CC、 フォレンジックベンダー等
	事実確認		
	被害範囲の特定（推定）	関連システムの所管部門の特定・周知	
社内対応	対策本部設置検討・実施	対策本部の設置検討・実施	–
	封じ込め・再発防止策の検討・実施 （侵入経路の特定・防御など）	インシデント発生の原因に対しての封じ込めなどを実施	システムベンダー　等
	復旧策の検討・実施 （応急措置対応）	予防策での対応検討、身代金支払いによる、復旧を検討	–
	ステークホルダー対応	ステークホルダーへの想定影響の検討	
社外機関を含めた対応	復旧対応の依頼・実施	外部ツールを用いた復旧の依頼・実施	セキュリティーベンダー、 情報機関
	警察への相談・届け出	刑事告訴のための事前準備（説明責任に備えて）	警察
	弁護士・専門家への相談	身代金支払い・対応策に関するリーガルチェックの確認 （平時に実施しておくことも効果的）、 犯人グループとの交渉依頼	弁護士等
	保険会社への相談	対応に係る費用についての保険金対応の可否相談	保険会社
	監督当局への報告	監督当局への脅迫の概要・対応報告	監督当局
	社外公表の検討	社外公表の是非検討・実施	弁護士・ 外部専門コンサルタント

インシデントへの心構え

緊急事態における経営判断

Question

脅迫文によって、ランサムウェア攻撃による被害発生の可能性に気付いた場合、経営者として何を考えなければならないか想像してみてください。



インシデントへの心構え

当局等への報告に関する規制等

各国当局	規制等の内容
金融庁	不審な動きを把握した場合は、速やかに報告することを求めている。
経済産業省	不審な動きを把握した場合は、速やかに報告することを求めている。
総務省	重大事故発生後、速やか（1時間以内（目安））に報告することを義務付けている。
シンガポール金融管理局（MAS：Monetary Authority of Singapore）	インシデント発見から1時間以内に報告することを義務付けている。 インシデント発見から（原則）14日以内で、根本原因および影響分析を記した報告書を提出することを義務付けている。
米国証券取引委員会（SEC：U.S. Securities and Exchange Commission）	重要と判断されたセキュリティインシデントを開示するとともに、インシデントの性質、範囲、時期、影響などを明らかにすることを義務付け。セキュリティインシデントが重大と判断されてから4営業日以内に提出することを求めている。 ただし、米国司法長官が即時の開示が国家安全保障または公共の安全に対する重大なリスクをもたらすと判断した場合は、その開示を延期することができる。
米国のランサムウェア報告法案（Ransom Disclosure Act）	すべてのランサムウェアの被害者（個人を除く）に対して、身代金の支払い後の48時間以内に、以下の情報を開示することを義務付けている。 身代金を要求された日、身代金が支払われた日、要求された身代金の金額、支払われた身代金の金額、身代金の支払いに使用された通貨（暗号通貨の種類を含む）、身代金を支払った組織が連邦資金を受け取っているかどうか、恐喝者の身元に関するあらゆる既知の情報
インドのコンピュータ緊急対応チーム（CERT-In：Indian Computer Emergency Response Team）	サービスプロバイダー、仲介業者、データセンター、法人、政府機関は、サイバーインシデントに気付いたとき、またはそのようなインシデントについて知らされたとき、6時間以内に報告することを義務付けている。

インシデントへの心構え

犯行グループとの交渉に関する考え方

ランサムウェア攻撃を受けた場合、犯行グループからの要求への対応については弁護士および専門家の助言を仰ぐことが重要。犯行グループとの交渉自体は違法ではないものの、交渉のやり取りが公開される可能性があり、脅迫の材料に使われるおそれがある。

Q3-2-2. 攻撃者と交渉を行うべきか？

通常、攻撃者と交渉を行うことは推奨されません。また、攻撃者から脅迫や提案のメッセージが届いたとしても、反応しないだけではなく交渉を検討するべきではありません。判断や対応にお困りの場合は、外部の専門機関や警察などへの相談を検討ください。

なお、攻撃者が用意するポータルやメールで交渉のために連絡を行う場合、状況によっては、攻撃者が交渉のやり取りを第三者に公開する可能性があります。また、ランサムウェアの種類によっては、被害組織と攻撃者が交渉を行うためのチャットルームを第三者が閲覧できてしまうケースがあり、身代金の交渉をしている事実が公知のものとなる恐れがあります。

侵入型ランサムウェア攻撃を受けたら読むFAQ
https://www.jpcert.or.jp/magazine/security/ransom-faq.html

国内におけるランサムウェア犯行グループとの交渉における留意点
弁護士または弁護士法人でない者は、報酬を得る目的で訴訟事件、非訟事件および審査請求、再調査の請求、再審査請求等行政庁に対する不服申立事件その他一般の法律事件に関して鑑定、代理、仲裁もしくは和解その他の法律事務を取り扱い、またはこれらの周旋をすることを業とすることができません（ただし、弁護士法または他の法律に特段の定めがある場合は、この限りではありません）。（弁護士法72条）

インシデントへの心構え

身代金の支払いに関する考え方

身代金の支払い是非にあたっては、さまざまな要素を基に慎重に判断することが求められ、安易に支払うことは善管注意義務違反を構成し得ると考えられます。制裁対象者への送金による各種法令・規則の違反を伴うおそれもあり、レピュテーションリスクや追徴金による財務リスクなど、さまざまなリスクにつながることを改めて認識しておく必要があります。

【コンプライアンスリスク】

- **善管注意義務（会社法第330条、民法第644条）違反**
- **外国為替及び外国貿易法違反**
- **OFAC（米国財務省外国資産管理局）規制違反**
- **個人情報保護法違反、GDPR違反**

【合理的判断に求められる要素例】
① 身代金を支払わずに復旧可能か
② （復旧可能な場合）復旧にかかるコスト
③ 身代金の金額と支払いによって得られると期待される効果のバランス
④ 身代金を支払ったとしても、攻撃者がデータの暗号化を解除し又は公表を中止する保証はないこと
⑤ 支払った身代金が攻撃者（犯罪者）の資金源となり、支払いの事実がランサムウェア攻撃が思惑どおりに機能していることを実証すること
⑥ 身代金の支払いは、間接的ではあるが攻撃者（犯罪者）に協力することを意味するため、当局等からそのような評価を受ける可能性があること
⑦ 身代金を支払った場合、攻撃者の「カモリスト」入りし、更なるランサムウェア攻撃を受ける可能性があること

（出典：内閣官房内閣サイバーセキュリティセンター「サイバーセキュリティ関係法令 Q&Aハンドブック Ver2.0」）

インシデントへの心構え

インシデント対応と改正個人情報保護法

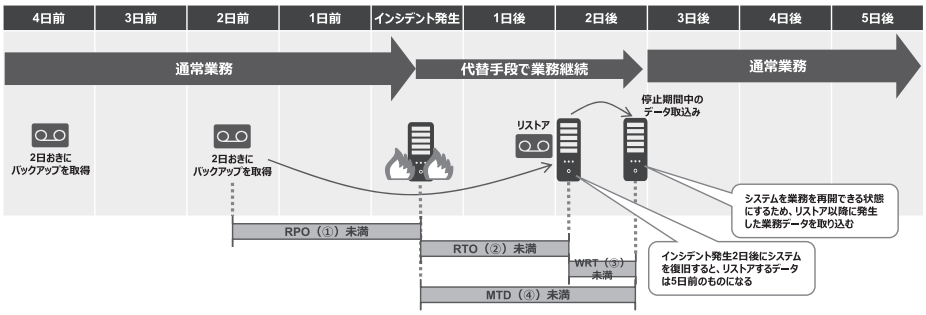
罰則・監督の強化	**法人への罰金上限の引き上げ（最大1億円）**
定義の変更・新概念の創設	**保有個人データの拡大（6ヵ月以内に消去する個人データ適用除外の撤廃）** 個人関連情報※の創設（Cookie、IPアドレス、端末固有ID等の識別子情報、位置情報、閲覧履歴、購買履歴等が該当すると考えられる） ※ 生存する個人に関する情報であって、個人情報、仮名加工情報および匿名加工情報のいずれにも該当しないもの
情報漏洩時の通知義務	**一定の類型（要配慮個人情報※1、財産的被害が発生する可能性※2、故意による漏洩※3）または一定の分量（1,000件以上）の個人データの漏洩に該当する場合等には個人情報保護委員会への報告および本人への通知が義務化。委託業務の場合は委託元にも通知の必要あり** ※1 本人の人種、信条、社会的身分、病歴、犯罪の経歴、犯罪により害を被った事実その他本人に対する不当な差別、偏見その他の不利益が生じないようにその取扱いに特に配慮を要するものとして政令で定める記述等が含まれる個人情報 ※2 クレジットカード番号やインターネットバンキングのID・パスワード等 ※3 不正アクセスや従業員による持ち出し等
個人情報保護委員会への報告内容	• 概要 • 漏洩等が発生し、または発生したおそれがある個人データの項目 • 漏洩等が発生し、または発生したおそれがある個人データに係る本人の数 • 原因 • 二次被害またはそのおそれの有無およびその内容 • 本人への対応の実施状況 • 公表の実施状況 • 再発防止のための措置 • その他参考となる事項

インシデントへの心構え

システム・データ復旧と業務復旧

バックアップからの復旧では、**いつまで（RTO）**、**どの時点（RPO）**の状態にシステムをリストアし、その後**業務を再開させるまでにどれだけの時間がかかるか（WRT）**を考慮する必要があります。それらは、事業として**許容可能な停止時間（MTD）**内に収まるように定める必要があります。

■ インシデント発生から通常業務復旧までのスケジュール（例）



①RPO（Recovery Point Objective／目標復旧時点）	リストアに用いるバックアップの取得時点。リストアを行うことにより、システムがその時点の状態にまで巻き戻る
②RTO（Recovery Time Objective／目標復旧時間）	システム復旧を終える目標のタイミング。別途、代替手段で業務を継続していた期間のデータ取込みが発生
③WRT（Work Recovery Time／業務復旧時間）	システムを業務が再開できる状態にする（停止中のデータを取り込む）時間。業務再開に向けた関係者との調整への考慮も必要
④MTD（Maximum Tolerable Downtime／最大許容停止時間）	インシデント発生から通常業務を再開させるまでの時間。この時間におさまるように復旧計画やバックアップ設計を定める

インシデントへの心構え

ランサム攻撃に遭った場合の対応のポイント

観点	ポイント
インシデントの事実確認、正確な状況把握	• 二重脅迫型の場合、データを持ち出してから暗号化が行われる • 近年ではバックアップデータを暗号化するなど、手口が巧妙化している • 暗号化は攻撃者にとってはバレやすくリスキーな処理のため、高速化が進んでいる • **最近は暗号化せずに、窃取した情報を公開することで脅迫する手口が増えている**
顧客・従業員・関係者の安全・利益の確保	• 窃取された情報に個人情報、特に**住所が含まれている場合は身の危険が及ぶおそれがある**ことから、判断が極めて困難となる場合がある
身代金支払い	• 身代金の要求は**数億円**に達する。ビットコインでの支払いが多い • 2023年2月時点で日本国内においては違法ではない。**経済産業省からは「厳に慎むべき」と通達** • **猶予期間は以前に比べて短縮化の傾向にある**。脅迫状の受領後数日以内に身代金を支払うことを求めるケースが多い（極めてビジネスライクな対応である） • 海外（米国・オーストラリア）では法制化されようとしており、犯罪者への利益供与の罪が問われることになる • 海外では交渉人を立てることが多い。交渉する目的は身代金の減額や時間の確保等。ただし、交渉人や警察に相談すると情報を公開するか売却するという脅し文句が書かれている脅迫状もある。日本国内では弁護士法により弁護士以外がこの類の交渉に立ってはならない
サービスの一時停止	• サービスを提供するシステムが攻撃を受けた場合は、被害の拡大や加害者になることを防ぐためにもサービスを止めることが賢明 • バックアップデータからデータを復旧した後、業務を再開できるために必要な作業（停止期間中のデータの取込み）にかかるリードタイムを見積もっておくことが重要
対外広報の実施	• 企業の方針によるが、**一般的に「身代金を脅迫されている」ことは公表しない** • **「不正アクセスを受けた」「情報が持ち出された可能性がある」「警察の捜査に協力している」が基本形**
グループ会社・当局等への報告	• 当局に対しては素早い報告が求められる • 被害者の立場を堅持するために、警察に被害届を出すことも考慮

インシデントへの心構え

インシデント対応から得られた教訓

01 攻撃と思われる事象に直面した場合、大抵の人は正常性バイアス※がはたらく
※自分にとって都合の悪い情報を無視したり、過小評価してしまう人の特性。「大丈夫だろう」

02 世論は、サービスを停止させることよりも、サイバー攻撃による被害を放置して拡大させることや、情報を隠すことの方に厳しい

03 サービスを停止させる判断よりも、サービスを再開させる判断の方が遥かに難しい

04 サイバー攻撃を受けた被害者であることを主張するためには、日頃の活動が最も重要である

KPMG

KPMGコンサルティング株式会社
PARTNER
薩摩 貴人
E: takato.satsuma@jp.kpmg.com