情報漏えい調査

Information breach investigation

株式会社 KPMG Forensic & Risk Advisory

KPMGは、内部不正による個人情報および機密情報漏えいの発生時に、初動対応支援、漏えいデータ、漏えい経路、行為者の特定といった調査、広報支援などのサービスを提供します。

2022年には改正個人情報保護法が施行され、個人情報の保護は企業にとって最優先課題の1つになっています。また、企業が保有する情報資産には顧客情報や従業員の個人情報のみならず、取引先情報、財務情報、製品の生産計画、仕様書、システムのソースコード等、多岐にわたります。内部統制や情報セキュリティの整備強化が進み、うっかりミスによる情報紛失や誤送信などについては、予防も対処も確立されつつある一方で、内部犯行者による深刻な情報漏えい事件も未だに後を絶たず、その対処に多くの困難を伴うのが実情です。

内部不正による個人情報・機密情報の漏えいの実態

以下に示すように、企業の従業員や委託会社などの関係者による内部犯行による重大な情報漏えい事案が多く発生しています。不正の意思を持って行為に及ぶケース以外に、従業員・内部関係者のセキュリティに関する理解の甘さや対策不備等により、誤って情報を流出させてしまうケースもあり、企業は常に内部不正による情報漏えいのリスクに晒されていると言えます。

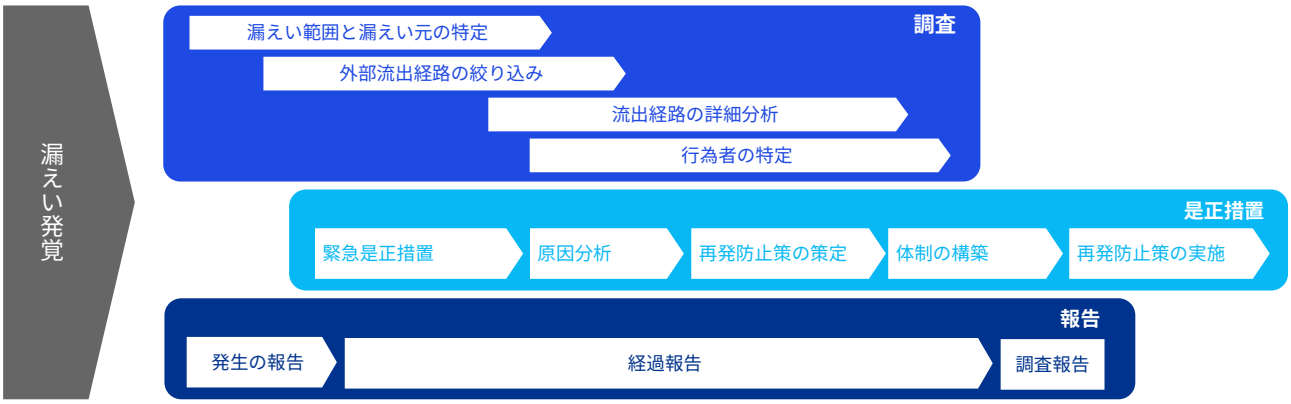
- 外部委託企業の派遣社員による個人情報持ち出し
- 技術者による転職先への研究情報提供
- システム管理者による特権アカウントを使用したデータアクセス・流出
- 個人情報を含む記憶媒体の紛失

情報漏えい発覚時の初動対応

内部犯行による重大な個人情報の漏えいは、顧客への勧誘電話・営業電話等の増加、カード不正利用の増加、外部アタックの検知、ファイル共有ネットワーク上のモニタリングなどによって発覚することが多く、ソーシャルメディア、マスメディアの報道、警察から連絡を受けて初めて知ったという事例もあります。機密情報の漏えいの場合、退職者（退職予定者）によってデータ持ち出しされるケースが多く、退職する数か月前から計画・実行され、退職後に漏えい元の顧客から情報漏洩の懸念が指摘されて発覚する等、実際の漏えいから一定の期間を経て発覚することが多いのが現状です。

社外からの情報によって漏えいが発覚した場合、情報の誤送信、コンピュータやメディアの紛失など、社内からの報告で発覚したミスによる情報漏えいとは異なり、既に恣意的に持ち出された情報が外部で流通し、具体的な被害が生じていることが多く、事態はより深刻です。こうした重大な情報漏えい事件が発覚した場合、警察へ報告するのみでなく、企業の社会的責任を全うすべく、社内でもしかるべき調査を実施し、被害者などのステークホルダーへ報告する必要があります。

情報漏えい発生後の対応



漏えいデータと漏えい元の特定

持ち出されたデータ範囲の把握と、漏えい元の特定は、想定される被害の範囲を公表するために、最優先で行うべきことです。漏えいしたデータそのものが入手できない場合には、被害報告等の分析のために、持出範囲を推定する必要があります。具体的には、情報漏えいに起因すると思われる顧客・取引先からの問い合わせや、カードの不正利用などの発生傾向および内容から、データ項目、データの並び順について、傾向と可能性を分析するといったアプローチです。なお、情報漏えいの発生を公表した後では、実際に被害を受けていない顧客からも問い合わせが多発するため、統計的分析を行う場合には留意が必要です。

被害状況から得られた情報は、社内に保存されているデータベース、データセット、データファイルのデータの並び順や項目、データ発生日時などと比較することにより、可能性のある漏えい元の範囲を限定するとともに、持ち出されたデータ範囲を限定することができる場合もあります。さらに、データベースの書き出しログ、データファイルへのアクセスログなどを調査することにより、漏えい元の候補を絞り込むことが可能です。また、定期的に更新されるデータセットが漏えい元である場合は、持出行為が行われた時期を特定できることがあります。

外部流出経路の絞り込み

内部不正により個人情報・機密情報が社外に持ち出される経路としては、下記が想定されます。
流出経路を特定するためには社用PCや携帯電話がどのように管理されているかの全容を把握する必要があります。セキュリティポリシー・ルールの順守状況や、セキュリティ管理システムの設定内容、ログ保管状況を把握することによって、流出経路が絞られ、ログ保管状況により詳細な解析が行うことができるか判断することが可能です。また、端末セキュリティ管理の徹底は、内部不正の抑止力となることも期待できる点をご留意ください。

- Web経由（webメールやクラウド上のファイル共有サービス）
- メール経由（携帯電話やPCからファイル添付の上、メール送信）
- 記憶媒体（USBフラッシュメモリや外付けHDD等の大容量記憶媒体）
- 紙媒体（必要な情報を印刷した上で持ち出し）

流出経路の詳細分析

漏えい元がある程度絞り込まれたら、社内から社外へどのような経路で持ち出されたかを特定します。漏えい経路の特定には、以下のような情報源および手法が有効と考えられます。

- データベースやシステムへのアクセスログ、コンピュータの操作ログなど、システムログ等の解析
- コンピュータやファイルサーバーのディスクイメージを対象に、漏えいデータと同パターンのデータ配列の検出
- コンピュータのレジストリー情報から、接続されたデバイスの種類、接続時期等の解析
- USBフラッシュメモリや外付けHDD、CD、DVD等の記憶媒体への書き出し記録の確認
- 電子メールの添付ファイルや本文の確認
- FTP、HTTP等の外部通信記録、外部サイトへのアクセス解析など
- サイバー攻撃による情報流出への対応（サイバーレスポンスサービスもご参照下さい）
- インターネットアクセスログ、ネットワーク通信ログ等の解析により、ファイル共有ネットワークへのアクセスの有無の確認

なお、限られた時間で、全ての調査対象を分析する事は非効率でもあるため、漏えい元や行為者の調査状況を考慮の上、調査対象の範囲や優先順位を予め決めておく必要があります。

行為者の特定

社内からの持出しが疑われる場合には、以下のような方法で行為者の特定をしていきます。

- 業務上、管理上の理由で、漏えい情報を取り扱っている、もしくは存在を認識している者の洗い出し
- 漏えい元データに対して、アクセス権を有する者の洗い出し
- 漏えい時期前後から、発覚するまでの間の退職者の洗い出し
- 漏えいが疑われる時期の勤怠記録、入退室記録、ログイン記録、アクセスログ等の確認
- 候補者および関連部署へのインタビューなど

行為者を特定する上で留意すべきことは、調査チームの組成と調査情報の統制です。情報漏えいの調査にあたっては、業務およびシステムに精通したメンバーが欠かせませんが、漏えいデータの所在の認識、システムへの精通、アクセス権などの点から調査対象者を選定した場合、往々にして調査協力者と調査対象者が重なることになります。また、コンピュータやメールの調査等のプライバシーの問題等を考慮し、早い段階で外部の調査専門会社への依頼することが推奨されます。

情報漏えい調査における留意事項

以下に挙げる項目は、情報漏えいの調査を行う上で困難やミスが生じやすく、調査の進捗や企業の信頼回復に影響を与えることがあり、特に留意が必要なポイントです。

証拠保全

限られた時間で調査している状況では、漏えい経路となったと疑われるコンピュータが特定でき次第、直ちにそのコンピュータを起動し、漏えいデータの痕跡が残されていないか確かめたくなりませんか。

調査分析の前には必ず証拠保全の手続きを踏む必要があります。コンピュータの場合は、ハードディスクのイメージコピーを2本取得し、1本を証拠保全用に保管し、もう1本を分析対象とします。サーバー等では、定期的なバックアップテープのデータからコピーを取得することも有効です。証拠保全の手続きを行わずに調査を実施した場合、さまざまな問題が生じることになります。例えば、情報漏えい経路であるコンピュータを、あわてて立ち上げて分析したために、調査行為によってハードディスク上のデータが更新され、レジストリーや削除ファイル領域のより詳細な調査ができなくなるといったケースもあります。また、調査担当者が普段利用しているコンピュータで情報漏えい調査を行ったために、調査に用いられた漏えいリストのデータがハードディスクに残っていたのか、実際の漏えいルートになったことの証跡なのかが、分からなくなるといった場合もあります。調査分析においては、真っ先に全ての調査対象の証拠保全を適切に行うことが重要です。

漏えいデータの回収

情報漏えいの被害者にとって、漏えいしてしまった情報の行き先を特定、回収し消去して欲しいと願うのは当然のことと言えます。しかし、ひとたび社外に情報を漏えいし、名簿業者やカード不正利用者の手に渡ってしまった場合、漏えい情報の全てを回収できる見込みは、残念ながら低いと言わざるをえません。判明した漏えい情報の拡散先と任意交渉を行うことになりますが、強制力があるわけではないため、回収に応じてくれるか否かは相手次第となります。また、情報、データというものの性質上、無数に複製が可能で、複製された数を知る方法がないため、回収したとしても拡散が完全に防止できるわけではありません。こうした現実を踏まえ、被害者に対しては、誠実に対応する必要があります。

「他にないこと」の証明

調査担当者は、行為者から自供が得られ、ログや各種の証拠からも漏えい経路が特定されたところで、「調査の目的は達成された」と考えるかもしれません。しかし、ここに落とし穴があります。ステークホルダーが真に望んでいるのは、「漏えいした全データがどの範囲で、事件の全容はどうであって、それ以外は問題がなかった」という報告であって、「調査の結果、最も疑わしい仮説の1つが立証された」という報告ではないのです。実際の漏えい事件においても、行為者の証言と各種証拠が一致したため、調査結果の報告を行った後に、余罪が判明して再調査を行うという例もあります。もちろん、完全に「ないこと」を証明するのは、原理的に不可能なのですが、報告に当たっては、行為者の余罪や、類似の不正の有無を「可能な限り」徹底して調査する必要があります。

こうした見落としを生じやすくするのが、「確証バイアス」と呼ばれる心理作用です。担当者は、調査開始にあたり、それまでに既に得られている限られた情報から「最も疑わしい仮説」を立てます。そして、「確証バイアス」の影響で、無意識にその仮説と整合する情報を中心に集め、その仮説を肯定するような解釈を行う傾向にあります。結果として、調査により得られた情報で仮説を修正する機会を失い、大きな見落としを生じるリスクを負うことになります。こうした事態を避けるためには、調査開始に当たって、判明している情報から可能性のある仮説シナリオを全て洗い出し、これらの仮説を調査から得られる情報によって「否定」していく、というアプローチを念頭に置く必要があります。

ステークホルダーへの報告

ステークホルダーに対して報告するタイミングは、大別すれば、情報漏えいが発覚した直後に行う情報漏えい発生の報告、調査完了後に行う調査報告、およびその間に必要に応じて適宜行う経過報告があります。

報告におけるひとつのジレンマは、情報の正確さと、報告の迅速さが、トレードオフの関係にあることです。まず最優先して報告すべき対象は、実害を被る可能性のある被害者です。しかし、情報漏えい発生が認識されてから、正確な被害実態が把握されるまでには、相応の時間がかかります。漏えいした情報の種類や被害範囲の可能性すら不明な状態では、報告すべき対象すら明らかになりませんし、正確をきすため、報告までに時間がかかり過ぎた場合、情報の隠蔽や初動対応の遅れを疑われるなど、透明性、誠実性の欠如と捉えられかねません。

情報漏えいが発覚した際には、速やかに被害が生じる可能性のある範囲を特定する事に全力を尽くします。そして、発覚の経緯と併せて、被害者となり得る顧客、関係者らに、漏えいした情報の内容と、想定されるリスクを併せて報告し、注意喚起を行います。第一報については速やかに行う必要があります。具体的なタイムリミットは一概には言えませんが、GDPRの施工により個人情報の侵害が発生した場合、検知後72時間以内に監督機関への報告が義務づけられたことを鑑みると72時間以内というのが一つの目安と言えるでしょう。第一報およびその後の報告において、もっとも犯しやすい間違いは、漏えい範囲を過小に見積もって報告してしまうことです。調査を十分に行うことができない段階で、あるいは調査を行っても証跡が十分に得られず、漏えいデータの全容が明らかにならないまま報告を行う場合があります。せめて漏えい可能性の範囲を絞り込むことができればいいのですが、「最大の可能性は、全顧客データ」ということは、めずらしくありません。報告した際に与えるインパクト、レピュテーションを想像すると、より少ない被害範囲を報告したいと強く思うことでしょう。しかし、調査分析を都合よく解釈し、漏えい範囲の可能性を過小に報告することは、絶対に避けなければなりません。実際、漏えい件数を過小に見積もった報告を行い、後に報告と異なる範囲から被害が発生し、調査の信頼性が根本的に損なわれ、監督官庁、ステークホルダーからの信頼喪失の影響が大きく、第三者を入れて全面的な再調査を行ったケースが何件もありました。場合によっては企業の存続を揺るがす事態に発展しかねません。まずは、最大限の被害可能性範囲を報告し、調査によって漏えい範囲を絞り込むことができた場合は、被害範囲の訂正報告をしていくべきでしょう。

是正措置

情報漏えいの是正措置としては、直接的な原因となったセキュリティホールや運用上の問題を塞ぐ緊急対応策と、ガバナンスや組織的な問題、コンプライアンス教育等を含めて全体を見直す抜本的な対策とに大別されます。まずは発覚後、速やかに、情報漏えいを可能にした原因を是正し、未だに継続して漏えいが発生している可能性や、新たに情報漏えいが発生する可能性を払拭する必要があります。一方で、抜本的な対策は、ガバナンスの確立と内部統制の整備が基本となります。権限者による不正行為は、アクセス制御等のセキュリティによって防ぐことはできませんし、内部統制の隙をついて行われることが多く、いくらルールを厳格化しても、業務の非効率が生じるのみで、効果的な不正防止には繋がりません。権限者の不正を防止するには、モニタリングによる抑止をうまく利用するのが効果的です。こうしたモニタリングを実施する場合でも、企業内に「どんな些細な不正も許さない」、「不正・不祥事リスクのコントロールは、価値ある活動である」といった意識が醸成されるようなガバナンスが確立され、内部統制とセキュリティが整備されていれば、モニタリングすべきリスクを最小化することができ、効率的・効果的に抑止することが可能となります。

KPMGの情報漏えい調査支援サービス

経験豊富な専門家が、仮説シナリオの洗い出し、調査ロジックの策定、漏えいデータ特定の統計的情報分析、デジタルフォレンジック技術による証拠保全、漏えい経路の調査分析、インタビューやログ分析による行為者の特定など、調査指針のアドバイスから専門技術を用いた分析まで、総合的に調査をサポートします。

広報支援サービス

情報漏えい被害のリスク分析、ステークホルダーの状況などに基づき、最適な情報開示（内容、方法、タイミング等）について、アドバイスを行います。具体的な例としては、開示内容のレビューによる、リスクを含む表現や不正確な表現の回避、重要顧客への説明に帯同し、アドバイザーとしての補足説明を行うなど、必要に応じて支援します。

再発防止策支援サービス

情報漏えい調査支援を通して収集した情報から、漏えい事件の発生原因およびセキュリティおよび内部統制の脆弱性を把握し、緊急是正措置と根本的な再発防止策の策定および実行を支援します。

本リーフレットで紹介するサービスは、公認会計士法、独立性規則及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。詳しくは株式会社 KPMG Forensic & Risk Advisoryまでお問い合わせください。

株式会社 KPMG Forensic & Risk Advisory

T: 03-3548-5773

E: FRA-Contact@jp.kpmg.com

kpmg.com/jp/fra