連載 第6回

リスクトピックをわかりやすく解説

企業リスクの現場

情報漏えいについて考える

トーマツ企業リスク研究所 研究員　**鳥越 しほり**

～ある日の社長室～

「社長、当社のお客様情報が漏れた可能性があります!」

ある朝、徳山社長が執務室でメールをチェックしていると、総務の吉田部長が飛び込んでくるなり悲鳴のような声を上げた。

外部委託先であるテクノIT社から、新製品であるサプリメントのモニターアンケートデータが保存されたUSBメモリを紛失したとの一報が入ったのだ。外部に漏えいした可能性を考えると、お客様へどれ程の影響を与えてしまうのかが気がかりだ。

早速緊急対策室を設置し、総務の吉田部長、情報システム部の木原部長、中田監査室長に加え、テクノIT社の社長と管理部長を招集して状況を把握することとした。

登場人物　企業リスクの現場


徳山社長

オーナー社長　64歳
- 大矢部長、前島主幹が勤める食品会社の社長。
- 長らく社長を務めてきたが、後継者育成がここのところの課題。


中田監査室長

海外子会社社長も経験している　48歳
- 海外強化の流れから白羽の矢が立つ。
- 内部監査は初心者であるが、ゼネラリストとしてのバランス感覚と愛社精神で、奮闘中。


吉田総務部長

吉田総務部長　42歳
- 総務部長歴一年目。この春から着任。
- 何事も一生懸命な姿勢は回りから高く評価されている。


森社長

テクノIT社 森社長　40歳
- 一代でテクノIT社を築いた企業家。
- 情報システム部の木原部長とは5年ほどの付き合い。


李須久先生

大手監査法人勤務のコンサルタントで公認会計士　徳山社長と同級の64歳
- 徳山社長の旧知の友で、リスクマネジメント・ガナバンスの第一人者。様々に知見がありいろいろな相談にのることとなる。


木原情報システム部長

情報システム設計をこよなく愛す45歳
- ITの最近の動向について知りたいとは思うものの、日々の業務でなかなか知識のアップデートの時間がないのが悩み


寺田管理部長

テクノIT社 寺田管理部長　38歳
- 創業時から森社長を支え、2年前より現職。
- 責任感が強く、対応は真摯。

徳山社長　当社の顧客情報が漏えいした可能性があるとのことだが、まずは状況を整理しよう。事の経緯から教えてくれないか。

徳山社長が吉田総務部長に回答を求めると、吉田総務部長は一呼吸おいてから説明を始めた。

吉田総務部長　はい。今回の新製品のモニターアンケート情報は、マーケティングシステムで管理しており、マーケティングシステムの運用管理はテクノIT社にお願いしております。ところが今日の朝になって、テクノIT社の寺田管理部長から、当社のマーケティングシステムのデータが保存されたUSBメモリを紛失したとの連絡を受けました。状況によっては、外部への漏えいの可能性もあると考えられます。テクノIT社からは、情報セキュリティポリシーや個人情報保護方針を定め、お客さまのデータの取扱いは厳重に管理していると聞いていたのですが、この様な事態となってしまいました。

徳山社長　現段階で情報漏えいは確認されているのか?

吉田総務部長　これまでのところ、幸いにもお客さまや外部から当社の情報が漏えいしたとの連絡は受けておりません。ただ今回の新製品のアンケートは、継続的に試していただく必要があることから、モニターの方々5,000人分の住所、電話番号に加え、生年月日や既往歴、クレジットカード情報も含まれております。こういった情報が含まれていることを考えますと、仮に漏洩していた場合には事態はかなり深刻かと…。

テクノIT社 森社長　この度はこのような事態を引き起こしてしまい、誠に申し訳ありません。。。実は昨日マーケティングシステムに不具合が生じまして、テスト環境で原因分析と障害対応を行いました。その際、テスト用のデータとして、USBメモリを用いて本番データを移行し使用した様でございます。ところが、今朝になってそのUSBメモリの現物確認ができていない事がわかりました。
担当者はデータ移行作業終了後、同僚に依頼して所定の管理ボックスに返すように依頼したとのことで、預かった人間に聞くと規定通りボックスに返したとのことでした。その後、担当者がデータの削除漏れに気づきUSBメモリを探したのですが所定の管理ボックスになく、フロア中を探してみてもどうしても発見できず、誤って廃棄した可能性もあると考えゴミ箱やビルのゴミ収集場まであさったものの発見に至りませんでした。
このUSBメモリは貴社のマーケティングシステムの管理業務専用でして、先ほど森部長からご説明のあったとおり、モニターの氏名、住所、電話番号、生年月日と既往歴、それとクレジットカード情報が約5,000名分含まれております。USBメモリは暗号化されているため、仮に、第三者に拾われてもそのままでは読み込めない仕様になっています。とは言えこのような事態を起こしてしまい、弁解の余地もございません。。。

テクノIT社　森社長は深々と頭を下げた。

木原情シス部長　暗号化されていると言っても安心はできないかもしれません。暗号化のパスワードを知っているか、知らなくとも解読できる技術も現に存在しますからね…。
ちなみにテスト用データではなく本番データをマスキングせずに使用されたということは、何か必要性があったのでしょうか?

テクノIT社 森社長　ご指摘はごもっともです。緊急対応で急いでいたこともあり、本番環境のデータと同等のデータを用意するのが難しかったため本番データを使用してしまいました。またマスキングについても、大変恐縮ながら緊急対応を優先するあまり対応できて

おりませんでした。本当に申し訳ありません。
作業が完了した時点でテスト環境のデータ削除は行いまして、USBメモリのデータも削除する手順でしたが、実際には削除されておりませんでした。完了手順書をチェックする際に本人が気付いてあわてて削除しようとしたのですが、気付いた際にはUSBは所定の場所になく、それからばたばたと捜索をしたのですが見つからなかったという次第です。

徳山社長　おおよその事の次第はわかった。今まずすべきは、引続きUSBの捜索を続けることと、該当のモニター5,000名の方々へ早急に連絡をとることかと思う。

中田監査室長　どのような情報を紛失しているかを文書で通知する必要がありますね。もし、情報漏えいが発生していたとしても、それに伴うお客さまの被害を最小限に抑えることにもなりますから。
書面は私のほうで早急に用意しますので、吉田部長、連絡体制の手配をお願いできますか?

吉田総務部長　わかりました、ぜひそのようにお願いします。書面の送付手配と、電話での一報連絡を早急にできるよう整えます。

テクノIT社森社長　本当に、この度はご迷惑をお掛けいたしまして申し訳ございません。私どもは引続きUSBメモリの捜索に注力致します。

― 30分後　会議室にて―

木原情シス部長　本当に見つかってよかったです。まさか昨晩作業にあたった方のデスクから出てくるとは。USBを取り違えて格納ボックスに収めたということだったんですね。。。今回は事なきを得ましたが、やはり抜本的に運用方法の見直しを行っていかなくてはなりませんね。

吉田総務部長　昨晩の行動を思い返し、社内関与者のデスク等も徹底的に調べた結果とのことでした。ログからUSBデータは外部媒体にコピー等されていないことも確認されたとのことです。

中田監査室長　今回は幸運にも見つかりましたが、そもそもあってはならない間違いですね。USBの運用方法含め、テクノIT社へ委託している業務の手順についても、今一度見直しを図り、今回のような一件が起きないような仕組み作りをしなくてはなりません。

木原情シス部長　当社が関与している委託先はテクノIT社だけでもないですからね。
情報管理体制や外部委託先管理方法をあらためて見直す必要があると思います。紛失などの事故だけではなく、中田監査室長がおっしゃったように、情報流出を防ぐ仕組み作りを早急にしなくてはなりませんね。私も情報システム部長として今回の一件は真摯に受け止めなくてはなりません。

中田監査室長　今後の内部監査においては、情報管理体制や外部委託先管理について、規程やルールどおりに業務が実施されているかだけではなく、規程やルールが十分にリスクをカバーできているか、という視点ももって内部監査を実施する必要がありますね。。

吉田総務部長　お二方ともお力添えいただき本当にありがとうございました。報告も兼ねて、早速社長に進言してみましょう。

―さらに後日、会議室にて―

徳山社長　李須久先生、お忙しいところお時間をいただきましてありがとうございます。先日、あやうく我が社に顧客情報漏えい事件が発生しそうになりました。外部への漏えいにはいたらなかったのですが、今後、同様の事件・事故が起こらないように、改めて、我が社の情報漏えい対策の状況を整理したいと考えております。

李須久先生　承知しました。顧客情報の漏えい未遂事件とは、大変でしたね。

徳山社長　はい。緊急対策室を設置して、現状把握から顧客への対応などを検討していました。今回は幸運にも外部への情報流出には至りませんでしたが、これを契機に、意図的に情報を持ち出されるリスクに対しても対策を見直すことにしました。そもそも現状の当社の管理体制で、情報漏えいを防ぐための対策が十分なのかどうか、先生のアドバイスをお願いいたします。

李須久先生　日本では得てして不正に手を染めるような人はうちには居ない、不正を他人事と思う意識がありました。しかし最近では、誰もが不正に関与する可能性があるという前提に立って情報漏えい対策を実施される会社がとても増えてきています。
そういった内部不正による情報漏えいへの対策としては、もともと日常的な業務で個人データなどを利用していて、正規に権限がある方が漏洩に関与することをどう防止するか、ということなので、その対策はなかなか難しいものです。電子データが保存されている先の技術的なセキュリティ対策はどのような状況でしょうか?

木原情シス部長　弊社内のシステムユーザーは、所属する部門のフォルダしかアクセスできない仕組みです。ただ、マーケティングシステムもお客さまシステムも文書管理サーバも保守業務を委託していますので、委託先担当者もアクセスが可能です。

李須久先生　個人データのデータダウンロードなどは、システム利用者の皆さんが可能なのでしょうか?

木原情シス部長　社員では、データダウンロード機能は管理者クラスであれば利用が可能です。委託先は保守作業を行いますので、データベースに直接アクセスすることが出来ます。

李須久先生　では、管理者クラスの社員が、個人情報をすべてダウンロードしてUSBメモリにコピーして社外に持ち出すことは可能ですか?

木原情シス部長　・・・可能です。以前、USBメモリやMOなどの外部記憶媒体への書き出しを制限するセキュリティソフトを導入して、あらかじめ登録したUSBメモリでないと接続して書き出しできなくしたのですが、USB利用の申請がとても多く。。。今のマーケティングシステムや文書管理サーバ利用者の多くがUSBメモリを利用している状況です。セキュリティソフトが記録しているUSBメモリへの書き出しのログも多く、正直申し上げましてチェックが十分にできているとは言えない状態です。

李須久先生　ログ検証の際には、ログ解析ツールを利用したり、検証対象を絞り込むことが大切ですね。書き出しのログについても、今回の個人データにアクセス可能な方に限定をすれば、大幅に少なくなりますよね。

木原情シス部長　そうですね。早速見直してみます。

徳山社長　今回のテクノIT社のUSBメモリへのデータのコピーは、木原部長が検知できる事項だったのだろうか?

木原情シス部長　USBメモリへのデータのコピーのログは残っていると思いますが、委託先の作業内容のチェックまではできていません。
外部委託先の保守作業の中でデータの修正をお願いする場合もありますし、今回のように、システムエラーが発生したときには、その原因究明のためにデータを解析する場合もあります。実際の作業の際には、マーケティングシステムとお客さまシステムは当社のサーバ室に委託先の担当者が来て作業していますので、何の作業をしているかは把握しています。
ただし、文書管理システムは保守をお願いしている委託先からインターネット回線経由でいつでもアクセスできるようになっています。
少なくとも本番環境のデータへのアクセスや、ましてやコピーしての持ち出しなどが簡単にできぬよう、システム自体の修正は早急に着手する予定です。

吉田総務部長　それから個人情報にアクセスする際には、事前に申請を出してもらう手順です。
また、作業によっては持ち出す場合もありますが、これはまた別に申請を受け付け、持ち出した情報の削除の報告も受けています。
マーケティングシステムのシステム障害分析については、テクノIT社から個人情報へのアクセス申請書を受けておりましたが、データ削除の報告は受けていませんでした。

徳山社長　テクノIT社については、データのコピーと削除の管理をもっとしっかりとしていくことが必要だ。USBなどの記憶媒体を使用するにあたる制限も検討する必要があるな。他の委託先に関しても、管理に注力していこう。

木原情シス部長　肝に銘じます。

吉田総務部長

李須久先生　委託先の作業の管理は、これまで以上に厳格にしていく必要がありそうですね。文書管理システムの保守委託先は、いつでもインターネット回線を通じてアクセスできるとのお話でしたが、業務上可能であればリモートアクセスの設定を変更して、通常はアクセスを遮断しておき、作業時にだけ接続できるように設定するという手続にされたほうがいいですね。

木原情シス部長　そうですね。情報漏えい事件が起こってしまうと本当に取り返しがきかないですから、しっかりとチェックしていこうと思います。

李須久先生　不正は不正のトライアングル（機会、動機、正当化）への対応を高める必要があります。特にリスクの評価と対応、統制活動、モニタリングの徹底により、不正を抑止するということが必要です。それと同時に、正しい行動は報われ、不正行為は必ず摘発され、当事者は処罰されるというコンプライアンス意識、ひいては企業風土を高めることも重要です。

徳山社長　李須久先生、アドバイスありがとうございます。我が社の情報漏えいのセキュリティ対策の問題点と改善の方向性が見えてきました。

中田監査室長　これから内部監査でも、内部不正による情報漏えいを防止できる体制となっているか、しっかりチェックしていきたいと思います。

情報漏えい対策立案のポイント

- ●誰もが不正に関与する可能性があるという前提に立って検討すること
- ●内部不正による情報漏えいへの対策として、アクセス権を制御できる仕組みと運用を構築すること
- ●リスクの評価と対応、統制活動、モニタリングを徹底すること
- ●正しい行動は報われ、不正行為は必ず摘発され、当事者は処罰されるというコンプライアンス意識の高い企業風土を築くこと