連載：第12回

類型別戦略論 - 情報流出編

東京青山・青木・狛法律事務所 弁護士・法学博士
（ベーカー＆マッケンジー外国法事務弁護士事務所外国法共同事業）
井上　朗

1．総論

連載第12回目は、すでに解説した、『企業不祥事』を好機に変えるための条件論及び戦略論に基づく、類型別の戦略論の第４回目として、企業が管理している情報が流出する類型の『企業不祥事』を扱います。

現代社会では、企業は、実に様々な個人情報を扱っており、大量の個人情報が集積しています。個人情報は、通常、インターネットに接続しているコンピューターによりセキュリティをかけた上で管理されています。個人情報の管理システムが完璧であり、およそ、情報流出が発生しないという前提が確立されることが理想ですが、現在の技術水準を前提とすると、このような前提が確立できているとはなかなかいえないのが現状です。

しかも、企業に集積された個人情報がひとたび流出すると、その影響は広範囲に及ぶ可能性があります。

例えば、コスモ石油事件がその好例として挙げることができます。コスモ石油事件は、2004年４月８日及び12日、コスモ石油発行のクレジットカード会員から「身に覚えのない携帯電話の有料サイトの利用料金請求書が、債権回収業者を名乗る者から郵便で届いた」との問い合わせがなされ、情報流出が発覚したことに端を発します。流出した個人情報項目は、カードの種別、発券サービスステーション、カード番号、入会年月日、更新年月日、氏名、郵便番号、住所、電話番号、性別、生年月日、車検年月、自動車登録番号です。銀行口座番号及び暗証番号は流出していませんでした。しかしながら、情報流出件数は92万3,239件にのぼり、また、債権回収業者を名乗る架空請求が合計11件なされ、400万円もの被害が発生しました。なお、コスモ石油事件では、事件発覚後、コスモ石油は、2004年４月13日、速やかに対策本部を設置し、同月16日には捜査機関に、また同月20日には社外の専門調査機関にそれぞれ捜査を依頼し、同月21日には流出事故の公表に踏み切るなど迅速に対応をし、被害の拡大を防止しています。ただ、情報流出の原因については特定することができず、有効な再発防止策を打ち出すことで信頼回復に繋げることができたか若干の疑問が残りました。

このように、企業に集積された個人情報は流出してしまうとその影響が極めて広範に及ぶ可能性があり、戦略的な対応が必要です。影響の拡大をいたずらに招けば、不祥事により企業に発生するインパクトは高くなり、インパクトにより被ったダメージからの回復に時間がかかり、失敗から教訓を学んで収益拡大に繋げることがより難しくなるためです。

そこで、実際の問題発覚時に、どのように動けばよいのか、また、何に注意すればよいのか、以下、戦略の概要について解説します。

2．対応マニュアル

①情報集出の判明

情報流出型の『企業不祥事』が発生した際にも、情報の収集に迅速さが要求されることは言うまでもありません。

情報流出の態様は、従業員が顧客リストを電車内に置き忘れて紛失してしまったといった目に見えてわかりやすいものから、情報セキュリティを掻い潜って不正アクセスにより情報が流出したケースまで多種多様ですが、最も多いのが、従業員及び委託先の何らかのミスで情報が流出してしまう場合であり、また、情報流出が発覚するのも、従業員及び委託先の報告により判明するケースです。国民生活センターの調査結果でも同様の調査結果が出ています。そのため、平時のリスクマネジメントの一環として、情報流出が発生した場合には、即座に報告するよう、従業員及び委託先を教育する必要があります。情報流出の判明が遅れれば遅れるだけ、被害の拡大を招くことを想起すべきです。

また、架空請求を受けた被害者が、個人情報が流出しているのではないかとクレームしてくる場合もあります。無論、勘違いの場合も多いのですが、同時期に同じ業者から架空請求されたとか、見知らぬ業者からセールスされたといったクレームが数多くなされた場合には、情報が流出している可能性があるので、注意して分析する必要があります。

②緊急対策委員会の編成

情報流出型の『企業不祥事』が発生したことが明らかになった時点で速やかに緊急対策委員会を編成します。緊急対策委員会の発足後は、情報収集と判断権限を集中させる必要があります。

情報流出が発生した場合には、場合により、緊急対策委員会が主導的に調査を指揮する必要がある場合もあります。情報収集を受動的に待っていては、事実認定ができない場合がその例に該当します。緊急対策委員会が主導的に調査を実施する際に最も重要なのは、調査のスケジューリングであり、想定される流出原因と流出の対象になった情報の双方に対して調査を実施し、情報流出が実際に発生したのかどうかを、どのようなタイム感で特定するのか確定する必要があります。

③事実関係の確認

緊急対策委員会において正確な事実関係を確認できるかどうか、情報提供の一貫性を確保できる事実関係を把握できるかどうかが肝要であることは、情報流出型の『企業不祥事』でも変わるところがありません。

また、情報流出の事実が確認できた時点で、本人に対する通知を実施する必要があります。なお、本人に対する通知は情報が流出した可能性があると判断される場合にも実施する必要があります。本人が架空請求に応じて支払いをしてしまうなどの被害が発生する事態を須らくして防止する必要があります。情報流出型の『企業不祥事』発生時の対応では、緊急対策委員会において、情報流出がないことが断定できる場合以外は、早急に本人に対する通知に踏み切り被害拡大を防止することが重要です。

④公式見解の作成

連載を通じて解説してきたとおり、『企業不祥事』発生時の情報発信の基本にして生命線になるのは、情報提供の一貫性であり、情報提供の一貫性を実現できるかどうかが公式見解にかかっています。情報流出が発生した場合には、主務大臣等の役所や上場企業であれば証券取引所へ報告する必要があり、また、マスコミに公表する必要がある場合も少なくありません。情報流出型の『企業不祥事』について外部的な発信をする際に根幹を形成するのが、公式見解です。

⑤危機時のリスクマネジメントの実践

危機時のリスクマネジメントの目的は、『企業不祥事』によるインパクトの最小化と早期の収束化の実現です。インパクトの最小化を実現するためには、被害拡大を防止するとともに、事実認定が完了し、情報流出の事実が認識できた時点で、お詫び料の支払いを検討する必要があります。国民生活センターの調査結果によると、流出事故を起こした企業のうち31パーセントが自社等の商品又はサービスを贈呈したり、金銭を支払っているとのことです。なお、対応金額は、一人当たり500円から5,000円程度のようです。

⑥回復時のリスクマネジメントの実践

回復時のリスクマネジメントの目的は、『企業不祥事』により被ったダメージの早期回復です。ダ

メージを回復するためには、情報流出が発生した原因を明らかにし、原因を除去し、再発防止策を打ち出し、当該再発防止策を実行に移すことが必要です。再発防止策としては、例えば財団法人日本情報処理開発協会の運営するプライバシーマーク制度により、プライバシーマーク付与認定事業者となり、より厳しい情報管理保護等を実施していくことが考えられます。また、安全管理措置を個別的に講じる義務がある以上、従業員に対して、弁護士ら企業外の専門家に研修を依頼することも考えられますし、シミュレーショントレーニングなどにより危機管理訓練を実施することも考えられます。

3．近時の事例研究

冒頭で紹介したコスモ石油事件と並んで紹介に値するのがソフトバンクＢＢ事件です。

同事件は、2006年１月中旬頃に、ソフトバンクＢＢに対して、被疑者から個人情報の流出をほのめかす電話があり、その直後である2006年１月14日、ソフトバンクＢＢが管理する242人の顧客情報のプリントアウトが郵送で同社に送付されてきたことにより発覚したものです。

2006年１月21日、ソフトバンクＢＢの渉外担当者が被疑者と接触し、残りの顧客情報のプリントアウトを手渡され、これを同社の顧客データーベースと照合したところ、本物であることが判明しました。そのため、ソフトバンクＢＢは、2006年１月23日、242人の顧客情報が流出したことをプレス公表し、また、同月27日、警察に正式に被害届を提出しました。2006年２月11日、警察は被疑者を逮捕しました。

ソフトバンクＢＢは、2006年２月27日以降、本人に対して、個別にメール等での通知を開始し、また、同社の現会員及び解約者を含めて一律に500円相当の金員を送付しました。

流出した情報は、ソフトバンクＢＢで管理している住所、氏名、電話番号、申込日、メールアドレスで、同社で管理しているクレジットカード番号やパスワード、利用履歴といった信用情報は含まれてはいませんでした。しかし、流出件数は、660万件にも上るものでした。

情報流出の原因は、過去にソフトバンクＢＢで業務委託者としてシステム関連の業務に従事していたものが、同社のリモートメンテナンスサーバーへアクセスするためのアカウントとパスワードを恐喝犯人らに伝え、犯人らが同サーバーを経由して顧客データーベースに不正アクセスし、顧客情報を持ち出したことが原因でした。

なお、ソフトバンクＢＢは再発防止策を速やかに実行に移しています。すなわち、2006年３月18日、ソフトバンクＢＢは、ホームページ上で、「ＢＢセキュリティ」というセキュリティソフトを、同年９月末までの間会員が自由にかつ無料でダウンロードできるようにしました。また、本人による自己防衛のため、ヤフーＢＢの会員のメールアドレスを自由に変更できるよう無料変更を許容することにしました。

その後、ソフトバンクＢＢの会員からソフトバンクＢＢに対しては、損害賠償の支払いを求める民事訴訟が提起され、2006年５月19日、大阪地裁は1人あたり6,000円の損害賠償を命ずる判決を発令しました。なお、ソフトバンクＢＢ事件の情報流出件数は660万件ですので、ソフトバンクＢＢは396億円もの賠償義務を負担する計算になります。

4．まとめ

以上、企業不祥事を好機に変えるための条件論と戦略論について12回にわたり解説を致しました。

最近の事例が示すとおり、いわゆる『企業不祥事』という危機的状況が企業経営に及ぼすインパクトは看過できないものがあります。『築城10年、落城１日』と評されるように、『企業不祥事』は、対応を間違えると、長時間かけて築きあげた企業のブランドや信用をわずか１日で破壊してしまいかねません。このような事態が発生しないよう、コンプライアンスを徹底して、およそ『企業不祥事』が発生しない社内体制を作り上げるとともに、『企業不祥事』が発生した場合にも、企業に発生するインパクトを最小限にとどめ、『企業不祥事』から教訓を学んで収益拡大に繋げるための戦略、すなわち『企業不祥事』を好機に変えるための戦略の策定が必要であることが、皆様にご理解いただけたことと思います。

私の若干の分析が多少なりとも皆様のお役に立つのであれば幸甚の極みです。