

経営 Q & A

相談に答える人

ニュースビット(株)代表取締役
栗原 達也

顧客情報管理の留意点

Question

当社は、業歴 30 年の書店です。店舗は駅前にあり、営業時間は午前 8 時から午後 11 時までと他の店より長く、学生や主婦、会社帰りのサラリーマンや OL などの利用が多いです。

本の取り寄せ注文で蓄積したお客さまに関する情報は、約 7,000 件に上ります。最近、テレビや新聞などで「顧客情報の紛失」とか「顧客情報の盗難」といったニュースを、よくみかけます。どんなことに注意したらよいか教えてください。

Answer

- ・顧客情報の管理には、さまざまなリスクが伴います。
- ・顧客情報の流出を防止するためには、内的要因と外的要因に対する方策が必要です。
- ・顧客情報の収集・活用については、管理リスクとのバランスを考慮することが重要です。

1 個人情報保護法の知識

2005年4月から施行される個人情報の保護に関する法律（個人情報保護法）には、個人情報（生存する個人に関する情報で特定の個人を識別可能なもの）を取り扱う企業に対して、義務規定が設けられています。そのため、該当する企業はこれまで以上に適切な情報管理が求められることとなりました。

（1）個人情報取扱事業者の定義

個人情報の取扱者は「一般私人」「個人情報取扱事業者」「政令で定める小規模事業者等」の三つに大きく分類されます。このうち個人情報取扱事業者が同法の適用を受けることとなります。

個人情報取扱事業者とは、特定の個人情報を容易に検索できるデータベース等を事業で利用している者を指します。

ただし、国や地方公共団体、さらには過去6カ月以内のいずれの日においても、顧客情報の数が、5,000を超えていない場合は、個人情報取扱事業者から除外されます。

(2) 個人情報取扱事業者の義務

個人情報取扱事業者には、主に次の七つの義務が課せられます。

正確性の確保

利用目的の達成に必要な個人情報を正確かつ最新の内容に保つことが義務付けられます。

苦情処理

個人情報の取り扱いに関して、本人が申し出た苦情には、適切かつ迅速に処理することが義務付けられています。また、そのための苦情受付窓口の設置や苦情処理手順の策定など必要な体制を整備しなければなりません。

適正な取得と利用目的の通知

不正な手段による個人情報の取得は禁止されています。また、個人情報を取得した際、本人に対してすみやかに利用目的を通知、または公表しなければなりません。本人から直接書面で取得する場合は、あらかじめ利用目的を明示する必要があります。

情報開示等

保有している個人情報の利用目的や、情報の開示等に必要な手続きなどについては、提供者本人に公表しなければなりません。また、提供者本人から個人情報についての開示、訂正、利用停止などの求めがあれば、それに応じなければなりません。

利用目的の特定と制限

個人情報を取り扱うに当たって、利用目的をできる限り特定し、特定された利用目的の達成に必要な範囲を超えた利用を制限します。

安全管理措置

個人情報の漏えいや滅失を防止するため、必要かつ適切な安全管理措置をとらなければなりません。また、個人情報に接する社員や管理委託先の監督に努めなければなりません。

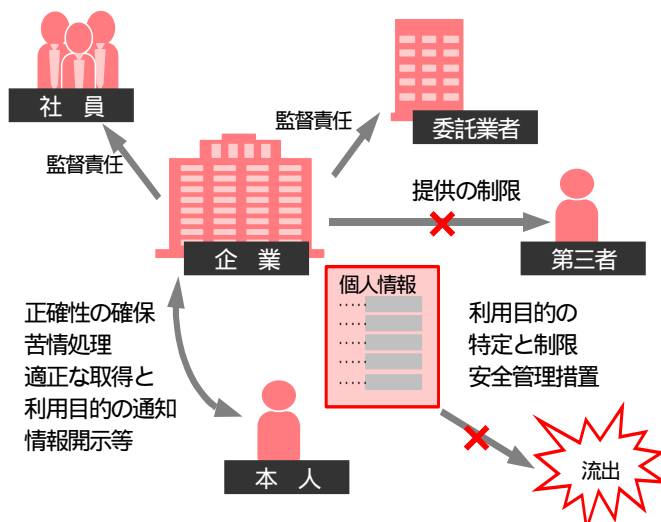
第三者提供の制限

本人の同意を得ずに個人情報を第三者へ提供することは、禁止されています。ただし、本人の求めに応じて第三者への提供を停止することにしていて、一定の事項をあらかじめ通知等をしている場合は、本人の同意を得ずに提供することができます。

また、個人情報を第三者に管理委託している場合や個人情報取扱事業者が第三者と合併等をする場合、さらには特定の者と共同で個人情報を利用する場合（一定事項の通知等を行っている場合）は、第三者提供とみなされません。

なお、主務大臣の命令に違反した場合は、6カ月以下の懲役または30万円以下の罰金、主務大臣への報告に関して違反した場合は、30万円以下の罰金となります。

図 - 1 個人情報取扱事業者の義務



2 顧客情報の流出によるリスク

政府が2004年7月6日に閣議決定した答弁書によれば、2001年4月から2004年5月までの約3年間で、情報の流出事件は官民合わせて378件に上ったということです。

顧客情報は、企業の売上を向上させるための重要な財産ですが、流出する危険と常にとり合わせであることを理解する必要があります。管理状況を今一度点検し、少しでも流出の可能性がある場合は、十分な対策をとることが重要です。

また、個人情報の不適切な管理によって負うことになるリスクは、個人情報保護法の罰則だけではありません。特に、個人情報が流出してしまった場合は、ほかにも次のようなリスクが考えられます。

プライバシー侵害による慰謝料の請求
流出した個人情報が利用された場合の賠償金の請求
社会的信用の失墜による事業への影響

また、万一顧客情報の流出が確認された場合や、流出の疑いがある場合は、それによる二次的な被害が発生する前に流出の事実を公表し、適切な対応をとることが企業に求められます。

3 流出要因別にみた情報管理の留意点

顧客情報の流出については、可能な限り防止する方策が必要です。

情報の流出は、外部からの要因が多いと思われがちですが、実は約8割が内部要因によるものといわれています。そのため、外部要因への対策だけでなく、内部要因への対策も講じる必要があります。

(1) 内部要因による流出

顧客情報を保持する企業内部の要因による情報の流出には、次のようなケースが考えられます。

社内関係者の持ち出しによる漏えい
情報の管理委託先からの漏えい
下請け企業などからの漏えい
誤操作（サーバーの設定ミス、電子メールの誤送信など）による漏えい
情報端末機器（ノートパソコンなど）の紛失による漏えい

こうした内部要因による流出を防ぐための対策をいくつか挙げましたので参考にしてください。

なお、すべての企業が、こうした対策をとることは難しいかもしれませんが、可能な範囲で対応するようにしてください。

顧客情報のデータベースは、立ち入りを制限した専用の部屋で管理する。
顧客情報のデータベースを操作できる担当者を特定の数人に絞り込む。また、操作作業は必ず複数名で行う。
情報管理に使用するパソコンの OS（基本ソフト）は、パスワードの設定ができるもの（例えば、Windows2000、WindowsXP Professional など）を使用する。また、誰でも使える共通のパスワードを発行しない。
データベースへのアクセス権をサーバーで設定し、データベース自体にもアクセスの制限をする。
データベースから印刷した顧客リストなどは、コピーを禁止する。また、不要となったリストの破棄は、必ずシュレッダーを使用する。
バックアップしたデータベースの保管を徹底する。
情報の管理委託先や下請け企業への指導を徹底する。
単純ミスを防止するための管理体制を構築する。
個人情報が入った情報端末機器は、原則として持ち出さない。

（２）外部要因による流出

外部要因による顧客情報の流出は、次のようなケースが考えられます。

顧客情報データの盗聴による漏えい
外部からの不正なネットワークへの侵入による漏えい

外部要因による流出を防ぐための対策は、以下のとおりです。

情報を収集する段階での盗聴や改ざんを防ぐ SSL（9 ページ参照）を設定する
データベースへの不正なアクセスを防止する

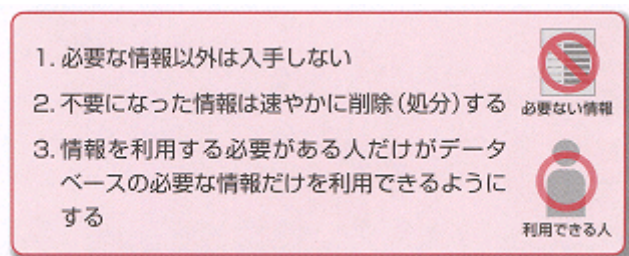
ただし、データベースへの不正アクセスを防止することは簡単ではありません。インターネットに接続されている限り、不正アクセスの危険性を排除することが難しいからです。

データベースと連動したウェブサイトは、サイトユーザーにとっても企業にとっても便利であることは説明しました。しかし、この場合、個人を特定できる情報やクレジットカード番号などのお金に関係するデータを扱うことが多いため、データベースの管理をセキュリティ専門会社に委託するなど、厳重な対策が必要となります。

4 情報管理のポイント

顧客情報は、管理するリスクを考えると非常にデリケートであるといえるでしょう。しかし、一方で活用するメリットが大きいことも事実です。そのため、顧客情報の「収集・活用」と「管理」のバランスをとる必要があります。蓄積した顧客情報は最大限活用するべきですが、不要となった顧客情報は削除するなど管理リスクを軽減することが大切です。

図2 情報管理のポイント



ITの普及によって、市場調査などの専門部署をもたない中小企業でも、顧客情報を生かした効率的なマーケティングが簡単にできるようになりました。

顧客情報を流出の危険から守る責任は、これまで以上に重いものとなっています。経営コンサルタントや弁護士など専門家の指導も仰ぎながら、万全の管理体制を整えておくことが大切です。