個人情報の保護

１．個人情報漏洩事件の頻発

最初の事件はというと、やはり最近新聞紙上をにぎわす個人情報の漏洩事件ではないでしょうか。読者のみなさんもお読みになって他人事とは思えないと頭を悩まされているのではないかと思います。ＡＤＳＬ接続サービス会社の事件では、何百万人という方の個人情報が流出したそうです。通信販売会社の事件も同様に大勢の方々の個人情報が流出しているそうですが、同性としてはやはり2年前にエステ会社から流出した個人情報が、未だにWinＭＸ等のファイル交換ソフトでファイル交換されているということは、非常に心が痛みますし、もし私が被害者だったらと考えると空恐ろしい気がします。

当事者の方々のご苦労はお察ししますが、このような被害者を増やさないために、そして何よりも「みなさんの会社が加害者にならないために」、個人情報漏洩事件を追ってみたいと思います。

この事件は、Ａ市が委託したシステム開発を受託した会社の孫請のアルバイト学生が持ち帰った約20万人分の住民情報データをＭＯにコピーして名簿業者に販売したというものでした。Ａ市側としては住民情報を持ち出された被害者であるはずが、最高裁まで持ちこまれたこの事件はＡ市に流出の責任を認めるという判断を下し、一人あたり1万5千円の損害賠償を命じています。

本来Ａ市としては、直接委託関係にないアルバイト学生にまで直接管理監督責任を負わないのではと思いますが、学生がデータを家に持ち帰って作業をすることをＡ市が認めていたため、実質的に管理監督下にあったとして責任を認められてしまったようです。

この事件の象徴的な点は、約20万人分もの個人情報が容易に持ち出されているということです。20万人分もの個人情報を紙で持ち出そうとすると、1ページに40人分の個人情報が記載されていたとしても5千ページにもなってしまい、ちょっとやそっとでは持ち出すことは出来ません。しかし、ＭＯなどの媒体ではそれを容易に持ち出せますし、作業場所からメールで送信してしまえば、何も持たずに個人情報を持ち出すことが可能になってしまうのです。

個人情報を預かる立場としては、大量の個人情報を容易に持ち出せる時代にあることを再認識する必要がありそうです。

ある協会のWEBサイトから個人情報が引き出され、その入手方法が公表された事件

この事件は、ある大学のＢ研究員がＣ協会のＷＥＢサイトで使用されているＣＧＩプログラムのセキュリティの脆弱性を突いてＣ協会に相談を寄せた方々の個人情報を不正に入手し、その入手方法をあるイベントで公表するとともに、その証拠として一部の方の個人情報を公開したというものです。現在Ｂ研究員は不正アクセス禁止法で起訴されているとともに、Ｃ協会から損害賠償請求訴訟を起こされています。

この事件の調査委員会の報告書によりますと、この事件の原因としてＣ協会がＣＧＩプログラムの採用にあたって十分なセキュリティのチェックを怠ったことと、必要以上に個人情報を収集していたことを、あげています。

この必要以上に個人情報を収集しないことという指摘は、インターネットビジネスを行なう上でとても重要な示唆だと思います。

以上二つの事件は、委託先からの漏洩、ＷＥＢサイトの設計ミスという違いはあるものの、どちらも誰が個人情報を持ち出したかということが特定できています。しかし、最初にあげましたADSL接続サービス会社の事件や通信販売会社の事件を始め、コンビニチェーンのカード会員の個人情報が流出した事件など、流出経路が特定できていない事件も数多くあります。

これらの他にも大きくは報道されていませんが、次のようなうっかりやＩＴの無知による事件が後を絶ちません。

(1)個人情報を保存したノートパソコンを電車の網棚に置き忘れた。
(2)個人情報を抹消せずにパソコンを廃棄し、個人情報が流出した。
(3)メールの同報送信にあたり、宛先をＢＣＣ欄でなくＣＣ欄に記載したため受信者全員にメールアドレスがわかってしまった。

２．個人情報保護法の成立－個人情報を保護する？

このような環境の中、昨年個人情報情報保護法が成立しました。この法律が完全に施行されるのは2005年の4月からですが、この個人情報保護法は、あくまでも企業（法律は個人情報取扱事業者）に求められる最低限の個人情報保護のルールを定めたに過ぎません。

上に書いた事件でおわかりのとおり、個人情報保護法が完全に施行されていなくても、個人情報を漏洩した企業のダメージははかりしれません。企業イメージの失墜はその最たるものですし、個人情報が流出した被害者への損害賠償（ADSL接続サービス会社の事件やコンビニチェーンの事件では一人あたり500～1,000円分の金券類が支払われたようです）、調査費用やそれらに要する人件費は膨大なものになります。

上の事件のように個人情報の流出事件では企業等における個人情報の安全管理措置が不十分であったことが個人情報の漏洩につながっており、インターネットビジネスでは、個人情報保護法を守るということは当然のことですが、個人情報を守るということがより重要だということを示唆しています。

＜個人情報保護法＞

第２０条（安全管理措置）
個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又はき損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない。
第２１条（従業者の監督）
個人情報取扱事業者は、その従業者に個人データを取り扱わせるに当たっては、当該個人データの安全管理措置が図られるよう、当該従業者に対する必要かつ適切な監督を行わなければならない。
第２２条（委託先の監督）
個人情報取扱事業者は、個人データの取り扱いの全部又は一部を委託する場合は、その取扱いを委託された個人データの安全管理が図られるよう、委託を受けた者に対する必要かつ適切な監督を行わなければならない。
以上が個人情報を安全に保護することを目的として定められた個人情報保護法上の条文です。
また先日（２００４年4月2日）閣議決定された個人情報保護法第7条第1項の規定に基づく「個人情報の保護に関する基本方針」では、個人情報取扱事業者に以下のことをさせて個人情報の保護を図ろうとしています。
(1)個人情報の保護方針（プライバシーポリシー）等を策定し、公表することにより対外的に個人情報を保護することを宣言すること。
(2)外部からの不正アクセス防御策、個人情報保護管理者の設置、内部者のアクセス管理や持ち出し防止策等の事業者内部の責任確保のための仕組みを整備すること。
(3)教育研修の実施などを通じて従業者に個人情報保護意識を徹底すること。

３．個人情報保護の具体的対策

個人情報をどのように保護するかと言いましても、個人情報を取得する時、保管しておく時、利用する時、廃棄する時、作業を委託する時と、その安全確保の方法は様々ですし、ビジネスの態様によって異なります。ましてや、上で述べました個人情報保護法の条文や政府の基本方針を読んでも、どのように個人情報を保護するかという答えはなかなか見出せません。
その答えは・・取り上げた事件の経緯や対処を見て行くとわかってくるような気がします。
例えばＡ市の事件であれば、学生に持ち帰って作業をさせなければこのような事件は起こらなかったかもしれませんし、Ｃ協会の事件では、ＷＥＢサイトを作る際に、採用するＣＧＩプログラムのセキュリティレベルを確認しておけば事件を防げたかもしれません。うっかりやＩＴの無知によって起こった事件は、個人情報の重要性やＩＴについて適切な教育をほどこしていれば、防げたかもしれません。政府の基本方針案でも取り上げられていますように、従業者に対する教育研修の実施は、必須のことでしょう。
事件にあった各社は、例えばADSL接続サービス会社のように再発防止策を公表している場合があります。この再発防止策も個人情報をどう保護するかの参考に非常になると思います。
みなさまの会社におかれましては、それぞれ企業風土ややり方がおありでしょうから、これらのことをそのまま展開するのはなかなか難しいと思われますが、次のようなことはぜひ検討された方が良いのではと思います。
(1)個人情報保護に関する社内の仕組みを作る
個人情報の保護に関する社内規定やマニュアルを作成し、個人情報保護管理者を始めとした組織を通じて社内周知を図る。
(2)個人情報を扱う場所、機器は物理的に安全な場所を選ぶ
個人情報を扱う居室やサーバー、パソコン等の機器の設置場所は、通常業務と切り離した場所とし、その入退室や使用状況については、アクセスログを取り、保存する。
(3)個人情報の運用は可能な限り安全な方法を選ぶ
個人情報にアクセスできる者を極力減らす。個人情報に誰がいつアクセスしたかログを取り、保存する。
(4)従業員への教育を行う
社内規定やマニュアルに基づく従業員の教育・研修を実施し、違反者には処罰があることを明確化する。
(5)業務委託先にも徹底する
委託先の個人情報の保護や管理義務が明確になっているか契約内容を再確認する。また、委託先が再委託する場合の条件についても十分確認する。
以上のことをされなかったからといって、それが直接個人情報の漏洩につながるわけではありません。しかし、先に書きましたＩＴの無知による個人情報の漏洩は、教育なくては防ぐことができません。個人情報のアクセスログを取らなければ、誰が持ち出したかわからないので、従業員や業務委託先は不正に持ち出してもわからないだろうと考えるかも知れません。
万一個人情報が流出してしまうと、
(1)どのように流出したのかを調べるための調査費用（有識者や弁護士を起用した調査委員会を設置すれば更に費用が生じます）。
(2)流出の事実を公表したり、調査経過を発表したりするための対外発表費用。
(3)謝罪広告等を新聞等に掲載する費用。
(4)情報が流出してしまった個人に対する補償（１００万人分流出してしまえば１人５００円としても５億円！！！）。

以上のような損失が発生しますが、最大の損失は長年かけて築いてきた企業イメージ・信頼の失墜です。一度失った信頼を取り戻すのは、大変なことです。
個人情報の漏洩事件では、個人情報を流出された被害者の方々にとっては、その個人情報を漏洩した企業が加害者です。「みなさんの会社が加害者にならないために」、今一度個人情報の管理状況を確認されてはいかがでしょうか？
本原稿は、これを利用する企業や個人の重大な経済的利益に関連する法律行為にかかわることが予想されますが、利用者は専ら自己の責任において本原稿をご利用頂きます。
些細な事実関係の違いが権利義務関係に影響を与えるため、様々な疑問点については、専門家に問い合わせることを強くお勧めします。
本原稿の内容は保証されるものではなく、利用者は本原稿の利用に起因して生じた一切の損害についていかなる請求をすることもできません。

個人情報の収集とその利用

１．個人情報の「収集」と「利用」

佐々木： では、さっそく今回のテーマである「個人情報の収集とその利用」についてお話を伺っていきたいと思います。
前回のご意見の中にもっと事例を紹介して欲しいという声があったのですが、インターネットビジネスにおける個人情報の「収集」と「利用」に関してはどのような事件があるのですか。
古田： あまりありません。実は個人情報の「収集」と「利用」については、公表されている裁判例は少ないのです。個人情報が流出や漏洩した場合は、被害が表に出るから問題になりやすいのですが、収集や利用のステップでは問題が表面化しないからです。
まず個人情報の「収集」は、インターネットでアンケートに答えるとか、懸賞に応募する時に自分の意思で氏名や住所を書き込むという、個人が任意に情報提供する場合がほとんどですから、事件として問題となることはほとんどありません。
次に個人情報の「利用」は、個人情報を一度提供してしまうとどのような利用がなされているのか外部からは知ることができず、本人が知ったならば文句を言いたいような問題も気付かれることのないままとなってしまう。だから、個人情報の「収集」と「利用」についてはあまり問題となっている裁判例などがないのです。
佐々木： そうですか。では今回のテーマでは特に問題はないということですか。
古田： いいえ、問題が表面化していないことと、問題がないということは、全く別問題です。
特にインターネットビジネスの場合には、ハッキング等により問題が表面化する可能性が高いのですから、問題を根本から解決する必要性が高いと言えます。
インターネットビジネスとはあまり関係ないのですが、参考になるケースがあるのでご紹介しましょう。

２．個人情報の「利用」が問題となった事例

古田： 外国要人による講演会を企画したある大学が講演会参加申込者の氏名、学籍番号、住所及び電話番号が記載された参加者名簿を、参加した人たちの同意を得ないで講演会の警備を担当する警視庁に提出したというケースがあります。大学が本人の同意を得ないで第三者提供という利用をしたということですね。
このケースでは、最高裁判所は、これらの行為がプライバシーの権利を侵害する行為に当たり、違法であるという判決をしました。佐々木さん、この判例はご存知でしたか。
佐々木： はい。平成１０年に中国の江沢民主席がいらしたときの件ですよね。昨年最高裁の判決が出て、新聞に大きく取り上げられていましたよね。最近はインターネットで検索するとすぐに情報が取り出せるので、新聞に出た後少し調べてみたので覚えています。
この件は東京高等裁判所の段階で２つの裁判所に係属して、出席者名簿の警視庁への提供を適法と判断した判決もありました。その理由としては、外国要人の警備・警護に万全を期すために個人情報を開示することは社会通念上許容されるというものでした。私個人としては、それなりに納得できる理由じゃないかという気もしましたが。
古田： しかし、最高裁判決では「提供についての承諾を求めることが困難だった事情はうかがわれないのに同意の手続きを取らなかった」点が重視されました。
佐々木： 個人情報を利用する場合には、できるかぎり承諾を求めなければならないということですね。
前回の個人情報漏洩事件では、自分に関する個人情報が、漏洩によってどこの誰に利用されているのか分からない点に空恐ろしい気がしました。
結局は、自分の個人情報がどのように利用されているのかを本人が把握できることが重要なのですね。
古田： そうです。大切なことは、個人情報を収集するときは利用目的を明示して収集し、その目的の範囲内に限って利用するということになります。２００５年４月から施行される予定の個人情報保護法第４章「個人情報取扱事業者の義務等」にも、この点は明示されています。
今回の大学は、本件があったためか以後の外国要人の講演会の参加者名簿の欄外に「参加者名簿を関係機関に提出することがある」旨注意書きしているそうです。

　個人情報を収集する側の立場から言えば、利用する可能性がある利用目的は列挙した上で個人情報を収集する、というのが以後のトラブルを避ける方策になると思います。個人情報保護法では、利用目的はあらかじめ公表しておけばいいのですから。
佐々木： 公表というのは、例えばホームページとかに書いておけばいいのですか？
古田： そうですね。まだ法律のこの部分は施行されていないので、どのように運用されるかはわかりませんが、ホームページにプライバシーポリシーを掲示して、その中で「当社はこのように取得した個人情報を利用します」というように表記するというのも利用目的の公表の一方策だと思います。
　ただ、インターネットを使えないような方の個人情報の利用目的についてまで、ホームページでの公表で十分かどうかは、議論を待たなくてはならないと思いますが。
佐々木： それはそうですね（笑）

３．個人情報とは

佐々木：ところで、先ほどのケースで出てきた学籍番号というのはそもそも個人情報として保護の対象となるのですか。
古田： いい指摘ですね。そもそも個人情報保護法でいうところの「個人情報」とは、生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）をいう、とされています。佐々木さん、学籍番号をこの定義に当てはめてみるとどうなりますか。
佐々木： 学籍番号は「他の情報と容易に照合することができ」ない限り、個人情報には該当しないということとなります。
古田： それじゃあ、大学にとってはどうでしょう？
佐々木： 大学にとっては、他の情報と容易に結びつけることができます。じゃあ個人情報になるのですね！
古田： いやちょっと待ってください。第三者にとってはどうでしょう？
佐々木： 第三者にとっては、学籍番号から特定個人を識別することは困難ですから、個人情報の定義には当てはまりませんね。ということは、個人情報とは非常に相対的なものだということですか。
古田： そうです。これは重要なポイントで、氏名と学籍番号を別個に保管しており、学籍番号の名簿のみが漏洩した場合には、情報の管理上の問題はもちろん生じますが、直ちに個人情報漏洩の問題にはつながらないということになるのです。
佐々木： そうなんですか！？
古田： ただ、これも物事を一面から見ているだけで、そうですね、例えば、漏洩したのが女子大の学籍番号の名簿だったとしましょう。
　もしメールアドレスが「学籍番号@大学名.ａｃ.ｊｐ」だったとしたら、その学籍番号を入手した者は、その入手したすべての女子大生に交際の申し込みのメールを送ることができるわけです。しかも無駄に男子大生にメールを送らずに、ですね。
佐々木： あっ！
古田： 確かにメールアドレスがわかったとしても、これで特定の個人を識別できるわけではありませんので、まだこれでも個人情報保護法上の個人情報の漏洩ということにはなりません。
　しかし、今の例のように情報管理上の責任を問われる可能性がありますので、インターネットビジネスにおいては、これは個人情報だから、大事に守らなくては、これはそうじゃないから適当でいいや、ということはありません。
佐々木： 良くわかりました。

４．個人情報の「収集」が問題となった事例

佐々木： では次に個人情報の「収集」についてお伺いしたいと思います。先ほど少しお話がありましたが、まずポイントとしては収集の際に利用目的を明らかにしなければならないということですね。
古田： そうですね。ただし、もっと大事なことがあるんです。事例をご紹介しましょう。
　平成１２年６月の千葉地方裁判所の判決で、ある会社が健康診断で採取した社員の血液を無断でＨＩＶ感染の検査を行ったことが違法だとされたケースです。
　判決では、事業主であっても、特段の必要性がない限り、ＨＩＶ抗体検査等によりＨＩＶ感染に関する従業員個人情報を取得し、あるいは取得してはならず、仮に、事業遂行のための労働衛生管理上の理由から、又は仕事に対する能力や適正判断のためなどから検査の必要性が合理的かつ客観的に認められる場合であっても、検査内容とその必要性を本人にあらかじめ告知し、その同意の上で行われるべきである、とされました。
　つまり、ＨＩＶ感染の有無という個人情報を取得する際には目的を通知して同意を得なければなりませんが、もっと大事なこととして、そもそも必要性と合理性がないかぎり、そのような個人情報を取得してはならないと判断されたわけです。
佐々木： なるほど、たとえ目的を明示して個人情報を収集しようとしても、そもそも収集することに必要性と合理性がなければならないということですね。
古田： そうです。

この事例は、ＨＩＶ感染という個人情報の中でも最も他人に知られたくない種類の情報、機微情報とか、センシティブ情報と言うこともありますが、それであったという側面もありますが、仮にＨＩＶ感染ほどの重要性がない情報であったとしても、目的達成のために不必要な情報を収集することは、たとえ本人の同意があったとしても控えるべきですね。

この事例でもう一つ注目すべき点は、このＨＩＶ検査を行った医療機関も本人の承諾なく検査を行うことだけでなく、検査の依頼主であるかないかにかかわりなく、検査結果を本人以外に知らせることは違法と判断されたことです。

佐々木： 本人の同意を得ないで第三者に個人情報を提供してはいけないということですね。

さて、企業の中には、顧客に関するあらゆる情報を集めてマーケティングに利用しようという向きもあると思いますが。

古田： しかし、先ほどお話したように、個人情報保護法の適用対象となるかぎり、個人情報の目的外の利用は原則として禁止されますから、個人情報を保有していても、自由に使用することはできません。

個人情報保護法の適用対象企業でない場合にも道義的には問題が残りますし、場合によっては前述の大学のように違法と評価されてしまうおそれもあります。

佐々木： 個人情報を保有するということは、個人情報漏洩のリスクを負っているということなんですね。

５．個人情報漏洩の慰謝料

古田： 前回も出てきた関西のある市の個人情報漏洩事件では、最高裁判所は、基本４情報（氏名、住所、性別、生年月日）を漏洩した場合、慰謝料は１人につき１万円と判断しました。

ＨＩＶ感染情報等の他人に最も知られたくない情報が漏洩した場合の慰謝料は、より高額となることは間違いないと思われます。

佐々木： 氏名、住所、性別、生年月日だけでも１万円ですね。２２万人の市だと２２億円ですか。個人情報漏洩のダメージは相当なものですね。

古田： ですから、リスク管理の観点からも不必要な情報はそもそも収集しないということが非常に重要なんですね。

６．まとめ

佐々木： 今回は、非常に重要なことが学べたと思います。

古田： インターネットビジネスはまだ、発展途上にあり、かつ、個人情報の収集と利用の問題は表面化しにくいために、未だ事件となっていないだけといえます。

インターネットビジネスでは、取引が直接会って行われるわけではないため、より多くの個人情報を収集する必要がありますし、不正な利用をしていることもハッキング等により明らかにされる可能性も高くなります。

インターネットビジネスでは、通常のビジネス以上に個人情報の収集と利用についてきちんとしなければならないかもしれません。

佐々木： そうですね。大事なことは、きちんと目的を明示して個人情報を収集し、本人の同意が得られない限りその目的以外には利用しないこと。

古田： そして、その大前提として、そもそも不必要な個人情報を収集しないことです。

佐々木： 古田先生、本日はどうもありがとうございました。

最後にもう少しお時間を頂戴して、前回のテーマに対するご感想の中に、「個人情報の保護は重要なことだとはわかるのだが、何をどうすれば良いのかわからない」というご意見があったのですが。

古田： そうですね、何から手をつければ、ということはとても難しいですよね。読者のみなさんの会社ごとにもちろん違いますし、どこまでやるかということもあると思います。

ここでは時間の都合があるので詳しくは無理ですが、一つは、個人情報の保護が適切にできているということを第三者的に認証する「プライバシーマーク」という制度があります。

このプライバシーマークを取得するかどうかは別として、取得のためのガイドブックの類が販売されていますので、これに従ってやってみるという手はあると思います。

また最近経済産業省から「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」が公表されました。これには個人情報を保護するために企業がしなくてはならないことがより具体的になっています。

個人情報保護法

第１５条（利用目的の特定）
個人情報取扱事業者は、個人情報を取り扱うに当たっては、その利用の目的（以下「利用目的」という。）をできる限り特定しなければならない。
（２項略）
第１６条（利用目的による制限）
個人情報取扱事業者は、あらかじめ本人の同意を得ないで、前条の規定により特定された利用目的の達成に必要な範囲を超えて、個人情報を取り扱ってはならない。
（２項以下略）

第１７条（適正な取得）
個人情報取扱事業者は、偽りその他不正の手段により個人情報を取得してはならない。
第１８条（取得に際しての利用目的の通知等）
個人情報取扱事業者は、個人情報を取得した場合は、あらかじめその利用目的を公表している場合を除き、速やかに、その利用目的を、本人に通知し、又は公表しなければならない。
（２項以下略）
第２３条（第三者提供の制限）
個人情報取扱事業者は、次に掲げる場合を除くほか、あらかじめ本人の同意を得ないで、個人データを第三者に提供してはならない。
一　法令に基づく場合
二　人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき。
三　公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき。
四　国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき。
（２項以下略）

著　：佐々木美咲
監修：弁護士法人古田アンドアソシエイツ法律事務所